



# **USER GUIDE REV2.5**

Software Version Number: 408.13 Version Date: January 30, 2020



## Table of Contents

1	INTR	ODUCTION	4
2	MAI	N FEATURES	4
3	SUP	PORTED WEB BROWSERS	4
4	LOG	IN INFORMATION	4
5	DAS	HBOARD	6
	5.1	GROUP VIEW	6
	5.1.1	Understanding the Dashboard- Group View Counts	15
	5.1.2		
	5.2	NODE VIEW	19
6	POLI	CY SETUP TOOL	29
	6.1	Defended Assets	.29
	6.1.1	User Defined Assets File Format	30
	6.1.2	2 Upload User Defined Assets File	30
	6.2	DEFENDED SERVICES	
	6.2.1	5 11	
	6.2.2		
	6.2.3	,	
	6.2.4		
	6.3	IDS RULES	
	6.3.1		
	6.4	AUGMENTATION	
	6.4.1		
	6.5	Active Triggers	
	6.6	PRECAPTURE FILTER.	
	6.6.1		
	6.6.2		
7	INVE	STIGATOR	
	7.1	CREATE SEARCH WORKFLOW	48
	7.2	Investigator Dashboard	50
8	SEAF	RCH	52
	8.1	Search Panel Overview	.52
	8.2	CREATING A NEW SEARCH	.65
9	VIEV	V METADATA	68
	9.1	Defended Alerts	71
	9.2	SuspDomains	
	9.3	SUSPSIG(JA3)ALERTS	
	9.4	MALWARE	
	9.5	SuspiPALerts	
	9.6	UNDEFENDEDALERTS	
	9.7	Active Triggers	
	9.8	FLOWS	
	9.9	DNS	-
	9.10	FILES.	
	9.11	НТТР	78
	9.12	SMB	79



	oundary 00, 2020
9.13 Email	
9.14 TLS/SSL	
9.15 VOIP	
10 REPORTS	84
11 CONFIGURATION	
11.1 Software Management	
11.1.1 License Management	
11.1.2 System Information	
11.1.3 Cluster Management	
11.2 AUTHENTICATION	
11.2.1 Local Authentication	
11.2.2 Remote Authentication	
11.3 AUTHORIZATION	
11.3.1 SSO, LDAP and RADIUS Authorization	
11.4 AUDITING	
11.5 System Events	
11.5.1 Generate Report	
12 NETWORK CONFIGURATION	
APPENDIX A: CLIENT SYSLOG CONFIGURATION PROCEDURES	102
APPENDIX B: LEEF MESSAGE FORMAT	
APPENDIX C: PCAP PORT INFORMATION	
APPENDIX D: BPF FILTER	
APPENDIX E: DECRYPTING PCAPS WITH SSL SESSION KEYS	442
APPENDIX F: UNDERSTANDING BEHAVIOR SEARCH	
APPENDIX G: UNDERSTANDING RULESETS	
APPENDIX H: FASTCOPY WORKFLOW	
APPENDIX I: TECHNICAL SUPPORT	
APPENDIX J: KEY TERMS	



Rev 2.0	Document Format and Design Revision	04/18/2018
Rev 2.1	Software update 408.10	11/1/2018
Rev 2.2	Software Update 408.11	3/12/2018
Rev 2.3	Software Update 408.12	5/1/19
Rev 2.4	Software Update 408.12_b13	8/26/19
Rev 2.5	Software Update 408.13	1/30/20

# **DOCUMENT REVISION HISTORY**



## **1 INTRODUCTION**

The SentryWire appliance captures and stores network traffic and analytics data from a live network interface at rates up to 100 Gbps (Gigabits per Second), and writes them to files without packet loss. SentryWire uses the standard PCAP file format to store network traffic.

SentryWire also has the ability to search captured network traffic by time and packet envelope data. Search and capture can be performed simultaneously, the 10G and 20G editions support the ability to create clusters, expanding upon the overall data storage and computational ability, when compared to a single standalone server.

## 2 MAIN FEATURES

- Use of the standard PCAP file format.
- High-performance packet-to-disk recording.
- Cluster-capable to increase capture data capacity.
- Real-Time indexing. This application is able to produce an index on-the-fly during packet capturing. The index can be queried using BPF search filters to quickly retrieve interesting packets in a specified time interval.
- Detailed insight and review of various alerts, conditions, events for intrusion detection, network security monitoring, and log management.
- Threat hunting and policy management.

## **3 SUPPORTED WEB BROWSERS**

The following web browsers support the SentryWire Application interface.

- Google Chrome 44.0.2403.157 or above.
- Mozilla Firefox version 45.0.1 or above.

## *Note*:

• There is no native support for chrome browser on CentOS system

## **4 LOGIN INFORMATION**

On any remote system connected to the network, open a supported web browser and enter the IP address using port number 41395 over https.

*For Example:* https://<IP Address>:41395



When the login screen appears, enter the username and password. The username and password is established during installation.

## Note:

- The account is locked after three failed login attempts in a ten minute period. The account is locked for 30 minutes. A system administrator can manually unlock the user account.
- If the system is configured to accept LDAP user/password, there is no default username/password. To login you must have a valid LDAP username/password.



## 5 DASHBOARD

The Federation Manager Dashboard is an interface that allows the users to configure groups and manage all Federated Nodes within the groups.

The dashboard has 2 display options:

- 1. Group View
- 2. Node View

The default view of the Dashboard is the Group View.

## 5.1 GROUP VIEW

View Nodes	Find Text	Group Details		IDS	ActiveTriggers		Suspicious Traffic		50	Events	Throughput	ntinuum Role:Admin A	Configuration	Performance
GroupName (NodeCo Boston (1) NewYork (1)	ount)	GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps (Click on data points zoom)
		Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526 0	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
		NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
		Total GroupCount: 2 NodeCount: 2	7 12 27609	50652 1070151	2 51	929 158	19235 0	1526 0	8084 0 1082057 744400	31 378 4	20.00 6.60 0	( 958.20 TB / 4.61 ) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Overview	1
			J						/44400					
			J					I	244400	U				
									744400				I	
			J						/******	U				

Figure 1-Default Dashboard Group View

The Group view dashboard displays the following:

- "View Nodes" button and Find Text search option. Clicking on "View Nodes" button shows the Federated Node view where each node's configuration, alert and storage information is displayed.
- UserName, License status and Authentication mode of the FM.
- Currently selected time interval and relevant data based on the selected option. The user can also change the duration of the data being displayed through the dropdown selection.

Note: Default Interval is "One Hour".

• Group Names and Node count per group.



## Notes:

- By Default, all groups are displayed in the FM.
- Any action performed on selected group from FM is applied to all the nodes included in the selected group only. If no group is selected, any action performed through FM applies to all groups in the FM.
- "+New Group" and "+New Node" buttons which allow the user to create new groups and add nodes to the groups. (Please refer to section 3.1.2 for more details)
- "Upload SigDetect Ruleset..." button at the bottom of the dashboard allows the user to upload SigDetect rules on Pcap data retrieved by searches for all the nodes that are part of the selected group.

## *Notes*:

- If no group is selected this action will be applied to all groups/nodes in the federation.
- This Rule file is separate/independent of the 50K rules enabled for capture going forward.
- To see search results with SigDetect rules, goto Search → Manager → Click on Log Data Hyperlink.

	Group Details		IDS	ActiveTriggers		Suspicious Traffic		DP	i Events	Throughput	Storage	Configuration	Performance
GroupName (NodeCount) Boston (1) NewYork (1)	GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	Max@bps Avg@bps DroppedPkts	(Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps (Click on data points to zoom)
	Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	
	NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	<u>]</u>
	Total GroupCount: 2 No Open	7 12	50652 1070151	2 51	929 158	19235 0	1526 0 ×	8084 0 1082057 744400	31 378 4 0	20.00 6.60 0	( 958.20 TB / 4.61 ) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Overview	<u>h</u>
	Crganize - This PC 3 3D Obje Desktop Downloo	New folder New folder New folder New folder New folder		*	Date mc 10/14/2019 3.11 1/2/2019 3.04 P	PM RULES	pe ^						
		File name:	0-		All Files     Open	Canc	v el						

Figure 2-Upload SigDetect

• The "Download SigDetect Ruleset" button on FM Dashboard downloads the SigDetect rules (if any) from the FM Node itself.

*For example:* If FM has 2 groups, 1 with 10 nodes including the current node and the other with 2 nodes. Upload SigDetect Ruleset option allows the user to upload to nodes of group1 or group2 or both. Download SigDetect Ruleset will download the last valid copy of SigDetect ruleset from the FM node itself.



	Group Details		IDS	ActiveTriggers		Suspicious Traffic		DP	Events	Throughput	Storage	Configuration	Performance
OroupName (NodeCount) Boston (1) NewYork (1)	GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps (Click on data points t zoom)
	Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526 0	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
	NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
	Total GroupCount: 2 NodeCount: 2	7 12 27609	50652 1070151	2 51	929 158	19235 0	1526 0	8084 0 1082057 744400	31 378 4 0	20.00 6.60 0	( 958.20 TB / 4.61 ) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Overview	1

Figure 3-Upload Sig Detect Ruleset

• "Pause Servers" and "Resume Servers" buttons which allow the user to pause or resume all servers with just one click action.

*Notes*:

- This is a global action and applies to the selected group only. If no group is selected, this action applies to all groups.
- If one or more of the nodes receiving the Pause Server message are already paused, this new request does not change the state of the servers. Each Paused server stays paused. Each server in running state will be paused.
- If one or more of the nodes receiving the Resume Server message are already running, this new request does not change the state of the servers. Each running server stays running. Each server in paused state will be resumed.
- The Group Details panel provides a quick insight into the selected group's aggregated data, events, alerts, throughput, storage, configuration and performance stat.

The **First column "Group Details"** provide the group name and the count of the nodes present in that group.

The Second column IDS has 2 subcategories:



View Nodes F	ind Text				Click						User:co	ntinuum Role:Admin A	AutnMode:local	Interval OneHour
GroupName (NodeCour Boston (1) NewYork (1)	nt)	Group Details GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Suspicious Traffic Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	Max@bps Avg@bps DroppedPkts	Storago (Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Configuration Authentication Licensing PreCaptureFilter ServerStatus	Performance Throughput Obps (Click on data points t zoom)
		Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526 0	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	
		NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	<u>l</u>
		Total GroupCount: 2 NodeCount: 2	7 12 27609	50652 1070151	2 51	929 158	19235 0	1526 0	8084 0 1082057 744400	31 378 4 0	20.00 6.60 0	(958.20 TB / 4.61) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Overview	1

Figure 4-Dashboard IDS Column sub-categories

• **First** sub-category shows Services, Assets and Defended Alerts. Each of these are hyperlinked to pivot to their relevant screens.

## For example:

- Clicking on "Services" sub-category pivots to Policy setup->Defended services screen.
- Clicking on "Assets" sub-category pivots to Policy setup->Defended assets screen.
- Clicking on "Defended Alerts" sub-category pivots to View Metadata->Defended Alerts screen.
- **Second** sub-category shows Active Rules and Undefended Alerts. Each of these are hyperlinked to pivot to their relevant screens.
  - Clicking on "Active Rules" sub-category pivots to Policy setup->IDS rule screen.
  - Clicking on "Undefended Alerts" sub-category pivots to View Metadata->Undefended Alerts screen.

## Note:

• Total alerts generated is equal to the sum of Defended Alerts and Undefended Alerts.

The **Third column Active Trig**gers shows Rules that are defined by users for that group and Events generated as a result of these rules.

- Clicking on "Rules" pivots to Policy setup->Active Triggers screen.
- Clicking on "Events" pivots to View Metadata ->Active Triggers tab.



Find Text						Click								OneHour
		Group Details GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	ActiveTriggers Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxQbps AvgQbps DroppedPkts	Storage (CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Configuration Authentication Licensing PreCaptureFilter ServerStatus	Performance Throughput Gbps (Click on data points zoom)
		Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526 0	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
		NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
		Total GroupCount: 2 NodeCount: 2	7 12 27609	50652 1070151	2 51	929 158	19235 0	1526 0	8084 0 1082057 744400	31 378 4 0	20.00 6.60 0	( 958.20 TB / 4.61 ) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Overview	1
	deCount)		GroupName NodeCount Boston 1 NewYork 1 Total GroupCount: 2	Second         Second         Second         Second         Assets         Assets         Assets         Detended Aerts         Second         T <tht< th=""> <tht< th="">         T</tht<></tht<>	Second         Services         Activitius           GroupName         Asset         Undefinited Akers         Undefinited Akers           NodeCoult         12         50652         812762           NewYork         6         257389         206666           Total         7         50652         206666           GroupCount: 2         7         50652         1070151	Second)         Services         Activities         Rules           Boston         7         50652         2           1         12         812762         46           NewYork         6         257389         5           Total         7         50652         1           1         10666         257389         5           Total         7         50652         2           GroupCount:         12         1070151         5	Group Name (acCount)         Group Name (account)         Group Name (account)         Services (account)         Activitives (account)         Rules (account)         PAddresses           Boston         7         50652 1         2         2         158         2         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         2         158         158         2         158         2         158         2         158         158         2         2         158         158         2         2         158	Group Dutails         Group Dutails         103         Active Rights         Testics           B         Group Name NodeCount         Services Assets         Active Rules Undefended Aurts         Rules Events         PAddresses Domains         Domains           B         Boston         7         50652         2         2         19235           1         12         27609         812762         46         158         0           NewYork         4         50652         1         929         19235           1         20666         257389         5         0         0           Total         7         50652         2         929         19235           GroupCount: 2         7         1070151         51         158         0	Group Dutails         Group Dutails         153         Active Rugers         Colous Braffic           B         Group Manne         Services Assets         Active Rules Undefended Avers         Rules Events         IPAdetessees         Domains         JA3 Signatures JA3 Signatures           B         Boston         7         50652         2         2         19235         1526           1         12         27609         812672         46         158         0         0           NewYork         4         50652         1         929         19235         1526           1         6         257389         5         0         0         0           Total         7         50652         2         929         19235         1526           GroupCount: 2         7         50652         2         92         92         19235         1526	Group Dutails         Group Dutails         155         ActivityTiggers         Joint Training         Joint Training <thjoint th="" training<=""> <thjoint th="" training<=""></thjoint></thjoint>	Group Dutain         Group Dutain         Differential Sector Training         Active Training         Colors Training         Ortice Sector Training         Price Sector Trai	Group Details         Group Details         15 <sup>4</sup> Active Triggers         - Locus Traility         OP Reversion         OP Reversion         Throughput           0         0         5         Active Triggers         - Active Trigers         - Active Triggers	Bit Control         Concert Fail         Concert Fail </td <td>Orcep Details         Orcep Details         105         ActiveRules NoteCount)         ActiveRules Reserves         ActiveRules NoteCount         ActiveRules NoteCount         ActiveRules Reserves         ActiveRules NoteCount         Processes NoteCount         ActiveRules NoteCount         Acti</td>	Orcep Details         Orcep Details         105         ActiveRules NoteCount)         ActiveRules Reserves         ActiveRules NoteCount         ActiveRules NoteCount         ActiveRules Reserves         ActiveRules NoteCount         Processes NoteCount         ActiveRules NoteCount         Acti

Figure 5-Dashboard Active Trigger column Rules Events

The Fourth column "Suspicious Traffic" has three sub-categories:

_		Group Details		IDS	ActiveTriggers		Suspicious Traffic	Click	-	l Events	Throughput	Storage	Configuration	Performance
GroupName ( Boston (1	(1)		Services	ActiveRules		IPAddresses		$\geq$	Files Emails Netflows	TLS/SSL HTTP VOIP	MaxGbps	(Compressed Total / CompressionRatio) FirstPCAP LastPCAP	Authentication	Throughput Gbps
NewYork	rk (1)	OroupName NodeCount	Assets Defended Alerts	Undefended Alerts	Rules Events	IPAddresses IPAlerts	DomainAlerts	JA3 Signatures JA3 SigAlerts	DNS	Critical	AvgGbps DroppedPkts	ClusterNodeCount	PreCaptureFilter ServerStatus	(Click on data point zoom)
		Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526 0	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
		NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
		Total	7	50652	2	929	19235			31	20.00	(958.20 TB / 4.61)		-
		GroupCount: 2 NodeCount: 2	12 27609	1070151	51	158	0	1526 0	8084 0 1082057 744400	378 4 0	6.60 0	0 0 0 0 0 0 0 0 0 0 0	Overview	
		GroupCount: 2	12						0 1082057	378 4	6.60	2019-12-12 02:32:59 2020-01-02 17:50:00	Overview	
		GroupCount: 2	12						0 1082057	378 4	6.60	2019-12-12 02:32:59 2020-01-02 17:50:00	Overview	<u> </u>
		GroupCount: 2	12						0 1082057	378 4	6.60	2019-12-12 02:32:59 2020-01-02 17:50:00	Overview	

Figure 6-Dashboard Suspicious Traffic Column sub-categories

• **First** sub-category shows the count of Suspicious IP Addresses uploaded by the user for the group, and the IP Alerts generated due to the uploaded IP Addresses. Each of these are hyperlinked to pivot to their relevant screens.

- Clicking on "IP Addresses" sub-category pivots to Policy setup->Augmentation screen.
- Clicking on "IPAlerts" sub-category pivots to View Metadata->SuspIPAlerts screen.
- **Second** sub-category shows the count of Suspicious Domains uploaded by the user for this group, and the Domain Alerts generated due to the uploaded Domains.
  - Clicking on "Domains" sub-category pivots to Policy setup->Augmentation screen.
  - Clicking on "DomainAlerts" sub-category pivots to View Metadata->SuspDomains screen.
- Third sub-category shows the count of Suspicious (JA3) signatures uploaded by the user for this group, and the Signature Alerts generated due to the uploaded Signatures.
  - Clicking on "JA3 Signatures" sub-category pivots to Policy setup->Augmentation screen.
  - Clicking on "JA3SigAlerts" sub-category pivots to View Metadata-> SuspSig(JA3)Alerts screen.

The **Fifth column DPI Events** shows events generated by the DPI engine running on each node of the group. It has two sub-categories:

View Nodes Find Text	Group Details		100						Events	Click			Performance
GroupName (NodeCount) Boston (1) NewYork (1)	Group Details GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	ActiveTriggers Rules Events	IPAddresses IPAlerts	Suspicious Traffic Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPixts	Storage (Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Configuration Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps (Click on data points zoom)
	Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526 0	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
	NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
	Total GroupCount: 2	7 12	50652 1070151	2 51	929 158	19235 0	1526 0	8084 0 1082057	31 378 4	20.00 6.60 0	(958.20 TB / 4.61) 2019-12-12 02:32:59 2020-01-02 17:50:00	Overview	1
	NodeCount: 2	27609						744400	0		0		
	NodeCount: 2	27609						744400	0		0		
	NodeCount: 2	27609						744400	0	8	0		
	NodeCount: 2	27609						744400	0		0		

Figure 7-Dashboard DPI Events Column sub-categories

• **First** sub-category shows the counts for Files, Emails, Netflows, and DNS events. Each of these are hyperlinked to pivot to their relevant screens.



- Clicking on "Files" sub-category pivots to View Metadata-> Files screen.
- Clicking on "Emails" sub-category pivots to View Metadata-> Emails screen.
- Clicking on "Netflows" sub-category pivots to View Metadata-> Netflows screen.
- Clicking on "DNS" sub-category pivots to View Metadata-> DNS screen.
- Second sub-category shows the counts for TLS/SSL, HTTP, VOIP and Critical events.
  - Critical events counts are displayed in red.
  - Clicking on "TLS/SSL" sub-category pivots to View Metadata-> TLS/SSL screen.
  - Clicking on "HTTP" sub-category pivots to View Metadata-> HTTP screen.
  - Clicking on "VOIP" sub-category pivots to View Metadata-> VOIP screen.
  - Clicking on "Critical events" sub-category pivots to Configuration->System Events screen.

The Sixth column Throughput has three data elements:

	Group Details		IDS	ActiveTriggers		Suspicious Traffic		DPI	Events	Throughput	Storage	Configuration	Performance
GroupName (NodeCount) Boston (1) NewYork (1)	GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps (Click on data points zoom)
	Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526 0	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
	NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
	Total GroupCount: 2 NodeCount: 2	7 12 27609	50652 1070151	2 51	929 158	19235 0	1526 0	8084 0 1082057 744400	31 378 4	20.00 6.60 0	( 958.20 TB / 4.61 ) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Overview	1
								111100			J		
									•		1		
											1		
											3		

Figure 8-Dashboard Throughput Column

- MaxGbps: The maximum throughput of sum of the maximum throughput of the nodes.
- AvgGbps: The average throughput of sum of the average throughput of the nodes.
- **Dropped Packets**: The sum of each node's dropped packets of that group.

The Seventh column Storage has four data elements:



## Figure 9-Dashboard Storage Column

1	 Group Details		IDS	ActiveTriggers		Suspicious Traffic		DP	Events	Throughput	Storage	Configuration	Performance
GroupName (NodeCount) Boston (1) NewYork (1)	GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbpr (Click on data points zoom)
	Boston 1	7 12 27609	50652 812762	2 46	2 158	19235 0	1526 0	829 0 632016 553964	22 124 0 0	10 6.48 0	(605.12 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
	NewYork 1	4 6 20666	50652 257389	1 5	929 0	19235 0	1526 0	7255 0 450041 190436	9 254 4 0	10 0.12 0	(353.08 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 17:50:00 0	Details	1
	Total	7	50652	2	929	19235	1526	8084	31	20.00	(958.20 TB / 4.61 ) 2019-12-12 02:32:59	Overview	12 A
	GroupCount: 2 NodeCount: 2	12 27609	1070151	51	158	0	0	0 1082057 744400	378 4 0	6.60 0	2019-12-12 02:32:59 2020-01-02 17:50:00 0	Overview	
			10/0151	51	158	0	0	1082057	4		2020-01-02 17:50:00	Overview	
			10/0151	51	153	0	0	1082057	4		2020-01-02 17:50:00		
			10/0151	51	153	0	0	1082057	4		2020-01-02 17:50:00		

- **CompressedTotal** is the total compressed storage used up by the capture data and **CompressionRatio** is the current compression ratio. (Dividing compressed storage by compression ratio gives the actual storage size.)
- **FirstPCAP** of each group is the earliest First PCAP among all nodes of the group.
- LastPCAP of each group is the latest Last PCAP among all nodes of the group. This allows users to see the full duration of data of the group.
- **ClusterNodeCount** shows the sum of all cluster nodes of each node of the group.

The **Eighth column Configuration** provides information about the Authentication, Licensing, PrecaptureFilter and ServerStatus.

- Clicking on "Authentication" sub-category pivots to Configuration-> Authentication screen.
- Clicking on "Licensing" sub-category pivots to Configuration -> Software Management screen.
- Clicking on "PrecaptureFilter" sub-category pivots to Policy Setup-> PrecaptureFilter screen. The entire group information can be viewed by clicking on the Details...." hyperlink for that group.
- Clicking on "Overview..." gives the aggregated information of all selected group.



		Group Details		IDS	ActiveTriggers		Suspicious Traffic			DPI Events	Throughput	Storag	30	Configuration	-
GroupName (NodeCount) Boston (1) NewYork (1)		GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerta	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(Compresse Compressio FirstPC LastPC ClusterNod	AP AP	Authentication Licensing PreCaptureFilter ServerStatus	Click Throughput Gb (Click on data poin zoom)
	_	Boston	7	50652	2	2	19235	1526	829	22	10	( 605.12 TB	No. Solid Shines		-
		1	12 27609	812762	46	158	0		Detail	Is for Group Boston		0040 40 404	32-59	Details	1
								1		Status	Cour				
		NewYork	4	50652 257389	1	929	19235 0	Nor	ie Status	Up	1		3.43) 2:32:59	Details	1
		1	20666	201000			0	1416505	ie Status	Down	0		:50:00	O'trano	+++++++++++++++++++++++++++++++++++++++
									entication	Local	1		_		
		Total GroupCount: 2	7	50652 1070151	2 51	929 158	19235		entication	LDAP	0		4.61) 1:32:59	Overview	The
		NodeCount: 2	27609					Auth	entication	Radius	0		:50:00		+
								Lie	censing	Permanent	1				
								Lie	censing	Evaluation	0				
								PreCa	ptureFilter	On	0				
								PreCa	ptureFilter	Off	2				

Figure 10-Dashboard Configuration Column

The **Performance Throughput Graph** allows the user to view thumbnail view of each group's aggregated throughput as a graph. Clicking on data points of the thumbnail shows a dialog box with more detailed version of the graph.



Figure 11-Dashboard Performance Throughput Graph



## 5.1.1 Understanding the Dashboard- Group View Counts

In Group view the elements that constitute the policy and have same property are listed below:

- IDS.Services
- IDS.Assets
- IDS.Active Rules
- ActiveTriggers.Rules
- SuspiciousTraffic.IPAddresses
- SuspiciousTraffic.Domains
- SuspiciousTraffic.JA3Signatures
- Storage.CompressionRatio

The Policy Counts for these items are the max of the policy counts of all the nodes in a group.

*For example*: If node1 and node2 belong to group1, and node1 has 5 Defended Services while node 2 has 12 Defended Services, then the group1 count for defended services shows as Max(5,12) = 12.

In Group view the elements that show the additive property are listed below:

- IDS.DefendedAlerts
- IDS.UndefendedAlerts
- ActiveTriggers.Events
- SuspiciousTraffic.IPAlerts
- SuspiciousTraffic.DomainAlerts
- SuspiciousTraffic.JA3SigAlerts
- DPIEvents (Files, Emails, Netflows, DNS, TLS/SSL, HTTP, VOIP, Critical)
- Throughput (MaxGbps, AvgGbps, DroppedPkts)
- Storage.CompressedStorage

The Counts for these Event/Alert items is a summation of all nodes in the group.

*For example:* If node1 has 2000 Undefended Alerts and node2 has 1400 Undefended Alerts, and node1,node2 belong to group1, then group1's UndefendedAlerts column will be displayed as 2000+1400=3400.

In Group View following elements are handled as described:

- Storage.FirstPCAP/LastPCAP: Group's FirstPCAP is the earliest of the FirstPCAP values of its nodes and the LastPCAP is the latest of the LastPCAP values of its nodes.
- Licensing: Is displayed as count of nodes that are permanent and/or evaluation. To view the license count click on "Details...".
- Authentication: Is displayed as count of nodes that have local authentication or Radius or LDAP. To view the authentication count click on "Details...".



• PreCaptureFilter: Is displayed as the number of nodes within the group that have precapture filter on and number of nodes that have pre-capture off. To view the pre-capture count click on "Details...".

## 5.1.2 Add/Delete Federated Groups and Federated Nodes

## • Adding a Federated Group

- To add a new group, click on the "+New Group" button on the FM Group View Dashboard. This presents the user with a pop window. Fill in the necessary details and click "Add Group"
- Once the group is added, user can now add nodes to the newly created group.

	 Group Details		105	ActiveTriggers		Suspicious Traffic		040	Events	Throughput	Storage	Configuration	Performance
GroupName (NodeCount) Boston (1) NewYork (1)	GroupName NodeCount	Services Assets Defended Alerts	ActiveRules	Ruies Events	IPAddresses IPAlerts	Domains DomainAlerts	JAS Signatures JAS Signatures	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gops (Click on data points zoom)
	Boston 1	7 12 28368	50652 837964	2 46	2 163	19235 0	1526 0	820 0 598018 533395	22 124 0 0	10 6.91 0	(604.83 TB / 1.18) 2019-12-12 03:32:58 2020-01-02 18:38:02 0	Details	
	NewYork 1	4 6 12340	50652 265994	1 6	929 0	19235 0	1526 0	7495 0 450509	9 254 4 0	10 0.12 0	(352.28 TB / 3.43) 2019-12-12 03:32:58 2020-01-02 18:38:02 0	Details	
	Total GroupCount: 2 NodeCount: 2	7 12 28368	50652 1103958	GroupName(No spac		d Group ters allowed)			31 378 4	20.00 7.03 0	(957.11 TB / 4.61) 2019-12-12 03:32:58 2020-01-02 18:38:02 0	Overview	1
				Add Group				Cancel	0		0		
								Cancel	0	1	U		
									0	1		I	
			[						0	I		1	

Figure 12-Dashboard Add Federated Group

## • Adding a Federated Node to a Group

• To add a new FN to a group, click on "+New Node" button.

*Note*: You must have at least one group to be able to add a node.

- Select Group selection drop down and select the desired group.
- Enter the IPAddress, Username and Password of the node to be added.
- Click on "Add Node".
- If the username and password are correct, the node will be added.
- $\circ$  Once the node is configured, it is available to the user under the desired group.



View Nodes Find Text						idNode	group			User.co	entinuum Role:Admin A	uthMode:local I	nterval OneHour
	 Group Details		IDS	Group			enter de	etails or	1 Events	Throughput	Storage	Configuration	Performance
GroupName (NodeCount)		í l		Select Group		-				1	(CompressedTotal /		
Boston (1)		Services		IPAddress					TLS/SSL HTTP	MaxGbps	CompressionRatio) FirstPCAP	Authentication	Throughput Gbpt
NewYork (1)	GroupName NodeCount	Assets Defended Alerts	ActiveRules Undefended Alerts	eg.,107.168.1.1					VOIP	AvgGbps DroppedPkts	LastPCAP ClusterNodeCount	PreCaptureFilter ServerStatus	{Click on data points zoom}
	 Boston	7	50652	UserName					22	10	(604.88 TB / 1.18)		
	1	12	840173	Upor Name					124	6.37	2019-12-12 03:32:58	Details	
		30269		Password				_	0	0	2020-01-02 18:32:00		
				Personnt					0				
	NewYork	4	50652	-					9 254	10 0.12	(352.39 TB / 3.43) 2019-12-12 03:32:58	122.00	
	1	6 13152	263066	Cancel				Add Node	4	0.12	2020-01-02 18:32:00	Details	
				4					0		0		
	Total	7	50652	2	929	19235	1526	8316	31	20.00	(957.27 TB / 4.61)		74
	GroupCount: 2	12	1103239	59	163	0	0	0	378	6.49	2019-12-12 03:32:58	Overview	M
	NodeCount: 2	30269						997206 729158	4	0	2020-01-02 18:32:00 0		31111111

Figure 13-Dashboard Add Federated Node

## • Deleting a Federated Group or Federated Node

• To delete a **Group**, simply click on the delete button next to the group name.

## *Notes*:

- A group with a node entry cannot be deleted. All the nodes in the group must be deleted individually.
- This group->node association is symbolic. A node is never affected by removal from a group. Each removed node can then be added to other groups.



SentryWire #Dashboard  Vary Nodes Find Text	🖈 Policy Setup 🧃	▶ Investigator	Q Search 🛔	10.91.170.11 Group Boston		before it can be	removed.			Userco	Reports Conf		Help 🕞 Logout
GroupName (NodeCount) Boston (1) NewYork (1)	Group Details GroupName NodeCount	Services Assets Defended Alerts	IDS ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAderts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	OK Files Emails Netflows DNS	DPI Events TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	Storage (CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Configuration Authentication Licensing PreCaptureFilter ServerStatus	Performance Throughput Gbps (Cilck on data points to zoom)
	Boston 1	7 12 40148	50652 953022	2 51	2 258	19235 0	1526 0	807 0 526253 599373	22 124 0	10 7.06 0	(604.91 TB / 1.18) 2019-12-12 02:32:59 2020-01-02 18:23:00 0	Details	zoomj
	NewYork 1	4 6 18902	50652 263611	1 6	929 0	19235 0	1526 0	7456 0 430019 187430	9 254 4 0	10 0.12 0	(352.53 TB / 3.43) 2019-12-12 02:32:59 2020-01-02 18:23:00 0	Details	
	Total GroupCount: 2 NodeCount: 2	7 12 40148	50652 1216633	2 57	929 258	19235 0	1526 0	8263 0 956272 786803	31 378 4 0	20.00 7.18 0	(957.44 TB / 4.61) 2019-12-12 02:32:59 2020-01-02 18:23:00 0	Overview	h
+ New Group + New Node			ᆂ Upi	load SigDete	ect Ruleset	. 🛓 Down	load SigDet	ect Rulese	et			ause Servers	Resume Servers

Figure 14-Dashboard Delete a Federated Group or Node Warning

- To delete an existing Federated Node, select the group to which the node belongs. Then click on the "View Nodes" button at the top. This brings you to the "Node view" dashboard. Once in the Node view dashboard, the user can delete the desired node by simply clicking on the delete icon under the action column.
- $\circ~$  Once deleted, the Federation cannot monitor the node.

## Notes:

- A node can exist only in one group.
- When a group is removed, all the nodes in that group are removed automatically.
- Each removed node can then be added to other groups.



Boston nc_113	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses	Domains								
nc_113			LYVING	IPAlerts	DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps Duration: Past 15 minutes (Cilick on data points to zoom)	Act
10.91.170.113	7 12 28368	50652 837964	2 46	2 163	19235 0	1526 0	820 2 598018 533395	22 124 0 0	10 6.36 0	(604.88 TB / 1.18) 2019-12-12 03:32:58 2020-01-02 18:38:02 0	local Evaluation Off Running		Pa
NewYork nc_157 10.91.170.157	4 6 12340	50652 265994	1 6	929 0	19235 0	1526 0	7495 8 450509 186244	9 254 4 0	10 0.11 0	(352.28 TB / 3.43) 2019-12-11 23:12:51 2020-01-02 18:39:14 0	local Permanent Off Running	1	Pa
Total NodeCount: 2	7 12 28368	50652 1103958	2 52	929 163	19235 0	1526 0	8315 0 1048527 719639	31 378 4 0	20.00 7.03 0	(957.11 TB / 4.61) 2019-12-12 03;32:58 2020-01-02 18;38:02 0	Overview	l	
	12						0 1048527	378 4	7.03	2019-12-12 03:32:58 2020-01-02 18:38:02	Overview		

## 5.2 NODE VIEW

The Node view of the dashboard can be accessed by clicking on the "View Nodes" button. Node View allows users to view node details, pivot to other panels for policy, alerts, events and configuration. Authorized users can remove a node from being monitored and pause/resume individual node's capture server.



Services IP         Activity Assets         Activity Defended Alerts         Rules         PAddresses         Domainis         JA3 Signatures Desaniders         Flies         Titos Liss Material         MesoBpe Assets         (compresentation) / Instruction         Automation Proception Despendents         Automation Proception Despendents         Instruction Proception Despendents         Automation Proception Despendents         Automation Proception Des	Through Duration: Pa (Click on data)	Authentication Licensing PreCaptureFilter ServerStatus	(CompressedTotal / CompressionRatio) FirstPCAP		Events							
12         837964         46         163         0         2         124         6.36         2019-12-12 03 259         Evaluation 2020-01-02 18.380.2         Foundation Running           0.113	1 7	tion and h		AvgGbps	TLS/SSL HTTP VOIP	Files Emails Netflows	Domains		Rules	ActiveRules	Services Assets	Node Détails GroupName NodeName NodeIP
6 265994 6 0 0 0 8 254 0.11 2019-12-11 23:12-51 Permanent	4	Evaluation Off	2019-12-12 03:32:58 2020-01-02 18:38:02	6.36	124 0	2 598018					12	Boston nc_113 0.91.170.113
450509 4 0 2020 01-02 10:00.14 0#	1	Permanent Off	2019-12-11 23:12:51 2020-01-02 18:39:14	0.11	254 4	8 450509					6	NewYork nc_157 ).91.170.157
II         7         50652         2         929         19235         1526         8315         31         20.00         (957.11 TB / 4.61)           12         1103958         52         163         0         0         0         378         7.03         2019-12-12 03:25.88         2026-01-02 18:38.02         0         0         1048527         4         0         2020-01-02 18:38.02         0         0         111111111111111111111111111111111111		Overview					19235	929				Total

Figure 16-Dashboard Node View Node Details Column

This dashboard displays the following:

- "View Groups" button and Find Text search option. Clicking on "View Group" button switches the dashboard back to the group view where each group's aggregated configuration, alert and storage information is displayed.
- UserName, License status and Authentication mode of the FM.
- Currently selected time interval and relevant data based on the selected option.

*Note:* Default Interval is "One Hour". Interval drop allows users to change the duration of the data being displayed below.

• The Node view dashboard provides the following information:

## The First column displays the Node Details which includes:

• GroupName, NodeName and NodeIP.

## Notes:

- Only selected group's nodes are displayed in the first column.
- If one or more Federated Node servers are down/stopped or unreachable, the dashboard displays the NodeName and NodeIP in red.
- Only action that can be performed for a node that is down is "Delete"



Mem     Services     Active/list     Rules     PAlers     Domains     JA3 Signatures     Piles     TLSSL     Maratops     Compress/Data     Authentiann     Throughut       Definided Alerts     Definided Alerts     Definided Alerts     Definided Alerts     Definided Alerts     JA3 Signatures     Piles     TLSSL     Maratops     Compress/Data     Authentiann     Throughut       1     7     50654     2     2     19235     1526     500     22     10     Compress/Data     Docalina     Licensing       3     12     592583     40     205     0     0     22     124     6.50     2019-12/12/03/284     Evaluation     Evaluation       1113     23665	15 minutes Acti nts to zoom)
12         592583         40         205         0         0         2         124         6.50         2019-12-12:03:258         Evaluation           23665         23665         297483         0         0         2020-01-02:19:47:00         0         111           .113         .113         .115         .116         .117         .117         .117         .118	Pa
k         4         50652         1         929         19235         1526         4518         9         10         (102.85 TB / L00)         local           7         6         17447         5         0         0         8         254         0.45         2019-12:112:31:251         Permanent           1033         1033         286245         4         0         2020-01-02:8462:1         Off           157         117104         0         0         Down	Do
nt: 2 12 767030 45 2929 19235 1526 5018 31 20.00 (707.45 TB / 2.18) 23865 205 0 0 0 378 7.27 2019.12.120.32.59 23866 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	

Figure 17-Dashboard Node Details

The Second column IDS has 2 subcategories:

• **First** sub-category shows Services, Assets and Defended Alerts. Each of these are hyperlinked to pivot to their relevant screens.

## For example:

- Clicking on "Services" sub-category pivots to Policy setup->Defended services screen.
- Clicking on "Assets" sub-category pivots to Policy setup->Defended assets screen.
- Clicking on "Defended Alerts" sub-category pivots to View Metadata->Defended Alerts screen.



NodeName	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Click					Events	Throughput	Storage	Configuration	Performance	
Boston	-		Conce	IPAddresses IPAJerts	DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Obps Duration: Pest 15 minutes (Click on data points to zoom)	Acti
nc_113 10.91.170.113	7 12 2454	50652 1.91M	2 39	929 0	19235 0	1526 0	1350 2 615230 21699	22 124 0 0	10 0.14 0	(605.76 TB / 1.19) 2019-12-11 08:32:56 2020-01-01 01:57:15	local Evaluation Off Running	1	Pau
New York nc_157 10.91.170.157	4 6 0	50652 15291	1 39	929 0	19235 0	1526 0	9033 8 195548 395190	9 254 4 0	10 0.18 0	(355.90 TB / 3.46) 2019-12-11 16:00:00 2020-01-01 01:57:13	local Permanent Off Running	1	Pau
Total NodeCount: 2	7 12 0	50652 15292	2 78	929 0	19235 0	1526 0	10383 0 810778 416889	31 378 4 0	20.00 0.31 0	( 961.31 TB / 4.65 ) 2019-12-11 08:32:56 2020-01-01 01:52:25 0	Overview	1	

Figure 18-Dashboard Node View IDS Column sub-categories

• Second sub-category shows Active Rules and Undefended Alerts. Each of these are hyperlinked to pivot to their relevant screens. Clicking on "Active Rules" sub-category pivots to Policy setup->IDS rule screen. Clicking on "Undefended Alerts" sub-category pivots to View Metadata->Undefended Alerts screen.

Note:

• Total alerts generated is equal to the sum of Defended Alerts and Undefended Alerts.

The **Third column Active Triggers** shows Rules that are defined by users and Events generated as a result of these rules. Clicking on "Rules" pivots to Policy setup->Active Triggers screen. Clicking on "Events" pivots to View Metadata ->Active Triggers tab.



Noc Brockstein         10 model         Active Transmission           Servopklame         Assets         Undefended Alerts         Brockstein           Nocker         Assets         Undefended Alerts         Brockstein           Boston         7         50652         2           nc_113         2454         30           10.91.170.113         0         0	s CIICK	DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails	Events TLS/SSL	Throughput MaxGbps	Storage	Configuration	Performance
nc_113 12 1.91M 38 10.91.170.113 2454				Netflows DNS	VOIP Critical	AvgGbps DroppedPkts	(CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Obps Duration: Past 15 minutes (Click on data points to zoom)
		19235 0	1526 0	1350 2 615230 21699	22 124 0 0	10 0.14 0	(605.76 TB / 1.19) 2019-12-11 08:32:56 2020-01-01 01:57:15	local Evaluation Off Running	1
New York         4         50652         1           nc_157         6         15291         38           10.91.170.157         0         38	929 0	19235 0	1526 0	9033 8 195548 395190	9 254 4 0	10 0.18 0	(355.90 TB / 3.46) 2019-12-11 16:00:00 2020-01-01 01:57:13	local Permanent Off Running	1
Total 7 50652 2 NodeCount: 2 12 15292 7 0		19235 0	1526	10383	31 378	20.00 0.31	(961.31 TB / 4.65) 2019-12-11 08:32:56	Overview	1

Figure 19-Dashboard Node View Active Triggers Column Rules Events

The Fourth column Suspicious Traffic has three sub-categories:

- First sub-category shows the count of Suspicious IP Addresses uploaded by the user for that node, and the IP Alerts generated due to the uploaded IP Addresses. Each of these are hyperlinked to pivot to their relevant screens. Clicking on "IP Addresses" sub-category pivots to Policy setup->Augmentation screen. Clicking on "IPAlerts" sub-category pivots to View Metadata->SuspIPAlerts screen.
- Second sub-category shows the count of Suspicious Domains uploaded by the user for the node, and the Domain Alerts generated due to the uploaded Domains. Clicking on "Domains" sub-category pivots to Policy setup->Augmentation screen. Clicking on "DomainAlerts" sub-category pivots to View Metadata->SuspDomains screen.
- Third sub-category shows the count of Suspicious (JA3) signatures uploaded by the user for that group, and the Signature Alerts generated due to the uploaded Signatures. Clicking on "JA3 Signatures" sub-category pivots to Policy setup->Augmentation screen. Clicking on "JA3SigAlerts" sub-category pivots to View Metadata-> SuspSig(JA3)Alerts screen.



Node Details GroupName NodeName NodeIP							Click					AuthMode:local Interval	
	Services Assets Defended Alerts	IDS ActiveRules Undefended Alerts	Active Triggers Rules Evonts	IPAddresses IPAlerts	Suspicious Tranic Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	Throughput MaxGbps AvgGbps DroppedPkts	Storage (Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Configuration Authentication Licensing PreCaptureFilter ServerStatus	Performance Throughput Obps Duration: Past 15 minutes (Click on data points to zoom)	Activ
Boston nc_113 10.91.170.113	7 12 2454	50652 1.91M	2 39	929 0	19235 0	1526 0	1350 2 615230 21699	22 124 0 0	10 0.14 0	(605.76 TB / 1.19) 2019-12-11 08:32:56 2020-01-01 01:57:15	local Evaluation Off Running	1	Pau
New York nc_157 10.91.170.157	4 6 0	50652 15291	1 39	929 0	19235 0	1526 0	9033 8 195548 395190	9 254 4 0	10 0.18 0	(355.90 TB / 3.46) 2019-12-11 16:00:00 2020-01-01 01:57:13	local Permanent Off Running	1	Pau
Total NodeCount: 2	7 12 0	50652 15292	2 78	929 0	19235 0	1526 0	10383 0 810778 416889	31 378 4 0	20.00 0.31 0	(961.31 TB / 4.65) 2019-12-11 08:32:56 2020-01-01 01:52:25 0	Overview	<u>l</u>	
	12						0 810778	378 4	0.31	2019-12-11 08:32:56 2020-01-01 01:52:25	Overview	1	

Figure 20-Dashboard Node View Suspicious Traffic Column sub-categories

The **Fifth column DPI Events** shows events generated by the DPI engine running on each node. It has two sub-categories:

- First sub-category shows the counts for Files, Emails, Netflows, and DNS events. Each of
  these are hyperlinked to pivot to their relevant screens. Clicking on "Files" sub-category
  pivots to View Metadata-> Files screen. Clicking on "Emails" sub-category pivots to
  View Metadata-> Emails screen. Clicking on "Netflows" sub-category pivots to View
  Metadata-> Netflows screen. Clicking on "DNS" sub-category pivots to View Metadata-> DNS screen.
- Second sub-category shows the counts for TLS/SSL, HTTP, VOIP and Critical events. Critical events counts are displayed in red. Clicking on "TLS/SSL" sub-category pivots to View Metadata-> TLS/SSL screen. Clicking on "HTTP" sub-category pivots to View Metadata-> HTTP screen. Clicking on "VOIP" sub-category pivots to View Metadata-> VOIP screen. Clicking on "Critical events" sub-category pivots to Configuration->System Events screen.



Node Details GroupName NodeName NodeIP Do	Services Assets	IDS							Click			AuthMode:local Interval	
	Defended Alerts	ActiveRules Undefended Alerts	Active Triggers Rules Events	IPAddresses IPAlerts	Suspicious framic Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	Events TLS/SSL HTTP VOIP Critical	MaxObps AvgGbps DroppedPkts	Storage (CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Configuration Authentication Licensing PreCaptureFilter ServerStatus	Performance Throughput Gbps Duration: Past 15 minutes (Click on data points to zoom)	Action
Boston nc_113 10.91.170.113	7 12 2454	50652 1.91M	2 39	929 0	19235 0	1526 0	1350 2 615230 21699	22 124 0 0	10 0.14 0	(605.76 TB / 1.19) 2019-12-11 08:32:56 2020-01-01 01:57:15	local Evaluation Off Running	1	Paus
New York nc_157 10.91.170.157	4 6 0	50652 15291	1 39	929 0	19235 0	1526 0	9033 8 195548 395190	9 254 4 0	10 0.18 0	(355.90 TB / 3.46) 2019-12-11 16:00:00 2020-01-01 01:57:13	local Permanent Off Running	1	Paus
Total NodeCount: 2	7 12 0	50652 15292	2 78	929 0	19235 0	1526 0	10383 0 810778 416889	31 378 4 0	20.00 0.31 0	(961.31 TB / 4.65) 2019-12-11 08:32:56 2020-01-01 01:52:25 0	Overview	1	

Figure 21-Dashboard DPI Events Column sub-categories

The Sixth column **Throughput** has three data elements:

- MaxGbps: The maximum throughput of each node.
- AvgGbps: The average throughput of each node.
- Dropped Packets: The number of packets dropped packets of that node.

NodelName Nodel         Assis         Undefended Alerts         Events         IPAlerts         DomainAlerts         JAJ SigAlerts         Emails NAI SigAlerts         HTTP Netfores         Angdips Dropped/Pists         CompressionExtition Psylind-April ClassificApril         Propages Dropped/Pists         CompressionExtition Psylind-April         Psylind-April         Psylin	Authentication Licensing PreCaptureFilter ServerStatus (1 local	Throughput Gbps Duration: Past 15 minutes (Click on data points to zoom)
nc_113 12 1.91M 39 0 0 0 0 2 124 0.14 2019-12-11 08:32:56 12 1.91M 39 0 0 0 0 2 124 0.14 2019-12-11 08:32:56 615230 0 0 0 2020-01-01 01:57:15	local	,,
	Evaluation Off Running	<u>]</u>
New York         4         50652         1         929         19235         1526         9033         9         10         (35590 TB/3.46)           nc_157         6         15291         39         0         0         8         254         0.18         2019-12-11 16:00.00           10.91.170.157         0         -         -         195548         4         0         2020-01-01 01:57:13	local Permanent Off Running	]
Total         7         50652         2         929         19235         1526         10383         31         20.00         (961.31 TB / 4.65)           NodeCount: 2         12         15292         78         0         0         0         378         0.31         2019-12-11 08:32:56         0           0         -         -         -         -         810778         4         0         2019-12-11 08:32:56         0           - <t< td=""><td>Overview</td><td>1</td></t<>	Overview	1

Figure 22-Dashboard Node View Throughput Column



The Seventh column Storage has four data elements:

- CompressedTotal is the total compressed storage used up by the capture data and CompressionRatio is the current compression ratio. (Dividing compressed storage by compression ratio gives the actual storage size.)
- FirstPCAP of each node. This value changes every time oldest capture files are removed to make space for the new capture files.LastPCAP of each node is the time when the latest PCAP has been stored. This allows users to see the full duration of data of the node.
- ClusterNodeCount shows the count of cluster nodes attached to the master node.

NodelP Defend Boston nc_113 10.91.170.113	IDS ActiveRules Sests Undefended Ale Alerts 7 50652 12 1.91M	ActiveTriggers Rules ts Events	IPAddresses IPAlerts	Suspicious Trainic Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files	Events TLS/SSL	Throughput MaxGbps	Storage (CompressedTotal /	Conliguration Authentication	Performance
nc_113 24	12 1.91M				and algebra	Emails Netflows DNS	VOIP Critical	Avg@bps DroppedPkts	CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Licensing PreCaptureFilter ServerStatus	Throughput Obps Duration: Past 15 minutes (Click on data points to zoom)
	454	2 39	929 0	19235 0	1526 0	1350 2 615230 21699	22 124 0 0	10 0.14 0	(605.76 TB / 1.19) 2019-12-11 08:32:56 2020-01-01 01:57:15	local Evaluation Off Running	1
nc 157	4 50652 6 15291 0	1 39	929 0	19235 0	1526 0	9033 8 195548 395190	9 254 4 0	10 0.18 0	(355.90 TB / 3.46) 2019-12-11 16:00:00 2020-01-01 01:57:13	local Permanent Off Running	1
NodeCount: 2	7 50652 12 15292 0	2 78	929 0	19235 0	1526 0	10383 0 810778 416889	31 378 4 0	20.00 0.31 0	(961.31 TB / 4.65) 2019-12-11 08:32:56 2020-01-01 01:52:25 0	Overview	1
NodeCount: 2	12 15292					0 810778	378 4	0.31	2019-12-11 08:32:56 2020-01-01 01:52:25	Overview	

The Eighth column Configuration provides information about the Authentication, Licensing, PrecaptureFilter and ServerStatus of the node.

- Clicking on "Authentication" sub-category pivots to Configuration-> Authentication screen.
- Clicking on "Licensing" sub-category pivots to Configuration -> Software Management screen.
- Clicking on "PrecaptureFilter" sub-category pivots to Policy Setup-> PrecaptureFilter screen. The aggregated configuration of all nodes in the group can be viewed by clicking on the Overview...." hyperlink.



Node Details		IDS	ActiveTriggers		Suspicious Traffic		DPI Evi	ents	Throughput	Storage	Configuration	Performance	
GroupName NodeName NodeIP	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(CompressedTotal / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PreCaptureFilter ServerStatus	Throughput Gbps Duration: Past 15 minutes (Click on data points to zoom)	A
Boston nc_113 10.91.170.113	7 12 2454	50652 1.91M	2 39	929 0	19235 0	1526 0	1350 2 615230 21699	22 124 0 0	10 0.14 0	(605.76 TB / 1.19) 2019-12-11 08:32:56 2020-01-01 01:57:15	local Evaluation Off Running	1	Pi
New York nc_157 10.91.170.157	4 6 0	50652 15291	1 39	929 0	19235 0	1526	9033 A	9 ggregated O	10 Iverview	( 355.90 TB / 3.46 )	local Permanent Off Running	1	Pi
Total	7	50652	2	929	19235	1526		Sta	atus	Count		7	
NodeCount: 2	12	15292	78	0	0	0	Node Status		Jp	2 6	Overview	+++++++++++++++++++++++++++++++++++++++	
	0						Node Status		own	0		301010101010101	
	4						Authentication		ocal	2			
							Authentication		DAP	0			
							Authentication		dius	0			
							Licensing		nanent	1			
							Licensing		uation	2			
							PreCaptureFilter		Dn	0			
							PreCaptureFilter	0	Off	2			

Figure 24-Dashboard Configuration Column Aggregated Overview details

The **Performance Throughput Graph** allows the user to view thumbnail view of each node's throughput. Clicking on data points of the thumbnail shows a dialog box with more detailed version of the graph.



Figure 25-Dashboard Node View Performance Throughput Graph

The **Action** column has the Pause/Resume button and delete button. User can pause or resume the capture server of an individual node by clicking on the Pause/Resume button. Clicking on the delete button deletes the node from the associated group.

## Note:

• The node→group association is symbolic. A node is never affected by removal from a group. The deleted node can be added to a different node or re-added to the same group if desired.

NewYork         4         50652         1         929         19235         1526         0         9         10         (272.89 TB / 2.65)           NewYork         6         0         3         0         0         0         8         254         0.10         2019-12-1123:12:51	Configuration Authentication Licensing PreCaptureFilter ServerStatus	(Compressed Total / CompressionRatio) FirstPCAP	Authentication	T
12         615063         48         162         0         2         124         6.56         2019-12-12 04:32-59           10.91.170.113         24828		ClusterNodeCount	PreCaptureFilter Duration: Past 15 minut	ites
6 0 3 0 0 0 8 254 0.10 2019-12-11 23:12:51	Off Running	2019-12-12 04:32:59 2020-01-02 20:07:01	Evaluation Off	
10_10/1 0 0 4 0 2020-01-02 20:15:19 10.91.170.157 0 0 0 0	local Permanent Off Running	2019-12-11 23:12:51 2020-01-02 20:15:19	Permanent Off	TTT (
Total         7         50654         2         929         19235         1526         743         31         20.00         (875.26 TB/3.81)           NodeCount: 2         12         615063         51         162         0         0         376         6.34         2019-12-12 04:32:59           24828         24828         378530         4         0         2020-1042 20:07:01	Overview	2019-12-12 04:32:59 2020-01-02 20:07:01	Overview	-

Figure 26-Dashboard Node View Action Column



## 6 POLICY SETUP TOOL

The policy setup tab allows the user to upload and update a category of policies for all the federated nodes in a group. The sub-menu items are as follows:

- Defended Assets Trusted Assets defined by IP address.
- Defended Services Defended Services defined port, priority, and description.
- IDS Rules Intrusion Detection System Rules.
- ThreatIPs Unsafe IPs that generate an alert.
- Active Triggers Generate an alert based on a specific event.
- PreCapture Filter Filters network traffic before writing it to disk.

Find Text	0% Defended Services										ntinuum Role:Admin A		Castree over -
eCount)	Augmentation     ActiveTriggers     PreCaptureFilter	Services Assets ended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLSISSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(Compressed Total / CompressionRatio) FirstPCAP LastPCAP ClusterNodeCount	Authentication Licensing PrsCaptureFilter ServerStatus	Throughput Gbps (Click on data points zoom)
	1	7 12 15735	50654 592241	2 42	2 67	19235 0	1526 0	731 0 380779 316421	22 124 0 0	10 6.25 0	(604.52 TB / 1.18) 2019-12-12 04:32:59 2020-01-02 20:16:05 0	Details	
	NewYork 1	4 6 0	50652 0	1 4	929 0	19235 0	1526 0	0 0 0	9 254 4 0	10 0.11 0	(267.71 TB / 2.60) 2019-12-12 04:32:59 2020-01-02 20:16:05 0	Details	1
	Total GroupCount: 2 NodeCount: 2	7 12 15735	50654 592241	2 46	929 67	19235 0	1526 0	731 0 380779 316421	31 378 4 0	20.00 6.36 0	(872.23 TB / 3.78) 2019-12-12 04:32:59 2020-01-02 20:16:05 0	Overview	1
	KSeuriti	Augmentation     GAugmentation     GAugmentation     GauveFilter     VerCaptureFilter     VerWYork     1     Total     GroupCount: 2	Count)  C Augmentation  C Aug	Construint         ◆ Augmentation (B) Active Triggers ▼ Precapture Filter         Ferries Stassa (C) Section (C) Section	Account         Account         Account         Account         Ruise           Image: Control of the Active Triggers         Account active Activ	Augmentation B Active Triggers         Envice Augmentation ▼ PreCaptureTiles         Envice Augmentation ▼ PreCaptureTiles         Envice Augmentation T 2         Precessor Soperation T 2         Precessor Soperation T 2         Precessor Soperation T 2         Precessor Soperation T 2         Precessor Soperation T 2         Precessoperation T 2         Precessor Soperation	Augmentation         Augmentation         Augmentation         Processing         Augmentation         Processing         Processing <th< td=""><td>Augmentation B Active Triggers Service Augmentation Berivice Active Augmentation Berivice PreCaptureFilter 7          Service Active Augmentation 1          Protect 1          Description 8          Protect 9          Protect 9</td><td>Augmentation BActive Triggers         Augmentation BActive Triggers         Bences Augmentation To S0054         Plate Finite S0054         Plate Finit</td><td>Augmentation         Automation         Rules         Prior Capture File         File         Tubes for the file         Automation         Rules         Prior Capture File         File         Tubes for the file         Automation         Rules         Prior Capture File         File         Tubes for the file         Automation         Rules         Prior Capture File         File         Tubes for the file         Automation         Automation<td>Account         Account         Account         Refer         Products         Contains         C</td><td>Augmentation B Active Triggers         Augmentation B Active Triggers         Bevice Augmentation T 22 592241         Network Composition Composition PARENTS         Domain Domain December         Domain Domain December         Tubes Composition Domain PARENTS         Price Domain Domain PARENTS         Price Domain Domain Domain PARENTS         Price Domain Domain PARENTS         Price Domain Domain Domain PARENTS         Price Domain Dom</td><td>Adjumentation         Adjumentation         Rules         Prior Adjumentation         Adjumentation         Rules         Prior Adjumentation         Adjumentation         Compresentation         Adjumentation         Compresentation         Adjumentation         Adjument</td></td></th<>	Augmentation B Active Triggers Service Augmentation Berivice Active Augmentation Berivice PreCaptureFilter 7          Service Active Augmentation 1          Protect 1          Description 8          Protect 9          Protect 9	Augmentation BActive Triggers         Augmentation BActive Triggers         Bences Augmentation To S0054         Plate Finite S0054         Plate Finit	Augmentation         Automation         Rules         Prior Capture File         File         Tubes for the file         Automation         Rules         Prior Capture File         File         Tubes for the file         Automation         Rules         Prior Capture File         File         Tubes for the file         Automation         Rules         Prior Capture File         File         Tubes for the file         Automation         Automation <td>Account         Account         Account         Refer         Products         Contains         C</td> <td>Augmentation B Active Triggers         Augmentation B Active Triggers         Bevice Augmentation T 22 592241         Network Composition Composition PARENTS         Domain Domain December         Domain Domain December         Tubes Composition Domain PARENTS         Price Domain Domain PARENTS         Price Domain Domain Domain PARENTS         Price Domain Domain PARENTS         Price Domain Domain Domain PARENTS         Price Domain Dom</td> <td>Adjumentation         Adjumentation         Rules         Prior Adjumentation         Adjumentation         Rules         Prior Adjumentation         Adjumentation         Compresentation         Adjumentation         Compresentation         Adjumentation         Adjument</td>	Account         Account         Account         Refer         Products         Contains         C	Augmentation B Active Triggers         Augmentation B Active Triggers         Bevice Augmentation T 22 592241         Network Composition Composition PARENTS         Domain Domain December         Domain Domain December         Tubes Composition Domain PARENTS         Price Domain Domain PARENTS         Price Domain Domain Domain PARENTS         Price Domain Domain PARENTS         Price Domain Domain Domain PARENTS         Price Domain Dom	Adjumentation         Adjumentation         Rules         Prior Adjumentation         Adjumentation         Rules         Prior Adjumentation         Adjumentation         Compresentation         Adjumentation         Compresentation         Adjumentation         Adjument

## 6.1 DEFENDED ASSETS

Assets are registers of IP addresses that are approved or recognized and considered to be safe within the network traffic. Since assets are considered as a reliable resource, a low priority alert is generated, and no further action is taken. Assets can be defined based on two categories.

- Critical IPs These IPs represent critical infrastructure of an organization.
- **Trusted IPs** These IPs represent hosts that are part of an organization or its partners. They are well-known and their state/purpose well-understood.

This application allows the user to create a user-defined list of Critical IPs /Trusted IPs and upload/apply them for alert monitoring.



- ALL CARLES ADDAS	hboard 🔦 Policy Setup 💿 Investigator Q Search 🎄 View Metadata			Reports Of Configuration Of Help Of Logo
Critical IPs		⊙ Upload	i List Details()	QFind Apply a display filter
NodeName	Name	Action	Resource	Description
NewYork::nc_139	1544725890464_Critical411.csv	View Delete		
DC::nc_w179	1544725890464_Critical411.csv	View Delete		
DC::nc_cm_jp	1544725890464_Critical411.csv	View Delete		
Trusted IPs		The second se		
		Opload		
NodeName	Name	O Upload		
	Name 1534686471661_TrusH09.cov			
NodeName		Action		
NodeName NewYork:::nc_139	1534868471661_TrusH09.csv	Action View Delete		
NodeName NewYork::nc_139 DC::nc_w179	1534868471661_TrusH09.csv 1534868471661_TrusH09.csv	Action View Delete View Delete		
NodeName NewYork::nc_139 DC::nc_w179	1534868471661_TrusH09.csv 1534868471661_TrusH09.csv	Action View Delete View Delete		
NodeName NewYork::nc_139 DC::nc_w179	1534868471661_TrusH09.csv 1534868471661_TrusH09.csv	Action View Delete View Delete		
NodeName NewYork::nc_139 DC::nc_w179	1534868471661_TrusH09.csv 1534868471661_TrusH09.csv	Action View Delete View Delete		

Figure 27-Policy Setup Overview

## 6.1.1 User Defined Assets File Format

Users can define a list of assets in a **csv** file as per the format below:

- **First column** of each row should state an IP address (resource)
- **Second column (optional)** of each row should describe the resource in the first column. This is optional but generally a good practice for easy reference.

**Example** of a CriticalIPs csv file:

192.1.1.1, System1 10.1.1.2 1.2.3.4, System2

Sentry Wire &Dashboard	Policy Setup 🔷 Threat Hunting Workflow		X	QMessaging	Configuration	Help •	(+ Logout
Critical IPs		© Upload	i List Deta	ih0	QFind Apply	a display filter	- I
	Select Defended Assets from the Policy Setup drop down menu.	View Delete		associat	upload to ed panel itical IP's	to defi	he
Trusted IPs		© Upload					
	Name 1513021572309_Trusted/Ps.cov	View Delete					
							F

28-Policy Setup Upload

## 6.1.2 Upload User Defined Assets File

- Create a <Filename>.csv file on your local system.
- Click on Upload button.
- Select file from the local system to be uploaded.

Sentry Wire ADashboard	d 🔦 Policy Setup 👁 Investigator Q Search 🗂 View Metadata			Reports 🌣 Configuration 🥥 Help 🕞 Logout
I∎Critical IPs		1 Lis	t Details()	QFind Apply a display filter
NodeName	Name	Action	Resource	Description
NewYork::nc_139	1544725890464_Critical411.csv	View Delete		
DC::nc_w179	1544725890464_Critical411.csv	View Delete		
DC::nc_cm_jp	1544725890464_Criticel411.csv	View Delete		
	© Open		×	
	← → → ↑ 🖡 > This PC > Desktop	v 0	Q	
	Organize - New folder	[iii · 二]	0	
I∎Trusted IPs	This PC Name	Date modified Type 7/25/2018 6:19 PM Micro		
NodeName	Desktop Critical411.csv	12/13/2018 1:30 PM Micro		
NewYork::nc_139	15 Documents			
DC::nc_w179	15 Downloads			
DC::nc_cm_jp	15 v ¢		•	
	File name:	All Files     Open     Cancel	~	
	L			

Figure 29-Policy Setup Upload User Defined Assets

- If the file contents are valid, the server adds the file to the list and prepends a timestamp to the filename.
- When an alert is generated due to a rule, the alert is displayed in Threat Hunting Workflow → IoC Manager → Defended Alerts tab, if the alert's source or destination IP address is a defended asset **AND** the alert's source or destination port is a defended service.
- When an alert is generated due to a rule, the alert is displayed in Threat Hunting Workflow→IoC Manager → Undefended Alerts tab if the alert's source or destination IP address is **NOT** a defended asset **OR** the alert's source or destination port is **NOT** a defended service.

	Upload	i Critical IPs List Details(1513921293530_CriticalIPs.csv)	QFind Apply a display filter
Name	Action	Resource	Description
1513921293530_CriticalIPs.csv		1.1.1.2	system 1
	View Delete	1.1.1.3	system2
		10.91.170.22	
		159.180.64.119	system3
usted IPs	@ Upload		
Name	Action		
1513921572399_TrustedIPs.csv	View Delete		

## Figure 30 - Policy Setup View User Defined Assets

- To view the contents of the file uploaded simply click view button next to the file.
- To do a text lookup simply type in the desired string in the Find textbox.



Sentry Wire	Babashboard ▲ Policy Setup ♦ Threat Hunting Workflow		QMessaging	Configuration 🥥 Help 👻 🕞 Logout
Critical IPs		Upload	i Trusted IPs List Details(1513921572399_TrustedIPs.cov)	QFind Apply a display filter
	Name	Action	Resource	Description
	1513921293530_CriticalIPs.csv	View Delete	172.16.1.116	Account Department
			100.103.185.154	HR
			1.1.1.2	Printer
Trusted IPs		● Upload		
	Name	Action		
	1513921572399_TrustediPs.csv	View Delete		

## Figure 31 - Policy Setup Delete Critical/Trusted IP List

• To delete an active Critical/TrustedIP list, click the delete button. Once deleted, the resources contained in the list are no longer active.

*Note*: A guest user cannot Upload/Delete CriticalIPs or TrustedIPs.

## 6.2 DEFENDED SERVICES

This tool is used to define the list of services that are defended. There are four types of defended services discussed in this section:

- Predefined Unmapped Services
- Activated Defended Services
- Defended Services
- Unmapped Services

## 6.2.1 Predefined Unmapped Services

These are list of frequently used service ports included with the application. These can be activated by clicking on the activate button. Once activated, an alert is triggered with defended asset and a defended service as part of its 5-tuple. This alert is displayed in Threat Hunting Workflow  $\rightarrow$  IoC Manager  $\rightarrow$  Defended Alerts tab.

*Note*: When an alert is triggered with either a defended asset or a defended service or neither, the alert is displayed in Threat Hunting Workflow  $\rightarrow$  IoC Manager  $\rightarrow$  Undefended Alerts tab.



				Defended S									
Prede	efined Unmapp	ed Services		Defended	services		1 Upload	Lownload	Unmapped s	Services			
Port	Priority	Description	Action	NodeName	Port	Priority	Description	Action	NodeName	Port	Priority	Description	
80	Operational	FTP(data)	Activate 🔔	Boston::nc_w160	20	Operational	FTP(data)	Deactivate					
1	Operational	FTP(control)	Activate	Boston::nc_w160	53	MissionCritical	DNS	Deactivate					
12	MissionCritical	SSH	Activate	Boston::nc_w160	80	MissionCritical	HTTP	Deactivate					
15	Operational	SMTP-unencrypted	Activate	Boston::nc_w160	443	MissionCritical	HTTPS	Deactivate					
13	MissionCritical	DNS	_	Boston::nc_w160	5060	Essential	SIP	Deactivate					
10	MissionCritical	HTTP	Activate	DC::nc_w179	20	Operational	FTP(data)	Deactivate					
			Activate	DC::nc_w179 DC::nc_w179	21	Operational MissionCritical	FTP(control) SSH	Deactivate					
10	Operational	IMAP-unencrypted and TLS	Activate	DC::nc_w179 DC::nc_w179	53	MissionCritical	DNS	Deactivate					
135	MissionCritical	EndPointMapper,Microsoft	Activate	DC::nc_w179	80	MissionCritical	HTTP	Deactivate					
152	Operational	Background File Transfer Program (BFTP)	Activate	DC::nc_w179	135	MissionCritical	EndPointMapper,Microsoft	Deactivate					
156	Operational	SQL Service	Activate	DC::nc_w179	443	MissionCritical	Nessus Security Scanner	Deactivate					
009	Essential	WebCenterContent Portable,Oracle	Activate	DC::nc_w179	1616	Essential	web	Deactivate					
43	MissionCritical	HTTPS	Activate	NewYork::nc_139	53	MissionCritical	DNS	Deactivate					
45	MissionCritical	DS Active Directory,Microsoft	Activate	NewYork::nc_139	80	MissionCritical	HTTP	Deactivate					
65	Operational	SMTP-SSL	Activate	NewYork::nc_139	443	Operational	Nessus Security Scanner	Deactivate					
87	Operational	SMTP-TLS											
	e Defended Ser	A DECOMPANY AND	Activate *										
	e Derenaea ee												
Port													
22													
Priority													
Select	Priority		•										
Descripti	on												
ServiceDe													
	en granne -	Activate											
		Acuvate											
									1				

Figure 32 – Policy Setup Predefined Unmapped Services

## 6.2.2 Activate Defended Services

Besides a predefined list, the application also allows the user to create/activate their own defended services by entering the port number, priority and description. Once activated these appear under the Defended Services column as activated.

Pred	efined Unmap	ped Services		Defended s	Services		1 Upload	La Download	Unmapped S	ervices			
Port	Priority	Description	Action	NodeName	Port	Priority	Description	Action	NodeName	Port	Priority	Description	
20	Operational	FTP(data)	Activate ^	Boston::nc_w160	20	Operational	FTP(data)	Deactivate					
1	Operational	FTP(control)	Activate	Boston::nc_w160	53	MissionCritical	DNS	Deactivate					
2	MissionCritical	SSH	Activate	Boston::no_w160	80	MissionCritical	HTTP	Deactivate					
15	Operational	SMTP-unencrypted	Activate	Boston::nc_w160	443	MissionCritical	HTTPS	Deactivate					
3	MissionCritical	DNS		Boston::nc_w160	5060	Essential	SIP	Deactivate					
			Activate	DC::nc_w179	20	Operational	FTP(data)	Deactivate					
80	MissionCritical	HTTP	Activate	DC::nc_w179	21	Operational	FTP(control)	Deactivate					
110	Operational	IMAP-unencrypted and TLS	Activate	DC::nc_w179	22	MissionCritical	SSH	Deactivate					
135	MissionCritical	EndPointMapper,Microsoft	Activate	DG::nc_w179	53	MissionCritical	DNS	Deactivate	-				
152	Operational	Background File Transfer Program (BFTP)	Activate	DC::nc_w179	80	MissionCritical	HTTP	Deactivate					
156	Operational	SQL Service		DC::nc_w179	135	MissionCritical	EndPointMapper,Microsoft	Deactivate					
			Activate	DC::nc_w179	443 1616	MissionCritical	Nessus Security Scanner web	Deactivate					
:00	Essential	WebCenterContent Portable.Oracle	Activate	DC::nc_w179 NewYork::nc_139	1010 53	Essential MissionCritical	DNS	Deactivate					
43	MissionCritical	HTTPS	Activate	NewYork::nc_139	80	MissionCritical	HTTP						
145	MissionCritical	DS Active Directory,Microsoft	Activate	NewYork::nc 139	443	Operational	Nessus Security Scanner	Deactivate					
65	Operational	SMTP-SSL	Activate	NewTORCIG_139	44.3	Operational	Nessus Security Scattrier	Deactivate					
87	Operational	SMTP-TLS	Activate *										
Activat	e Defended Se		Concerne of										
Port													
22													
Priority													
Selec	t Priority		*										
Descripti	ion												
ServiceDe													
ServiceDi	iscription.	Activate											

Figure 33 – Policy Setup Activate Defended Services

## 6.2.3 Defended Services

This panel displays all the active defended service ports. These defended services are also displayed in the dashboard defended services graph if there is a match for defended IP and defended port. Whenever an alert is triggered with defended asset and a defended service as part of its 5-tuple it is displayed in Threat Hunting Workflow  $\rightarrow$  IoC Manager  $\rightarrow$  Defended Alerts tab.



•

*Note*: When an alert is triggered with either a defended asset or a defended service or neither, the alert is displayed in Threat Hunting Workflow  $\rightarrow$  IoC Manager  $\rightarrow$  Undefended Alerts tab.

- Clicking on upload allows the user to upload a csv file with multiple service ports.
  - File Format must be <port number>, <Priority>, <Description>

*Note:* The Priority is case sensitive. There are 3 priority namely: Mission Critical, Operational and Essential.

Clicking on Download allows the user to download all activated service ports.

Pred	fined Unmap	bed Services		Defended a	Services		1 Upload	Lownload	Unmapped S	ervices			
Port	Priority	Description	Action	NodeName	Port	Priority	Description	Action	NodeName	Port	Priority	Description	
20	Operational	FTP(data)	Activate	Boston::nc_w160	20	Operational	FTP(data)	Deactivate					
1	Operational	FTP(control)	Activate	Boston::nc_w160	53	MissionCritical	DNS	Deactivate					
22	MissionCritical	SSH	Activate	Boston::nc_w160	80	MissionCritical	HTTP	Deactivate					
25	Operational	SMTP-unencrypted	Activate	Boston::nc_w160	443	MissionCritical	HTTPS	Deactivate					
3	MissionCritical	DNS		Boston::nc_w160	5060	Essential	SIP	Deactivate					
			Activate	DC::nc_w179	20	Operational	FTP(data)	Deactivate					
90	MissionCritical	HTTP	Activate	DC::nc_w179	21	Operational	FTP(control)	Deactivate					
110	Operational	IMAP-unencrypted and TLS	Activate	DC::nc_w179	22	MissionCritical	SSH	Deactivate					
35	MissionCritical	EndPointMapper,Microsoft	Activate	DC::nc_w179 DC::nc_w179	53 80	MissionCritical MissionCritical	DNS	Deactivate					
52	Operational	Background File Transfer Program (BFTP)	Activate	DC::nc_w179 DC::nc_w179	135	MissionCritical	EndPointMapper.Microsoft	Deactivate					
56	Operational	SQL Service	Activate	DC::nc_w179	443	MissionCritical	Nessus Security Scanner	Deactivate					
00	Essential	WebCenterContent Portable.Oracle	Activate	DC::nc w179	1616	Essential	web	Deactivate					
43	MissionCritical	HTTPS		NewYork::nc_139	53	MissionCritical	DNS	Deactivate					
			Activate	NewYork::nc_139	80	MissionCritical	HTTP	Deactivate					
45	MissionCritical	DS Active Directory, Microsoft	Activate	NewYork::nc_139	443	Operational	Nessus Security Scanner	Deactivate					
65	Operational	SMTP-SSL	Activate										
87	Operational	SMTP-TLS	Activate *										
ctivat	e Defended Se	ervice											
Port													
22													
Priority													
-Select	Priority		*										
Descripti	on .												
ServiceDe													
001100000		Activate											

Figure 34 – Policy Setup Defended Services



## 6.2.4 Unmapped Services

This panel displays any services that were once active. These services can be reactivated by clicking activate or deleted by clicking delete button respectively.

Priority Description Action   0 Operational FPT(stab) Action   0 Operational FPT(stab) Action   1 Operational FPT(strab) Action   2 Massic/Critical SB1 Action   2 Massic/Critical SB1 Action   3 Massic/Critical NMP4-unencrypted and TLS Action   3 Massic/Critical EndPerature refered SP2   4 Massic/Critical NM4-unencrypted and TLS Action   3 Massic/Critical SARP-encodenter Fortable/Actional Action   3 Massic/Critical SReserver Refered SP2   4 Massic/Critical SReserver Refered SP2   0 Massic/Critical SReserver Refered   3 Massic/Critical SReserver Refered SP2   0 Operational Action   10 Operational SReserver   10 Operational SReserver   10 Operational Action   10 Operational Action   10 SReserver SReserver   10 Massico-Critical Massico-Critical   10 Massico-Critical Massico-Critical <th>Operational     FPR (aba)     Actional     Actional     Calo     Calo</th> <th>Pred</th> <th>efined Unmapp</th> <th>ed Services</th> <th></th> <th colspan="3">Defended Services</th> <th colspan="2">1 Upload 2 Download</th> <th colspan="2">Unmapped Services</th> <th></th> <th></th> <th></th> <th></th>	Operational     FPR (aba)     Actional     Actional     Calo	Pred	efined Unmapp	ed Services		Defended Services			1 Upload 2 Download		Unmapped Services					
Norm         Price         Description         Price         Description         Description<	Operational         FTP(corror)         Activation         Activ	Port	Priority	Description	Action	NodeName	Port	Priority	Description	Action	NodeName	Port	Priority	Description		Action
Second         Second         Active           Main/Chied         Second         Active         Active </td <td>Mainor Chinal         Self-order (No. 1000)         Control (</td> <td>0</td> <td>Operational</td> <td>FTP(data)</td> <td>Activate 📥</td> <td>Boston::no_w160</td> <td>53</td> <td>MissionCritical</td> <td>DNS</td> <td>Deactivate</td> <td>Boston::nc w160</td> <td>20</td> <td>Operational</td> <td>FTP(data)</td> <td>Dr</td> <td>elete Activa</td>	Mainor Chinal         Self-order (No. 1000)         Control (	0	Operational	FTP(data)	Activate 📥	Boston::no_w160	53	MissionCritical	DNS	Deactivate	Boston::nc w160	20	Operational	FTP(data)	Dr	elete Activa
aska         Actual         Actual         Actual           Go Queritorial         SNP-concepted on Concepted on Co	NameSamActionOperationalSamActionMasion-CriticalDNSActionalMasion-CriticalINTPActionalOperationalHTTPActionalOperationalEnd-warryptica vari TLSActionalOperationalEnd-warryptica vari TLSActionalOperationalEnd-warryptica vari TLSActionalOperationalEnd-warryptica vari TLSActionalOperationalEnd-warryptica vari TLSActionalOperationalSeleginand TRE Transfer Program (BTTP)ActionalOperationalSeleginand TRE Transfer Program (BTTP)ActionalMasion-CriticalVinto-CriticalActionalOperationalSeleginand TRE Transfer Program (BTTP)ActionalMasion-CriticalNational-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalMasion-CriticalNational-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-CriticalActionalOperationalSeleginal-Critical<	1	Operational	FTP(control)	Activate	Boston::no_w160	80	MissionCritical	HTTP	Deactivate	DC::no_w179					
a       Matrine Arrow       SMT P-unencrypted       Antioned       Small       S	Operational     SMP-sunarcognited     Activation       Masico-Critical     NPS     Activation       Operational     SMP-sunarcognited     Activation       Operational     Masico-Critical     Masico-Critical     Masico-Critical     SMP-sunarcognited     Activation       Operational     Masico-Critical     Masico-Critical     SMP-sunarcognited     Activation       Operational     Subjecture Plantafor Program (BTPP)     Activation     Masico-Critical     Masico-Critical<	2	MissionCritical	SSH	Activate					Deactivate						
Maiori/Rola         DNS         Maiori/Rola         DNS         Maiori/Rola         DNS         Maiori/Rola         Description         Description           1         Maiori/Rola         HTTP         Activation         SH         Description         Description           0         Operational         MAP-remorphice Marcal         Activation         Description         Descrip	Maior Critical         DNB         Activation         Dicts::::::::::::::::::::::::::::::::::::	e	Operational	SMTP-unencrypted												
0         Maiori-Chical         HTTP         Actival         Doct. vir70         S.3         Maiori-Chical         DNS         Doct.vir80           0         Operational         MAP-arencrysted and TLS         Actival         DS         Disc. vir70         S.3         Maiori-Chical         DNS         Doct.vir80           20         Operational         ExpRiverint/argue Moreound         Actival         DS         Maiori-Chical         HTTP         Doct.vir80	Mainot Chies         MTP         Active         Softward         Softward           Operational         MAP-smort/pited and TLS         Active         Active         Mainot Chies															
0     Operational     MAP-arencrypted and TLS     Activate       10     Operational     MAP-arencrypted and TLS     Activate       12     Operational     EndP-arintApper: Marsonich     Activate       13     Operational     Science xr17     15     Masion-Chical     BordPaintApper: Marsonich     Doctore triate       14     Operational     Science xr17     15     Masion-Chical     Masion-Chical     Doctoretriate       15     Operational     Science xr17     15     Masion-Chical     Masion-Chical     Doctoretriate       16     Operational     Science xr17     15     Masion-Chical     Masion-Chical     Doctoretriate       16     Operational     Science xr17     15     Masion-Chical     Masion-Chical     Doctoretriate       16     Operational     Masion-Chical     Masion-Chical     Masion-Chical     Masion-Chical     Masion-Chical     Doctoretriate       16     Massion-Chical     Masion-Chical     Masion-Chical     Masion-Chical     Masion-Chical     Masion-Chical     Doctoretriate       16     Massion-Chical     Masion-Chical	Operational         MMA-varencypited and TLS         Activate Mainero-Critical         Exel-bicitMagnex, Monoral         Activate Descriptional         Bob Mainero-Critical         HTTP         Descriptional         Bob Mainero-Critical         Headborn Mainero-Critical															
Operation         Marked Marged Moreadity (all parameters)         Activation         Conce yr170         453         Masion/Chical         Ford-Marged Moreadity         Description           52         Operational         Background File Transform (specin (BFTP))         Activation         Activation         Operational         Scileser/170         453         Masion/Chical         Ford-Marged Moreadity         Description           53         Massion/Chical         Scileser/170         453         Masion/Chical         Description         Description           43         Massion/Chical         Scileser/170         453         Massion/Chical         Description         Description           43         Massion/Chical         Scileser/170         453         Massion/Chical         Description         Description           43         Massion/Chical         Operational         Scileser/170         453         Massion/Chical         Description         Description           43         Massion/Chical         Operational         Skileser/180         Description         Description         Description           443         Massion/Chical         Skileser/180         Description         Description         Description         Description           70         Operational <td< td=""><td>Amainor Chang     Bender Mannamer Change     Activate       Amainor Chang     Background File Transfer Program (BFTP)     Activate       Operational     Background File Transfer Program (BFTP)     Activate       Search     Mainor Chang     Mainor Change     Mainor Change     Mainor Change       Search     Wackersch     Search     Search     Mainor Change     Mainor Change&lt;</td><td>3</td><td>MissionCritical</td><td></td><td>Activate</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	Amainor Chang     Bender Mannamer Change     Activate       Amainor Chang     Background File Transfer Program (BFTP)     Activate       Operational     Background File Transfer Program (BFTP)     Activate       Search     Mainor Chang     Mainor Change     Mainor Change     Mainor Change       Search     Wackersch     Search     Search     Mainor Change     Mainor Change<	3	MissionCritical		Activate											
Sector         EndPaintAppend Macroardia         Actual         Macaro/Findia         EndPaintAppend Macroardia         Actual         Macaro/Findia         Measor/Macia         Mea	MainoCitical         Balagenation         Activation         Conce, pri/10         MainoCitical         MainoCitical </td <td>10</td> <td>Operational</td> <td>IMAP-unencrypted and TLS</td> <td>Activate</td> <td></td>	10	Operational	IMAP-unencrypted and TLS	Activate											
Q2         Qperational         Basignumer File Transfer Program (BFTP)         Activational         Qperational         Basignumer File Transfer Program (BFTP)         Activational         Qperational         Status         Qperational         Status         Concervant Program         Qperational         Status         Statu	Operational     Bolgmound Pite Trainer Program (BTPY)     Activate (Descriptional     Solutional Pite Trainer Program (BTPY)     Activate (Descriptional     Solutional Pite Trainer Pite Trainer (Solutional Pite Trainer Pite Pite Trainer Pite Trainer Pite Pite Pite Pite Pite Pite Pite Pite	35	MissionCritical	EndPointMapper,Microsoft	Activate	and the second second second										
96     Operational     SQL Service     Actual       90     Operational     SQL Service     Actual       91     Operational     ThTP     Operational       131     Massion-Critical     ITTP     Operational       132     Massion-Critical     Operational     Mithion-Critical     Mithion-Critical     Mithion-Critical       133     Massion-Critical     SALtheo Directory,Microsoft     Actual       143     Operational     SMTP-TLS     Actual       144     Defended Service     Actual       144     The Service     Service	Operational     SQL Bervide     Activate       Exact fail     Work/Artine/Content Portabile/Condee     Activate       Maisson/Orical     HTTP     Operational       Maisson/Orical     Database     Activate       Operational     SATAre Directory/Morocold     Activate       View/Index.vsc     Satare Directory/Morocold     Satare Directory/Morocold       View/Index.vsc     Satare Directory/Morocold     Satare Directory/Morocold       View/Index.vsc     Satare Directory/Morocold     Neison/Satare Directory/Morocold       View/Index.vsc     Satare Directory/Morocold	52	Operational	Background File Transfer Program (BFTP)	Activate											
30     Exernital     WebCarter-Context Pondate, Conde     Actuate       43     Masion-Citodi     HTTP     Deactivate       54     Masion-Citodi     DSA Actuate     Actuate       55     Operational     DSA Actuate     Actuate       56     Operational     SMTP-TL3     Actuate       57     Operational     SMTP-TL3     Actuate       60     Peratoral     Actuate       70     Operatoral     SMTP-TL3     Actuate       71     Operatoral     SMTP-TL3     Actuate       72     Operatoral     SMTP-TL3     Actuate       73     Operatoral     SMTP-TL3     Actuate       74     Operatoral     SMTP-TL3     Actuate       75     Operatoral     SMTP-TL3     Actuate       76     SMTP-TL3     Actuate     SMTP-TL3       76     SMTP-TL3     Actuate     SMTP-TL3       76     SMTP-TL3     SMTP-TL3     SMTP	Exacritial     Web/Centrac-Constant     Activation       Mainson-Critical     HTTPS     Activation       Mainson-Critical     Demotros/Marconal     Activation       Operational     SATP-SAL     Activation       Operational     SATP-SAL     Activation       Operational     SATP-TLIS     Activation       Operational     SATP-TLIS     Activation       Interpretation     SATP-TLIS     Activation	56	Operational	SQL Service	Activate						-					
Alternation         Attraction         Attractractraction         Attraction <t< td=""><td>Masion/Orical     MTTPS     Actival       Masion/Orical     DS Active Dendory.Moroandt     Actival       Operational     DS Active Dendory.Moroandt     Actival       Operational     SMTP-SSL     Actival       Operational     SMTP-SSL     Actival       Vater Defended Service     Service     Service</td><td>10</td><td>Essential</td><td>WebCenterContent Portable Oracle</td><td></td><td>Contraction and the second second</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Masion/Orical     MTTPS     Actival       Masion/Orical     DS Active Dendory.Moroandt     Actival       Operational     DS Active Dendory.Moroandt     Actival       Operational     SMTP-SSL     Actival       Operational     SMTP-SSL     Actival       Vater Defended Service     Service     Service	10	Essential	WebCenterContent Portable Oracle		Contraction and the second second										
Actual Antra Actual Act	Maidor Chada Maidor Chada Operational DA Adve Dividely Marcault Actualia Operational BMTP-SBL Actualia Operational BMTP-TLB Actualia Vate Defended Service Figure Service Servic										-					
45         Operational         SMTP-SSL         Actual           47         Operational         SMTP-TLS         Actual           40         SMTP-TLS         Actual         Contract           40         SMTP-TLS         Actual         Contract           40         SMTP-TLS         Actual         Contract           50         SMTP-TLS         Actual         Contract           50         SMTP-TLS         SMTP-TLS         SMTP-TLS           50         SMTP-TLS         SMTP-TLS         SMTP-TLS           50         SMTP-TLS         SMTP-TLS         SMTP-TLS           50         SMTP-TLS         SMTP-TLS         SMTP-TLS	Operational BATTP-4SL   Operational BATTP-4SL   Operational BATTP-4SL   Actual   Operational BATTP-4SL     Actual     Operational     BATTP-4SL     Actual     Operational     BATTP-4SL     Actual     Operational     BATTP-4SL     Actual     Product     Actual     Actual </td <td></td> <td></td> <td></td> <td>Activate</td> <td></td> <td></td> <td></td> <td>,</td> <td></td> <td>-</td> <td></td> <td></td> <td></td> <td></td> <td></td>				Activate				,		-					
and the second secon	Coperational SMTIP-TLS Activation vate Defended Service  ity cates Prosty  rption cates prosty		MissionCritical		Activale											
ctivate Defended Service     Item       tott     Item       22     Item       onsite Monty-     Item       -description     Item	vate Defended Service	65	Operational	SMTP-SSL	Activate											
Not Contemp of the second seco	Ny Company Com	87	Operational	SMTP-TLS	Activate *											
22. rioritySeec Prosty-	Applies Thotage and the second s	ctivat	e Defended Se	rvice												
hiotity Seas Photy Description	Applies Thotage and the second s	Port														
Jeast Invary-  Description	Applies Thotage and the second s	22														
Description	Applion buchesoppins buchesoppi	Priority														
		Select	Priority													
		Descripti	on													
	Adivate	OBYORUS	scripton													
Activate				Activate												

Figure 35–Policy Setup Unmapped Services

## 6.3 IDS RULES

Signatures play a very important role in Suricata. The system is shipped with several packaged rulesets. When enabled these rules generate alerts based on the actions specified in the rules. These alerts can be viewed in the Threat Hunting Workflow $\rightarrow$ IoC Manager  $\rightarrow$  Defended Alerts (Only if the alert's source or destination IP address is a defended asset **AND** the alert's source or destination port is a defended service.) or Undefended Alerts tab (Only if the alert's source or destination IP address is **NOT** a defended asset **OR** the alert's source or destination port is **NOT** a defended service). The IDS rules tab allows the user to:

- Choose a set of available rules sets to be loaded for monitoring. Each ruleset has its own count which is displayed in brackets next to the rule name.
- Clicking on an available alert rule set, displays the details of the rules for that category. These rules can also be downloaded to the system.
- User can view, activate, deactivate or delete pre-installed and user defined rules.
- Deleting an active ruleset also deletes the ruleset from the active list and the ruleset is no longer available.



EAlert Rulesets(Click to view Ruleset contents)	1 Upload	A Alert Ruleset Contents Activate Ruleset Download UserRules1.rules(7)	Activated Alext Rolesets	Alert Ruleset Contexts Deactivate Ruleset Download
merging-web_specific_apps.rules-6.rules (500)	Ŭ	QFind Click to	(Click to view Ruleset contents)	
merging-web_specific_apps.rules-7.rules (500)	<b>D</b>	Protocol Description Activate	combinedrules-TEST-50K-ONLY.rules(50652)	Protocol Description
emerging-web_specific_apps.rules-8.rules (500)	<b>a</b>	ip [198.19.1.1 is Critical2]; sid:3333;	drop.rules-1.rules(34)	
merging-web_specific_apps.rules-9.rules (500)	Ð	ip [4.4.10.90 is Critical1]; sid:4444; ip [6.6.8.114 is Critical2]; sid:5555;	emerging-ftp:rules-1.rules(61) emerging-trojan.rules-10.rules(500)	
merging-worm.rules-1.rules (11)	<b>a</b>	ip [10.91.170.22 is Critical1]; sid:6666; tcp [186 not is OK]; sid:7777;	_	
rotocol-voip.rules (265)	Û	ip [22 is the best]; sid:8888;	-	
ule_file_40000.rules (40039)	Û			
22.rules (1)				
2.rules (1)				
or.rules-1.rules (499)	÷			
or.rules-2.rules (267)	Đ			
JserRules12.rules (3) Click to View				
serRules1.rules.(7)				
		*		

### Figure 36 – Policy Setup IDS Rules

- Create/upload user defined rulesets and activate them in the application. (Refer section 6.3.1 for more details)
- Only the type of protocol and associated description is displayed for a listed alert rule file.
- To view an alert rule file the user must click the desired alert file for display (Only the selected alert rule file data is displayed)
- The monitoring application allows up to 54K set of rules to be active at any one time.
- If a user uploaded IDS ruleset has one or more errors, this ruleset is shown with *icon*. Clicking on this icon will download a csv file with error text.

Alert Rulesets(Click to view Ruleset contents)	1 Upload	A Alert Rolewer Contents & Download Wd22vWes(1) A rule with error Unit-54000 CurrentCourts1247 QFind
merging-web_specific_apps.rules-6.rules (500)	ū	QFind     Click to view Ruleset contents)
merging-web_specific_apps.rules-7.rules (500)	Û	Protocol Description     protocol Description     protocol Description     protocol Description     protocol Description     protocol Description
merging-web_specific_apps.rules-8.rules (500)	1	e8 a8 be e8 ab 96;rewbyte sid: 13411535; drop.rules-1.rules(34)
merging-web_specific_apps.rules-9.rules (500)	Û	emerging-troj rules-1 rules(61) emerging-trojen rules-10 rules(500)
merging-worm.rules-1.rules (11)	<b></b>	
rotocol-voip.rules (265)	Û	AutoSeve €eve 🛅 🗇 🤆 + tet2zeleve Storev Excel File Home Insert Daze Reyout Formulas Data Review View Help D Tell me what you want to do
ule_file_40000.rules (40039)		Image: Image: A contact of the second se
22.rules.(1)	<b>D</b>	- Parter · Of Format Neither B / U · □ · ☆ · ▲ · 臣 臣 臣 冠 冠 別Marge & Center · \$ · % 9 1 余 4 Conditioner Format Review - · · · · · · · · · · · · · · · · · ·
e2.rules (1)	<b>• •</b>	A1 * [ X V fs 12/4/2019 - 05:07:34 - Enro[EIRCODE: SC_ERR_INVALID_SIGNATURE[39]] - error parsing signature *adiadasad* from the /usr/local/ul/public/data/userideIneetrolesets/t
or.rules-1.rules (499)	Ŭ	A         B         C         D         E         G         H         I         J         K         L         M         N         O         P         Q         R           12/4/2015/-         65.07.34 - Enror[ERECORE: SC_EDB_UNALD_SEGMATURE[10])         - error parsing signature "adaptased" from life / art/local/ul/public/data/data/secret/endeducents/he22.r/ms. at line 1
or.rules-2.rules (267)	<b>D</b>	2 13/4/2019 – 50:373 - Enror[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature "astandadi" from life /our/local/si/phbl/data/astellenedvleest/h22z.rulest at line 2 3 13/4/2019 – 50:373 - Enro[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature "astandadi" from life /our/local/si/phbl/data/astellenedvleest/h22z.rulest at line 3 4 13/4/2019 – 50:373 - Enro[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature "astandadi" from life /our/local/si/phbl/data/astellenedvleest/h22z.rulest at line 3 4 13/4/2019 – 50:373 - Enrol[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature "astandadi" from life /our/local/si/phbl/data/astellenedvleest/h22z.rulest at line 3 4 13/4/2019 – 50:373 - Enrol[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature "astandadi" from life /our/local/signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature "astandadi" from life /our/local/signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 52, BRI_WAND_DSWATURE[39]] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 55, BRI_WAND_DSWATURE[39] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 55, BRI_WAND_DSWATURE[30] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 55, BRI_WAND_DSWATURE[30] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 55, BRI_WAND_DSWATURE[30] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 55, BRI_WAND_DSWATURE[30] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 55, BRI_WAND_DSWATURE[30] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE: 55, BRI_WAND_DSWATURE[30] - error parsing signature" astandadi 4 13/4/2019 – 50:373 - Enrol[BRECORE:
IserRules12.rules (3)		5 12/4/2019 - 05:07:34 - Emer[FRECODE: SC. ERR.]INVALID_SIGNATURE[191] error parsing signature "worproprocession" is any any -> any any (mgr [PayloadSearchFilter_Assets ctfd): Ziev="; content." [e7 bit 8 6 7
IserRules1.rules (7)		

Figure 37- Policy Setup Error

• IDS **does not** allow duplicate file names. If a user uploads a rule file which has same name, the user is prompted to remove the existing file or to rename the file to be loaded.



Alert Rulesets(Click to view Ruleset contents)	<b>0 1</b> 0	pload	A Alert QFir	!WARNING! UserRules1.rules exists. Remove the existing fil the new file before uploading again.	e or rename	esets unt.51247	Alert Ruleset Contents Deactivate Ruleset
merging-web_specific_apps.rules-6.rules (500)	Û				ок	t contents)	
nerging-web_specific_apps.rules-7.rules (500)	Û		Protoco	y Description		TEST-50K-ONLY.rules(50652)	Protocol Description
nerging-web_specific_apps.rules-8.rules (500)	Û				drop.rules-1.rule emerging-ftp.rul		
nerging-web_specific_apps.rules-9.rules (500)	Û					.rules-10.rules(500)	
merging-worm.rules-1.rules (11)	Û						
otocol-voip.rules (265)	Û						
le_file_40000.rules (40039)	Û						
22.rules (1)		<b>A</b>					
2.rules (1)		▲					
rules-1.rules (499)	Û						
File already	Û						
serRules12.rules (3) exists							
serRules1.rules (7)							
			Ŧ				

Figure 38-Policy Setup Duplicate Filename Error Warning

• The monitoring application allows up to 54K set of rules to be active at any one time.

## 6.3.1 Creating and Uploading User Defined IDS Alert Rulesets

Besides the list of extensive rules and signature based alerts which come packaged with the system, the application also allows the user to define their own rulesets and upload/activate them for alert monitoring based on their specific needs.

• In order to create a ruleset, it is important to understand the rule format supported by Suricata.

Note: Please refer to Appendix G "Understanding Rulesets" for more details).

- Once the user is familiar with the rule format it is easy to create user defined rule-set. These rules must be created in a **plain text file** and saved with extension (.rules), in order to be recognized by the application.
- Once the rule is created/saved, it can be uploaded into the application to produce desired alerts.

Perform the following to create and upload a user defined ruleset file:

### <u>Step 1</u>

- Create a plain text file using a note pad (Windows) or vi editor (Linux/Unix)
- Type in the ruleset in the correct format (Described in the section Understanding a ruleset Appendix F) and save with extension as (.rules).

Example:

```
UserDefined.rules - Notepad
```

```
File Edit Format View Help

pass tcp [192.168.16.11/20] any -> any 1616 (msg:"[abcd not is OK]"; sid:59890; )

alert ip [1.1.127.126] any -> any any (msg:"[1.1.127.126 is OK]"; sid:300; )

alert ip [1.1.66.11/10] any -> any any (msg:"[1.1.66.11/10 is working]"; sid:302; )
```

Step 2

×



.

### • On the UI go to Policy Setup $\rightarrow$ IDS Rules tab.

Alert Rulesets(Click to view Ruleset contents)	Upload	A Alert Ruleset Contexts Activate Ruleset Download UserRulest.rules(7) QFind	EActivated Alert Roberts Limit:54000 CurrentCount:51247 (Click to view Ruleset contents)	A Alert Ruleset Contents Deactivate Ruleset
Deskap > Rules > test Crigaria     New Color     Son Color     Deskap     Deskap     Document     Docume	V D Search Inst P DesencoEfficie  VTF4/0218 12:05 MM VTF4/0218 12:05 MM V All Files (?; Open Cancel  All	Click to         Click to           p         (5.5.5.5) is Critically ud2222;         p           p         (15.5.5.5) is Critically ud2224;         p           p         (15.1.1) is Critically ud2233;         p           p         (16.6.1.1) is Critically ud224;         p           p         (16.7.1.7.2.2) is Critically ud226;         p           p         (10.6.1.7.2.2) is Critically ud2266;         p           tp         (10.6.1.7.2.2) is Critically ud2666;         tep           tp         [166 not is OK; ud2777;         p         [22 is the bed]; uid 8688;	Cost is view indext commit cost-in-indextex-TEST-SOLVEY.nikes(59652) drop.nike-1.nikes(30) emerging-trajen.nikes-10.nikes(500) emerging-trajen.nikes-10.nikes(500)	Protocol Description
4es-1 rules (499) des-2 rules (267) Rules 12 rules (3) Rules 1 rules (7)		~	· · · · ·	

#### Figure 39-Policy Setup Upload Step 2

- Click on upload button at the top.
- Select the ruleset you want to upload.
- Once uploaded, click the ruleset to display its contents.
- Click "Activate Ruleset" to activate the User Defined ruleset. All activated rules appear in the activated ruleset column.
- Once the ruleset is activated, the capture server generates an alert, as defined by the alert ruleset. These alerts can be viewed in the Threat Hunting Workflow→IoC Manager → Defended Alerts (Only if defended asset and a defended service are part of its 5-tuple, and alert's source or destination IP address is a defended asset AND the alert's source or destination port is a defended service) or Undefended Alerts tab (Only if the alert's source or destination IP address is NOT a defended asset OR the alert's source or destination port is NOT a defended service).

		tup 👁 Investigator Q Search 🛔 View Meta		🖺 Reports 🌣 Configuration 🥹 Help 🔅
		Adalware      SuspIPAlerts      UndefendedA     Defended Alerts: nc 113	lerts <u></u> ActiveTriggers ≡NetFlows <b>@</b> DNS <b>∦</b> Files ⊘ I	HTTP SEmail STLS/SSL VOIP We UserAgents Find Text Setresh Page Download Copy to
Q Search Logs	Federated Nodes	Defended Alerta. Ito_113		Phild Text
	g1::nc 113		H Prev Page 1	Next Page 🍽
Begin Time		loC	Timestamp	SessionInfo
2019-12-31 19:55:00	g2::nc_157	291 [1.1.66.11/10 is working]	2020-01-01 00:49:08	1.1.71.4:52263 TCP 1.2.123.51 21
		291 [1.1.66.11/10 is working]	2020-01-01 00:49:08	1.2.123.51:21 TCP 1.1.71.4 52263
nd Time		291 [1.1.66.11/10 is working]	2020-01-01 00:44:56	1.1.71.4:52263 TCP 1.2.123.51 21
2019-12-31 19:55:00		291 [1.1.66.11/10 is working]	2020-01-01 00:44:56	1.2.123.51:21 TCP 1.1.71.4 52263
Constant Filling 170		32 File Found over SMB	2020-01-01 00:43:07	192.168.15.67:54051 TCP 192.168.16.11 445
og Search Filter [?]		32 File Found over SMB	2020-01-01 00:43:07	192.168.15.67:54051 TCP 192.168.16.11 445
etum only events that have the supplied pattern(s)		32 File Found over SMB	2020-01-01 00:43:07	192.168.15.67:54051 TCP 192.168.16.11 445
		32 File Found over SMB	2020-01-01 00:43:07	192.168.15.67:54051 TCP 192.168.16.11 445
ax Rows		32 File Found over SMB	2020-01-01 00:43:07	192.168.15.67:54051 TCP 192.168.16.11 445
000 🗘		32 File Found over SMB	2020-01-01 00:43:07	192.168.15.67:54051 TCP 192.168.16.11 445
		32 File Found over SMB	2020-01-01 00:43:07	192.168.15.67:54051 TCP 192.168.16.11 445
SentryWire	iboard 🖪 Policy Set	32 File Found over SMB tup ● Investigator Q Search	2020-01-01 00:43:07	192.168.15.67.54051 TCP 192.168.16.11 445
SentryWire #Dash	SuspSig(JA3)Alerts	tup 👁 Investigator Q Search 🗂 View Metad		🖺 Reports 🌣 Configuration 🛛 Help 🔅
SentryWire #Dash	Federated Nodes	tup @ Investigator Q Search 🛱 View Metad	lata	Reports & Configuration @ Help @
SentryWire ∰Dash	Federated Nodes	tup @ Investigator Q Search 🛱 View Metad	iala erts eActiveTriggers MENetFlows GONS #Files ()) i	TTP Temail &TLS/SSL VOIP & UserAgents Find Text @Refresh Page & Download Copy to the Copy
SentryWire #Dash DefendedAlerts &SuspDomains & Q Search Logs gin Time	Federated Nodes	Investigator Q Search & View Meta Maiware OsuspiPAterts Undefended At Undefended Aterts: nc_113	iata ActiveTriggers ExetFlows QONS # Files () f (# Prev Page 1	TTP SEmail &TLS/SSL VOIP & UserAgents Find Text CRefresh Page Download Cropy to 1 Next Page >>
Sentry Wire #Dash DefendedAlerts &SuspDomains & Q Search Logs gin Time 015/231 154400	Federated Nodes	II Uup © Investigator Q Search & View Metar Matware ©SuspIPAterts & UnderendedAt Underended Aterts: nc_113 Inderended Aterts: nc_113	lata ActiveTriggers IENetFlows QDNS & Files ()   (4 Prev Page 1 Timestamp	Reports & Configuration Q Help      TTP      Email & TLS/SSL \VOIP & UserAgents     Find Text     Refresh Page & Download & Copy tor     Next Page      Sessioninto
Sentry Wire #Dash DefendedAlerts \$SuspDomains \$ Q Search Logs ngin Time 015-1231 194400	Federated Nodes	II Ung @ Investigator Q Search & View Metar Malware & SuspiPAterts & UndefendedAt UndefendedAterts: nc_113 Inc BC @0711 [1:259.105 is very useful]	ents CActiveTriggers EENetFlows QDNS IF Files () 1 (4 Prev Page 1 Timestamp 2020-01-01 00 30 04	Reports  Configuration
SentryWire #Dash DefendedAlerts \$SuspDomains \$ a Search Logs gin Time Dish231 184400 d Time	Federated Nodes	II View Metael View Materia SuspiPAteria View Metael Materia SuspiPAteria Undefended Al Undefended Aleria: nc, 113 Inc. 66711 [12.29.105 is very useful] 66711 [12.29.105 is very useful] 67711 [12.29.105	ActiveTriggers         ENetFlows         ODNS         #         Files         I           Immestamp         2008-01-01         00.004         2008-01-01         00.004           2008-01-01         00.00.004         2008-01-01-01         2008-01-01-01         2008-01-01-01         2008-01-01-01         2008-01-01-01         2008-01-01-01         2008-01-01-01 </td <td>Reports &amp; Configuration Q Help      TTP = Email &amp; TLS/SSL &lt; VOIP &amp; UserAgents     Find Text     Refersh Page Download C Copy to     Sessionine     1.2.0.105.21 TCP 1.1.7.22 16461     1.2.0.105.21 TCP 1.1.7.20 1646</td>	Reports & Configuration Q Help      TTP = Email & TLS/SSL < VOIP & UserAgents     Find Text     Refersh Page Download C Copy to     Sessionine     1.2.0.105.21 TCP 1.1.7.22 16461     1.2.0.105.21 TCP 1.1.7.20 1646
SentryWire &Dash DefendedAlerts &SuspDomains & & Search Logs gin Time 715-12-31 1844 00 d Time DISh12-31 1844 00	Federated Nodes	Average of the set of the se	ActiveTriggers ENetFlows QDNS IF Files () 1 (I Prov Page 1 2020-01-01 00.30.04 2020-01-01 00.30.03 2020-01-01 00.30.03 2020-01-01 00.30.03 2020-01-01 00.20.00	Reports  Configuration
Sentry Wire Dash DefendedAlerts &SuspDomains & Q Search Logs gin Time ors:1231 19460 d Time g Bearch Filter [7]	Federated Nodes	II	Image: Termingers         ExhetFlows         QONS         # Files         1           Image: Termingers         Termingers         Termingers         1           Termingers         2008-01-01 00-30.064         2008-01-01 00-30.064         2008-01-01 00-30.063         2008-01-01 00-30.003         2008-01-01-01 00-30.003         2008-01-01-01-01-01-01-01-01-01-01-01-01-01-	Reports  Configuration
Sentry Wire #Dash DetendedAlerts &SuspDomains & Search Logs gin Time 01543231 184400 d Time 5154231 184400 g Bearch Filter [7]	Federated Nodes	II         IVerstigator         Q Search         IVers Metar           Up         Investigator         Q Search         IVers Metar           Mahware         SupplPAtents         IUndefendedAlerts         IVers           UndefendedAlerts         Inc.         III3         IVers           60711 [12.28.105 is very usetel]         60711 [12.28.105 is very usetel]         27 Firs Foord over SMB         22 Firs Foord over SMB         23 Firs Foord over SMB         24 Firs Foord over SMB         25 Firs Foord over SMB<	Initial         Image: Im	Reports         Configuration         Q Help           ITTP         Email         ▲TLS/SSL         ▲VOIP         ▲ UserAgents           Find Text         ● Refresh Page         ▲ Download         ● Copy to           Nott Page         ●         ●         ●           12.69 H0521 TCP 11.792 16451         12.69 H0521 TCP 11.792 16451         12.69 H0521 TCP 11.792 16451           172.20 130 52.445 TCP 112.20 39 154 46523         172.20 130 52.445 TCP 112.20 39 154 46223         172.20 130 52.445 TCP 112.20 39 154 46223           172.20 130 52.445 TCP 112.20 39 154 46223         172.20 130 52.445 TCP 112.20 39 154 46223         172.20 130 52.445 TCP 112.20 39 154 46223
Sentry Wire Dash Control Cont	Federated Nodes	II IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Image: Control of the second	Reports   Configuration
Sentru Wire      Composition     Composit	Federated Nodes	II	ActiveTriggers IENetFlows QDNS IN Files ()	Reports         Configuration         Q Help           HTTP         Email         ▲TLS/SSL         ▲VOIP         ▲ UserAgents           Find         C Refresh Page         ▲ Download         C Copy for           Next Page         ●         ●         ■         ■         C Copy for           12.69.10521 TCP 11.732 15461         1.26.910521 TCP 11.732 15461         ■ </td
Sentry Wire & Dash DefendedAlerts & SuspDomains &      Q Search Logs      egin Time      2016-12-31 104-00      og Search Filler [7]      og Search Filler [7]      tax Rows	Federated Nodes	II IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Image: Control of the second	Reports   Configuration

#### Figure 40-Defended vs. Undefended Alerts

• To stop receiving alerts for User Defined Ruleset simply click on the Deactivate ruleset button. The ruleset is still available in the Ruleset library and can be reactivated until deleted permanently.



*Note*: A guest user cannot Add or Delete rules.

## 6.4 AUGMENTATION

Augmentation allows users to upload additional data that can be used to enhance the value of stored data and allow data correlation.

Augmentation panel allows users to upload 4 types of meta-metadata that allows analysts and the DPI engine to augment it. **Note**: The system comes preloaded with all Suspicious TLS/SSL Signatures, Suspicious IP Addresses, Suspicious Domains and Malware . A user can also upload their own list for monitoring.

- Suspicious TLS/SSL Signatures
  - JA3 is a method for creating TLS/SSL client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.
  - Clicking on the hyperlink **Suspicious TLS/SSL Signatures** will display all the currently uploaded Suspicious TLS/SSL clients in Kibana.

SentryWire #Dashboard Policy Setup @ Inv	estigator 🝳 Search 着 View Metadata	🖺 Reports 🌣 Configuration 🛛 Ø Help	o 🕞 Logout
置Augmentation			
	Discover / ja3	¢	0 0
	New Save Open Share Inspect		
	# ~ Search	KQL C'R	Refresh
E			
	?_source     > JA3: b386946a5e44d1ddcc843bc75336dfce Description: Dridex _id: oMRKYW8BpZXwqft       Available fields     o	'8vzfW _type: ssltls _index: ja3_01012020	
¢	Popular         > JA3: 8991a387e4cc841740f25d6f5139f92d Description: Adware _id: ocRKYW88pZXwqf           t_lype         _score: 0	8vzfW _type: ssltls _index: ja3_01012020	
	? Description       JA3:       cb98a24eedb9134448ffb5714fd870sc       Description:       Dridex       _id:       osRKYW88pZXwqf       _score:	/8vzf₩ _type: ssltls _index: ja3_01012020	
- 6	The second se	<pre>ifT8vzfW _type: ssltls _index: ja3_01012020</pre>	
< > 6	JAS: 3089080TD1T844491108T8/5238T80800 Description: Adware _10: pMMKTW88p2XwqT	/8vzfW _type: ssltls _index: ja3_01012020	
			* *

Figure 41-Policy Setup Suspicious TLS/SSL Signatures

- When a Suspicious JA3 appears in the traffic the system generates an alert. This can be viewed in View Metadata→SuspSig(JA3)Alert tab for each Group:Node.
- To upload a user desired list for JA3 simply click on the upload icon. The user can then upload a .csv file that must contain JA3 signature name, comma separator and an optional description. (For more details on upload please refer to section 4.4.1)
- The user can also download a list by clicking the download button as a csv.
- Suspicious IP Addresses



- These are class of IP addresses that are considered as unsafe and unreliable within a network traffic.
- Clicking on the hyperlink Suspicious IPAddresses will display all the currently uploaded Suspicious IPAddresses in Kibana.

icious IPAddresses	Discover	Share In	snert		0
icius Domains 📩 🛓	Image: Open with the second secon	ondre m.		KQL	C Refresh
	suspicious-ip*       Selected fields       It     SuspiPAddress       It     description       Available fields       It     _id       It     _index	o	description           > port 447, TrickBot           > port 80, Heodo           > port 8080, Heodo           > port 8080, Heodo           > port 808, Heodo           > port 80, Heodo           > port 447, TrickBot	1,486         hits           SuspIPAddress           107.172.29.110           210.224.65.117           176.106.183.253           1.32.54.12           188.216.24.204           130.45.45.31           64.44.133.151           144.217.50.246	
· · · · ·	© ⊕ ⇒		> port 443, Heodo > port 88, Heodo > port 8080, Heodo	193.33.38.208 188.230.134.205 58.171.42.66	

Figure 42-Policy Setup Suspicious IPAddresses

- When a SuspiciousIP appears as source IP or destination IP in the traffic the system generates an alert. This can be viewed in View Metadata→SuspIPAlert tab for each Group:Node
- To upload a user desired list for SuspiciousIPs simply click on the upload icon. The user can then upload a .csv file that must contain SuspiciousIPs name, comma separator and an optional description. (For more details on upload please refer to section 4.4.1)
- The user can also download a list by clicking the download button as a csv.
- Suspicious Domains
  - Domain names are an important avenue to investigate security incidents or to prevent some malicious activity to occur on your network.
  - Clicking on the hyperlink Suspicious Domains will display all the currently uploaded Suspicious Domains in Kibana.



User Guide January 30, 2020

Sentry Wire #Dashboard 🔦 Policy Setup	Invest	tigator 🍳 Search 🛔 View Meta				Reports 🏟 Configuration	Help	🕞 Logo
Augmentation								
spicious TLS/SSL Signatures		Discover					0	e
spicious IPAddresses								-
spicious Domains	O	New Save Open Share	Insp	ect				-
liware 1	0	# 🗸 Search				KQL	C Ref	resh
		suspicious-doma 🗸 🔇	3	1	136 hits			
	企	Selected fields		SuspDomain		Description		
	5	t Description	>	p237996.mybestmv.com		-		
	盦	? SuspDomain	>	vsedveri-33.ru		141) 141		
		Available fields	>	www.hanecaklaw.com				
	69	t_id	>	www.chemes.eu		-		
		t _index	>	chong.joelle.free.fr				
	G	# _score	>	audetlaw.com				
	E	t _type						
	5		>	kahverengider.org		-		
			>	businessaviators.com		-		
	5		>	bucksmedia.go2cloud.org				
			>	estudiobarco.com.ar				
	⇒		>	bolizarsospos.com				

Figure 43-Policy Setup Suspicious Domain

- When a Suspicious Domain appears in the traffic the system generates an alert. This can be viewed in View Metadata→SuspDomain alert tab for each Group:Node
- To upload a user desired list for Suspicious Domain simply click on the upload icon. The user can then upload a .csv file that must contain Suspicious Domain name, comma separator and an optional description. (For more details on upload please refer to section 4.4.1)
- The user can also download a list by clicking the download button as a csv.
- Malware
  - This category allows users to upload known bad md5sums for allowing the software to identify/alert when a file with bad md5sum is being transmitted.
  - Clicking on the hyperlink Malware will display all the currently uploaded md5sum in Kibana.



SentryWire #Dashboard < Policy Setup @	linves	itigator 🍳 Search 🗂 View Metao	lata	🖺 Reports 🌣 Configuration 🛛 Help 🛛 Թ Logou
Augmentation				
Suspicious TLS/SSL Signatures	K	Discover		© •
Suspicious IPAddresses	O	New Save Open Share In	ispect	
Suspicious Domains	0	# ✓ Search		KQL C Refresh
		md5sum_* 🗸 🔇	134	1,727 hits
		Selected fields	MD5sum	Description
	5	t Description	> 5aa907731a03af160a45ec3050cf40a2	Heodo
	â	t MD5sum	> 973eb0b20c62c0ebb87e56fcd0c141a1	Heodo
	٩	Available fields	> 7197c3b9b14a4a192d627d27b5eb8c8a	Heodo
	69	t _id	> a02507baeafecc1929a3e43e2d409158	Heodo
	G	t _index	> a49dd325a6c86a8325319f19bf8b0ae0	Heodo
	ľ	# _score	> a51cb71ebe049e3797a40b57c3b421fa	Heodo
		t _type	> a0a96bbb99dd5a46cd338b3f5330e5b3	Heodo
	2		> 54bae4a4efe461f6a677199483ede11e	Heodo
۳ ۱	3		> 675f13cf69de5400be60bc61407bbfc1	Heodo
	⊕		> d330a103fbb36b659f17d5448efa5dc0	Heodo
	⇒		> 654db8856278f3f219bfc7713ad6a16b	Heodo

Figure 44-Policy Setup Malware

- When a Suspicious Malware appears in the traffic the system generates an alert. This can be viewed in View Metadata→Malware alert tab for each Group:Node
- To upload a user desired list for Malware simply click on the upload icon. The user can then upload a .csv file that must contain Malware name, comma separator and an optional description. For more details on upload please refer to section 6.4.1
- The user can also download a list by clicking the download button as a csv.

## 6.4.1 Uploading Augmentation

User can upload augmentation data in a csv file format as below.

- First column of each row should state a resource
- Second column (optional) of each row should describe the resource in the first column. This is optional but generally a good practice for easy reference.

**Example** of a SuspiciousIPs csv file:

172.20.17.67, system1 100.100.100.104, system2 8.8.8.8 8.8.4.4, system3

To upload the data simply click on upload icon. Once uploaded they are displayed in Kibana.



Sentry Wire *Dashboard  Policy Setup	nvestigator Q Se	arch 💩 View Metadata	E R	eports 🌣 Configuration 🛛 Ə Help	D 🕩 Logout
Augmentation					
Suspicious TLS/SSL Signatures	K Di Di	cover / ja3			o 💿 🔒
Suspicious IPAddresses	-				
Suspicious Domains		e Open Share Inspect			_
	# ~	Open	×	KQL C F	Refresh
Malware 📩 🛓		- 🔶 👻 🛉 🧯 > This PC > Desktop	✓ Ů Search test		
	ŵ · ·	Organize • New folder	Æ · 🔳 🙆		
	ja3_*	Shared favorites ^ Name	Date modified Type		
	Selecte	This PC	4/16/2018 4:09 BM		
	2_sour	3 3D Objects Critical 171.csv	7/2/2018 2:12 PM Microsoft T8vzfW _ty	e: ssltls _index: ja3_01012020	
	Availab	Desktop			
	Popular	Documents	Tour fill the	e: ssltls _index: ja3_01012020	
	t_type	Downloads	IOV21W _CVI	e. ssicis _index. ja5_01012020	
	Car ? Desc	♪ Music	1		
	🗐 ? JA3	F Pictures	T8vzfW _typ	e: ssltls _index: ja3_01012020	
		Videos			
	E t_id	👟 OS (C:)	-57054	ype: ssltls _index: ja3_01012020	
	ी t_inde	🛋 Matuark 🗸 🤟	> 41107214 -	ype, ssicis _index, jas_01012020	
4 · · · · · ·	# _scor	File name:	Microsoft Excel Comma Separat		
	۵	Price Harries	T8vzfW_ty	e: ssltls _index: ja3_01012020	
	⇒		Open Cancel		
	_				*

Figure 45-Policy Setup Upload Augmentation file

## 6.5 ACTIVE TRIGGERS

Active triggers allow you to get alerts when you specify an event to cause the trigger.

*For example*: You can specify an IP address as the search filter and you will see an alert when traffic containing the IP address is captured.

- To generate a trigger specify the trigger name and time frame (Seconds Before and Seconds After) and a valid BPF filter.
- The Add button allows the user to create an active trigger (max 100)
- The delete button allows you to delete the configured trigger.



Sentry	Wire #Da	shboard	Policy Setup @ Inve	estigator 🝳 Search 🛔 View Metadata	Reports 🌣 Configuration	Help	
EActive Triggers ( ?	Maximum Count: 100	)					
Node Name	Trigger Name	Seconds Before	Seconds After	Search Filter		Action	÷
	AT_14_53_47	30 🗘	30 0	searchfilter="tep or udp"		+ Add	
Boston::nc_113	AT_0_28_57	30	30	top		1 Delete	
Boston::nc_135	AT_1_9_10	30	30	udp.		Delete	
Boston::nc_113	AT_14_35_1	30	30	host 10.91.170.22 and port 38638 and host 204.11.16.106 and port 25 and tcp		1 Delete	
Boston::nc_113	AT_14_35_41	30	30	(host 10.0.2.20 and port 5060 and host 10.0.2.15 and port 5060 )		Delete	
Boston::nc_135	AT_14_36_31	30	30	host 10.91.170.22 and port 38638 and host 204.11.16.106 and port 25 and tcp		Delete	

#### Figure 46 Add Active Trigger

Q Search Logs	Federated Nodes	Active Triggers: nc_113		Find Text CRefresh Page Download Copy to Ch
	Bostonine 113		H Prev Page 1	Next Page >>
egin Time	DOMONTING_113	loC	Timestamp	SessionInfo
2020-01-1/ 12:50.00	California::no_130	AT_1_9_10-udp	2020-01-17 17:48:33	195.241.77.54:53 udp 172.16.9.171:1306
		test-top or udp	2020-01-17 17:48:33	172.16.9.171:2544 top 64.233.183.103:80
nd Time		AT 12 11 0-tcp	2020-01-17 17:48:33	172.16.9.171:2544 top 64.233.183.103:80
2020 01 17 12 50 00		AT 0 28 57-tco	2020-01-17 17:48:33	172.16.9.171:2544 top 64.233.183.103:80
		AT 1 9 10-udp	2020-01-17 17:46:23	195,241,77,54:53 udp 172,16.9,171:1042
og Search Filter [?]		test-tcp or udp	2020-01-17 17:46:23	172.16.9.171:2544 top 64.233.183.103:80
return only oversits that have the supplied pattern(s)		AT 12 11 0-lcp	2020-01-17 17:46:23	172.16.9.171:2544 top 64.233.183.103:80
		AT_0_28_57-1cp	2020-01-17 17:46:23	172.16.9.171.2544 top 64.233.183.103.80
lax Rows		AT_1_9_10-udp	2020-01-17 17:46:23	195.241.77.54:53 udp 172.16.9.171:1042
2000		test-tcp or udp	2020-01-17 17:46:23	172.16.9.171:2544 top 64.233.183.103:80
		AT_12_11_0-lcp	2020-01-17 17:46:23	172.16.9.171:2544 top 64.233.183.103:80
Q Search Logs		AT_0_28_57-1cp	2020-01-17 17:46:23	172.16.9.171.2544 top 64.233.183.103:80
		AT_1_9_10-udp	2020-01-17 17:26:50	195.241.77.54:53 udp 172.16.9.171.2586
		test-tcp or udp	2020-01-17 17:26:50	172.16.9.171:2544 tep 64.233.183.103:80
		AT_12_11_0-tcp	2020-01-17 17:26:50	172.16.9.171:2544 lop 64.233.183.103:80
		AT_0_28_57-tcp	2020-01-17 17:26:50	172.16.9.171:2544 top 64.233.183.103:80
		test-tcp or udp	2020-01-17 17:24:40	195.241.77.54:53 udp 172.16.9.171:1042
		AT_1_9_10-udp	2020-01-17 17:24:40	195.241.77.54:53 udp 172.16.9.171:1042
		AT_12_11_0-lcp	2020-01-17 17:24:40	172.16.9.171:2542 lop 64.233.183.103:80
		AT_0_28_57-tcp	2020-01-17 17:24:40	172.16.9.171:2542 top 64.233.183.103:80

Figure 47 - View Active Trigger Events

- The trigger events can be seen in the Threat Hunting Workflow → IoC Manager → Active triggers tab.
- Clicking on an active trigger event will automatically fill out a search request within the specified time parameters around the triggered event (Seconds Before and Seconds After).

#### Note:

Please refer to Appendix D for more information about the BPF filters supported by the application A guest user cannot add or delete Active Trigger.

### 6.6 PRECAPTURE FILTER

PreCapture filter filters network traffic before writing the traffic to disk. A PreCapture filter can be specified within the PreCapture Filter menu. PreCapture Filter can be set in one of two methods discussed in the following sections.

Note:

If a BPF filter is set and a set of IPaddresses are loaded, the **BPF** filter is **ignored**. A guest user cannot add or delete PreCapture



## 6.6.1 Applying a Berkeley Packet Filter (BPF)

A capture filter can be applied in the form of a BPF filter. As a BPF filter the PreCapture takes the form of primitive expressions connected by conjunctions (and/or) and optionally preceded by not.

- To specify a PreCapture filter fill out the "Filter Name" and "Search Filter", then select the "Set" button to apply the PreCapture filter.
- Select the delete button to permanently delete the filter.

Below are some use cases examples of PreCapture filter application:

- "not dst port 80" will drop all traffic destined for port 80
- "host 1.2.3.4 or host 1.1.1.1" captures only the traffic for these two hosts while filtering out the rest of the traffic.

Sentry Wire	BaDashboard 🔦 Policy Setup ♦ Threat Hunting Workflow		Q	Messaging 🔅 C	onfiguration 🛛 Help 👻 🗭 Logout
I PreCaptureFilter		PreCaptureFilter:On	Critical Alerts		<b>≛</b> Download
Filter Name	Search Filter	Action	TimeStamp	Туре	Message
Filter1	searchfilter="tcp or udp"	+ Set	2018-07-26 16:08:48	ActiveTrigger	Deleted,AT_0_11_1
Filter1			2018-07-26 06:18:45	AnalyticsMode	Changed,On
Piller)	tcp	Delete	2018-07-26 06:18:37	AnalyticsMode	Changed,Off
			2018-07-25 16:55:02	Admin	UserAdded,User test1234 has been added
			2018-07-24 19:28:49	PreCaptureFilter	Reset
			2018-07-24 19:28:17	AnalyticsMode	Changed,On
			2018-07-24 19:28:15	PacketCapture	Started
			2018-07-24 19:28:03	PreCaptureFilter	Reset
i■PreCapture Assets		Upload	i Precapture Assets D	etails() Address	
	Name	Action	IPA	adress	Name

Figure 48-Applying BPF Filter

Notes:

- A detailed list of valid BPF filters supported is provided in Appendix D
- When a valid BPF filter is applied the status bar reports "PreCapture filter: **On**"
- When an invalid filter is applied "PreCapture filter: **Off**" status is displayed both on dashboard and *PreCapture filter tab status bar*.

### 6.6.2 Uploading PreCapture Assets as a File

In addition to the BPF filter, the application also allows the user to upload a list of IP addresses to be applied as a PreCapture filter. Multiple files that contain a list of valid IP addresses can be uploaded at the same time. The application allows only a maximum of 32 unique IP addresses to be applied at a given time.

Note: If a BPF filter is set and a set of IP addresses are loaded, the **BPF** filter is **ignored**.

Perform the following to create and upload a PreCapture Filter:

### Step 1: PreCapture Assets File Format

Users can define a list of IPs intended to be applied as PreCapture filters, in a **csv** file as per the format below:

- First column of each row should state an IP address (resource).
- **Second column (optional)** of each row should describe the resource in the first column. This is optional but generally a good practice for easy reference.



Example of a PreCapture Assets csv file:

1.2.112.6, System1

1.2.30.6

## Step 2: Uploading a User PreCapture Assets File

- Create a <Filename>.csv file on your local system.
- Click on Upload button.
- Select file from the local system to be uploaded.

PreCaptureFilter		PreCaptureFilter:On	Critical Alerts	5		Down
Filter Name	Search Filter	Action	TimeStamp	Туре	Message	
Filter1	searchfilter="top or udp"	+ Set	2018-07-26 16:08:48	ActiveTrigger	Deleted,AT_0_11_1	
			2018-07-26 06:18:45	AnalyticsMode	Changed,On	
Filter1	tcp	🛍 Delete	2018-07-26 06:18:37	AnalyticsMode	Changed,Off	
			2018-07-25 16:55:02	Admin	UserAdded,User test1234 has been	n added
			2018-07-24 19:28:49	PreCaptureFilter	Reset	
			2018-07-24 19:28:17	AnalyticsMode	Changed,On	
			2018-07-24 19:28:15	PacketCapture	Started	
			2018-07-24 19:28:03	PreCaptureFilter	Reset	
PreCapture Assets	Name	O Upload	i Precapture Assets D	Address	Name	
PreCapture Assets	Name					
PreCapture Assets	Name	© Open	- IP/	Address	×	
■PreCapture Assets	Name	© Open ← → ~ ↑ ■ > This PC > Desktop > 4	- IP/	Address	x arch 409TestBed	
PreCapture Assets	Name	© Open	- IP/	Address ✓ ঊ Sea	arch 409TestBed P	
PreCapture Assets	Name	© Open ← → → ↑ → This PC > Desktop > 4 Organize • New folder Name	109TestBed	Address	arch 409TestBed P 	
PreCapture Assets	Name	Open $\leftarrow \rightarrow \land \uparrow \blacksquare \rightarrow This PC > Desktop > 4     Organize · New folder     # Quick access                                 $	109TestBed	Address ✓ ঊ Sea	arch 409TestBed P 	
PreCapture Assets	Name	© Open ← → → ↑ → This PC > Desktop > 4 Organize * New folder # Quick access → Desktop # □ Rame □ PrecaptureAsse	109TestBed	Address	arch 409TestBed P 	
EPreCapture Assets	Name	Open     ← → → ↑ → This PC > Desktop > 4     Organize * New folder     # Outck access     # Destrop → 4     Downloads →	109TestBed	Address	arch 409TestBed P 	
EPreCapture Assets	Name	© Open ← → → ↑ ▲ → This PC → Desktop → 4 Organize * New folder # Quick access ▲ Desktop → 4 ▲ Desskop → 4	109TestBed	Address	arch 409TestBed P 	
EPreCapture Assets	Name	© Open ← → → ↑ → This PC > Desktop > 4 Organize • New folder → Quick access → Desktop → → Downloads + → Downloads + → Pictures +	109TestBed	Address	arch 409TestBed P 	
EPreCapture Assets	Name	© Open ← → → ↑ ▲ → This PC → Desktop → 4 Organize * New folder # Quick access ▲ Desktop → 4 ▲ Desskop → 4	109TestBed	Address	arch 409TestBed P 	
EPreCapture Assets	Name	© Open ← → → ↑ → This PC > Desktop > 4 Organize • New folder → Quick access → Desktop → → Downloads + → Downloads + → Pictures +	109TestBed	Address	rch 409TestBed P Fill - Microsoft Excel * 220 PM Microsoft Excel	

Figure 49 Uploading PreCapture Asset File

• The figure below depicts one PreCapture IP asset list containing 13 IP addresses.



PreCaptureFilter     NodeName	Filter Name	Search Filter	Action	i Precapture Assets Details NodeName:nc_130 FileName:1580182177253_PrecaptureAssetList.csv		
Nodename	Filter Name		Action	IPAddress	Name	
	Filter1	searchfilter="tcp or udp"	+ Set	1.2.112.6		
BostonMA::nc 130	Filter1	udp		1.2.30.6		
			T Delete	172.16.133.6		
NashuaNH::nc_113	Filter1	udp	1 Delete	173.194.123.76		
				192.168.43.1		
				43.143.186.83		
				69.191.6.64		
				74.125.226.89		
				8.8.8		
ImpreCapture Assets		Narna	© Upload			
I■PreCapture Assets NodeNam BostonMA::nc	ne	Name 1980 1821 77253. PreceptureAssetList.csv	Action	-		
NodeNam BostonMA::no	ne c_130	1580182177253_PrecaptureAssetList.csv				
NodeNam	ne c_130		Action			

## Figure 50-Sample Pre-capture IP Asset List

• As more files are uploaded, the application takes the first 32 unique IP addresses and allows the traffic only if source IP or destination IP is among these 32 addresses.

*Note*: A guest user cannot add or delete PreCapture.



# 7 INVESTIGATOR

Investigator panel allows users to view Kibana Dashboard and Discover views of each federated node. It also allows the users to create a search across all selected nodes for further analysis.

Users can switch to the desired Kibana Discover window by selecting a node from the list displayed in the left sub panel.

SentryWire #Da	ashboard 🔸 Policy Setu	🐠 👁 Investigator 🝳 Search 畠 View Metadata		🔓 Reports 🔅 Configuration	Help	🕩 Logout
PreCaptureFilter				Precapture Assets Details NodeName:nc_130 FileName:1580182177253_PrecaptureAssetList.csv		
NodeName	Filter Name	Search Filter	Action	IPAddress	Name	
	Filter1	searchfilter="tcp or udp"	+ Set	1.2.112.6		
BostonMA::nc_130	Filter1	udp		1.2.30.6		
bootonin care_100	1 1001	unb.	T Delete	172.16.133.6		
NashuaNH::nc_113	Filter1	udp	Delete	173.194.123.76		
				192.168.43.1		
				43.143.186.83		
				69.191.6.64		
				74.125.226.89		
				8.8.8		
<u></u>						
I∎PreCapture Assets			€ Upload			
NodeName		Name	Action			
BostonMA::nc_	130	1580182177253_PrecaptureAssetList.csv	View Delete			
NashuaNH::nc_	_113	1580182177253_PrecaptureAssetList.csv	View Delete			

Figure 51-Policy Setup Kibana Node Selection

The following types of metadata are available for analysis and discovery through Kibana:

Event Type	KQL Search Filter
Alert	event_type:'alert'
File	event_type:'fileinfo'
DNS	event_type:'dns'
SMTP	event_type:'smtp'
ActiveTrigger	event_type:'activetrigger'
HTTP	event_type:'http'
TLS/SSL	event_type:'tls'
SMB	event_type:'smb'
VOIP	event_type:'voip'
Suspicious IP Alerts	event_type:'suspip'
Suspicious Signature Alerts	event_type:'ja3'
Suspicious Domains	event_type:'suspdomain'

## 7.1 CREATE SEARCH WORKFLOW

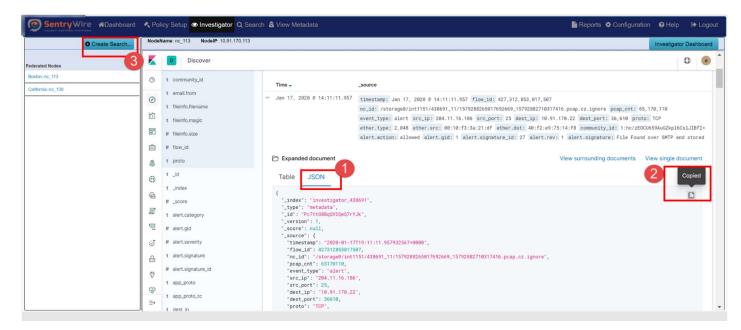


1. Once inside the Kibana Discover view of the node, select one of the displayed documents to view details(by clicking on the > of the document).

SentryWire #Dashboard	♣ Policy Setup ● Investigator Q Search  Â View Metadata	🖺 Reports 🏶 Configuration 🛛 Help 🕞 Logout
Create Search	NodeName: nc_113 NodeIP: 10.91.170.113	Investigator Dashboard
Federated Nodes	Discover	۵ 📀
Boston::nc_113 California::nc_130	# aler.rev     Itimestamp par minute       Iticommunity_id     Itimestamp par minute       Itimestamp ar minute     Itimestamp ar mi	2710317416.pcap.cz.ignore pcap_cnt: 65,170,110 10.91.170.22 dest_port: 36,610 proto: TCP
	# fileinfo.size     alert.action: allowed alert.gid: 1 alert.signature_id: 27 ale       # flow_id     t proto       It     t proto       It     id       Table     JSON	rt.rev: 1 alert.signature: File Found over SKTP and stored View surrounding documents View single document
	#_score     t_id     Pc7ttG88qQY2QeQ7rYJk       W     t_index     investigator_438691       #_score     -       #_storgd     #_score       #_storgd     t_type       #+alert_seventy     t_alert.action	

Figure 52-Investigator Window

2. Click on JSON hyperlink. This shows the JSON data for this document. Top right corner of the JSON view panel shows an icon that allows users to copy the JSON data being shown.



- 3. Click on Create button of the left sub-panel. A dialog box appears with a search name filled in and an area to paste the copied json data.
- 4. Users can modify the search name if desired.
- 5. Paste the copied JSON data and click the "Create Search" button.



			Create Search Investiga	ator Dashboard
ted Nodes	K	Discover	SearchName Search name can be modified	0
n::nc_113 mka::nc_130	©	t community_id t email.from	Search Filter  t	
	0	· · · · · · · · · · · · · · · · · · ·	1.type': metadaa', 1.st: <u>Petrussequided27/48'</u> , 2.st: <u>Petrussequided27/48'</u> , Paste the json	
	尬	t fileinfo.filename	score': null, data here //692669_15/92882/1831/416.pcap.cz.ignore pcap_cnt: 65,178,118	
	611	t fileinfo.magic	"source" [ "2020-01-17110-1111162732552-0000", "	
	30	# fileinfo.size	Thew 61 42711283007587, The 61 10 10 10 10 10 10 10 10 10 10 10 10 10	
	â	# flow_id	*/some@/wttl5/48691_11/1572882600769269_15728827037246.pono.c 2.0000: been col: 6570110,	
	2	t proto	E vewst.spen Taket, View surrounding documents View single of to the surrounding documents view single of to t	document
	Ð	t _id	"dect.ig": "10.91.170.22", "dect.port": 36610,	
	9	t _index	ipeto 1027, ieder 10 ippet 204,	D
		# _score	Create Search Cancel Request	
		t alert.category		
	ę	# alert.gid	'_score': null,	
	Î	# alert.severity	"_source": { "timestamp": "2020-01-17T19:11:11.957932567+0000",	
	<b>A</b>	t alert.signature	"flow_1d": 427312853017507, "nc_1d": "/storage0/int1151/438691_11/1579288265017692669_15792882710317416.pcap.cz.ignore",	
	(9	# alert.signature_id	"pcap_cnt": 65170110, "event_type": "alert",	
	5	t app_proto	"src_1p": "204.11.16.106", "src_port": 25,	
	ŝ	t app_proto_tc	"dest_pr(: 18.91.170.22", "dest_pr(: 36610,	

Figure 53-JSON Create Search

- 6. This allows the server to create a search based on the pasted JSON data on all the selected federated nodes.
- 7. Once the search is submitted successfully, the following alert is displayed.

Sentry wire aDashboard		cy Setup 👁 Investigator Q Search 🛔	10.91.1 says		📑 Reports 🛭 🛱 Configura	ation 🥑 Help	Le Logo
O Create Search	NodeN	ame: nc_113 NodelP: 10.91.170.113	New search named fms_2020_01_17_14_56_25_881 is in progress. Switch to Search page for status and results.			Investigator D	ashboard
	K	D Discover	ок			Q	) (e)
rated Nodes		t_index	UK .				
donting_113	O	F	app processing ,	-	View surrounding documents	View single docu	ment
fornia::nc_130		# _score	'app_proto_tc': 'failed', 'flow': {		view surrounding documents	view single docu	
	0	t alert.category	"pkts toserver": 4,				
			<pre>bts_toclient": 3, "bvtes_toserver": 289,</pre>				
	龄	# alert.gid	"bytes tacileof: 286, "start": "2020-01-17719:50:17,445654587+0000"				-
		# alert.severity	start : 2020-01-1/119(2017,445624367+0000			l	
	5		], "Welds": [				
		t alert.signature	"flow.start": [				
	<u><u></u></u>	# alert.signature_id	2020-01-17719:50:17.4452				
			"timestamp": [				
	٩	t app_proto	"2020-01- <u>17719:50:17.4457</u> "				
	0		3				
	121	t app_proto_tc	"sort") [ 1579290617445	i170317554.pcap.cz.ignore",			
	G	t dest_ip	1				
	I	# dest_port	Create Search Cancel Request				
		? dns.answers		>			
	9		"proto": "TCP",				
		? dns.authorities	"ether": {				
	3	t dns.flags	"type": 2048,				
			"src": "00:10:f3:3a:21:df",				
	ß	t dns.grouped.A	"dst": "40:f2:e9:75:14:f8"				
	4.6	# dns.id	<pre>}, "community_id": "1:TpCBkMr/qTRjmDu+2B/xG+fND2k=",</pre>				
			"alert": {				
	6	I dns.qr	"action": "allowed",				
			"gid": 1,				
	$\Rightarrow$	O dns.ra	"signature_id": 27, "rev": 1,				

Figure 54-JSON Search Success Alert

- 8. Each selected node will perform the search and return results to the Search panel.
- 9. To view and manage these searches, switch to the Search panel from the main menu.

## 7.2 INVESTIGATOR DASHBOARD



Once inside the Kibana Discover view of the node, clicking on the Investigator Dashboard button will switch to Kibana Dashboard view for the selected node.

O Create Search	NodeNa	Ime: nc_113 NodelP: 10.91.170.113					Investigator Dashboard
ated Nodes	K	Dashboard / Investigato	r_Main_DB				0
on::nc_113		Full screen Share Clone Ed	:•				
ornia::nc_130	0	Full screen Share Clone Ed	IL				
		# ✓ Search			KQL	🛗 🗸 Last 1 day	Show dates C Refresh
	0						
	企	0					
	5	Network Connections			Files		
		SourceIP	DestIP≑	Count		etile/preinstall	
	命	10.91.170.22	10.91.170.186	35,672	/ADSAdClie		
	۹	10.91.170.22	204.11.16.106	688	<u></u>	g6ywwnRqTq5.txt	
		10.91.170.22	10.91.170.1	385	/isapi/redir.		
	0	192.168.16.11	192.168.15.67	5,347	/menu/img_	_menu.gif	
	6	192.168.16.11	192.168.15.64	4,476	/minitri.flg	ments/blank.gif	
		192.168.16.11	192.168.15.93	3,980		s/whitepixel.gif	
	I	192.168.16.11	64.15.168.192	2,820	/filling.htm		
	Ę	192.168.16.11	192.168.15.71	2,491	/select.php		
		192.168.16.11	192.168.15.59	2,365	/firefox	ł.	
	9	192.168.16.11	192.168.15.60	2,252	/fd/ls/lsp.as	env	
	6				/mail/html/l		
		Export: Raw & Formatted &			manymenny	our and the second s	

Figure 55-Investigator Dashboard



# 8 SEARCH

### 8.1 SEARCH PANEL OVERVIEW

The Search panel allows users to create and manage searches, view individual streams, objects and packets of each search. All search data can be viewed, analyzed and optionally downloaded by authorized users for further analysis.

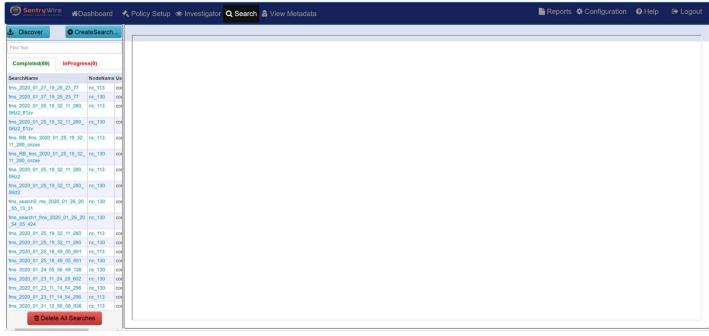


Figure 56-Search Screen

The Search screen is divided into two main panels:

- 1. Left panel allows the user to :
  - **Discover** This button shows search events as logged in ElasticSearch/Kibana store. Search creation events, search completion events, search deletion events and any other search related events are displayed in this window in reverse chronological order.



First bar       Image: State Sta	Sentry Wire			1		etup   Investigator Q S	earch		rts 🌣 Configuration		
Complexit(i)         InProgress(i)         Discover         Implexit         Discover           Searchhame         Nodel J27, 10, 25, 23, 77         no.110         Now Save Open Share Inspect         Note Save Open Share Inspect           Implexitor J27, 10, 25, 23, 77         no.110         Now Save Open Share Inspect         Note Save Open Share Inspect           Implexitor J27, 10, 25, 12, 27, 12, 20, no.110         Now Save Open Share Inspect         Note Save Open Share Inspect         Note Save Open Share Inspect           Implexitor J12, 20, 20, 12, 30, 12, 31, 32, 11, 200, no.110         Now Save Open Share Inspect         Note Save Open Share Inspect         Note Save Open Share Inspect           Implexitor J12, 200, 12, 13, 21, 12, 20, no.110         Now Save Open Share Inspect         Note Save Open Share Inspect         Note Save Open Share Inspect           Implexitor J12, 200, 12, 13, 21, 12, 20, 13, 13, 12, 200, 13, 19, 22, 11, 20, no.110         Note Save Open Share Inspect         Note Save Open Share Inspect           Implexitor J12, 200, 12, 13, 21, 12, 20, 13, 13, 12, 200, 13, 19, 22, 11, 20, no.110         Note Save Open Share Inspect         Note Save Open Share Inspect           Implexitor J12, 200, 12, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 13, 21, 12, 20, 20, 20, 21, 21, 21, 21, 20, 20, 20, 21, 21, 21, 21, 20, 20, 20, 2	1. Discover	O Crea	iteSearch	ni Node	le:10.91	1.170.130 Search: -		Streams Objects	Search Analyzer	Packets	Manager
Comparison         Nodelane	Find Text										_
Imm_2020_01_27_19_25_22_77       R_113       C       KOL       C       Refresh         Imm_2020_01_27_19_25_22_77       R_113       C       Imm_2020_01_25_19_22_11_20       R_113       C       Imm_2020_01_25_19_32_11_20       R_113       C       Imm_2020_01_25_19_32_1R_20       R_113       C       Immediate and the plane in the pla	Completed(69)	nProgres	s(0)			Discover				0	9 <b>0</b>
Sing 2020 01 92 19 22 92 77       cc 130       COL       C Refresh         mag 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       CO       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 19 32 11 200       nc 113       Image 2020 01 95 11 82 11 800 1180       Image 2020 01 95 118 80 1180       Image 2	SearchName		NodeName U	s O		New Save Open Share	e Insp	ect			
ms 2020 01 25 19 32 11 280       nc 113       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 19 32 11 280       nc 130       co         image 2020 01 25 10 42 11 28 128	ms_2020_01_27_19_25_	23_77	nc_113 c	01		=					
max 2000 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, 2020 01 25, 19, 32, 11, 280       mc, 130       mc         ms, sawatch, fms, 2020, 01, 28, 19, 32, 11, 280       mc, 130       mc         ms, sawatch, fms, 2020, 01, 28, 19, 32, 11, 280       mc, 130       mc         ms, 2020, 01, 28, 19, 32, 11, 280       mc, 130       mc         ms, 2020, 01, 28, 19, 32, 11, 280       mc, 130       mc         ms, 2020, 01, 28, 19, 32, 11, 280       mc, 130       mc         ms, 2020, 01, 28, 19, 32, 11, 280       mc, 130       mc         ms, 2020, 01, 28, 19, 32, 11, 280       mc, 130       mc         ms, 2020, 01, 28, 19, 49, 65, 691       mc, 130       mc         ms, 2020, 01, 21, 12, 14, 28, 280	ms_2020_01_27_19_25_	23_77	nc_130 c		0				KQ	GR	<u>efresh</u>
Nac2 110 <sup>2</sup> <t< td=""><td></td><td>11_280_</td><td>nc_113 c</td><td></td><td></td><td>😌 – + Add filter</td><td></td><td></td><td></td><td></td><td></td></t<>		11_280_	nc_113 c			😌 – + Add filter					
mar. R8. max. 2020. 01 25 19 32       nc. 113       corre		11_280_	nc_130 c		-	(chonge)	0	20 hits			
ms. Ref. ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 32, 11, 280, ns. 130 ms. 2020, 01, 25, 19, 490, 5941 ms. 2020, 01, 21, 19, 49, 280, ns. 130 ms. 2020, 01, 21, 19, 49, 280, ns. 130 ms. 2020, 01, 21, 19, 49, 280, ns. 130 ms. 2020, 01, 21, 19, 49, 280, ns. 130 ms. 2020, 01, 21, 19, 49, 280, ns. 130 ms. 2020, 01, 21, 19, 49, 208, ns. 130 ms. 2020, 01, 21, 19, 49, 280, ns. 130 ms. 2020, 01, 21, 19, 49, 280, ns. 130 ms. 2020, 01, 21, 19, 49, 280, ns. 130 ms. 2020, 01, 21, 11, 45, 298, ns. 130 ms. 2020, 01, 21, 11, 45, 298, ns. 130 ms. 2020, 01, 21, 11, 45, 298, ns. 130 ms. 2020, 01, 21, 11, 45, 298, ns. 130 ms. 2020, 01, 21, 11, 45, 298, ns. 130 ms. 2020, 01, 21, 11, 45, 298, ns. 130 <		5_19_32_	nc_113 c	. 20	8						
<pre>ms_2020_01_25_19_32_11_280 m_m13 co bdz</pre> search_name: fms_2020_01_25_19_32_11_280 m_m13 co ms_2020_01_25_19_32_11_280 m_m13 co bdz search_name: fms_2020_01_25_19_32_11_280 m_m13 co bdz search_name: fms_2020_01_26_10 m_m13 co bdz search_name: fms_2020_01_26_10 m_m13 co bdz search_name: fms_2020_01_26_10 m_m13 co ms_2020_01_25_18_40_65_691 m_m13 co ms_2020_01_25_18_40_65_691 m_m13 co ms_2020_01_25_18_40_65_691 m_m13 co ms_2020_01_21_11_24_26_602 m_m13 co ms_2020_01_21_11_24_26_602 m_m13 co ms_2020_01_21_11_24_26_602 m_m13 co ms_2020_01_21_11_24_26_602 m_m13 co ms_2020_01_21_11_24_26_602 m_m13 co ms_2020_01_21_11_24_26_602 m_m13 co ms_2020_01_21_11_45_426 m_m13 co ms_200_01_21_11_45_426 m_m13 co ms_200_00_21_11_45_4080		5_19_32_	nc_130 c	or 💼			>	username: continuum auth_token: b0dc9dee-a805-4b37-9883-dca377f5537e capture_interfaces:			
ns_2020_012_519_32_11_24_0 _ nc_130		11_280_	nc_113 c	01	2	0				ackets: 217	2319
ms_search_ims_2020_01_26_20 nc_130 co ssearch_ims_2020_01_26_20 nc_130 co ssearch_ims_2020_01_26_20 nc_130 co ssearch_ims_2020_01_26_19_32_11_280 nc_133 co ms_2020_01_26_19_32_11_280 nc_133 co ms_2020_01_26_16_40_566 in nc_133 co ms_2020_01_28_16_40_566 in nc_133 co ms_2020_01_28_16_40_566 in nc_133 co ms_2020_01_28_11_48_40_286 nc_133 co ms_2020_01_28_11_48_4286 co ms_2020_01_28_11_48_4286886e-co ms_2020_01_28_11_48_4286 co ms_2020_01_28_11_48_4286 co ms_2020_01		11_280_	nc_130 c							tasearch	
mms_sace/it fms_2020_01_28_20       nc.130       cn         6.06_04_24       fs_0.06_24       fs_0.06_16       fs_0.06_24       fs_0.06_16       fs_0.06_24       fs_0.06_16       fs_0.06_16 <td></td> <td>1_26_20</td> <td>nc_130 c</td> <td></td> <td></td> <td></td> <td></td> <td>_index: metasearch_inprogress _score: 0</td> <td></td> <td></td> <td></td>		1_26_20	nc_130 c					_index: metasearch_inprogress _score: 0			
ms_2020_0125_19.32_11240 nc_113 co ms_2020_0125_19.32_11240 nc_130 co ms_2020_0125_18_49_05.691 nc_130 co ms_2020_0125_18_49_05.691 nc_130 co ms_2020_0125_18_49_05.691 nc_130 co ms_2020_0125_18_49_05.691 nc_130 co ms_2020_0123_1124_28_602 nc_130 co ms_2020_0123_1124_28_602 nc_130 co ms_2020_0123_1124_28_602 nc_130 co ms_2020_0123_1124_28_602 nc_131 co ms_2020_0123_1124_28_602 nc_131 co ms_2020_0123_1124_58_60 nc_113 co ms_2020_0123_1124_58_6		01_26_20	nc_130 c	DI		t LogSearchFilter	>				
max_2020_01_25_16_34_05_691       nc_130       corr       Corr       PayloadSearchFilter       SnapLen:       fmuser:       continuum       id:       Lg/scatch       corr       corr <td< td=""><td>ns_2020_01_25_19_32_</td><td>11_280</td><td>nc_113 c</td><td></td><td>71</td><td>A 11</td><td></td><td></td><td></td><td></td><td></td></td<>	ns_2020_01_25_19_32_	11_280	nc_113 c		71	A 11					
w 2020 01 25 18.49.06 991       nc.113       core       PayloadSearchFilter         w 2020 01 25 18.49.06 991       nc.113       core       0       SnapLen:       fmuser: continuum ld: eJC15688905ChWYjqEEk _type: metasearch _infex: metasearch _infex: metasearch _infex: metasearch _infex:         w 2020 01 25 18.49.06 991       nc.113       core       0       SnapLen:       fmuser: continuum ld: eJC15688905ChWYjqEEk _type: metasearch _infex: metasearch _infex:         w 2020 01 25 18.49.06 991       nc.130       core       0       SnapLen:       fmuser: continuum ld: eJC15688905ChWYjqEEk _type: metasearch _infex: metasearch _infex:         w 2020 01 23 11, 24.28.602       nc.130       core       core       i.jd       search_name: fms_2020_01.23.11, 24.28.602       begin time: 2020-01-23 16:15:28 end_time: 2020-01-23 16:24:28 max_packets: 1000       search_filter: PcapData, tcp or udp LogSearchFilter:       PayloadSearchFilter:       Mergeap: PCAP Count &ti=16 SnapLen:         w 2020 01 21 12 26 06 938       nc.113       core       fmuser: continuum _id: E4w402888Wee-c60MPEp _type: metasearch _index: metasearch _inprogress _score: 0	ns_2020_01_25_19_32_	11_280	nc_130 c		2	@ mergecap			* .		
xx 2020_0124_105_58.49_126       nc.130       co         xx 2020_0124_105_58.49_126       nc.130       co         xx 2020_0123_11_24_28_202       nc.130       co         xx 2020_0123_11_46_1226       nc.130       co         xx 2020_0123_11_46_1226       nc.130       co         xx 2020_0123_11_46_1226       nc.130       co         xx 2020_0123_11_46_1266       nc.130       co         xx 2020_0121_12_56.08_586       nc.113       co         xx 2020_0121_12_56.08_586       nc.113       co         xx 2020_012_11_12_56.08_586       nc.113       co         xx 2020_012_11_12_56.08_586       nc.113       co         xx 200_012_11_12_56.08_586       nc.113       co	ns_2020_01_25_18_49_	05_691	nc_113 c			② PayloadSearchFilter		SnapLen: fmuser: continuum _id: eJC15G8B9o5ChNYjq0Ek _type: metasearch _index: metasearch_	inprogress _score:	0	
10:2000 01:24.05.56.49:128       nc.130       col         10:2000 01:24.11.45.4286       nc.130       col         10:2000 01:23.11:24.28.600       nc.130       col         10:2000 01:23.11:45.4286       nc.130       col         10:2000 01:23.11:45.4286       nc.130       col         11:25.56.08.9886       nc.113       col         11:25.56.08.9886       nc.113       col         11:25.50.08.9886       nc.113       col	ns_2020_01_25_18_49_	05_691	nc_130 c	° 🕤	ĵ						
ms_2020_01_23_11_14_54_286 mc_130 co ms_2020_01_23_11_14_54_286 nc_113 co ms_2020_01_23_11_14_54_286 nc_113 co ms_2020_01_21_12_56_08_988 nc_11	ns_2020_01_24_05_56_	49_126	nc_130 c			③ SnapLen	>	username: continuum auth_token: 037b4a16-5a43-4f57-81e9-5867b0507e9a capture_interfaces:			
ns_2020_01_23_11_14_54_298 nc_130 co ns_2020_01_23_11_14_54_298 nc_113 co ns_2020_01_21_12_56_08_938 nc_113 co ns_2020_01_21_12_56_08_938 nc_113 co fmuser: continuum _id: E4w4028B8Mee-c60MpEp _type: metasearch _index: metasearch_inprogress _score: 0	ns_2020_01_23_11_24_	28_602	nc_130 c	a 🖶	6	1 id		search name: fms 2020 01 23 11 24 28 602 begin time: 2020-01-23 16:15:28 end time: 2020-01-2	3 16:24:28 max pack	ets: 1000	
ns_2020_01_21_12_56_08_936 nc_113 co fmuser: continuum _1d: E4w482888Mee-c60MpEp _type: metasearch _index: metasearch_inprogress _score: 0	ns_2020_01_23_11_14_	54_296	nc_130 c	DI		•			-		
			-	이 (?)	?	t _index				1.	
Delete All Searches	ms_2020_01_21_12_56_	08_936	nc_113 c					Tmuser: continuum _id: E4W482888Mee-c6UMpEp _type: metasearch _index: metasearch_inprogress	_score: 0		
E dusername: continuum auth_token: 397021cd-305d-43e4-9301-4d569af02f9e capture_interfaces:	Delete A	II Search	nes		_		>	username: continuum auth_token: 397021cd-305d-43e4-9301-4d569af02f9e capture_interfaces:			

Figure 57-Search Discover Button

• Create Search - This button opens a popup window to allow users to create a search. For more info on creating a search please refer to section 6.1

1. Discover	CreateSearch			Create Search	
Find Text			SearchName	2	
			fms_2020_01_28_00_35_43_40	04	
Completed(69) InP	ogress(0)		BeginTime		
earchName	NodeName	Us	2020-01-28 05:26:43		
ms_2020_01_27_19_25_23	77 nc_113	cor	EndTime		
ns_2020_01_27_19_25_23	77 nc_130	COF	2020-01-28 05:35:43		
ms_2020_01_25_19_32_11 H6z2_f11zv	280_ nc_113	cor	Search Filter	Fill in details	
lms_2020_01_25_19_32_11 Di6z2_fi1zv	280_ nc_130	cor	bpf <bpffilter> logtext <logse< td=""><td>archfilter</td><td></td></logse<></bpffilter>	archfilter	
fms_RB_fms_2020_01_25_1 11_280_cnzxe	9_32_ nc_113	COF	MaxPacketCount		
ms_RB_fms_2020_01_25_1 11 280 cnzxe	9_32_ nc_130	cor	Stream Search Results		
ms_2020_01_25_19_32_11 Di6z2	280_ nc_113	cor	Create Search	Cancel Request	
fms_2020_01_25_19_32_11 0i6z2	280_ nc_130	cor			
ms_search2_ms_2020_01_3 55 13 31	6_20 nc_130	cor			
fms_search1_fms_2020_01_ _54_05_424	26_20 nc_130	cor			
ms_2020_01_25_19_32_11	280 nc_113	cor			
ms_2020_01_25_19_32_11	280 nc_130	cor			
ms_2020_01_25_18_49_05	691 nc_113	cor			
ms 2020 01 25 18 49 05	691 nc_130	cor			
fms_2020_01_24_05_56_49	126 nc_130	cor			
ms_2020_01_23_11_24_28	602 nc_130	cor			
ms_2020_01_23_11_14_54	296 nc_130	cor			
ms_2020_01_23_11_14_54	296 nc_113	cor			
	936 nc_113	001			

Figure 58-Create Search Button

- Find Text area Displays content with the matching text only.
- **Completed-** This tab shows all the completed and cancelled searches. To see the username of each search and delete option, search scroll to the right (as shown in the



picture below). Clicking on the hyperlinked Search name or node name displays the stream view of the clicked search.

Sentry Wire	🖺 Reports 🌣 Configuration 🛛 🤡 Help	🕩 Logout
1 Discover CreateSearch		
Find Text		
Completed(69) InProgress(0)		
SearchName NodeName UserName		
1_27_19_25_23_77 nc_113 continuum 1 1_27_19_25_23_77 nc_130 continuum 1		
125-19-32, 11, 280, no. 113 continuum fi		
_25_19_32_11 280_ nc_ 30 continuum		
20 Clicking on Search www 8		
° name or node name 20 opens the Stream View num ∎		
20 opens the stream view num a		
1_2 <del>5_19_32_11_20U102_113Comm</del> huum		
1.25.19.32_11_280_ nc_130 continuum 2		
2_ms_2020_01_26_20 nc_130 continuum 🔋		
[ms_2020_01_26_20_nc_130 continuum 1		
1_25_19_32_11_280 nc_113 continuum 8 1_25_19_32_11_280 nc_130 continuum 8		
125 19 32 11 200 nc 130 continuum e		
25.18.49.05.691 nc_130 continuum i		
1_24_05_56_49_126 nc_130 continuum 2		
1_23_11_24_28_602 nc_130 continuum 🗄		
1_23_11_14_54_296 nc_130 continuum 😫		
1_21_11_6_94_296 nc_113 continuum e		
Delete All Searches		
Scroll		

Figure 59-Completed Search View

• **InProgress-** This tab shows the list of searches that are in Pending/InProgress state. Scrolling to the right allows the user to delete any search in Pending/InProgress state by clicking on the delete icon.

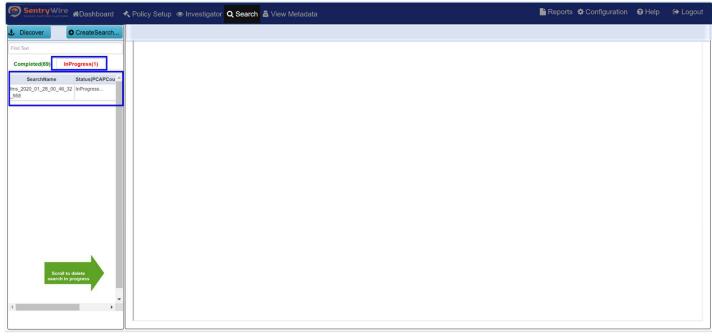


Figure 60-Search InProgress screen



Pending	View o	f a search		
SearchName	Status	s(PCAPCount,TotalSize	e]	
fms_search1_fms_2020_01_2 6_20_54_05_424	Pendi	ng	×	
fms_search2_ms_2020_01_2 6_20_55_13_31	Pendi	ng	×	
InPro	gress	View of a searc	h	
SearchName		Status(PCAPCou	unt, Tota	alSiz
fms_2020_01_28_09_5 _221	69_53	InProgress(277, 1	4.00 G	B)

Note:

- Searches are split into 64MB PCAPs for ease of downloading and viewing by tools such as Wireshark. For small searches, the search may be completed before the status changes from InProgress... to include the pcap count. For larger searches, user will see the count and the search size in bytes go up while the search is in progress.
- Multiple searches can be in progress simultaneously.
- Clicking on X cancels a search in progress. It can then be deleted from Completed searches tab.
- Delete All Searches- This button allows the user to delete ALL searches across all nodes of all selected groups. This action is not reversible.

Sentry Wir	n an	shboard	4
£ Discover	O Crea	ateSearch	
Find Text			
0			
Completed(69)	InProgres	IS(0)	
SearchName		NodeNam	e U
fms_2020_01_27_19_2		nc_113	C
fms_2020_01_27_19_2		nc_130	C
fms_2020_01_25_19_3 0i6z2_f11zv	2_11_280_	nc_113	CI
fms_2020_01_25_19_3 0i6z2_f11zv	2_11_280_	nc_130	co
fms_RB_fms_2020_01 11_280_cnzxe	25_19_32_	nc_113	cor
fms_RB_fms_2020_01_ 11_280_cnzxe	25_19_32_	nc_130	COL
fms_2020_01_25_19_3 0i6z2	2_11_280_	nc_113	COI
fms_2020_01_25_19_3 0i6z2	2_11_280_	nc_130	co
fms_search2_ms_2020 _55_13_31	01_26_20	nc_130	co
fms_search1_fms_2020 54 05 424	_01_26_20	nc_130	co
fms 2020 01 25 19 3	2_11_280	nc_113	co
fms_2020_01_25_19_3			co
fms_2020_01_25_18_4			cc
fms_2020_01_25_18_4			0
fms_2020_01_24_05_5			C
fms_2020_01_23_11_2			0
fms_2020_01_23_11_1		nc_130	CI
fms_2020_01_23_11_1 fms_2020_01_21_12_5		nc_113	00
Delete			CO

Figure 61-Delete All Search screen and button

2. Right panel allows the user to:



- View and analyze the search streams and packets, objects extracted, and, manage a specific search.
- To view search streams, simply click on a search. This displays the **Streams List** available for the search selected.
- The Streams view is further divided into a Packet list and Stream info sections.
  - Clicking on a particular stream displays packet data within the selected stream along with the stream info (the Follow TCP|UDP Stream view of the selected stream) Note: Packets list and StreamInfo are not populated until a stream from this list is selected.
  - Once a stream is selected from the Streams list, the packets belonging to this stream are displayed in Packets list as shown the picture below.

Discover	O Crea	teSearch	Find Text				Node: 149	Search: fms_2020_	01_23_16_12_04_814					Streams Objects	Search A	nalyzer	Packets	Manager							
Find Text				Streams			Packet Da	ata Within the S	elected Stream							Find Text									
			172.16.9.171	:3043 tcp 87.23	3.145.146:80	0	Timest	amp	Source	Destination	Protocol	Length	Packetin	nfo		Expertinfo									
Completed(20)	InProgress	(0)	172.16.9.171	:3039 tcp 213.2	44.168.235:8	80	> 157981	3207.786819248	172.16.9.171:2837	66.249.91.83:80	TCP	120	POST /m	nail/channel/bind?at=6c2db5ff4e1e5995-											
earchName		NodeName U	216.251.105.	120:80 tcp 172.	16.9.171:304									5245&VER=2&SI											
ns_2020_01_27_12_5	1_09_161	sw_149 c	207.68.179.2	19:80 tcp 172.1	6.9.171:3034	4	> 157981	3207.786819248	172.16.9.171:2837	66.249.91.83:80	HTTP	105		hail/channel/bind?at=6c2db5ff4e1e5995- 5245&VER=2&SI		(Chat/Seque	nce): POST	1.58							
s_2020_01_27_12_5	0_10_386	sw_149 c	172.16.9.171	:3036 tcp 64.4.1	15.61:80		> 157081	3207 786825965	172.16.9.171:2837	66.249.91.83:80	TCP	60	2837 å	80 [ACK] Seg=1578 Ack=235 Win=17	7286 Len=0	maircnahne	voind rat=0020	Doll							
ns_2020_01_24_15_5	1_48_227	sw_149 c	131.107.113.	76:80 tcp 172.10	6.9.171:3008				172.16.9.171:2947	145.72.70.20:80	TCP	62	2947 â	80 [SYN] Seg=0 Win=16384 Len=0 M		(Chat/Seque	nce): Connecti	on establish							
s_2020_01_24_09_2	8_13_200	sw_149 c	65.54.239.21	4:80 tcp 172.16	9.171:3021							01	SACK_P		100-1100	request (SYI									
s_2020_01_24_09_2	7_07_503	sw_149 c	172.16.9.171	:3008 tcp 131.1	07.113.76:80	D	> 157981	3207.786980837	145.72.70.20:80	172.16.9.171:2947	TCP	62		2947 [SYN, ACK] Seq=0 Ack=1 Win=43	80 Len=0		nce): Connecti	on establish							
s_2020_01_24_09_2	1_47_590	sw_149 c	66.249.91.83	:80 tcp 172.16.9	9.171:2837								MSS=14			acknowledge	) (S								
2020_01_24_09_2	0_43_331	sw_149 c	207 46 213 1	23:80 tcp 172.1	6 9 171-3049	0			172.16.9.171:2947	145.72.70.20:80	TCP	60 453	2947 â	80 [ACK] Seq=1 Ack=1 Win=17520 L		(Chat/Seque									
_2020_01_24_09_0	2_43_450	sw_149 c		120:80 tcp 172.			> 157981	3207.786980837	172.16.9.171:2947	145.72.70.20:80	HTTP	453	GET /ima	ages/css/whitepixel.gif?1175694378181 I	HTTP/1.1		nce): GE1 whitepixel.gif?1	1175							
_2020_01_24_08_5	8_06_675	sw_149 c		:80 tcp 172.16.9			> 157981	3207.786994131	145.72.70.20:80	172.16.9.171:2947	HTTP	449	HTTP/1.1	1 200 OK (GIF89a)		(Chat/Seque	nce): HTTP/1.1	1 200 OK/r/n							
2020_01_24_08_3	9_04_975	sw_149 c		(1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997) (1997)		_	> 157981	3207.786994131	172.16.9.171:2947	145.72.70.20:80	TCP	60	2947 â	80 [ACK] Seq=400 Ack=396 Win=171	25 Len=0										
5_2020_01_24_00_5	1_10_92	sw_149 c		:2843 tcp 72.14			> 157981	3207.786994131	172.16.9.171:2947	145.72.70.20:80	HTTP	482	GET /par	rticulieren/internetbankieren/ HTTP/1.1		(Chat/Seque									
s_2020_01_23_23_4	9_15_990			:3042 tcp 216.2		80										/particulieren	/internetbankie	re							
s_2020_01_23_23_4	6_45_434	sw_149 c	84.53.136.15	2:80 tcp 172.16	.9.171:3 C	lick a str	eam to		145.72.70.20:80	172.16.9.171:2947	TCP	1514		1 200 OK [TCP segment of a reassemble											
s_2020_01_23_23_3	4_08_261	sw_149 c	172.16.9.171	:3044 tcp 216.2		iew pack		207.786994131	145.72.70.20:80	172.16.9.171:2947	TCP	1514	80 â Len=146	2947 [PSH, ACK] Seq=1856 Ack=828 V	/in=5207										
s_2020_01_23_23_2	8_29_391	sw_149 c	72.14.217.18	9:80 tcp 172.16	.9.171:2	stream	info	207 786004131	172.16.9.171:2947	145.72.70.20:80	TCP	60	2947 å	80 [ACK] Seg=828 Ack=3316 Win=17	520 Len=0										
s_2020_01_23_23_0	9_14_575	sw_149 c	172.16.9.171	:3034 tcp 207.6	8.179.219:8		> 157981		145.72.70.20:80	172.16.9.171:2947	TCP	1514		2947 [PSH, ACK] Seg=3316 Ack=828 V											
s_2020_01_23_23_0	0_03_557	sw_149 c	172.16.9.171	:2953 tcp 145.7	2.70.20						101	1014													
s_2020_01_23_17_2	9_53_296	sw_149 c	172.16.9.171	:2837 top 66.24	9.91.83:80	3	StreamIn	fo									View	vPackets							
2020_01_23_17_2	6_51_833	sw_149 c	172 16 9 171	:3033 tcp 213.1	99 166 30 80								101												
_2020_01_23_16_1	2_04_814	sw_149 c		:80 tcp 172.16.9		-								t/GetClientConfig" Content-Type: text/xm Connection: Keep-Alive Cache-Control:			ngth: 447 User	-Agent:							
				:2947 tcp 145.7										ulW:F; ushpcli=0H.0.1IG.0.1IZ.0.1IR.0.1 =E9B362AE392484C6045603A5FFFFFF			0.1.LN:WNBC;								
						N	AP=V=1.5&	E=4ff&C=K2lxctJ	PRZIaaYHJdt1YrpwFU7	pKLYNIB/GBpLkRzSFDtMi	ROhqqmQ&V	V=1 447	ml version=	="1.0" encoding="utf-8"?> <soap:envelop< td=""><td>e xmlns:xsi</td><td>"http://www.wa</td><td></td><td></td></soap:envelop<>	e xmlns:xsi	"http://www.wa									
				:80 tcp 172.16.9										<soap:body><getclientconfig p2p"="" xmins="h&lt;br&gt;fo&gt; &lt;/GetClientConfig&gt;&lt;/soap:Body&gt;&lt;/s&lt;/p&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;:3048 tcp 146.1&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;n n&lt;/td&gt;&lt;td&gt;ame="></getclientconfig></soap:body>	Entry hr="0x820	000012" action="3" />E	ntry hr="0x82000013" actio	n="3" />Entry	hr="0x820	00016" actic	on="3" /> <entry action="&lt;/td" hr="0x82000017"><td>"3" /&gt;Entry</td><td>y hr="0x820000</td><td>18" action="3"</td><td>/&gt;Entry</td></entry>	"3" />Entry	y hr="0x820000	18" action="3"	/>Entry
				:3021 tcp 65.54		-								it>1 <oemdisplaylimit>1</oemdisplaylimit>				abdata> <tab:< td=""></tab:<>							
-			213.199.166.	30:80 tcp 172.1	6.9.171:3033	3  n	l/services_ta	b/services_tab.ht	ml <hiturl>h</hiturl>	ttp://c.msn.com/c.gif?di=23	08&	tp=http://me	ssengertab	s.msn.com/nInl/jouw <siteid>0<td>iteid&gt;notifie</td><td>cationid&gt;0<td>ificationid&gt;<td>b&gt;<tab></tab></td></td></td></siteid>	iteid>notifie	cationid>0 <td>ificationid&gt;<td>b&gt;<tab></tab></td></td>	ificationid> <td>b&gt;<tab></tab></td>	b> <tab></tab>							
Delete	All Search	es	172.16.9.171	:3035 tcp 84.53	136.160:80									ne> <type>match</type> <tooltip>MSN D 8&amp;:amp:tp=http://messengertabs.ms</tooltip>											

Figure 62-Search Stream view

- Several column data have been hyperlinked.
  - Clicking on any hyperlinked info takes to the All Packet view for further analysis.
  - Clicking on a packet's Timestamp hyperlink in this column will pivot to Packets tab to display all the packets with the same timestamp.
  - Clicking on a packet's Source hyperlink will pivot to Packets tab to display all the packets with the same source IP and source port.
  - Clicking on a packet's Destination hyperlink will pivot to Packets tab to display all the packets with the same dest IP and dest port.
  - Clicking on a packet's Protocol hyperlink will pivot to Packets tab to display all the packets with the same Protocol.
- The Find Text input area allows the user to find packets with the supplied text within the Packets list. This will not pivot to Packets tab.



Discover	CreateSearch	Find Text		e:149 Search: fms_2020_0					Streams Objects Search	h Analyzer Packets Manage
Find Text		Streams	Pac	cket Data Within the Se	elected Stream					Find Text
		172.16.9.171:3043 tcp 87.233.145.146:80		Timestamp	Source	Destination	Protocol	Length	Packetinfo	Expertinfo
Completed(20) InProg	ress(0)	172.16.9.171:3039 tcp 213.244.168.235:80	>	1579813207.786819248	172.16.9.171:2837	66.249.91.83:80	TCP	120	POST /mail/channel/bind?at=6c2db5ff4e1e5995-	
earchName	NodeName	U 216.251.105.120:80 tcp 172.16.9.171:3044							111bcd55245&VER=2&SI	
ns_2020_01_27_12_51_09_16	sw_149	cc 207.68.179.219:80 tcp 172.16.9.171:3034	>	1579813207.786819248	172.16.9.171:2837	66.249.91.83:80	HTTP	105	POST /mail/channel/bind?at=6c2db5ff4e1e5995-	(Chat/Sequence): POST /mail/channel/bind?at=6c2db5ff
ns_2020_01_27_12_50_10_38	sw_149	cc 172.16.9.171:3036 tcp 64.4.15.61:80		1579813207.786825965	170 16 0 171-2827	66.249.91.83:80	TCP	60	111bcd55245&VER=2&SI 2837 â 80 [ACK] Seg=1578 Ack=235 Win=17286 Ler	
ms_2020_01_24_15_51_48_22	sw_149	cc 131.107.113.76:80 tcp 172.16.9.171:3008		1579813207.786980837		145.72.70.20:80	TCP	62	2947 å 80 [SYN] Seg=0 Win=16384 Len=0 MSS=146	
ns_2020_01_24_09_28_13_20	) sw_149	∝ 65.54.239.214:80 tcp 172.16.9.171:3021			1.2.1.0.0.1.1.2.0.11		6		2011 0 00 1011 0 00 0 Lotte 0 1000-14	request (SYN):
ns_2020_01_24_09_27_07_50	sw_149	∝ 172.16.9.171:3008 tcp 131.107.113.76:80	>	1579813207.786980837	145.72.70.20:80	172.16.9.171:2947	TCF		king on any K] Seq=0 Ack=1 Win=4380 Len=	
ns_2020_01_24_09_21_47_59	) sw_149	cc 66.249.91.83:80 tcp 172.16.9.171:2837							red info takes to	acknowledge (S
s_2020_01_24_09_20_43_33	sw_149	cc 207.46.213.123:80 tcp 172.16.9.171:3049		1579813207.786980837 1579813207.786980837		145.72.70.20:80 145.72.70.20:80	7/4		Packet view for ner analysis vel.gil?1175694378181 HTTP/1.	1 (Chat/Sequence): GET
s_2020_01_24_09_02_43_45	) sw_149	a 216.251.105.120:80 tcp 172.16.9.171:3042	1	1579613207.760960637	172.10.9.171:2947	145.72.70.20.00	1	Turth	ter analysis kei.gir/175694378181 HTTP/I.	/images/css/whitepixel.gif?1175
s_2020_01_24_08_58_06_67	5 sw_149	cc 194.129.79.9:80 tcp 172.16.9.171:3046	>	1579813207.786994131	145.72.70.20:80	172.16.9.171:2947	HTTP	449	HTTP/1.1 200 OK (GIF89a)	(Chat/Sequence): HTTP/1.1 200 OK/r/n
s_2020_01_24_08_39_04_97		cc 172.16.9.171:2843 tcp 72.14.217.189:80	>	1579813207.786994131	172.16.9.171:2947	145.72.70.20:80	TCP	60	2947 å 80 [ACK] Seq=400 Ack=396 Win=17125 Len:	=0
s_2020_01_24_00_51_10_92	sw_149	cc 172.16.9.171.2843 tcp 72.14.217.169.80	>	1579813207.786994131	172.16.9.171:2947	145.72.70.20:80	HTTP	482	GET /particulieren/internetbankieren/ HTTP/1.1	(Chat/Sequence): GET
ns_2020_01_23_23_49_15_99				1579813207.786994131		172.16.9.171:2947	TCP	1514		/particulieren/internetbankiere
ns_2020_01_23_23_46_45_43		cc 84.53.136.152:80 tcp 172.16.9.171:3047		1579813207.786994131 1579813207.786994131		172.16.9.171:2947	TCP	1514	HTTP/1.1 200 OK [TCP segment of a reassembled PDU] 80 å 2947 [PSH, ACK] Seg=1856 Ack=828 Win=520]	7
ns_2020_01_23_23_34_08_26		cc 172.16.9.171:3044 tcp 216.251.105.120:80	1	1578615207.760884151	145.72.70.20.00	172.10.3.171.2347	ICF	1514	Len=1460 [TCP s	
ns_2020_01_23_23_28_29_39		C 72.14.217.189:80 tcp 172.16.9.171:2843	>	1579813207.786994131	172.16.9.171:2947	145.72.70.20:80	тср	60	2947 å 80 [ACK] Seq=828 Ack=3316 Win=17520 Ler	n=0
ns_2020_01_23_23_09_14_57		CC 172.16.9.171:3034 tcp 207.68.179.219:80	>	1579813207.786994131	145.72.70.20:80	172.16.9.171:2947	TCP	1514	80 å 2947 [PSH, ACK] Seq=3316 Ack=828 Win=5207	7
ns_2020_01_23_23_00_03_55 ns_2020_01_23_17_29_53_29		172.16.9.171:2953 tcp 145.72.70.20:80	C to	eaminfo						
ns 2020 01 23 17 26 51 83		172.16.9.171:2837 tcp 66.249.91.83:80	Su	eamino						ViewPackets
is 2020_01_23_17_28_51_65		172.16.9.171:3033 tcp 213.199.166.30:80							enger/Client/GetClientConfig" Content-Type: text/xml; charse	
0_0000_01_00_10_12_04_01	011_140	145.72.70.20:80 tcp 172.16.9.171:2947							er.msn.com Connection: Keep-Alive Cache-Control: no-cach IT:5IE:5ID:bluIW:F; ushpcli=0IH.0.1IG.0.1IZ.0.1IR.0.1.capIC.0	
		172.16.9.171:2947 tcp 145.72.70.20:80	ushpw	rea=wc:USNY0996; MUID	=3EC3A4151B324496/	4B8ECE3B27E024C; ush	ppr=H:1:0704	04; zip=1000	0; ANON=A=E9B362AE392484C6045603A5FFFFFFF&E=	559&W=1;
		145.72.70.20:80 tcp 172.16.9.171:2953							xml version="1.0" encoding="utf-8"?> <soap:envelope xmlns<br="">/envelope/"&gt;<soap:body><getclientconfig 3"<="" td="" xmlns="http://www&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;172.16.9.171:3048 tcp 146.101.162.215:80&lt;/td&gt;&lt;td&gt;&lt;client&lt;/td&gt;&lt;td&gt;tinfo&gt; &lt;Country&gt;NL&lt;/Cou&lt;/td&gt;&lt;td&gt;ntry&gt; &lt;CLCID&gt;0409&lt;/C&lt;/td&gt;&lt;td&gt;LCID&gt; &lt;PLCID&gt;0409&lt;/PL0&lt;/td&gt;&lt;td&gt;CID&gt; &lt;GeoID:&lt;/td&gt;&lt;td&gt;244&lt;/Geol&lt;/td&gt;&lt;td&gt;D&gt; &lt;/clientinfo&gt; &lt;/GetClientConfig&gt;&lt;/soap:Body&gt;&lt;/soap:Env&lt;/td&gt;&lt;td&gt;elope&gt; 536 &lt;/Feature&gt;&lt;Feature type="></getclientconfig></soap:body></soap:envelope>	
		172.16.9.171:3021 tcp 65.54.239.214:80	hr="0x	(82000019" action="3" /><	/Feature> <td>nseTable&gt;<tabc< td=""><td>onfig&gt;msnta</td><td>bsettings&gt;&lt;</td><td>00016" action="3" /&gt;<entry action="3" hr="0x82000017"></entry>&lt; coemtotallimit&gt;1<coemdisplaylimit>11</coemdisplaylimit>111<td>playlimit&gt;<tab< td=""></tab<></td></td></tabc<></td>	nseTable> <tabc< td=""><td>onfig&gt;msnta</td><td>bsettings&gt;&lt;</td><td>00016" action="3" /&gt;<entry action="3" hr="0x82000017"></entry>&lt; coemtotallimit&gt;1<coemdisplaylimit>11</coemdisplaylimit>111<td>playlimit&gt;<tab< td=""></tab<></td></td></tabc<>	onfig>msnta	bsettings><	00016" action="3" /> <entry action="3" hr="0x82000017"></entry> < coemtotallimit>1 <coemdisplaylimit>11</coemdisplaylimit> 111 <td>playlimit&gt;<tab< td=""></tab<></td>	playlimit> <tab< td=""></tab<>
		213.199.166.30:80 tcp 172.16.9.171:3033							pe>jouw <t 536="" ooltip="">Jouw MSNccontentu</t>	
@ Delete All Se	inches	172.16.9.171:3035 tcp 84.53.136.160:80							lerland <type>match</type> <tooltip>MSN Dating - N</tooltip>	

Figure 63-Search Screen Packet Data within Stream view

• Clicking on the View Packets button allows the user to view packet details of a selected stream for a specific text of interest. This Packet view is more focused on the packet data which contain the search string as requested by the user.

Discover	CreateSearch	Find Text	Node:149 Search: fms_2020_	01_23_16_12_04_814				Stre	ams Ot	ojects	Search Ar	nalyzer Packet	s Manage
nd Text		Streams	Packet Data Within the S	elected Stream								Find Text	
		172.16.9.171:3043 tcp 87.233.145.146:80	Timestamp	Source	Destination	Protocol	Length	PacketInfo				Expertinfo	
completed(20) InProg	ress(0)	172.16.9.171:3039 tcp 213.244.168.235:80	> 1579813207.786819248	172.16.9.171:2837	66,249,91,83:80	TCP	120	POST /mail/channel	//bind?at=6c2db	5ff4e1e59	95-		
archName	NodeName U	216.251.105.120:80 tcp 172.16.9.171:3044						111bcd55245&VER	=2&SI				
2020 01 27 12 51 09 16	sw_149 (	207.68.179.219:80 tcp 172.16.9.171:3034	> 1579813207.786819248	172.16.9.171:2837	66.249.91.83:80	HTTP	105	POST /mail/channel		5ff4e1e59	95-	(Chat/Sequence): POS	
2020 01 27 12 50 10 38		172.16.9.171:3036 tcp 64.4.15.61:80						111bcd55245&VER				/mail/channel/bind?at=	3c2db5ff
2020 01 24 15 51 48 22		x 131.107.113.76:80 tcp 172.16.9.171:3008	> 1579813207.786825965		66.249.91.83:80	TCP	60		<] Seq=1578 Act				
2020 01 24 09 28 13 20		x 65.54.239.214:80 tcp 172.16.9.171:3021	> 1579813207.786980837	172.16.9.171:2947	145.72.70.20:80	TCP	62	2947 å 80 [SYN SACK PERM=1	N] Seq=0 Win=1	6384 Len:	=0 MSS=1460	(Chat/Sequence): Con request (SYN):	nection establish
2020 01 24 09 27 07 50			> 1579813207.786980837	145 72 70 20:80	172.16.9.171:2947	TCP	62	and the second sec	N, ACK] Seq=0 A	ck=1 Win	=4380 Len=0	(Chat/Sequence): Con	ection establish
2020 01 24 09 21 47 59		x 172.16.9.171:3008 tcp 131.107.113.76:80						MSS=1460 SACK_	411014 004-01			acknowledge (S	
2020 01 24 09 20 43 33		66.249.91.83:80 tcp 172.16.9.171:2837	> 1579813207.786980837	172.16.9.171:2947	145.72.70.20:80	TCP	60	2947 å 80 [ACH	Seq=1 Ack=1	Win=1752	0 Len=0		
		207.46.213.123:80 tcp 172.16.9.171:3049	> 1579813207.786980837	172.16.9.171:2947	145.72.70.20:80	HTTP	453	GET /images/css/wi	hitepixel.gif?117	56943781	81 HTTP/1.1	(Chat/Sequence): GET	
2020_01_24_09_02_43_45		216.251.105.120:80 tcp 172.16.9.171:3042										/images/css/whitepixel	gil?1175
2020_01_24_08_58_06_67		194.129.79.9:80 tcp 172.16.9.171:3046	> 1579813207.786994131	145.72.70.20:80	172.16.9.171:2947	HTTP	449	HTTP/1.1 200 OK (	GIF89a)			(Chat/Sequence): HTT	P/1.1 200 OKv/r
2020_01_24_08_39_04_97		x 172.16.9.171:2843 tcp 72.14.217.189:80	> 1579813207.786994131	172.16.9.171:2947	145.72.70.20:80	TCP	60	2947 å 80 [ACH	<] Seq=400 Ack	=396 Win=	17125 Len=0		
2020_01_24_00_51_10_92	sw_149 (	x 172.16.9.171:3042 tcp 216.251.105.120:80						1 4100 1700			_		
2020_01_23_23_49_15_99			StreamInfo								POST		ViewPackets
2020_01_23_23_46_45_43		x 84.53.136.152:80 tcp 172.16.9.171:3047											-
2020_01_23_23_34_08_26		x 172.16.9.171:3044 tcp 216.251.105.120:80	POST /Config/MsgrConfig.asm Mozilla/4.0 (compatible; MSIE 6										Jser-Agent:
2020_01_23_23_28_29_39	sw_149 0	× 72.14.217.189:80 tcp 172.16.9.171:2843	MC1=V=3&GUID=10533b8a7b	b74defa0d10b651f123a8	Be; mh=MSFT; CULTURE=	EN-US; ushps	vr=M:5IF:5I	T:5IE:5ID:blulW:F; ush	pcli=0IH.0.1IG.0	0.1IZ.0.1IF	1.0.1.capIC.0.1.lg	newyorknylL.0.1.LN:WN	IBC;
2020_01_23_23_09_14_57	i sw_149 d	x 172.16.9.171:3034 tcp 207.68.179.219:80	ushpwea=wc:USNY0996; MUIE NAP=V=1.5&E=4ff&C=K2IxctJF										YMI Schoma
2020_01_23_23_00_03_55	sw_149 c	x 172.16.9.171:2953 tcp 145.72.70.20:80	instance" xmlns:xsd="http://www	w.w3.org/2001/XMLSche	ma" xmlns:soap="http://so	hemas.xmlsoa	p.org/soap/	envelope/">soap:Bod	ty> <getclientco< td=""><td>onfig xmln:</td><td>s='http://www.ms</td><td>n.com/webservices/Mes</td><td>enger/ lient'&gt;</td></getclientco<>	onfig xmln:	s='http://www.ms	n.com/webservices/Mes	enger/ lient'>
2020_01_23_17_29_53_29	sw_149 c	x 172.16.9.171:2837 tcp 66.249.91.83:80	<pre><clientinfo> <country>NLname="P2P"&gt;Entry hr="0x820"</country></clientinfo></pre>			CID> <geoid></geoid>	-244 <td>D&gt;  <td>lientConfig&gt;<td>oap:Body:</td><td><td>e&gt; 536 <feat< td=""><td>ure type 23"</td></feat<></td></td></td></td>	D> <td>lientConfig&gt;<td>oap:Body:</td><td><td>e&gt; 536 <feat< td=""><td>ure type 23"</td></feat<></td></td></td>	lientConfig> <td>oap:Body:</td> <td><td>e&gt; 536 <feat< td=""><td>ure type 23"</td></feat<></td></td>	oap:Body:	<td>e&gt; 536 <feat< td=""><td>ure type 23"</td></feat<></td>	e> 536 <feat< td=""><td>ure type 23"</td></feat<>	ure type 23"
2020_01_23_17_26_51_83	sw_149 c	172.16.9.171:3033 tcp 213.199.166.30:80	hr="0x82000019" action="3" />-	/Feature>/ErrorRespo	nseTable><1			etup + Investigator Q Search & I					
2020_01_23_16_12_04_81	sw_149 d	x	<image/> http://www.msn.nl/img/ nl/services_tab/services_tab.html			lacover O Create	Seatth	Seeds Inc. 200, 21, 21, 20, 22, 20, 21				Streams Objects Search	Analyzer Packets M
		145.72.70.20:80 tcp 172.16.9.171:2947	<pre><image/>http://cp.intl.match.con</pre>			a.	Al Pack					Q	
		172.16.9.171:2947 tcp 145.72.70.20:80	ushpwea=wc:USNY0996; MUIE			uived20 infrogreed)	True > 19798	WTS Source	Destration Pro	Hoad Length	leko POST / nabitiumellond1at-6/28	Equite's and a second s	
		145.72.70.20:80 tcp 172.16.9.171:2953	NAP=V=1.5&E=4ff&C=K2IxctJF instance" xmIns:xsd="http://www		and the second second second second		additione (0 > 19/30	10217 798819248 1172 783 171 2027	612031.010 H	125	POST (nahramation)a=6:23	Billeteittis Egect in Dathearen	OET multiteer effer ET
		172.16.9.171:3048 tcp 146.101.162.215:80	<clientinfo> <country>NL<td>ntry&gt; <clcid>0409<td>LCID&gt; <plcid>0409&lt;</plcid></td><td>10.01.01.02.00.00 m</td><td></td><td></td><td></td><td></td><td>WedSP6415h345</td><td>48-4-20059-414-0000- 1112-4052-56-1074-2005-1 72-56-62-1020-4-101791, 744</td><td>10140733/0300-0444-4</td></clcid></td></country></clientinfo>	ntry> <clcid>0409<td>LCID&gt; <plcid>0409&lt;</plcid></td><td>10.01.01.02.00.00 m</td><td></td><td></td><td></td><td></td><td>WedSP6415h345</td><td>48-4-20059-414-0000- 1112-4052-56-1074-2005-1 72-56-62-1020-4-101791, 744</td><td>10140733/0300-0444-4</td></clcid>	LCID> <plcid>0409&lt;</plcid>	10.01.01.02.00.00 m					WedSP6415h345	48-4-20059-414-0000- 1112-4052-56-1074-2005-1 72-56-62-1020-4-101791, 744	10140733/0300-0444-4
		172.16.9.171:3021 tcp 65.54.239.214:80	name="P2P"> <entry 0x82000019"="" action="3" hr="0x820&lt;br&gt;hr="></entry>			BUCKBUCK -		120 MAR 171 BB7	82684810	P 1514	(TCP Previous segment not capture traditioners/forefliced		e Previous argument)( nor capitured )
			<image/> http://www.msn.nl/img/	/nl/nl-nl/services_tab/em	_wink8.png		548 of \$ 12780	1007 787 42405 (72 ALA 174 2807	8363(D10 TC	P 112	POST /welcherweicherfter Acid mtxxd8/2/683/ER-268	ESPain(SII)-	
_		213.199.166.30:80 tcp 172.16.9.171:3033	nl/services_tab/services_tab.html			10 ET 34 (0 3) 45 314 w	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	12227 707142103 172.103(171.2027	6524631.5230 HT	77 124	POST / webcher webbend hat die das		faidementant 120
Delete All Se	irches	172.16.9.171:3035 tcp 84.53.136.160:80	<image/> http://cp.intl.match.com	/msn/icons/heart_msnnl	.png <name></name>	10, p. N. R. R. R. M. M.					110000000000000000000000000000000000000	dr-Arizabilituri alimi tritoatte 2454 v E-Arizabilituri tritoatte 2454 v E-Arizabilituri	1014915X/0340-3498

Figure 64-Search View Packets button

• **Objects Button**: Clicking on the **Objects** button for a search displays the object info including the FileName, Size, MD5 and View action.



Discover	O CreateSearch	Find Text				E Node:149 Scarch: fms_2020_01_23_16_12_04_814 Streams	Objects	Search Analyzer	Packets N
nd Text		FileName	Size	MD5					
		object159(1)	77	2b63a0dbf	۲				
Completed(20) In	Progress(0)	msnlogo(1).gif	899	afc8089d681f					
archName	NodeName	object191(1).image%2fpng	1759	5528aca1bbd					
s_2020_01_27_12_51_0		Local.css(3).aspx%3fSubSite=M essenger	6652	b0ca45df1bca					
s_2020_01_27_12_50_1		Local.css(4).aspx%3fSubSite=M	767	3cf6bebb95cd					
s_2020_01_24_15_51_4		essenger							
s_2020_01_24_09_28_1		Local.css(5).aspx%3fSubSite=M	796	ebdcb3dd42f9					
s_2020_01_24_09_27_0		× essenger							
ns_2020_01_24_09_21_4		x ac_aanvragen.gif.meta	610	c9181b79a2ff	۲				
ns_2020_01_24_09_20_4		× audio(1).jpg	847	142c46ee5b4	۲				
s_2020_01_24_09_02_4		audio.jpg	847	142c46ee5b4	۲				
ns_2020_01_24_08_58_0		boy1f(1).j		2072	۲				
ns_2020_01_24_08_39_0 ns_2020_01_24_00_51_1			cking on the						
ns_2020_01_24_00_51_1		huperlink	ked filename	takes	۲				
ns_2020_01_23_23_46_4		em_winke to the A	Il Packet vie	w for	۲				
ns 2020 01 23 23 34 0		em y nk furt	ther analysis	30d	۲				
ns 2020 01 23 23 28 2		wnitepixel.gif	43	bff56ce49dd4					
ns_2020_01_23_23_09_1		em_wink8.png.meta	627	3dc8d7ec5f50	۲				
ns 2020 01 23 23 00 0		x internetbankieren.html	15438	108d5af0fc2e					
ns_2020_01_23_17_29_5	_296 sw_149	x internetbankieren.meta	604	d7c4f0364288	۲				
ns_2020_01_23_17_26_5	_833 sw_149	search(1).jpg	776	6fb48b4bd7cb	۲				
ms_2020_01_23_16_12_0	4_814 sw_149	x search.jpg	776	6fb48b4bd7cb	۲				
		sgmserver.dll.meta	529	131b/64/b671	۲				
					-				
		whitepixel.gif.meta	616	537685a458f7	۲				
		all_files_in_one.pdf	128067	0ac94829617	۲				

Figure 65-Search Object button

- If a file name is hyperlinked, clicking on the link will pivot to Packets View to show the packets that are related to the hyperlinked file.
- The MD5sum value of the file is displayed in red color and hyperlinked if the md5sum matches one of the known bad md5sum values uploaded via Policy→ Augmentation → Malware. Clicking on this hyperlink will display corresponding description of the MD5sum entry.
- Clicking on View icon allows the user to view the extracted object as a pdf (if it is viewable)

Discover	O CreateSearch	Find Text				Node:149 Search: fms_2020_01_23_16_12_04_814 Streams	Objects Search Analyzer Packets
nd Text		FileName	Size	MD5		all_files_in_one.pdf	
		object159(1)	77	2b63a0dbf	۲		
ompleted(20)	InProgress(0)	msnlogo(1).gif	899	afc8089d681f			
chName	NodeName	u object191(1).image%2fpng	1759	5528aca1bbd			
2020_01_27_12_5		Local.css(3).aspx%3fSubSite=M essenger	6652	b0ca45df1bca			
2020_01_27_12_50 2020_01_24_15_5		CLocal.css(4).aspx%3fSubSite=M essenger	767	3cf6bebb95cd			
2020_01_24_09_2		C Local.css(5).aspx%3fSubSite=M essenger	796	ebdcb3dd42f9			
2020_01_24_09_2	_47_590 sw_149	x ac_aanvragen.gif.meta	610	c9181b79a2ff	۲		
2020_01_24_09_2	_43_331 sw_149	audio(1).jpg	847	142c46ee5b4	۲		
2020_01_24_09_0		audio.jpg	847	142c46ee5b4	۲		
2020_01_24_08_5	_06_675 sw_149	×	14201	da406ca2072			
_2020_01_24_08_3		x boy11(1).jpg			۲		15 M
_2020_01_24_00_5		x boy1f.jpg	14201	da406ca2072	۲		
_2020_01_23_23_4		em_wink8(1).png	1440	31e512f0230d	۲		Rec 1
2020_01_23_23_4		em_wink8.png	1440	31e512f0230d	۲		
2020_01_23_23_3		whitepixel.gif	43	bff56ce49dd4			
2020 01 23 23 0		em_wink8.png.meta	627	3dc8d7ec5f50	۲		
2020 01 23 23 0		x internetbankieren.html	15438	108d5af0fc2e			
s_2020_01_23_17_2	_53_296 sw_149	x internetbankieren.meta	604	d7c4f0364288	۲		
2020_01_23_17_2	_51_833 sw_149	search(1).jpg	776	6fb48b4bd7cb	۲		
s_2020_01_23_16_1	_04_814 sw_149	search.jpg	776	6fb48b4bd7cb	۲		
		sqmserver.dll.meta	529	131bf64fb671	۲		
		whitepixel.gif.meta	616	537685a458f7			
		all files in one.pdf	128067	0ac94829617	_		
		an_mes_in_one.pdf	128067	uac94829617	۲		

Figure 66-Search Download Objects button



- Clicking on Download Objects button downloads the zip file that contains the raw files as they are extracted.
- Search Analyzer button: Clicking on the Search Analyzer button displays the Kibana investigator that shows all metadata related to the selected search.

🕥 Sentry	Wire Das	shboard 🔦	Policy S	etup	a View Metadata			Reports	Configuration	O Help	🕞 Logout
± Discover	O Crea	ateSearch	I Node:1	49 Search: fms_2020_01_23_16_12_04_8	4		Streams	Objects S	earch Analyzer	Packets	Manager
Find Text											
Completed(20)	InProgress	i(0)	K	Discover							0 1
SearchName		NodeName U		New Save Open Share Ir	spect						
fms_2020_01_27_1	2_51_09_161	sw_149 cc	©	New Save Open Share in	spect						
fms_2020_01_27_1		sw_149 cc		□ Uindex :"ncsearch_fms.	2020_01_23_16_12_04_814"	KQL	🛗 🗸 Last 7 days		Show date	es C	Refresh
fms_2020_01_24_1		sw_149 cc	0			_					
fms_2020_01_24_0		sw_149 cc		🗊 – + Add filter							
fms_2020_01_24_0 fms_2020_01_24_0		sw_149 cc sw_149 cc	111								
fms_2020_01_24_0		sw_149 ct sw_149 ct		ncsearch_* (change)	5		<b>750</b> hits				
fms_2020_01_24_0		sw_149 cc		0	Jan 21, 2020 @ 10	24:50.56	3 - Jan 28, 2020 @ 10:24:50.563	- Auto	~		
fms_2020_01_24_0		sw_149 cc	â	Q Search field names							
fms_2020_01_24_0		sw_149 cc	1003	<ul> <li>Filter by type</li> <li>O</li> </ul>							
fms_2020_01_24_0	0_51_10_92	sw_149 cc			600						
fms_2020_01_23_2	3_49_15_990	sw_149 cc	- T	Selected fields	<b>t</b> 400						
fms_2020_01_23_2	3_46_45_434	sw_149 cc	8		Ö						
fms_2020_01_23_2	3_34_08_261	sw_149 cc		_source	200						
fms_2020_01_23_2		sw_149 cc	5	Available fields							
fms_2020_01_23_2		sw_149 cc		t_id	0						
fms_2020_01_23_2		sw_149 cc	5	1 _0	2020-01-21 12:00 2020-01-22 12:00 2020-01-23	2:00	2020-01-24 12:00 2020-01-25 12:00	2020-01-26 12:0	0 2020-01-27 1	2:00	
fms_2020_01_23_1 fms_2020_01_23_1		sw_149 cc		t _index			timestamp per 3 hours				
fms_2020_01_23_1 fms_2020_01_23_1		sw_149 cc sw_149 cc	5		Timesource						
1115_2020_01_23_1	0_12_04_014	5W_145 CL		# _score							
				t _type	> Jan 23, 2020 @ 16:07:43.875 timestamp: Jan 2	8, 2020 @	16:07:43.875 flow_id: 1,441,11	8,480,505,520.25	5		
			(2)		nc_id: /storage@	int1267/4	38837_07/1579813658621033413_15	79813664006754.	pcap.cz.ignore p	cap_cnt: 9	02,755,502
			- <u>-</u>	t alert.action	event_type: file	info ip_m	ap_id: NULL src_ip: 84.53.136.	152 src_port: 86	0 dest_ip: 172.1	6.9.171	
			ŵ	t alert.category	dest_port: 2,798	proto: T	CP ether.type: 2,048 ether.srd	: 00:0e:0c:72:03	3:1c ether.dst:	00:18:4d:7	0:65:d1
					http.hostname: i	nages.app]	e.com http.url: /global/elemen	ts/prettysearch/	searchfield_left	cap.png	
🗎 Del	lete All Search	es	≣⇒	alert.gid							
					1 1 1 A. A.A. A.A.A. A. A.A. A.A. A.A.						

Figure 67-Search Analyzer Button

- The default view filter is the selected search name only.
- To search for a specific metadata type, add the type to the filter

## For example:

The following change will show only the **38** file events( out of **750** total events of all types) that belong to the search being analyzed.



Sentry Wir	e 🏦 Das	shboard 🔦	Policy S	etup    Investigator    Q Search	a View M	etadata					🖹 Repo	orts & Configuration	🛛 Help	🕒 Logout
1. Discover	O Crea	ateSearch	Mode:10	0.1.55.149 Search: fms_2020_01_24_15_51_48_	227					Streams	Objects	Search Analyzer	Packets	Manager
Find Text														
Completed(22)	InProgress	s(0)	K	D Discover									٩	⊠ 😐
SearchName		NodeName U		New Save Open Share In	nspect									
fms_2020_01_28_11_1	0_49_336	sw_149 cc	C	□ v _index :"ncsearch_fms	2020 01 22	16 12 04 914" and over	at type:'fileipfe'	KQL		Last 7 days		Show dat	00	Update
fms_2020_01_28_10_5		sw_149 cc	and the second		2020_01_23	10_12_04_014 and ever	ictype. menno	NUL		Last / uays		Show uar	<b>CS S</b>	opuate
fms_2020_01_28_10_5		sw_149 cc	$\bigcirc$	(=) - + Add filter										
fms_2020_01_28_10_5		sw_149 cc		0										
fms_2020_01_27_12_5		sw_149 cc		ncsearch_* (change)						38 hits				
fms_2020_01_27_12_5 fms_2020_01_24_15_5		sw_149 cc		(ondige)			lan 21 2020 @	12-16-35 177	7 - Jan 3	28, 2020 @ 12:16:35.177 -	Auto	~		
fms_2020_01_24_09_2		sw_149 cc		Q Search field names			5811 21, 2020 @	12.10.00.177	/ - Jan 2	.0, 2020 @ 12.10.33.177	Auto	·		
fms_2020_01_24_09_2		sw_149 cc	<b>a</b>	<u> </u>										
fms_2020_01_24_09_0		sw_149 cc	1000	<ul> <li>Filter by type</li> <li>O</li> </ul>	30									
fms_2020_01_24_08_5		sw_149 cc		Selected fields	¥									
fms_2020_01_24_08_3	9_04_975	sw_149 cc		Selected news	20 Count									
fms_2020_01_24_00_5	1_10_92	sw_149 cc	60	<pre>_source</pre>	10									
fms_2020_01_23_23_4	9_15_990	sw_149 cc		Available fields										
fms_2020_01_23_23_4		sw_149 cc	8		0									
fms_2020_01_23_23_3		sw_149 cc		t_id		2020-01-22 00:00 2	020-01-23 00:00 2	2020-01-24 00:00	0 2	020-01-25 00:00 2020-01	26 00:00	2020-01-27 00:00 2	020-01-28 00:00	5
fms_2020_01_23_23_2		sw_149 cc	50	t _index					time	stamp per 3 hours				
fms_2020_01_23_23_0		sw_149 cc			Time -		_source							
fms_2020_01_23_23_0 fms_2020_01_23_17_2		sw_149 cc sw_149 cc	5	# _score	Time 🗸		_aource							
fms_2020_01_23_17_2		sw_149 cc	-1		> Jan 24	, 2020 @ 15:48:31.513	event_type: file	einfo times	stamp:	an 24, 2020 @ 15:48:31.	513 flow_id	1,428,383,047,086,	436	
fms_2020_01_23_16_1		sw_149 cc	9	t _type			nc id: /storage	0/int1248/4	38869 4	3/1579898909661163931_1	79898934663	6369 pcap cz ignore		
			⊕	t alert.action						: NULL src_ip: 72.167.			10.1.1.52	
			ę	t alert.category			dest_port: 52,7 http.hostname:			er.type: 2,048 ether.s	c: 58:49:3b	:07:dd:11 ether.dst	90:fb:5b:	e6:7c:82
		_		# alert.gid			ncep.nostname:	ocsp.godadd	y.com					
a Delete	All Search	Ies	⇒	a alast sau	∨ Jan 24	, 2020 @ 15:48:29.155	event_type: file	<mark>einfo</mark> times	stamp: 、	lan 24, 2020 @ 15:48:29	155 flow_id	1: 683,311,443,832,66	5	

Figure 68-Search Analyzer Results view

The following types of metadata are available for analysis and discovery through Kibana:

Event Type	KQL Search Filter
Alert	event_type:'alert'
File	event_type:'fileinfo'
DNS	event_type:'dns'
SMTP	event_type:'smtp'
ActiveTrigger	event_type:'activetrigger'
НТТР	event_type:'http'
TLS/SSL	event_type:'tls'
SMB	event_type:'smb'
VOIP	event_type:'voip'
Suspicious IP Alerts	event_type:'suspip'
Suspicious Signature Alerts	event_type:'ja3'
Suspicious Domains	event_type:'suspdomain'

• **Packets** button: Clicking on the **Packets** button displays the first page of packets of the search. If the search contains multiple pages of packets, each page can be viewed one after the other. The user can also switch to a specific page before going to next page or previous page.



Sentry Wire	#Dasi		Policy Setup   Investigation (%)		a View Metadata						Repor	ts 🌣 Configuratior	1 🕑 Help	🕞 Logo
Discover	Create	Search	Node: 130 Search: fms_2020_0	1_25_19_32_11_280						Streams	Objects	Search Analyzer	Packets	Manager
find Text			All Packets		Search					Q			@ to []	$\langle \rangle$
Completed(17) Inl	rogress(	0)	Timestamp	Source	Destination	Protocol	Length	Info			Expertinfo			
			> 1579998191.029989775	192.168.16.200 49152	192.168.15.52 52056	UDP	78	49152 â	52056 Len=32					
earchName		NodeName	> 1579998191.029990095	192.168.15.224 50940	192.168.16.200 49154	UDP	78	50940 â	49154 Len=32					
ns_search2_ms_2020_01_	26_20_5	nc_130	> 1579998191.029990095	192.168.16.200 49154	192.168.15.224 50940	UDP	78	49154 å	50940 Len=32					
13_31			> 1579998191.029990927	192.168.16.200 49152	192.168.15.52 52056	UDP	78	49152 å	52056 Len=32					
ns_search1_fms_2020_01	26_20_5	nc_130	> 1579998191.029990927	192.168.15.224 50940	192.168.16.200 49154	UDP	78	50940 â	49154 Len=32					
_05_424			> 1579998191.029990927	192.168.16.200 49152	192.168.15.52 52056	UDP	78	49152 å	52056 Len=32					
ms_2020_01_25_19_32_11	_280	nc_130	> 1579998191.029990927	192.168.16.200 49154	192.168.15.224 50940	UDP	78	49154 â	50940 Len=32					
ns_2020_01_25_18_49_0	_691	nc_130	> 1579998191.029990927	192.168.15.224 50940	192.168.16.200 49154	UDP	78	50940 â	49154 Len=32					
ms_2020_01_24_05_56_4	_126	nc_130	> 1579998191.029990927	192.168.16.200 49154	192.168.15.224 50940	UDP	78	49154 å	50940 Len=32					
ns_2020_01_23_11_24_28	_602	nc_130	> 1579998191.029990927	192.168.16.200 49152	192.168.15.52 52056	UDP	78	49152 å	52056 Len=32					
ns_2020_01_23_11_14_54	296	nc_130	> 1579998191.029990927	192.168.15.224 50940	192.168.16.200 49154	UDP	78	50940 â	49154 Len=32					
ns_2020_01_21_12_56_0	_936	nc_130	(											
ms_2020_01_19_22_25_5	_240	nc_130	frame.time_epoch:		1579998191.029990927									
ns_2020_01_19_18_42_3	343	nc_130	frame.ip.src:		192.168.15.224									
ns 2020_01_17_14_50_3		nc_130	frame.tcp.srcport:											
ns_2020_01_16_20_56_1		nc 130	frame.udp.srcport:		50940									
ns 2020 01 16 20 40 5		nc_130	frame.ip.dst:		192.168.16.200									
ns 2020 01_16_19_29_1		nc_130	frame.tcp.dstport:											
ns 2020 01 16 19 07 4		nc_130	frame.udp.dstport:		49154									
			ip.protocol:		UDP									
ns_2020_01_16_18_56_24		nc_130	info:		50940 å 49154 Len=32									
ns_2020_01_16_11_21_08	_765	nc_130	expert:											
			data:		80128666e2c6a399505606f	c28e6d420191f	14d446fe3c3f7	ed315a88d54b	b44					
			}											
			> 1579998191.029991227	192.168.16.200 49154	192.168.15.224 50940	UDP	78	49154 å	50940 Len=32					
			> 1579998191.029992179	192.168.16.200 49152	192.168.15.52 52056	UDP	78	49152 å	52056 Len=32					
			> 1579998191.029992179	192.168.15.224 50940	192.168.16.200 49154	UDP	78	50940 â	49154 Len=32					
			> 1579998191.029992179	192.168.16.200 49154	192.168.15.224 50940	UDP	78	49154 â	50940 Len=32					
💼 Delete All	Searche		> 1579998191.029992179	192.168.16.200 49152	192.168.15.52 52056	UDP	78	49152 å	52056 Len=32					

Figure 69-Search Packets results

• Clicking on the Search bar allows free form text search for packets. In the image below, the search string is Application.

Sentry Wire #Da	ashboard	Policy Setup   Inve	estigator Q Search	View Metadata				Reports 🌣 Configurat	ion 🕑 Help	🕩 Logo
Discover O Cre	ateSearch	Node: 130 Search: fms_2020_01	_25_19_32_11_280				Streams	Objects Search Analyze	Packets	Manage
Find Text		All Packets	[	Application			Q		e to 0	
Completed(17) InProgre	ee/(I)	Timestamp	Source	Destination	Protocol	Length	Info	Expertinfo		
	(-)	> 1579998191.000016443	52.91.234.203 443	192.168.15.68 53541	TLSv1	511	Application Data			
earchName	NodeName	> 1579998191.006805851	192.168.15.68 52541	63.251.34.147 443	TLSv1.2	92	Application Data			
ms_search2_ms_2020_01_26_20	5 nc_130	> 1579998191.006805851	63.251.34.147 443	192.168.15.68 52541	TLSv1.2	92	Application Data			
_13_31		> 1579998191.010654065	192.168.15.224 50943	192.168.16.200 5005	RTCP	282	Sender Report Source description Application specific ( -A			
ns_search1_fms_2020_01_26_20	_5 nc_130	> 1579998191.020985197	63.251.34.137 443	192.168.15.64 61017	TLSv1.2	104	Application Data			
_05_424		> 1579998191.020986059	192.168.15.64 61017	63.251.34.137 443	TLSv1.2	104	Application Data			
ns_2020_01_25_19_32_11_280	nc_130	> 1579998191.026123887	192.168.15.55 64514	143.127.136.95 443	TLSv1.2	111	Application Data			
ms_2020_01_25_18_49_05_691	nc_130	> 1579998191.030005935	192.168.15.59 52312	63.251.34.137 443	TLSv1.2	92	Application Data			
ms_2020_01_24_05_56_49_126	nc_130	> 1579998191.040964155	192.168.15.59 54961	143.127.136.95 443	TLSv1.2	111	Application Data			
ms_2020_01_23_11_24_28_602	nc_130	> 1579998191.040989113	192.168.16.3 443	192.168.15.79 59103	TLSv1	316	Application Data			
ms_2020_01_23_11_14_54_296	nc_130	> 1579998191.041584712	192.168.15.224 50943	192.168.16.200 5005	RTCP	270	Sender Report Source description Application specific ( -A			
ms_2020_01_21_12_56_08_936	nc_130	> 1579998191.049315164	143.127.136.95 443	192.168.15.68 52562	TLSv1.2	111	Application Data			
ms_2020_01_19_22_25_53_240	nc_130	> 1579998191.049325614	192.168.15.71 54134	143.127.136.95 443	TLSv1.2	111	Application Data			
ms_2020_01_19_18_42_34_343	nc_130	> 1579998191.060946530	143.127.136.95 443	192.168.15.67 49533	TLSv1.2	111	Application Data			
ms 2020 01 17 14 50 34 727	nc 130	> 1579998191.060948163	192.168.15.77 49192	63.251.34.208 443	TLSv1.2	92	Application Data			
ms_2020_01_16_20_56_15_14	nc_130	> 1579998191.060950829	63.251.34.208 443	192.168.15.77 49192	TLSv1.2	92	Application Data			
ms_2020_01_16_20_40_53_756	nc_130	> 1579998191.060978501	143.127.136.95 443	192.168.15.61 61886	TLSv1.2	111	Application Data			
ms_2020_01_16_19_29_12_754	nc_130	> 1579998191.064782862	192.168.15.79 49435	52.91.234.203 443	TLSv1	383	Change Cipher Spec, Encrypted Handshake Message, Application Dat			
ms_2020_01_16_19_07_44_628 ms_2020_01_16_18_56_24_435	nc_130 nc_130	> 1579998191.064789815	52.91.234.203 443	192.168.15.79 49435	TLSv1	511	[TCP ACKed unseen segment] , Application Data	Expert Info (Warning/Sequence): ACKe (common at capture start)	d segment that wasn'	't captured
ms_2020_01_16_11_21_08_765	nc_130	> 1579998191.068663648	192.168.16.6 3389	192.168.15.55 58009	TLSv1.2	159	Application Data			
		> 1579998191.080959914	192.168.15.61 61176	63.251.34.133 443	TLSv1.2	92	Application Data			
		> 1579998191.080959914	63.251.34.133 443	192.168.15.61 61176	TLSv1.2	92	Application Data			
		> 1579998191.080995541	192.168.15.62 57864	143.127.136.95 443	TLSv1.2	111	Application Data			
		> 1579998191.084118521	143.127.136.95 443	192.168.15.60 62350	TLSv1.2	111	[TCP ACKed unseen segment] , Application Data	Expert Info (Warning/Sequence): ACKe (common at capture start)	d segment that wasn'	't captured
		> 1579998191.084123580	192.168.15.94 49194	143.127.136.95 443	TLSv1.2	111	Application Data			
		> 1579998191.121215425	192.168.15.52 52059	192.168.16.200 5005	RTCP	266	Sender Report Source description Application specific ( -A			
		> 1579998191.121392961	192.168.15.77 49213	143.127.136.95 443	TLSv1.2	111	Application Data			
Delete All Searc	hes	> 157000R101 12205R600	143 127 136 95 443	192 168 15 77 49213	TI Sv1 2	111	Application Data			

Figure 70-Search Packets Search Bar

- Clicking on All Packets button reverts to display all packets.
- Clicking on Source or Destination hyperlink displays all packets with IP and port matching the ones selected. In the example below, clicking on the hyperlinked source (192.168.16.3 443), displays all packets that have IP address 192.168.16.3 and port 443.



Sentry Wire	#Dash	nboard	<b>≮</b> P	olicy Setup 👁 Inve	stigator Q Search	a View Metadata						Repor	ts 🌣 Configuratio	on 🛛 Help	🕞 Log
Discover O	Create	Search	Nox	le:130 Search: fms_2020_0	01_25_19_32_11_280						Streams	Objects	Search Analyzer	Packets	Manage
Find Text			All	Packets		Search					Q			e to 0	$\langle \rangle$
Completed(17) InPr	rogress(		_	Timestamp	Source	Destination	Protocol	Length	Info			Expertinfo			
completed(17)	iogress(	0)	>	1579998191.040989113	192.168.16.3 443	192.168.15.79 59103	TCP	1437	[TCP segment of a	a reassembled	PDU]				
SearchName		NodeName	>	1579998191.040989113	192.168.16.3 443	192.168.15.79 59103	TLSv1	316	Application Data						
ms_search2_ms_2020_01_20 5_13_31	26_20_5	nc_130	>	1579998191.452190018	192.168.16.3 443	192.168.15.79 59	011-1-1-			gment not cap	tured] , Application Data	Expert Info (Wa (common at ca	arning/Sequence): Previou pture start)	is segment(s) not o	aptured
ms search1 fms 2020 01 2	26 20 5	nc_130	>	1579998191.572199125	192.168.16.3 443	192.168.15.7	Clickir	ng on	the	CK] Seq=1 /	Ack=1 Win=508 Len=0				
4_05_424 fms 2020 01 25 19 32 11	280	nc 130	>	1579998191.572199125	192.168.15.79 59103	192.168.16.3	yperlin	k sor	s and	segment] 5	59103 å 443 [ACK]	Expert Info (Wa (common at ca	arning/Sequence): ACKed pture start)	segment that was	n't captured
ms 2020 01 25 18 49 05		nc_130	>	1579998191.572199125	192.168.16.3 443	192.168.15.7	isplays	the n	ackote	CK] Seq=1 /	Ack=373 Win=506 Len=0				
ms_2020_01_24_05_56_49_		nc_130	>	1579998191.575151982	192.168.15.79 59103					n segment] 5	59103 â 443 [ACK]	Expert Info (Wa (common at ca	aming/Sequence): ACKed pture start)	segment that was	n't captured
ms_2020_01_23_11_24_28_0	_602	nc_130	>	1579998191.591862355	192,168,16,3 443		of selec	tea I	and	ent not cap	tured] . Application Data	1	arning/Sequence): Previou	is segment(s) not c	aptured
ms_2020_01_23_11_14_54_3	296	nc_130					port co	mhin	ation			(common at ca			
ms_2020_01_21_12_56_08_1	_936	nc_130	>	1579998191.591862355	192.168.16.3 443 🥌	192.168.15.79	port 00			ACK] Seq=1 /	Ack=1545 Win=508 Len=0				
ms_2020_01_19_22_25_53_	_240	nc_130		1579998191.591863256	192.168.16.3 443	192.168.15.79 5910									
ms_2020_01_19_18_42_34_	_343	nc_130		1579998191.591863256	192.168.16.3 443	192.168.15.79 59102	TCP	64	11.040.040 P.040.040.04		Ack=1885 Win=507 Len=0				
ms_2020_01_17_14_50_34_	_727	nc_130		1579998191.640890283	192.168.16.3 443	192.168.15.79 59102	TCP	64			Ack=4615 Win=512 Len=0				
ms_2020_01_16_20_56_15_ ms_2020_01_16_20_40_53_		nc_130	,	1579998191.640890283	192.168.16.3 443	192.168.15.79 59103	TCP	1437	[TCP Previous seg reassembl	gment not cap	tured] [TCP segment of a	Expert Info (Wa (common at ca	arning/Sequence): Previou pture start)	is segment(s) not c	aptured
ms_2020_01_16_19_29_12_		nc_130	>	1579998191.640890283	192.168.16.3 443	192.168.15.79 59103	TCP	1437	443 å 59103 [/ Len=1379 [TCP se		59 Ack=1 Win=513				
ms_2020_01_16_19_07_44_	628	nc_130	>	1579998191.640890283	192.168.16.3 443	192.168.15.79 59103	TLSv1	1420			tured], Ignored Unknown	Expert Info (Wa	aming/Sequence): Previou	is segment(s) not c	aptured
ms_2020_01_16_18_56_24_	_435	nc_130							Record			(common at ca			
ms_2020_01_16_11_21_08_	_765	nc_130	>	1579998191.640890283	192.168.16.3 443	192.168.15.79 59103	TCP	1437	[TCP Out-Of-Order Ack=1 Win=513 Le		59103 [ACK] Seq=8397	Expert Info (Wassegment	arning/Sequence): This fra	me is a (suspected	i) out-of-order
			>	1579998191.640890283	192.168.15.79 59103	192.168.16.3 443	TCP	64	[TCP ACKed unser Seq=1 Ack=7038 V		59103 â 443 [ACK]	Expert Info (Wa (common at ca	arning/Sequence): ACKed pture start)	segment that was	n't captured
			>	1579998191.640891726	192.168.16.3 443	192.168.15.79 59103	TCP	1417	[TCP Out-Of-Order Seg=7038 Ack=1 V		59103 [PSH, ACK]	Expert Info (Wasegment	aming/Sequence): This fra	me is a (suspected	i) out-of-order
			>	1579998191.640891726	192.168.15.79 59103	192.168.16.3 443	тср	70	[TCP Dup ACK 12: Ack=7038 Win=37	365#1] 59103	å 443 [ACK] Seq=1	-	te/Sequence): Duplicate /	ACK (#1)	
			>	1579998191.640891726	192.168.15.79 59103	192.168.16.3 443	TCP	70	[TCP Dup ACK 12: Ack=7038 Win=37	365#2] 59103	å 443 [ACK] Seq=1	Expert Info (No	te/Sequence): Duplicate /	ICK (#2)	
2 Delete All S	Searche	s	`	1570000101 640001700	100 100 10 70 00100	100 100 10 0 440	TOD	0 A			Ank-11190 145n-900 1 nn-0				

Figure 71-Search Packets Results Source or Destination

• Clicking on a packet's Protocol hyperlink displays all packets with the same protocol. In the following example, all packets with protocol TLSv1 or TLSv1.2 are displayed.

Sentry Wir	mDas		🛠 Policy Setup 🗶 Inve		a view Metadata					rts 🌣 Configuration	- Ontop	🕩 Logo
Discover	O Creat	eSearch	III Node:130 Search: fms_2020_01_25_19_32_1	11_280				Streams	Objects	Search Analyzer	Packets	Manage
Find Text			All Packets		Search			Q			@ to (0)	$\langle \rangle$
Completed(17)	InProgress	(0)	Timestamp	Source	Destination	Protocol	Length	Info	Expertinfo			
			> 1579998191.000016443	52.91.234.203 443	192.168.15.68 53541	TLSv1	511	Application Data				
earchName		NodeName	> 1579998191.006805851	192.168.15.68 52541	63.251.34.147 443	TLSv1.2	92	Application Data				
ns_search2_ms_2020	01_26_20_5	nc_130	> 1579998191.006805851	63.251.34.147 443	192.168.15.68 52541	TLSv1.2	92	Application Data				
13_31			> 1579998191.020985197	63.251.34.137 443	192.168.15.64 61017	TLSv1.2	104	Application Data				
ns_search1_fms_2020	_01_26_20_5	nc_130	> 1579998191.020986059	192.168.15.64 61017	63.251.34.137 443	TLSv1.2	104	Application Data				
_05_424			> 1579998191.026123887	192.168.15.55 64514	143.127.136.95 443	TLSv1.2	111	Application Data				
ns_2020_01_25_19_3		nc_130	> 1579998191.030005935	192.168.15.59 52312	63.251.34.137 443	TLSv1.2	92	Application Data				
ns_2020_01_25_18_4	9_05_691	nc_130	> 1579998191.040964155	192.168.15.59 54961	143.127.136.95 443	TLSv1.2	111	Application Data				
ns_2020_01_24_05_5	6_49_126	nc_130	> 1579998191.040989113	192.168.16.3 443	192.168.15.79 59103	TLSv1	316	Application Data				
ns_2020_01_23_11_2	4_28_602	nc_130 (	> 1579998191.049315164	143.127.136.95 443	192.168.15.68 52562	TLSv1.2	111	Application Data				
ns_2020_01_23_11_1	4_54_296	nc_130	> 1579998191.049325614	192.168.15.71 54134	143.127.136.95 443	TLSv1.2	111	Application Data				
ns_2020_01_21_12_5	6_08_936	nc_130	> 1579998191.060946530	143.127.136.95 443	192.168.15.67 49533	TLSv1.2	111	Application Data				
ns_2020_01_19_22_2	5_53_240	nc_130	> 1579998191.060948163	192.168.15.77 49192	63.251.34.208 443	TLSv1.2	92	Application Data				
ns_2020_01_19_18_4	2_34_343	nc_130	> 1579998191.060950829	63.251.34.208 443	192.168.15.77 49192	TLSv1.2	92	Application Data				
ns_2020_01_17_14_5	0_34_727	nc_130	> 1579998191.060978501	143.127.136.95 443	192.168.15.61 61886	TLSv1.2	111	Application Data				
ns_2020_01_16_20_5		nc_130	> 1579998191.064782862	52.91.234.203 443	192.168.15.79 49435	TLSv1	207	Server Hello, Change Cipher Spec, Encrypted Handsha Message	keys (Session	ote/Sequence): This session resumption)	reuses previously	y negotiated
ns_2020_01_16_20_4 ns_2020_01_16_19_2		nc_130 +	> 1579998191.064782862	192.168.15.79 49435	52.91.234.203 443	TLSv1	383	Change Cipher Spec, Encrypted Handshake Message, Application Dat				
ns_2020_01_16_19_0		nc_130	> 1579998191.064789815	52.91.234.203 443	192.168.15.79 49435	TLSv1	511	[TCP ACKed unseen segment] , Application Data	Expert Info (Wa (common at ca	arning/Sequence): ACKed si	egment that wasn	n't captured
ns_2020_01_16_18_5		nc_130	> 1579998191.068663648	192,168,16,6 3389	192,168,15,55 58009	TLSv1.2	159	Application Data	(common at ca	plure starty		
ns_2020_01_16_11_2	1_08_765	nc_130	> 1579998191.080959914	192.168.15.61 61176	63.251.34.133 443	TLSv1.2	92	Application Data				
			> 1579998191.080959914	63.251.34.133 443	192.168.15.61 61176	TLSv1.2	92	Application Data				
			> 1579998191.080995541	192.168.15.62 57864	143.127.136.95 443	TLSv1.2	111	Application Data				
			> 1579998191.084118521	143.127.136.95 443	192.168.15.60 62350	TLSv1.2	111	[TCP ACKed unseen segment] , Application Data	Expert Info (Wa (common at ca	arning/Sequence): ACKed se	egment that wash	n't captured
			> 1579998191.084123580	192.168.15.94 49194	143.127.136.95 443	TLSv1.2	111	Application Data	(section of or			
			> 1579998191.121392961	192.168.15.77 49213	143.127.136.95 443	TLSv1.2	111	Application Data				
			> 1579998191,122958699	143.127.136.95 443	192.168.15.77 49213	TLSv1.2	111	Application Data				
n Delete	All Search	es	> 1579998191.188509375	192.168.15.55 64514	143.127.136.95 443	TLSv1.2	111	Application Data				

Figure 72-Search Packets Results Protocols view

• **Manager** button: Clicking on the **Manager** button displays the search details of the search including UserName, SearchName, BeginTime, EndTime, Duration, SearchFilter and Results.



Discover         Objects         Sterem	SentryWir	e 🏦 Dasi	nboard 🔦	Policy Setup	👁 👁 Investigator 🝳 Search 🗂 View Metadata			Report	s 🌣 Configuration	🕜 Help	🕞 Lo
Instruction	Discover	O Crea	teSearch	I Node:149	Search: fms_2020_01_23_16_12_04_814	Stre	ams	Objects	Search Analyzer	Packets	Manag
Begin Time         Souther Constraints         Begin Time         2020-01.27:1.25:0.01         Begin Time         2020-01.27:1.20:0.01         Begin Time         2020-01.27:0.01         Begin Time         Perturbation Constraints         Perturba	i Text			UserName	continuum						
analysis         before         second         secon	ompleted(20)	InProgress	0)	SearchName	fms_2020_01_23_16_12_04_814						
words         words <td< td=""><td></td><td></td><td></td><th>BeginTime</th><td>2020-01-23 21:00:04</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>				BeginTime	2020-01-23 21:00:04						
Subscripting         Subscripi Subscripi Subscripting         Subscripting				EndTime	2020-01-23 21:12:04						
accord 124 15.61.40 22         accord 124 10.62 11 2000         accord 12			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1								
weile       Period											
2020_01_24_002_17_260         wi-14         x           2020_01_24_002_01_34         wi-14         x           2020_01_24_02_01_34         wi-144         x           2020_01_24_02_01_34         x				Result	Pkts=1724 Seconds=3 TotalSize=117KB MergeCount:16 SnapLen=All						
2020 0 1 2 4 02, 2 1 4 7 300     91, 4 9     0       2020 0 1 2 4 02, 2 04, 2 4 3 4     91, 4 9     0       2020 0 1 2 4 02, 5 04, 4 5     91, 4 9     0       2020 0 1 2 4 02, 5 04, 5 7     91, 4 9     0       2020 0 1 2 4 02, 5 04, 5 7     91, 4 9     0       2020 0 1 2 4 02, 5 04, 5 7     91, 4 9     0       2020 0 1 2 4 02, 5 04, 5 7     91, 4 9     0       2020 0 1 2 4 02, 5 4 1, 5 90     91, 4 9     0       2020 0 1 2 4 02, 5 4 1, 5 90     91, 4 9     0       2020 0 1 2 4 2 4 1, 5 90     91, 4 9     0       2020 0 1 2 4 2 4 1, 5 90     91, 4 9     0       2020 0 1 2 3 2 4 1, 5 90     91, 4 9     0       2020 0 1 2 3 2 4 1, 5 90     91, 4 9     0       2020 0 1 2 3 2 4 1, 5 90     91, 4 9     0       2020 0 1 2 3 2 4 1, 5 90     91, 4 9     0       2020 0 1 2 3 2 4 1, 5 91     91, 4 9     0       2020 0 1 2 3 2 4 1, 5 91     91, 4 9     0       2020 0 1 2 3 2 4 1, 7 95, 5 03     91, 4 9     0       2020 0 1 2 3 2 4 1, 7 2 5 5, 3 10     91, 4 9     0											
2020.01.24.09.02.44.340       w1.49       v2.         2020.01.24.09.02.44.340       w1.49       v2.         2020.01.24.09.02.470       w1.49       v2.         2020.01.24.09.02.170       w1.49       v2.         2020.01.24.09.01.170       w1.49       v2.         2020.01.24.09.01.170       w1.49       v2.         2020.01.23.24.04.01.100       w1.49       v2.											
2020,01,24,02,63,06,675       w1.49       ox         2020,01,24,02,63,04,075       w1.49       ox         2020,01,24,02,63,04,075       w1.49       ox         2020,01,24,02,64,04,04       w1.49       ox         2020,01,23,23,44,04,841       w1.49       ox <td></td> <td></td> <td></td> <th></th> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>											
020.01.24.06.56.06.75         wn.140         xo.           020.01.24.00.50.44.757         wn.140         xo.           020.01.24.00.51.74         wn.140         xo.           020.01.24.00.45.74         wn.140         xo.           020.01.24.00.45.74         wn.140         xo.           020.01.24.02.45.74         wn.140         xo.           020.01.23.01.46.74         wn.140         xo.           020.01.23.01.46.75         wn.140         xo.           020.01.23.01.46.											
0202.01_24.06_30,04.975     w1.40     w2       0202.01_23.23,40.910     w2.10     w2       0202.01_23.23,40.821     w1.40     w2											
2020_01_24_00_51_09_20     wr_149     or       2020_01_23_23_44_15_000     wr_149     or       2020_01_23_23_44_54_54     wr_149     or       2020_01_23_23_45_15_00     wr_149     or       2020_01_23_23_45_15_00     wr_149     or       2020_01_23_23_04_15_75     wr_149     or       2020_01_23_23_05_157     wr_149     or       2020_01_23_23_05_158     wr_149     or       2020_01_23_17_29_153_84     wr_149     or											
2020_01_23_23_40_454.34     wn.149     x       2020_01_23_23_40_561     wn.149     x       2020_01_23_23_20_91     wn.149     x       2020_01_23_23_20_01_45.75     wn.149     x       2020_01_23_23_20_01_45.75     wn.149     x       2020_01_23_27_20_53.296     wn.149     x       2020_01_23_17_20_51.293     wn.149     x											
2020_01_23_23_24_04_9_261         wr.149         oc           2020_01_23_23_02_01_575         wr.149         oc           2020_01_23_23_00_14575         wr.149         oc           2020_01_23_23_00_3575         wr.149         oc           2020_01_23_23_00_3575         wr.149         oc           2020_01_23_17_29_05_3266         wr.149         oc	2020_01_23_23_49	_15_990	sw_149 cc								
2020_01_23_23_28_29_31       w1.49       oc         2020_01_23_23_00_14_575       w1.49       oc         2020_01_23_23_00_01_57       w1.49       oc         2020_01_23_17_26_51_833       w1.49       oc	2020_01_23_23_46	45_434	sw_149 cc								
2020_01_23_23_00_01_45_75         wn_149         c           2020_01_23_23_00_01_557         wn_149         c           2020_01_23_17_29_51_833         wn_149         c	2020_01_23_23_34	_08_261	sw_149 cc								
2020_01_23_23_00_03_557	2020_01_23_23_28	_29_391	sw_149 cc								
2020_01_23_17_28_53_286	2020_01_23_23_09	_14_575	sw_149 cc								
2020_01_23_17_26_51_833 sw_149 cc	2020_01_23_23_00	_03_557	sw_149 cc								
			sw_149 cc								
_2020_01_23_16_12_04_814											
	_2020_01_23_16_12	_04_814	sw_149 cc								
						1 8	📥 PcapI	ata 📥 Logi	Data Stream Search I	caps 🖸 🖸 🕻	Clone Sear
1 🙄 🕹 PeapData 🕹 LogData 🏕 Stream Search Peaps 🛱 Clone Se	_										
1 🕤 📥 PeapData 📥 LogData 🏕 Stream Search Peaps 🛱 Clone Sea		All Searche									

Figure 73-Search Manager Button view

The links at the bottom are as follows:

- **PcapData link**: This link allows the user to view/download the PCAPs available for the respective search. Select a pcap number and choose PcapData link to download the specified pcap.
- **LogData link:** Clicking on this link downloads a zip file of the metadata of the search.

Discover	CreateSearch	I Node: 149	Search: fms_2020_01_23_16_12_04_814		Streams	Objects Search Ana	lyzer Packets	Manage
nd Text		UserName	continuum					
	-	SearchName	fms 2020 01 23 16 12 04 814					
Completed(20)	nProgress(0)	BeginTime	2020-01-23 21:00:04					
archName	NodeName U							
2020 01 27 12 51		EndTime	2020-01-23 21:12:04					
2020_01_27_12_51		Duration	00:00:12:20					
		SearchFilter	PcapData,port 80					
2020_01_24_15_51_ 2020_01_24_09_28	Contraction of the second s	Result	Pkts=1724 Seconds=3 TotalSize=117KB MergeCount:16 SnapLen=All					
				File Home Share V	fiew Compressed Folder Tools			~
_2020_01_24_09_27_				🔺 🖻 🖻 🕹 🖓			🕞 📙 Open 🔹 🔠 Sel	and all
_2020_01_24_09_21_					py path	Easy access •		lect none
2020_01_24_09_20_					ste shortcut to to Deleti	e Rename New folder	Properties	vert selection
_2020_01_24_09_02_				Clipboard	Organize	New		Select
2020_01_24_08_58_					> Downloads > metadata_fms_202			
_2020_01_24_08_39_				← → ∽ ↑ 🚺 > This PC	> Downloads > metadata_tms_202	0_01_23_16_12_04_814.2ip	v Ö Searc	n metad
2020_01_24_00_51_				S This PC	lame	Туре	Compressed size	Passwo
_2020_01_23_23_49_				3D Objects	alert.json	JSON File	19 k	KB No
_2020_01_23_23_46_	and the second				dns.json	JSON File	7 K	B No
_2020_01_23_23_34_	08_261 sw_149 cc				fileinfo.json	JSON File		KB No
_2020_01_23_23_28_	29_391 sw_149 cc			Downloads	flow.json	JSON File	810 K	KB No
_2020_01_23_23_09_	14_575 sw_149 cc			Music				
_2020_01_23_23_00_	03_557 sw_149 cc			E Pictures				
_2020_01_23_17_29_	53_296 sw_149 cc			🖉 Videos 🗸 🧹				
2020 01 23 17 26	51_833 sw_149 cc			4 items				
	04_814 sw_149 cc							

Figure 74-Search Packets Manager LogData results

• Stream Search PCAPs link: Clicking on this link allows the user to stream pcap data of the search to an external interface, for other applications to further analyze



the data. Stream Search Results option checkbox is available under "**Create Search**". Search Results can also be streamed after the search is completed. The results of a stream search are logged and available as part of metadata zip file.

Discover	O CreateSearch	I Node: 149 Search: fms_2020_01_23_16_12_04_814	Streams Objects Search Analyzer Packets Manager
nd Text Completed(20) sarchName s_2020_01_27_12_ s_2020_01_27_12_ s_2020_01_24_15_ s_2020_01_24_09_ s_2020_01_24_09_ s_2020_01_24_09_	50_10_386         sw_149         cc           51_48_227         sw_149         cc           28_13_200         sw_149         cc           27_07_503         sw_149         cc           21_47_590         sw_149         cc	UserName         continuum           SearchName         fms. 2020, 01; 23_16; 12, 04, 814           BeginTima         2020-01: 23 21:00:04           EndTime         2020-01: 23 21:10:04           Duration         00:00:12: 20           SearchFilter         PcapData,port 80           Result         Pkts=1724 Seconds=3 TotalSize=117KB MergeCount:16 SnapLen=All	
10         2020         01         24         09           10         2020         01         24         08           10         2020         01         24         08           10         2020         01         24         08           10         2020         01         24         08           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23           10         2020         01         23         23 <td>58,06,075         sw_149         cx           30,04,075         sw_149         cx           51,022         sw_149         cx           10,10,22         sw_149         cx           10,10,22         sw_149         cx           10,15,900         sw_149         cx           10,45,434         sw_149         cx           10,45,2931         sw_149         cx           28,29,391         sw_149         cx           0,04,575         sw_149         cx           0,03,577         sw_149         cx           29,53,2936         sw_149         cx</td> <td></td> <td></td>	58,06,075         sw_149         cx           30,04,075         sw_149         cx           51,022         sw_149         cx           10,10,22         sw_149         cx           10,10,22         sw_149         cx           10,15,900         sw_149         cx           10,45,434         sw_149         cx           10,45,2931         sw_149         cx           28,29,391         sw_149         cx           0,04,575         sw_149         cx           0,03,577         sw_149         cx           29,53,2936         sw_149         cx		
15_2020_01_23_17_i 15_2020_01_23_16_			1 ☺ ▲ PcapData ▲ LogData ♥Stream Search Peaps ♥ Clone Search

Figure 75-Search Manager Button Stream Search PCAPs view

• Clone Search link: Clicking on this link allows the user to recreate or clone the search. The new search name by auto filling the search parameters. The new search name is appended with a unique tag in the end in order to separate it from the original search. Begin/End Time, Search Filter are copied from the selected search. The user can modify any of these fields before submitting a clone search request.



🕥 Sentry W	Vire <b>#</b> Da	ishboard 🔸	Policy Setu	p @ Investigator Q Search	a View Metadata		Repoi	rts 🌣 Configuration	🛛 Help	🕩 Logout
± Discover	O Cre	eateSearch	III Node: 149	Search: fms_2020_01_23_16_12_04_814		Streams	Objects	Search Analyzer	Packets	Manager
Find Text Completed(22)	InProgres	is(0)	UserName SearchName	continuum fms_2020_01_23_16_12_04_814	Create Search					
			BeginTime	2020-01-23 21:00:04						
SearchName		NodeName U	EndTime	2020-01-23 21:12:04	SearchName					
fms_2020_01_28_11		sw_149 cc	Duration	00:00:12:20	fms_2020_01_23_16_12_04_814_uc8c9					
fms_2020_01_28_10		sw_149 cc	SearchFilter	PcapData,port 80	BeginTime					
fms_2020_01_28_10		sw_149 cc	Result	Pkts=1724 Seconds=3 TotalSize=117	2020-01-23 21:00:04					
fms_2020_01_28_10 fms_2020_01_27_12		sw_149 cc			EndTime					
fms_2020_01_27_12		sw_149 cc			2020-01-23 21:12:04					
fms_2020_01_24_15		sw_149 cc			2020-01-23 21:12:04					
fms_2020_01_24_05		sw 149 cc			Search Filter					
fms 2020_01_24_05		sw_149 cc			port 80					
fms 2020 01 24 05		sw_149 cc			MaxPacketCount					
fms 2020_01_24_08		sw_149 cc			1000					
fms_2020_01_24_08		sw_149 cc								
fms_2020_01_24_00	0_51_10_92	sw_149 cc			Stream Search Results					
fms_2020_01_23_2	3_49_15_990	sw_149 cc			Create Search Cancel Request					
fms_2020_01_23_2	3_46_45_434	sw_149 cc								
fms_2020_01_23_23	3_34_08_261	sw_149 oc								
fms_2020_01_23_2		sw_149 cc								
fms_2020_01_23_23		sw_149 cc								
fms_2020_01_23_23		sw_149 cc								
fms_2020_01_23_17		sw_149 cc								
fms_2020_01_23_17		sw_149 oc								
fms_2020_01_23_10	6_12_04_814	sw_149 cc								
					1	🔅 📥 Pca	pData 📥 Log	Data Data Stream Search I	Peaps 000	Ilone Search
3 Del	ete All Searc	hes								

Figure 76-Search Manager Button Stream Clone Search view

### 8.2 CREATING A NEW SEARCH

• To create a new search, click on **CreateSearch** button. This will pop up Create Search dialog.

Sentry Wire	Dashboa	rd 🔺	Policy Setup 👁 Investigator Q Search 🛔 View Metadata	Reports 🌣 Configuration	😮 Help	🕩 Logout
1 Discover	reateSear	ch				
Find Text						
Completed(80) InPro	ıress(1)					
SearchName	NodeNa	me Us				
fms_2020_01_28_09_59_53_2	1 nc_113	COL	Create Search			
fms_2020_01_28_10_04_39_7	7 nc_113	COL	SearchName			
fms_2020_01_28_10_04_39_76			fms 2020 01 28 19 17 22 224			
fms_2020_01_28_09_59_03_13		1000				
fms_2020_01_28_09_59_03_13			BeginTime			
fms_2020_01_10_01_29_56_44 1xcav	4_ nc_113	COL	2020-01-29 00:08:22			
fms_2020_01_10_01_29_56_44	4_ nc_130	COT	EndTime 2020-01-29 00:17-22			
fms 2020 01 28 00 47 17 6	pc 130	004	All fields can be modified			
fms_2020_01_28_00_47_17_66			Search Filter			
fms_2020_01_28_00_46_32_98		_	bpf «bpffitter» logtext «logtext-filter»			
fms 2020 01 28 00 46 32 9			MaxPacketCount			
fms 2020 01 27 19 25 23 7			1000			
fms_2020_01_27_19_25_23_7	nc_130	COT	Stream Search Results			
fms_2020_01_25_19_32_11_28 0i6z2_f11zv	0_ nc_113	COT	Create Search Cancel Request			
fms_2020_01_25_19_32_11_28 0i6z2_fi1zv	0_ nc_130	COT				
fms_RB_fms_2020_01_25_19_ 11_280_cnzxe	32_ nc_113	COI				
fms_RB_fms_2020_01_25_19_ 11_280_cnzxe	82_ nc_130	COI				
fms_2020_01_25_19_32_11_28 0i6z2	0_ nc_113	COT				
fms_2020_01_25_19_32_11_28 0i6z2	0_ nc_130	COT				
🛢 Delete All Se	arches					

Figure 77- Search Create New Search view

• The SearchName field is auto filled but editable.



- Provide a value or change the defaults for the begin time and end time. The begin time field is auto filled to be 4 minutes prior to the current UTC time. The end time field is auto filled to be the current UTC time. The user can change them as needed.
- The Search Filter can be specified as a **bpf** or log**text or both**.
  - Enter a valid bpf packet filter following the keyword **bpf. (For more information on bpf filters refer to Appendix D)**
  - Enter text search string following the keyword **text**
  - If search string has bpf and text strings, **bpf** must precede **text**
  - If neither keyword is entered, the search filter is taken as a bpf string.

The following are examples of some valid search strings:

bpf port 80 text hello

IP host 192.168.0.1

tcp or udp text hello

port 80 text hello

text hello

The following are examples of some **invalid** search strings:

Hello

text hello port 80

blah hello

bpf weqrwr

- The MaxPacketCount field allows the user to specify the packet count as desired for a search within a specific timestamp. To get all packets for a particular timestamp the max packet count must be set to 0.
- Stream Search Results checkbox when checked, allows the user to stream search results to an external interface, for other applications to further analyze the data. Search Results can also be streamed after the search is completed.



SentryWire #D	ashboard	*	Policy Setup 👁 Investigator 🝳 Search 🛔 View Metadata	Reports 🌣 Configuration	Help	🕩 Logou
Discover O Cre	eateSearch					
Find Text						
Completed(80) InProgra	aee/1)					
		_				
SearchName	NodeNam					
ms_2020_01_28_09_59_53_221		COI	Create Search			
ms_2020_01_28_10_04_39_767		COL	SearchName			
ms_2020_01_28_10_04_39_767 ms_2020_01_28_09_59_03_131		COI	fms 2020 01 28 19 17 22 226			
ms 2020 01 28 09 59 03 131 ms 2020 01 28 09 59 03 131		COI	BeginTime			
ms 2020 01 10 01 29 56 444		COI				
1xcav		001	2020-01-29 00:08:22			
ms_2020_01_10_01_29_56_444_ Ixcav	nc_130	cor	EndTime 2020-01-29 00:17:22			
ns 2020 01 28 00 47 17 68	nc_130	COT	Search Filter			
ms_2020_01_28_00_47_17_68	nc_113	cor	top text helio			
ms_2020_01_28_00_46_32_958	nc_113	cos				
ms_2020_01_28_00_46_32_958	nc_130	cor	MaxPacketCount			
ms_2020_01_27_19_25_23_77		COT	0			
ms_2020_01_27_19_25_23_77		COT	Stream Search Results			
ims_2020_01_25_19_32_11_280 Di6z2_f11zv	nc_113	COT	Create Search Cancel Request			
ms_2020_01_25_19_32_11_280_ W6z2_f11zv	nc_130	cor				
ms_RB_fms_2020_01_25_19_32 11_280_cnzxe	_ nc_113	COT				
ms_RB_fms_2020_01_25_19_32 11_280_cnzxe	_ nc_130	cor				
ns_2020_01_25_19_32_11_280_ i6z2	nc_113	cor				
ms_2020_01_25_19_32_11_280 N622	nc_130	COI				
Delete All Sear	ches					

#### Figure 78-Stream Search Results button

- Once all the details are provided, click on Create Search button to create a search.
- The search created can be seen under the Pending searches tab while in progress. A pending or InProgress search can be cancelled at any time.
- Once completed the search appears under the completed search tab for further analysis.
- Note: If no group is selected the search request goes to all groups/nodes in the federation



# 9 VIEW METADATA

The application collects, analyzes, stores and reports on network security log events from each included federated node to help monitor threats, attacks and security breaches. This application engine provides useful information by converting raw events from network and security devices, servers and operating systems, applications, endpoints and more into actionable, investigable intelligence data.

The View Metadata screen presents the user with several menu tabs. Clicking on each tab and selecting the desired node, displays the corresponding details for the selected node.

Q Search Logs		Defended Alerts: nc 113	ts <u>ActiveTriggers</u> ≣Flows @DNS ∦ Files <a> HTTP</a>	Find Text	C Refresh Page & Downloa	d Copy to ClipBoa
C Search Logs	Federated Nodes					
	BostonMA::nc 130		H Prev Page 1	Next Page 🎔		
legin Time		loC	Timestamp	SessionInfo		
020-01-21 14:23:00	NashuaNH::nc_173	32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
	NashuaNH::nc 113	32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
End Time	1103100111.110 110	32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
2020-01-21 14:23:00		32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
og Search Filter [?]		32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
return only events that have the supplied pattern(s)		32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
tax Rows		32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
2000		32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:17	192.168.15.6	7:53896 TCP 192.168.16.11 445	
Q Search Logs		32 File Found over SMB	2020-01-21 19:17:16	192.168.16.1	1:445 TCP 192.168.15.67 53986	
		32 File Found over SMB	2020-01-21 19:17:16	192.168.15.6	7:53986 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.16.1	1:445 TCP 192.168.15.64 57607	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	
		32 File Found over SMB	2020-01-21 19:17:14	192.168.15.6	4:57607 TCP 192.168.16.11 445	

Figure 79-View Metadata screen view

• The "Find Text" option allows the user to enter a desired string to specify the type of event or alert message the user is interested in. This will display the messages containing the specified search text string only. If there is text entered in "Find Text" box, the text must be cleared for all the data to be displayed.



Q Search Logs		HTTP: nc_113		C	Find Text		
Contra Logo	Federated Nodes				appie	Copy to ClipBoard	Carl Refresh Page
	BostonMA::nc_130			D 0			
Begin Time	NashuaNH::nc 173			Page Si	ze 500 •	« Prev 1 2 3 Next »	
2020-01-21 18:55:47	NashudiNHIIC_TTS	-					
nd Time	NashuaNH::nc_113	TimeStamp	SessionInfo	CommunityID	HostName	URL	UserAgent
		2020-01-21 19:19:57	172.16.9.171:2781 TCP 17.254.0.91:80	1:GrMyky4+Uzzm	www.apple.com	/macpro/styles/macpro.css	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
2020-01-21 19:25:47	1	2020-01-21 19:19:57	172.16.9.171:2781 TCP 17.254.0.91:80	1:GrMyky4+Uzzm	www.apple.com	/global/styles/ie.css	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
og Search Filter [?]		2020-01-21 19:19:57	172.16.9.171:2781 TCP 17.254.0.91:80	1:GrMyky4+Uzzm	www.apple.com	/global/styles/skins/defaultblack.css	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
return only events that have the supplied pattern(s)	1	2020-01-21 19:19:59	192.168.15.71:60575 TCP 199.73.44.40:80	1:Umcvq5rQlzjUPi	library.ashford.edu	/images/icons/maginfyingglass100.png	Mozilla/5.0 (Windows NT 6.1; WOW64) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
lax Rows		2020-01-21 19:19:59	192.168.15.71:60574 TCP 199.73.44.40:80	1:jyrj0Pj+xU6DQvE	. library.ashford.edu	/images/icons/mortar-board-coloredin100.png	Mozilla/5.0 (Windows NT 6.1; WOW84) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
2000 🌲		2020-01-21 19:20:00	172.16.9.171:3079 TCP 17.254.0.91:80	1:QDFGSQn/U1qZ	www.apple.com	/euro/main/css/globalprint.css	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
		2020-01-21 19:20:04	172.16.9.171:2785 TCP 84.53.136.152:80	1:RNNZN8uXFR7c	images.apple.com	/macpro/images/header_macpro20060807.jpg	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Q Search Logs		2020-01-21 19:20:04	192.168.15.71:60573 TCP 199.73.44.40:80	1:uQpt0g7nEtb931	library.ashford.edu	/images/icons/quickanswers-person100.png	Mozilla/5.0 (Windows NT 6.1; WOW64) Apple/WebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
	_	2020-01-21 19:20:07	172.16.9.171:2596 TCP 17.254.0.91:80	1:eZcpRpO7hew0	wdirect.apple.com	/main/js/browserdetect.js	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
		2020-01-21 19:20:07	172.16.9.171:2596 TCP 17.254.0.91:80	1:eZcpRpO7hew0	wdirect.apple.com	/main/js/randinator.js	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
		2020-01-21 19:20:07	172.16.9.171:2596 TCP 17.254.0.91:80	1:eZcpRpO7hew0	wdirect.apple.com	/home/wdirect/ticker.js	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
		2020-01-21 19:20:14	172.16.9.171:2593 TCP 17.254.0.91:80	1:Pr/c7t3Yom34VR	www.apple.com	1	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
		2020-01-21 19:20:14	172.16.9.171:2593 TCP 17.254.0.91:80	1:Pr/c7l3Yom34VR	www.apple.com	/main/css/global.css	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
		2020-01-21 19:20:14	172.16.9.171:2593 TCP 17.254.0.91:80	1:Pr/c7t3Yom34VR	www.apple.com	/home/2007/ticker.rss	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
		2020-01-21 19:20:18	192.168.15.71:61034 TCP 199.73.44.216:80	1:VV1p9AYpG+VS	eds.a.ebscohost.c library.ashford.edu	/eds/detail/detail?sid=45162e23-36f2-42aa-8247- 93291e2a7ba1%40sessionmgr4006&vid=6&hid=4	Mozilla/5.0 (Windows NT 6.1; WOW64) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
		2020-01-21 19:20:24	192.168.15.71:60679 TCP 199.73.44.216:80	1:DSF98xzjVQ1zJ	eds.a.ebscohost.c library.ashford.edu	/eds/Search/PerformSearch?sid=45162e23-36f2- 42aa-8247-93291e2a7ba1@sessionmgr4006&vid=1	Moziila/5.0 (Windows NT 6.1; WOW64) AppleWebKii/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
		2020-01-21 19:20:31	192.168.15.71:60570 TCP 199.73.44.40:80	1:jONHrHh9c6Mph	library.ashford.edu	/Styles/tooltipster-light.css	Mozilla/5.0 (Windows NT 6.1; WOW84) Apple WebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36

Figure 80-View Metadata Find Text Option view

- The "Copy to Clipboard" option allows the user to copy the entire event/message display to any location or application allowing the user to share the information via email for reporting or recording purpose.
- The "**Download**" option allows the user to download data to help record and monitor both existing and new events, threats, alerts and rules to maintain uninterrupted log source data collection and storage. This can be done by clicking the download button on the top allowing the user to download the data in a .csv format.



Q Search Logs		Files: nc_130		Find Text	2 Refresh Page 🛓 Download	Copy to Clip
	Federated Nodes					
	BostonMA::nc_130		H Prev Page 1	Next Page 🎔		
egin Time	No.1. 191	loC	TimeStamp	SessionInfo	Size(bytes)	
020-01-22 18:03:00	NashuaNH::nc_173	/4/forum.php	2020-01-22 22:59:57	92.53.107.93:80 TCP 10.4.23.101 49	290 12	
	NashuaNH::nc_113	/4/forum.php	2020-01-22 22:59:57	10.4.23.101:49290 TCP 92.53.107.9	3 80 120	
nd Time		/4/forum.php	2020-01-22 22:59:57	92.53.107.93:80 TCP 10.4.23.101 49	469 12	
020-01-22 18:03:00		/4/forum.php	2020-01-22 22:59:57	10.4.23.101:49469 TCP 92.53.107.9	3 80 120	
g Search Filter [?]		/fd/ls/lsp.aspx	2020-01-22 22:59:5 AutoSave	回り、 ペーマ fileevents	_nc_13 🔎 🙀 🖬	- 0
	_	/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR0JBRnBp/14Jg/Xj4aa6BlKIQ	2020-01-22 22:59:5		382	
turn only events that have the supplied pattern(s)		data		ome Insert Draw Page Layout	Formulas Data Review View	Help
-		/consumer\$20licensing\$20technologies_15.0_symalllanguages_livetri.zip	2020-01-22 22:59:5			
IX Rows		/1476723932jtun_irev161016068.7z	2020-01-22 22:59:5 A1	• $X \checkmark f_x$ timestam		
100		/c.gif	2020-01-22 22:59:5	B C D	E F G H	L E L
	_	/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBTMbSIc9rRVLC+HkV9a/vDh7s	2020-01-22 22:59:5 1 timestar	mp message session eventtype flo	wid app proto FileName FilePath	FileSize ioc
Q Search Logs		/qsml.aspx	2020-01-22 22:59:5 2 ########		15E+15 http /4/forum.php	12
		/c.gif	2020-01-22 22:59:5 3 #######	### /4/forum.p 10.4.23.10:fileinfo 1	15E+15 http /4/forum.php	120
		/c.gif	2020-01-22 22:59:5 4 ########	### /4/forum.p 92.53.107.fileinfo 1	94E+15 http /4/forum.php	12
		/norton\$202015\$20core\$20virus\$20definitions\$20x64_microdefsb.error_sy	2020-01-22 22:59:5 5 ########	### /4/forum.p 10.4.23.10:fileinfo 1	94E+15 http /4/forum.php	120
		/fd/ls/lsp.aspx	2020-01-22 22:59:5 6 ########	### /fd/ls/lsp.a 192.168.15 fileinfo 2	08E+15 http /fd/ls/lsp.aspx	452
		/fd/ls/lsp.aspx	2020-01-22 22:59:5 7 #######	### /MFEwTzBI23.4.59.27:fileinfo 1	.85E+15 http /MFEwTzBNMEswSTA	J 1595
		/fd/ls/lsp.aspx		### /consumer: 23.78.220.4 fileinfo 1	33E+15 http /consumer\$20licensing	£ 16
		/vast XML 1.0 document, ASCII text, with very long lines, with no line		### /14767239 23.78.220.+fileinfo 9	26E+14 http /1476723932jtun_irev	v 3253
		terminators	10 #######	### /c.gif 192.168.15 fileinfo 1	13E+15 http /c.gif	137
			11 #######	### /MEOwSzBJ 184.25.251 fileinfo	5.4E+14 http /MEOwSzBJMEcwRTAJ	2116
	1		12 #######	### /qsml.aspx 13.107.5.8(fileinfo 2	13E+15 http /qsml.aspx	497
			12 *******	r## /qsmi.aspx 15.107.5.6(memo 2	15C+15 nup /dsmi.aspx	497

Figure 81-View Metadata Download Button view

- The "**Refresh**" option allows the user to retrieve the most recent event data from the server for display. Note: This is the only way to bring in the most recent event data associated with the tab option selected. This retrieved data remains current as the user navigates through different option tabs allowing the user to investigate multiple tabs at a time. In order to view the current event data the user must click refresh for each tab option within that tab.
- The "**Page Size**" option allows the user to choose the number of rows the user would like to see in one page. By default this count is 500. When the user selects a different display count the number of pages change accordingly. User can easily navigate through pages by scrolling through previous or next page option or clicking on the desired page number.
- The "Search Log" option allows the user to display alerts and events within the specified range of time. It also allows the user to specify a log search filter for a more specific search within the logs. User needs to click refresh again to see the current events.



Q Search Logs		HTTP: nc_130		c	Find Text			
	Federated Nodes					Copy to ClipBoard	oad C Refresh Page	
Begin Time	BostonMA::nc_130			Page Size	500 v «	Prev 1 2 3 4 5	Next »	
2020-01-23 16:50:37	NashuaNH::nc_173			, ago oizo	500 •		NOAL #	
	NashuaNH::nc_113	TimeStamp	SessionInfo	CommunityID	HostName	URL	UserAgent	
End Time 2020-01-23 17:20:37		-	192.168.15.64:56822 TCP 192.168.16.11:1616	1:41eL2kSU5gwos		/api/UserNotifications? s=947453140BFC795CC3059F6DD11BEE9A994F		
Log Search Filter [?]		2020-01-23 17:13:59	192.168.15.64:56896 TCP 192.168.16.11:1616	1:EpTwuMZV1Zb9	192.168.16.11	s=54745314057C795CC305976DD11BE548594F /api/UserNotifications? s=E55367FF3BD001FAC9E8FDB7730E683A48D		
return only events that have the supplied pattern(s)		2020-01-23 17:14:00	192.168.15.93:64619 TCP 162.208.22.39:80	1:u2K1+8wtuq+JR	geo-um.btrll.com	/v1/map/fff6bcfb8b87c020/a5604f1479f20b6ebee2	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	
Max Rows		2020-01-23 17:14:00	192.168.15.93:84614 TCP 162.208.22.34:80	1:/2eT6zYUYCvJ6I	vast.bp3856327.btr	/vast/3856327? n=1476723622780&br_w=0&br_h=0&br_pageurl=	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	
2000		2020-01-23 17:14:00	192.168.15.93:64657 TCP 205.185.216.42:80	1:F14aXDKUviNS/	ad.lkqd.net	/vpaid/vpaid.swf	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	
Q Search Logs		2020-01-23 17:14:00	192.168.15.93:64567 TCP 23.110.194.130:80	1:2vO/20mNxmoW	. static.rlicil.com	/vpaid21.swf	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	
	_	2020-01-23 17:14:01	192.168.15.55:52762 TCP 184.30.192.238:80	1:wOSWLBTwXcT	www.microsoft.com	/pkiops/crl/Microsoft%20Windows%20Verification	Microsoft-CryptoAPI/6.1	
		2020-01-23 17:14:01	192.168.15.59:56103 TCP 131.253.40.50:80	1:mQcl/wDBzcYICr	. c.bing.com	/c.gif?Red3=MSNLI_pd&rid=86585106-dca7-43c4- 9d8d-6bb6a15c0a26&ing=en- us&dgk=tmx.pc.ms.ie10plus&imd=0&pn=startpage	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	
		2020-01-23 17:14:01	192.168.15.59.56103 TCP 131.253.40.50:80	1:mQcl/wDBzcYICr	. c.bing.com	/c.gif?aol_uid=TA229437fa-84fd-11e6-af56- 00163e82216c&uac_muid=1ee7f863bcfc62cc272d	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	
		2020-01-23 17:14:00	192.168.15.55:51926 TCP 8.18.45.65:80	1:UqDT09a7+wpc	t.mplxtms.com	/lags? callback=jQuery17207764588411158433_1476723 us%27%22%2C%22referrer%22%3A%22%22%2 coa5-boc0-3579- 64fb387656b%22%7D&=1476723549644	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	
		2020-01-23 17:14:00	192.168.15.93:64298 TCP	1:ImQMqsQu9oGD	. 192.168.16.11	/api/UserNotifications?		

Figure 82-View Metadata Search Logs Function view

## 9.1 DEFENDED ALERTS

The FM displays alerts generated due to a rule for each node in the federation, only if the alert's source or destinationIPaddress is a defended asset **AND** the alert's source or destination port is a defended service.

**Note**: The defended asset and defended service that are assigned by the "Policy Setup" tab from FM are global and apply to all nodes. (For more information refer to section 4.1 and 4.2)



Search Logs		Defended Alerts: nc_113		Find Text CRefresh	Page 📥 Download 🖪 Copy to Clip
	BostonMA::nc 130		M Prev Page	1 Next Page >>	
in Time		loC	Timestamp	SessionInfo	
0-01-23 13:35:00	NashuaNH::nc 113	32 File Found over SMB	2020-01-23 18:31:50	192.168.15.64:57607 TCP 192.1	68.16.11 445 Click to
		32 File Found over SMB	2020-01-23 18:31:50	192.168.15.64:57607 TCP 192.1	68.16.11 445 investigate
lme		3303 [192.168.16.11 is in watchlist]	2020-01-23 18:31:50	192.168.16.11:445 TCP 192.168.	15.93 49223
01-23 13:35:00		3303 [192.168.16.11 is in watchlist]	2020-01-23 18:31:49	192.168.16.11:445 TCP 192.168.	15.67 53986
	-	32 File Found over SMB	2020-01-23 18:31:49	192.168.15.55:52574 TCP 192.1	
earch Filter [?]		32 File Found over SMB	2020-01-23 18:31:49	192.168.15.55:52574 TCP 192.1	68.16.11 445
only events that have the supplied pattern(s)		32 File Found over SMB	2020-01-23 18:31:49	192.168.15.55:52574 TCP 192.1	68.16.11 445
		32 File Found over SMB	2020-01-23 18:31:49	192.168.15.55:52574 TCP 192.1	68.16.11 445
ows		32 File Found over SMB	2020-01-23 18:31:49	192.168.15.55:52574 TCP 192.1	68.16.11 445
\$		32 File Found over SMB	2020-01-23 18:31:49	192.168.15.55:52574 TCP 192.1	68.16.11 445
		32 File Found over SMB	at Daubbarred & Da	toircy Setup	Reports O Configuration O Help
Q Search Logs		32 File Found over SMB		odeName.nc_113 NodelP_10.91.170.113	
		32 File Found over SMB			Investigator Di
		32 File Found over SMB	Pederated Nodes		c
		32 File Found over SMB	DesterVer rc, 150	9 New Save Open Share Inspect	
		32 File Found over SMB	0		ast 1 week Show dates C Re
		32 File Found over SMB	10	Add filter	
		32 File Found over SMB	80		9,404 hits
		32 File Found over SMB	÷	Selected fields Jan 16, 2020 @ 13:36:31:284 - Jan 22	2000 ( 1000 Julio - 1000 -
		32 File Found over SMB	8		
		32 File Found over SMB	6	Fapular 2 (0.00)	
		32 File Found over SMB		1 Jype 10,000	
		32 File Found over SMB		2000-01-17 00:00 2020-01-18 00:00 2020-01-18 00:00	2020-01-20-00-00 2020-01-21-00-00 2020-01-22-00-03 2022-01-23-0 mestamp per 3 hours
		32 File Found over SMB		t community,id	
		32 File Found over SMB		e fosja	2.168.15.00 timestamp: Jan 22, 2020 # 15:55:56.888
				1 proto Tiov_541 1,761,571,968,942,991	
				1 Jd 00_242 /50074260/20050/448876_56/	1579740956175354383_15797409570245522.pcap.cz_ignore gm: alert src.port: 445 dest.port: 49.223 proto: TCP

Figure 83-View Metadata Defended Alerts view

• Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

### 9.2 SUSPDOMAINS

The SuspDomains alerts are generated when a domain from DNS event is one of the suspicious domains that have been uploaded via the Policy  $\rightarrow$  Augmentation  $\rightarrow$  Suspicious Domains list. Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.



-	Federated Nodes			Find Text CRefresh Page	Download Copy to ClipH
	BostonMA::nc 130		H Prev Page 1	Next Page	
Time	SSSIGHTER LINE TOO	loC		Tir Click to investigate Sessioninfo	
01-23 13:58:00	NashuaNH::nc_113	us.pool.ntp.org			UDP 192.168.15.251 49153
		us.pool.ntp.org		2020-01-23 15:59:08	9153 UDP 192.168.16.1 53
lime		us.pool.ntp.org		2020-01-23 15:59:08 192.168.16.1:53 L	UDP 192.168.15.251 49153
01-23 13:58:00		us.pool.ntp.org		2020-01-23 15:59:08 192.168.16.1:53 L	UDP 192.168.15.251 49153
		us.pool.ntp.org		2020-01-23 15:59:08 192.168.15.251:49	9153 UDP 192.168.16.1 53
earch Filter [?]		us.pool.ntp.org		2020-01-23 15:59:08 192.168.15.251:49	9153 UDP 192.168.16.1 53
only events that have the supplied pattern(s)		us.pool.ntp.org		2020-01-23 15:59:08 192.168.15.251:49	9153 UDP 192.168.16.1 53
		us.pool.ntp.org	ADastboard -	≮ Policy Setup ● Investigator Q. Search	
Rows		us.pool.ntp.org	O Deate Search	KodeKaner nc_532 NodeP; 93 P1 (70:133	Investigation
\$		us.pool.ntp.org	Federated Notes	🗶 🔲 Discover	0
		us.pool.ntp.org	Burnette, w_03	New Save Open Share Inspect	
Q Search Logs		us.pool.ntp.org	Neuhadot ec./13	sec.jp: 19276815.251 and sec.port/6953 and desc.jp:192768351 and dest.p KOL 1 ~ Last 1 wee	ek Show Galles C
		us.pool.ntp.org		S - Add filter	
		us.pool.ntp.org		investigator,* (change) 0 248,369 h	
		us.pool.ntp.org		30 Jan 18, 2020 (p 13:59:15:384 - Jan 23, 2020 (p	/12:59:15:384 - Auto V
		us.pool.ntp.org		C Filter by type	
		us.pool.ntp.org		Belanded fields B 1000	
		us.pool.ntp.org		2 Available fields	
		us.pool.ntp.org			10 2327-0-17-01404 2020-0-12240-0 2020-0-15-0540
		to and she are		C Joon Inselan per	3 hours
				3         • 100/2         • 400/2         • 10	1.1 Linealamp. Jan 23, 2020 9 10.59:55.033
				A r prite Tile, 12, 228, 112, 16	

Figure 84-View Metadata SuspDomains Function view

# 9.3 SUSPSIG(JA3)ALERTS

The SuspSig(JA3) alerts are generated when JA3 hash of the TLS event matches with one of the JA3 hash values uploaded via the Policy  $\rightarrow$  Augmentation  $\rightarrow$  Suspicious TLS/SSL Signatures list.

0.0.1.7		SuspSig(JA3) Alerts:nc_130				Fine	i Text 🛛 📿 Refresh Page 📥 Dov	wnload Copy to ClipBo
<b>Q</b> Search Logs	Federated Nodes	ouspoig(sho) Histis.ite_100				1 110	Kenesh rage	Поац Сору ю Спрво
	BostonMA::nc 130			H Prev Page	1	Next Page	•	
egin Time		IoC(JA3)	TimeStamp	SessionInfo		Subject,IssuerDN,Versio	n	Serial, Fingerprint
020-01-23 14:09:00	NashuaNH::nc_113	20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:55	192.168.15.71:61002 TCP 199.73.44.90.4	43	UNDETERMINED		
		20dd18bdd3209ea718989030a6/93364	2020-01-23 19:05:54	192.168.15.71:60962 TCP 199.73.44.65:4	Click t	RMINED		
d Time		20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:54	192.168.15.71:61003 TCP 199.73.44.90:4	43 investig	ate		
020-01-23 14:09:00	1	93d056782d649deb51cda44ecb714bb0	2020-01-23 19:05:53	192.168.15.71:60675 TCP 54.67.32.43:44	3	UNDETERMINED		
20-01-23 14:08:00		20dd18bdd3209ea718989030a6f93384	2020-01-23 19:05:52	192.168.15.71:60324 TCP 72.21.81.253:4	43	UNDETERMINED		
g Search Filter [?]		20dd18bdd3209ea718989030a6i93364	2020-01-23 19:05:52	192.168.15.71:60322 TCP 72.21.81.253:4	43	UNDETERMINED		
turn only events that have the supplied pattern(s)	1	20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:52	192.168.15.71:60453 TCP 104.239.223.12	2:443	TLS 1.2		
		20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:51	192.168.15.71:60323 TCP 72.21.81.253:4			anta Monica, O=EdgeCast Networks, Inc., OU=Security,	02:44:04:FB:04:49:24:CF:6.
x Rows					The second se	CN=edgecasterin net C=U loy Setup	S. O=DigiCert Inc. CN=DigiCert SHA2 Secure Server CA TI	Reports O Configuration O Help
000		20dd18bdd3209ea718989030a6193364	2020-01-23 19:05:51	192.168.15.71:60382 TCP 19		Norme nr. 131 KodelP. 18.14.72.130	B VIEW INCLUDIED	Investigator
Ť		20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:50	192.168.15.71:60321 TCP 72		Discover		and the second se
0.0.11		20dd18bdd3209ea718989030a6f93384	2020-01-23 19:05:39	192.168.15.71:61001 TCP 19	•			0
Q Search Logs		20dd18bdd3209ea718989030a6/93384	2020-01-23 19:05:39	192.168.15.71:61001 TCP 19 Becommerce 10 192.168.15.71:61004 TCP 19 Recommerce 10	0	New Save Open Share Inspe		
	-	20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:39	192.168.15.71.61005 TCP 19	0		, port/51002 and dest, p:199.72.44.90 and dest, p KOL 🔐 🗸 Last 1 week	Show dates O
		20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:38	192.168.15.71.60490 TCP 10	12	🗇 - + Add filter		
		20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:38	192.168.15.71.60490 TCP 10	85	investigator,* (change)	7,307 hits Jan 16, 2020 @ 14:09:55.652 - Jan 23, 2020 @ 14:09:5	5.652 - Ann V
		93d056782d649deb51cda44ecb714bb0	2020-01-23 19:05:38	192.168.15.71:60563 TCP 17	±	Q Search field names		
		20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:35	192.168.15.71:60447 TCP 10	8	😁 Filter by type 🛛 🔕	500 400	بإنبالييل. إن
		20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:37	192.168.15.71:60501 TCP 10	8	Selected fields	200	
		20dd18bdd3209ea718989030a6f93364	2020-01-23 19:05:37	192.168.15.71.60582 TCP 19	8	Aussiadale fields		
		93rl056782rl649rleh51crtad.dech71dbb0	2020-01-23 19:05:37	192.168.15.71.60532 TCP 18	0	Popular		120-31-21 (20:0) 2120-07-22 10:00 2020-07-23 00:00
			2020000223 18 02124			<ul> <li>Japa</li> <li>Anna A</li> </ul>	timestamp per 3 hours	
					3		Jan 22, 2020 9 14-25-15-011 sre.jp. 192,108,15,71 dost.jp. 109,72.44.90 tipe	stamp: Jan 23, 2028 8 14 85 55 (4)
						1.31	flow_5d: 1.155.455.795.590.597 event_type: tis is	p_nep_bd: vs virtual retwork src.port: 61.002
						1.3000	<pre>dead.port: 443 proto: 70* 81a.ant; and authors.e t1a.1a0.hosh: 20001004330100100710000000010304 81</pre>	

Figure 85- View Metadata SuspSig(JA3) Alerts view



# 9.4 MALWARE

The Malware alerts are generated when a MD5 value of an object produced by a search matches one of the MD5 values uploaded via the Policy $\rightarrow$  Augmentation $\rightarrow$ Malware list.

Clicking on the hyperlinked IoC pivots to the investigator screen that shows the matching MD5 information for further analysis.

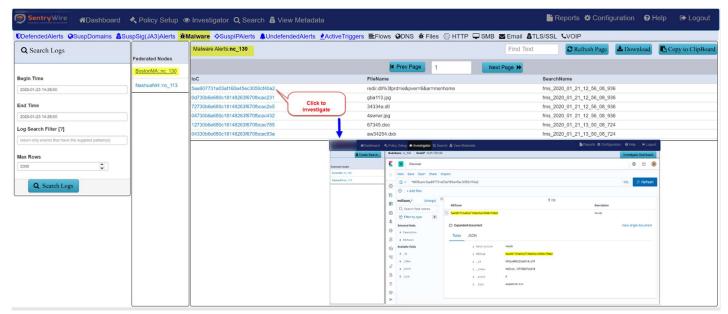


Figure 86-View Metadata Malware Alerts view

# 9.5 SUSPIPALERTS

The SuspIP alerts are generated when an IP address matches with one of the suspicious IP that have been uploaded via the Policy  $\rightarrow$  Augmentation  $\rightarrow$  Suspicious IPAddresses list.



#### User Guide January 30, 2020

Search Logs		SuspIP Alerts:nc_130		Find Text 2 Refresh Page	Download 🖪 Copy to Cli
	Federated Nodes				
	BostonMA::nc 130		K Prev Page 1	Next Page >>	
in Time		loC	Timestamp	Sessioninfo	
0-01-23 15:11:00	NashuaNH::nc_113	192.168.15.79	2020-01-23 20:08:53	192.168.15.79:65478 TCP 192.168.16.11:1616	
		192.168.15.79	2020-01-23 20:08:53	192.168.15.79:65490 TCP 192.168.16.11:1616	Click to
Time		192.168.15.79	2020-01-23 20:08:53	192.168.15.79:65332 TCP 192.168.16.11:1616	investigate
0-01-23 15:11:00		192.168.15.79	2020-01-23 20:08:53	192.168.16.11:1616 TCP 192.168.15.79:65511	
Search Filter [?]		6.1.1.10	2020-01-23 20:08:53	6.1.1.10:137 TCP 198.19.23.240:208	
		192.168.15.79	2020-01-23 20:08:53	192.168.15.79.65484 TCP 192.168.16.11:1616	
n only events that have the supplied pattern(s)		192.168.15.79	2020-01-23.20:08:53	102 168 16 11-1616 TCD 102 168 15 70-00376	
_		6.1.1.10	2020-01-	< Pricy Setup Setup Investigator Q, Search & View Metadata	Reports O Configuration O Help
Rows		192.168.15.79	2020-01- O Create Second	Kodelkame ng_130 NodelP 10 91 170 130	investigat
¢		6.1.1.10	2020-01- Reduced Notes	K 🔲 Discover	0
	192.168.15.79	2020-01-	New Save Open Share Inspect		
Q Search Logs		192.168.15.79	2020-01-	Image: Strong to 192,108,15,79 and strong port/sil5478 and dest, jp:192,198,16,11 and dest, p         KOL         Image: Strong to 192,108,15,79 and strong port/sil5478 and dest, jp:192,198,16,11 and dest, p	Show dates
		6.1.1.10	2020-01-	⊘ + Add filter	
		192.168.15.79	2020-01-	investigator,* (change) 0 Jan 10, 2020 (s) 15/11/27.396 - Jan 22, 2020 (s) 15/11/27.576 - Jan 22, 2020 (s) 15/11/2700 (s) 15/11/270 (s) 15/11/270 (s) 15/11/27	1127396 - 440
		192.168.15.79	2020-01-	Q Search field names     G Fitter by type     G	
		192.168.15.79	2020-01-	Started Balls I	
		192.168.15.79	2020-01-	S v.source S	
		6.1.1.10	2020-01-	E Available Fairds	
		6.1.1.10	2020-01-:	Popular     200-0-1/0000 200-0-10000 200-0-10000 200-0-10000     foreture per 3hours     foreture per 3hours	2022-01-21 20:00 2025-01-22 00:03 2025-01-22 00:00
		C 4 4 40	2020.04	C r comunitadi Timeassess	
					Elementary: Jan 23, 2020 0 11:17:10.104 02371005_1157070624200075_posp.cz.lpnow pow_ont: k arcjart: 05,475_deat_part: 1,516_prode: 10*

Figure 87-View Metadata SuspIPAlerts view

## 9.6 UNDEFENDEDALERTS

These alerts are generated when the alert's source or destinationIPaddress is **NOT** a defended asset **OR** the alert's source or destination port is **NOT** a defended service.

Pederated       Begin Time       2020-01-23 14.51.00       End Time       2020-01-23 14.51.00       Log Search Filter [?]       return only events that have the supplied pattern(s)       Max Rows       2020       Q. Search Logs	Inc., 130 Inc., 130 32 File Found over SMB 32 File Found over SMB	Imestamp         7           Timestamp         2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34           2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34           2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34           2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34           2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34           2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34         2020-01-23 19:47:34	Click to           192.168.15.55.51729 TCP 192.168.16.7.445           192.168.15.55.51729 TCP 192.168.16.7.445           192.168.15.55.51729 TCP 192.168.15.7.445           192.168.15.55.51729 TCP 192.168.15.55.51729           192.168.15.55.51729 TCP 192.168.15.75.51729           192.168.15.56.53428 TCP 192.168.15.7445
legin Time NashuaNi 2005-01-23 14:51:00 2005-01-23 14:51:00 og Gearch Filter [7] return only events that have the supplied pattern(s) hax Rows 2000	Inc         Inc           32 File Found over SMB         32 File Found over SMB           32 File Found over SMB         32 File Found over SMB           32 File Found over SMB         32 File Found over SMB           32 File Found over SMB         32 File Found over SMB           32 File Found over SMB         32 File Found over SMB           32 File Found over SMB         32 File Found over SMB           32 File Found over SMB         3303 [192.168.16.11 is in watchlist]           32 File Found over SMB         3203 [192.168.16.11 is in watchlist]	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.15.35.51729 TCP 192.168.16.7.445 192.168.16.35.51729 TCP 192.168.15.55.51729 192.168.15.55.51729 TCP 192.168.15.7.445 192.168.15.55.51729 TCP 192.168.15.55.51729 192.168.15.55.51729 TCP 192.168.15.7.445 192.168.15.55.51729 TCP 192.168.15.7.445 192.168.15.55.51729 TCP 192.168.15.55.51729 192.168.16.7.445 TCP 192.168.15.55.51729 192.168.16.7.445 TCP 192.168.15.55.51729 192.168.15.26.53248 TCP 192.168.15.55.51729 192.168.15.26.53248 TCP 192.168.15.7.445 192.168.15.26.53428 TCP 192.168.16.7.445
00200-01-23 54:81:00           nd Time           00200-01-23 54:81:00           0rg Search Filter [7]           etum only events that have the supplied pattern(s)           ax Rows           0000	32 File Found over SMB           32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.16.7.445 TCP 192.168.15.56 51729         Click to           192.168.15.55.1729 TCP 192.168.16.7.445         Investigate           192.168.15.55.51729 TCP 192.168.15.55 51729         Investigate           192.168.15.745         Investigate
20-01-23 14:01:00  g Search Filter [?] Immonly events that have the supplied pattern(s)  x Rows  x00	32 File Found over SMB 32 File Found over SMB 3303 [192.168.16.1 is in watchlist] 32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.15.55-51729 TCP 192.168.16.7 445 192.168.16.7.445 TCP 192.168.16.5 65 61729 192.168.16.55.51729 TCP 192.168.16.7 445 192.168.16.55.51729 TCP 192.168.16.7 445 192.168.16.7.445 TCP 192.168.16.5 65 1729 192.168.15.55.51729 TCP 192.168.16.5 445 192.168.16.7.445 TCP 192.168.15.65 63729 192.168.16.7.445 TCP 192.168.15.65 63729 192.168.15.56.51729 TCP 192.168.15.65 63729 192.168.15.68.53428 TCP 192.168.15.65 63051 192.168.15.68.53428 TCP 192.168.16.7 445
20-01-23 14:01:00  g Search Filter [?] Immonly events that have the supplied pattern(s)  x Rows  x00	32 File Found over SMB 32 File Found over SMB 32 File Found over SMB 32 File Found over SMB 32 File Found over SMB 33 File Found over SMB 330 2192 - 188.16.11 is in watchlist] 32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.166.15.35317291CP192.168.167.445 192.168.167.445 192.168.167.445 192.168.15.55.51729TCP192.168.155.551729 192.168.15.55.51729TCP192.168.15.551729 192.168.15.55.51729TCP192.168.15.551729 192.168.15.55.51729TCP192.168.15.551729 192.168.15.55.51729 192.168.15.65.553129 192.168.15.66.53428TCP192.168.15.551729 192.168.15.66.53428TCP192.168.15.7445
g Search Filter [7] Ann only events that have the supplied patient(s) ix Rows 000	32 File Found over SMB 32 File Found over SMB 32 File Found over SMB 32 File Found over SMB 33 File Found over SMB 3300 [192 - [88.16.1 is in watchist] 32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.15.255.1729 TCP 192.168.15.55 51729 192.168.15.55.51729 TCP 192.168.16.7445 192.168.16.555.1729 TCP 192.168.16.7445 192.168.16.7:445 TCP 192.168.16.56 51729 192.168.15.55.51729 TCP 192.168.16.7445 192.168.16.7445 TCP 192.168.15.56 51729 192.168.15.11:1616 TCP 192.168.15.56 50051 192.168.15.68.53428 TCP 192.168.16.7445
num only events that have the supplied pattern(s) ix Rows 000	32 File Found over SMB 32 File Found over SMB 33 File Found over SMB 32 File Found over SMB 3303 [192.168.16.11 is in watchlist] 32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.15.35.51729 TCP 192.168.16.7.445 192.168.16.7.445 TCP 192.168.15.55 51729 192.168.15.55.51729 TCP 192.168.15.55 51729 192.168.16.7.445 TCP 192.168.15.55 51729 192.168.15.116161 TCP 192.168.15.65 60051 192.168.15.68.53428 TCP 192.168.16.7.445
tum only events that have the supplied pattern(s) x Rows 000	32 File Found over SMB 32 File Found over SMB 32 File Found over SMB 3303 [192.168.16.1 is in watchlist] 32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.16.7.445 TCP 192.168.15.55 51729 192.168.15.55.51729 TCP 192.168.15.745 192.168.16.7.445 TCP 192.168.15.55 51729 192.168.16.17.445 TCP 192.168.16.56 50051 192.168.15.68.53428 TCP 192.168.16.7.445
x Rows	32 File Found over SMB 32 File Found over SMB 3303 [192.168.16.11 is in watchlist] 32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.15.55.51729 TCP 192.168.16.7 445 192.168.16.7.445 TCP 192.168.15.55 51729 192.168.16.161 FC P1 92.168.165 50515 192.168.15.66.53428 TCP 192.168.16.7 445
00	32 File Found over SMB 3303 [192.168.16.11 is in watchlist] 32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.16.7.445 TCP 192.168.15.55 51729 192.168.16.11.1616 TCP 192.168.15.60 50051 192.168.15.86.53428 TCP 192.168.16.7.445
	3303 [192.168.16.11 is in watchlist] 32 File Found over SMB	2020-01-23 19:47:34 2020-01-23 19:47:34	192.168.16.11:1616 TCP 192.168.15.60 50051 192.168.15.68.53428 TCP 192.168.16.7 445
	32 File Found over SMB	2020-01-23 19:47:34	192.168.15.68.53428 TCP 192.168.16.7 445
Q. Search Logs			
Q Search Logs		2020 01 02 17 2 2	
	32 File Found over SMB	2020-01-23 19:47:34	192 168 15 68 53428 TCP 192 168 16 7 445
	32 File Found over SMB		Policy Setup 👁 Investigator Q, Search & View Methodata 🔹 🖥 Reports O Configuration O Help 🗇
	32 File Found over SMB	O Create Search	KodelProg 10 KodelProg 10 (2017/2017)
	32 File Found over SMB	Pederahed Modes	💈 Discover 🗘
	3303 [192.168.16.11 is in watchlist]		() New Save Open State Import
	32 File Found over SMB	hersehilts,10	src, jp: 192.168.15.55 and src, port.51729 and dest, jp: 192.168.15.7 and dest, jp: KD. Rv Last 1 week Show dates C Refre
	32 File Found over SMB		C Add fiter
	32 File Found over SMB		Investigator,*          0         511 hits           Selected fields         Jan 16, 2020 (p 14:54:018.096 - Jan 23, 2022 (p 14:5
	32 File Found over SMB	:	
	32 File Found over SMB	:	Available fields 0 200
	32 File Found over SMB	-	C Provier B to-
	32 File Found over SMB		In seriestion         0           10000 en U della         2000 e
	32 File Found over SMB		E # directory Envertempor 3 Nors
	32 File Found over SMB		U I COMUNEX,IS TimeSearce
	32 File Found over SMB		G 3 Jan 22, 2425 6 19:35:12,345 erc.102 192.080 15 37 Jan 22, 2126 6 19:35:12,345
	32 File Found over SMB	-	1.8     10.00     10.
	32 File Found over SMB		Op         page.com          page.com         p

Figure 88-View Metadata Undefended Alerts view



## 9.7 ACTIVE TRIGGERS

The Active triggers are generated when a user specified BPF filter, through Policy Setup $\rightarrow$  Active Triggers, causes an alert.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

Q Search Logs	Federated Nodes	Active Triggers: nc_130		Find Text	C Refresh Page 🛓 Download	Copy to ClipBoar
	BostonMA::nc 130	-	✓ Prev Page 1	Next Page 🕨		
egin Time		loC	Timestamp	SessionInfo		
020-01-27 12:36:00	NashuaNH::nc_113	test-tcp or udp	2020-01-27 17:34:07	1.2.75.248:21	tcp 1.1.67.212:47292	lick to
		AT 17 40 11-tcp or udp	2020-01-27 17:34:07	1.2.75.248:21		restigate
ad Time		AT_12_35_57-tcp	2020-01-27 17:34:07	1.2.75.248:211	tcp 1.1.67.212:47292	
020-01-27 12:36:00		AT_12_11_0-tcp	2020-01-27 17:34:07	1.2.75.248:21	tcp 1.1.67.212:47292	
		test-tcp or udp	2020-01-27 17:14:10	5.5.5.5:80 top 6	5.6.8.61:800	
g Search Filter [?]		AT_12_36_42-port 80	2020-01-27 17:14:10	5.5.5.5:80 tcp (	5.6.8.61:800	
etum only events that have the supplied pattern(s)		AT_12_35_57-tcp	2020-01-27 17:14:10	5.5.5.5:80 tcp (	5.6.8.61:800	1
100 <b>_</b> 100000		AT_17_40_11-tcp or udp	2020-01-27 17:14:05			O Configuration O Help @ Lapout
ax Rows		AT_12_11_0-tcp	2020-01-27 17:14:05	oley Selap	I Higons	and a second second
6000		AT_12_36_42-port 80	2020-01-27 17:13:25			Investigator Dashboard
C		test-tcp or udp	2020-01-27 17:13:25 Period Refer	Discover		G 🖂 🛞
Q Search Logs		AT_17_40_11-tcp or udp	2020-01-27 17:13:28 Named to 1	New Save Open Share Inspect	the last of the second second	Thow dates C Refresh
	1	AT_12_35_57-tcp	2020-01-27 17:13:2		strangeducersed we D.+ restance	C MILLER
		AT_12_11_0-tcp	2020-01-27 17:13:28	investigator.* (change) 0	67 htts	
		AT_17_40_11-tcp or udp	2020-01-27 17:05:28	G. Search field names	Jan 20, 2020 @ 12:37:15:954 - Jan 27, 2020 @ 12:37:15:955 Auto	×
		AT_12_11_0-tcp	2020-01-27 17:05:28	🛞 Filter by type 🛛 🕫 🕫		
		test-tcp or udp	2020-01-27 17:05:10	Selected fields		
		AT_12_36_42-port 80	2020-01-27 17:05:10	Anakata fata		
		AT_12_35_57-tcp	2020-01-27 17:05:10	Filler state		0-04104 10-0-72100
		AT 47 40 44 tan aruda	0000 04 07 47.04.EC	r Jos	timestamp.cor 3 hours	
		AT AT AT AS too or lide		e samulijid	JANNE 18.75 Inc. J. E. Leitz M. Kon, Dr. E. Leitz JV, Landston, Jan 27, 2021 4 52, Friedler, St. 1017, 20170, 101 Inc. J. Inc. Inc. Inc. Inc. Inc. Inc. Inc. Inc	DH analog lighter (7.15) prote: 109 ether type: 2.8

Figure 89-View Metadata Active Triggers view

# 9.8 FLOWS

The Flows tab shows bi-directional and one-way flows found in received network traffic for each node in the federation. FlowInfo shows community id, packet count, byte count, start time and end time of each flow. Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.



#### User Guide January 30, 2020

Q Search Logs	Federated Nodes	Flows: nc_113			Find Text Crefresh Page Download	Copy to ClipH
	BostonMA::nc_130			H Prev Page 1	Next Page 🕨	
egin Time	Mashushiking 442	Timestamp	Sessioninfo	FlowInfo		
020-01-24 14:41:00	NashuaNH::nc_113	2024-09-18 16:30:08	5.5.5.5:80 TCP 6.6.7.88 800		VclwghxQaP3w=,pkts_toserver=8,pkts_toclient=0,bytes_toserver=12112,bytes_toclient=0,start=2019-12- +0000,end=2019-12-25T21:21:32.215533945+0000,age=0,state=new,reason=timeout,alerted=false	0
nd Time		2020-01-24 19:35:59	10.4.23.102:49224 TCP 199.188.200.49 80		5brhXme4Ddk=,pkts_toserver=8414,pkts_toclient=17646,bytes_toserver=505830,bytes_toclient=206750 5+0000,end=2020-01-24T19:35:57.359664666+0000,age=88,state=closed,reason=timeout,alerted=false	
020-01-24 14:41:00	1	2020-01-24 19:35:59	192.168.15.93:49314 TCP 152.163.66.132 443		QYMmhMXqA=,pkts_toserver=37,pkts_toclient=27,bytes_toserver=10886,bytes_toclient=3624,start=202 0+0000,end=2020-01-24T19:35:57.46765653+0000,age=81,state=closed,reason=timeout,alerted=false	
turn only events that have the supplied pattern(s)	1	2020-01-24 19:35:59	192.168.15.93:49349 TCP 69.147.86.11 443		JIHNbAHen11=,pkts_toserver=75,pkts_toclient=97,bytes_toserver=9264,bytes_toclient=121189,start=202 i2+0000,end=2020-01-24T19:35:57.74332207+0000,age=43,state=closed,reason=timeout,alerted=false	
x Rows		2020-01-24 19:35:59	192.168.15.93:65322 TCP 54.192.123.84 443	24T19:3		figuration O Help
000		2020-01-24 19:35:59	192.168.15.93:49784 TCP 184.26.62.130 80	1:Bd7A: 24T19:5 Petersted Score	Of State         Notifierer         Notifier	Investigator D
Q Search Logs		2020-01-24 19:35:59	192.168.15.93:49735 TCP 52.52.86.176 443	1:Ivw9C 24T19:3		Show cattes C. R
		2020-01-24 19:35:59	192.168.15.68:53545 TCP 64.4.54.253 443	1:J+vIX 24T19:3		
		2020-01-24 19:35:59	192.168.15.93:65454 TCP 23.220.224.224 443	1:uf62r\ 24T19:3	Image: Selector Teles         .3n 10, 2020 @ M-4224.650 - 3an 34, 2020 @ M-4224.650 - Auto         ✓           Image: Angle Selector Teles         .3n 10, 2020 @ M-4224.650 - 3an 34, 2020 @ M-4224.650 - Auto         ✓	
		2020-01-24 19:35:59	192.168.15.93:49597 TCP 23.78.221.219 80	1:gJZf/r 24T19:3	a Available feelss ● Poular	
		2020-01-24 19:35:59	192.168.15.93:49752 TCP 216.58.216.198 443	1:MMIB 24T19:3	<sup>2</sup> <sup>3</sup> <sup>1</sup> <sup>1</sup>	21 20 20 20 20 20 20 20 20 20 20 20 20 20
					Q         Lynn         Tex.         Jacob           S         1.4         3. as its 2010 10 1000 are pointed with a sector model on the sector model on	224 dest_port: 60

Figure 90-View Metadata Flows view

## 9.9 DNS

The DNS tab displays the displays DPI events for port 53.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the metadata events with the same 5 tuple information for further analysis.

Q Search Logs		DNS: nc_130			Find Text	C Refresh Page & Download	Copy to ClipBo
C Scarch Logs	Federated Nodes				(		
	BostonMA::nc 130		H Prev Page	1	lext Page Click to investigate		
egin Time		Message			Timestamp	SessionInfo	
020-01-24 14:48:00	NashuaNH::nc_113	1:ebQRIJaIDQxt4u9N9c4A3h+91T0=,type=query,id=4350,rrname=200.43.168.192.in-ad	dr.arpa,rrtype=PTR,tx_id	=16379	2020-01-24 19:45:53	192.168.43.200:51147 UDP 192.1	68.43.1 53
d Time		1:ebQRIJalDQxt4u9N9c4A3h+91T0=,version=2,type=answer,id=8445,flags=8580,qr=tru addr.arpa,rrtype=PTR,rcode=NOERROR,answers=,grouped=	ie,aa=true,rd=true,ra=true	e,rmame=200.43.168.192.i	n- 2020-01-24 19:45:53	192.168.43.1:53 UDP 192.168.43	200 51147
020-01-24 14:48:00		1:QEWTPf028JC31s0pkJMIEKuea+w=,version=2,type=answer,id=3369,flags=8180,qr=t	rue,rd=true,ra=true,rrnam	ne=sync.go.sonobi.com,rrty	pe= 2020-01-24 19:45:53	192.168.43.1:53 UDP 192.168.43	200 52066
	-	1:ebQRIJaIDQxt4u9N9c4A3h+91T0=,type=query,id=8445,rrname=200.43.168.192.in-ad	dr.arpa,rrtype=PTR,tx_id	=16377	2020-01-24 19:45:53	192.168.43.200:51147 UDP 192.1	68.43.1 53
g Search Filter [?]		1:tfERp/Cd/HIZEIoRzi6FoZSW4/I=,version=2,type=answer,id=21191,flags=8180,qr=true,	rd=true,ra=true,rrname=f	fanatics.frgimages.com,rrty	pe= 2020-01-24 19:45:53	192.168.4.1:53 UDP 192.168.43	200 50797
turn only events that have the supplied pattern(s)		1:LIW5Kb4IIDnjmO42N18zBA4j5C8=,type=query,id=56982,rrname=static.ak.fbcdn.net,i	Dashboard	A Policy Setup Investigator Q Se			
		1:ebQRIJaIDQxt4u9N9c4A3h+91T0=,type=query,id=24825,rmame=200.43.168.192.in-a	O Create Search	NodeName (12, 130 NodelP. 10.91, 170, 13	2		Investigator Dashippan
x Rows		1:Tv6vT8lX7lWjlxFlh+wLYtsBsGs=,version=2,type=answer,id=12945,flags=8180,qr=tru bh.ybp.yahoo.com,rrtype=A,rcode=NOERROR,answers=,grouped=	Federaled Nodes	Discovar			0 0 0
Q.		1:B08Zbhmf27BSPGjG+EkgS1oAqLc=,type=query,id=33534,rmame=px.steelhousemer			and srt_port.51147 and dest_kt 192.168.43.1 and	I dest KOL this Last Livesk	Shew dates C Refresh
Q Search Logs		1:krwxMp+Vfvf0hZKDFhQ++qtuPkl=,type=query,id=60190,rmame=sp.analytics.yahoo.c		0 + Add BMr			
C incluent rogs		1:ebQRIJalDQxt4u9N9c4A3h+91T0=,version=2,type=answer,id=28920,flags=8183,qr=t addr.arpa,rrtype=PTR,rcode=NXDOMAIN,authorities=		B envestigator_* (change)	) Jan 17, 203	8,007 hits 0 @ 14:48:57.262 - Jan 24, 2020 @ 14:48:57.263 Auto Auto	
		1:sxxuOWS8WF5fLYg+sZEFIL5LYtA=,version=2,type=answer,id=27084,flags=8180,qr=		El O Fitter by type	1300		
		1:wb2g/ledHssMM2ewkS0sHfVDuTk=,type=query,id=33540,rmame=insidenfl.nflshop.cx		& Selected fields	4330 E 3330		
		1:krwxMp+Vfvf0hZKDFhQ++qtuPkl=,version=2,type=answer,id=60190,flags=8180,qr=tr		le cource	8 2000		
		1:ebQRIJaIDQxt4u9N9c4A3h+91T0=,type=query,id=28920,rrname=24.24.25.69.in-addr		Austitute fields	0		
		1:BFKwrBmkDfevb49fZiBM2evisvQ=,type=query,id=19157,rrname=com-footballfan.netr		42) I .7550	2020-01-06.00/00 2020-01-06.00/00	2005-01-20 00 00 2020-01-20 00 2020-01-20 00 2020-01-20 0 Emotioning per 3 hours	100 2000-01-04 00:00
		1:u+eYYWZhasoFCq3CeEM4YTudzZ0=,version=2,type=answer,id=5288,flags=8180,qr		😨 ı community;)d	Time - Jacorte		
				a romo	*lev_10:	102. 148. 43. 200 dest. 50: 192.158.43.3 timestamp: Jan 24, 2822 0 1: 411, 552, 451, 607, 135, 538 thorapph/cm1165/438859, 45/1075095152075123165, 1571055154064655, g	
				6 I.J.		8,882,294,321 event_typa: dis src_port: \$1,147 cest_port: \$3	

Figure 91-View Metadata DNS view

### 9.10 FILES

The Files tab displays IDS alerts of type 'file\_type'.



Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

Q Search Logs		Files: nc_130			Fin	d Text	C Refresh Page & Download	d Copy to ClipBe
Contri Dogo	Federated Nodes							
	BostonMA::nc 130		e Pre	Click to investigate	Next Page	₩		
egin Time	·	loC	TimeStamp		SessionInfo		Size(byte	s)
020-01-24 14:57:00	NashuaNH::nc_113	b744cc16f32095065aa635509383c4bc.jpeg	2020-01-24 19:53:43		72.21.91.121:80 TCP	72.16.133.93 61147	1692	
	-	/cgi-bin/m	2020-01-24 19:53:43		138.108.6.20:80 TCP	72.16.133.93 61136	44	
d Time		/cgi-bin/m GIF image data, version 89a, 1 x 1	2020-01-24 19:53:43		138.108.6.20:80 TCP	72.16.133.93 61111	44	
020-01-24 14:57:00		/cgi-bin/m GIF image data, version 89a, 1 x 1	2020-01-24 19:53:43	· · · · ·	138.108.6.20.80 TCP	72 16 133 95 57201	44	
g Search Filter [?]	-	/vi/z0NCSPh4HvM/mqdefault.jpg JPEG image data, JFIF standard 1.01	2020-01-24 19:53:43	#Dashboard	A Policy Setup 👁 Investigator Q Sea			
		/cgi-bin/m	2020-01-24 19:53:42	O Create Search.	NoteName nc., 100 NodelP: 1231.172.130			Investigator Dashboa
turn only events that have the supplied pattern(s)		/AI/Api/v1/UserRest.svc/Provider/EFD5B938-837D-4375-9FCF- 5937CC010DA6/User/uaeWOF6W99Odg9JH/gif	2020-01-24 19:53:42	Pederalist Nodes Desker/VA re: 122	K 🛽 Discover			0 10 (
ax Rows		/Al/Api/v1/UserRest.svc/Provider/39CD8FF4-531A-4266-A340- 45548C451F45/User/5102bdc5f2add3f1/gif	2020-01-24 19:53:42	Network (20, 11)	New Save Open Share In     Sec.jp: 72.21.91.121 and		Dano dest, port KIL 👔 🗸 Last 1 week	Show dates C Refresh
		/js/plusone.js ASCII text, with very long lines	2020-01-24 19:53:42	-	· · Add filter			
Q Search Logs		/cgi-bin/m GIF image data, version 89a, 1 x 1	2020-01-24 19:53:42		se investigator_* (change)		26 hits	
a oranin Logo		/~/st/i/y.gif	2020-01-24 19:53:42		Q Search field names	J	an 17, 2020 @ 14.58:06.847 - Jan 24, 2020 @ 14:58:06.647 - Auto	×
C Statut Logs		/xl/PROD/18022/creatives/mat_grl_SPM_NoBorderNew2imgDissGmSqrSM Macromedia Flash data (compressed), version 8	2020-01-24 19:53:42		C Fiber by type D Selected fields			
		/cgi-bin/m	2020-01-24 19:53:42		sue, o 8	8		
		/wp-content/thumbnails/featured-thumbnail/5b0f5ffa979ab50_135_90.jpg JPEG image data, JFIF standard 1.01, comment: "CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 100"	2020-01-24 19:53:42		8 Auslable Fadds Reputy t June C Auslable Fadds		Envisions per 3 hours	009-09-25-30-30 2020-29-34-63-08
		/cgi-bin/m GIF image data, version 89a, 1 x 1	2020-01-24 19:53:42		a tertaterare	Time -	30/000	
		/coi-bin/m	2020-01-24 19:53:42		A fertisson g finals e sonis e sonis		Milling 2021/00/20 (edited), 822/01/20 (edited), 844-02/170402 (edited) 10:52-02-02 (edited) 10:52,02-02 (edited) 10:52-02-02 (edited) 10:52-02-02 (edited) 10:52-02-02 (edited) 10:52-02-02 (edited) 10:52-02-02-02-02-02-02-02-02-02-02-02-02-02	omition poquite ignore superi: M destuport: \$1,147 prote: TC 20:67:15:0f

Figure 92--View Metadata Files view

# 9.11 HTTP

The HTTP tab displays the DPI events for port 80 for each node selected.



User Guide January 30, 2020

Q Search Logs		HTTP: nc_130			QFind Text			
Column Logs	Federated Nodes					Copy to ClipBoard	▲ Download C Refresh Page	
Begin Time 2020-01-27 17:55:46	BostonMA::nc_130 NashuaNH::nc_113			Page Size	500 <b>v</b>	Prev 1 2 3	4 5 Next »	
End Time		TimeStamp	SessionInfo	CommunityID	HostName	URL	UserAgent	
2020-01-27 18:25:46		2020-01-27 18:16:44	172.16.9.171:2559 TCP 213.254.245.30:80	1:USiwRihj739cbp.	stj.msn.com	/br/om/js/1/s_code.js	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	
og Search Filter [?] return only events that have the supplied pattern(s)		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83.80	1:923+51zdGl0	Click to investigate	/mail/? auth=DQAAAHQAAAC0wP4hfXK1i ZEZg4iGSxIUkK1_ljzXN2amwGhEl h8ZKX9EI9XLjfWaymP13NI0TxbGl	RRxSImSrcICN	
lax Rows		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGl0DE.	mail.google.com	/mail/? view=page&name=browser&ver=1g	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) g6sx25oiht2t	
2000		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.		WDishboard & Policy Setup & Investigator (		leporta O Configuration O Help (+ Lopo
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail	Create Search		Investigator Davabaard
Q Search Logs		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail Petersiel Notes	Concerns Store Open Sha	a lasted	0 0 0
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail hamanatics		71 and src_port:2836 and cest.jp:66.249.91.83 and dest, por IN2L III VIL Last 1 week	Show dates O Refresh
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail	• Acc filter		
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail	investigator_* (change		
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail	C) Search field names	Jan 20, 2020 g 13:26:23:474 - Jan 27, 2020 g 13:26:23:474 - A	uto V
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail	A Filter by type 3	· ··· · · · · · · · · · · · · · · · ·	
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail	B ch. stores		
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGl0DE.	mail	Available feature	326 	
		2020-01-27 18:16:43	192.168.43.200:54015 TCP 50.97.130.118:80	1:rr/DKBZXZpEaX.	dx.s	e comunicate d nouse	Time	. 2020 0 19(17)07.721
		2020-01-27 18:16:44	172.16.9.171:2836 TCP 66.249.91.83:80	1:923+51zdGI0DE.	mail	6 e poso 7 e Juli 1 poso 1 poso	Flam, Md. 1, 648, 322, 523, 489, 416 million (2017) retrievant (1977) retrievant (1977) retrievant (1978) programming (1978) retrievant (1978) retrievant (1978) retrievant (1978) programming (1	s_port: 2,835 dest_port: 60 prote: TCP
						9 / Jone	> Jan 27, 2020 0 13:17:27.721 arc.1p: 172.10.0.371 rest.1p 00.240.01.80 threstamp: Jan 27	. 2020 # 13:17:37.721

Figure 93-View Metadata HTTP view

## 9.12 SMB

SMB panel displays DPI events for port 445.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

Q Search Logs	Federated Nodes	SMB: nc_130		Q Find Text	py to ClipBoard	Download CRefresh Page	
legin Time	BostonMA::nc_130 NashuaNH::nc_113			Page Size 500 • « P	rev 1 2 Ne	ext »	
2020-01-27 16:56:04	NashuaNH::nc_113	_					
nd Time		TimeStamp	SessionInfo	Click to investigate	ommand	KerberosRealm	н
id fille	_	2020-01-27 17:15:53	1.1.31.38:34819 TCP 1.2.24.10 139		MB1_COMMAND_TREE_COM	INECT ANDX	
020-01-27 17:26:04		2020-01-27 17:15:53	1.1.31.38:34819 TCP 1.2.24.10 139		MB1 COMMAND TREE COM		
g Search Filter [?]		2020-01-27 17:15:53	1.1.31.38:34819 TCP 1.2.24.10 139		MB1 COMMAND SESSION		
		2020-01-27 17:15:53	1.1.85.80:60645 TCP 1.2.98.160 139	#Davy	oard A Policy Setup Investigator Q	Search & View Metadata	Configuration @ Help (+ Lo
turn only events that have the supplied pattern(s)		2020-01-27 17:15:53	1.1.85.80:60645 TCP 1.2.98.160 139	O Create Se			Investigator Dashbo
-		2020-01-27 17:15:52	1.1.36.133:45192 TCP 1.2.37.169 139	Under St			
ix Rows		2020-01-27 17:15:52	1.1.36.133:45192 TCP 1.2.37.169 139	Performed Secon	🕺 🙍 Discover		0 🛛 (
000		2020-01-27 17:15:52	1.1.36.133:45192 TCP 1.2.37.169 139	Redenicity, vo. 10	G New Save Open Share	a Inspect	
		2020-01-27 17:15:51	1.1.23.48:44753 TCP 1.2.24.119 139	Network F2_113	Ø E ✓ src.jp: 11.31.38 and	d src_port/34819 and dest_jor1.2.24.10 and dest_port/338 KQL @ V Last 1 week	Show dates C Refrest
Q Search Logs		2020-01-27 17:15:50	1.1.126.76:59421 TCP 1.2.127.0 139		· Add fitter		
		2020-01-27 17:15:50	1.1.126.76:59421 TCP 1.2.127.0 139		and a second second	G 1,102 hits	
		2020-01-27 17:15:44	1.1.15.40:64279 TCP 1.2.60.88 139		C Search field names	Jan 20, 2020 @ 12:26:55:540 - Jan 27, 2020 @ 12:26:55:540 - Auto	~
		2020-01-27 17:15:44	1.1.19.46:13110 TCP 1.2.28.76 139		E Titler by type 0	200	
		2020-01-27 17:15:44	1.1.19.46:13110 TCP 1.2.28.76 139		Selected fields	701 7	
		2020-01-27 17:15:44	1.1.14.90:42705 TCP 1.2.15.198 139		O	10 Ge	
		2020-01-27 17:15:44	1.1.14.90:42705 TCP 1.2.15.198 139		available fields		densis_ini_
		2020-01-27 17:15:44	1.1.52.108:49163 TCP 1.2.1.146 139		d) Poster	1025-0-31008 2025-0-112300 2025-0-312300 2025-0-312308 2025-0-324248 2025-0-	-36.40 30 333/6-01-07 03.30
		2020-01-27 17:15:44	1.1.68.85:20720 TCP 1.2.113.148 139		1 399	tinestang per 3 hours	
		2020-01-27 17:15:44	1.1.68.85:20720 TCP 1.2.113.148 139		1 Distanti	TineSource	
		2020-01-27 17:15:44	1.1.68.85:20720 TCP 1.2.113.148 139		S e shert.rev	3 Jan 27, 2828 6 12:18:00.443 src_13: 5.1.31.38 dest_tp: 1.2.24.18 timestamp: Jan 27, 2828 6 12:18:0 no. 447 / 1200-14241003042	
		4			<ul> <li>e community_ki</li> </ul>	posp.ort: 12,449.318.444 event.type: seb 3p.rep.3d: NAL src.port: 34	
					e / fex.id	ether.type: 2,048 ather.are: 02:14:05:02:00:00 ather.dat: 02:14:05:01	101:00 and.1d1 3

Figure 94-View Metadata SMB view

#### **9.13 EMAIL**

The Email tab displays the DPI events for port 25 for each node in the Federation.



Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

				01	Find Text						
Q Search Logs	Federated Nodes	EMail: nc_130			IIIG TEXT	Cop	y to ClipBoard	Download	C Refresh Page		
Segin Time	BostonMA::nc_130 NashuaNH::nc_113			Page Size	e 500	• « Prev	1 2 3	Next »			
ind Time		TimeStamp	SessionInfo	CommunityID	From	То			Subject	Details	
2020-01-27 18:37:24		2020-01-27 18:32:14	1.1.70.253:5002 TCP 1.2.123.51:25	1:7gsRdV2VR2eMy	Click to	cample.com> (* <rec< td=""><td>ipient@example.com&gt;"]</td><td></td><td>Business and cold respectfulness.</td><td>client- 10171eb.example.</td><td>int,HEADE</td></rec<>	ipient@example.com>"]		Business and cold respectfulness.	client- 10171eb.example.	int,HEADE
.og Search Filter [?]			0.91.170.22:36612 TCP 204.11.16.106:25 10.91.170.22:41604 TCP 10.91.170.186:25	Tior to age 200001	vestigate	M4-003> [* <adii M4-003&gt; [*<bot< td=""><td>ian@lartc.org&gt;*] oby&gt;']</td><td></td><td>tost</td><td>3650M4-003,HEAD 3650M4-003,BOD</td><td>-</td></bot<></adii 	ian@lartc.org>*] oby>']		tost	3650M4-003,HEAD 3650M4-003,BOD	-
return only events that have the supplied pattern(s)		2020-01-27 18:33:31	1.1.70.253:5002 TCP 1.2.123.51:25	1:7gsRd VR2eMyXT/	<sender@< td=""><td></td><td>ipient@example.com&gt;"] Policy Setup @ Investigator 0, Se</td><td></td><td>Business and cold respectfulness.</td><td>client- leports O Contiguration O H</td><td>ialp (+ Logo</td></sender@<>		ipient@example.com>"] Policy Setup @ Investigator 0, Se		Business and cold respectfulness.	client- leports O Contiguration O H	ialp (+ Logo
flax Rows			2 1.1.70.253:5000 TCP 1.2.123.51:25	1:QiaG1nnoTfom4WuC		Create Search	Noteliare m. 133 NotelP 10 M 170.1	3			ligator Dashboard
Q Search Logs			<ul> <li>1.1.70.253:5001 TCP 1.2.123.51:25</li> <li>10.91.170.22:36810 TCP 204.11.16.106:25</li> </ul>	1:NIIMSxmKukXOkc1P 1:holzEOCU659AuGZk	BoctorSiA.va	000 	Discover O New Save Open Share				
		2020-01-27 18:33:43	10.91.170.22:36610 TCP 204.11.16.106:25 172.16.9.171:2991 TCP 195.241.79.132:25	1:hc/zEOCU659AuGZk	<rox< td=""><td></td><td>⊘ (1) v stc.jp:11.70.203 and ⊙ + Add filter</td><td>src, port 5002 and dest, jp:1.2.12</td><td>KQL () V Last 1 week</td><td>Show dates</td><td>C Refresh</td></rox<>		⊘ (1) v stc.jp:11.70.203 and ⊙ + Add filter	src, port 5002 and dest, jp:1.2.12	KQL () V Last 1 week	Show dates	C Refresh
		2020-01-27 18:33:44	172.16.9.171:3285 TCP 195.241.79.132:25	1:vaXWMDS+c67l82Fa	<ac< td=""><td></td><td>80 R Search field names</td><td></td><td>36,562 hits Jan 20, 2020 § 13:38:57.074 - Jan 27, 2020 § 13:38:57.074 - Ar</td><td>uto v</td><td></td></ac<>		80 R Search field names		36,562 hits Jan 20, 2020 § 13:38:57.074 - Jan 27, 2020 § 13:38:57.074 - Ar	uto v	
			10.91.170.22:36612 TCP 204.11.16.106:25 1.1.70.253:5002 TCP 1.2.123.51:25	1:9RaugDzeJ9bHEOS. 1:7gsRdV2VR2eMyXT/			Filter by type     Selected fields	2008 0558 0000 1538	. B.		
		2020-01-27 18:33:51	1.1.70.253:59404 TCP 1.2.123.51:25	1:5MzvphWhuwInudYP	<so< td=""><td></td><td>Available fields     Popular</td><td>1000 520 0</td><td></td><td></td><td></td></so<>		Available fields     Popular	1000 520 0			
		2020-01-27 18:33:51	1.1.70.253:5000 TCP 1.2.123.51:25	1:QiaG1nnoTfom4WuC	<se< td=""><td></td><td>T Jobe T Alertactice</td><td>Time -</td><td>timestamp per 3 hours "stource</td><td></td><td></td></se<>		T Jobe T Alertactice	Time -	timestamp per 3 hours "stource		
		2020-01-27 18:33:51	1.1.70.253:5001 TCP 1.2.123.51:25	1:NIIMSxmKukXOkc1P	<so< td=""><td></td><td>i     + austrov       iii     + constructly, d       iii     + construction       iii     + construction       iii     + construction</td><td>) Jan 27, 2008 8 13:32:18</td><td>207 sector \$1,00,033 dett_09,12,035 disenting: Jen 27, 10 Gardid 1,00,700,200,046,034 sector type: dert sector: a commung.id: 1/paterzydaept0.0023/t0000 sizet.action: a alart.rev. 1 alart.signature: file found over BDP and tored settable.cleme.9076.com/l.std.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/l.std.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sectoral.id.std.sectoral.id.std.sector.action.edu/ sectoral.id.sectoral.id.std.sectoral</td><td>1,002 dest_port: 25 proto: 10P Howed alert.gid: 1 alert.sign # alert.rategory: alert.sever</td><td>store_1d. 2)</td></so<>		i     + austrov       iii     + constructly, d       iii     + construction       iii     + construction       iii     + construction	) Jan 27, 2008 8 13:32:18	207 sector \$1,00,033 dett_09,12,035 disenting: Jen 27, 10 Gardid 1,00,700,200,046,034 sector type: dert sector: a commung.id: 1/paterzydaept0.0023/t0000 sizet.action: a alart.rev. 1 alart.signature: file found over BDP and tored settable.cleme.9076.com/l.std.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/l.std.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sector.action.edu/ settable.cleme.9076.com/lstd.sectoral.id.std.sectoral.id.std.sectoral.id.std.sector.action.edu/ sectoral.id.sectoral.id.std.sectoral	1,002 dest_port: 25 proto: 10P Howed alert.gid: 1 alert.sign # alert.rategory: alert.sever	store_1d. 2)
							CO / Taking Aire	) Jun 27, 2100 0 13:32:14	154 are to: 1.1.70.253 dect_tp: 1.2.135.51 timetrep: Jac 27, 20 Gov.10 1.000.700.293.228.071		

Figure 95-View Metadata Email view

### 9.14 TLS/SSL

The TSL/SSL tab displays the DPI events for port 443 for each node in the Federation. All events are clickable and searchable.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

If a TLS/SSL event's JA3 signature matches known bad JA3 signatures uploaded via Augmentation panel, this event also appears as a Suspicious Signature event.



#### User Guide January 30, 2020

Q Search Logs		TLS/SSL: nc_130		QFind Tex							
C Search Logs	Federated Nodes					Copy to ClipBoard	🛓 Download	C Refresh Page			
egin Time	BostonMA::nc_130			Page Siz	« Prev	v 1 2 3	Next »				
020-01-27 18:21:05	NashuaNH::nc_113			Click to Investig							
nd Time		TimeStamp	SessionInfo	Community	ID	JA3	Subject	IssuerDN	Version	Serial, Fingerpr	int
020-01-27 18:51:05		2020-01-27 18:44:27	1.1.14.216:18396 TCP 1.2.66.238:443	1:jg6pbCtRCZ7D5	jSTDNZR	042c053a3350b75bbc96d5	C=US, ST=UT, L=mrmcQlwryAYhCgJ O=ICZLxxjyZyQrsmjol CN=HVItmXCjHWfWS		TnEPOy.	00:93:DE:77:F4	f1:4c:89:b5:.
turn only events that have the supplied pattern(s)		2020-01-27 18:44:27	1.1.80.129:23891 TCP 1.2.88.132:443	1:Jv8xnqv6cEt	#Desht	nboard A Policy Selup Investigator Q NodeRame nc. 10 NodeP: 10.91.170			🗎 Reș	orts O Configuration O	Help 🕑 Logo
ax Rows		2020-01-27 18:44:26	1.1.7.182:35880 TCP 1.2.15.111:443	1:ndP/S7FIxq7i	enaled Nodes docKM mc_03 alexaNet.cc_113	Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constraint of the state         Image: Constraint of the state           Image: Constate         Image: Constraint of the state <td></td> <td>238 and dest, portold KOL 😭 🗸 La</td> <td>ist 1 sovjek</td> <td>Show dates</td> <td>C Refresh</td>		238 and dest, portold KOL 😭 🗸 La	ist 1 sovjek	Show dates	C Refresh
		2020-01-27 18:44:27	1.1.99.37:25770 TCP 1.2.95.215:443	1:Tsu4qLppNav		的 investigator_* [change] 可 C. Search field names	0	<b>8</b> Jan 20, 2020 @ 13:52:09:529 - Jan 27;	8 hits 2020 g 13:52:09:529 — Aut	• •	
		2020-01-27 18:44:28	1.1.71.67:59447 TCP 1.2.79.116:443	1:jpi8GICg/LQJx		Fitter by type     Enerted fields     Gource     Available failte	40 20 20 20				
		2020-01-27 18:44:28	1.1.43.242:41165 TCP 1.2.28.7:443	1:iuvXkHk6PASIk		D Papaler e Jope C e alertaction	Time .	janes	ng per 3 hours	2629-01-26 00:00 2022-27-27	2000
		2020-01-27 18:44:28	1.1.119.37:33789 TCP 1.2.75.22:443	1:Kqey2UV5088!		e startine e contrastituid e formatituid e porto	> Jan 27, 2020 6 13:38:58.	<sup>171</sup> Src.p: 1.1.14.210 dest.p: 1.2.46 Flow_161 1.643,830,235,925,853 nt_161 /storage0/lat1118/438306_38/ pcag_ont: 15.432,821,246 event_top etner.type: 2.646 etner.src. 62:15	1580158022020545667,158015803 8: alert <u>Wrc.port:</u> 10,016 de	39037119.pcsp.tz.lgnore st_port: 443 proto: 70P	
						Q 1.0	) Jan 27, 2828 # 15:33:20.	115 srz.1p: 1.1.14.216 dzst.1p: 1.2.69 film.15: 1.643,826,214,168,548	194 timestamp: Jan 17, 2020	0 18:33:20.415	

Figure 96-View Metadata TLS/SSL view

# 9.15 VOIP

Each VOIP session entry displays Begin time of the session, Sessioninformation, RequestMethod, From (From, From\_tag), Call-id, CSeq (Call sequence), ResponseMethod, To (To, To\_tag) and the Jitter value for the session.

The VOIP tab provides two ways of filtering VOIP session data displayed.

- "Find Text" Filter:
  - When this field is empty, all VOIP sessions are displayed.

<b>Q</b> Search Logs	Federated Nodes	VOIP: nc_130	QFind Text	м	in Jitter:0	Max Jitter: 999	99 🖪 Copy to C	lipBoard	Lownload	Refresh Page	
legin Time 2020-01-27 19:40:00	BostonMA::nc_130 NashuaNH::nc_113			Page Size	500 <b>v</b>	Prev 1	2 3 4	5 Next	»		
ind Time		Timestamp SessionIn	fo	RequestMethod	From		Call-Id	CSeq	ResponseMethod	То	Jitter
2020-01-27 20:10:00		2020-01-27T19:54:16 10.33.6.10 10.33.6.10		BYE	<sip:101@10.33.6.1< td=""><td>00;user=phone&gt;</td><td>190798326327120108 544@10.33.6.101</td><td>3 1 BYE</td><td>ок</td><td><sip:mp114.fxs1@192.168.2.160></sip:mp114.fxs1@192.168.2.160></td><td></td></sip:101@10.33.6.1<>	00;user=phone>	190798326327120108 544@10.33.6.101	3 1 BYE	ок	<sip:mp114.fxs1@192.168.2.160></sip:mp114.fxs1@192.168.2.160>	
og Search Filter [?]		2020-01-27T19:54:15 10.0.2.20: 10.0.2.15:		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ок</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
eturn only events that have the supplied pattern(s)		2020-01-27T19:54:15 10.0.2.15: 10.0.2.20:		INVITE	L16/48000 <sip:sipp< td=""><td>@10.0.2.20:5060&gt;</td><td>1-2123@10.0.2.20</td><td>1 INVITE</td><td>ок</td><td>test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060></td><td>5012</td></sip:sipp<>	@10.0.2.20:5060>	1-2123@10.0.2.20	1 INVITE	ок	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	5012
000		2020-01-27T19:54:15 10.0.2.20: 10.0.2.15		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2121@10.0.2.20</td><td>99750240 BYE</td><td>ок</td><td>L16/11025 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2121@10.0.2.20	99750240 BYE	ок	L16/11025 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
Q Search Logs		2020-01-27T19:54:15 10.0.2.20: 10.0.2.15:		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-4269@10.0.2.20</td><td>99791983 BYE</td><td>ОК</td><td>iLBC/8000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-4269@10.0.2.20	99791983 BYE	ОК	iLBC/8000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
C Scaren Logs		2020-01-27T19:54:15 10.0.2.15: 10.0.2.20:		BYE	test <sip:test@10.0.< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ОК</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0.<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ОК	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.20: 10.0.2.15		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2120@10.0.2.20</td><td>99750234 BYE</td><td>ок</td><td>L16/16000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2120@10.0.2.20	99750234 BYE	ок	L16/16000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.15: 10.0.2.20:		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ОК</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ОК	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.15: 10.0.2.20:		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ок</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.20: 10.0.2.15	060 UDP	BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2118@10.0.2.20</td><td>99750230 BYE</td><td>ОК</td><td>L16/8000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2118@10.0.2.20	99750230 BYE	ОК	L16/8000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.15: 10.0.2.20:	060 UDP	BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ок</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	

Figure 97-View Metadata VIOP view



# • As the user enters text into this text field, only the matching rows are displayed.

<b>Q</b> Search Logs	Federated Nodes	VOIP: nc_130	QFind Text	BYE	1in Jitter:0	Max Jitter: 999	999 Copy to C	lipBoard	La Download	Refresh Page	
egin Time	BostonMA::nc 130 NashuaNH::nc 113	_		Page Size	500 •	Prev 1	2 3 4	5 Next	»		
2020-01-27 19:40:00		-									
nd Time		Timestamp SessionInf		RequestMethod	From		Call-Id	CSeq	ResponseMethod		Jitter
2020-01-27 20:10:00	)	2020-01-27T19:54:16 10.33.6.101 10.33.6.100		BYE	<sip:101@10.33.6.1< td=""><td>00;user=phone&gt;</td><td>190798326327120108 544@10.33.6.101</td><td>3 1 BYE</td><td>OK</td><td><sip:mp114.fxs1@192.168.2.160></sip:mp114.fxs1@192.168.2.160></td><td></td></sip:101@10.33.6.1<>	00;user=phone>	190798326327120108 544@10.33.6.101	3 1 BYE	OK	<sip:mp114.fxs1@192.168.2.160></sip:mp114.fxs1@192.168.2.160>	
og Search Filter [?]		2020-01-27T19:54:15 10.0.2.20:50 10.0.2.15:50		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ок</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
eturn only events that have the supplied pattern(s)		2020-01-27T19:54:15 10.0.2.15:50 10.0.2.20:50		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ок</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
lax Rows		2020-01-27T19:54:15 10.0.2.20:54		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2121@10.0.2.20</td><td>99750240 BYE</td><td>ОК</td><td>L16/11025 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2121@10.0.2.20	99750240 BYE	ОК	L16/11025 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
Q Search Logs		2020-01-27T19:54:15 10.0.2.20:5 10.0.2.15:5	060 UDP	BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-4269@10.0.2.20</td><td>99791983 BYE</td><td>ОК</td><td>iLBC/8000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-4269@10.0.2.20	99791983 BYE	ОК	iLBC/8000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
Staten Logs		2020-01-27T19:54:15 10.0.2.15:5 10.0.2.20:5		BYE	test <sip:test@10.0.< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>OK</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0.<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	OK	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.20:50 10.0.2.15:50		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2120@10.0.2.20</td><td>99750234 BYE</td><td>ок</td><td>L16/16000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2120@10.0.2.20	99750234 BYE	ок	L16/16000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.15:50 10.0.2.20:50		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>OK</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	OK	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.15:50 10.0.2.20:50		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ок</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.20:5 10.0.2.15:5		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2118@10.0.2.20</td><td>99750230 BYE</td><td>ок</td><td>L16/8000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2118@10.0.2.20	99750230 BYE	ок	L16/8000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15 10.0.2.15:50 10.0.2.20:50		BYE	test <sip:test@10.0< td=""><td>2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ОК</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td></td></sip:test@10.0<>	2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ОК	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	

Figure 98-View Metadata VOIP Find Text view

- "Min Jitter" and "Max Jitter" Filter:
  - When both "Min Jitter" and "Max Jitter" fields are empty, only the sessions without RTCP packets are displayed.

Q Search Logs		VOIP: nc_130	QFind Text	N	Ain Jitter: 0 Max Jitter: 999	999 🖪 Copy to C	lipBoard	La Download	Refresh Page	
	Federated Nodes				DEFAULT					
egin Time 2020-01-27 19:40:00	BostonMA::nc_130 NashuaNH::nc_113			Page Size	500 v « Prev 1	2 3 4 5	5 Next	»		
nd Time		Timestamp	Sessioninfo	RequestMethod	From	Call-Id	CSeq	ResponseMethod	То	Jitter
020-01-27 20:10:00	1	2020-01-27T19:54:16	10.33.6.101:5060 UDP 10.33.6.100:5060	BYE	<sip:101@10.33.6.100;user=phone></sip:101@10.33.6.100;user=phone>	1907983263271201083 544@10.33.6.101	3 1 BYE	ок	<sip:mp114.fxs1@192.168.2.160></sip:mp114.fxs1@192.168.2.160>	
g Search Filter [?]		2020-01-27T19:54:15	10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
	J	2020-01-27T19:54:15	10.0.2.15:5060 UDP 10.0.2.20:5060	INVITE	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	1-2123@10.0.2.20	1 INVITE	ОК	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	5012
ax Rows		2020-01-27T19:54:15	10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2121@10.0.2.20	99750240 BYE	ок	L16/11025 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
Q Search Logs		2020-01-27T19:54:15	10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-4269@10.0.2.20	99791983 BYE	ОК	iLBC/8000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15	10.0.2.15:5060 UDP 10.0.2.20:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2123@10.0.2.20	99750244 BYE	OK	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15	10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2120@10.0.2.20	99750234 BYE	ОК	L16/16000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15	10.0.2.15:5060 UDP 10.0.2.20:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2123@10.0.2.20	99750244 BYE	OK	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15	10.0.2.15:5060 UDP 10.0.2.20:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15	10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2118@10.0.2.20	99750230 BYE	ОК	L16/8000/2 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	
		2020-01-27T19:54:15	10.0.2.15:5060 UDP 10.0.2.20:5060	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ОК	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	

Figure 99-View Metadata VOIP Min and Max Jitter field view



 When the user enters values into both "Min Jitter" and "Max Jitter" fields, only the sessions with jitter values that are >= "Min Jitter" and <= "Max Jitter" are displayed.

<b>Q</b> Search Logs	Federated Nodes	VOIP: nc_130	QFind Text	М	in Jitter: 5012	Max Jitter: 999	999 🖪 Copy to 0	ClipBoard	Ł Download 2	Refresh Page	
egin Time 2020-01-27 19:40:00	BostonMA::nc_130 NashuaNH::nc_113	_		Page Size	500 •	« Prev 1	2 3 4	5 Nex	t »		
nd Time		Timestamp	SessionInfo	RequestMethod	From		Call-Id	CSeq	ResponseMethod	То	Jitter
2020-01-27 20:10:00		2020-01-27T19:54:16	10.33.6.101:5060 UDP 10.33.6.100:5060	BYE	<sip:101@10.33.6< td=""><td>.100;user=phone&gt;</td><td>19079832632712010 544@10.33.6.101</td><td>83 1 BYE</td><td>ОК</td><td><sip:mp114.fxs1@192.168.2.160></sip:mp114.fxs1@192.168.2.160></td><td>5012</td></sip:101@10.33.6<>	.100;user=phone>	19079832632712010 544@10.33.6.101	83 1 BYE	ОК	<sip:mp114.fxs1@192.168.2.160></sip:mp114.fxs1@192.168.2.160>	5012
.og Search Filter [?]		2020-01-27T19:54:15	10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.< td=""><td>0.2.15:5060&gt;</td><td>1-2123@10.0.2.20</td><td>99750244 BYE</td><td>ОК</td><td>L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td>5012</td></sip:test@10.<>	0.2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ОК	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	5012
return only events that have the supplied pattern(s)		2020-01-27T19:54:15		INVITE	L16/48000 <sip:sip< td=""><td>p@10.0.2.20:5060&gt;</td><td>1-2123@10.0.2.20</td><td>1 INVITE</td><td>OK</td><td>test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060></td><td>5012</td></sip:sip<>	p@10.0.2.20:5060>	1-2123@10.0.2.20	1 INVITE	OK	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	5012
lax Rows		2020-01-27T19:54:15		BYE	test <sip:test@10.< td=""><td>0.2.15:5060&gt;</td><td>1-2121@10.0.2.20</td><td>99750240 BYE</td><td>ОК</td><td>L16/11025 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td>5012</td></sip:test@10.<>	0.2.15:5060>	1-2121@10.0.2.20	99750240 BYE	ОК	L16/11025 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	5012
Q Search Logs		2020-01-27T19:54:15	10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.< td=""><td>0.2.15:5060&gt;</td><td>1-4269@10.0.2.20</td><td>99791983 BYE</td><td>ОК</td><td>iLBC/8000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060></td><td>5012</td></sip:test@10.<>	0.2.15:5060>	1-4269@10.0.2.20	99791983 BYE	ОК	iLBC/8000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	5012

Figure 100-View Metadata VOIP Min and Max Jitter results

• Both "Find Text" and Jitter filters can be used together:

<b>Q</b> Search Logs	Federated Nodes	VOIP: nc_130	QFI	nd Text BY		Ain Jitter: 5012 Max Jitter: 999	1999 Copy to C	ipBoard	La Download	Kelresh Page		
Begin Time 2020-01-27 19:40:00	BostonMA::nc_130 NashuaNH::nc_113	-			Page Size	500 • Rrev 1	2 3 4 5	Next	»			
End Time		Timestamp	SessionInfo	F	RequestMethod	From	Call-Id	CSeq	ResponseMethod	То	Jitter	
2020-01-27 20:10:00		2020-01-27T19:54:1	6 10.33.6.101:5060 UDF 10.33.6.100:5060	P E	BYE	<sip:101@10.33.6.100;user=phone></sip:101@10.33.6.100;user=phone>	1907983263271201083 544@10.33.6.101	1 BYE	ОК	<sip:mp114.fxs1@192.168.2.160></sip:mp114.fxs1@192.168.2.160>	5012	
og Search Filter [?] return only events that have the supplied pattern(s)		2020-01-27T19:54:1	5 10.0.2.20:5060 UDP 10.0.2.15:5060	E	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ок	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	5012	
	_1	2020-01-27T19:54:1	5 10.0.2.15:5060 UDP 10.0.2.20:5060	E	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2123@10.0.2.20	99750244 BYE	ОК	L16/48000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	5012	
ax Rows		2020-01-27T19:54:1	5 10.0.2.20:5060 UDP 10.0.2.15:5060	E	3YE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>	1-2121@10.0.2.20	99750240 BYE	ОК	L16/11025 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	5012	
Q Search Logs		2020-01-27T19:54:1	5 10.0.2.20:5060 UDP 10.0.2.15:5060	E	BYE	test <sip:test@10.0.2.15:5060></sip:test@10.0.2.15:5060>		99791983 BYE	ОК	iLBC/8000 <sip:sipp@10.0.2.20:5060></sip:sipp@10.0.2.20:5060>	5012	

Figure 101-View Metadata VOIP Min and Max Jitter and Find Text combined field view

VOIP sessions allow searching for SIP, RTP and RTCP packets for each session.

"SessionInfo" column for SIP sessions displays:

• SIP source IP address, SIP source port



- SIP destination IP address, SIP destination port
- RTP inviter IP address, RTP inviter port.
- RTP invitee IP address, RTP invitee port.

"SessionInfo" column for RTP and RTCP sessions displays:

- SIP source IP address, SIP source port
- SIP destination IP address, SIP destination port
- RTP inviter IP address, RTP inviter port.
- RTP invitee IP address, RTP invitee port.

Jitter summary column displays the data extracted from RTCP packets for the session:

Note: If the session does not contain any RTCP packets the Jitter summary column can be blank.

Clicking on the hyperlinked sessioninfo pivots to the investigator screen that shows the events with the same 5 tuple information for further analysis.

Q Search Logs		VOIP: nc_130	QFind Text		Min Jitter: 0	Max Jitter: 999	999 🖪 Copy to C	lipBoard 📥	Download 2 Refre	sh Page		
Begin Time	Federated Nodes BostonMA::nc 130				Page Size 5	00 v « Pr	ev 1 Next »					
2020-01-27 21:48:00	NashuaNH::nc_113	_										
nd Time		Timestamp	SessionInfo	RequestMetho	d		Call-Id	CSeq R	esponseMethod To		Jitter	
2020-01-27 21:48:00		2020-01-28T02:36:54	4 10.33.6.101:5060 UDP 10.33.6.100:5060	BYE	Click to investig	ate er=phone>	1907983263271201083 544@10.33.6.101	B 1 BYE O	K <sip:1< td=""><td>MP114.FXS1@192.168</td><td>3.2.160&gt;</td><td></td></sip:1<>	MP114.FXS1@192.168	3.2.160>	
og Search Filter [?]		2020-01-28T02:36:53	3 10.0.2.20:5060 UDP 10.0.2.15:5060	OYE	test <sip:test@10.0< td=""><td>0.2. 5:5060&gt;</td><td>1-24411@10.0.2.20</td><td>100001580 O BYE</td><td>K G729</td><td>%8000 <sip:sipp@10.0.< td=""><td>2.20:5060&gt;</td><td></td></sip:sipp@10.0.<></td></sip:test@10.0<>	0.2. 5:5060>	1-24411@10.0.2.20	100001580 O BYE	K G729	%8000 <sip:sipp@10.0.< td=""><td>2.20:5060&gt;</td><td></td></sip:sipp@10.0.<>	2.20:5060>	
eturn only events that have the supplied pattern(s)		2020-01-28T02:36:53	3 10.0.2.15:5060 UDP 10.0.2.20:5060	INVITE	G729/8000 <sip:sip< td=""><td>op@ 10.0.2.20:5060&gt;</td><td>1-24411@10.0.2.20</td><td>1 INVITE O</td><td>K test &lt;</td><td>sip:test@10.0.2.15:50</td><td>60&gt;</td><td></td></sip:sip<>	op@ 10.0.2.20:5060>	1-24411@10.0.2.20	1 INVITE O	K test <	sip:test@10.0.2.15:50	60>	
ax Rows		2020-01-28T02:36:52	2 10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0< td=""><td></td><td>1-2123@10.0.2.20</td><td>99750244 O</td><td></td><td>18000 <sip:sipp@10.0.3< td=""><td></td><td></td></sip:sipp@10.0.3<></td></sip:test@10.0<>		1-2123@10.0.2.20	99750244 O		18000 <sip:sipp@10.0.3< td=""><td></td><td></td></sip:sipp@10.0.3<>		
Q Search Logs		2020-01-28T02:36:52	2 10.0.2.15:5060 UDP 10.0.2.20:5060	INVITE	L16/48000 <sip:sip< td=""><td>Create Search</td><td>1 Chicy Setup Convertigator Q 1</td><td></td><td>)<sup>0</sup></td><td>L.</td><td>eports O Configuration O Help (+)</td><td></td></sip:sip<>	Create Search	1 Chicy Setup Convertigator Q 1		) <sup>0</sup>	L.	eports O Configuration O Help (+)	
Generi Logs		2020-01-28T02:36:52	2 10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0< td=""><td>Pederated Nation Booker UNLow, 133 National VELSE, 113</td><td><ul> <li>Discever</li> <li>New Save Open Share</li> </ul></td><td></td><td></td><td></td><td>0 10</td><td></td></sip:test@10.0<>	Pederated Nation Booker UNLow, 133 National VELSE, 113	<ul> <li>Discever</li> <li>New Save Open Share</li> </ul>				0 10	
		2020-01-28T02:36:52	2 10.0.2.15:5060 UDP 10.0.2.20:5060	INVITE	L16/11025 <sip:sip< td=""><td></td><td>🖉 👻 - Adomter</td><td>nd sec.,port \$900 and dest,</td><td>Jo 10.33.6.190 and cest, port.5 KDL 5</td><td></td><td>Show dates C Refre</td><td>2</td></sip:sip<>		🖉 👻 - Adomter	nd sec.,port \$900 and dest,	Jo 10.33.6.190 and cest, port.5 KDL 5		Show dates C Refre	2
		2020-01-28T02:36:52	2 10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0< td=""><td></td><td>C. Search field names</td><td>3</td><td>Jan 20, 2020 @ 21-48-05.724</td><td>3 hits - Jan 27, 2020 @ 21.48:05.724 — Au</td><td>do v</td><td></td></sip:test@10.0<>		C. Search field names	3	Jan 20, 2020 @ 21-48-05.724	3 hits - Jan 27, 2020 @ 21.48:05.724 — Au	do v	
		2020-01-28T02:36:52	2 10.0.2.15:5060 UDP 10.0.2.20:5060	INVITE	L16/16000/2 <sip:sipp@10.0.2.2< td=""><td></td><td>Selected fields</td><td>Count</td><td></td><td></td><td></td><td></td></sip:sipp@10.0.2.2<>		Selected fields	Count				
		2020-01-28T02:36:52	2 10.0.2.20:5060 UDP 10.0.2.15:5060	BYE	test <sip:test@10.0< td=""><td></td><td>8 Australia facilia Propular 1 Jugan</td><td>05 0 1021-9-20100</td><td>1620-0-1230-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-</td><td>20-10-10-00 2021-9-20 2020 2020 Generalized per Shoury</td><td>-19 (M MAR) 2020-17 100.00</td><td></td></sip:test@10.0<>		8 Australia facilia Propular 1 Jugan	05 0 1021-9-20100	1620-0-1230-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-280-0-	20-10-10-00 2021-9-20 2020 2020 Generalized per Shoury	-19 (M MAR) 2020-17 100.00	
		2020-01-28T02:36:52	2 10.0.2.15:5060 UDP 10.0.2.20:5060	INVITE	L16/8000/2 <sip:sip< td=""><td></td><td>₩ . tor,si Ø i pros</td><td>Time -</td><td>_searce (27.19.302 are_ts: 10.33.6.101 feet_ flee.11 1.716.003.00.001</td><td></td><td>ND2 8 21:04:04:04</td><td></td></sip:sip<>		₩ . tor,si Ø i pros	Time -	_searce (27.19.302 are_ts: 10.33.6.101 feet_ flee.11 1.716.003.00.001		ND2 8 21:04:04:04	
							A interv		00.11 /storaget/101100.00	04008_25/1500178586456661282_156E1766	t_port: 5,000 proto: iDP ather.typs: 2,0	212
							ge t met.jp	> Jan 27, 2020 0 21	(21:52.14) Arr. 13 10.33 4 101 deat.		NON # 21:29:52-148	

Figure 102-View Metadata VOIP SessionInfo Results view

# **10 REPORTS**

The Reports tab allows the users to initiate requests for several types of reports that can be viewed and printed.

To generate a report, follow the steps below:



- 1. Select a Federated Node
- 2. Set Reports Settings(optional)
  - FilterString to be passed on to Kibana as a query filter.
  - Duration for the report data. Default Is 1 hour.
- 3. Click on one of the hyperlinks available in Reports List portion of the panel

		Report Log					
	FilterString	Timestamp	NodelP(NodeName)	UserName	ReportType	Duration	SearchFilter
derated Nodes		2020-01-28T22:40:16.938Z	10.91.170.130(nc_130)	continuum	Investigator->DashboardView	1 Hours	event_type:'http
stonMA::nc 130		2020-01-28T22:53:38.898Z	10.91.170.130(nc_130)	continuum	Augmentation->Suspicious Signatures(JA3)	1 Hours	
ZONMA::nc_130	Report Duration 1	2020-01-28T22:54:07.306Z	10.91.170.130(nc_130)	continuum		1 Hours	
huaNH::nc_113		2020-01-28T22:54:25.102Z	10.91.170.130(nc_130)	continuum	Augmentation->Suspicious Signatures(JA3)		
	🖩 Reports List	2020-01-28T22:54:54.742Z	10.91.170.130(nc_130)	continuum	Investigator->DashboardView	1 Hours	
	Investigator->DashboardView	2020-01-28T22:55:43.712Z	10.91.170.130(nc_130)	continuum	Augmentation->Malware	2 Hours	
	nivesigator->Dashboardview	2020-01-28T22:59:48.447Z	10.91.170.130(nc_130)	continuum		1 Hours	
	Augmentation->Suspicious Signatures(JA3)	2020-01-28T23:02:17.959Z	10.91.170.130(nc_130)	continuum	Augmentation->Suspicious IPAddresses	1 Hours	
	Augmentation=>Mativare Search=>Metadata Investigator=>Metadata	Click any hypericked category from the					

Figure 103-Reports Screen

- 4. A new browser tab will appear with the relevant Kibana interface.
- 5. Review data and modify the duration as needed.
- 6. From the browser's File Menu, choose Print.



#### User Guide January 30, 2020

© ←	Federation Manager x → C ▲ Not secure	Keport_Main_DB - Kibana X		-014174b50227?_g=(ref	reshInterval:(pause:!t,value:0)	),time:(from:now-1h,t	o:now))&_a=(description:",fil	- ₽0; iters:!(),full Q ☆ 🔗 🔳 🚺
<ul> <li>N</li> <li>N</li></ul>	Dashboard / Report_Main_DB           Full screen         Share           Clone         Edit           Y         Search           O         + Add filter           Network Connections		Value           C         1 famous reportungit           0         -famous rep	And (a) (A - See (a) (b) (A - See (b) (b) (b) (b) (b) (b) (b) (b) (b) (b)	0 0 +	Print Destination Pages Layout	3 pages S Save as PDF All Landscape	New tab C0+i+T New window C0+3hit+N New incognito window C0+3hit+N Hotory Downloads C0+3 Bookmarks C0+1 Bookmarks C0+1 Print_ 00% + C1 Print_ C0+6
<u>ن</u>	SourceIP = 172.16.133.6 172.16.133.6 172.16.133.6	DestIP = 8.8.8.6 8.8.4.4 172.16128.202	d     d     source     d     source     t     source     t	аналы та малалы та алалы та алалы ала ала	B6 85	More settings		Cast Find Ctrl+F More tools Edit Cut Copy Paste
9 9	17216.133.6 172.16.133.6 8.8.8.8 8.8.8.8	172.16.128.202 172.16.128.169 172.16.133.6 172.16.133.233	Tel Blanc	31,810 Abad dark 108 -	0	Paper size Pages per sheet	Letter 👻	Settings Help Exit. tormin
1	192.168.15.93 192.168.15.93 192.168.15.93 192.168.15.93	192168.16.11 192168.16.1 192168.16.7 184.26.62.130	facStorieth Higo/1131/23023021igs/dawskibidHowd21dd 1250202 K I Stribust Popel,540,54		en Balante Indenterio et die Unanzen Frist nach (La Missenskien VIII. 13) Indenterio	Margins Scale	Default 👻 Default 👻	
43 cs	192.168.15.93 192.168.15.93 <b>Top 5 HTTP Hostnames</b>	162.208.22.34 69.147.86.11		4-04 04.004         M         4           4-04 04.004         44         0           4-04 04.004         0         0           100         0         0           100         0         0           100         0         0           100         0         0	• (1) • (2) • (2)	Options	Headers and footers Background graphics	↓ Log Counts
0			112 168.16.11 - cdn.altitude-a	rena.com - ads.altitu	de-arena.com - tags.rllcll.c	com -	5 Save Cancel	<b>130,407</b> dns - Count
	Top 5 IDS Alerts	31 810		Major Services	tp (1.42%)		● smb ● http	32,942 2,392 alert - Count tis - Count
⇒		31,810 File Found over SMB -						2,120 1,765 http - Count smb - Count

Figure 104-Reports Results Screen

- 7. When a print dialog appears, choose landscape layout, and the destination to be 'Save As PDF'
- 8. Report is saved as PDF on user's system.



# **11 CONFIGURATION**

The Configuration tab is a drop down menu providing access to the following functions:

- Software Management License and Cluster management.
- Authentication User Management
- Authorization User roles and permissions.
- Auditing Rsyslog configuration, SNMP configuration, and Log Manager settings.
- View System Events Observe system events.
- Generate Report Custom Reporting

	Group Details		DS	ActiveTriggers		Suspicious Traffic		DPI	Events	Throughput	Authentic		omance
GroupName (NodeCount) BostonMA (1) NashuaNH (1)	GroupName NodeCount	Services Assets Defended Alerts	ActiveRules Undefended Alerts	Rules Events	IPAddresses IPAlerts	Domains DomainAlerts	JA3 Signatures JA3 SigAlerts	Files Emails Netflows DNS	TLS/SSL HTTP VOIP Critical	MaxGbps AvgGbps DroppedPkts	(Compared Q Auditoriz		(liput Gbps dita points to com)
	BostonMA 1	8 12 221	50659 266016	7 79	94 8023	19235 0	1526 0	17950 0 266178 130555	22 124 0 0	10 0.32 0	(42.44 TB / 7.13) 2020-01-26 01:12:54 2020-01-27 19:23:04 0	Details	1
	NashuaNH 1	8 12 2187987	50659 1116711	13 545	2 3084	19235 0	1526 0	26876 0 2632213 3	22 124 0 0	10 2.77 0	( 6588.03 TB / 12.90 ) 2020-01-26 01:12:54 2020-01-27 19:23:04 0	Details	]
	Total GroupCount: 2 NodeCount: 2	8 12 2188208	50659 1382727	13 624	94 11107	19235 0	1526 0	44826 0 2898391 130558	44 248 0 0	20.00 3.09 0	( 6630.47 TB / 20.03 ) 2020-01-26 01:12:54 2020-01-27 19:23:04 0	Overview	1
	nouceount r	2100200									0		

Figure 105-Configuration Options

### 11.1 SOFTWARE MANAGEMENT

This panel allows the user to perform license management and software update management.

#### 11.1.1 License Management

Once a license key has been forwarded, copy and paste the provided string into the License Installer in the web user interface. Note: If it is cluster enabled configuration each node needs to be licensed individually. If you do not have any data nodes, you will only need to apply the master license.



Role	UserName	Password	ConfirmPassword	Action	License Key Updar
er2 •	User Name	Password	Confirm Password	&+ Add	
Tier2	n u m			Edit &xDelete	<b>↑</b>
Tier2	= n			Edit AscDelete	
Tier1				Edit & Delete	
Tier2	han w			Edit AxDelete	
Tier2	388by			/ Edit &xDelete	
Tier2	2~9 880			/ Edit & Delete	
Tier2	-			/ Edit & Delete	
Tier2				/ Edit anDelete	
Tier2				/ Edit & Delete	

Figure 106-Configuration Master License Update function

## **11.1.2 System Information**

Clicking on Show System Info button displays a pop up window containing the following information:

- Storage capacity of the Master and enabled Cluster nodes
- Search Storage Statistics
- Memory Statistics
- Five most recent Pcap files stored
- Interfaces configured for capture

Sentry Wire	@Dashboard 🔸 Policy Se	tup 💠 Threat Hunting Workflow	Configuration	O Help -	G Logout
Master Node		Status Running License Evaluation Show System Info			
	System ID 36343638-3532-4d32-3	System Info X			
Cluster Node I	System ID 96343638-3632-4632-3:	Filesystem         Size         Used Avail UseK           MasterRode Storage         5197         517         647         108 -           ClusterModeStorage         5197         517         647         108 -           Search Storage         5197         517         647         108 -           Search Storage         5197         517         647         108 -			
	Ucense Key	procs			
Cluster Node2	System ID	List of the most recent capture files [Non Feb 4 21:09:07 UTC 2019]			
	License Key	154031453877286(1287,15403145390827836), pcop 154931453898443914,15493145390837837, pcop 154931459084220143,1540145390578379, pcop 154931453947296440,154931453908278395, pcop 1549314539428124409a,154931453908278375, pcop			
		Interfaces capable of capturing data			
		0000:17:00.0 "Ethernet Controller X710 for 1005E SFP+ 1572" drw-igb_urio unused- 0000:37:00.1 "Ethernet Controller X710 for 1005E SFP+ 1572" drw-igb_urio unused-			

Figure 107-Configuration Show System Info Button results

### 11.1.3 Cluster Management

The appliance can function as a standalone server or a cluster of servers. This allows for the expansion of data storage and computational ability of the system. Software Configuration panel displays the Master



Node and the configurable Cluster Nodes as shown below.

Master Node	Status:Running License:Evaluation Show System Info		
0	Show System mo		
License Key	532-432-3238-353130304647 Cony Update		
Cluster Node1	Status:Enabled License:Evaluation Disable Cluster Node	1	
System ID 36343638-35	532-4d32-3238-353130344233 Copy		
License Key	Update		
Cluster Node2	Status:Disabled License:Evaluation Enable Cluster Node		
System ID	Сору		
License Key	Update		

Figure 108-Cluster Node Management view

Note: By default – Cluster Nodes are disabled.

### 11.1.3.1 Enable Cluster Node

- Before enabling a data node, the user must ensure the capture server is running and the Cluster node is connected to the master node.
- When the Cluster Node1 is ready to be included in the cluster, the user must press "Enable Cluster Node" button for Cluster Node1. This will change button label to "Disable Cluster Node".
- Now the server is aware of the newly enabled Cluster Node(s).
- If these servers are enabled, up and connected the status of the respective nodes in the cluster will change to "Running".
- If Data Node1 and/or any node available are licensed, then the license label will display Permanent/Evaluation based on the license used.

#### 11.1.3.2 Disable Cluster Node

- To disable the Data Node, the user should click the "Disable Cluster Node" button for that node under the cluster tab.
- Now the disabled Cluster Node is not associated with the master.
- The node will no longer store data.

### 11.1.3.3 Software Update Management

This panel allows downloading capture software upgrades from a central server and pushing these updates to the Nodes.

User provides the URL for checking/downloading software updates and click on "Check for Update" button.



Sentry Wire	BDashbo	ard 🔹 Policy Setup 💠 Threat Hunting Workflow			Configuration	🛛 Help 👻	Logout
Master Node		Status:Running License:Evaluation Show System Info	• Software Update M	anager		Last Update:	7.3.0.309-408.12
	System ID License Key	36343636-3532-4632-3236-353130304647 CCopy	URL	., https://sharefile.example.com	Che	ck for Updates	
			Software Update L	•			
Cluster Node1		Status:Running License:Permanent Disable Cluster Node	Date 2018-12-20 22:19:01	Message url:https://sharefile.example.com/g23e333243242			
	System ID	4C4C4544-0050-5410-8034-B8C04F343832 Copy	2010-12-20 22-18-01	una nupsarsinaremet.example.com/q29033243242			
	License Key						

Figure 109-Software Update Manager view and Check for Updates button

If an update is available, "Apply Update" button is displayed. Clicking on this button updates the software.

Sentry Wire			& Configuration 🛛 Help 👻 🕞 Logout
Master Node	Status:Running License:Evaluation Show System Info	Software Update Manager	Last Update: 7.3.0.309-408.12
	System ID         365343638-3532-4d32-3238-353130304847         Copy           License Key         Update	URL e.g., https://sharefie.example.com	Check for Updates Apply Update
		Software Update Log	
Cluster Node1	Status:Running License:Permanent Disable Cluster Node	Date         Message           2018-12-20 22:19:01         url:https://sharefile.example.com/q23e333243242	
	System ID 4C4C4544-0050-5410-8034-B8C04F343832 Copy		
1	License Key		

Figure 110-Software Update Manager function and Apply Update button



# **11.2 AUTHENTICATION**

This panel allows users to choose from one of the following authentication mechanisms:

- 1. Local Authentication
  - This is the default Authentication.
  - Backward compatible with earlier versions of the software.
  - Server switches over to Local Authentication if SSO, LDAP, or other allowed/configured authentications fail.
- 2. Remote Authentication
  - This tab allows the user to switch to SSO, LDAP, Radius or other allowed/configured authentication modes.
  - Note: Only one authentication mode can be active at a given time.

### 11.2.1 Local Authentication

Local authentication is used to manage local users.

# 11.2.1.1 Adding Users

Perform the following to add a new user:

- 1. Select the role for the user being created from the drop down
  - a. Roles are created and assigned through Configuration→ Authorization tab. Please refer to section 9.3 for more details.
- 2. Enter Username and Password for the new user
- 3. Retype and confirm the password
- 4. Click on the Add button.
- 5. Once the user is added, the users list is refreshed to show the newly added user. This may take few seconds.

SentryWire #Dashb	oard 🛛 🔦 Policy Setup 👁 Investigator	Q Search 🚨 View Metadata		Reports Configuration O Help G Logo			
cal Autoentication Remote Autoentication							
	ger; one or more lower case letters, one or more upper c 5 Note: \$ is not allowed as the first character.	ase letters, one or more these special characters					
Role	UserName	Password	ConfirmPassword	Action			
Admin •	User Name	Password	Confirm Password	2+ Add			
Admin	continuum			✓ Edit ▲xDelete			
Search Manager	User1234			🖋 Edit 🤹Delete			

Figure 111-Add Users view

### 11.2.1.2 Activate Local Authentication Mode

This button appears on the Authentication  $\rightarrow$  Local screen only if the currently logged user is not a local user. If the current user is a LDAP, SSO or Radius user and wants to change back to a local user the user is presented with "Activate Local Authentication Mode" button. Clicking on this button, closes any active connection to LDAP, SSO or Radius server. The user can login again using the local user from the local database.



#### Note:

- In case of any failure, the user automatically falls back to the local user.
- At a given time only one authentication mode is active. If the user wants to change to a different authentication mode, the user has to first fall back/activate the local mode, re-login as local user and then activate desired authentication mode. Once the new authentication is activated, the user can now logout as local user and login back using the newly activated authentication mode.

Sentry Wire	Sentry Wire & Dashboard & Policy Setup & Threat Hunting Workflow & Configuration @ Help • @ Logout									
Local Authentication Remote Auth	hentication									
	rs or longer; one or more lower case letters, one or more u I@#&* Note: \$ is not allowed as the first character.	oper case letters, one or more these special characters								
Role	UserName	Password	ConfirmPassword	Action						
Admin •	User Name	Password	Confirm Password	<b>å</b> + Add						
Admin	continuum									
Search Manager	User1234			Sedit Edit						
		Activate	Local Authentication Mode	This button appears only if the current user is not a local user						

Figure 112-Activate Local Authentication Mode button view

## **11.2.1.3 Deleting Users**

Perform the following to delete a user:

- 1. To delete a user, click on the Delete button of the user to be deleted.
- 2. Once a user has been deleted, this username and password cannot be used for either UI login or REST login.
- 3. To delete an existing user, you must be logged in to the system as admin.

#### *Note*:

• Any user who is currently logged into the system cannot be deleted.

Sever Management								
Password requirements: 8 chars or longer; one or more lower case letters, one or more upper case letters, one or more these special characters Allowed special characters are 1@#4:\$ Note, \$ is not allowed as the first character.								
Role	UserName	Password	ConfirmPassword	Action				
Admin •	User Name	Password	Confirm Password	<b>4</b> ≠ Add				
Admin	continuum			Zdit AscDelete				
Search Manager	User1234			✓ Edit AscDelete				

Figure 113-User Management Delete User Button view



Role	UserName	Password	ConfirmPassword	Action	License Key Updat
er2 •	User Name	Password	Confirm Password	&+ Add	
Tier2	n u m			/ Edit AnDelete	_
Tier2	= 12			/ Edit astDelete	
Tier1				/ Edit & Delete	
Tier2	tura m			/ Edit & Delete	
Tier2	Male <sub>2</sub>			Edit AstDelete	
Tier2	2~9 880			Fedit AscDelete	
Tier2	-			ZEdit BeDelete	
Tier2	-			Fedit & Delete	
Tier2	0× 5 P			Edit AnDelete	

Figure 114-User Management Delete User Button view

# 11.2.1.4 Modifying Users

1. To modify a password for a user click the Edit button for that user.

a Automatication Renote Automatication ©User Munargement associations: 6 datass of longing on or more longer case letters, one or more these special characters								
	Note: \$ is not allowed as the first character.	ен сазе нецена, отле от плоте штезе зрескої спонахлена.						
Role	UserName	Password	ConfirmPassword	Action				
Admin •	User Name	Password	Confirm Password	Add				
Admin	continuum			✓ Edit acDelete				
Search Manager	User1234			Edit Edit				

Figure 115-Manage Users Modify/Edit User button

2. Enter a new password and confirm password. Click save.

Sentry Wire	Sentry Wire & Dashboard 🖈 Policy Setup & Threat Hunting Workflow & Configuration 🛛 Help - 🗇 L								
User Management Password requirements: 8 chart	Password requirements: 8 chars of longer; one or more lower case letters, one or more typer case letters, one or more these special characters. Allowed special characters are 1@#4:5% Alder, \$ is not ellowed as the first character.								
Role	UserName	Password	ConfirmPassword	Action					
Admin •	User Name	Password	Confirm Password	Add					
Admin	continuum			ZEdit ArDelete					
Search Manager	User1234	New Password	New Confirm Password	Save Cancel ExDelete					

Figure 116-Manage Users Change Password button

*Note*:

- Only Tier2 user can modify the password for a user (including himself or another Tier2(admin)/Tier1(Guest))
- If the user is currently logged into the session, he should be prompted to login again with the new password. The previous login session is no longer valid.



# 11.2.1.5 Unlock User

To unlock a user login to the system as admin. Click on the unlock button for that user.

🔊 Sentry W	/ire 🚯 Dashboard 🐟 P	olicy Setup 💠 Threat Hunting	QMessaging 🌣 Configura	tion 🕜 Help 👻 🕞 Logout		
	acnt 8 chars or longer; one or more lower case let rs arc /#8#4*\$ Note: \$ is not allowed as the	Master License     System ID 4C4C4544-0059-4610-8034-	Evaluation C2C04F503232 Copy			
Role	UserName	Password	ConfirmPassword	Action	License Key	Update
Tier2 •	User Name	Password	Confirm Password	Add		
Tier2	continuum			/ Edit		
Tier1	Test1234			Edit AcDelete UnLock		

Figure 117-Manage Users Unlock User button

# 11.2.2 Remote Authentication

Use Remote Authentication to configure and enable SSO, LDAP, or Radius authentication methods.

Sentry Wire &Dashboard < Policy Set	🍄 Configuration 🛛 Help 👻 🕞 Logout			
Local Authentication Remote Authentication	Enter the necessary details			
≣ SSO Configuration	and click "Activate"	Radius Configuration	■ PKI Configuration	
Server IP	Server IP	Server IP	Certificate Data	
eg192.168.1.1	og_192.168.1.1	eg_192.168.1.1	Copy/Paste the certificate to be uploaded.This must correspond to the private key entered below.	
UserName	Port	Port	entres below.	
User Name	cg.,389	cg_1812		
Password	UserName	UserName		
Password	User Name	User Name		
Realm	Realm Password			
Realm Name	Password	Password		
ClientID	CommonName	Secret		
ClientID	commoname	Secret	Private Key	
	DomainComponent		CopylPaste the corresponding private key to be uploaded. This must correspond to the certificate data entered above.	
	domaincomponent			
	DomainComponent			
	domaincomponent			
Activate SSO Reset Fields	Activate LDAP Reset Fields	Activate Radius Reset Fields	Upload PKI Certificate Reset Fields	

Figure 118-Remote Authentication Configuration view

*Note*:

- In case of any failure, the user automatically falls back to the local user.
- At a given time only one authentication mode is active. If the user wants to change to a different authentication mode, the user has to first fall back/activate the local mode, re-login as local user and then activate desired authentication mode. Once the new authentication is activated, the user can now logout as local user and login back using the newly activated authentication mode.



#### 11.2.2.1 Activate SSO Authentication

- Enter SSO server IP address, UserName, Password, Realm, and ClientID.
- Click "Activate SSO" button and confirm.
- If the SSO IP Address, username, password are valid for the specified Realm and Client, the Node server switches to SSO mode.
- User must log out and log back in using the SSO credentials.

## 11.2.2.2 Activate LDAP Authentication

- Enter LDAP server IP address, Port, UserName, Password, CommonName, and DomainComponent.
- Click "Activate LDAP" button and confirm.
- If the LDAP IP Address, Port, UserName, Password, CommonName, and DomainComponent are valid, the Node server switches to LDAP mode.
- User must log out and log back in using the LDAP credentials.

## 11.2.2.3 Activate RADIUS Authentication

- Enter RADIUS server IP address, Port, UserName, Password, and Secret.
- Click "Activate Radius" button and confirm.
- If the RADIUS IP Address, Port, UserName, Password, and Secret are valid, the Node server switches to RADIUS mode.
- User must log out and log back in using the RADIUS credentials.

# 11.2.2.4 Mapping a role to a RADIUS user

The Map Role button allows mapping Radius users to roles defined via Authorization tab.

Sentry Wire &Dashboard A Policy Setu	☆ Threat Hunting Workflow				🌣 Configuration 🛛 Help 👻 🕞 Logout	
Local Authentication Remote Authentication						
III SSO Configuration	III LDAP Configuration			₩ PKI Configuration		
Server IP	Server IP eg.,102.168.1.1	Map Radius User	to a Role 2	9	Certificate Data CopyPatile the certificate to be uploaded. This must correspond to the private key entered below.	
UserName UserName Password	eg.,309	Enter User Na oleName Admin	ime to be mapped			
Password Realm Pastm Name	Password + Curr	Map Role Cancel + Current Radius User Role Assignment				
CilentiD	CommonName	UserName RoleName			Private Key	
	DomainComponent domaincomponent	nancy	Admin 💼		CopylPaste the corresponding private key to be uploaded. This must correspond to the certificate data enforced above.	
	DomainComponent domaincomponent	testuser testuser.1 P	Guest 💼			
		testuser.5 P	olicyManager			
Activate SSO Reset Fields	Activate LDAP	Reset Fields	Activate Radius Map Rol	Reset Fields	Upload PKI Certificate Reset Fields	

Figure 119-Mapping a Role to a RADIUS user

- Click on the "Map Role..." button.
- Enter radius UserName.
- Choose a RoleName from the drop-down list of available roles and click on "Map Role" button to map a radius user to the role.



- The newly assigned role and username are displayed as a list for quick reference. To delete a role mapping, simply click on the delete icon next to the role.
- When a radius user logs into the capture UI, the capture server checks the role status and use the assigned role to determine the authorization level of the user. If the signed in user us not mapped to a role, the capture server assigns "Guest" role.

# 11.2.2.5 Upload PKI Certificate

This panel allows PKI (Public Key Infrastructure) certificate to be uploaded to be used by the application web server. Copy and Paste Certificate data and Private key data into text areas shown below and press Upload PKI Certificate button. If the certificate and private key are valid and md5sums match, the server will restart with the new certificate. The user must login again.

Local Authentication Remote Authentication							
SSO Configuration	IDAP Configuration	I Radius Configuration	E PKI Configuration				
Server IP	Server IP	Server IP	Certificate Data				
og.,192.168.1.1	eg.,192.168.1.1	eg.,192.168.1.1	Copy/Paste the certificate to be uploaded.This must correspond to the private key entered below.				
UserName	Port	Port	Shourse Derow.				
User Name	cg.389	cg_1812					
Password	UserName	UserName	-				
Password	User Name	User Name					
Realm	Password	Password					
Realm Name	Password	Password					
ClientID	CommonName	Secret					
ClientID	commoname	Secret	Private Key				
	DomainComponent		Copy/Paste the corresponding private key to be uploaded. This must correspond to the certificate data entered above.				
	domaincomponent						
	DomainComponent						
	domaincomponent						
Activate SSO Reset Fiel	ds Activate LDAP Reset Fields	Activate Radius Reset Fields	Upload PKI Certificate Reset Fields				

Figure 120-Upload PKI Certificate view

### **11.3 AUTHORIZATION**

Authorization tab allows adding new roles and setting permissions for each role. When a user is assigned a role, the node UI menus are enabled/disabled based on the permissions of the role. Once created these roles are provided as a dropdown list for each of the authentication modes under the Authentication tab and can be assigned to a user at the time of user creation.



### Note:

- Authentication permission controls Authentication tab
- Licensing permission controls Software management tab and licensing.
- DeleteSearch permission can Delete Searches.
- Auditing permission controls Auditing features.
- Dashboard permission controls all dashboard features.
- Policy permission controls Policy menu items and Authorization tab.
- Default role "Admin" and "Guest" cannot be modified.
- Guest role allows view only permission
- Policy permission DOES NOT control Authentication, Licensing, Delete Search, Auditing, or Dashboard.
- To add a role click on the "Add Role" button at the top right of the panel.

							+ Ada
Role Name	Dashboard	Policy	Licensing	Authentication	Auditing	DeleteSearch	Actions
Admin	2	8	8	2	92	8	
Guest	6		8	8	<b>a</b>	0	
				Add Role	×		
			Role Name	Manager			
			0	Note: Only Alphanumeric characters allo	bwed		
			Add Role	Cancel			
					-		

Figure 121-Authorization Add Role button

- Once a role is created assign the permission by checking the boxes.
- Click "Apply"
- Once created these roles are provided as a drop down list for each of the authentication modes under the Authentication tab and are available to be assigned to the users.



Roke         Dothoad         Policy         Losensign         AuthenCation         Authe								+ Ad
Cuest         Cuest <th< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Actions</th></th<>								Actions
					1796			
Nenger		3385		(enc)		22017		(Incompany)
	Manager		U	U	W		8	Apply

Figure 122-Authorization Apply Role button

### 11.3.1 SSO, LDAP and RADIUS Authorization

Capture server platform honors any role associated with users created via SSO, LDAP or RADIUS authentication modes. If this role is not defined as part of the Authorization in the capture application, any user associated with this role will have READ-ONLY access to the application.

This role must be added to the application via the Authorization panel and assigned the desired permissions. From here on, any user with this role will be authorized to access the functions based on the permissions assigned.

*Note*: It is advisable to create required roles and assign permissions via the Authorization panel before logging in to the application as a SSO, LDAP, or RADIUS user.

### Use Case:

When a user logs in with an authentication mode other than the Local and has permission to only view the content of the application, there may be two scenarios:

<u>Scenario1</u>- The role of the user exists in the capture application but has "read-only" permission to all the functions of the application. In this case, the user must request an Admin user to login and modify the permissions of the role.

<u>Scenario 2</u>- The role of the user does not exist in the capture application. In this case, the user must request an Admin user to create the role and assign permissions to the role.

In either scenario, the user must logout and log back in for the authorization changes to take effect.



# 11.4 AUDITING

Auditing has three separate functional groups: Rsyslog configuration, SNMP configuration, and Log Manager settings. Each of these can be configured independent of the other. Two Rsyslog server settings can be provided for high-availability. Similarly, two SNMP server can be provided for high-availability.

SentryWire &Dashboard < Policy Setup & Threat Huntin	ng Workflow		Configuration	0 Help 👻	🕩 Logout
≣ Syslog Server1	SNMP Server1	Elogging Options			
IP Address	IP Address	Logging Resource			
10.91.170.191	10.01.170.181	Critical Events			
Port	Port	Alerts			
514	162	Search			
Update Frequency (Seconds)	Update Frequency (Seconds)	StorageInfo			
10	10	Active Trigger Events			
Configure	Configure	-			
Reser		Upload Data			
III Syslog Server2	SNMP Server2	Download Data			
IP Address	IP Address				
10.01.170.114	10.01.170.179				
Port	Port				
514	162				
Update Frequency (Seconds)	Update Frequency (Seconds)				
10	10				
Configure	Configure	Set			Reset

Figure 123-Auditing Function view

Each of the syslog servers can be setup to receive syslog messages at the configured frequency. Reset button on each panel removes the Syslog server setting. (Refer to Appendix A for Syslog server setup) Each of the SNMP servers can be setup to receive SNMP traps. Reset button removes on each panel the SNMP server setting.

Logging options panel shows options to enable/disable logging for different functions:

- Critical Events this is always enabled, cannot be disabled. Log all critical events such as disk space full, critical component failure
- Alerts this is always enabled, cannot be disabled. Suricata rule-based alerts of any severity
- Search Log events for create/delete/cancel search, search completion, pause, resume.
- StorageInfo Log events to show how much of Capture Storage is used/free, Search Storage is used/free.
- Active Trigger Events Log active trigger events
- Upload Data Log every upload file action from the UI (Upload search back rules, upload critical IPs and so on)
- **Download Data** Log Download actions from the UI (Download PCAP data, Download searchback rules and so on)

### **11.5 SYSTEM EVENTS**

The System event tab displays the Timestamp, Type and associated Message with severity. All events are clickable and searchable.



#### Severity can be one of three values: 1: Severe, 2: Warning, 3: Informational

<b>Q</b> Search Logs	Federated Nodes	SystemEvents: nc_113		QFind Text Copy to ClipBoard Download CRefresh Page		
egin Time	BostonMA::nc_130	-		Page Size         500         •         e Prev         1         Next »		
2020-01-28 00:05:59 nd Time		TimeStamp	Type	Message	Severity	
2020-01-28 00:35:59		2020-01-28 00:25:42	Search	Completed,Name=fms_2020_01_27_19_25_23_77, Filter=PcapData,tcp or udp,	3	
og Search Filter [?]		2020-01-27 22:45:05 2020-01-27 22:45:05	ActiveTrigger ActiveTrigger	Leaded,tcp Leaded,udp	3	
eturn only events that have the supplied pattern(s) ax Rows		2020-01-27 22:45:05 2020-01-27 22:45:05	ActiveTrigger ActiveTrigger	Loaded,host 10.91.170.22 and port 38638 and host 204.11.16.106 and port 25 and tcp Loaded, (host 10.0.2.20 and port 5060 and host 10.0.2.15 and port 5060 )	3	
2000 C Search Logs		2020-01-27 22:45:05 2020-01-27 22:45:05	ActiveTrigger ActiveTrigger	Loaded, host 10.91.170.22 and port 38638 and host 204.11.16.106 and port 25 and tcp Loaded, ( host 10.0.2.20 and port 5060 and host 10.0.2.15 and port 5060 )	3	
		2020-01-27 22:45:05 2020-01-27 22:45:05	ActiveTrigger ActiveTrigger	Loaded.tcp Loaded.host 192.168.5.6 and port 50121 and host 169.44.67.161 and port 80 and tcp	3	
		2020-01-27 22:45:05	ActiveTrigger ActiveTrigger	Loaded,host 192,168.5.6 and port 50121 and host 169.44.67.161 and port 80 and tcp Loaded tcp or udp	3	
		2020-01-27 22:45:05	ActiveTrigger	Loaded, port 80	3	
		2020-01-27 22:45:05 2020-01-27 22:44:37	ActiveTrigger PreCaptureFilter	Loaded.tcp or udp 2.0,Continuum,Changed.tcp	3	
		2020-01-27 22:18:43 2020-01-27 21:15:33	CaptureServer CaptureServer	Started 2.0.Continuum.Stopped	3	
		2020-01-27 21:07:47	PacketCapture	NoNetworkTraffic,Review troubleshooting guide or check capture interface cabling, correct span/tap ports	3	
		2020-01-27 19:13:14 2020-01-27 19:10:02	Search Search	Completed Name=fms_2020_01_25_19_32_11_280_0/622_f11zv, Filter=PcapData.tcp or udp, Completed Name=fms_2020_01_25_19_32_11_280_0/622, Filter=PcapData.tcp or udp,	3	
		2020-04-07-40-40-24	Caarah	Completed Managemen, DD fine, 2020, 04, 05, 40, 20, 44, 200, entries, Elitery-Bane Date ten	2	

Figure 124-Node System Events view

#### 11.5.1 Generate Report

The Generator Report tab allows the user to specify various parameters for generating reports that can be downloaded for review and analysis.

🔊 Sentry Wi	re @Dashboard	🛠 Policy Setup 💠	Threat Hunting Workflow		Configuration	🕜 Help 🝷	🕞 Logout
CReport Generator				Report Details			
Report Name				Report Name			
Report_2019_8_26_12_40_7	_continuum			Report_2019_8_26_12_40_7_continuum			
* Begin Time ( YYYY-MM-DD	HH:MM:SS Capture Server Time	.)		Begin Time			
2019-06-20 23:38:00				2019-06-20 23:38:00			
• End Time ( YYYY-MM-DD)	HH:MM:SS Capture Server Time	)		End Time			
2019-03-21 16:49:07				2019-03-21 16:49:07			
Log Search Filter (Default: Bl	ank => No Filter)			Log Search Filter			
80\192.168.1.100				80/192.168.1.100			
Output Categories Chee	ck All			Output Categories			
ThreatIPs	✔ Alerts	Assets	Search Performance	ThreatIPs,Alerts,SearchPerformance,HTTP,TLS,CompletedSearches,NetFlows			
✓ HTTP	TLS	DNS	Completed Searches	Export Format			6
Emails	NetFlows	File Logs		JSON			
Active Triggers	System			Message			
Export Format	JSON	i csv	) XML				
							6
Generate Re	eport		Reset Fields	Download Report			

Figure 125-Report Generator view

- Report Name System provides a default used name based on the current time. This can be edited to provide a suitable name.
- Begin/End time The report output is restricted to the events and alerts between the times specified in these fields.
- Log Search Filter The report output can be further restricted by log search filter. The rules of the Linux *grep* command's search string apply to this field.



# Use Case

OR condition:

• *pattern1* || *pattern2* returns strings that have either pattern1 OR pattern2 or both.

*For example*: *google*\|*Microsoft* search filter returns strings like the ones shown below. This filter skips any string that does not include neither google nor Microsoft.

- $\circ$  google may have been the first to implement this technology.
- o Microsoft is not too far behind.
- Both google and Microsoft are fighting to take market share.

AND condition:

• *pattern1*. \**pattern2* returns strings that contain pattern1 before pattern2 in a string. It does not return strings that have pattern2 before pattern1.

*For example: google*.\**Microsoft* search filter will return strings such as follows: • Both google and Microsoft are fighting for market share

- The above string skips the following sentences:
  - o google has not commented on the news. (only *pattern1*, no *pattern2*)
  - Microsoft and google are fighting for market share (*pattern2* followed by *pattern1*)
- Output Categories Allows user to select different types of event and alert data to be included in the report.
- Export Format By default format is JSON. User can also specify the output to be in XML or CSV format.

To generate a report, user must click the "Generate Report" button, once the required fields are filled. The server will generate a *<ReportName>.zip* file that includes one file for each selected category. This zip file can be downloaded by clicking on Download Report button.

# **12 NETWORK CONFIGURATION**

In order for this application to be accessible remotely, an IP address must be assigned to one of the Ethernet ports (typically eth0, eth1, or eth2). For initial configuration you may need to connect a VGA compatible monitor, boot up the system locally, login, and configure a static or DHCP IP address for your own network. After starting the system login as the root user (username: root, password: Contact support for default password to access the system or to change the password.)

**<u>Remote Login:</u>** After setting up an IP address locally, you can perform future operating system administrative functions by remote login via an SSH client. Configure your SSH client to connect using port 22.

### Network Settings

Protocol

Description



DHCP	<ul> <li>RHEL/CentOS, edit the following settings at: "/etc/sysconfig/network-scripts/ifcfg-eth2" (or eth3, etc.).</li> <li>BOOTPROTO=dhcp</li> <li>NM_CONTROLLED=yes</li> </ul>
	ONBOOT=yes
	<ul> <li><i>For example</i>: edit the following settings at: "/etc/sysconfig/network-scripts/ifcfg-eth2" (or ifcfg-eth3, etc.).</li> <li>BOOTPROTO=static</li> </ul>
	• BROADCAST=192.168.1.255
Static	• DNS1=75.75.75.75
IP	• DNS2=75.75.76
	• GATEWAY=192.168.1.2
	• IPADDR=192.168.1.1
	• NETMASK=255.255.255.0
	NM_CONTROLLED=yes
	• ONBOOT=yes



# **APPENDIX A: CLIENT SYSLOG CONFIGURATION PROCEDURES**

1. Edit /etc/rsyslog.conf

[root@client ~]# vi /etc/rsyslog.conf

2. At the end of file place the following line to point the client message log to the server

\*.info;mail.none;authpriv.none;cron.none @192.168.0.105

Note: Optionally choose hostname or IP address.

3. Restart the syslog service

[root@client ~]# service rsyslog restart

Message logs are now sent to both the central log server and local log files.

4. Verify Firewall Port opening(optional)

Generally production environments are protected by a hardware firewall. The following ports need to be opened: TCP & UDP 514. Verify the port opening by issuing the following command from the client:

```
[root@client ~]# telnet 192.168.0.105 514
Trying 192.168.0.105...
Connected to 192.168.0.105.
Escape character is '^]'.
```

If telnet is not available, use ssh to verify communications with server on port 514.

```
[root@localhost ~]# ssh -p 514 -v root@10.91.170.20
OpenSSH_5.3p1, OpenSSL 1.0.1e-fips 11 Feb 2013
debug1: Reading configuration data /etc/ssh/ssh config
debug1: Applying options for *
debug1: Connecting to 10.91.170.20 [10.91.170.20] port 514
debug1: Connection established
debug1: permanently set uid: 0/0
debug1: identify file /root/.ssh/identify type -1
debug1: identify file /root/.ssh/identify-cert type -1
debug1: identify file /root/.ssh/id rsa type -1
debug1: identify file /root/.ssh/id rsa-cert type -1
debug1: identify file /root/.ssh/id dsa type -1
debug1: identify file /root/.ssh/id dsa type -1
debug1: identify file /root/.ssh/id dsa type -1
debug1: identify file /root/.ssh/id dsa-cert type -1
debug1: identify file /root/.ssh/id ecdsa type -1
```

5. To test that it is working perform the following command, and then confirm a record of the command restart is recorded in the logs:



[root@client~]# service ntpd restart Shutting down ntpd: [OK]

Verify that similar messages appear in /var/log/messages Client:

Aug 18 20:10:33 R730-2 ntpd[40092]: 0.0.0.0 c016 06 restart Aug 18 20:10:34 R730-2 ntpd[40092]: 0.0.0.0 c012 02 freq\_set kernel 4.085 PPM

Server:

Aug 18 20:10:33 R730-2 ntpd[40092]: 0.0.0.0 c016 06 restart Aug 18 20:10:33 R730-2 ntpd[40092]: 0.0.0.0 c012 02 freq\_set kernel 4.085 PPM

# APPENDIX B: LEEF MESSAGE FORMAT

The syslog messages are generated and reported in the format

<DateTime> <localhost> LOGMSG: 2.0| OrgName |BrandName |Version|<ID>|cat=<category> msg=<message>

*For example*: when capture server starts on the localhost, the following syslog message is added to /var/log/messages file:

Jan 06 22:27:49 localhost LOGMSG: 2.0| OrgName | BrandName|Version| Started |cat= PacketCapture LOGMSG: 2.0| OrgName|BrandName|Version| Changed |cat=PrecaptureFilter msg= <text> - This event is generated when a PreCapture filter is added or updated.

LOGMSG: 2.0| OrgName|BrandName|Version| Reset |cat=PrecaptureFilter msg<text> This event is generated when a PreCapture filter is deleted.

LOGMSG: 2.0| OrgName|BrandName|Version|Loaded|cat=ActiveTrigger msg <text>-This event is generated when an active trigger is added.

LOGMSG: 2.0| OrgName|BrandName|Version| Updated |cat=ActiveTrigger msg <text>- This event is generated when an active trigger is updated.

LOGMSG: 2.0| OrgName|BrandName|Version| Deleted|cat=ActiveTrigger msg <text>- This event is generated when an active trigger is deleted.

LOGMSG: 2.0| OrgName|BrandName|Version|Triggered|cat=ActiveTrigger msg <text>- This event is generated when an active trigger is fired.

LOGMSG: 2.0| OrgName|BrandName|Version| Created|cat= Search msg <text>- This event is generated when a search is created.

LOGMSG: 2.0| OrgName|BrandName|Version| Completed|cat= Search msg <text>- This event is generated when a search is completed.

LOGMSG: 2.0| OrgName|BrandName|Version| Deleted|cat= Search msg <text>- This event is generated when a search is deleted.

LOGMSG: 2.0| OrgName|BrandName|Version| Cancelled|cat= Search msg <text> - This event is generated when a search is cancelled.

LOGMSG: 2.0| OrgName|BrandName|Version| Failed|cat= Search msg="Search storage full. Remove old search data and try again" - This event is generated when a search storage is full.

LOGMSG: 2.0| OrgName|BrandName|Version| Pause|cat= Search msg="Search storage full. Remove old search data. Search will automatically resume after old search data removed." - This event is generated when an ongoing search pauses because the search storage is full.

LOGMSG: 2.0| OrgName|BrandName|Version| Resume|cat= Search msg="Search resumed as the storage space freed up" - This event is generated when a currently paused search resumes as the user has freed up search storage space by deleting old search(es).

LOGMSG: 2.0| OrgName|BrandName|Version| SessionReset|cat= Admin - This event is generated when a user with Admin privilege has pressed the "Reset Session" button.

LOGMSG: 2.0| OrgName|BrandName|Version|UserAdded|cat= Admin- This event is generated when a user new user has been added.

LOGMSG: 2.0| OrgName|BrandName|Version| UserDeleted|cat= Admin- This event is generated when an existing user has been deleted.



LOGMSG: 2.0| OrgName|BrandName|Version| UserError|cat= Admin -This event is generated when an error occurred on adding/updating/deleting a user.

LOGMSG: 2.0| OrgName|BrandName|Version| UserChanged|cat= Admin -This event is generated when an existing user's password or role has been changed.

LOGMSG: 2.0| OrgName|BrandName|Version| UserLocked|cat= Admin - This event occurs to alert that a user has been locked after 3 unsuccessful attempts to login with a span of 30 minutes

LOGMSG: 2.0| OrgName|BrandName|Version| UserUnlocked|cat= Admin - This event occurs to alert that a previously locked user has been unlocked by an Admin user or 30 minutes have elapsed since the user has been locked.

LOGMSG: 2.0| OrgName|BrandName|Version|Demo|cat=Licensing msg <text> - This event is generated to alert that the license that has been applied is a Demo license.

LOGMSG: 2.0| OrgName|BrandName|Version| Expired|cat=Licensing msg <text> -This event is generated to alert that the license has expired.

LOGMSG: 2.0| OrgName|BrandName|Version| Permanent|cat=Licensing msg <text> -This event is generated to alert that the license that has been applied is a Permanent license.

LOGMSG: 2.0| OrgName|BrandName|Version| HyperThreading NotEnabled|cat=PacketCapture msg ="Warning: HyperThreading must be enabled." - This event is generated to alert that hyper threading has not been enabled as it is a requirement for successful operation of a capture server.

LOGMSG: 2.0| OrgName|BrandName|Version| Started|cat=PacketCapture - This event is generated to alert that capture server has been started.

LOGMSG: 2.0| OrgName|BrandName|Version| Stopped|cat=PacketCapture - This event is generated to alert that the capture server has been stopped.

LOGMSG: 2.0| OrgName|BrandName|Version| NoNetworkTraffic|cat= PacketCapture msg="Review troubleshooting guide or check capture interface cabling, correct span/tap ports"- This event is generated to alert that the capture server is not receiving any traffic at the moment.

LOGMSG: 2.0| OrgName|BrandName|Version| CaptureStats |cat= PacketCapture msg="LOGMSG: 2.0| OrgName|BrandName|Version| PacketCapture|cat=CaptureStats msg=Throughput:7.71, PacketsPerSec:1357894, TCP:1357794, UDP:100, Other:0, CompressionRatio:1.21" - This is a stat reporting event, occurs once every minute.

LOGMSG: 2.0| OrgName|BrandName|Version|System|cat=RootFileSystem msg=WARNING: / file system usage is above 70%.0..the system will be shut down if above 90%

LOGMSG: 2.0| OrgName|BrandName|Version|CaptureServerSetup|cat=System msg=WARNING: One or more directories/symlinks are invalid. Please contact support.



# **APPENDIX C: PCAP PORT INFORMATION**

The following list of TCP ports need to be opened for external access on a PCAP master:

- 4477 ssh port
- 41395 WEB UI access
- 41392 PCAP REST API access

In Clustered environments, the following list of TCP ports must be opened for <u>**Data Node**</u> access on a PCAP master:

- 41391, 41393 through 41396 data node send node status, license info, system usage info and search lists and search data
- 41500 data node send node status, license info, system usage info and search lists and search data

In case of Cluster, the following list of TCP ports must be opened for PCAP <u>Master Node</u> access on EACH PCAP data node:

- 4477 ssh port
- 5000 through 5021 PCAP master sends PCAP data and status requests. All of these ports must be open

Note: All the ports mentioned above are TCP.

*Note*: *There should be no ports open for external access on a PCAP data node.* 



# **APPENDIX D: BPF FILTER**

Berkeley Packet Filter (BPFs) are a raw interface to data link layers in a protocol independent fashion. They are a powerful tool for intrusion detection analysis. Using them will allow the user to quickly drill down specific packets to see and reduce large packet captures down to the essentials.

The BPF syntax consists of one or more primitives. Primitives usually consist of an id(name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

#### type

qualifiers say what kind of thing the id name or number refers to. E.g., host, net, port, port range. If there is no qualifier, host is assumed

#### dir

qualifiers specify a particular transfer direction to and/or from id. Possible directions are src,dst,src or dst. E.g., dst net 128.3

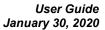
#### proto

qualifiers restrict the match to the particular protocol. Possible protocols are: ether, fddi,tr, wlan, IP, IPv6, arp, rarp, decnet, tcp and udp.

#### **Primitive Filters**

Allowable primitives are given below for reference:

Primitive Filters	Description
[src dst] host <host> E.g., src host &lt;<i>host&gt;</i> dst host &lt;<i>host&gt;</i> host &lt;<i>host&gt;</i> IP host &lt;<i>host&gt;</i></host>	<ul> <li>Matches a host as the IP source, destination, or either.</li> <li>These host expressions can be used in conjunction with other protocols like IP, arp, rarp or ip6</li> </ul>
ether [src dst] host <ehost> E.g., ether host <mac> ether src host <mac> ether dst host <mac></mac></mac></mac></ehost>	Matches a host as the Ethernet source, destination, or either





Primitive Filters	Description
[src dst] net < <u>network</u> >	Matches packets to or from source/destination or either, residing in a network.
E.g., dst net 192.168.1.0 src net 192.168.1	
dst net 172.16	An IPv4 network number can be specified as:
src net 10	• Dottedquad(e.g., 192.168.1.0)
net 192.168.1.0 net 192.168.1.0/24	<ul> <li>Dotted triple (e.g., 192.168.1)</li> <li>Dotted pair (e.g., 172.16)</li> </ul>
src net 192.168.1/24	<ul> <li>Or single number (e.g., 10)</li> </ul>
[src dst] net <network> mask <netmask> or</netmask></network>	Matches packets with specific netmask. /len can also be specified to capture traffic from range of IP addresses.
[src dst] net <network>/<len> E.g., dst net 192.168.1.0 mask 255.255.255.255 or</len></network>	• Netmask for dotted quad (e.g.,
dst net 192.168.1.0/24 src net 192.168.1 mask 255.255.255.0 <b>or</b>	<ul><li>192.168.1.0) is 255.255.255.255</li><li>Netmask for dotted triple (e.g.,</li></ul>
src net 192.168.1/24	192.168.1) is 255.255.255.0
dst net 172.16 mask 255.255.0.0 src net 10 mask 255.0.0.0	• Netmask for dotted pair (e.g.,172.16) is 255.255.0.0
	• Or single number (e.g.,10) is 255.0.0.0
[src dst] port <port> or</port>	Matches packets sent to/from port
[tcp udp] [src dst] port <port> e.g., src port 443 dst port 20</port>	• Protocols (e.g., tcp/udp/IP etc.) can be
port 80	applied to a port to get specific results
[src dst] portrange <p1>-<p2> or</p2></p1>	Matches packets to/from a port in the given
[tcp udp] [src dst] portrange <p1>-<p2> E.g., src portrange 80-88</p2></p1>	<ul><li>Protocols can be applied to port range to</li></ul>
tcp portrange 1501-1549	filter specific packets within the range
less <length> E.g., less 300</length>	Matches packets less than or equal to length
greater <length> E.g., greater 301</length>	Matches packets greater than or equal to length
(ether ip ip6) proto <protocol> E.g., ether proto 0x888e IP proto 50</protocol>	<ul> <li>Matches an Ethernet, IPv4, or IPv6 protocol</li> <li>Protocol can be a number or name. (Except for named protocols that bpf is aware of such as icmp, tcp, udp,dns, etc)</li> </ul>
(ip ip6) protochain <protocol> E.g., ip6 protochain 6</protocol>	Matches IPv4, or IPv6 packets with a protocol header in the protocol header chain
(ether ip) broadcast	Matches Ethernet or IPv4 broadcasts



Primitive Filters	Description
(ether ip ip6) multicast E.g., ether[0] & 1 != 0	Matches Ethernet, IPv4, or IPv6 multicasts
<ul> <li>vlan [<vlan>]</vlan></li> <li>E.g., vlan 100 &amp;&amp; vlan 200</li> <li>(filters on vlan 200 encapsulated within vlan 100)</li> <li>vlan &amp;&amp; vlan 300 &amp;&amp; IP</li> <li>(filters IPv4 protocols encapsulated in vlan 300 encapsulated within any higher order vlan)</li> </ul>	Matches 802.1Q frames optionally with a VLAN ID of vlan
mpls [ <label>] o E.g., mpls 100000 &amp;&amp; mpls 1024</label>	Matches MPLS packets, optionally with a label of label
(filters packets with outer label 100000 and inner Label 1024) o mpls && mpls 1024 && host 192.9.200.1(filters packets to and from 192.9.200.1 with an inner label of 1024 and any outer label)	<ul> <li>mpls expression may be used more than once, to filter on MPLS hierarchies.</li> </ul>

### Protocols

Various protocols can be combined with primitive BPF filters using modifiers and operators.

Types of valid Protocols are given below:

arp	ip6	udp	fddi	link	slip	rarp
ether	IP	wlan	icmp	tcp	radio	ppp

### Modifiers

Types of valid modifiers/operators:

Parentheses	()
Negation	!=
Concatenation	'&&' or 'and'
Alteration	'  ' or 'or'



## Examples of some filters using operators and modifiers:

udp dst port not 53	UDP not bound for port 53				
host 10.0.0.1 && host 10.0.0.2	Traffic between these hosts				
Tcp dst port 80 or 8080	Packets to either tcp ports				
	**				
ether[0:4] & 0xffffff0f > 25	Range based mask applied to bytes greater				
	than 25				
IP[1] != 0	Captures packets for which Types of				
	Service(TOS) field in the IP header is not				
	equal to 0				
ether host 11:22:33:44:55:66	Matches a specific host with that Mac address				
ether[0] & $1 = 0$ and IP[16] >= 224	Captures IP broadcast or multicast broadcast				
	that were not sent via Ethernet				
	broadcast/multicast				
icmp[icmptype] != icmp-echo	Captures all icmp packets that are not echo				
	requests				
IP[0] & 0xf !=5	Catches all IP packets with options				
IP[6:2] & 0x1fff = 0	Catches only unfragmented IPv4 datagrams				
	and frag zero of fragmented ipv4 datagrams				
tcp[13] & 16 != 0	Captures tcp-ack packets				
tcp[13] & 32 !=0	Captures tcp-urg packets				
tcp[13] & 8!=0	Captures tcp-psh packets				
tcp[13] & 4!=0	Captures tcp-rst packets				
tcp[13] & 2!=0	Captures tcp-syn packets				
tcp[13] & 1!=0	Captures tcp-fin packets				
tcp[tcpflags] & (tcp-syn tcp-fin) != 0	Captures start and end packets (the SYN and				
	FIN packets) of each TCP conversation				



# APPENDIX E: DECRYPTING PCAPS WITH SSL SESSION KEYS

Decrypting PCAP data using SSL session key

This workflow presumes a set of SSL Session keys for decrypting PCAP data is available.

#### 1. Download one or more (encrypted) PCAPs from a completed PCAP search.

Note: If the sessionized TLS/SSL search results in more than 1 PCAP, the PCAPs must be merged into a single PCAP so that one complete session can be loaded into Wireshark in order to decrypt it with a key.

- 2. User can download all PCAPs using the "Download All" option.
- 3. Once downloaded the PCAPs should be merged.
  - a. To merge PCAPs on a windows operating system follow the below steps:
    - i. Click "Download All" to download the PCAPs on the system.
    - ii. Launch Wireshark and select any one downloaded PCAP to open it.

The Wireshar	rk Network	Analyzer							-	×	
File Edit View				Wireless Tools Help							
Open Open Recent	CH+0 .	S 9 + + 5	平土區 🔳	9, 9, 9, <u>II</u>							
Merge Import from Hex Dump Close	CHAIN	Kireshark: Oj		Downloade	d Pcap to	-					×
Seve Seve As	Chi+S Chi+Shift+S	Look in:	Downloads		0.7						
File Set		-	Name			Date modified	Туре	Size			^
Export Specified Packets Export Packet Dissections		<b>X</b>	First.pcap			5/15/2017 3:31 PM	PCAP File	2,498 KB			
Export Packet Bytes Export PDUs to File	Col+H	Quick access	Second.pcap	p		5/15/2017 3:31 PM	PCAP File	4,033 KB			
Export SSL Session Keys Export Objects			Third.pcap			5/15/2017 3:31 PM	PCAP File	2,485 KB			
Print_	Chi+P Chi+Q	Desktop									
		Libraries Dibraries This PC									
		Network									~
			File name:	First.pcap						×	Open
			Files of type:	All Files						$\sim$	Cancel
											Help
			Read filter:		Format:	Wireshark - nanosecond	libpcap				
			Automatic	~	Size:	2557194 bytes					
			MAC name res	solution	Packets:	10530					
			Transport nam	ne resolution	First Packet:	2017-05-15 11:22:49					
	1		Network name	resolution	Elapsed:	00:00:15					
			Use external r	network name resolver							
										_	

- iii. Once opened, the File→Merge option will be available for use.
- iv. Select the PCAP that needs to be merged. Once the PCAP is merged save the new merged PCAP and repeat the steps to merge all PCAPs associated with that session.



First.pcap									_			-	0
	ture Analyze Statistic	s Telephony Wireless To	ols Help										
Open	Ctrl+O	11 = = 444	<u>II</u>										
Open Recent	,											•••	Expression.
Merge_		Time		Source	Destination	Protocol	Length Info						
Import from Hex Dur	mp	1 2017-05-11 00	:25:46.698455	644 10.91.170.22	204.11.16.10	6 TCP	74 37646+25	[SYN] Seq=0	Win=14600 Len=0 MSS=14	460 SACK_PERM=1 TSval=37377	76639 TSecr	=0 WS=128	
Close	Ctrl+W			645 204.11.16.106						en=0 MSS=1460 WS=256 SACK_F		=2062515290	TSe_
Save	Ctrl+S			646 10.91.170.22						TSval=3737776706 TSecr=200	2515290		
Save As	Ctrl+Shift+S			647 204.11.16.106 648 10.91.170.22				ail.cloudema					
File Set				649 10.91.170.22 649 10.91.170.22			83 C: HELO		Ack=30 Win=14/20 Len=0	0 TSval=3737776771 TSecr=20	62515296		
		7 2017-05-11 00		049 10.91.1/0.22	204.11.10.10	0 SHIP	63 CT HELD	3030/14-003					
Export Specified Pack		8 2017-05-11 0	First.pcap									- 0	N N
Export Packet Dissect		9 2017-05-11 04	Wireshark: Me	rge with capture file							×		
Export Packet Bytes	Ctrl+H	10 2017-05-11 00	Look in:	Downloads							_	61 · 64	resir. ·
Export PDUs to File		11 2017-05-11 00		Name			Date modified		Size		· · ·	ecr=0 W5=128	_
Export SSL Session K		12 2017-05-11 04	*	First.pcap			5/15/2017 3:31 PM	Type PCAP File	2,498 KB		PERM+1 TSV	val-2062515290 T	Se.
Export Objects	,	13 2017-05-11 00	Quick access	Second.pcap			5/15/2017 3:31 PM	PCAP File	4.033 KB		062515290		
Print	Ctrl+P			Third.pcap			5/15/2017 3:31 PM	PCAP File	2,485 KB		2062515296		
Quit	Ctrl+Q	167817-850	Desktop										
1		17 2017-05-11 0	Centrop										
		18 2017-05-11 00	-										
		19 2017-05-11 0	Libraries										
		20 2017-05-11 0											
		21 2017-05-11 04	This PC										
		22 2017-05-11 06	-										
		23 2017-05-11 00											
		24 2017-05-11 00 25 2017-05-11 00	Network			-							
1											- T		
		6 bits), 117 bytes		File name: Second	рсөр	s	elect an			<ul> <li>Open</li> </ul>			
		1:df (00:10:f3:3a:		Files of type: All Files			option			<ul> <li>Cence</li> </ul>			
> Internet Protoco > Transmission Con		c: 204.11.16.106,				5				Help			
> Simple Mail Tran		SPC POPE: 25, USE											
· sample mail man	ISTEL PLOCOLOX			Read filter:		Format	Wireshark - nanosecond	Порсар					
				~		Size:	4129380 bytes						
				O Prepend packets to existi		Packets:	17004						
0000 40 f2 e9 75	14 40 00 10 40	3a 21 df 08 00 45		Merge packets chronolog		First Packet	2017-05-15 11:23:21						
		6b cc 0b 10 6a 0a		Append packets to existing	ng file	Elapsed.	00:00:23				1.11		
		02 6a ad b1 0d 86	0000 40 f2 e9 75	14 f8 00 10 f3 3a 21 d		A							
0030 01 03 6d bb		0a 7a ef 7c 74 de	0010 00 67 65 14 0020 as 16 00 15	40 00 74 05 10 6b cc 0 93 0e 2b 10 de 02 6a a		ge t k.							
		3c 63 6c 61 62 61	0030 01 03 6d ba	00 00 01 01 08 0a 7a e 30 20 4f 4b 20 3c 63 6									
		6f 6d 70 75 74 65		4- 40 30 34 43 44 44 3		ini@next coe							
0060 67 2e 63 6f 0070 20 6f 6b 0d	6d 3e 20 52 65	63 69 70 69 65 6e	0050 67 2e 63 6f	6d 3e 20 52 65 63 69 7		com> R eci ok	pient						
20 01 00 00													
			e 7 Testi							Packets: 56 - Displayed: 56 (300.0%) - Load tire	e 0.0,2	1	hufie: Default

- b. To merge PCAPs on a unix operating system follow the below steps:
  - i. Click "Download All PCAP" hyperlink to download all PCAPs on to a unix system. This will download the .zip file containing all the PCAPs.
  - ii. cd <downloads folder>
  - iii. unzip the .zip file that has just been downloaded.

Example: unzip 46106e0a-fce5-4cc5-8046-fb8090767e16.zip

Where 46106e0a-fce5-4cc5-8046-fb8090767e16 is the search uuid

- iv. cd 46106e0a-fce5-4cc5-8046-fb8090767e16
- v. ls -l\*.PCAP
- vi. This will show all downloaded PCAPs

Example Figure:

```
Is -1 *.pcap

-rw-r--r--. 1 root root 347304 May 7 16:32 0.pcap

-rw-r--r--. 1 root root 351645 May 7 16:32 1.pcap

-rw-r--r--. 1 root root 1046205 May 7 16:32 2.pcap

-rw-r--r--. 1 root root 1775493 May 7 16:32 3.pcap

-rw-r--r--. 1 root root 2652375 May 7 16:32 4.pcap
```

vii. Use mergecap command to combine these PCAPs into a single PCAP.

viii. Perform the following command:

mergecap -a -w combined.pcap 0.pcap 1.pcap 2.pcap 3.pcap 4.pcap ls -l combined.pcap

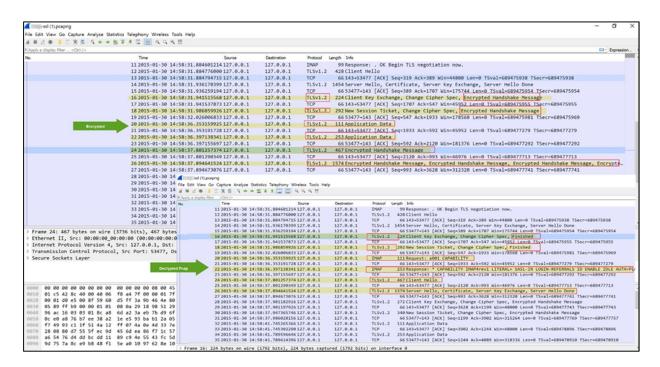
- ix. This PCAP contains all the data produced by the search.
- x. Copy/Download this PCAP to a system that has Wireshark application.



- 4. Now open the merged PCAP in Wireshark
- 5. Select Edit  $\rightarrow$  Preferences...
- 6. Select and expand Protocols, scroll down and select SSL (or type ssl)

	dit View Go Capt	ture Analyze Statistics	Telephony Wireless Tools Help	1 x				
- 5	Find Packet		miter de est journet					- Expre
	Find Next Find Previous	Column Date Name			Destination	Protocol Length Info	-	( Deprin
	Mark/Unmark Packet	Capture American American American						
	Mark All Displayed	C Internation	Terrente da		127.0.0.1	IMAP 99 Response: . OK Begin TLS negotiation now. TLSv1.2 428 Client		
	Unmark All Displayed Next Mark	S Manta	a sector from the sector of th					
	Previous Mark	Abartal Cons and	C Namerika M. Anali garray tubar 19 aguna C Namerika M. Anistan Jan garray tubar M. Anish		127.0.0.1	TCP 66 143+53 Encrypted data 319 Ack=389 Win=44800 Len=0 TSval=689475938 TSecr=689475938		
	Ignore/Unignore Recket	<	C Respectedent (cla (RC), provine Mod Respectedent		127.0.0.1	TLSv1.2 1454 Server meTlo, Certificate, Server Key Exchange, Server Hello Done TCP 06 53477+143 [ACK] Seg=389 Ack=1707 Win=175744 Len=0 TSval=689475954 TSecr=689475954		
	Ignore All Displayed Unignore All Displayed	2 1 3			127.0.0.1			
	Set/Unset Time Reference	-			127.0.0.1	TLSv1.2 224 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message TCP 66 143+53477 [ACK] Seg=1707 Ack=547 Win=45952 Len=0 TSval=689475955 TSecr=689475955		
	Urset All Time References	<	Apply 15L Key	0	127.0.0.1	TISV1.2 292 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message		
	Next Time Reference Previous Time Reference	2 minut			127.0.0.1	TCP 66 53477+143 [ACK] Seg=547 Ack=1933 Win=178560 Len=0 TSval=689475981 TSecr=689475969		
	Time Shift	CH-SHR+T	20 2015-01-30 14:58:36.353159925		127.0.0.1	TLSv1.2 111 Application Data		
	Packet Comment	Chi+Alt+C	21 2015-01-30 14:58:36.353191728		127.0.0.1	TCP 66 143+53477 [ACK] Seq=1933 Ack=592 Win=45952 Len=0 TSval=689477279 TSecr=689477279		
	Configuration Profiles	Chi-ShiR+A	22 2015-01-30 14:58:36.397138341		127.0.0.1	TLSv1.2 253 Application Data		
	Pelevences.	Cut-Shift-P	23 2015-01-30 14:58:36.397155697		127.0.0.1	TCP 66 53477+143 [ACK] Seq=592 Ack=2120 Win=181376 Len=0 TSval=689477292 TSecr=689477292		
			24 2015-01-30 14:58:37.801257374		127.0.0.1	TLSv1.2 467 Encrypted Handshake Message		
			25 2015-01-30 14:58:37.801290349		127.0.0.1	TCP 66 143+53477 [ACK] Seq=2120 Ack=993 Win=46976 Len=0 TSval=689477713 TSecr=689477713		
			26 2015-01-30 14:58:37.894641524		127.0.0.1	ILSv1.2 1574 Encrypted Handshake Message, Encrypted Handshake Message, Encrypted Handshake Messag	e. End	covot
			27 2015-01-30 14:58:37.894673076		127.0.0.1	TCP 66 53477-143 [ACK] Seg=993 Ack=3628 Win=312320 Len=0 TSval=689477741 TSecr=689477741		
			28 2015-01-30 14:58:37.901182916		127.0.0.1	TLSv1.2 272 Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message		
			29 2015-01-30 14:58:37.901197926	127.0.0.1	127.0.0.1	TCP 66143+53477 [ACK] Seg=3628 Ack=1199 Win=48000 Len=0 TSval=689477743 TSecr=689477743		
			30 2015-01-30 14:58:37.947365746		127.0.0.1	TLSv1.2 340 Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message		
			31 2015-01-30 14:58:37.986028156	127.0.0.1	127.0.0.1	TCP 66 53477+143 [ACK] Seq=1199 Ack=3902 Win=315264 Len=0 TSval=689477769 TSecr=689477757		
			32 2015-01-30 14:58:41.745265366	127.0.0.1	127.0.0.1	TLSv1.2 111 Application Data		
			33 2015-01-30 14:58:41.745302290	127.0.0.1	127.0.0.1	TCP 66143+53477 [ACK] Seq=3902 Ack=1244 Win=48000 Len=0 TSval=689478896 TSecr=689478896		
			34 2015-01-30 14:58:41.789596646	127.0.0.1	127.0.0.1	TLSv1.2 253 Application Data		
			35 2015-01-30 14:58:41.789614396	127.0.0.1	127.0.0.1	TCP 66 53477+143 [ACK] Seq=1244 Ack=4089 Win=318336 Len=0 TSval=689478910 TSecr=689478910		
Et! In! Tri	hernet II, Sro ternet Protoco	c: 00:00:00_00:00 ol Version 4, Src: ntrol Protocol, Sr	bits), 467 bytes captured (3736 00 (00:00:00:00:00:00), Dst: 00:0 127.0.0.1, Dst: 127.0.0.1 c Port: 53477, Dst Port: 143, Seq	0:00_00:00:00	(00:00:00:00			

- 7. Click Browse button under (Pre)-Master-Secret log filename.
- 8. Select the Session Key filename to be loaded.
- 9. [Optional] To produce a debug file, click Browse button under SSL debug file and provide a location/filename for a debug file. Note: Wireshark will write to this file.
- 10. Click OK
- 11. If the Session Key is correct/matching, the loaded PCAP file will be decrypted





- Wireshark automatically tries to decrypt any other PCAPs using the SSL Session Key loaded currently. To remove this file or replace with a new file, repeat the steps 3 through 8.
- Wireshark can only decrypt SSL/TLS packet data if RSA keys are used to encrypt the data.
- Wireshark can only decrypt SSL/TLS packet data if the capture includes the initial SSL/TLS session establishment. Re-used sessions cannot be decrypted; you can identify these as the server will not send a certificate or alternatively, the Wireshark SSL debug file will display a ssl\_restore\_session can't find stored session error message.
- Duplicate packets may cause issues and prevent all relevant packets being decrypted.



# **APPENDIX F: UNDERSTANDING BEHAVIOR SEARCH**

This feature provides sessioninfo of a URL based relationship between a HTTP and Email session or between a DNS, HTTP and Email session. Alerts are generated if a particular URL is present in both a HTTP stream AND an email body. If the domain/sub-domain associated with that particular URL appears in a DNS session, then DNS session is also included in the alert. These alerts help to analyze and track activities based on user's behavior/actions.

#### For example:

- Has the user clicked on a URL received in an email body?
- Does the URL string indicate the domain of a well-known company (bofa.com) but the underlying hostname resolves to a blacklisted IP address?
- Has the user visited the web page?
- What kind of links are attracting the users to click on and what kinds are being ignored?

The Behavior search feature under Log Manager is a user-friendly capability that requires no setup nor prior knowledge of which domains to look for.

The following use cases provide a better understanding of this feature:

Use Case 1: Email, DNS, HTTP correlation event

- 1. A user receives an email. The email body contains invitation to click on a URL: http://www.visitparadise.us.
- 2. This action will result in one email alert under Log Manager  $\rightarrow$  Email tab
- 3. The user clicks on the URL.
- 4. As this host is unknown, the system generates a DNS query for www.visitparadise.us.
- 5. This action results in one DNS alert under Log Manager  $\rightarrow$  DNS tab.
- 6. When the http request is successful and the user is now on http://www.visitparadise.us page an HTTP alert is produced/displayed under Log Manager → HTTP tab.
- 7. As the same URL appears in both HTTP and Email sessions and its associated domain request appears in a session, a new alert appears under Log Manager  $\rightarrow$  Behavior Search tab.

# *Note*: The Log Manager $\rightarrow$ Behavior Search $\rightarrow$ DNS, HTTP, Email Correlation Alert is NOT generated if either step 3, step 4 OR 6 is skipped.

<u>Use Case 2</u>: Email, HTTP correlation event

- 1. A user receives another email. The email body contains invitation to click on http://www.visitparadise.us again.
- 2. This action will result in one email alert under Log Manager  $\rightarrow$  Email tab.
- 3. The user clicks on the URL.
- 4. As this host is now known, there is no DNS query hence no DNS alert.
- 5. The http request is successful and the user is now on http://www.visitparadise.us page.
- 6. This will generate/display one HTTP alert under Log Manager  $\rightarrow$  HTTP tab.
- 7. As the same URL appears in both HTTP and Email sessions, a new alert appears under Log Manager → Behavior Search tab with session details for HTTP and Email.



*Note:* The Log Manager  $\rightarrow$  Behavior Search  $\rightarrow$  HTTP, Email Correlation Alert is NOT generated if step 3 is skipped.



# **APPENDIX G: UNDERSTANDING RULESETS**

In order to create a ruleset it is important to understand the rule format supported by Suricata. A rule/signature consists of the following Action, Header and Rule-options.

**Example**: alert IP [100.64.0.0/10]  $1024 \rightarrow 5.6.7.8$  80 (msg:"[100.64.0.0/10]"; sid:300;)

In the above example: alert is an action. IP  $[100.64.0.0/10] \ 1024 \rightarrow 5.6.7.8 \ 80$  is a header. (msg:"[100.64.0.0/10]"; sid:300;) is a rule-option.

#### Action:

The action property determines what will happen when a signature matches. Suricata processes these rules based on priorities associated with the signature. The most important signatures will be scanned first.

Action	Description
Pass	If a signature matches and contains pass, Suricata stops scanning the packet and skips to the end of all rules (only for the current packet).
Drop	This only concerns the IPS/inline mode. If the program finds a signature that matches, containing drop, it stops immediately. The packet will not be sent any further. Drawback: The receiver does not receive a message of what is going on, resulting in a time-out (certainly with TCP). Suricata generates an alert for this packet.
Reject	This is an active rejection of the packet. Both receiver and sender receive a reject packet. There are two types of reject packets that will be automatically selected. If the offending packet concerns TCP, it will be a Reset-packet. For all other protocols it will be an ICMP-error packet. Suricata also generates an alert. When in Inline/IPS mode, the offending packet will also be dropped like with the 'drop' action.
Alert	If a signature matches and contains alert, the packet will be treated like any other non-threatening packet, except for this one an alert will be generated by Suricata. Only the system administrator can notice this alert.

Below is a summary of actions in default order based on priority:

**Example Rule:** alert IP [100.64.0.0/10] 1024 → 5.6.7.8 80 (msg:"[100.64.0.0/10]"; sid:300;)



This rule sets an alert action when source IP [100.64.0.0/10] matches with the destination IP 5.6.7.8

#### Header:

The header part of the rule allows to keep a watch on the protocols concerned, the source and destination IP- addresses, ports involved and their direction of flow.

#### Protocol:

This keyword in a signature tells Suricata which protocol we want our rule to keep an eye out for. Below are the five options to choose from.

- 1. IP When IP is specified it will watch for all or any packets on the network.
- 2. tcp When tcp is specified it will match a rule against TCP traffic.
- 3. udp When udp is specified it will match a rule against UDP packets.
- 4. icmp When icmp is specified it will match a rule for ICMP packets.
- 5. Suricata also allows you to specify layer 7 protocols like HTTP (http), SSL and TLS (tls for both), FTP (ftp) and SMB (smb) as well.

#### Source and Destination IP and Port:

This allows you to assign source and destination IP-addresses (IPv4 and IPv6 combined as well as separated) and the desired ports.

Sign	Description	Example
!	An exclamation specifies "not"	Ex: !1.1.1.1 which means any IP except 1.1.1.1
[] and ,	A square bracket is used to specify multiple IPs or ports separated by comma	Ex: ![1.1.1.1,1.1.2] Every IP address but 1.1.1.1 and 1.1.1.2 Ex: [10.0.0.0/24, !10.0.0.5] Except 10.0.0.5 matches all 10.0.0.0/24
:	A colon is used to specify range	<ul> <li>Ex.: [80, 81, 82]</li> <li>Includes port 80, port 81,port82</li> <li>Ex: [80:82]</li> <li>Includes port range from 80 till 82</li> <li>Ex: [1024: ]</li> <li>From 1024 till the highest port-number</li> <li>Ex: !80</li> <li>Every port but 80</li> <li>Ex: [80:100,!99]</li> <li>Range from 80 till 100 but 99 excluded</li> </ul>

*Note*: In addition to set specific IP addresses you can also use a Yaml-file to set IP- addresses for variables such as HOME\_NET or EXTERNAL\_NET. These settings will be used when you use these variables in a rule. In source and destination you can make use of signs like ! And [].

Using variable HOME\_NET allows you to set the relevant IP-address for several rules. This option contains the address group vars that will be passed in a rule.

Using EXTERNAL\_NET signifies ! HOME\_NET

(For more information on using variable see refer to the link below http://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html#suricata-yaml-rule-vars

### **Direction Specification:**

Between the IP and ports is the direction of packet flow. The direction tells in which way the signature has to match.

	This is the most common and means only check if the source IP and port
	are coming in to the destination IP and port
<>	This will match packet flow in either direction

#### Example Rule1:

alert tcp [100.64.0.0/10]  $1024 \rightarrow 5.6.7.8$  80 (msg:"[100.64.0.0/10]"; sid:300;)

This rule sets an alert action when protocol tcp, source [100.64.0.0/10], port 1024 matches with the destination IP 5.6.7.8, port 80

### Example Rule2:

drop tcp \$HOME NET any  $\rightarrow$  \$EXTERNAL NET any (msg:"[OK to drop]"; sid:500;)

This rule sets a drop action when protocol tcp, source \$HOME\_NET port any matches with the destination
\$EXTEPNAL NET and port any

\$EXTERNAL\_NET and port any

Where: \$HOME\_NET and \$EXTERNAL\_NET are variables set for IP-addresses as defined in the Yaml-file.

#### **Rule-options:**

There are many rule-options but they can be categorized mainly into 5 categories.

1. Meta-settings: This is the most used rule-option. Meta-settings have no effect on Suricata's



inspection, but they do affect the way event are reported in Suricata. The 3 main meta-settings are:

- msg: The keyword msg gives more information about the signature and the possible alert. Example- msg: "Attack Forbidden";
- sid: The keyword sid gives every signature its own unique id. This id is stated with a number Example- sid:123;
- rev: The sid keyword is almost every time accompanied by rev. Rev represents the version of the signature. If a signature is modified, the number of rev will be incremented by the signature writers. Example- rev:123;

**Example Rule:** alert tcp [100.64.0.0/10]  $1024 \rightarrow 5.6.7.8$  80 (msg:"[100.64.0.0/10]"; sid:300; rev2;)

For more information on meta-settings, please refer to the following link:

http://suricata.readthedocs.io/en/latest/rules/meta.html

2. Payload: Payload keywords inspect the content of the payload of a packet or stream (the packet data itself, such as IRC commands). For more information on meta-settings, please refer to the following link:

http://suricata.readthedocs.io/en/latest/rules/payload-keywords.html

3. HTTP: These keywords make sure the signature checks only specific parts of the network traffic. For instance, to check specifically on the request URI, cookies, or the HTTP request or response body, etc. For more information on meta-settings, please refer to the following link:

http://suricata.readthedocs.io/en/latest/rules/http-keywords.html

4. Flowbits: Flowbits consists of two parts. The first part describes the action it is going to perform, the second part is the name of the flowbit. Flowbits can make sure an alert will be generated when, for example two different packets match. An alert will only be generated when both packets match. For more information on meta-settings, please refer to the following link-

http://suricata.readthedocs.io/en/latest/rules/flow- keywords.html

5. IP Reputation Rules: Gives an idea if an IP is legit or known to be associated with malware, spam, etc. For more information on meta-settings, please refer to the following linkhttp://suricata.readthedocs.io/en/latest/reputation/ipreputation/ip-reputation-rules.html

*Note*: For a more descriptive information about creating user defined rule-sets please refer to the link below:

http://suricata.readthedocs.io/en/latest/rules/intro.html



# APPENDIX H: FASTCOPY WORKFLOW

FastCopy workflow allows Federation Manager initiated search data from multiple Federation Nodes to be merged to a single Federation Node.

#### Workflow

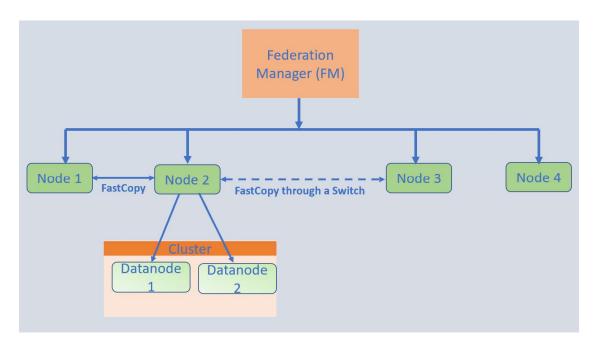
- When a search is created from Federation Manager, the search request goes to all selected Federated Nodes.
- When a search is complete, the PCAPs are merged based on the connectivity and connection status of each node.
- Each Federation Node is in one of the given FastCopy states:

Icon	Action	Description	
X	FastCopyOff	When a Federation Node does not participate in	
		FastCopy workflow	
	FastCopyDisabled	When a Federation Node is configured to participate in	
FC		FastCopy workflow, but it is currently disabled	
or 🐻	FastCopySingle	When a Federation Node is connected to one other	
		Federation Node for FastCopy	
FC	FastCopyDual	When a Federation Node is connected to two other	
		Federation Node for FastCopy	

### <u>UseCase</u>

#### For Example:

Node 1 is FastCopySingle node, Node 2 is FastCopyDual node, Node 3 is FastCopySingle node and Node 4 is FastCopyOff.





### • Scenario 1:

- If Node1 and Node3 are connected to Node2.
- And a search is sent to three nodes Node1, Node2, and Node3 from FM
- Node1 and Node3 send their search PCAPs to Node2.
- Federation Manager will show one row for a single merged pcap for the pcap data from Node1, Node2 and Node3

### • Scenario 2:

- If Node1 and Node3 are connected to Node2.
- And a search is sent to all four nodes in the federation Node 1, Node 2, Node 3 and Node 4.
- Where Node4 is not connected to Node2.
- Node1 and Node3 send their search PCAPs to Node2.
- o Node4 does not send its PCAPs.
- Federation Manager will show two rows:
- One row for a single merged pcap for the pcap data from Node1, Node2 and Node3
- 2<sup>nd</sup> row for a single pcap for the pcap on Node4



# **APPENDIX I: TECHNICAL SUPPORT**

SentryWire is proud to offer 24x7 support for all SentryWire products.

SentryWire support requests will be acknowledged on the following schedule:

Features	Product Support Response Time	Support Request Method
Hours of Operation	Normal Business Hours: 8AM to 11PM EST 24 Hours/Day 7 Days/Week 365 Days/Year	Phone: 443-561-0510 Web: http: //support.sentrywire.com
Critical (Severity 1) - Includes hardware based issues that impact the ability to capture and search	30 Min or Less: 24x7	Phone support only after Normal Business Hours
Major (Severity 2) - Includes non- hardware related issues that impact the ability to capture and search	1 hour or Less: 24x7	Phone support only after Normal Business Hours
Minor (Severity 3) - Includes issues that do not impact capture or search capability such as product updates	Within 8 hours: Normal Business Hours	Phone or Web
Informational (Severity 4) - Includes How-To and What-If type questions	Within 12 hours: Normal Business Hours	Phone or Web

Software:

12 Months of software support

Hardware:

Includes 36 Months of Hardware Service and Support provided on all parts and labor by hardware manufacturer.

On-site, On-Line VIP Service Portal, Global Remote Service and On Site Engineer as required, 7x24x365.



# **APPENDIX J: KEY TERMS**

The following table provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

TERM	DEFINITION
BPF	Berkely Packet Filter
Gbps	Gigabits per second
IP	Internet Protocol
НТТР	Hyper Text Transfer Protocol
IDS	Intrusion Detection System
IoC	Indicators of Compromise
LEEF	Log Event Extended Format
РСАР	In the field of computer network administration, PCAP consists of an application programming interface for capturing network traffic.
Suricata	Suricata is a free and open source, mature, fast and robust network threat detection engine. The Suricata engine is capable of real time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM) and offline PCAP processing.
ТСР	Transmission Control Protocol
UDP	User Datagram Protocol
UI	User Interface