Trellix ePO Saas Connector App for QRadar

Contents

Overview	2
Terms and Definitions	2
Architecture	2
Pre-requisites	3
Before Getting Started (Mandatory)	3
Apply Trellix ePO Saas Tag	4
Trellix ePO Saas Device Details	4
Poll Threat Events from Trellix ePO Saas	5
Software version and platform details	7
Step by Step Instruction to use Trellix ePO Saas for QRadar App	7
Acquiring client credentials from Trellix Marketplace	8
Configure/Provision Trellix ePO Saas Connector for QRadar App	8
Apply Trellix ePO Saas Apply Tags	15
Apply Trellix ePO Saas Remove Tags	19
Trellix ePO Saas Device Details	23
Create/Update EDR Investigation for an offense in QRadar	24
Poll Threat and Insights Events from Trellix ePO Saas to QRadar	27
Poll Configuration	27
MVISION Insights	32
MVISION Insights Campaign's	33
MVISION Insights Campaign's IOC	34
MVISION Insights Campaign's Galaxies	36
Audit Log	37
Important things to know	38
Steps to follow if exception is displayed while clicking on Create/Update EDR Investigation button	38
Steps to follow if 'SSL: CERTIFICATE_VERIFY_FAILED' message appears in app log	39

Overview

As part of our "Together is Power" strategy, we have built a new eco system wherein we have enabled our key Trellix products (Trellix ePO Saas, MVISION EDR and Insights) features inside the IBM's QRadar (SIEM) server. We have created "Trellix ePO Saas Connector" for QRadar app to implement this eco system and it will provide the following actions for IBM QRadar admin users:

- Can create/update an EDR investigation for an offense from IBM QRadar console. An EDR SOC admin will continue the investigation for the given endpoint (IP, Hostname). Investigation contains IP, Severity and offense description.
- Can apply Trellix ePO Saas policy, based on a tag assigned at IBM QRadar console to an IP.
- Can enrich endpoint system data from Trellix ePO Saas to IBM QRadar console.
- Can ingest Trellix ePO Saas threat events in IBM QRadar event logs for correlation.
- Can ingest MVISION Insights events in IBM QRadar event logs for correlation.

Terms and Definitions

Term	Definition
Trellix ePO Saas	Trellix e-Policy Orchestrator Saas
MVISION EDR	MVISION Endpoint Detection & Response

Architecture

The high-level architecture of "Trellix ePO Saas Connector for QRadar" app is shown below:



Pre-requisites

Before we start using "Trellix ePO Saas Connector" App, user must make sure that the following applications are up and running and the same should be accessible by them from QRadar server network.

- Trellix ePO Saas Server
- MVISION EDR
- MVISION Insights

Before Getting Started (Mandatory)

Since we have transitioned from McAfee to Trellix, we have rebranded our app. The following steps will be performed to make this app work as expected.

- "Trellix ePO Saas Connector" App will not support the upgrade.
- Users must uninstall the older version of app (McAfee MVISION Connector).
- Following entries will not be removed as part of the Uninstall of McAfee MVISION Connector. Please make sure that the following entities are removed properly
 - 1. Admin | Log Sources | Launch | Log Sources (Manage Log Sources) | select MVISION ePO Threat Events | click on menu | Delete

- 2. Admin | Log Source Extensions | MVISIONEPOThreatEventsCustom_ext | Delete
- 3. Admin | Custom Event Properties | MVISION ePO Events | select all | Delete
- 4. Admin | DSM Editor | MVISION ePO Threat Events | Delete
- Install the "Trellix ePO Saas Connector" App.

Apply Trellix ePO Saas Tag:

- Before applying Trellix ePO Saas tags action, user must make sure the tags to be applied on the system(s) are created in Trellix ePO Saas server Tag Catalog.
 For e.g. Create a tag with name Server
- Refer the screenshot below -

\equiv Trellix	Protection Workspace MVISION Marketplace Client Task	ks Product Deployment	Tag Catalog 🛛 🗸	₽ ⑦	£	:::
Tag Catalog						
Tag Group Tree	My Tags					:
New Subgroup	This Tag Group Only 🗸 þearch	× Show unus	ed tags	63 Tags New	Tag 🗸	
> My Tags	Tags	Edited By	Edited On	✓ Tag Type		
	Image: Server Default tag for systems identified as a Server	system	9/6/21 8:04:56 PM IST	Mixed		
	Image: Workstation Default tag for systems identified as a Workstation	system	9/6/21 8:04:56 PM IST	Mixed		
	Escalated	system	9/6/21 8:05:01 PM IST	Manual		

Trellix ePO Saas Device Details:

- Before fetching Trellix ePO Saas Device Details, user must make sure the device for which the details need to obtain should be managed in the Trellix ePO Saas. For e.g.- system IP -10.254.46.95 is managed in ePO.
- Refer the screenshot below:

\equiv Trellix	Protection Workspace	System Tree	MVISION Marketplace	Client Tasks Product Depl	oyment 🗸 🌲	. 🤊 👤 🔛
System Tree 🛛 🔤	/ Systems New Subgroups System	n Tree Permissions				
System Tree	Systems Policies Client Ta	sks Sorting De	ploy			
✓ My Organization	Preset:	Custom:	Quick find:			
mani	This Group and All Subgroups	s V None	×	Apply Clear	Show selected rows	
My System Tree Group	System Name	✓ Managed	State Tags	IP address	User Name	Last Commi
My System Tree Group 2		Managed	Escalated,	Server	cloudadmin	11/1/21 9:3
My System Tree Group 3		Managed	879de20e	-5b30-4369-83547f30e9	N/A	5/16/22 9:4
silambu		Managed	879de20e	5b30-4369-8699-ee354	Cloudadmin	5/6/22 11:4
Lost and Found		Managed	879de20e	-5b30-4369-83547f30e9 10.254.46.95	cloudadmin	5/16/22 9:5

Poll Threat Events from Trellix ePO Saas:

 Before starting poll for threat events make sure to increase Max UDP Syslog Payload Length to 8192 so that events are not truncated. To do this login to QRadar console and navigate to Admin panel > click on System Settings icon > click Advanced button on left bottom corner and then change Max UDP Syslog Payload Length to 8192 and click Save. Make sure to initiate a Full Configuration deployment so that changes are deployed for QRadar server as shown below:

System Settings			
	System Settings		
System Settings	Administrative Email Address	root@localhost	
Database Settings	Alert Email From Address	QRADAR@localhost.localdomain	
Ariel Database Settings	Fmail Locale	English	•
Custom Rule Settings	Max Email Attachment Size (KB)	15,360	*
	Delete Root Mail	Yes	*
Transaction Sentry Settings	Temporary Files Retention Period	6 hours	*
SNMP Settings	Coalescing Events	Yes	*
Embedded SNMP Daemon Settings	Store Event Payload	Yes	*
Console Settings	Global Iptables Access (comma separated)		
M(N) C C-Hi	Syslog Event Timeout (minutes)	720	*
WINS Settings	Partition Testers Timeout (seconds)	30	*
Reporting Settings	Max UDP Syslog Payload Length	8,192	*
Data Export Settings	Max TCP Syslog Payload Length	4,096	*
QElow Settings	Max Number of TCP Syslog Connections	2,500	*
ODedes Naturals Insights Cattings	Max TCP Syslog Connections Per Host	10	*
QRadar Network insights Settings	Timeout for Idle TCP Syslog Connections (seconds)	900	*
Geographic Settings	Log and Network Activity Data Export Temporary Directory	/store/exports	
	Display Country/Region Flags	Yes	*
	Display Embedded Maps in IP Address Tooltips	Yes	*
	Enable X-Force Threat Intelligence Feed	No	*
	Host Profile Reporting Interval	900	*
	Host Profiler Reporting Interval Counter	15	*
	Lag time to remove expired reference data (minutes)	5	*
Switch to:	Database Settings		
Basic	User Data Files	/store/users/	
Duolo	Accumulator Retention - Minute-by-Minute	1 week (default)	*
	Accumulator Retention - Hourly	33 days (default)	*

- As part of the Trellix ePO Saas Connector app, custom log source, log source type, log source extension and custom properties will be populated which help in parsing the threat events on QRadar and display them accordingly.
- Log Source types: Trellix ePO Saas Threat Events and MVISION Insights Events log source types will be created on installing this app.
- Log Sources: Trellix ePO Saas Threat Events and MVISION Insights Events log source with log source identifier Trellix_ePO_Saas_event and MVISION_Insights are created by this app.
- Log Source Extensions: TrellixEPOSaasThreatEventsCustom_ext and
 MVISIONInsightsEventsCustom_ext are created by app upon installation as shown below:

Edit a Log Source Extension



Save Cancel



Save Cancel

0

 Custom Properties: Few custom properties specific to Trellix ePO Saas and MVISION INSIGHTS will be created on app installation as shown below:

Property Name	Type	Property	Log Source Type	Log Source	Event Name	Category	Expression	Username	Enabled	Creation Date	Modification
riopenty manie	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Description	Log course type	Log course	Literititatile	outogoty	Expression	osername	Entioned	oreation bute	Date
AgentGUID	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"agentguid"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
AnalyzerDetect	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"analyzerdetec	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
AnalyzerHostN	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"analyzerhostn	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
AnalyzerID	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"analyzer"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
AnalyzerIPV4	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"analyzeripv4"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
AnalyzerMAC	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"analyzermac"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
AnalyzerName	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"analyzername"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
AnalyzerVersion	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"analyzerversion"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
DetectedUTC	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"detectedutc"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
ReceivedUTC	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"receivedutc"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
SourceHostName	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"sourcehostna	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
SourceProcess	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"sourceproces	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
SourceURL	JSON Keypath	Field to fetch S	Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"sourceurl"	admin	True	Apr 30, 2021, 3	May 9, 2022, 1
SourceUserName	JSON Keypath	Field to fetch S	Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"sourceuserna	admin	True	Apr 30, 2021, 3	May 9, 2022, 1
TargetFileName	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"targetfilename"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
TargetHostName	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"targethostname"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
TargetProcess	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"targetprocess	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
ThreatActionTa	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threatactionta	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
ThreatCategory	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threatcategory"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
ThreatEventID	JSON Keypath	Custom propert	Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threateventid"	admin	True	May 17, 2021,	May 9, 2022, 1
ThreatHandled	JSON Keypath	p p	Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threathandled"	admin	True	Oct 3, 2020, 3:	May 9, 2022, 1
ThreatName	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threatname"	admin	True	Oct 3, 2020, 3	May 9, 2022. 1
ThreatSeverity	JSON Keypath	Custom field to	Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threatseverity"	admin	True	May 18, 2021	May 9, 2022.
ThreatTyne	ISON Keynath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threattyne"	admin	True	Oct 3, 2020, 3	May 9, 2022 1

Add 📑 Edit	🗋 Add 📄 Edit 🗈 Copy 🔣 Enable/Disable 🚳 Delete 🛛 mixision 🔍										0
Property Name	Туре	Property Description	Log Source Type	Log Source	Event Name	Category	Expression	Username	Enabled	Creation Date	Modification Date
AgentGUID	JSON Keypath		MVISION Insights Events	N/A	N/A	N/A	/"agentGuid"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
AnalyzerID	JSON Keypath		MVISION Insights Events	N/A	N/A	N/A	/"analyzerld"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
AnalyzerName	JSON Keypath		MVISION Insights Events	N/A	N/A	N/A	/"analyzerName"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
Campaign Id	JSON Keypath	Custom field to	MVISION Insights Events	N/A	N/A	N/A	/"campaign-id"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
DetectedUTC	JSON Keypath		MVISION Insights Events	N/A	N/A	N/A	/"timestamp"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
Hostname	JSON Keypath	Default custom	MVISION Insights Events	N/A	N/A	N/A	/"computerName"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
MD5 Hash	JSON Keypath	Default custom	MVISION Insights Events	N/A	N/A	N/A	/"md5"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
OS Name	JSON Keypath	Default custom	MVISION Insights Events	N/A	N/A	N/A	/"osType"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
SHA256 Hash	JSON Keypath	Default custom	MVISION Insights Events	N/A	N/A	N/A	/"sha256"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1
ThreatEventID	JSON Keypath	Custom propert	Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threateventid"	admin	True	May 17, 2021,	May 9, 2022, 1
ThreatSeverity	JSON Keypath	Custom field to	Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threatseverity"	admin	True	May 18, 2021,	May 9, 2022, 1
User Domain	JSON Keypath	Default custom	MVISION Insights Events	N/A	N/A	N/A	/"domainName"	admin	True	Jul 14, 2021, 1:	May 9, 2022, 1

- Make sure UDP port 514 is enabled as QRadar Syslog server uses this port to listen to incoming messages.
- Make sure to deploy changes from QRadar Admin panel before starting poll so that Log source changes are deployed properly.

Software version and platform details

Below is the list of components that we have used to test Trellix Connector for QRadar app.

Service name	Component version and platform details
Trellix ePO Saas server	As per the details mentioned in on-boarding welcome mail
MVISION EDR	As per the details mentioned in on-boarding welcome mail
MVISION Insights	As per the details mentioned in on-boarding welcome mail
IBM QRadar Server	IBM QRadar v7.5.0 Build 20211220195207 and above

Step by Step Instruction to use Trellix ePO Saas for QRadar App

As part of this app documentation we assume that all Trellix ePO Saas related operation and configuration will be performed only by Trellix ePO Saas sever **tenant** users and all QRadar related operation and configuration will be done by QRadar server **admin** user.

Acquiring client credentials from Trellix Marketplace

- 1. As part of the workflow customer/tenant should login into Trellix Marketplace using their Trellix credential.
- Customer/tenant then should register and get IBM QRadar app (Trellix Saas App for IBM QRadar) from Trellix Market place. After opening the IBM QRadar app in marketplace, click on "configure" button to configure actual QRadar server URL and click "Launch" button.
- 3. The "Launch" action will open the given QRadar Server URL in a separate browser window.
- 4. Now enter the QRadar server credentials to login into QRadar console.
- Now you must install "Trellix ePO Saas Connector app" into QRadar server. In order to achieve this, you have two options
 Option #1: Go to Menu | Admin | Extension Management page in QRadar server and click "IBM Security App Exchange" button to download "Trellix ePO Saas Connector app".
 Option #2: Go to IBM X-Force Exchange website
 (https://exchange.xforce.ibmcloud.com/hub?q=Trellix) to download the latest "Trellix ePO Saas Connector app".
 Exchange and the download "Trellix app Saas Connector app".
 Option #2: Go to IBM X-Force Exchange website
 (https://exchange.xforce.ibmcloud.com/hub?q=Trellix) to download the latest "Trellix ePO Saas Connector app".
 Exchange and "Trellix app Saas Connector app".
 Exchange and "Trellix app Saas Connector app".
 Exchange and the adverter adverter and the adverter adver
- 6. Install the downloaded "Trellix ePO Saas Connector" app into QRadar Server.
- 7. Open the "Trellix ePO Saas Connector" app landing page to configure Trellix ePO Saas credentials.

Note: Go back to IBM QRadar app in Trellix Market place to copy Client ID, Client Secret, and API Key, and provide the same in corresponding input fields.

- If the configuration saved successfully, following task can be performed by QRadar admin user.

 a. Create Investigation in MVISION EDR for the QRadar offences based on the app scheduler/filter configuration.
 - b. Right click option in QRadar console to apply a tag for an IP in Trellix ePO Saas.
 - c. Right click option in QRadar console to show additional device details from Trellix ePO Saas.

Configure/Provision Trellix ePO Saas Connector for QRadar App

Before the QRadar admin takes advantage of actions that are provided by Trellix ePO Saas Connector for QRadar App, the QRadar admin user should configure/provision Trellix ePO Saas server inside the Trellix ePO Saas Connector for QRadar app.

Refer the screenshot below-



Also, the same app will be shown as part of QRadar ribbon tab. Refer the screenshot below-

E IBM QRadar		
Dashboard Offenses Log Activity Netv	ork Activity Assets Reports Risks Vulnerabilities Admin Pulse Use Case Manag	ger Trellix ePO Saas Connector
Trellix Trellix ePO Saas Config Trellix	PO Saas Events Config Audit Log	
	Trellix ePO Saas Server Configuration	
	API Gateway URL:	
	URL	0
	Client ID:	
	ClientId	0
	Client Secret:	
	Client Secret	0
	API Key:	
	API Key	0
	Proxy	
	Save Test Cancel	

Provide the values under Trellix ePO Saas Server Configuration page like the sample data given below:

Field Name	Sample Value	Description
API Gateway URL	https://api.dev.mvision.mcafee.com	Provide URL of Trellix API Gateway (IP address or number inputs are not allowed)
Client ID	<client from="" id="" market="" place="" trellix=""></client>	Provide valid Client ID which is generated by the Tenant ID provided in the activation mail.
Client Secret	<client from="" market="" place="" secret="" trellix=""></client>	Provide valid Client Secret which is generated by the Tenant ID provided in the activation mail.
API Key	<api from="" key="" market="" place="" trellix=""></api>	Provide valid API Key which is provided as part of the activation mail for a Tenant ID.
Proxy	Checkbox	This checkbox should be checked if proxy is required to be configured.
Proxy Server URL	Proxy URL	Provide valid Proxy server URL. For eg. Sample.proxy.com
Proxy Port	Port Number	Provide valid proxy port number associated with the proxy URL. For e.g 9090

Once all the fields are populated, click on **Test** button to validate the given credentials.

≡	IBM QRadar	÷									
Dashboar	d Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
Trellix	Trellix ePO Sa	as Config	Trellix ePO Saas Ev	ents Config	Audit L	_og					
			Client Client Client Proxy Proxy Sa Conn	ellix ePC ateway URL: ID: Secret: ey: Server URL:) Saas Se : : : : : : :	cancel To save th	Trellix ePO Sa e current config	aas 💽	Proxy Por		

If the test is successful, click on **Save** button to save this configuration. Refer the screenshot below-

≡ !	BM QRadar										
ashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
ellix	Trellix ePO Saa	as Config	Trellix ePO Saas Ev	ents Config	Audit Lo	og					
			/ Tr	ellix ePO	Saas Se	rver Co	nfiguration				
			API Ga	teway URL:							
										0	
			Client	ID:							
							•			0	
			213								
			Client	Secret:							
										0	
			API Ke	ey:							
										0	
			Proxy								
			Proxy	Server URL:					Proxy Por	b.	
							0		1 Jen)	
							12		6 7		
									10		
			Ed	it Te	est (Cancel	Trellix ePO Sa	as 🤣			
			API G	ateway conf	figuration is	s saved			<i></i>		
							•				

If the Test fails, a failure message will be displayed. Check if valid inputs are provided and retry. Refer the screenshot below-

≡	IBM QRadar										(1888)
Dashboard	d Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
Trellix	Trellix ePO Sa	as Config	Trellix ePO Saas Ev	ents Config	Audit L	.og					
			✓ Tr APIG Client Client ••• APIK Proxy ✓ Proxy	ellix ePC ateway URL ID: Secret: ey: Server URL) Saas Se : : : : :	cancel way. Chec	Trellix ePO Sa	nas 🗨	Proxy Port		

It is mandatory that Test should pass to Save and proceed and perform other actions.

Once the Save is completed, user can Edit the Trellix ePO Saas server details by clicking Edit button. Refer the screenshot below-

≡	IBM QRadar										
Dashboard	I Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
Trellix	Trellix ePO Sa	as Config	Trellix ePO Saas Eve	ents Config	Audit L	og					
			True API Ga Client Client Client Proxy Proxy Client API Ke API Ke API Ke API API Ga	ellix ePC ateway URL ID: Secret: 'y: Server URL it T	o Saas Se	Cancel	onfiguration	15 🤡	Proxy Port:		9 9 9

After editing server details QRadar admin can change the details and Test, then Save the Trellix ePO Saas details. If the QRadar admin does not want to provision again then the admin must click "Cancel" button to retain old settings. Refer the screenshot below-

≡	IBM QRadar										
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
Trellix	Trellix ePO Saa	as Config	Trellix ePO Saas Eve	ents Config	Audit Lo	og					
Trellix	Trellix ePO Saa	as Config	Trellix ePO Saas Eve Trellix ePO Saas Eve API Ga Client Client eve API Ke Proxy Proxy Proxy	ID: Secret:	Audit L	es rver Cor	nfiguration		Proxy Port		
			Sa	ve T	est	Cancel]				

Apply Trellix ePO Saas Apply Tags

The "**Trellix ePO Saas Apply Tag**" action in QRadar console will allow the QRadar user to select an IP from "**Log Activity**" page (only if the selected IP is managed by ePO server) and apply any tag which exists in the configured ePO on a system/IP. This action from QRadar server can initiate ePO's automatic tag-based policy/task as a remediation action.

Before performing "**Trellix ePO Saas Apply Tag**" action from QRadar console, login to Trellix ePO Saas server and go to **Menu | Systems | System Tree** page and search for the "IP" (in our example it is "10.254.46.95") and check the list of tags applied for this IP. Refer the screenshot below-

\equiv Trellix	Protection Workspace S	System Tree MVI	SION Marketplace	Client Tasks	Product Deployment	~ 🌲	?	£	:::
System Tree	Systems New Subgroups System Tr	ree Permissions							
System Tree	Systems Policies Client Tasks	Sorting Deploy							
✓ My Organization	Preset:	Custom:	Quick find:						
mani	This Group and All Subgroups ~	None ~			Apply <u>Clear</u> Show	v selected rows			
My System Tree Group	System Name	 Managed State 	Tags		IP address	User Name		Last Comm	n
My System Tree Group 2	CLDBGQAE00260	Managed			10.254.46.95	cloudadmin		5/16/22 9:	5
My System Tree Group 3									
silambu									
Lost and Found									

Note: At this stage the IP (10.254.46.95) does not have any tag applied.

Go to "Log Activity" page in QRadar console and right click on **Source IP** column and select **More Options** | **Trellix ePO Saas Apply Tag.** This action will open a new page to perform "**Trellix ePO Saas Apply Tag**" action.

	IBM QRadar								(Ċ	<u>0</u>
shboare	rd Offenses Log Activity Network Activity Assets	Reports Risks Vulnerabilities	Admin Pulse Use Case Ma	inager Trelix ePO Saas Connector						System Tim	ne: 5:09 PN
											_
arch	 Quick Searches Y Add Fitter Save Criteria Save Results 	Gancel 🤸 False Positive Rules ♥ Act	ions 🔻								U
			Δ.				A.				
5							A				
0											-
	11:30 AM 12:00 PM 12:30	PM 1:00 PM	1:30 PM 2:00 PM	2:30 PM	3:00 PM	3:30 PM	4:00 PM	4:30 F	PM	5:00 PM	E.
			Update	Details							
			(Hide	Charto)							
	Event Name	Log Source	Event Time T	Low Level Category	Source II	P Source	Destination IP	Destinat	lisername	Magnit	ehute
In	Varied Be delated	Trailix aDO Saas Threat Events	Count 6 May 0 2022 4 05 10 DM	Virue Datacted	10.254.46.05	Port	10.254.46.95	Port	CLORCOAE	magni	iouc.
10	fected file deleted	Trailix ePO Sads Threat Events	6 May 9, 2022, 4:05:19 PM	Virus Detected	10.204.40.90	0	10.204.46.90	0	CLDBGQAE.		
64	le infacted No classer susibilite file delated successfully	Tralix and Saar Threat Events	1 May 9, 2022, 4:05:19 PM	Virus Detected	10.254.46.95	0	10.254.46.55	0	CLOBGQAE		_
100	le infected. No cleaner available, file deleted successfully	Trelly ePO Saas Threat Events	1 May 9, 2022, 4:05:19 PM	Max Delected	10.254	0	10.204.40.00		CLDBCOAE		in i
In	Vected file deleted	Trellix ePO Saas Threat Events	1 May 9 2022, 4:05:19 PM	Virus Detected	10.254	liter on Source IP is 10	254.46.95		CLOBGOAE		
In	vierted file deleted	Trellix ePO Saas Threat Events	1 May 9 2022 4 05 19 PM	Virus Detected	10.254 F	Filter on Source IP is no	t 10.254.46.95		CLDBGOAE		
16	le infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1 May 9 2022 3 05 20 PM	Virus Detected	10.254 F	Filter on Source or Dest	ination IP is 10.254.46.95		CLDBGQAE		
In	viected file deleted	Trellix ePO Saas Threat Events	13 May 9 2022 3 05 20 PM	Virus Detected	10 254 9 0	Quick Filter		•	CLDBGQAE		
The	le infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1 May 9 2022 3:05:20 PM	Virus Detected	10.254 + F	alse Positive			CLDBGQAE		
In	nfected file deleted	Trellix ePO Saas Threat Events	1 May 9, 2022, 3 05:20 PM	Virus Detected	10.254 🏷 V	/iew path from 10.254.4	46.95 to 10.254.46.95		CLDBGQAE		
In	nfected file deleted	Trellix ePO Saas Threat Events	1 May 9, 2022, 3:05:20 PM	Virus Detected	10.254 V	/iew in DSM Editor			CLDBGQAE.		
In	nfected file deleted	Trellix ePO Saas Threat Events	1 May 9, 2022, 3:05:20 PM	Virus Detected	10.254	Aore Ontions			lavianto		
110	le infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254 40 50		46.95	10	vavigate		-
file	le infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	nformation		•
510	le infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0 F	Run Forensics Re	ecovery	
file	le infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	OF	Run Forensics Se	earch	
In	nfected file deleted	Trellix ePO Saas Threat Events	13 May 9, 2022, 1 50 20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	Plugin options	_	`
In	nfected file deleted	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0/1	Freilix ePO Saas	Apply Tag	
								The second second	and the second	COLUMN TWO IS NOT	And the owner of the
1 Inf	nfected file deleted	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95		relix ePO Saas	Remove 1a	30

Refer the screenshot below-

If the selected **Source IP** address is managed by ePO server, the new page will allow the user to select a tag from the list and click "Apply". If the tag is applied successfully in ePO server, you will get "**<tagname>** is applied to the selected device." Message as shown in the screenshot below-

now 10 v entries	Search:
Select	Tags available in Trellix ePO Saas :
0	gmfgn
۲	fireeye
0	dec21
0	mani123
0	abc123
0	Jan4
0	test1
0	mcafee
<u></u>	textTag1
nowing 51 to 60 of 74 entries	Previous 1 4 5 6 7 8 Next

Note: If the selected tag is already applied for the system IP in the ePO, you will receive "**This device is** already tagged with <tagname>." as a response message.

Refer the screenshot below-

Trellix ePO Saas Tags Show 10 entries	Search:
Select	Tags available in Trellix ePO Saas :
0	gmfgn
۲	fireeye
0	dec21
0	mani123
0	abc123
0	Jan4
0	test1
0	mcafee
<u> </u>	testTag1
Showing 51 to 60 of 74 entries	Previous 1 4 5 6 7 8 Next
Apply tag	3

Once the "**Trellix ePO Saas Apply Tag**" action in QRadar server is successful you can see the same in the Trellix ePO's Saas system tree page next to the selected system. Refer the screenshot below-

\equiv Trellix	Prote	ction Work	space	Syster	n Tree	MVI	SION Marke	tplace	Client Tasks	Product De	eployment	~		0	£	
System Tree	/ Systems	New Subgrou	ups System	Tree Perr	nissions											
System Tree	Syste	ms Policies	Client Task	s So	ting	Deploy										
\sim My Organization	Pres	et:		Cu	stom:		Quick find:				Char					
mani	This	Group and A	II Subgroups	~ N	one	~				Apply <u>Cle</u>	ar	selected row	s			
My System Tree Group	1	System M	lame	~	Manag	ed State		Tags		IP address		User Name			Last Corr	ımı
My System Tree Group 2					Manag	ed		fireeve		10.254.46.95		cloudadmin			5/16/22	9:5
My System Tree Group 3				-			-		_	-						
silambu																
Lost and Found																

Note: In case the selected IP is not managed by the Trellix ePO Saas configured in the QRadar-Right click on **Source IP** column and select **More Options | Trellix ePO Saas Tags** will display a message indicating "This system is not managed by currently configured Trellix ePO Saas". Refer the screenshot below-

🖊 Trellix ePO Tags

This system is not managed by currently configured Trellix ePO Saas

When the Trellix ePO Saas Connector has not been configured at all, Following failure message will be displayed-

/ Trellix ePO Tags

Configure Trellix ePO Saas Connector to proceed.

Apply Trellix ePO Saas Remove Tags

The "**Trellix ePO Saas Remove Tag**" action in QRadar console will allow the QRadar user to select an IP from "**Log Activity**" page (only if the selected IP is managed by ePO server) and apply any tag which exists in the configured ePO on a system/IP. This action from QRadar server can initiate ePO's automatic tag-based policy/task as a remediation action.

Before performing "**Trellix ePO Saas Remove Tag**" action from QRadar console, login to Trellix ePO Saas server and go to **Menu | Systems | System Tree** page and search for the "IP" (in our example it is "10.254.46.95") and check the list of tags applied for this IP. Refer the screenshot below-

\equiv Trellix	Protection Workspace	System Tree	MVISION Marketplace	Client Tasks F	Product Deployment	~ .	➁ 👤 🗰
System Tree	v Systems New Subgroups System	Tree Permissions					
System Tree	Systems Policies Client Task	s Sorting D	ploy				
\sim My Organization	Preset:	Custom:	Quick find:				
mani	This Group and All Subgroups	✓ None	~		Apply <u>Clear</u> Show	v selected rows	
My System Tree Group	System Name	✓ Manage	I State Tags	IP a	address	User Name	Last Commu
My System Tree Group 2	8 0	Manage	1	10.	254.46.95	cloudadmin	5/16/22 9:5
My System Tree Group 3				_			
silambu							
Lost and Found							

Note: At this stage the IP (10.254.46.95) does not have any tag applied.

Go to "Log Activity" page in QRadar console and right click on **Source IP** column and select **More Options** | **Trellix ePO Saas Remove Tag.** This action will open a new page to perform "**Trellix ePO Saas Remove Tag**" action.

Refer the screenshot below-

IDM Grada										Ċ
d Offenses	Log Activity Network Activity Assets	Reports Risks Vulnerabilities	Admin Pulse Use Case Ma	nager Trellix ePO Saas Connector						System Time
Ouick Searcher	rs 🔻 🍟 Add Filter 🕌 Save Criteria 🗊 Save Result	ts 👰 Cancel 🤸 False Positive Rules 🔻 Actio	ns Ŧ							
								5/3/22, 3	17 PM - 5/10/22, 3	3.17 PM 🗸
30 PM	May 4 5:30 PM 1	May 5 5:30 PM Ma	y 6 5:30 PM	May 7 5:30 PM Details	May 8	5:30 PM	May 9 5	:30 PM	May 10	
			(contraction)							
			(Hide C	harts)						
	Event Name	Log Source	Event Time -	Low Level Category	Source	IP Source	Destination IP	Destina	at Username	Magnitu
fected file delete	Event Name	Log Source Trelix ePO Saas Threat Events	(Hot 0 Event Time ▼ Count 6 May 9, 2022, 4:05:19 PM	Low Level Category Virus Detected	Source	IP Source Port Filter on Source IP is 1	Destination IP 0.254.46.95	Destina Port	t Username	Magnitu
lected file delete	Event Name	Log Source Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events	Event Count Time ▼ 6 May 9, 2022, 4:05:19 FM 1 May 9, 2022, 4:05:19 PM 5 May 9, 2022, 4:05:19 PM	Low Level Category Virus Datasted Virus Detected	Source 10.2544 10.2544	IP Source Port Filter on Source IP is 1 Filter on Source IP is n	Destination IP 0.254.46.95 of 10.254.46.95	Destina Port	Username CLDBGQAE CLDBGQAE	Magnitu
fected file delete fected file delete e infected. No cle	Event Name	Log Source Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events	(Hot Count Time Count 6 May 9, 2022, 4:05:19 PM 1 May 9, 2022, 4:05:19 PM 1 May 9, 2022, 4:05:19 PM 1 May 9, 2022, 4:05:19 PM	Low Level Category Virus Detected Virus Detected Virus Detected Virus Detected	Source 10.254.4 10.254.4 10.254.4 10.254.4	IP Source Port Filter on Source IP is 1 Filter on Source IP is n Filter on Source or Des	Destination IP 0.254.46.95 of 10.254.46.95 stination IP is 10.254.46.95	Destina Port	at Username CLDBGQAE CLDBGQAE CLDBGQAE	Magnitu
level liedelee fected file delete e infected. No cle e infected. No cle	Event Name	Log Source Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events	Event Count Time ▼ 6 May 9, 2022, 4:05:19 FM 1 May 9, 2022, 4:05:19 FM	Low Level Category Virus Detected	Source 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4	IP Source Port Filter on Source IP is 1 Filter on Source IP is n Filter on Source or Des Ouick Filter	Destination IP 0.254.46.95 of 10.254.46.95 stination IP is 10.254.46.95	Destina Port	t Username CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE	Magnitu
fected file delete fected file delete e infected. No cle e infected. No cle fected file delete fected file delete	Event Name cl cd earer available, file deleted successfully earer available, file deleted successfully cl cd	Log Source Treltx ePO Saas Threat Events Treltx ePO Saas Threat Events	Event Count Time ▼ 6 May 9, 2022, 4205 19 PM 1 May 9, 2022, 4205 19 PM	Low Level Category Virus Detected Virus Detected Virus Detected Virus Detected Virus Detected Virus Detected	Source 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4	IP Source Port Filter on Source IP is 1 Filter on Source IP is n Filter on Source or Des Quick Filter False Posttive	Destination IP 0.254.46.95 ot 10.254.46.95 stination IP is 10.254.46.95	Destina Port	t Username CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE	Magnitu
Cored landscore fected file delete e infected. No cle fected file delete fected file delete e infected. No cle	Event Name	Log Source Trielix ePO Saas Threat Events Trelix ePO Saas Threat Events	Event Count Tme ▼ 6 May 9, 2022, 4:05:19 PM 1 May 9, 2022, 4:05:19 PM	Low Level Category Virus Detected Virus Detected Virus Detected Virus Detected Virus Detected Virus Detected Virus Detected	Source 10254.4 10254.4 10254.4 10254.4 10254.4 10254.4 10254.4	IP Source Port Filter on Source IP is 1 Filter on Source IP is n Filter on Source or Des Quick Filter False Positive View path from 10 254	Destination IP 0.254.46.95 of 10.254.46.95 stination IP is 10.254.46.95	Destina Port	t Username CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE	Magnitu
fected file delete fected file delete e infected. No cle e infected. No cle fected file delete fected file delete infected. No cle infected. No cle	Event Name di disaner available, file deleted successfully di di di di di di di di di di	Log Source Trelix eFO Saas Threat Events Trelix eFO Saas Threat Events	(in the control of the control	Low Level Category Whis Detected Whis Detected Whis Detected Whis Detected Whis Detected Whis Detected Whis Detected Whis Detected Whis Detected Whis Detected	Source 10254.4 1025	IP Source Port Filter on Source IP is 1 Filter on Source IP is 1 Filter on Source or Des Quick Filter False Positive View path from 10.254 View path Filter.	Destination IP 0.254.46.95 ot 10.254.46.95 stination IP is 10.254.46.95 46.95 to 10.254.46.95	Destina Port	t Username CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE	Magnitu
lected tile delete fected file delete e infected. No cle fected file delete fected file delete e infected. No cle fected file delete e infected No cle	Event Name d d d exert subscription d d d d d d d d d d d d d	Log Source Treate eFO Saas Threat Events Treate eFO Saas Threat Events	Event Count Time ♥ 6 May 9, 2022, 4 (05:15) FM. 1 May 9, 2022, 4 (05:20) FM. 1 May 9, 2022, 3 (05:20) FM. 1 May 9, 2022, 3 (05:20) FM.	Anni) Low Level Category Virus Detected Virus Detec	Source 10.254.4	IP Source Part Filter on Source IP is 1 Filter on Source or Des Quick Filter False Positive View path from 10.254 View DRM Editor	Destination IP 0.254.46.95 of 10.254.46.95 titnation IP is 10.254.46.95 46.95 to 10.254.46.95	Destina Port	t Username CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE CLDBGQAE	Magnitu
fected file dealers fected file dealers e infected. No cle fected file dealers fected file dealers infected. No cle fected file dealers e infected. No cle fected file dealers	Event Name d d dener svalable, file odelted successfully d d d d d d d d d d d d d	Log Source Trelix eFO Saas Threat Events Trelix eFO Saas Threat Events	Image Image Image 6 May 9, 2022, 403:19 PM 1 May 9, 2022, 403:19 PM 1 May 9, 2022, 405:19 PM 1 May 9, 2022, 405:10 PM 1 May 9, 2022, 405:20 PM 1 May 9, 2022, 305:20 PM	Low Level Category Vers Detected	Source 10.254.4 10.25	IP Source Part Filter on Source IP is 1 Filter on Source IP is n Filter on Source or Des Quick Filter False Positive View path from 10.254 View in DSM Editor More Options	Destination IP 0.254.46.95 ct 10.254.46.95 stration IP is 10.254.46.95 46.95 to 10.254.46.95	Destina Port	at Username CLDBGQAE. CLDBGQAE. CLDBGQAE. CLDBGQAE. CLDBGQAE. CLDBGQAE. CLDBGQAE. Navigate	Magnitu
lected file delete infected file delete infected. No cie infected. No cie fected file delete fected file delete infected file delete infected. No cie fected file delete infected file delete	Event Name SI	Log Source Treative 640 Saas Thread Events Treative 640 Saas Thread Events	Unit Unit <t< td=""><td>Low Level Category Viris Detected Viris Detected</td><td>Source 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4</td><td>IP Source Port Filter on Source IP is 1 Filter on Source IP is n Filter on Source IP is 0 Source Filter. False Positive View path from 10.254 View In DSM Editor More Options</td><td>Destination IP 0.254.46.95 ot 10.254.46.95 stination IP Is 10.254.46.95 46.95 to 10.254.46.95</td><td>Destina Port</td><td>St Username CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE Navigate Information</td><td>Magnitu</td></t<>	Low Level Category Viris Detected	Source 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4 10/254.4	IP Source Port Filter on Source IP is 1 Filter on Source IP is n Filter on Source IP is 0 Source Filter. False Positive View path from 10.254 View In DSM Editor More Options	Destination IP 0.254.46.95 ot 10.254.46.95 stination IP Is 10.254.46.95 46.95 to 10.254.46.95	Destina Port	St Username CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE Navigate Information	Magnitu
fected file delate e infected. No cle infected. No cle fected file delate e infected. No cle fected file delate e infected. No cle fected file delate fected file delate fected file delate fected file delate	Event Name St d d camer available, file deleted successfully d mamer available, file deleted successfully d camer available, file deleted successfully d d d d	Log Source Trelix ePO Saas Threat Events Trelix ePO Saas Threat Events	Unit Time ♥ 6 May 9, x0x2, 405 19 PM 1 May 9, x0x2, x0.51 9 PM 1 May 9, x0x2, x0.52 0 PM 1 May 9, x0x2, x0.52 0 PM 1 May 9, x0x2, x0.52 0 PM 1 May 9, x0x2, x0.50 2 PM	Low Level Category Vers Detected Vers Detect	Source 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 5.95 10.254.46.95	IP Source Pert Filter on Source IP is 1 Filter on Source or Des Quick Filter False Positive View path from 10.254 View In DSM Editor More Options 0	Destination IP 0.254.46.95 ct 10.254.46.95 stination IP is 10.254.46.95 46.95 to 10.254.46.95 10.254.46.95 10.254.46.95	Destina Port	St Username CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE Navigate Information Run Forensics Ré	Magnitu
ficited file detects ficited file detects inflected. No cle filected file detects inflected file detects inflected. No cle fected file detects filected file detects file dete	Event Name SI	Log Source Testix cFO Saas Thread Events Trafix cFO Saas Thread Events	Unit Time ▼ 6 May €, 2022, 400-119 PM 1 May €, 2022, 400-219 PM 1 May €, 2022, 300-20 PM	Low Level Category Viris Detected	Source 10.254.4	IP Source P to Port Filter on Source IP is 1 Filter on Source IP is 1 Filter on Source IP is 1 Filter on Source or Des Quick Filter. False Postive View path from 10.254 View path from 10.254 View path from 10.254 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Destination IP 0.254.46.95 010.254.46.95 stination IP is 10.254.46.95 46.95 to 10.254.46.95 10.254.46.95 10.254.46.95 10.254.45.95	Destin: Port	t Username CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE Navigate Information Run Forensics Re Run Forensics Se	Magnitu
Excel Incolored fected file delete infected. No cle fected file delete fected file delete infected. No cle infected. No cle fected file delete fected file delete fected file delete infected. No cle infected. No cle	Event Name St	Log Source Trelix eFO Saas Threat Events Trelix eFO Saas Threat Events	Unit Time ♥ 6 May 9, 2022, 403 19 PM 1 May 9, 2022, 403 19 PM 1 May 9, 2022, 405 19 PM 1 May 9, 2022, 305 20 PM	Low Level Category Viss Detected	Source 10,254.4 10,254.4 10,254.4 10,254.4 10,254.4 10,254.4 10,254.4 10,254.4 10,254.4 10,254.4 10,254.4 10,254.46,95 10,254.46,95	IP Source IP is Port Filter on Source IP is n Filter on Source or Des Quick Filter False Postit View path from 10.254 View in DRM Filter 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Destination IP 0.254.45 95 40 10.254.45 95 Almation IP Is 10.254.45 95 10.254.46 95 10.254.46 95 10.254.46 95 10.254.46 95	Destin: Port	t Username CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE CLDBGOAE Navigate Information Run Forensics Re Run Forensics Re	Magnitu
Includ Ste Goods fected file delete e infected. No cle e infected. No cle fected file delete infected file delete e infected. No cle fected file delete fected file delete e infected. No cle e infected. No cle e infected. No cle	Event Name	Log Source Trelix cFO Saas Threaf Events	Unit Unit <thunit< th=""> Unit Unit <th< td=""><td>Low Level Category Wins Delicated Wins Delicated</td><td>Source 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.46 10.254.46 10.254.46 10.254.46 10.254.46 10.254.46 10.254.46 10.254.46</td><td>IP Source IP is Filter on Source or Des Quick Filter False Positive View path from 10.254 View path from 10.254 View path from 10.254 More Options</td><td>Destination IP 0.254.46.95 01.0254.45.95 atmation IP is 10.254.46.95 10.254.46.95 10.254.46.95 10.254.46.95 10.254.46.95 10.254.46.95</td><td>Destina Port</td><td>t Username CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE Navigate Information Run Forensics Re Run Forensics Se Plugin options.</td><td>Magnitu</td></th<></thunit<>	Low Level Category Wins Delicated	Source 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.4 10.254.46 10.254.46 10.254.46 10.254.46 10.254.46 10.254.46 10.254.46 10.254.46	IP Source IP is Filter on Source or Des Quick Filter False Positive View path from 10.254 View path from 10.254 View path from 10.254 More Options	Destination IP 0.254.46.95 01.0254.45.95 atmation IP is 10.254.46.95 10.254.46.95 10.254.46.95 10.254.46.95 10.254.46.95 10.254.46.95	Destina Port	t Username CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE CLDBGDAE Navigate Information Run Forensics Re Run Forensics Se Plugin options.	Magnitu
Encode the delete infected file delete infected file delete infected file delete fected the delete infected file delete infected file delete fected the delete infected. No cic infected file delete infected file delete infected file delete infected file delete infected file delete infected file delete infected file delete infected. No cic	Event Name St	Log Source Teslex eFO Saas Thread Events Trelix eFO Saas Thread Events	Unit Time ✓ 6 May 9, 2022, 400 19 PM 1 May 9, 2022, 400 19 PM 1 May 9, 2022, 401 19 PM 1 May 9, 2022, 402 19 PM 1 May 9, 2022, 402 19 PM 1 May 9, 2022, 20 502 PM 1 May 9, 2022, 3062 0PM 1 May 9, 2022, 1502 0PM	Low Level Category Visis Detected	Source 10.254 4 10.254 46.95 10.254 46.95 10.254 46.95 10.254 46.95	IP Source IP is Teleson Source IP is Teleson Source IP is Teleson Source IP is n Fitter on Source or Des Quick Fitter. Fatse Postfer Nore Options- 0 0 0 0 0 0 0 0 0	Destination IP 0.254.46.95 0.254.46.95 0.254.46.95 0.254.46.95 0.0.254.46.95 0.0.254.46.95 0.0.254.46.95 0.0.254.46.95 0.0.254.46.95 0.0.254.46.95 0.0.254.46.95	Destina Port	tusername CLDBGDAE Tellix ePO Saas Tellix ePO Saas	Magnitu ecovery earch Apply Tag
Exceed the deleted fected the delete infected. No clic infected No clic fected the delete fected the delete infected. No clic fected the delete fected the delete	Event Name	Log Source Technology Sease Thread Events Trelix ePO Saas Thread Events	Image Image Control Tana ♥ May 9, 2022, 403:19 FM May 9, 2022, 403:19 FM May 9, 2022, 405:19 FM May 9, 2022, 405:20 FM May 9, 2022, 305:20 FM M	Low Level Category Vess Detected	Source 10/254 10	IP Source IP is Filter on Source IP is Filter on Source IP is Filter on Source Or Des Quick Filter. Palse Positive Outer Filter. View palt from 10 254 View palt from 10 254 More Options.	Destination IP 0 254.46.95 0 254.46.95 atmation IP is 10 254.46.95 46.95 to 10 254.46.95 10 254.46.95 10 254.46.95 10 254.46.95 10 254.46.95 10 254.46.95 10 254.46.95	Destin: Port	t Username CLDBGOAE C	Magnitu Becovery earch Apply Tan Remove Ta

If the selected **Source IP** address is managed by ePO server, the new page will allow the user to select a tag from the list and click "Remove tag". If the tag is removed successfully in ePO server, you will get

Sw 10 V entries	Search:
Select	Tags applied in Trellix ePO Saas :
	Server
	879de20e-5b30-4369-8699-ee3547f30e9bManikandan
	879de20e-5b30-4369-8699-ee3547f30e9bMd4aandan
	879de20e-5b30-4369-83547f30e9bMd4aandan
	879de20e-5b30-4369-8699-ee354bMd4aandan
	mani1234
	sssmani1234
	sssmaniSIL1234
	sssmaniSI
owing 1 to 10 of 11 entries	Previous 1 2 Ne

"<tagname> is removed from the selected device." Message as shown in the screenshot below-

Note: If the selected tag is already removed for the system IP in the ePO, you will receive "**This device is** already removed with <tagname>" as a response message.

Refer the screenshot below-

bw 10 V entries	Search:						
Select	Tags applied in Trellix ePO Saas :						
	Server						
	nidhi33						
	nidhi303						
	fireeye						
wing 1 to 4 of 4 entries	Previous 1 Nex						

Once the "**Trellix ePO Saas Remove Tag**" action in QRadar server is successful you can see the same in the Trellix ePO's Saas system tree page next to the selected system. Refer the screenshot below-

\equiv Trellix	Protection Workspace	System Tree	MVISION Marketplace	Client Tasks Produc	t Deployment	~ 🌲	0 👤 🗰
System Tree	Systems New Subgroups System	em Tree Permissions					
System Tree	Systems Policies Client	Tasks Sorting De	ploy				
\vee My Organization	Preset:	Custom:	Quick find:				
mani	This Group and All Subgroup	ps 🗸 None	~	Apply	<u>Clear</u> Show se	lected rows	
My System Tree Group	System Name	✓ Managed	State Tags	IP address	Us	ser Name	Last Commu
My System Tree Group 2	CLDBGOAE00260	Managed		10.254.46.9	5 clo	oudadmin	5/16/22 9:5
My System Tree Group 3							
silambu							
Lost and Found							

Note: In case the selected IP is not managed by the Trellix ePO Saas configured in the QRadar-Right click on **Source IP** column and select **More Options | Trellix ePO Saas Tags** will display a message indicating "This system is not managed by currently configured Trellix ePO Saas". Refer the screenshot below🖊 Trellix ePO Tags

This system is not managed by currently configured Trellix ePO Saas

When the Trellix ePO Saas Connector has not been configured at all, -Following failure message will be displayed-

🖊 Trellix ePO Tags

Configure Trellix ePO Saas Connector to proceed.

Trellix ePO Saas Device Details

The **"Trellix ePO Saas Device Details**" action in QRadar console will allow the QRadar user to select an IP from **"Log Activity**" page (only if the selected IP is managed by ePO server).

Refer the screenshot below-

≡	IBM QRadar									(Ċ	9
Dashbo	oard Offenses Log Activity Netwo	ork Activity Assets	Reports Risks Vulnerabilities	Admin Pulse Use Case M	anager Trellix ePO Saas Connector						System Time: 7:0	31
Search	V Duick Searches V VAdd Filler	Criteria	Cancel S False Positive Rules * Art	lons ¥								
0	,									JV		
	9:30 PM 1:30 AM ML	ay / 9:30 AM	1:30 PM 5:30 PM 9:3	30 PM 1:30 AM May 8	9:30 AM 1:30 PM	5/30 PM 9.	30 PM 1:30 AM	May 9 9:	30 AM	1:30 PM	5:30 PM	
				Update	n Details							
				(Hide	Charts)							
	Event Name		Log Source	Event Time -	Low Level Category	Source	IP Source	Destination IP	Destinat	Username	Magnitude	
6	Infected file deleted		Trellix ePO Saas Threat Events	6 May 9 2022 4:05:19 PM	Virus Delected	10 254 40.05	Port	40.054 10.05	Port	CLDBGQAE		ų
•	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 4:05 19 PM	Virus Detected	10.254	Filter on Source IP is 10	1.254.46.95		CLDBGQAF		1
	file infected. No cleaner available, file deleter	d successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 4:05:19 PM	Virus Detected	10.254	Filter on Source IP is no	10.254.46.95		CLDBGQAE		
6	file infected. No cleaner available, file delete	d successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 4:05:19 PM	Virus Detected	10.254	Filter on Source or Dest	nation IP is 10.254.46.95	6	CLDBGQAE	-	
	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 4:05:19 PM	Virus Detected	10.254	Quick Filter		•	CLDBGQAE	-	
•	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 4.05 19 PM	Virus Detected	10.254	False Positive			CLDBGQAE	-	
	file infected. No cleaner available, file delete	vd successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 3:05:20 PM	Virus Detected	10.254	View path from 10.254.4	16.95 to 10.254.46.95		CLDBGQAE	-	
•	Infected file deleted		Trellix ePO Saas Threat Events	13 May 9, 2022, 3.05:20 PM	Virus Detected	10.254	View In DSM Editor	and the state of the		CLDBGQAE	-	
•	file infected. No cleaner available, file delete	d successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 3:05:20 PM	Virus Detected	10.254	More Ontions			OLDBOOME		
•	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 3:05:20 PM	Virus Detected	10.254	more options		-	avigate		
•	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 3.05:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0 11	ntormation		
	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 3:05:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0 R	tun Forensics Re	covery	
•	file infected. No cleaner available, file delete	d successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0 R	tun Forensics Sei	arch	
	file infected. No cleaner available, file delete.	d successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0 P	lugin options		j
	file infected. No cleaner available, file delete	d successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0 / 1	rellix ePO Saas A	Apply Tag	
•	file infected. No cleaner available, file delete	d successfully	Trellix ePO Saas Threat Events	1 May 9, 2022, 1.50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0 1	rellix ePO Saas F	Remove Tag	
•	Infected file deleted		Trellix ePO Saas Threat Events	13 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	rellix ePO Saas F	Device Details	
•	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	ter e eddart		
•	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 1:50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	CLDBGQAE		
۲	Infected file deleted		Trellix ePO Saas Threat Events	1 May 9, 2022, 1.50:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	CLDBGQAE		
	file infected. No cleaner available, file delete	d successfully	Trellix ePO Saas Threat Events	1 May 6, 2022, 7.12:33 PM	Virus Detected	10.254.36.82	0	10.254.36.82	0	CLDBGDEV		
	The intected. No cleaner available, file delete.	na successfully	Trellix ePO Saas Threat Events	1 May 6, 2022, 7:12:33 PM	virus Detected	10.254.36.82	0	10.254.36.82	0	LDBGDEV	the second se	

This action will open a new popup page to show system details from Trellix ePO Saas server. Considering the system 10.254.46.95. Refer the screenshot below-



In case the selected IP is not managed by the Trellix ePO Saas configured in the QRadar-

Right click on **Source IP** column and select **More Options | Trelix ePO Saas Device Details** will display a message indicating "This system is not managed by currently configured Trellix ePO Saas". Refer the screenshot below-

Trellix ePO Device Details

This device is not managed by currently configured Trellix ePO Saas

When the Trellix ePO Saas config is not present and admin tried to take an action then following failure message will be displayed:

/ Trellix ePO Device Details

Configure Trellix ePO Saas Connector to proceed.

Create/Update EDR Investigation for an offense in QRadar

QRadar Admins can create an Investigation for any offense to have additional insight about the offense in MVISION EDR. Admins will have the option to either create a new Investigation or update an existing Investigation for an offense in MVISION EDR.

Note: Only Offense types with IP and Hostname are supported to create EDR Investigation. And EDR supports creation/update of 20 investigations in a single day.

• Go to Offense page in QRadar console

 Before taking any action, select any offense for which EDR Investigation to be created as shown below:

													() <i>(</i>)	<u>o</u>
Dashboard Offenses Lo	g Activity	Netwo	k Activity Assets Reports Risks Vulnerabilities	Admin Pulse	Use Case Manager	Trellix ePO	Saas Connector						System Tim	e: 7:11 PM
Offenses	Search	🕶 📕 s	ave Criteria 🛛 Actions 🔻 📇 Print 🎾 Tune 🏏 Create/Update Investigation i	in MVISION EDR								Last Ref	esh: 00:00:20	ø 0
My Offenses All Offenses	Current	t Search de Hidde	Parameters: n Offenses (Clear Filter), Exclude Closed Offenses (Clear	All O	ffenses View Offe	nses with: Sele	ct An Option:	~						
By Source IP	9	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start I	Date
By Destination IP		1	MVISION Insights Event preceded by Infected file deleted preced	Source IP	10.254.46.95		10.254.46.95	10.254.46.95	Multiple (2)	Multiple (2)	146	0	May 6, 2022, 1	1:14:28 AM
By Network														
Rules														

Click on Create/Update Investigation in MVISION EDR button available on offense toolbar as shown below:

≡ IBM QRadar												į	t ç	<u> </u>
Dashboard Offenses Lo	a Activity	Netwo	nk Activity Assets Reports Risks Vulnerabilities	Admin Pulse	Use Case Manager	Trelik ePO	Saas Connector						System Time	8. 7:11 PM
Offenses	Search.	•	šave Criteria Actions 🔻 📇 Print 🥻 Tun 🖊 Create/Update Investigation I	n MVISION EDR								Last Refre	sh: 00:00:20	20
My Offenses All Offenses By Category	Curren	it Searc de Hidd	h Parameters: en Offenses (Clear Filter), Exclude Closed Offenses (Clear	All O Filter)	ffenses View Offe	nses with: Sele	ct An Option:	~						
By Source IP	9	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start D	Jate
By Destination IP By Network Rules		1	MVISION insights Event preceded by infected file deleted preced.	Source IP	10.254.46.95	-	10.254.46.95	10.254.46.95	Multiple (2)	Multiple (2)	146	0	May 6, 2022, 11	:14:28 AM

• If the existing Investigation doesn't exist, then Admin will see a window where details of newly created EDR Investigation will be shown as depicted below:

MVISIONEDR	Investigation Status
Investigation id: c17f6	5e0-cf83-11ec-a903-000000000000 is created for offense id: 1.
Investigation Details :	
ld:c17f65e0-cf83-11e	c-a903-00000000000
Name : MVISION Insig	hts Event preceded by Infected file deleted preceded by file deleted successfully preceded by file infected. No
CaseHint	
CaseType : others	
CasePriority : High	

• If the investigation already exists in MVISION EDR then Admin will be presented with a window with Investigation id detail as shown below:

/ MVISION EDR Investigation Status	
Investigation id: c17f65e0-cf83-11ec-a903-000000000000 has already been created for this offense id: 1. If you want to update this inv Update.	estigation, click
Update	

• Admin can decide whether they want to update the EDR Investigation details. In case if they choose to update, they will be presented with updated EDR Investigation details as shown below:

MVISION	EDR Investigation Status
Investigation i Update.	d: c17f65e0-cf83-11ec-a903-00000000000 has already been created for this offense id: 1. If you want to update this investigation, click
Update	
Investigation i	d: c17f65e0-cf83-11ec-a903-00000000000 for this offense id: 1 is updated.
Investigation [Details:
Id: c17f65e0-c	:f83-11ec-a903-00000000000
Name: MVISIC	<u>2N Insights</u> Event preceded by Infected file deleted preceded by file deleted successfully preceded by file infected. No
CaseHint	
CaseType: oth	ers

• In case where EDR investigation creation fails, below mentioned failure message will be displayed:

MVISION EDR Investigation Status Failed to create EDR Investigation for offense id: 2

Poll Threat and Insights Events from Trellix ePO Saas to QRadar

This feature enables QRadar Admins to fetch threat and insights events from Trellix ePO Saas and show on Log Activity page. Admins must configure scheduling criteria for polling the events by providing how frequently polling must be done.

Poll Configuration

To configure this, navigate to **Trellix ePO Saas Connector** App > click **on Trellix ePO Saas Events Config** tab as shown below:

≡	IBM QRadar											
Dashboard	d Offenses	Log Activity	Network	Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
Trellix	Trellix ePO Sa	as Config	Trellix ePO	Saas Ev	ents Config	Audit L	og					
				Schedu	heduling at Event ION Insight ule polling ir	s Events s tevents tart Pollin	a for po nutes):	lling MVISIC	ON Insigh	nts and o	ePO Saas	

Admin can specify polling interval in minutes. Range of the interval is : 5 minutes to 2880 minutes

=	IBM QRadar										
Dashboard	Offenses	Log Activity	Network A	Activity Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
Trellix	Trellix ePO Saa	as Config	Trellix ePO	Saas Events Config	Audit Lo	og					
				Scheduling Threat Even MVISION Insigh Schedule polling 10 Edit S Saved polling cri	g Criteria ts ts Events nterval (min itart Polling teria for Tre	utes):	top Polling aas and MVISIO	N Insigh	ts and of the second seco	ePO Saas	

Once the interval is saved, Admins will be able to start the poll for threat events. Once the poll is started, background process will fetch the events generated between the poll start time and interval specified. For example: if poll started at 2:00 PM and interval specified is 10 minutes then it will pull all events received on Trellix ePO Saas between 2:00 PM and 2:10 PM in the first go. In next poll, background process will pull all events received on ePO from 2:10 PM to 2:20 PM and so on.

Note: UTC time is considered for performing polling operation. Make sure QRadar server and Trellix ePO Saas are time-synced.

To start polling, click on **Start Polling** button once polling interval is saved as shown below:

≡	IBM QRadar									
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports F	Risks Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
Trellix	Trellix ePO Sa	as Config	Trellix ePO Saas E	vents Config	Audit Log					
			Sche Start	cheduling eat Events SION Insight dule polling in dit St eed polling Tre	Criteria fo 5 s Events terval (minute art Polling ellix ePO Saas	or polling MVISI s): Stop Polling and MVISION Insigh	DN Insights	events.	PO Saas	

To stop polling, click on **Stop Polling** button as shown below:

≡	IBM QRadar										
Dashboa	ard Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connector
Trellix	Trellix ePO Sa	as Config	Trellix ePO Saas Eve	ents Config	Audit L	og					
			Schedu Schedu 10 Ed Stoppe	heduling at Event ON Insight ule polling ir it SI	s Criteria S ts Events nterval (min tart Polling rellix ePO S	utes):	top Polling MVISION Insigh	DN Insigh	nts and o	ePO Saas	

Note: Threat events will be fetched only for the time duration when polling is active. Any events generated before start of event poll or after the poll has been stopped will not be fetched on QRadar.

On successful poll of threat events, Admins can see events on **Log Activity** page as shown below:

≡	IBM QRadar												Ļ
Dashb	poard Offenses Log Activity Network Activity	Assets Reports Risks	: Vulnerabiilies	Admin	Pulse Use Case N	tanager Trellix ePC) Saas Connector						System Time: 7:28
Search	ch 🔻 Quick Searches 🔻 🍟 Add Filter 🗮 Save Criteria 📲 S	ave Results 🔍 Cancel 🔧 False	Positive Rules T Acti	ons 🔻									
Curr	ent Filters:												
Log	Source is Trellix ePO Saas Threat Events (Clear Fil	lter)											
► CL	urrent Statistics												
Reco	ords Matched Over Time												
De											5/0/22 11	20 DM - 5/0/22	7-20 DM M
7	E										Urdizz, 1.	23 - 111 - 0/3/22,	7.20 FM ¥
1.													
2.	5												
i	1:30 PM 2:00 PM 2:30 PM	3:00 PM	3:30 PM		4:00 PM	4:30 PM	5:00 PM	5:30 PM	6:00 PM	6:30 PM		7:00 PM	
					Updat	te Details							
					(Hide	Charts)							
	Event Name	L	.og Source	Event	Time 🕶	Low Leve	el Category	Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
	Infected file deleted	Trellix ePO 5	Saas Threat Events	6 1	May 9, 2022, 4:05:19 PN	1 Virus Detected		10.254.46.95	0	10.254.46.95	0	CLDBGQAE	
	Infected file deleted	Trellix ePO :	Saas Threat Events	11	May 9, 2022, 4:05:19 PN	I Virus Detected		10.254.46.95	0	10.254.46.95	0	CLDBGQAE	
۲	file infected. No cleaner available, file deleted successfully	Trellix ePO :	Saas Threat Events	11	May 9, 2022, 4:05:19 PN	1 Virus Detected		10.254.46.95	0	10.254.46.95	0	CLDBGQAE	-
•	file infected. No cleaner available, file deleted successfully	/ Trellix ePO	Saas Threat Events	1	May 9, 2022, 4:05:19 PN	I Virus Detected		10.254.46.95	0	10.254.46.95	0	CLDBGQAE	
۲	Infected file deleted	Trellix ePO 3	Saas Threat Events	1 1	May 9, 2022, 4:05:19 PN	1 Virus Detected		10.254.46.95	0	10.254.46.95	0	CLDBGQAE	
۲	Infected file deleted	Trellix ePO 3	Saas Threat Events	11	May 9, 2022, 4:05:19 PN	1 Virus Detected		10.254.46.95	0	10.254.46.95	0	CLDBGQAE	_
۲	file infected. No cleaner available, file deleted successfully	Trellix ePO :	Saas Threat Events	11	May 9, 2022, 3:05:20 PN	1 Virus Detected		10.254.46.95	0	10.254.46.95	0	CLDBGQAE	

Event is parsed using the custom properties and DSM parser which is defined for Trellix ePO Saas Threat events as shown below:

≡	IBM QRadar															(III)	Ċ
Dashboard	Offenses	Log Activity	Network Activity	Assets F	Reports Risks	Vul	nerabilities	Admin I	Pulse	Use Case Manager	Trellix ePO Saas C	onnector				Sy	stem Time: i
🕒 Return to	Raham to Event List 🔞 Offense 🗞 Mag Event 🔧 False Positive 🍺 Extract Property 🚯 Previous 😍 Head 🔒 Point 🔞 Obfacación 🔻																
vent Inf	ormation																
Event Na	ime	The infected. No cleaner available, The deleted successfully															
Low Lev	el Category	my Vius Detected															
Event De	scription	file infected. No cleaner available, file deleted successfully															
Magnitud	de	(7)			Relevance		6				Severity	8	Credibility	5			
Usernam	10	CLDBGQAE00260/cloudadmin															
Start Tim	1e	May 9, 2022,	4:05:19 PM				Storage Ti	me	May 9	, 2022, 4:05:19 PM			Log Source Time	May 9, 2022, 4:05	19 PM		
AgentGL	JID (custom)	06c59f50-903	4-46aa-82d9-b5e5	6bb21d44													
Analyzer (custom)	DetectionMethod	On-Access S	can														
Analyzer (custom)	HostName	CLDBGQAEC	0260														
Analyzer	ID (custom)	ENDP_AM_1	070														
Analyzer	IPV4 (custom)	10.254.46.95															
Analyzer	MAC (custom)	005056afb7b	В														
Analyzer	Name (custom)	McAfee Endp	oint Security														
Analyzer	Version (custom)	10.7.0.3299															
Detected	IUTC (custom)	16520923330	00														
Received	dUTC (custom)	16520924221	85														
SourceH (custom)	ostName	null															
SourceP (custom)	rocessName	C:\Windows\S	System32\notepad.	exe													
SourceU	RL (custom)	null															
SourceU (custom)	serName	null															

Threat Event in JSON format fetched from Trellix ePO Saas

- IDM ODedat				A	đ							
= IBM QRadar				ţi.	÷							
Dashboard Offenses Log A	ctivity Network Activity Assets Reports Risks Vulnerabilities Admin Pulse Use Case M	anager Trellix ePO Saas Connect	or	s	ystem Time: 7:3							
Return to Event List 🚺 Offense	🕽 Map Event 🐁 False Positive 🄀 Extract Property 🛛 🞧 Previous 🙆 Next 🖂 Print 🔓 Obfuscation 🔻											
Source and Destination Infor	mation											
Source IP	10.254.46.95	Destination IP	10.254.46.95									
Source Asset Name	N/A	Destination Asset Name	N/A									
Source Port	0	Destination Port	0									
Pre NAT Source IP		Pre NAT Destination IP										
Pre NAT Source Port	0	Pre NAT Destination Port	0									
Post NAT Source IP		Post NAT Destination IP										
Post NAT Source Port	0	Post NAT Destination Port	0									
Source IPv6	0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0									
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00									
Payload Information												
utf hex base64												
Wrap Text												
Source IPv6 0:00:00:00 Destination IPv6 0:00:00:00 Source MAC 0:00:00:00:00 Destination MAC 0:00:00:00 Payload Information Composition Destination MAC 0:00:00:00:00 Composition Composition Destination MAC 0:00:00:00:00:00 Payload Information Composition Composition Composition Composition Composition <thcompositicon< th=""> Compositicon Comp</thcompositicon<>												

Note: All Trellix ePO Saas Threat events will have the following mapping:

Event Name	Trellix ePO Saas Threat Event
Low Level Category	We have mapped with 302 known event categories, if any event
	doesn't fall under these 302 category will be classified as Alert

On successful poll of MVISION Insights events, Admins can see events on **Log Activity** page as shown below:

≡	IBM QRadar							ŧ	Ċ	<u> </u>					
Dast	nboard Offenses Log Activity Network Activity Assets Re	eports Risks Vulnerabilities Admin	Pulse Use Case Manage	r Trellix ePO Saas Connector					System Time:	1:49 PM					
Sea Q	Search. Y Ouck Searches Y Y Add Fiter Save Cottonia C Save Results C Concol & False Positive Rules Y Actions Y Ouck Filter Y														
	Start Time 5/	/5/2022 * 1:50 PM View: Select An Option: * Dis	End Time 5/12/202 play: Default (Normalized)	2 • 1:50 PM • Results Limit	* Update			Com	mieted	1					
Cur Lo ► (rrent Filters: g Source is MVISION Insights Events (Clear Filter) Zurrent Statistics							Com	ihieren						
Re	cords Matched Over Time									a I.					
R							5/5/22, 1:5	0 PM - 5/12/22, 1	1:50 PM 🗸	11					
4	3														
1	5:30 PM May 6 5:30 PM May 7	7 5:30 PM May 8	5:30 PM	May 9 5:30 PM	May 10 5:3	30 PM May 11	5:30 PM	May 1	2						
			Update Deta	ais						- 1					
			(Hide Charb	8)						- 1					
	Event Name	Log Source Even Court	t Time 🕶	Low Level Category	Source IP	Source Port Destination IP	Destinat Port	Username	Magnitud	le					
	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 5:42:38 PM AI	ert	10.254.46.95	0 10.254.46.95	0	cloudadmin							
	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 4:32:46 PM AI	ert	10.254.46.95	0 10.254.46.95	0	cloudadmin							
•	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 4:32:37 PM AI	ert	10.254.46.95	0 10.254.46.95	0	cloudadmin							
	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 12:22:38 PM AI	ert	10.254.41.30	0 10.254.41.30	0	Cloudadmin							
	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 12:22:37 PM AI	ent	10.254.41.30	0 10.254.41.30	0	Cloudadmin							

Event is parsed using the custom properties and DSM parser which is defined for MVISION Insights events as shown below:

BM QRadar									(),	Ċ	<u> </u>
Dashboard Offenses	Log Activity Network Activity Assets Reports Risks Vul	nerabilities Admin P	ulse Use Case Manager	Trellix ePO Saas Connect	lor				Sys	stern Time: 1	50 PM
Return to Event List 💿 Offe	nse 📀 Map Event 🤸 False Positive 👔 Extract Property 🛛 🚱 Previous 🔮 Next	🚔 Print 🔒 Obfuscation 🔻									
Event Information											^
Event Name	MVISION Insights Event										1
Low Level Category	Alert										1
Event Description	Generic mapping for IM/ISION Insights Event										1
Magnitude	(5)	Relevance	6			Severity	5	Credibility	5		1
Username	cloudadmin										
Start Time	May 6, 2022, 4:32:37 PM	Storage Time	May 6, 2022, 4:32:37 PM			Log Source Time	May 6, 2022, 4:32:	37 PM			1
AgentGUID (custom)	841146ab-b317-4101-be95-2506/738cf49										
AnalyzerID (custom)	MVISION Insights]
AnalyzerName (custom)	MVISION Insights										1
Campaign Id (custom)	d5a2a7e9-caf5-11ea-9477-02d538d9640e										1
DetectedUTC (custom)	2022-05-06T10:53:17.000Z										1
Hostname (custom)	CLDBGQAE00260										1
MD5 Hash (custom)	69038f728c3e7d0011791c31fed971b4										1
OS Name (custom)	Windows Server 2016 Standard										
SHA256 Hash (custom)	a4e5cfbeedb7f8be6a2efafb521bbc555e753225efa4380976fd5c6ea6bc99d4										
User Domain (custom)	WORKGROUP										
Domain	Default Domain]
Source and Destination	Information										
Source IP	10.254.46.95		Dest	ination IP	10.254.46.95						1
Source Asset Name	N/A		Dest	ination Asset Name	N/A						1
Source Port	0		Dest	ination Port	0						-

Insights Event in JSON format fetched from MVISION INSIGHTS

				(Ċ	<u> </u>
Dashboard Offenses Log A	ctivity Network Activity Assets Reports Risks Vulnerabilities Admin Pulse Use Case M	lanager Trellix ePO Saas Connect	or	Syste	em Time: 1:	52 PM
🗄 Return to Event List 🜘 Offense	🕽 Map Event 🔸 False Positive 🔞 Extract Property 🛛 🚱 Previous 🔮 Next 🛛 😓 Print 🔒 Obfuscation 🔻					
Source and Destination Infor	mation					•
Source IP	10.254.46.95	Destination IP	10.254.46.95			ī
Source Asset Name	N/A	Destination Asset Name	N/A			1
Source Port	0	Destination Port	0			1
Pre NAT Source IP		Pre NAT Destination IP				1
Pre NAT Source Port	0	Pre NAT Destination Port	0			1
Post NAT Source IP		Post NAT Destination IP				1
Post NAT Source Port	0	Post NAT Destination Port	0			
Source IPv6	0.0.0.0.0.0.0	Destination IPv6	0.0.0.0.0.0.0			
Source MAC	00:50:56:AF:B7:B8	Destination MAC	00:50:56:AF:B7:B8			
Payload Information						
ut nex base54 ©/WapTet 2 cla2:37 W/TS1 "computements" 'CLOBQCQC "doe3af728c3e7d0011791c317	ON[Insights ("agentõuid": "801f46ab-b317-4101-be95-25667738cf40", "analyzerid": "MVISION Insight 0200", "domainiama": "Wohkkokop", "eventid": "MVISION Insights Event", "insights gradarcategory" ed07164", "ostype": "Windows Server 2010 Standard", "sna256": "a46scfbeedb)f8be6a2efafb521bbc556	s", "analyzerName": "MVISION "TWISION Insights Event", 733123ef44300970fdSc0eadbc09	Inights", "campaign-1d": "d5223769-csf5-11es-0477-020538050480", [pAddrest", "10.154.40.957, "macAddrest": "00:50:50:161.47:187;10", "4d5"; d4", "Limestamp": "2022-85-00120:53:17.0002", "userName": "Lioudadsin"}			

Note: All MVISION Insights events will have the following mapping:

Event Name	MVISION Insights Events
Low Level Category	Alert

MVISION Insights

MVISION Insights provides actionable and preemptive threat intelligence by leveraging Trellix cuttingedge threat research, augmented with sophisticated Artificial intelligence (AI) applied to real-time threat telemetry.

The integration of MVISION Insights significantly enhances the capabilities of Trellix award winning endpoint security platform by managing the attack surface, preventing ransomware and aiding security teams to easily investigate and respond to advanced attacks.

≡	i IBM QRadar							(),	Ċ	<u>0</u>
Dashb	hboard Offenses Log Activity Network Activity Assets Reports F	lisks Vulnerabilities Admin Puls	e Use Case Manager Trellix ePO	Saas Connector					System Time: 9	k 43 AM
Searc	rch 🔻 Quick Searches 🔻 🍟 Add Filter 🕌 Save Criteria 🔋 Save Results 🔗 Cancel 🤸 F	alse Positive Rules V Actions V								0
Qui	uick Filter 🔹								Search	
		Start Time 5/3/2022 View: Select An Option:	9:43 AM End Time 5/10 Jisplay: Default (Normalize	2022 • 9:43 AM • Update d) • Results Limit •					Completed	
Curro Log ► Cu	rrent Filters: g Source is MVISION Insights Events (Clear Filter) Current Statistics									
Rec	cords Matched Over Time									
Ro 3 2 1 0	1507 2007 2	May 5 1:30 PM 9:30 PM	May 6 1:30 PM 9:	10 PM May 7 1:30 PM 1	2:30 PM May 8 1:30 1	54 9:30 PM May 9	5/3/22, 1:30 PM	9:30 PM	2, 9:43 AM V	
			Updati (Hde	Details Charts)						
	Event Name	Log Source	Event Time -	Low Level Category	Source IP	Source Destination IP	Destinatic	Username	Magnite	ude
۲	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 5:42:38 PM	Alert	10.254.46.95	10.254.46.95	0	cloudadmin		
۲	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 4:32:46 PM	Alert	10.254.46.95	10.254.46.95	0	cloudadmin		
۲	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 4:32:37 PM	Alert	10.254.46.95	10.254.46.95	0	cloudadmin		
	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 12:22:38 PM	Alert	10.254.41.30	10.254.41.30	0	Cloudadmin		
	MVISION Insights Event	MVISION Insights Events	1 May 6, 2022, 12:22:37 PM	Alert	10.254.41.30	10.254.41.30	0	Cloudadmin	_	
	MVIOION Insights Event	MVISION Insights Events	1 May 5, 2022, 10:24:33 PM	Alert	10.254.46.95	10.254.46.95	0	cioudadmin	-	

The integration of MVISION Insights will provide the Insights for the following information

1.MVISION Insights Campaign's 2.MVISION Insights Campaign's IOC 3.MVISION Insights Campaign's Galaxies

≡ IBM QRadar											(⊫ ¢ 2
Dashboard Offenses Log	clivity N	ietwork Activity Assets Reports Risi	s Vulnerabilities Admin	Pulse Use Case	Manager Trellix ePO Si	aas Connector						System Time: 9:44 AM
Search ¥ Quick Searches ¥ ¥	dd Filter 🕌	Save Criteria 👔 Save Resulta 🔗 Concel 🤸 Fala	Positive Rules ¥ Actions ¥									0
Quick Filter *												Search
			Start Time 5/3/2022	* 9:44 AM	* End Time 5/10/2	022 -	9:44 AM • Update					
			View: Se	lect An Option: •	Display: Custom *	Results Limit	1,000					Completed
Current Filters: Log Source is MVISION Insig Current Statistics	its Events	(Clear Filter)										
Records Matched Over Time												
Reset Zoom											5/3/22, 9:44 AM - 5/	10/22, 9:44 AM 🗸
3												
2												
1				\wedge								
0 1:30 PM 9:30 PM	Ма	ý 4 1:30 PM 9:30 PM N	ay 5 1:30 PM 9	30 PM May 6	1:30 PM 9:30	PM May	7 1:30 PM 9:	IÓ PM M	ay 8 1:30 PM 9:30 P	M May 9	1:30 PM 9:30 PM	May 10
					(Hde Cr	harts)						
Eve	nt Name	Log Source	Event Count	Start Time 🔻	Low Level Category	Source II	Source Port	Destina	tion IP Destination Port	Username	Magnitude	Campaign Id (custom)
MVISION	Insights Ev.	MVISION Insights Events		May 6, 2022, 5:42:38	Alert	10 254 46 95	0	10.254.46	Filter on Campaign Id (custo	n) is d5a2a7e9-caf5-11	ea-9477-02d538d9640e	2a7e9-caf5-11ea
MVISION	Insights Ev.	MVISION Insights Events		May 6, 2022, 4:32:46	Alert	10.254.46.95	0	10.254.48	Filter on Campaign Id (custo	n) is not d5a2a7e9-caf5	-11ea-9477-02d538d9640e	ta7e9-caf5-11ea
MVISION	Insights Ev.	MVISION Insights Events		May 6, 2022, 4:32:37	Alert	10.254.46.95	0	10.254.46	Quick Filter			ra7e9-cal5-11ea
MVISION	Insights EV.	MVISION Insights Events		May 6, 2022, 12:22:3	Alert	10.254.41.30	0	10.254.41	 False Positive 			ta7e9-caf5-11ea
MVISION	Insights Ev.	MVISION Insights Events		May 5, 2022, 10:24:3	Alert	10.254.46.95	0	10.254.46	New path from 10 254 46 95	to 10 254 46 95		a7e9-caf5-11ea
MVISION	Insights Ev.	MVISION Insights Events		May 5, 2022, 10:24:3	Alert	10.254.46.95	0	10.254.48	View in DSM Editor			ta7e9-caf5-11ea
							Million Compaign Data		Plugin options			
						1	MINIOLON Campaign Detail	Dataila				-
						1	MINISION Campaign's IOC	Details				
						4	MVISION Campaign's Gala	coes Details				

MVISION Insights Campaign's

The "MVISION Insights Campaign's" action in QRadar console will allow the QRadar user to select a Campaign Id from "Log Activity" page.

This action will open a new popup page to show Insights Campaign's details from MVISION ePO server.

E IBM QRad	ar											()	¢
shboard Offenses	Log Activity Ne	twork Activity Assets Reports Risks	Vulnerabilities Admin	Pulse Use Case	Manager Trello: ePO Sa	as Connector						Sys	slem Time. 1
aarrith 🔻 Oh inte Samara		ana Criteria 🖉 Sana Banulta 🔍 Concort 🐴 Entra D	antina Rulas V. Artises V.										
		e											
Quick Filter *												5	jearch
			Start Time 5/3/2022	• 9:44 AM	* End Time 5/10/2	9.44	AM • Update						0.
			View: Se	elect An Option: *	Display. Custom *	Results Limit 1,	000						
urrent Filters:												Con	apleted
og Source is MVIS	ION Insights Events	(Clear Filter)											
Current Statistics													
	- -												
cords Matched OV	er time										5000 A.U.M. 5		
1											D/3/22, 9:44 MW - D/	10/22, 9	2.44 /001
2				1									
				Δ.									
1				Λ									
					$(\land \land$								
0 1:30 PM	9:30 PM May	4 1:50 PM 9:50 PM May	5 1:30 PM 9	30 PM May 6	1:30 PM 9:50	PM May 7	1:30 PM 9:30	PM May S	1:30 PM 9:30 PM	May 9	1:30 PM 9:30 PM	s ()	May 10
					Update D	etalle							
					(Hide Ch	arta)							
	Event Name	Log Source	Event Count	Start Time 🔻	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	C	ampaign (custom)
	MVISION Insights Ev	MVISION Insights Events		May 6, 2022, 5:42:38	Alert	10.254.46.95	0	10.254.46.0	Eller on Cempsion Id (custom)	is (5979769.cet5.116	a.9477.07453849640a	- Pa	7e9-cal5-1
	MVISION Insights Ev	MVISION Insights Events		1 May 6, 2022, 4:32:46	Alert	10.254.46.95	0	10.254.46	Ther on Compaign Id (custom)	is not deployed on the	11ee 0477 004500406	ta	7e9-caf5-*
	MVISION Insights Ev	MVISION Insights Events		1 May 6, 2022, 4:32:37	Alert	10.254.46.95	0	10.254.46	wat ou campaign in (cristour)	19 1101 03424749-calo	-1169-9#11-050320080408	20	7e9-caf5-1
	MVISION Insights Ev	MVISION Insights Events		1 May 6, 2022, 12:22:3	Alert	10.254.41.30	0	10.254.41	Julick Filter			P 23	7e9-caf5-1
	MVISION Insights Ev.	MVISION Insights Events		1 May 6, 2022, 12:22:3	Alert	10.254.41.30	0	10.254.41 🔸 F	False Positive			28	7e9-cat5-*
	MVISION Insights Ev.	MVISION Insights Events		1 May 5, 2022, 10:24:3.	Alert	10.254.46.95	0	10.254.46	New path from 10.254.46.95 to	10.254.45.95		tai	7e9-cat5-*
	MVISION Insights Ev	MVISION Insights Events		1 May 5, 2022, 10:24:3	Alert	10.254.46.95	0	10.254.46	dew in DSM Editor	25		ta.	.7e9-caf5-1
						A 1	DUDION OF THE DUDION	6	Flugin options				
						1 1	IVISION Campaign Details	F	Plugin options			*	
						1	VISION Campaign Details	erails	lugin options			۲	

Considering the campaign d5a2a7e9-caf5-11ea-9477-02d538d9640e . Refer the screenshot below-

Threat Level id	Name	Description	External Analysis
2	Operation Iron Ore	This is a clone of "Campaign Molerats Delivers Spark Backdoor" for MFE JDP Testing purposes." The Molerats threat group targeted multiple sectors across six countries with spear-phishing emails containing malicious attachments or links to exfiltrate sensitive information. The actor, also known as the Gaza Hacking Team and the Gaza Cybergang, infected systems with the Spark backdoor which has been attributed to the group and used in previous attacks since at least 2017. Molerats has been attacking multiple sectors since at least 2011 and use various public and custom backdoors during their operations. Associated IoCs: Payload Delivery (MD5): 666fb7ca1c9ccc0cab7ce8f3280fc192 C&C IP: 213.124.66.12	 https://unit42.paloaltonetworks.com/molerats- delivers-spark-backdoor/ https://www.cybereason.com/blog/new-cyber- espionage-campaigns-targeting-palestinians-part- one

MVISION Insights Campaign's IOC

The "MVISION Insights Campaign's IOC" action in QRadar console will allow the QRadar user to select a Campaign Id from "Log Activity" page.

This action will open a new popup page to show Insights Campaign's IOC details from MVISION ePO server.

=	IBM QRad	lar											ŧ	¢	<u>0</u>
Dashbox	ard Offense	s Log Activity N	etwork Activity Assets Reports	Risks Vulnerabilities Adm	in Puise Use Cas	a Manager Trellix ePO Sa	as Connector						Sy	stem Time.	9.44 AM
			Ina Caluira - C. Canal - A	Fries Parties - Data + Autors +										_	0
oearon.		ves. I worke Mi	and criteria El sand Hearter of Control A	Pase Positive Holes * Publics *											
Quic	k Filter *													Search	
				Start Time 5/3/2022	• 9:44 AM	* End Time 5/10/20	9.44	AM * Update						÷.,	
				View:	Select An Option: *	Display Custom +	Results Limit 1,	000							
													Con	npleted	
Curre	nt Filters: Source is MV/S	SION Insights Events	(Clear Filter)												
► Cur	rent Statistic:	sione margina Leanna	(creat i nor)												
Recor	ds Matched Ov	ver Time													
Rep	et Zoom											5/3/22, 9:44 AM - 5	5/10/22,1	9.44 AM	~
3															
5															
1 -					Δ										
0 -	1:30 PM	9.30 PM May	4 1:30 PM 9:30 PM	May 5 1:30 PM	9.30 PM May 6	1.30 PM 9.30	PM May 7	1:30 PM 9:30	PM Ma	/ 8 1:30 PM 9:30 PM	May 9	1:30 PM 9:30 PM	6 7	May 10	-
						Update D	etaile								
						(Hide Ch	arta)								
		Event Name	Log Source	Event Count	Start Time 🕶	Low Level Category	Source IP	Source Port	Destinati	on IP Destination Port	Username	Magnitude	C	ampaign	Id
0		MVISION Insights Ev.	MVISION Insights Events		1 May 6, 2022, 5:42:38	Alert	10.254.46.95	0	10.254.46	Elter on Campaign Id (custom	is (5979749.cof5.11	00.0477-024538496400	1	7e9-cal5	11ea
۲		MVISION Insights Ev.	MVISION Insights Events		1 May 6, 2022, 4:32:46.	Alert	10.254.46.95	0	10.254.46	Filter on Campaign Id (custom	in not d6a2a7a0 cat	5 1100 0477 00452940640c	ha	7e9-caf5-	11ea
0		MVISION Insights Ev.	MVISION Insights Events		1 May 6, 2022, 4:32:37.	Alert	10.254.46.95	0	10.254.46	Course Chara	12 1101 03828768-081	2-1168-0411-02030000406	ta la	7e9-cat5-	11ea
		MVISION Insights Ev.	MVISION Insights Events		1 May 6, 2022, 12:22:3.	Alert	10.254.41.30	0	10.254.41.	MANUN PINES			** 2a	J769-caf5-	11ea
		MVISION Insights Ev.	MVISION Insights Events		1 May 6, 2022, 12:22:3.	Alert	10.254.41.30	0	10.254.41	+ False Positive			20	17e9-cat5-	11ea
		MVISION Insights EV.	MVISION Insights Events		1 May 5, 2022, 10:24:3.	Alert	10.254.48.95	0	10.254.46	New path from 10.254.46.95 t	10.254.45.95		1	7=0 +===	110d
		myraiony insights Ev.	Inviorone insignes Evenes		1 may 5, 2022, 10:24:3.	ANT	10.204.40.95	v	10.254.40.	View in DSM Editor	_		19	./ ws-calo-	riva
							1	VISION Campaign Details		Plugin options					
								WEION Campalan's IOC D	latalla						
								working anglis for b	COLDING T						
							-	motion campaigns Galax	ies Decilis						

Considering the campaign d5a2a7e9-caf5-11ea-9477-02d538d9640e . Refer the screenshot below-

w 10 🗸 entries			Search:	:		
Id	Category 🖨	Туре	Value	Lethality	Determinism	
64e5263-6945-11ea- 942-06365ef617e6	Payload delivery	sha256	a4e5cfbeedb7f8be6a2efafb521bbc555e753225efa4380976fd5c6ea6bc99d4	None	None	
3c19373-6945-11ea- 942-06365ef617e6	Payload delivery	sha1	d992676eee27d18b67c1b97b7f87bfdd081b3017	None	None	
9ca5276-6945-11ea- 942-06365ef617e6	Payload delivery	md5	69038f728c3e7d0011791c31fed971b4	None	None	
812e29f-ad78-11ea- 477-02d538d9640e	Network activity	domain	webtutorialz.com	None	None	
81c4161-ad78-11ea- 477-02d538d9640e	Network activity	domain	nysura.com	None	None	
828a1be-ad78-11ea- 477-02d538d9640e	Network activity	domain	motoqu.com	None	None	
82cd4f5-ad78-11ea- 477-02d538d9640e	Network activity	domain	laceibagrafica.com	None	None	
b5f3149-9c82-11ea- 942-06365ef617e6	Payload delivery	sha256	b84f2497e4cfeac240b1815b22741609e5a31f0be11667a3c7256c16788728ec	None	None	
b63b764-9c82-11ea- 942-06365ef617e6	Payload delivery	sha1	c88b3db1a4387c523f9324706c67b3d964bb2a36	None	None	
b682445-9c82-11ea- 942-06365ef617e6	Payload delivery	md5	d35be65d011bcad42a9bdca3276449ed	None	None	

MVISION Insights Campaign's Galaxies

The "MVISION Insights Campaign's Galaxies" action in QRadar console will allow the QRadar user to select an Campaign Id from "Log Activity" page.

This action will open a new popup page to show Insights Campaign's Galaxies details from MVISION ePO server.

IBM QRadar												¢
ard Offenses Log Activity	Network Activity Assets Reports Risks	Vulnerabilities Admin I	Pulse Use Case	Manager Trellix ePO Sa	as Connector						Syste	m Time: 9
. V Quick Searches V 🖓 Add Filter	📕 Save Criteria 📲 Save Resulta 👰 Concel 🤸 False P	ostive Rules ¥ Actions ¥										
k Filter 👻											Se	arch
		Start Time 5/3/2022	* 9:44 AM	* End Time 5/10/20	9.44	AM * Update						o',
		View: Select A	n Option: 💌 I	Display Custom *	Results Limit 1,	000					Comr	hatad
nt Filters:											comp	10100
Source is MVISION Insights Even	nts (Clear Filter)											
rent Statistics												
ds Matched Over Time												
										5/3/22, 9:44 AM - 5	/10/22, 9.4	44 AM
				A A								
		A										
1:30 PM 9:30 PM	May 4 1:30 PM 9:30 PM May	5 1:30 PM 9:30 PM	May 6	1:30 PM 9:30	PM May 7	1:30 PM 9:30	PM May 8	1:30 PM 9:30 PM	May 9	1:30 PM 9:30 PM	M	fay 10
				Update D	otalla							
				(Hide Ch	(che							
Event Nam	Log Source	Event Count	Start Time 💌	Low Level Category	Source IP	Source Port	Destination	IP Destination Port	Username	Magnitude	Car	mpaign
MVISION Insight	Ev MVISION Insights Events	1 May	6, 2022, 5.42.38	Alert	10.254.46.95	0	10.254.46.0	Filter on Compaign (d (sustem)	in disalatan coli di	00.0177.024530405400	2070	19-cal5
MVISION Insights	Ev. MVISION Insights Events	1 May	6, 2022, 4:32:46	Alert	10.254.46.95	0	10.254.46.	Piliter on Campaign id (custom)	15 03828769-0815-11	ea-9477-02033603640e	ta7e	s9-cat5
MVISION Insights	Ev. MVISION Insights Events	1 May	6. 2022. 4.32:37	Alert	10.254.46.95	0	10.254.46	Finer on Campaign Id (custom)	is not d5a2a7e9-cat	5-11ea-9477-02d538d9640e	ta7e	19-cars
MVISION Insight	Ev MVISION Insights Events	1 Maj	6, 2022, 12 22 3	Alert	10.254.41.30	0	10.254.41	Quick Filter			► 2a7c	s9-caf5
MVISION Insights	Ev. MVISION Insights Events	1 Maj	6, 2022, 12:22:3	Alert	10.254.41.30	0	10.254.41	False Positive			2876	e9-cat5
MVISION Insights	Ev. MVISION Insights Events	1 May	5, 2022, 10:24:3.	Alert	10.254.46.95	0	10.254.46.	View path from 10.254.46.95 to	10.254.45.95		ta7e	a9-caf5
MMR10N Inrichh	Ev MVISION Insights Events	1 May	5, 2022, 10:24:3	Alert	10.254.46.95	0	10.254.46	View in DSM Editor			ta7e	x9-caf5
merorore integral												
Invision might					1 . I.			Plugin options				
in the second seco					/ M	VISION Campaign Details		Plugin options			•	

Considering the campaign d5a2a7e9-caf5-11ea-9477-02d538d9640e. Refer the screenshot below-

ow 10 🗸 en	tries		Search:					
ld	Category	Name	Description					
04bd9b95- 5aec-11ea- 3942- 06365ef617e6	mitre- attack- pattern	Custom Cryptographic Protocol	Adversaries may use a custom cryptographic protocol or algorithm to hide commar and control traffic. A simple scheme, such as XOR-ing the plaintext with a fixed key, will produce a very weak ciphertext. Custom encryption schemes may vary in sophistication. Analysis and reverse engineering of malware samples may be enoug to discover the algorithm and encryption key used. Some adversaries may also attempt to implement their own version of a well-known cryptographic algorithm instead of using a known implementation library, which may lead to unintentional errors. (Citation: F-Secure Cosmicduke)					
45418178- 6916-11ea- 8942- 06365ef617e6	sector	Telecoms						
486e7429- 9c82-11ea- 3942- 06365ef617e6	sector	Insurance						
4e573350- 964d-11ea- 3942- 06365ef617e6	mitre- attack- pattern	Signed Binary Proxy Execution	Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed binaries. Binaries signed with trusted digital certificates can execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files.					
4fa36414- 5f7e-11ea- 3942- D6365ef617e6	mitre- attack- pattern	Multi-Stage Channels	Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and addition RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks o [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the origina					

Audit Log

This feature is provided to the Admins to see actions performed on Trellix ePO Saas Connector for QRadar App. This page will hold list of most recent 15 activities performed on the App for example saving ePO config etc. as shown below:

≡	IBM QRadar											
Dashboar	d Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vulnerabilities	Admin	Pulse	Use Case Manager	Trellix ePO Saas Connect	or
Trellix	Trellix ePO Sa	as Config	Trellix ePO Saas Ev	ents Config	Audit Lo	g						
				ſ								
					🖊 Displa	ys the la	atest 15 ac	tivities p	erforme	d on Trellix Co	onnector App	C 🔳
					Recent Activ	vities:						
					Activity							Time
					Successfu	lly stopp	ed polling th	reat event	s on Trell	lix ePO Saas.		09/05/2022,
					Successful	llv starte	ed polling thr	eat events	on Trelli	x ePO Saas.		09/05/2022,
												19:25:20 09/05/2022,
					Successfu	lly stopp	ed polling th	reat event	s on Trell	lix ePO Saas.		19:25:17
					Successfu	lly updat	ted Trellix eP	O Saas Ev	ents poll	interval.		19:25:14
					Successfu	lly updat	ted Trellix eP	O Saas Ev	ents poll	interval.		09/05/2022, 19:23:47
					Successfu	lly updat	ted Investiga	tion ID:c1	7f65e0-c	f83-11ec-a903-(000000000000 in	09/05/2022,
					No events	found o	n MVISIONI	 Inciante in	this poll			09/05/2022,
					No events	Touria o		insignes in	tins poil.			19:13:08
					No events	found o	n Trellix ePC) Saas in th	is poll.			19:13:08
					Failed to for currently of	etch dev configur	rice details fo ed Trellix eP	or system: : O Saas.	172.16.2	14.200. System i	s not managed by	09/05/2022, 19:10:07
					Successful	lly fetche	ed device det	tails for sy	stem ip: 1	10.254.46.95.		09/05/2022,
					No events	found o	n Trellix ePC	Saas in th	is noll			09/05/2022,
					i to events	Tound o	in menix er e	500511101	is poin.			18:58:08
					No events	found o	n MVISION I	nsights in	this poll.			18:58:08
					No events	found o	n MVISION I	nsights in	this poll.			09/05/2022, 18:43:08
					No events	found o	n Trellix ePC	Saas in th	is poll.			09/05/2022,
					No events	found o		neighte in	this poll			09/05/2022,
					NO EVENILS	Touriu O	IN MUSICINI	inaiginta III	uns poli.			18:28:08

- To see the most recent logs, Admin must click on "Refresh" icon available on the top-right corner.
- To delete the logs, Admin can click on "**Delete**" icon. This action will delete all the audit logs captured for the app.

Important things to know

Steps to follow if exception is displayed while clicking on Create/Update EDR Investigation button

In case if Admin encounters an exception while executing EDR Create/Update action, try reloading the page by doing a refresh, or re-login to QRadar console or try on a different browser like chrome.

≡ IBM QRadar										(ġ,	2
Dashboard Offenses	Log Activity	Network Activity	Assets Reports Admin	Pulse Use Case Manager Mc/	fee MVISION Connector					Syster	n Time: 4.43	PM
Offenses	Search 🔻 🔛 Save Criteria Actions 🔻 🔄 Pint 🎾 Create/Update Investigation in MMSION EDR											0
My Offenses All Offenses By Category	All Offenses View Offenses with Select An Option.											
By Source IP	🤊 Id		Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Fic
By Desthation IP By Network Rules		1 File And	Jyaa Completed	Client Exception The following client exception acc response (0) ReferenceError: showMcAreeED	urred while handling th	te server dined	1-33 124 59	1	System	bið	36,669	0
	< Displayi	ng 1 to 1 of 1 item	s (Elapsed time: 0:00:00.038)									,

Steps to follow if 'SSL: CERTIFICATE_VERIFY_FAILED' message appears in app log

There might be two reasons if you see SSL: CERTIFICATE_VERIFY_FAILED in the container app log: **Reason #1**: Since Trellix MVISION connector app is accessing Trellix's API which is hosted in

AWS gateway, it is required that the QRadar server should have the latest AWS cert chain in the QRadar cert bundle. Hence, make sure that the QRadar server has the required AWS cert chain the QRadar server certificate bundle.

Reason #2: If the Trellix MVISION connector app is configured with the proxy server and if the proxy server requires the certificate for any outbound request/communication, then you must have the corresponding proxy server certificate in the QRadar server certificate bundle.