Trellix ePO Saas Connector App for QRadar

Contents

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:

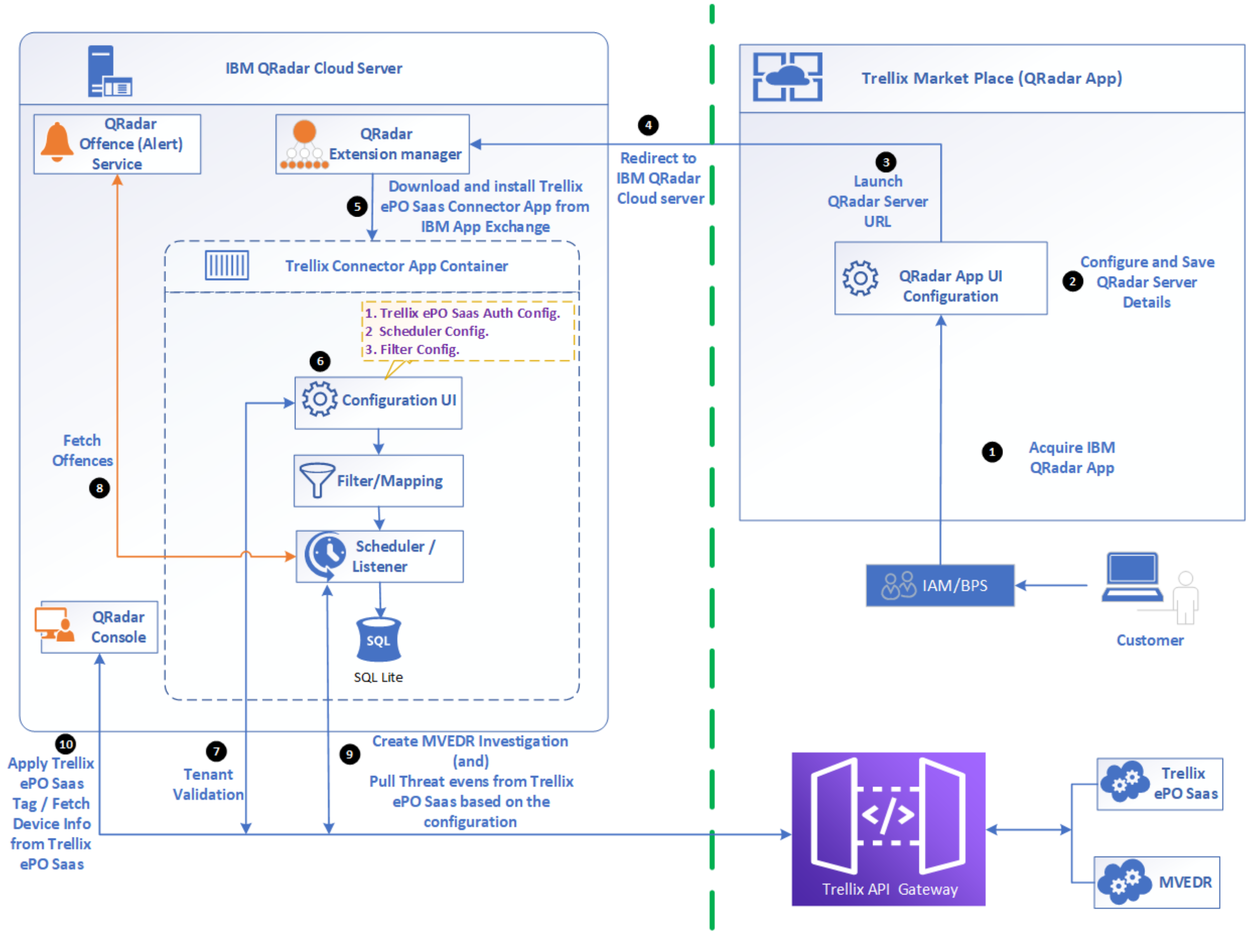
- Can create/update an EDR investigation for an offense from IBM QRadar console. An EDR SOC admin will continue the investigation for the given endpoint (IP, Hostname). Investigation contains IP, Severity and offense description.
- Can apply Trellix ePO Saas policy, based on a tag assigned at IBM QRadar 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:


IBM QRadar Cloud Server
QRadar Offence (Alert) Service
QRadar Extension manager
Download and install Trellix ePO Saas Connector App from IBM App Exchange
5
Trellix Connector App Container
1. Trellix ePO Saas Auth Config.
2 Scheduler Config.
3. Filter Config.
6
Configuration UI
Filter/Mapping
Scheduler / Listener
SQL
SQL Lite
Fetch Offences
8
QRadar Console
10
Apply Trellix ePO Saas Tag / Fetch Device Info from Trellix ePO Saas
7
Tenant Validation
9
Create MVEDR Investigation (and) Pull Threat evens from Trellix ePO Saas based on the configuration
4
Redirect to IBM QRadar Cloud server
Trellix Market Place (QRadar App)
3
Launch QRadar Server URL
QRadar App UI Configuration
2
Configure and Save QRadar Server Details
1
Acquire IBM QRadar App
IAM/BPS
Customer
Trellix API Gateway
Trellix ePO Saas
MVEDR

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

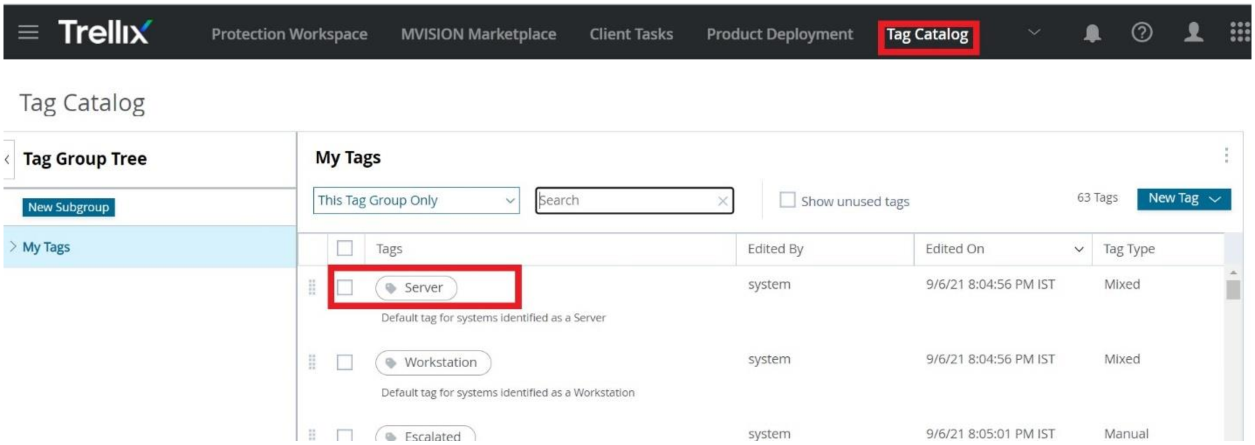
    1. Admin | Log Sources | Launch | Log Sources (Manage Log Sources) | select MVISION ePO Threat Events | click on menu | Delete

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:

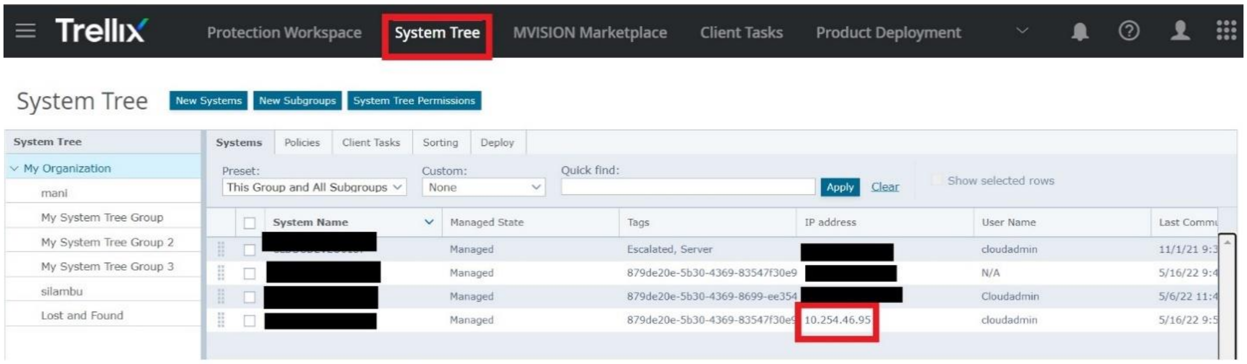
- Before applying Trellix ePO Saas tags action, user must make sure the tags to be applied on the system(s) are created in Trellix ePO Saas server Tag Catalog.
  For e.g. - Create a tag with name - Server
- Refer the screenshot below –



	Tags	Edited By	Edited On	Tag Type
□	Server Default tag for systems identified as a Server	system	9/6/21 8:04:56 PM IST	Mixed
□	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:

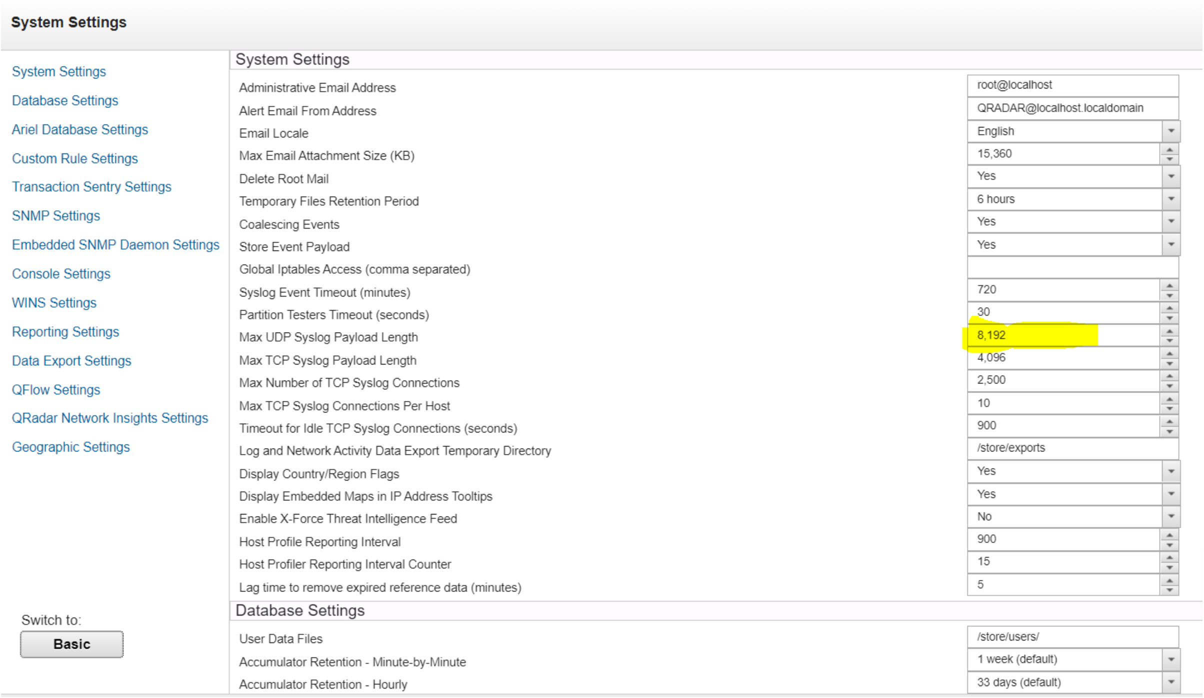


Preset: This Group and All Subgroups
Custom: None
Quick find:

□	System Name	Managed State	Tags	IP address	User Name	Last Commu
□	[redacted]	Managed	Escalated, Server	[redacted]	cloudadmin	11/1/21 9:3
□	[redacted]	Managed	879de20e-5b30-4369-83547f30e9	[redacted]	N/A	5/16/22 9:4
□	[redacted]	Managed	879de20e-5b30-4369-8699-ee354	[redacted]	Cloudadmin	5/6/22 11:4
□	[redacted]	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:



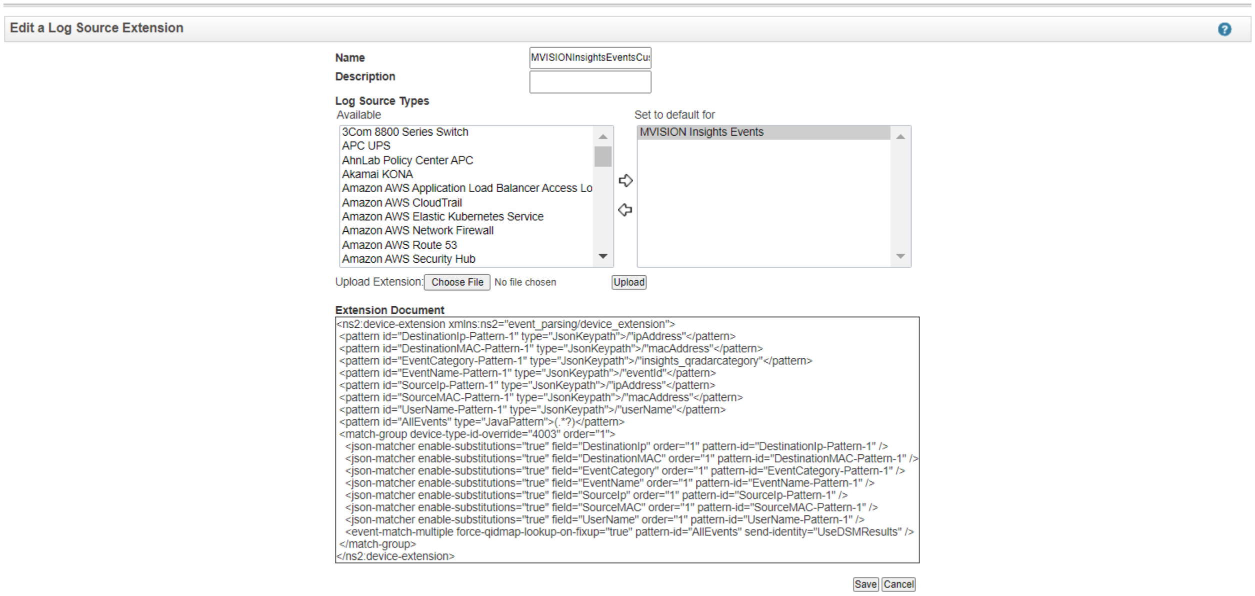
System Settings

Administrative Email Address	root@localhost
Alert Email From Address	QRADAR@localhost.localdomain
Email Locale	English
Max Email Attachment Size (KB)	15,360
Delete Root Mail	Yes
Temporary Files Retention Period	6 hours
Coalescing Events	Yes
Store Event Payload	Yes
Global Iptables Access (comma separated)	
Syslog Event Timeout (minutes)	720
Partition Testers Timeout (seconds)	30
Max UDP Syslog Payload Length	8,192
Max TCP Syslog Payload Length	4,096
Max Number of TCP Syslog Connections	2,500
Max TCP Syslog Connections Per Host	10
Timeout for Idle TCP Syslog Connections (seconds)	900
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

Database Settings

User Data Files	/store/users/
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:



Name: MVISIONInsightsEventsCu:

Description:

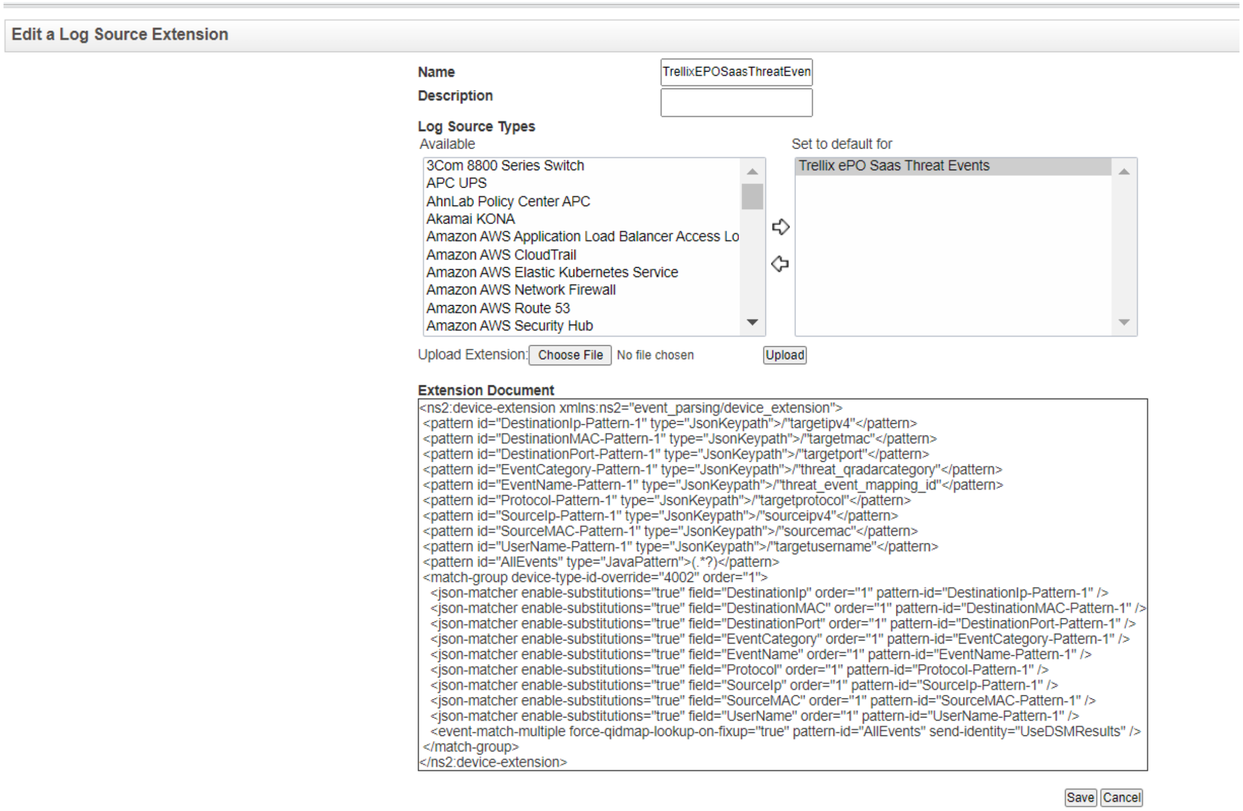
Log Source Types

Available:
- 3Com 8800 Series Switch
- APC UPS
- AhnLab Policy Center APC
- Akamai KONA
- Amazon AWS Application Load Balancer Access Lo
- Amazon AWS CloudTrail
- Amazon AWS Elastic Kubernetes Service
- Amazon AWS Network Firewall
- Amazon AWS Route 53
- Amazon AWS Security Hub

Set to default for:
- MVISION Insights Events

Extension Document

```
<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
 <pattern id="DestinationIp-Pattern-1" type="JsonKeypath">/"ipAddress"</pattern>
 <pattern id="DestinationMAC-Pattern-1" type="JsonKeypath">/"macAddress"</pattern>
 <pattern id="EventCategory-Pattern-1" type="JsonKeypath">/"insights_qradarcategory"</pattern>
 <pattern id="EventName-Pattern-1" type="JsonKeypath">/"eventId"</pattern>
 <pattern id="SourceIp-Pattern-1" type="JsonKeypath">/"ipAddress"</pattern>
 <pattern id="SourceMAC-Pattern-1" type="JsonKeypath">/"macAddress"</pattern>
 <pattern id="UserName-Pattern-1" type="JsonKeypath">/"userName"</pattern>
 <pattern id="AllEvents" type="JavaPattern">(.*?)</pattern>
 <match-group device-type-id-override="4003" order="1">
  <json-matcher enable-substitutions="true" field="DestinationIp" order="1" pattern-id="DestinationIp-Pattern-1" />
  <json-matcher enable-substitutions="true" field="DestinationMAC" order="1" pattern-id="DestinationMAC-Pattern-1" />
  <json-matcher enable-substitutions="true" field="EventCategory" order="1" pattern-id="EventCategory-Pattern-1" />
  <json-matcher enable-substitutions="true" field="EventName" order="1" pattern-id="EventName-Pattern-1" />
  <json-matcher enable-substitutions="true" field="SourceIp" order="1" pattern-id="SourceIp-Pattern-1" />
  <json-matcher enable-substitutions="true" field="SourceMAC" order="1" pattern-id="SourceMAC-Pattern-1" />
  <json-matcher enable-substitutions="true" field="UserName" order="1" pattern-id="UserName-Pattern-1" />
  <event-match-multiple force-qidmap-lookup-on-fixup="true" pattern-id="AllEvents" send-identity="UseDSMResults" />
 </match-group>
</ns2:device-extension>
```



Name: TrellixEPOSaasThreatEven

Description:

Log Source Types

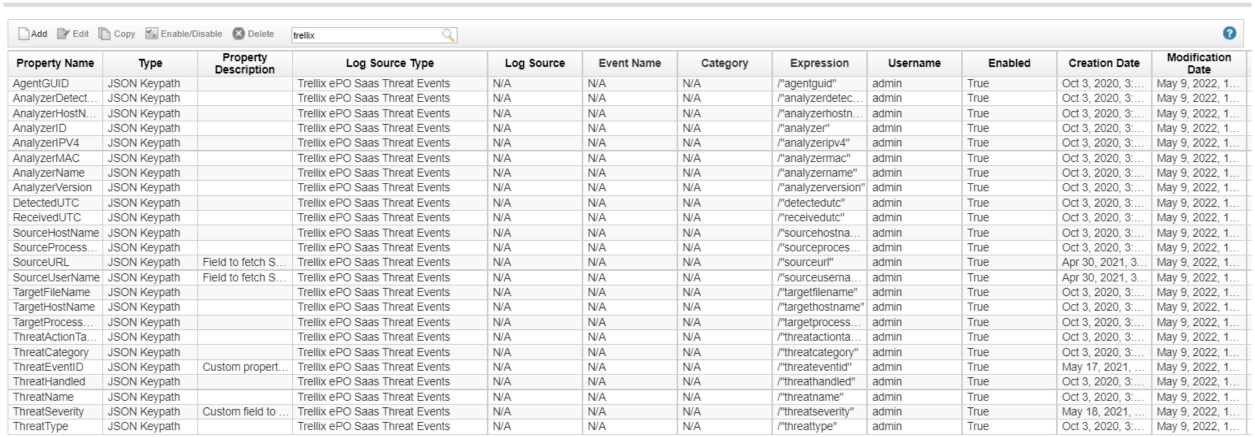
Available:
- 3Com 8800 Series Switch
- APC UPS
- AhnLab Policy Center APC
- Akamai KONA
- Amazon AWS Application Load Balancer Access Lo
- Amazon AWS CloudTrail
- Amazon AWS Elastic Kubernetes Service
- Amazon AWS Network Firewall
- Amazon AWS Route 53
- Amazon AWS Security Hub

Set to default for:
- Trellix ePO Saas Threat Events

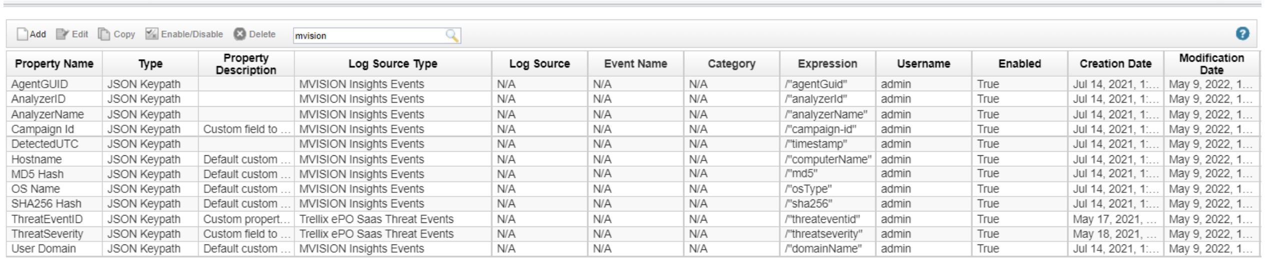
Extension Document

```
<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
 <pattern id="DestinationIp-Pattern-1" type="JsonKeypath">/"targetipv4"</pattern>
 <pattern id="DestinationMAC-Pattern-1" type="JsonKeypath">/"targetmac"</pattern>
 <pattern id="DestinationPort-Pattern-1" type="JsonKeypath">/"targetport"</pattern>
 <pattern id="EventCategory-Pattern-1" type="JsonKeypath">/"threat_qradarcategory"</pattern>
 <pattern id="EventName-Pattern-1" type="JsonKeypath">/"threat_event_mapping_id"</pattern>
 <pattern id="Protocol-Pattern-1" type="JsonKeypath">/"targetprotocol"</pattern>
 <pattern id="SourceIp-Pattern-1" type="JsonKeypath">/"sourceipv4"</pattern>
 <pattern id="SourceMAC-Pattern-1" type="JsonKeypath">/"sourcemac"</pattern>
 <pattern id="UserName-Pattern-1" type="JsonKeypath">/"targetusername"</pattern>
 <pattern id="AllEvents" type="JavaPattern">(.*?)</pattern>
 <match-group device-type-id-override="4002" order="1">
  <json-matcher enable-substitutions="true" field="DestinationIp" order="1" pattern-id="DestinationIp-Pattern-1" />
  <json-matcher enable-substitutions="true" field="DestinationMAC" order="1" pattern-id="DestinationMAC-Pattern-1" />
  <json-matcher enable-substitutions="true" field="DestinationPort" order="1" pattern-id="DestinationPort-Pattern-1" />
  <json-matcher enable-substitutions="true" field="EventCategory" order="1" pattern-id="EventCategory-Pattern-1" />
  <json-matcher enable-substitutions="true" field="EventName" order="1" pattern-id="EventName-Pattern-1" />
  <json-matcher enable-substitutions="true" field="Protocol" order="1" pattern-id="Protocol-Pattern-1" />
  <json-matcher enable-substitutions="true" field="SourceIp" order="1" pattern-id="SourceIp-Pattern-1" />
  <json-matcher enable-substitutions="true" field="SourceMAC" order="1" pattern-id="SourceMAC-Pattern-1" />
  <json-matcher enable-substitutions="true" field="UserName" order="1" pattern-id="UserName-Pattern-1" />
  <event-match-multiple force-qidmap-lookup-on-fixup="true" pattern-id="AllEvents" send-identity="UseDSMResults" />
 </match-group>
</ns2:device-extension>
```

- **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 Description	Log Source Type	Log Source	Event Name	Category	Expression	Username	Enabled	Creation Date	Modification 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		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, 1...
ThreatType	JSON Keypath		Trellix ePO Saas Threat Events	N/A	N/A	N/A	/"threattype"	admin	True	Oct 3, 2020, 3:...	May 9, 2022, 1...



Property Name	Type	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	/"analyzerId"	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.

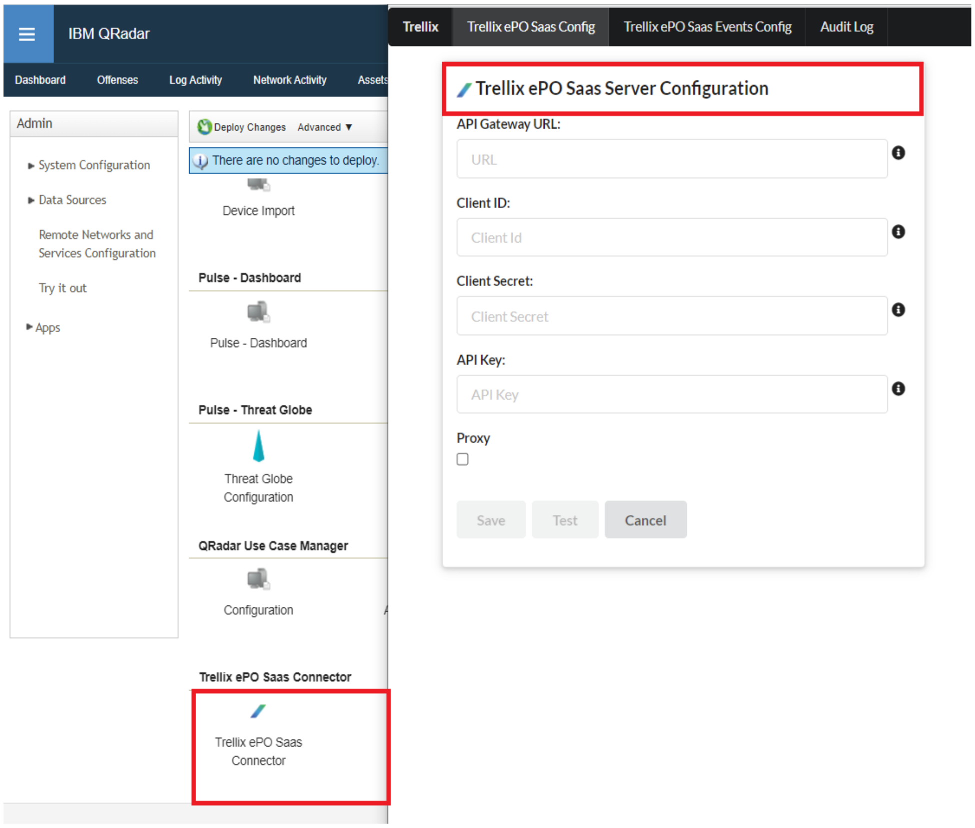
Acquiring client credentials from Trellix Marketplace

1. As part of the workflow customer/tenant should login into Trellix Marketplace using their Trellix credential.
2. 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.
5. 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**”.
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.
8. 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-



Trellix ePO Saas Server Configuration

API Gateway URL: URL

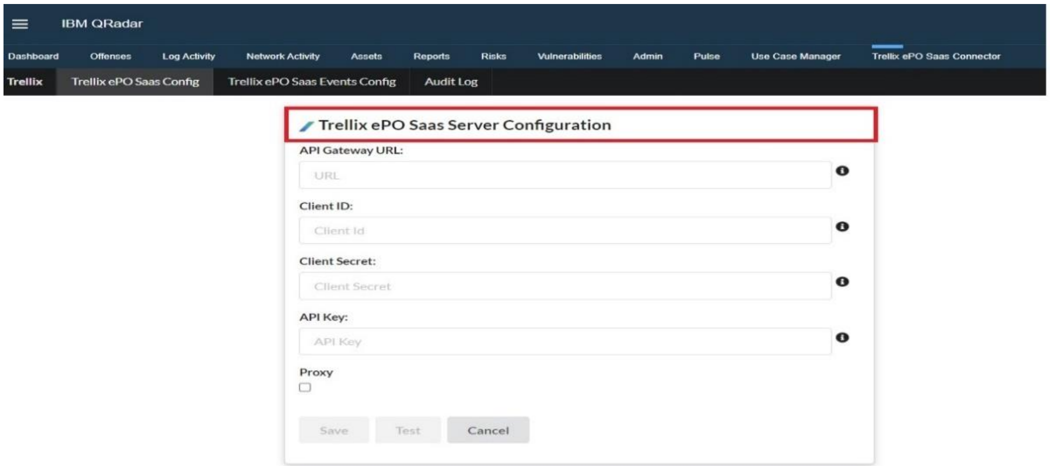
Client ID: Client Id

Client Secret: Client Secret

API Key: API Key

Proxy
□

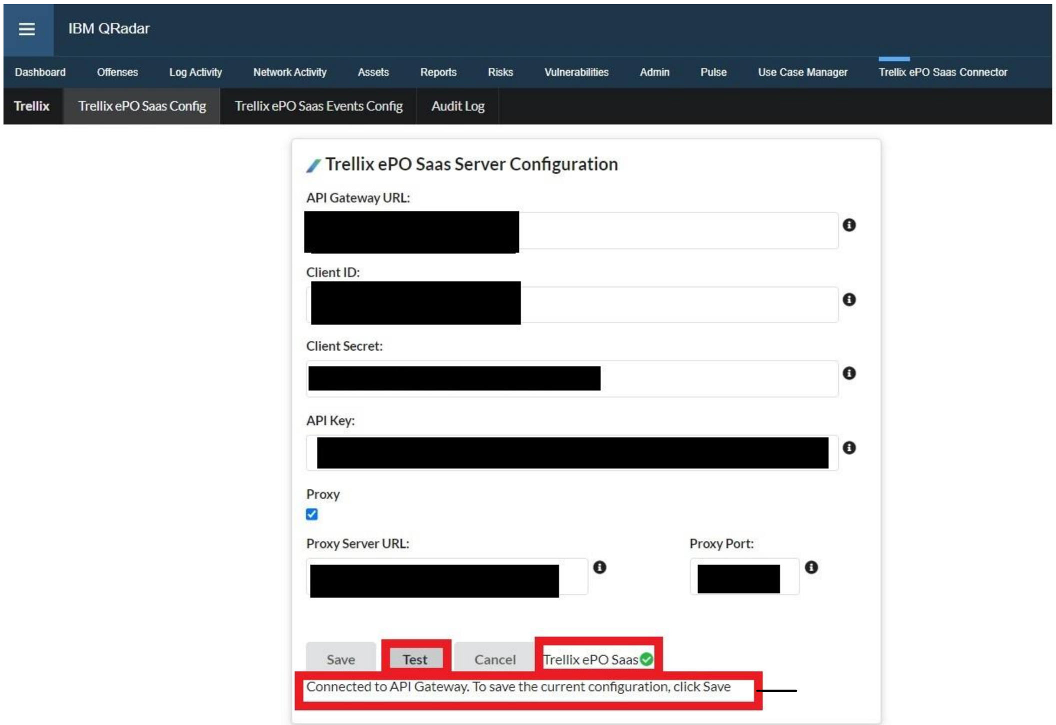
Also, the same app will be shown as part of QRadar ribbon tab. Refer the screenshot below-



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 id from Trellix Market place>	Provide valid Client ID which is generated by the Tenant ID provided in the activation mail.
Client Secret	<client secret from Trellix Market place >	Provide valid Client Secret which is generated by the Tenant ID provided in the activation mail.
API Key	<api key from Trellix Market place>	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.



Trellix ePO Saas Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: [redacted]

API Key: [redacted]

Proxy
☑

Proxy Server URL: [redacted]

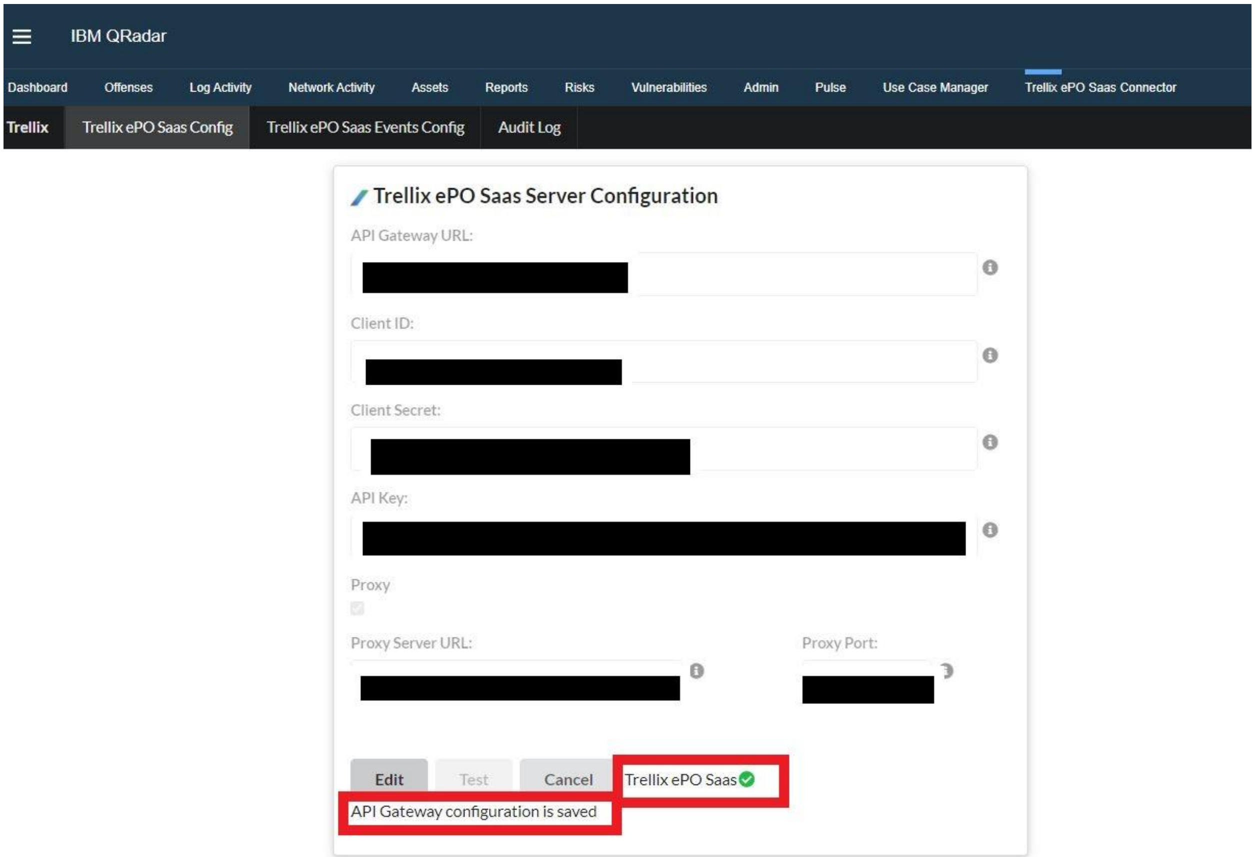
Proxy Port: [redacted]

Trellix ePO Saas ✓

Connected to API Gateway. To save the current configuration, click Save

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

Refer the screenshot below-



Trellix ePO Saas Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: [redacted]

API Key: [redacted]

Proxy

☑

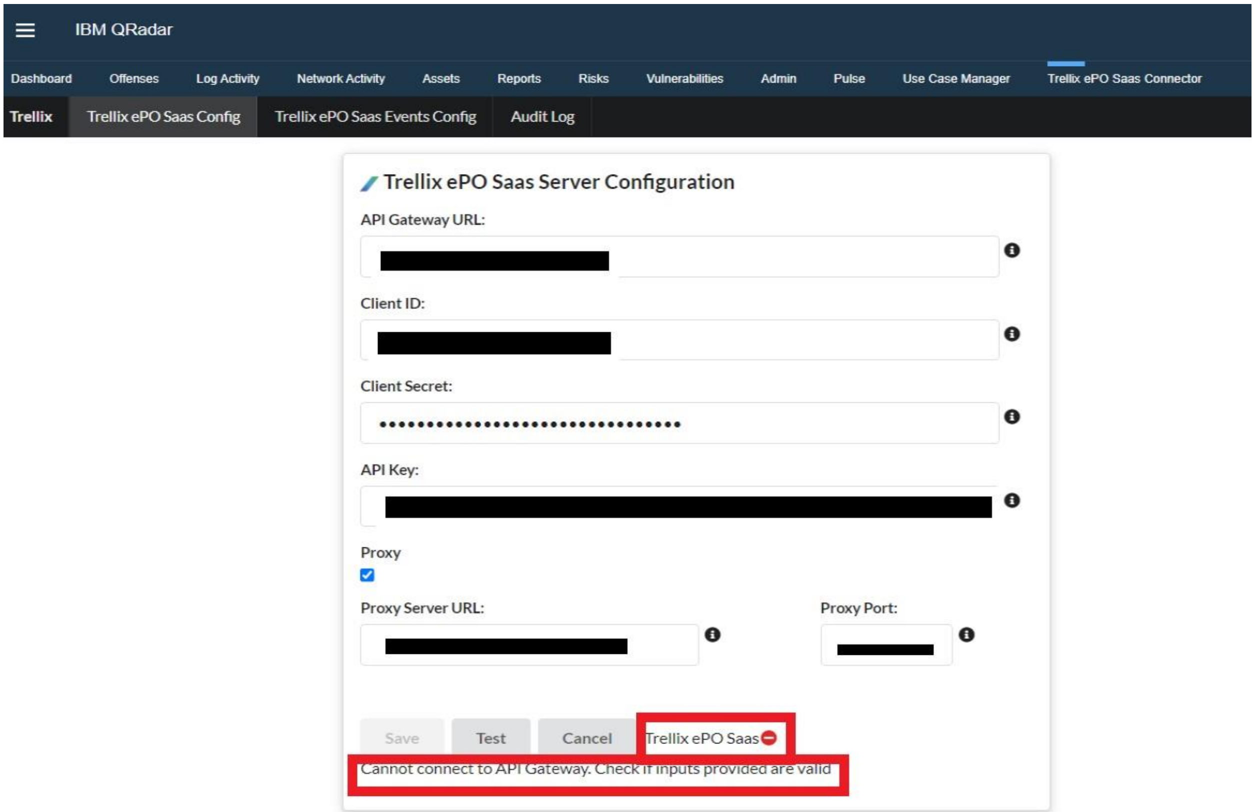
Proxy Server URL: [redacted]

Proxy Port: [redacted]

Trellix ePO Saas ✓

API Gateway configuration is saved

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



Trellix ePO Saas Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: ••••••••••••••••••••••••••••••••

API Key: [redacted]

Proxy ☑

Proxy Server URL: [redacted]

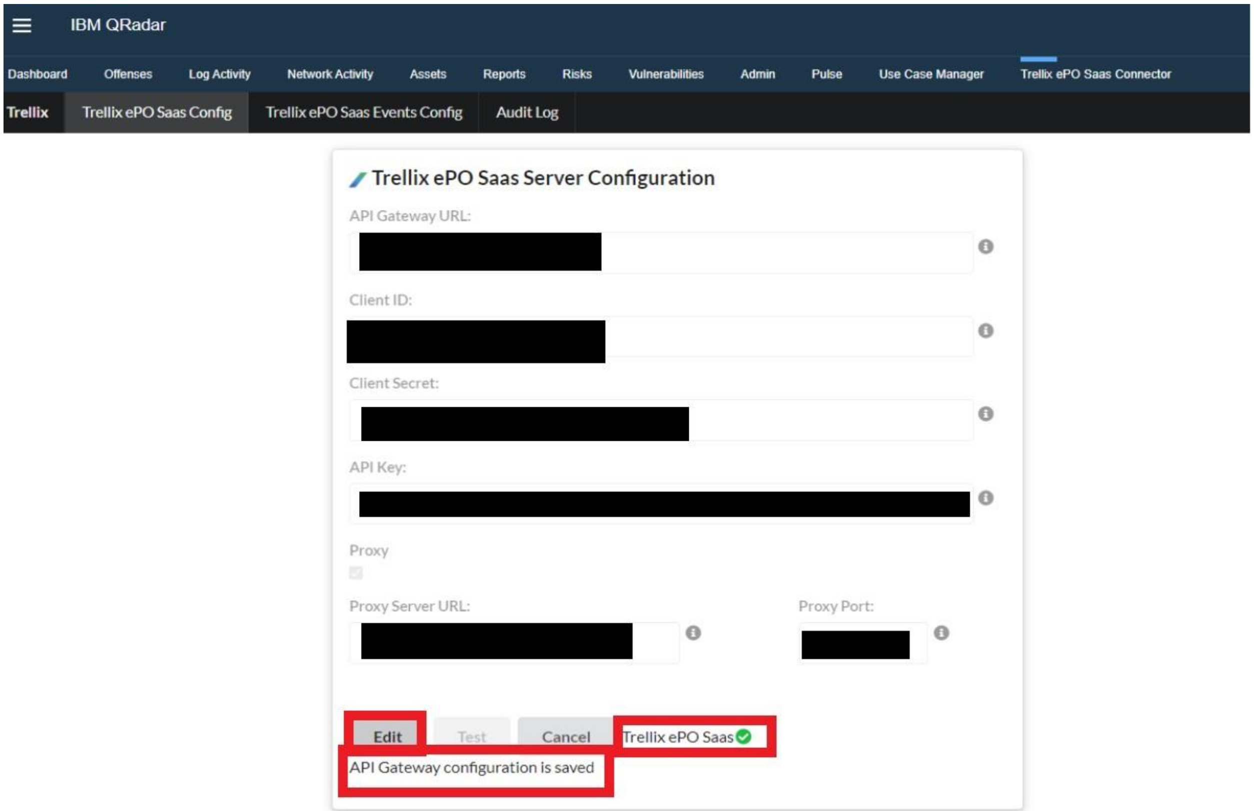
Proxy Port: [redacted]

Trellix ePO Saas ⛔

Cannot connect to API Gateway. Check if inputs provided are valid

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-



Trellix ePO Saas Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: [redacted]

API Key: [redacted]

Proxy

☑

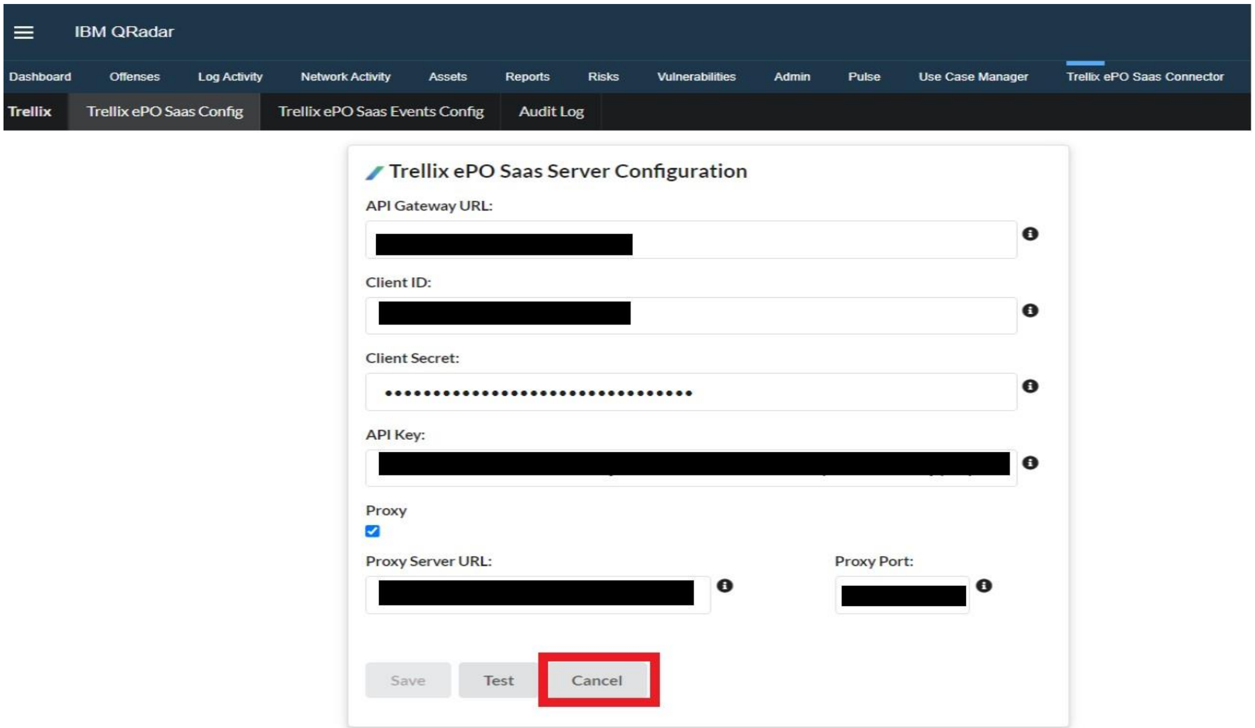
Proxy Server URL: [redacted]

Proxy Port: [redacted]

Trellix ePO Saas ✓

API Gateway configuration is saved

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-



Trellix ePO Saas Server Configuration

API Gateway URL: [redacted]

Client ID: [redacted]

Client Secret: ••••••••••••••••••••••••••••••••••

API Key: [redacted]

Proxy
☑

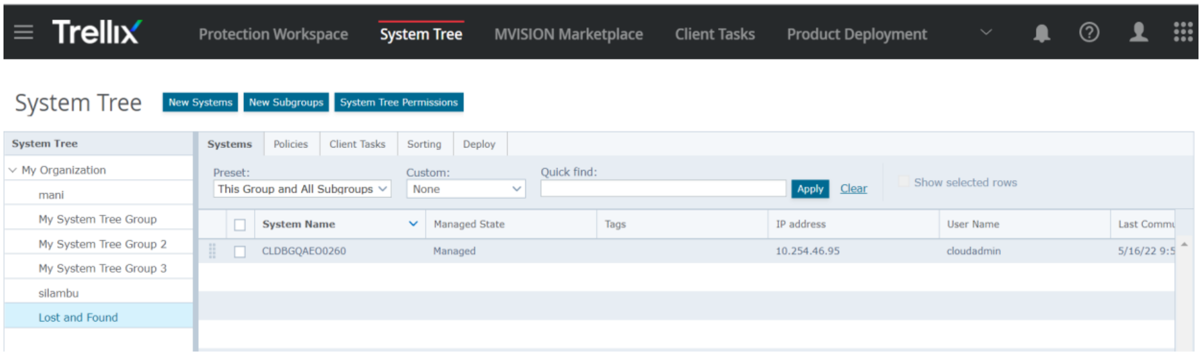
Proxy Server URL: [redacted]

Proxy Port: [redacted]

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-



Preset: This Group and All Subgroups

Custom: None

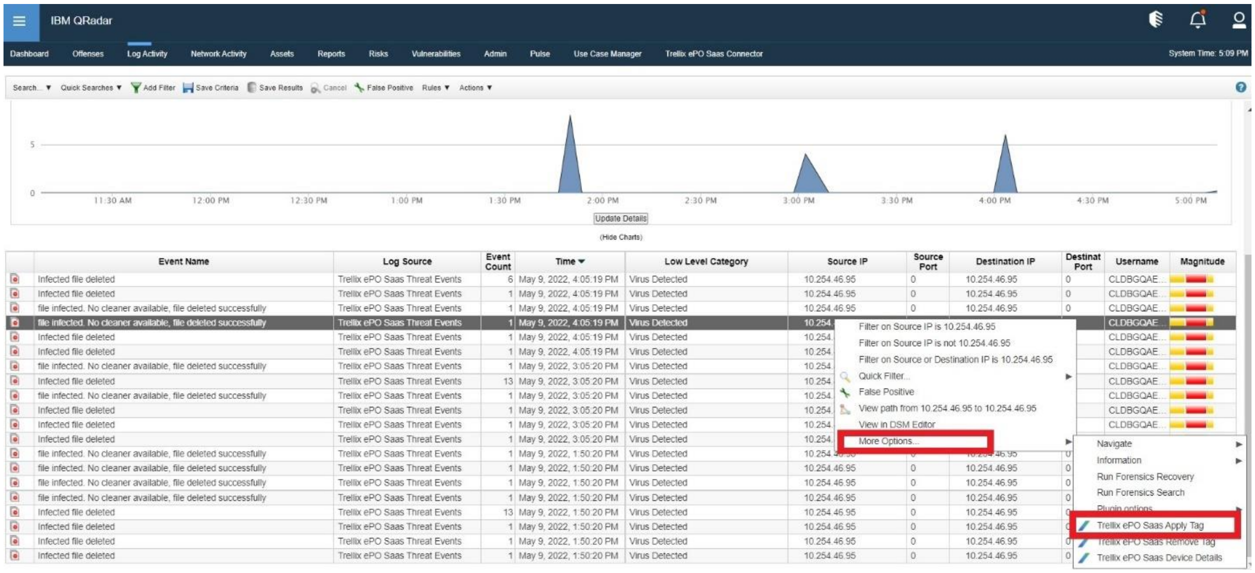
Quick find:

System Name	Managed State	Tags	IP address	User Name	Last Commu
CLDBGQAEO0260	Managed		10.254.46.95	cloudadmin	5/16/22 9:5

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

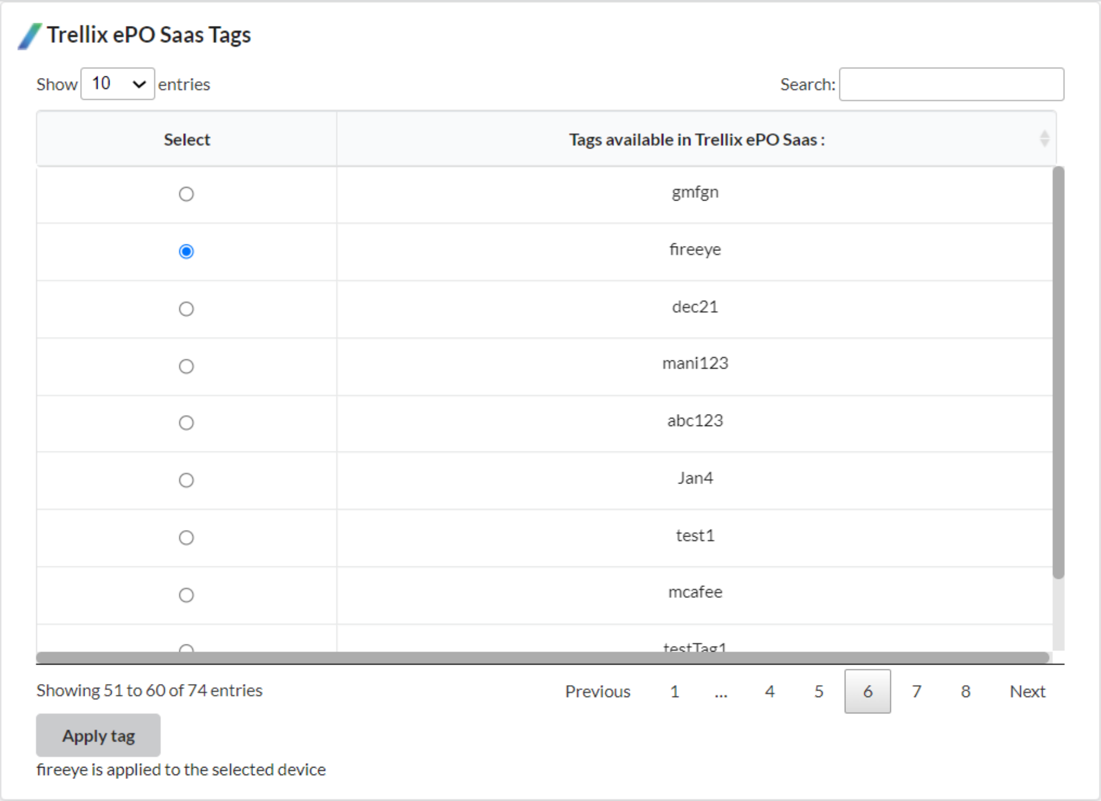
Go to “Log Activity” page in QRadar console and right click on **Source IP** column and select **More Options | Trellix ePO Saas Apply Tag.** This action will open a new page to perform “**Trellix ePO Saas Apply Tag**” action.

Refer the screenshot below-



Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
Infected file deleted	Trellix ePO Saas Threat Events	6	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	CLDBGQAE...	🟨🟥🟨
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	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 PM	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 PM	Virus Detected	10.254.				CLDBGQAE...	🟨🟥🟨
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.				CLDBGQAE...	🟨🟥🟨
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.				CLDBGQAE...	🟨🟥🟨
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254.				CLDBGQAE...	🟨🟥🟨
Infected file deleted	Trellix ePO Saas Threat Events	13	May 9, 2022, 3:05:20 PM	Virus Detected	10.254.				CLDBGQAE...	🟨🟥🟨
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254.				CLDBGQAE...	🟨🟥🟨
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254.				CLDBGQAE...	🟨🟥🟨
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254.				CLDBGQAE...	🟨🟥🟨
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254.					
file 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		
file 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		
file 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		
file 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		
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		
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		
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		
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		

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-



Trellix ePO Saas Tags

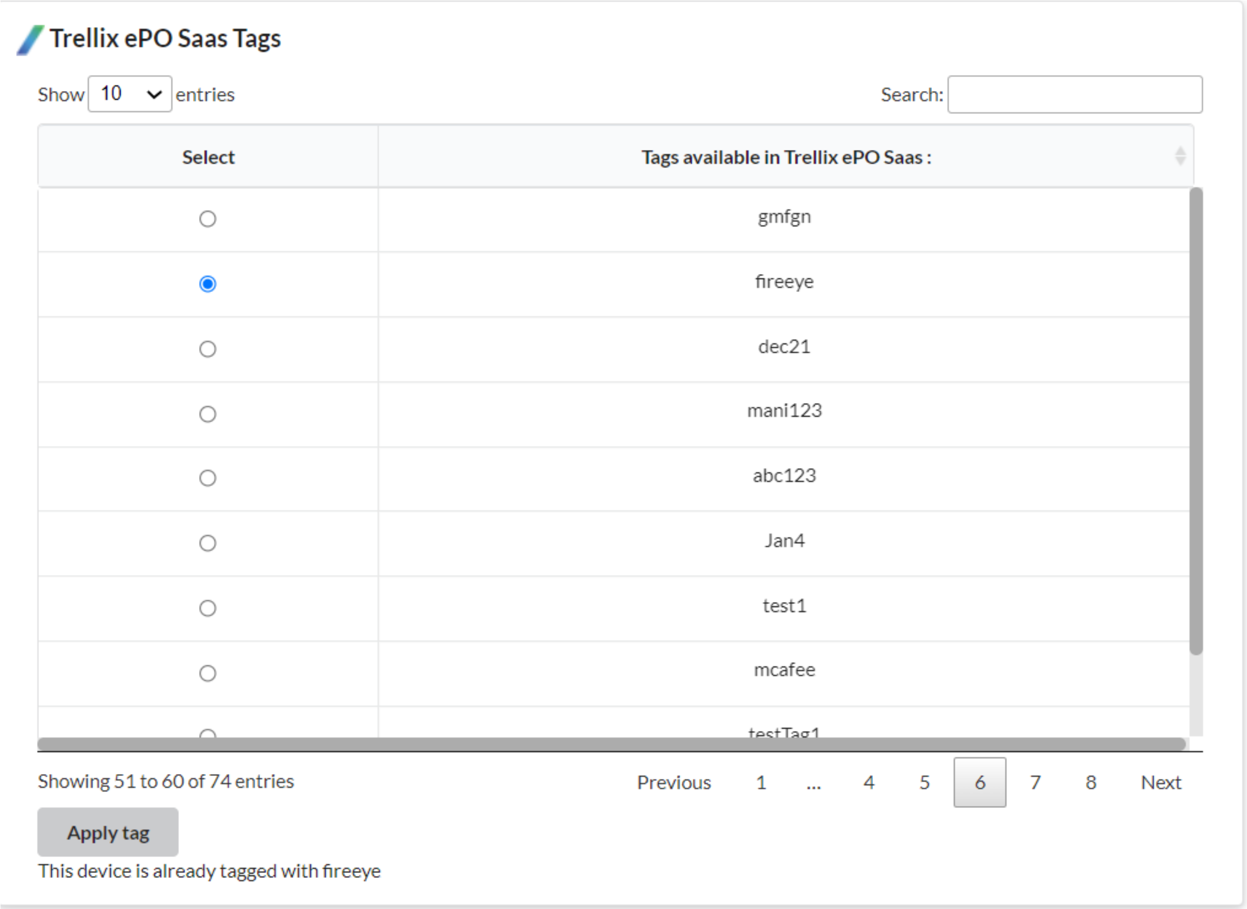
Select	Tags available in Trellix ePO Saas :
○	gmfgn
●	fireeye
○	dec21
○	mani123
○	abc123
○	Jan4
○	test1
○	mcafee
○	testTag1

Showing 51 to 60 of 74 entries

fireeye is applied to the selected device

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

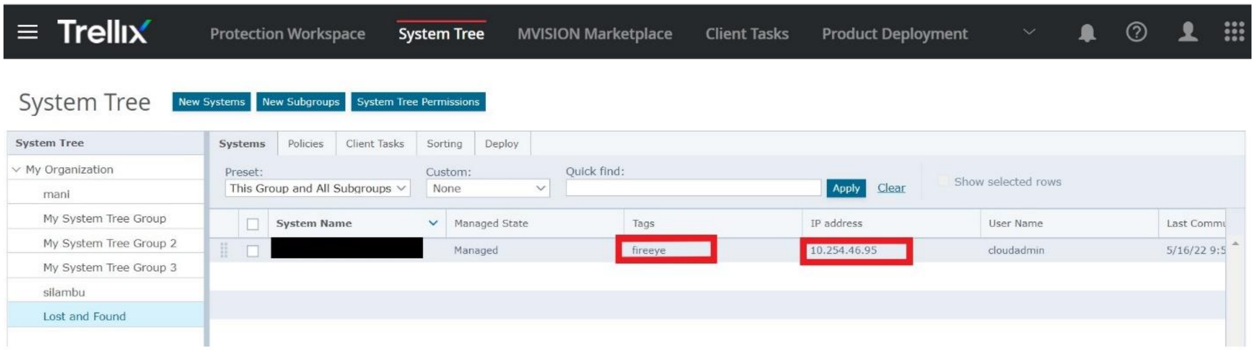
Show 10 entries Search:

Select	Tags available in Trellix ePO Saas :
○	gmfgn
●	fireeye
○	dec21
○	mani123
○	abc123
○	Jan4
○	test1
○	mcafee
○	testTag1

Showing 51 to 60 of 74 entries

This device is already tagged with fireeye

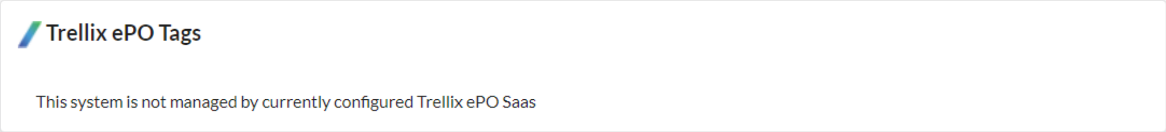
Once the "**Trellix ePO Saas Apply Tag**" action in QRadar server is successful you can see the same in the Trellix ePO's Saas system tree page next to the selected system. Refer the screenshot below-



Preset: This Group and All Subgroups
Custom: None
Quick find:

	System Name	Managed State	Tags	IP address	User Name	Last Commu
□	[redacted]	Managed	fireeye	10.254.46.95	cloudadmin	5/16/22 9:5

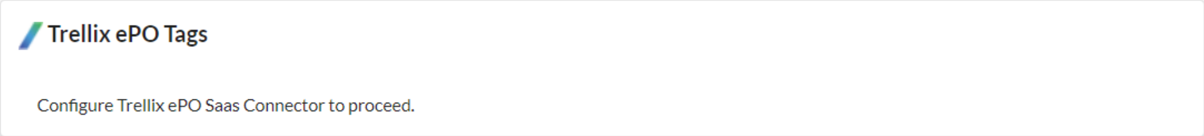
Note: In case the selected IP is not managed by the Trellix ePO Saas configured in the QRadar-Right click on **Source IP** column and select **More Options | Trellix ePO Saas Tags** will display a message indicating "This system is not managed by currently configured Trellix ePO Saas". Refer the screenshot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



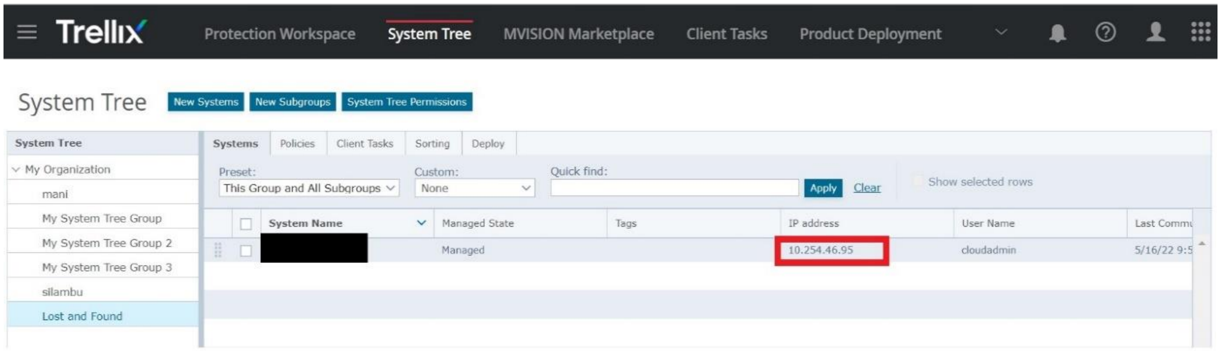
Trellix ePO Tags

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-



Preset: This Group and All Subgroups

Custom: None

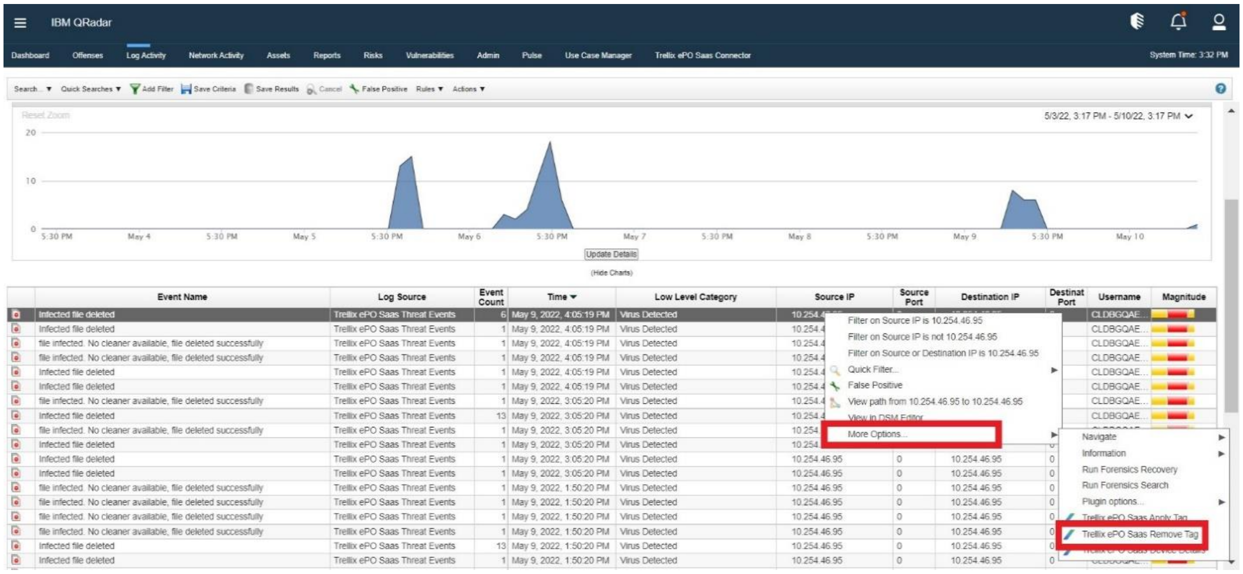
Quick find:

□	System Name	Managed State	Tags	IP address	User Name	Last Comm
□	[redacted]	Managed		10.254.46.95	cloudadmin	5/16/22 9:5

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.

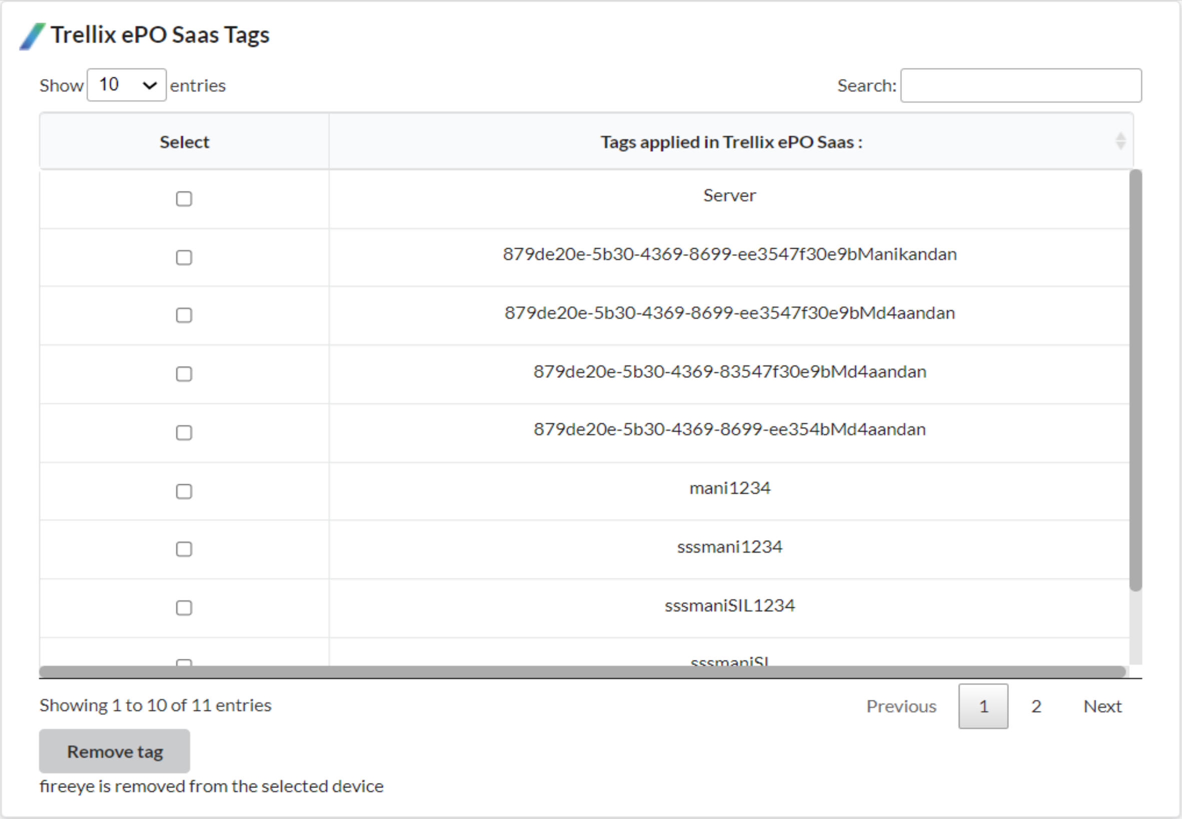
Refer the screenshot below-



Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
Infected file deleted	Trellix ePO Saas Threat Events	6	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.4				CLDBGQAE...	
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.4				CLDBGQAE...	
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.4				CLDBGQAE...	
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.4				CLDBGQAE...	
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.4				CLDBGQAE...	
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.4				CLDBGQAE...	
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254.4				CLDBGQAE...	
Infected file deleted	Trellix ePO Saas Threat Events	13	May 9, 2022, 3:05:20 PM	Virus Detected	10.254.4				CLDBGQAE...	
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254					
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254			0		
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		
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		
file 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		
file 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		
file 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		
file 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		
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		
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		

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

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



Trellix ePO Saas Tags

Show 10 entries

Search:

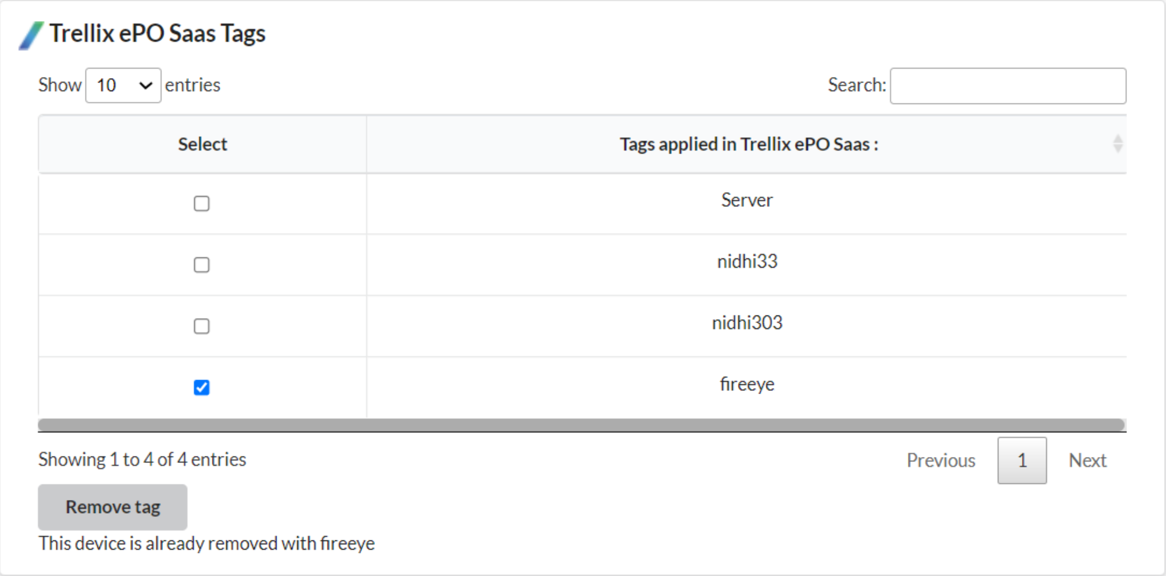
Select	Tags applied in Trellix ePO Saas :
□	Server
□	879de20e-5b30-4369-8699-ee3547f30e9bManikandan
□	879de20e-5b30-4369-8699-ee3547f30e9bMd4aandan
□	879de20e-5b30-4369-83547f30e9bMd4aandan
□	879de20e-5b30-4369-8699-ee354bMd4aandan
□	mani1234
□	sssmani1234
□	sssmaniSIL1234
□	sssmaniSI

Showing 1 to 10 of 11 entries

fireeye is removed from the selected device

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-



Trellix ePO Saas Tags

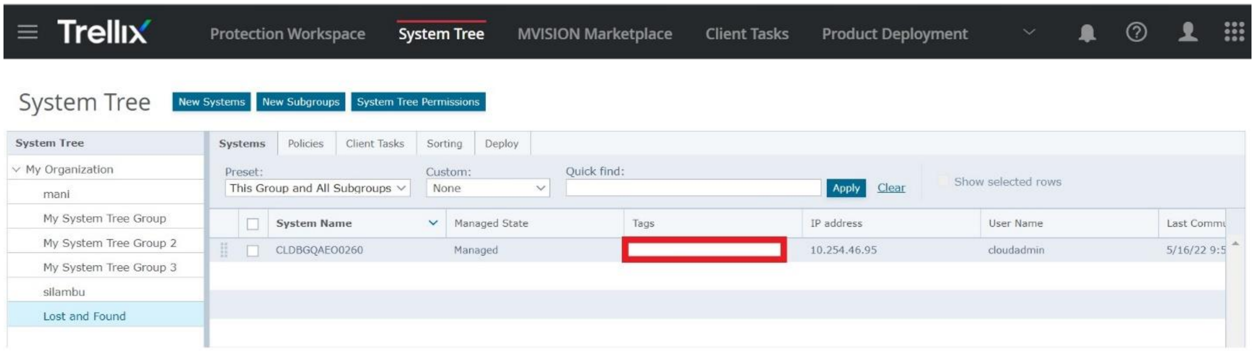
Show 10 entries Search:

Select	Tags applied in Trellix ePO Saas :
☐	Server
☐	nidhi33
☐	nidhi303
☑	fireeye

Showing 1 to 4 of 4 entries

This device is already removed with fireeye

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-



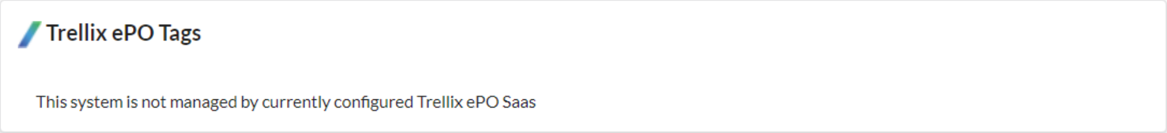
Preset: This Group and All Subgroups

Custom: None

Quick find:

☐	System Name	Managed State	Tags	IP address	User Name	Last Commu
☐	CLDBGQAEO0260	Managed		10.254.46.95	cloudadmin	5/16/22 9:5

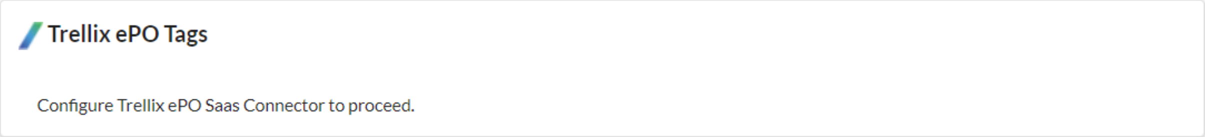
Note: In case the selected IP is not managed by the Trellix ePO Saas configured in the QRadar-Right click on **Source IP** column and select **More Options | Trellix ePO Saas Tags** will display a message indicating “This system is not managed by currently configured Trellix ePO Saas”. Refer the screenshot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



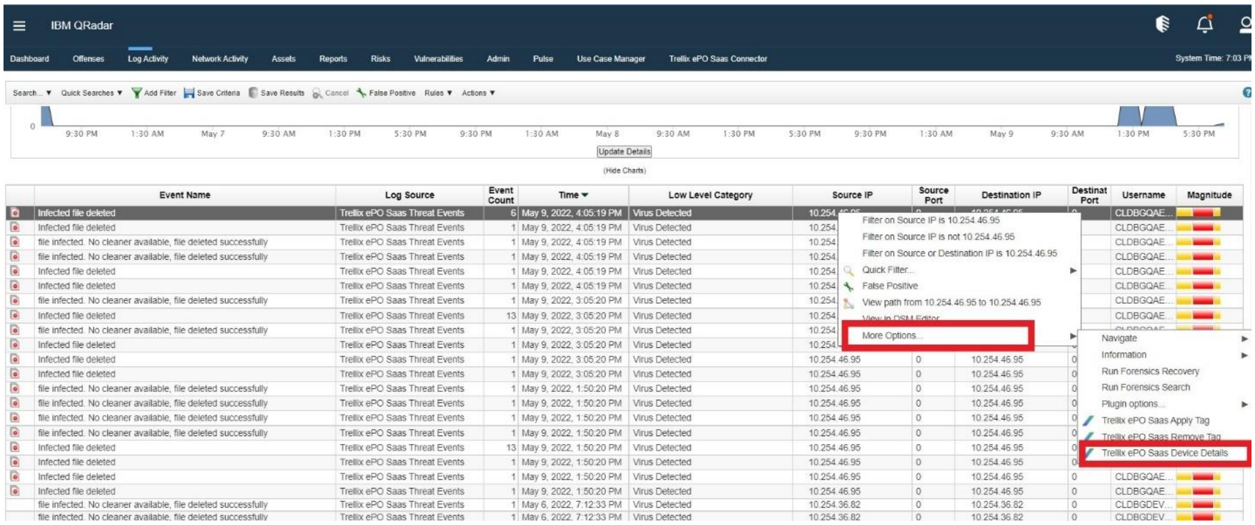
Trellix ePO Tags

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).

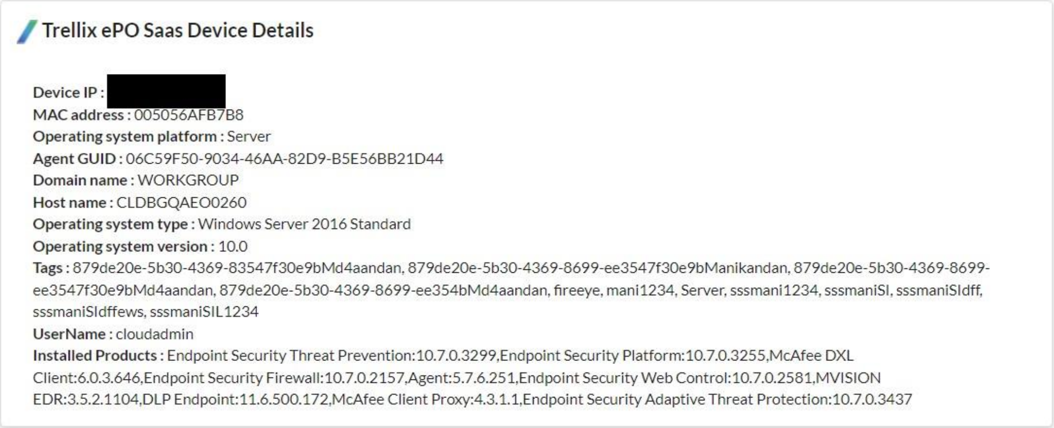
Refer the screenshot below-



Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
Infected file deleted	Trellix ePO Saas Threat Events	6	May 9, 2022, 4:05:19 PM	Virus Detected	10.254				CLDBGQAE...	
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254				CLDBGQAE...	
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254				CLDBGQAE...	
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254				CLDBGQAE...	
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254				CLDBGQAE...	
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254				CLDBGQAE...	
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254				CLDBGQAE...	
Infected file deleted	Trellix ePO Saas Threat Events	13	May 9, 2022, 3:05:20 PM	Virus Detected	10.254				CLDBGQAE...	
file infected. No cleaner available, file deleted successfully	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254					
Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 3:05:20 PM	Virus Detected	10.254					
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		
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		
file 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		
file 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		
file 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		
file 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		
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		
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		
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...	
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 deleted 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...	
file infected. No cleaner available, file deleted 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...	

This action will open a new popup page to show system details from Trellix ePO Saas server.

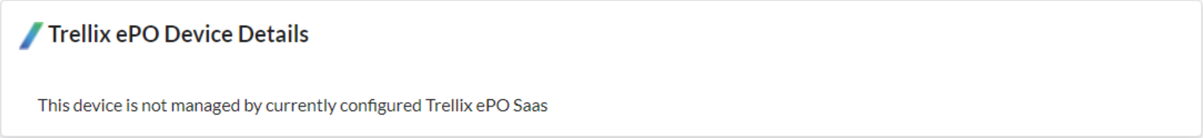
Considering the system 10.254.46.95. Refer the screenshot below-



Trellix ePO Saas Device Details

Device IP : [redacted]
MAC address : 005056AFB7B8
Operating system platform : Server
Agent GUID : 06C59F50-9034-46AA-82D9-B5E56BB21D44
Domain name : WORKGROUP
Host name : CLDBGQAEO0260
Operating system type : Windows Server 2016 Standard
Operating system version : 10.0
Tags : 879de20e-5b30-4369-83547f30e9bMd4aandan, 879de20e-5b30-4369-8699-ee3547f30e9bManikandan, 879de20e-5b30-4369-8699-ee3547f30e9bMd4aandan, 879de20e-5b30-4369-8699-ee354bMd4aandan, fireeye, mani1234, Server, sssmani1234, sssmaniSI, sssmaniSIdff, sssmaniSIdffews, sssmaniSIL1234
UserName : cloudadmin
Installed Products : Endpoint Security Threat Prevention:10.7.0.3299,Endpoint Security Platform:10.7.0.3255,McAfee DXL Client:6.0.3.646,Endpoint Security Firewall:10.7.0.2157,Agent:5.7.6.251,Endpoint Security Web Control:10.7.0.2581,MVISION EDR:3.5.2.1104,DLP Endpoint:11.6.500.172,McAfee Client Proxy:4.3.1.1,Endpoint Security Adaptive Threat Protection:10.7.0.3437

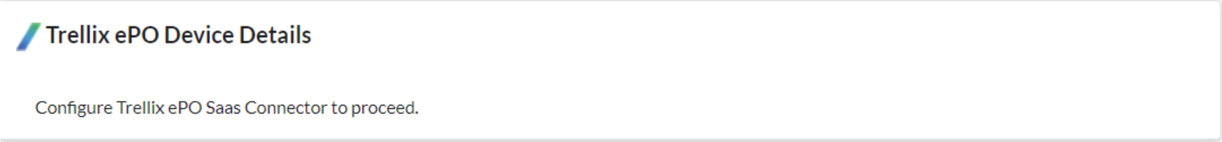
In case the selected IP is not managed by the Trellix ePO Saas configured in the QRadar-
Right click on **Source IP** column and select **More Options | Trelix ePO Saas Device Details** will display a message indicating "This system is not managed by currently configured Trellix ePO Saas". Refer the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

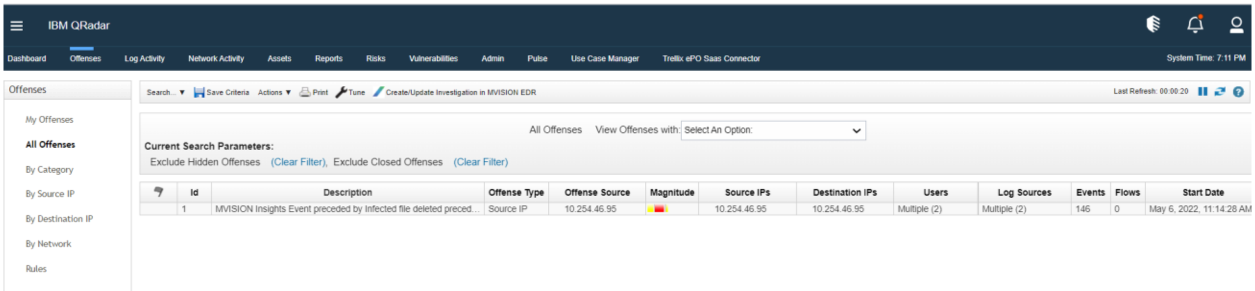
Configure Trellix ePO Saas Connector to proceed.

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:

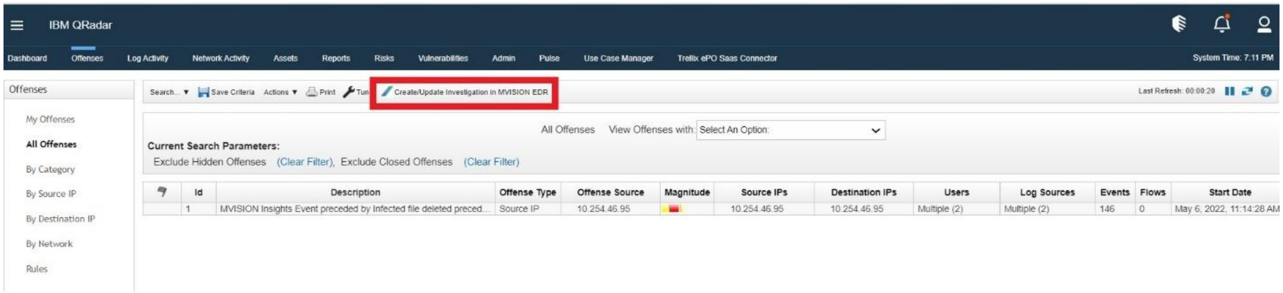


All Offenses View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start Date
	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

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

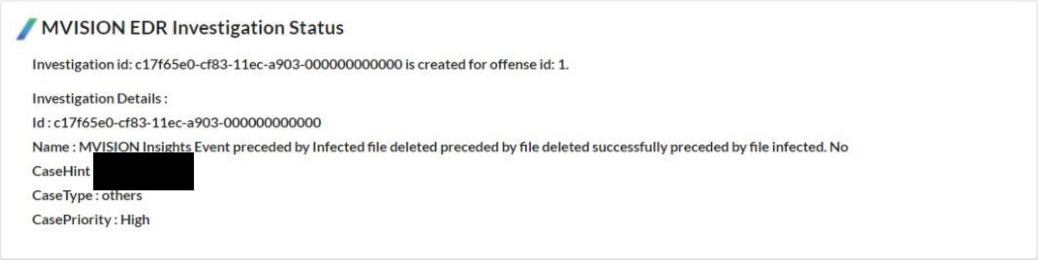


All Offenses View Offenses with: Select An Option:

Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flows	Start Date
	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:

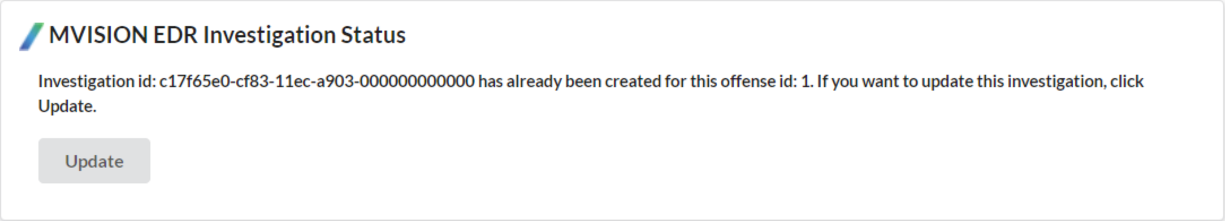


MVISION EDR Investigation Status

Investigation id: c17f65e0-cf83-11ec-a903-000000000000 is created for offense id: 1.

Investigation Details :
Id : c17f65e0-cf83-11ec-a903-000000000000
Name : MVISION Insights Event preceded by Infected file deleted preceded by file deleted successfully preceded by file infected. No
CaseHint [redacted]
CaseType : others
CasePriority : High

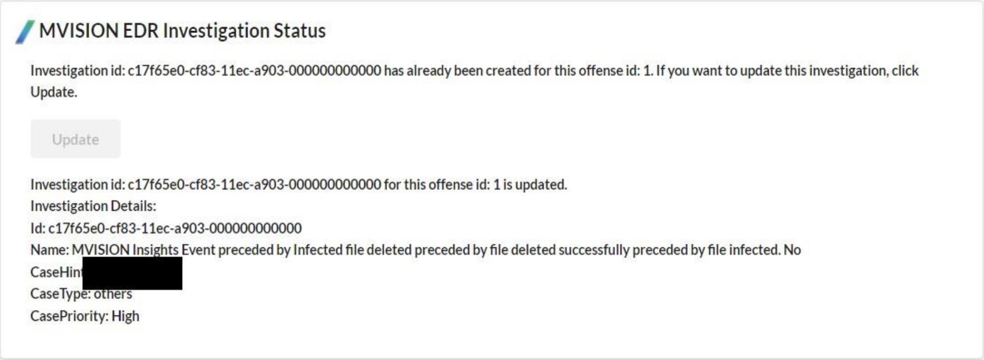
- If the investigation already exists in MVISION EDR then Admin will be presented with a window with Investigation id detail as shown below:



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 investigation, 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:

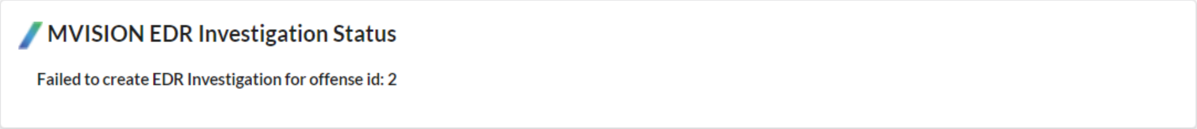


MVISION EDR Investigation Status

Investigation id: c17f65e0-cf83-11ec-a903-000000000000 has already been created for this offense id: 1. If you want to update this investigation, click Update.

Investigation id: c17f65e0-cf83-11ec-a903-000000000000 for this offense id: 1 is updated.
Investigation Details:
Id: c17f65e0-cf83-11ec-a903-000000000000
Name: MVISION Insights Event preceded by Infected file deleted preceded by file deleted successfully preceded by file infected. No
CaseHin[redacted]
CaseType: others
CasePriority: High

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



MVISION EDR Investigation Status

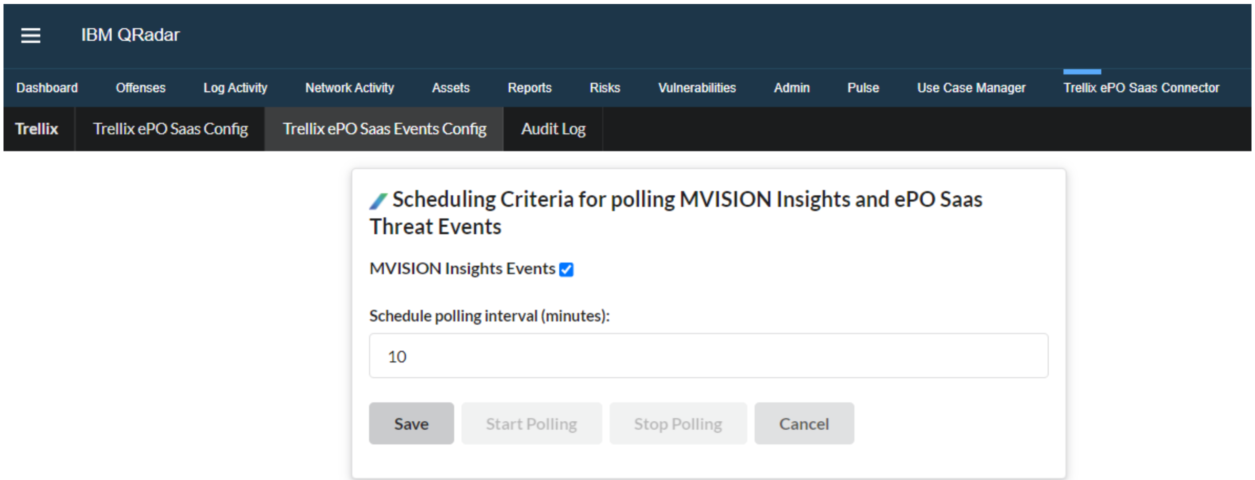
Failed to create EDR Investigation for offense id: 2

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:



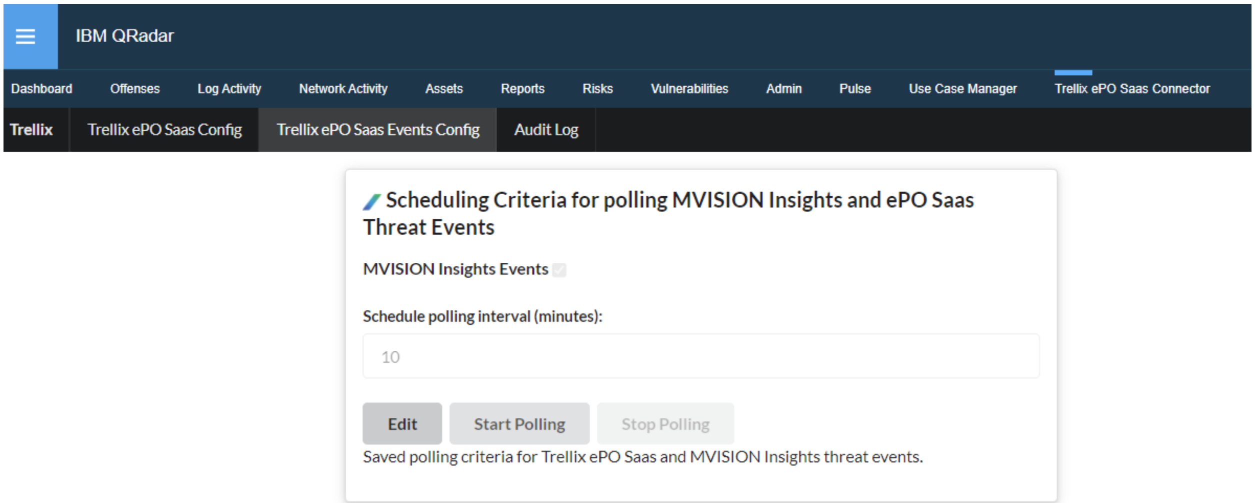
Scheduling Criteria for polling MVISION Insights and ePO Saas Threat Events

MVISION Insights Events ☑

Schedule polling interval (minutes):

10

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



Scheduling Criteria for polling MVISION Insights and ePO Saas Threat Events

MVISION Insights Events ☑

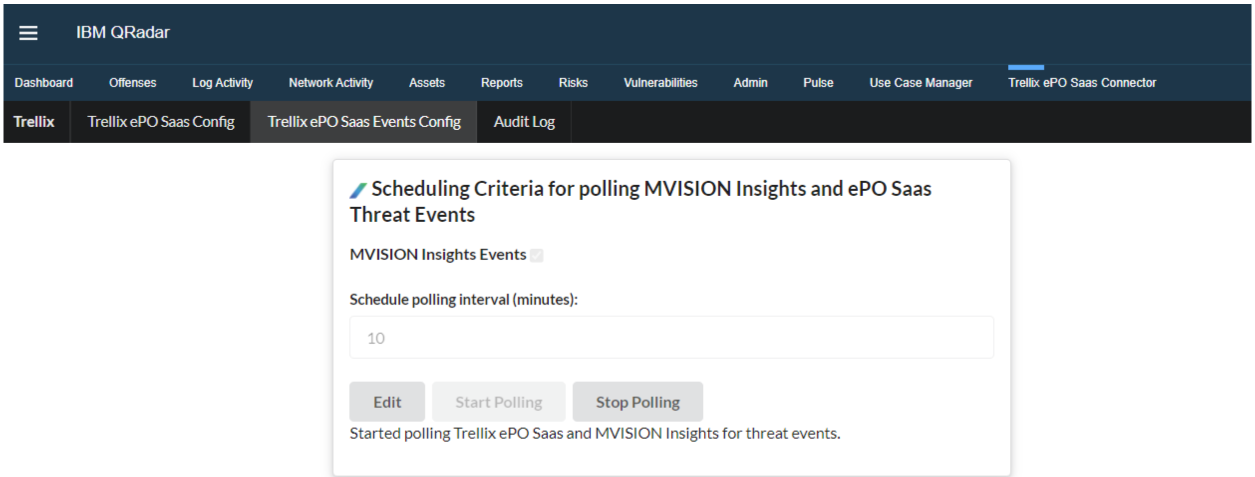
Schedule polling interval (minutes): 10

Saved polling criteria for Trellix ePO Saas and MVISION Insights threat events.

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:



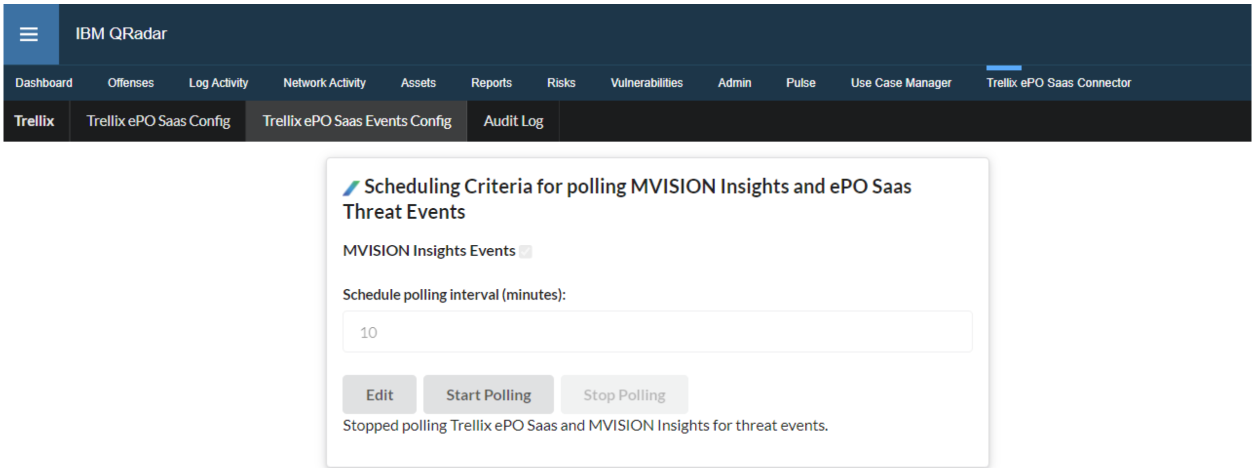
Scheduling Criteria for polling MVISION Insights and ePO Saas Threat Events

MVISION Insights Events ☑

Schedule polling interval (minutes): 10

Started polling Trellix ePO Saas and MVISION Insights for threat events.

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



Scheduling Criteria for polling MVISION Insights and ePO Saas Threat Events

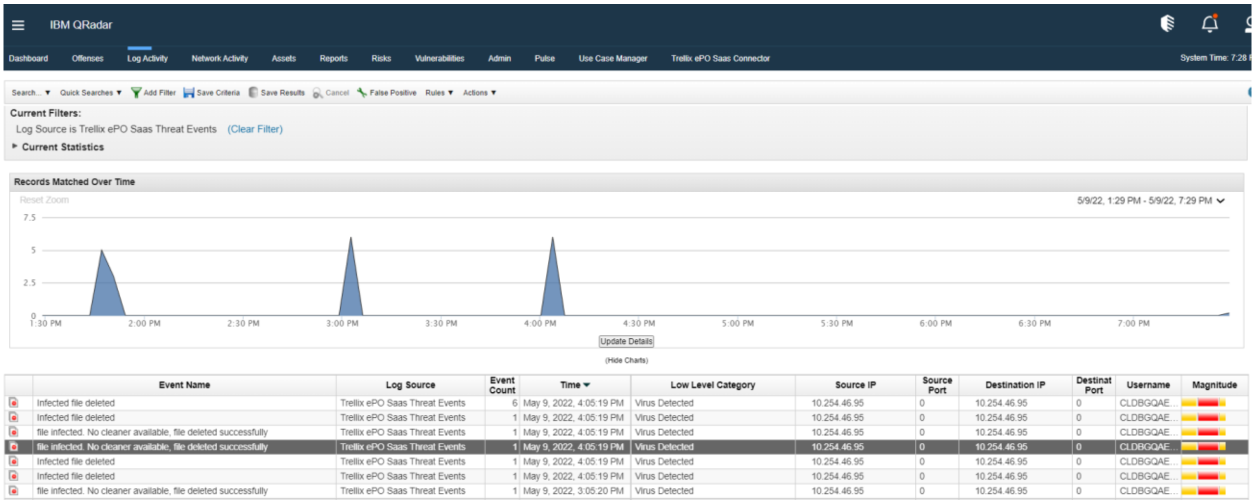
MVISION Insights Events ☑

Schedule polling interval (minutes): 10

Stopped polling Trellix ePO Saas and MVISION Insights for threat events.

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.

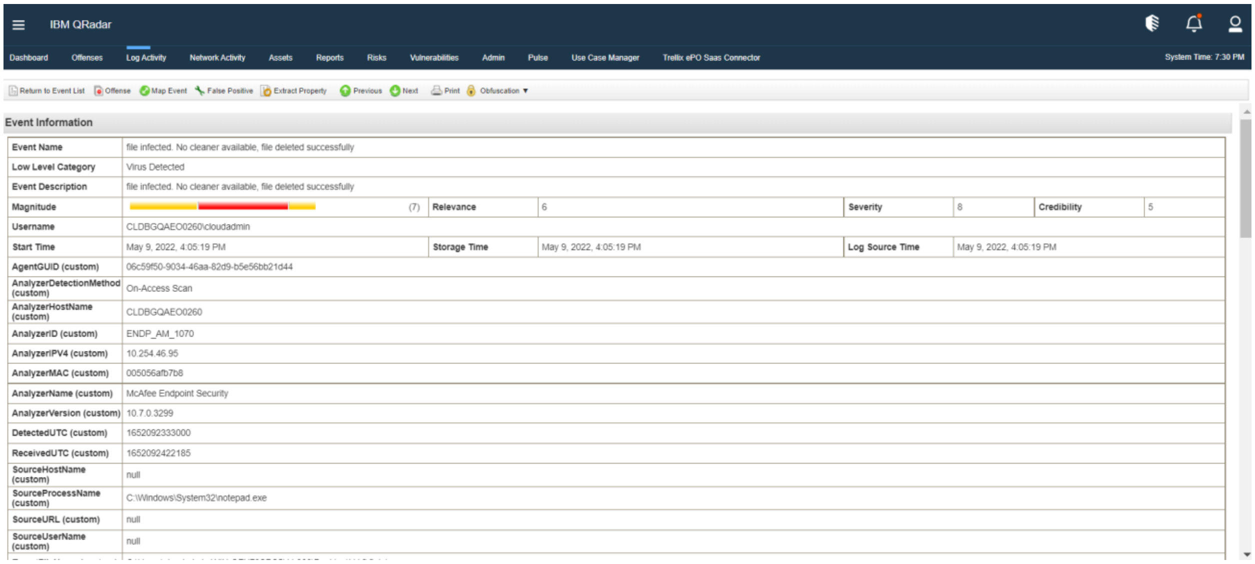
On successful poll of threat events, Admins can see events on **Log Activity** page as shown below:



Current Filters:
Log Source is Trellix ePO Saas Threat Events (Clear Filter)
▸ Current Statistics

	Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
	Infected file deleted	Trellix ePO Saas Threat Events	6	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	CLDBGQAE...	🟨🟥🟨
	Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	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 PM	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 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	CLDBGQAE...	🟨🟥🟨
	Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	CLDBGQAE...	🟨🟥🟨
	Infected file deleted	Trellix ePO Saas Threat Events	1	May 9, 2022, 4:05:19 PM	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, 3:05:20 PM	Virus Detected	10.254.46.95	0	10.254.46.95	0	CLDBGQAE...	🟨🟥🟨

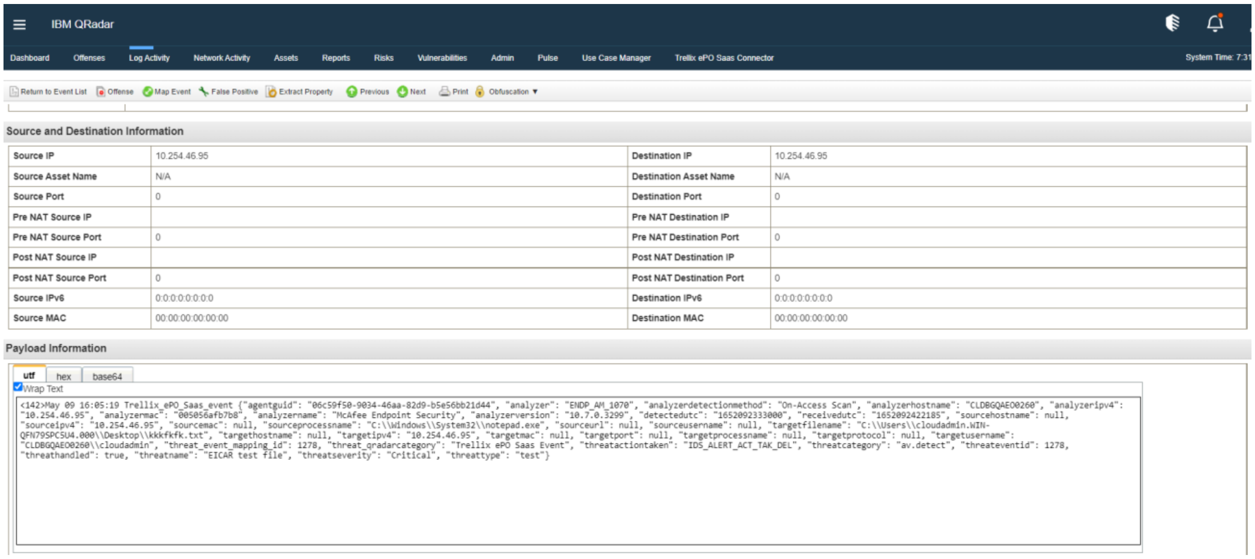
Event is parsed using the custom properties and DSM parser which is defined for Trellix ePO Saas Threat events as shown below:



Event Information

Event Name	file infected. No cleaner available, file deleted successfully						
Low Level Category	Virus Detected						
Event Description	file infected. No cleaner available, file deleted successfully						
Magnitude	(7)	Relevance	6	Severity	8	Credibility	5
Username	CLDBGQAEO0260\cloudadmin						
Start Time	May 9, 2022, 4:05:19 PM	Storage Time	May 9, 2022, 4:05:19 PM	Log Source Time	May 9, 2022, 4:05:19 PM		
AgentGUID (custom)	06c59f50-9034-46aa-82d9-b5e56bb21d44						
AnalyzerDetectionMethod (custom)	On-Access Scan						
AnalyzerHostName (custom)	CLDBGQAEO0260						
AnalyzerID (custom)	ENDP_AM_1070						
AnalyzerIPV4 (custom)	10.254.46.95						
AnalyzerMAC (custom)	005056afb7b8						
AnalyzerName (custom)	McAfee Endpoint Security						
AnalyzerVersion (custom)	10.7.0.3299						
DetectedUTC (custom)	1652092333000						
ReceivedUTC (custom)	1652092422185						
SourceHostName (custom)	null						
SourceProcessName (custom)	C:\Windows\System32\notepad.exe						
SourceURL (custom)	null						
SourceUserName (custom)	null						

Threat Event in JSON format fetched from Trellix ePO Saas



Source and Destination Information

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	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

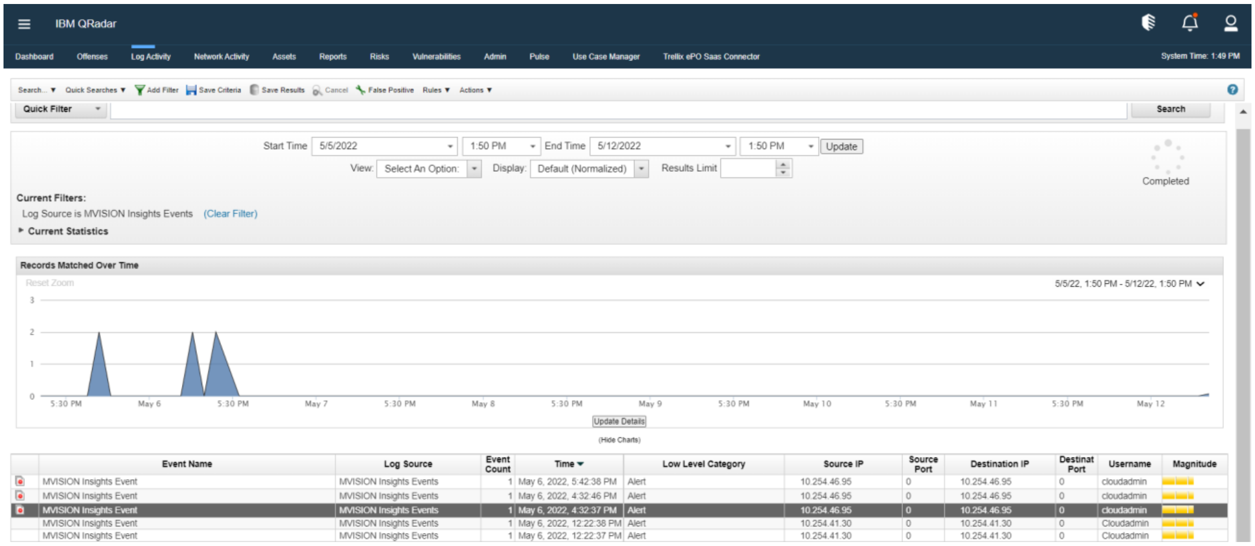
☑Wrap Text

```
<142>May 09 16:05:19 Trellix_ePO_Saas_event {"agentguid": "06c59f50-9034-46aa-82d9-b5e56bb21d44", "analyzer": "ENDP_AM_1070", "analyzerdetectionmethod": "On-Access Scan", "analyzerhostname": "CLDBGQAEO0260", "analyzeripv4":
"10.254.46.95", "analyzermac": "005056afb7b8", "analyzername": "McAfee Endpoint Security", "analyzerversion": "10.7.0.3299", "detectedutc": "1652092333000", "receivedutc": "1652092422185", "sourcehostname": null,
"sourceipv4": "10.254.46.95", "sourcemac": null, "sourceprocessname": "C:\\Windows\\System32\\notepad.exe", "sourceurl": null, "sourceusername": null, "targetfilename": "C:\\Users\\cloudadmin.WIN-
QFN79SPC5U4.000\\Desktop\\kkkfkfk.txt", "targethostname": null, "targetipv4": "10.254.46.95", "targetmac": null, "targetport": null, "targetprocessname": null, "targetprotocol": null, "targetusername":
"CLDBGQAEO0260\\cloudadmin", "threat_event_mapping_id": 1278, "threat_qradarcategory": "Trellix ePO Saas Event", "threatactiontaken": "IDS_ALERT_ACT_TAK_DEL", "threatcategory": "av.detect", "threateventid": 1278,
"threathandled": true, "threatname": "EICAR test file", "threatseverity": "Critical", "threattype": "test"}
```

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:



Start Time: 5/5/2022 1:50 PM End Time: 5/12/2022 1:50 PM

View: Select An Option: Display: Default (Normalized) Results Limit

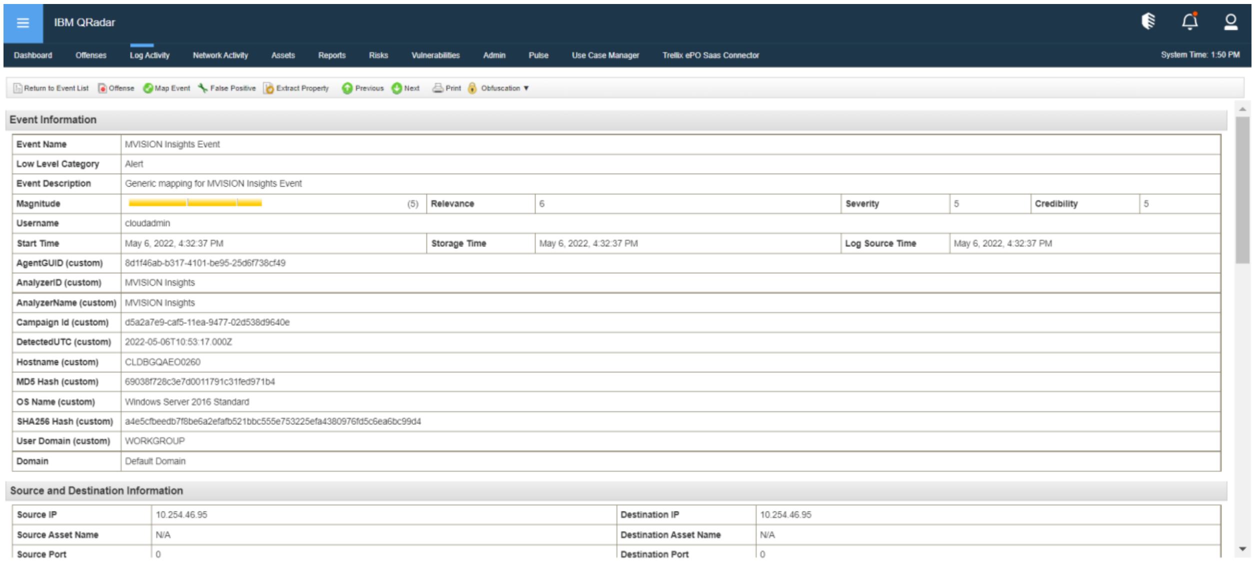
Current Filters:

Log Source is MVISION Insights Events (Clear Filter)

Current Statistics

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destinat Port	Username	Magnitude
MVISION Insights Event	MVISION Insights Events	1	May 6, 2022, 5:42:38 PM	Alert	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	Alert	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	Alert	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	Alert	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	Alert	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:



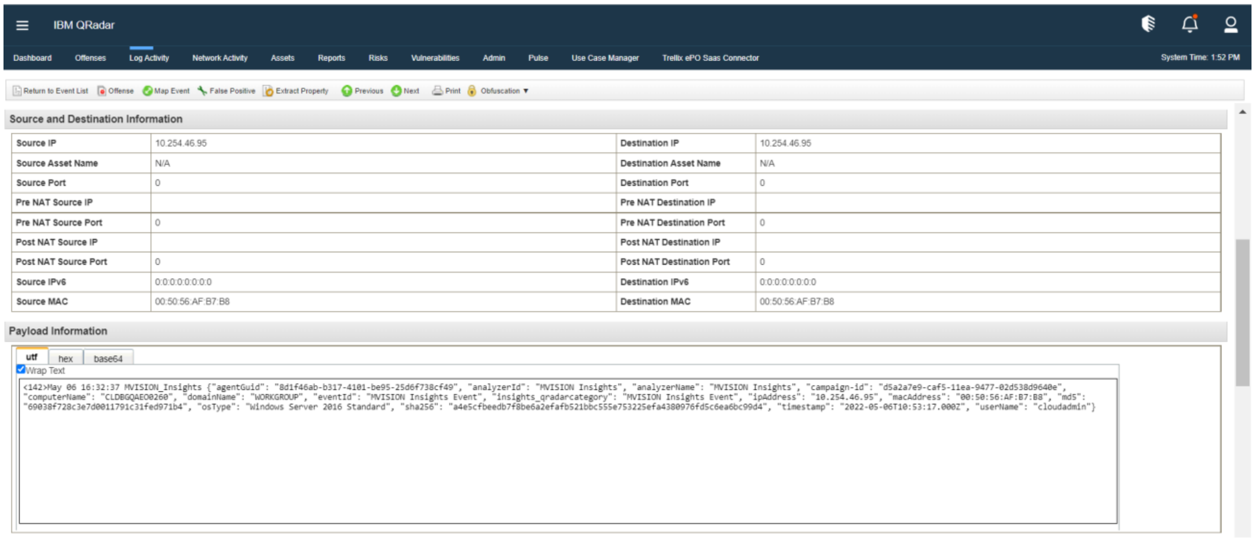
Event Information

Event Name	MVISION Insights Event						
Low Level Category	Alert						
Event Description	Generic mapping for MVISION Insights Event						
Magnitude	▬▬▬ (5)	Relevance	6	Severity	5	Credibility	5
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		
AgentGUID (custom)	8d1f46ab-b317-4101-be95-25d6f738cf49						
AnalyzerID (custom)	MVISION Insights						
AnalyzerName (custom)	MVISION Insights						
Campaign Id (custom)	d5a2a7e9-caf5-11ea-9477-02d538d9640e						
DetectedUTC (custom)	2022-05-06T10:53:17.000Z						
Hostname (custom)	CLDBGQAEO0260						
MD5 Hash (custom)	69038f728c3e7d0011791c31fed971b4						
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	Destination IP	10.254.46.95
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0

Insights Event in JSON format fetched from MVISION INSIGHTS



Source and Destination Information

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	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:50:56:AF:B7:B8	Destination MAC	00:50:56:AF:B7:B8

Payload Information

utf hex base64

☑ Wrap Text

```
<142>May 06 16:32:37 MVISION_Insights {"agentGuid": "8d1f46ab-b317-4101-be95-25d6f738cf49", "analyzerId": "MVISION Insights", "analyzerName": "MVISION Insights", "campaign-id": "d5a2a7e9-caf5-11ea-9477-02d538d9640e", "computerName": "CLDBGQAEO0260", "domainName": "WORKGROUP", "eventId": "MVISION Insights Event", "insights_qradarcategory": "MVISION Insights Event", "ipAddress": "10.254.46.95", "macAddress": "00:50:56:AF:B7:B8", "md5": "69038f728c3e7d0011791c31fed971b4", "osType": "Windows Server 2016 Standard", "sha256": "a4e5cfbeedb7f8be6a2efafb521bbc555e753225efa4380976fd5c6ea6bc99d4", "timestamp": "2022-05-06T10:53:17.000Z", "userName": "cloudadmin"}
```

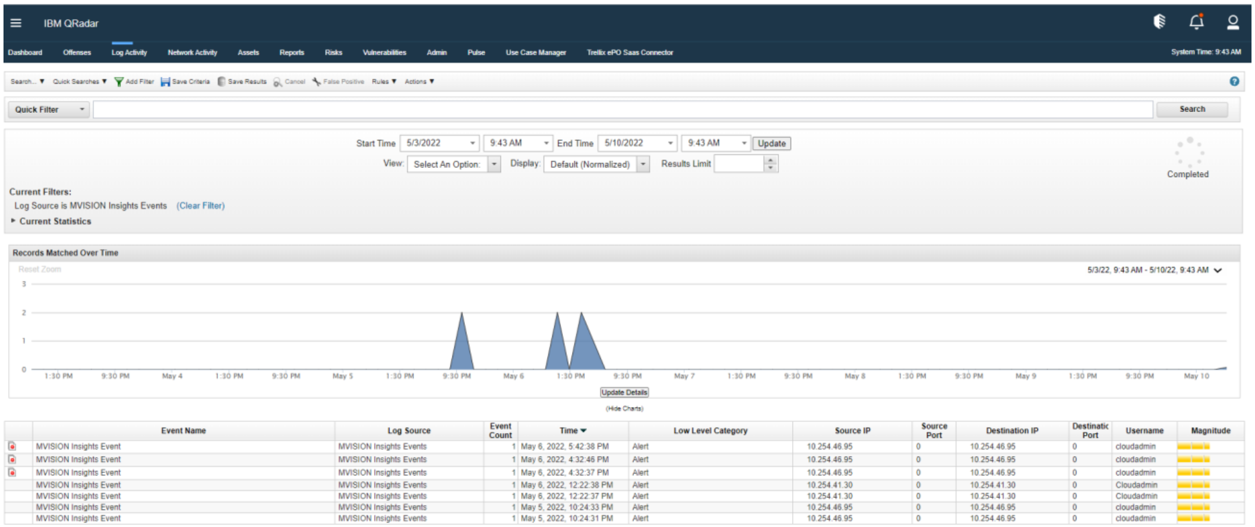
Note: All MVISION Insights events will have the following mapping:

Event Name	MVISION Insights Events
Low Level Category	Alert

MVISION Insights

MVISION Insights provides actionable and preemptive threat intelligence by leveraging Trellix cutting-edge 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.



Start Time 5/3/2022 9:43 AM End Time 5/10/2022 9:43 AM

View: Select An Option: Display: Default (Normalized) Results Limit

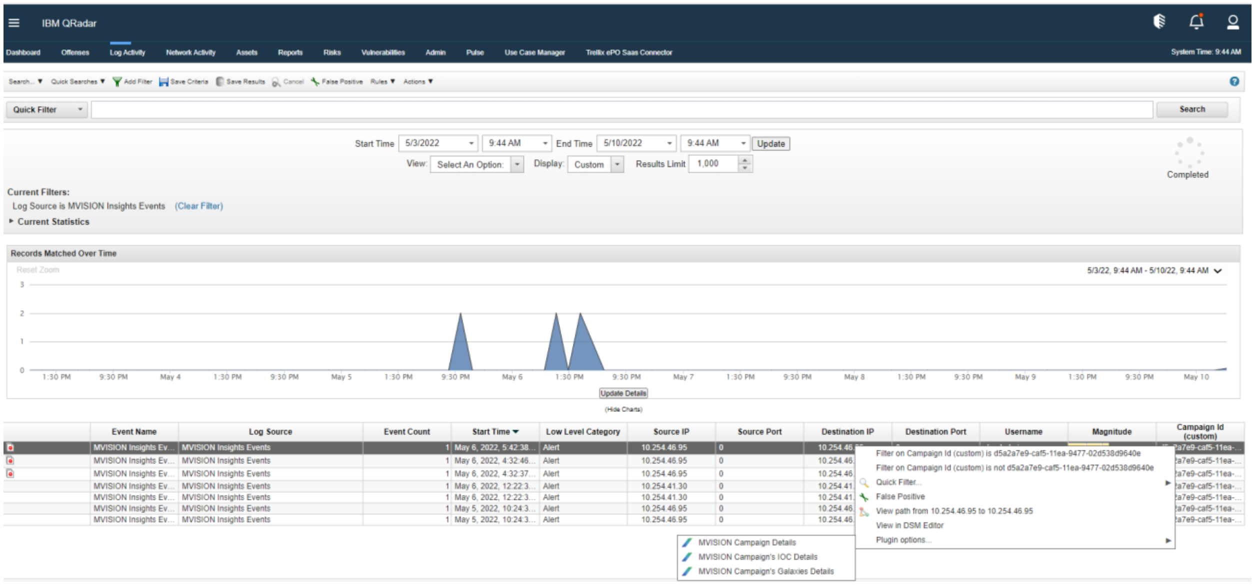
Current Filters:
Log Source is MVISION Insights Events (Clear Filter)

▸ Current Statistics

	Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source IP	Source Port	Destination IP	Destinatic Port	Username	Magnitude
●	MVISION Insights Event	MVISION Insights Events	1	May 6, 2022, 5:42:38 PM	Alert	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	Alert	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	Alert	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	Alert	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	Alert	10.254.41.30	0	10.254.41.30	0	Cloudadmin	▬▬▬
	MVISION Insights Event	MVISION Insights Events	1	May 5, 2022, 10:24:33 PM	Alert	10.254.46.95	0	10.254.46.95	0	cloudadmin	▬▬▬
	MVISION Insights Event	MVISION Insights Events	1	May 5, 2022, 10:24:31 PM	Alert	10.254.46.95	0	10.254.46.95	0	cloudadmin	▬▬▬

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



Start Time 5/3/2022 9:44 AM End Time 5/10/2022 9:44 AM

View: Select An Option: Display: Custom Results Limit 1,000

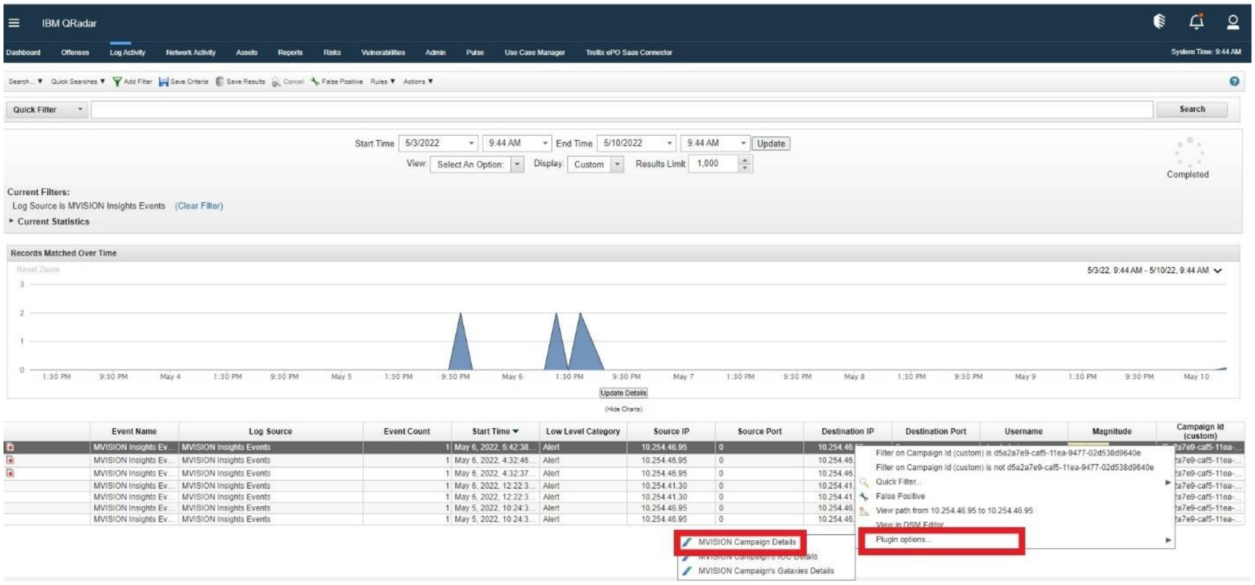
Current Filters:
Log Source is MVISION Insights Events (Clear Filter)
▸ Current Statistics

	Event Name	Log Source	Event Count	Start Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	Campaign Id (custom)
	MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 5:42:38...	Alert	10.254.46.95	0	10.254.46.				a7e9-caf5-11ea-...
	MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 4:32:46...	Alert	10.254.46.95	0	10.254.46.				a7e9-caf5-11ea-...
	MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 4:32:37...	Alert	10.254.46.95	0	10.254.46.				a7e9-caf5-11ea-...
	MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 12:22:3...	Alert	10.254.41.30	0	10.254.41.				a7e9-caf5-11ea-...
	MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 12:22:3...	Alert	10.254.41.30	0	10.254.41.				a7e9-caf5-11ea-...
	MVISION Insights Ev...	MVISION Insights Events	1	May 5, 2022, 10:24:3...	Alert	10.254.46.95	0	10.254.46.				a7e9-caf5-11ea-...
	MVISION Insights Ev...	MVISION Insights Events	1	May 5, 2022, 10:24:3...	Alert	10.254.46.95	0	10.254.46.				a7e9-caf5-11ea-...

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.



Start Time 5/3/2022 9:44 AM End Time 5/10/2022 9:44 AM

View: Select An Option: Display: Custom Results Limit 1,000

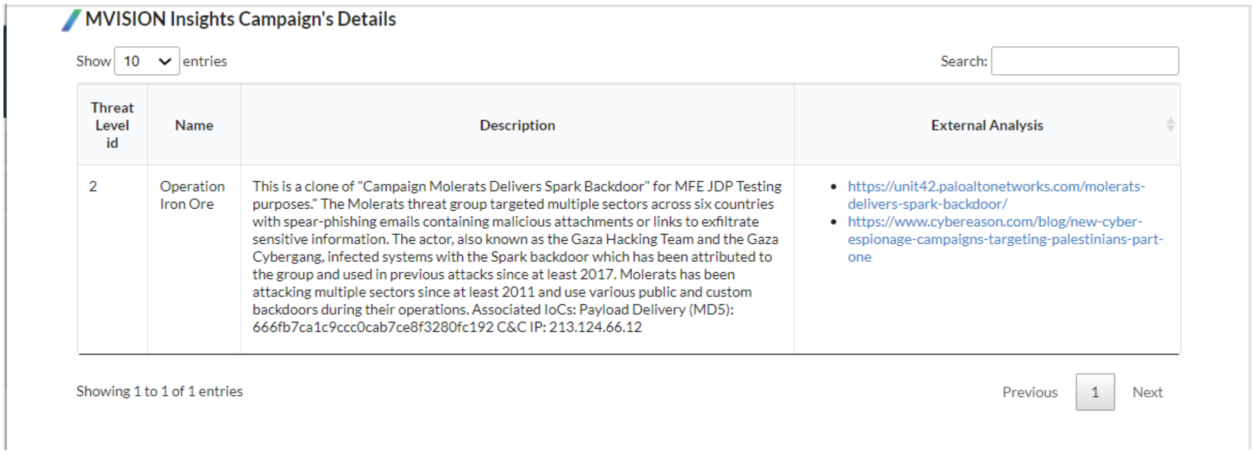
Current Filters:

Log Source is MVISION Insights Events (Clear Filter)

▸ **Current Statistics**

Event Name	Log Source	Event Count	Start Time ▾	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	Campaign Id (custom)
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 5:42:38...	Alert	10.254.46.95	0	10.254.46				a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 4:32:46...	Alert	10.254.46.95	0	10.254.46				a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 4:32:37...	Alert	10.254.46.95	0	10.254.46				a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 12:22:3...	Alert	10.254.41.30	0	10.254.41				a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 12:22:3...	Alert	10.254.41.30	0	10.254.41				a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 5, 2022, 10:24:3...	Alert	10.254.46.95	0	10.254.46				a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 5, 2022, 10:24:3...	Alert	10.254.46.95	0	10.254.46				a7e9-caf5-11ea-...

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



MVISION Insights Campaign's Details

Show 10 entries Search:

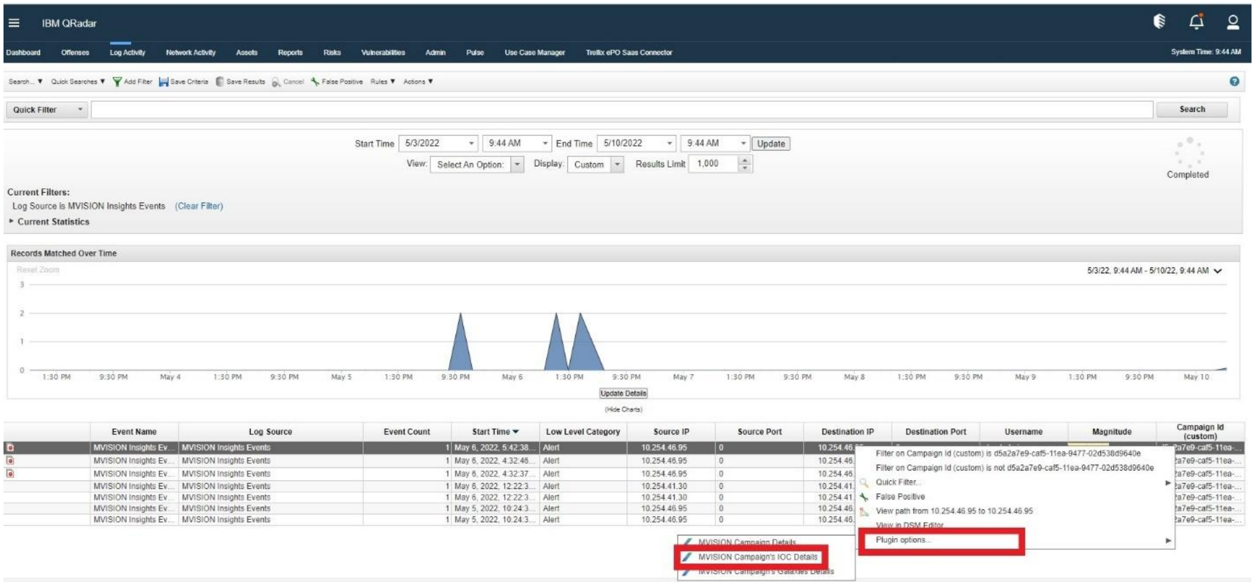
Threat Level id	Name	Description	External Analysis
2	Operation Iron Ore	This is a clone of "Campaign Molerats Delivers Spark Backdoor" for MFE JDP Testing purposes." The Molerats threat group targeted multiple sectors across six countries with spear-phishing emails containing malicious attachments or 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

Showing 1 to 1 of 1 entries

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.



Start Time 5/3/2022 9:44 AM End Time 5/10/2022 9:44 AM

View: Select An Option: Display: Custom Results Limit 1,000

Current Filters:

Log Source is MVISION Insights Events (Clear Filter)

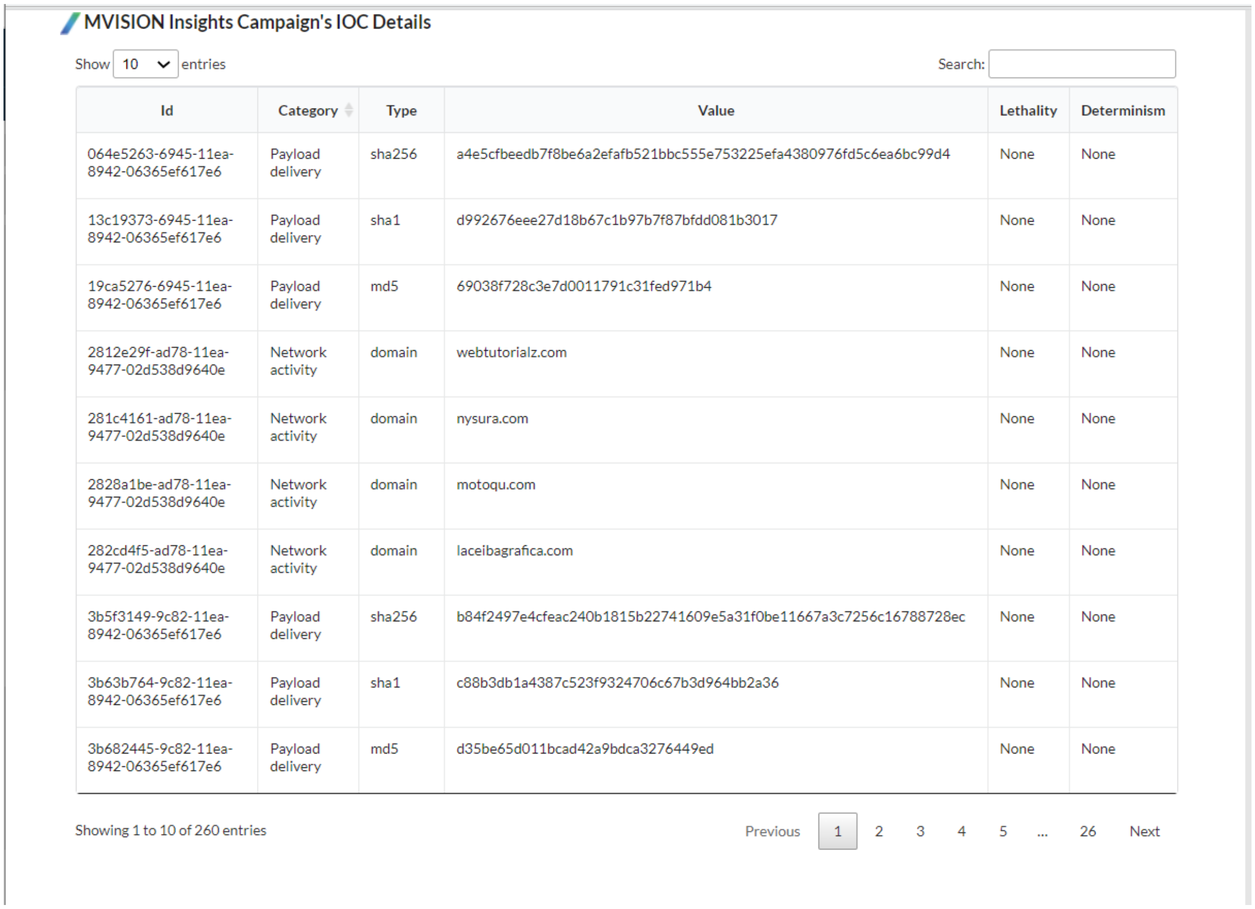
▸ Current Statistics

Records Matched Over Time

5/3/22, 9:44 AM - 5/10/22, 9:44 AM

Event Name	Log Source	Event Count	Start Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	Campaign Id (custom)
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 5:42:38...	Alert	10.254.46.95	0	10.254.46.				a2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 4:32:46...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 4:32:37...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 12:22:3...	Alert	10.254.41.30	0	10.254.41.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 12:22:3...	Alert	10.254.41.30	0	10.254.41.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 5, 2022, 10:24:3...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 5, 2022, 10:24:3...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...

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



MVISION Insights Campaign's IOC Details

Show 10 entries Search:

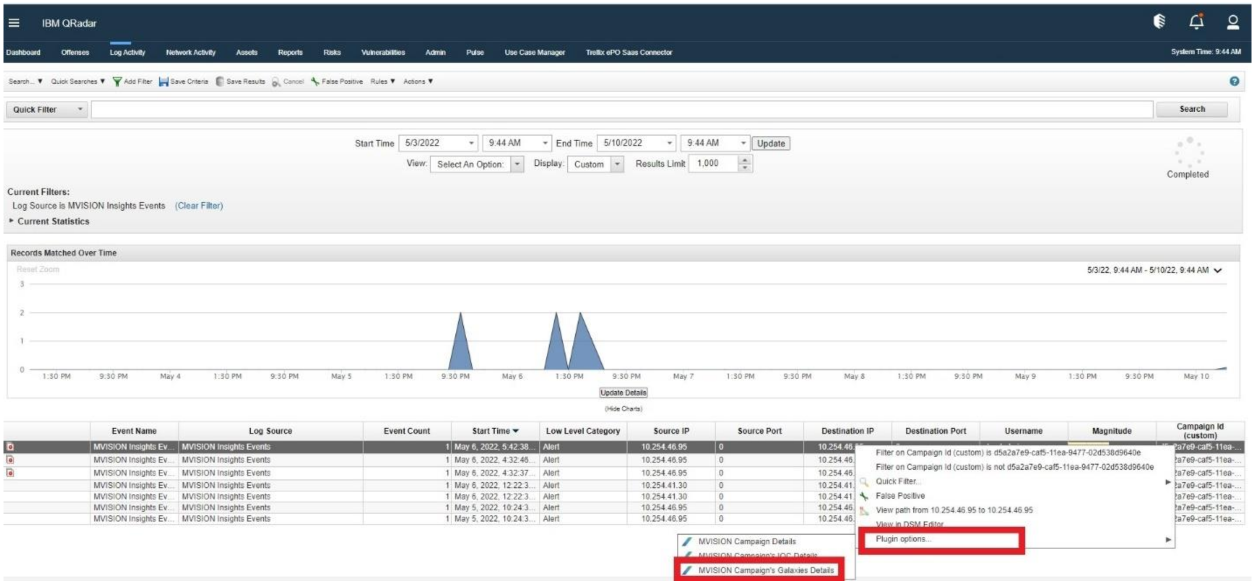
Id	Category	Type	Value	Lethality	Determinism
064e5263-6945-11ea-8942-06365ef617e6	Payload delivery	sha256	a4e5cfbeedb7f8be6a2efafb521bbc555e753225efa4380976fd5c6ea6bc99d4	None	None
13c19373-6945-11ea-8942-06365ef617e6	Payload delivery	sha1	d992676eee27d18b67c1b97b7f87bfdd081b3017	None	None
19ca5276-6945-11ea-8942-06365ef617e6	Payload delivery	md5	69038f728c3e7d0011791c31fed971b4	None	None
2812e29f-ad78-11ea-9477-02d538d9640e	Network activity	domain	webtutorialz.com	None	None
281c4161-ad78-11ea-9477-02d538d9640e	Network activity	domain	nysura.com	None	None
2828a1be-ad78-11ea-9477-02d538d9640e	Network activity	domain	motoqu.com	None	None
282cd4f5-ad78-11ea-9477-02d538d9640e	Network activity	domain	laceibagrafica.com	None	None
3b5f3149-9c82-11ea-8942-06365ef617e6	Payload delivery	sha256	b84f2497e4cfeac240b1815b22741609e5a31f0be11667a3c7256c16788728ec	None	None
3b63b764-9c82-11ea-8942-06365ef617e6	Payload delivery	sha1	c88b3db1a4387c523f9324706c67b3d964bb2a36	None	None
3b682445-9c82-11ea-8942-06365ef617e6	Payload delivery	md5	d35be65d011bcad42a9bdca3276449ed	None	None

Showing 1 to 10 of 260 entries

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.



Start Time 5/3/2022 9:44 AM End Time 5/10/2022 9:44 AM

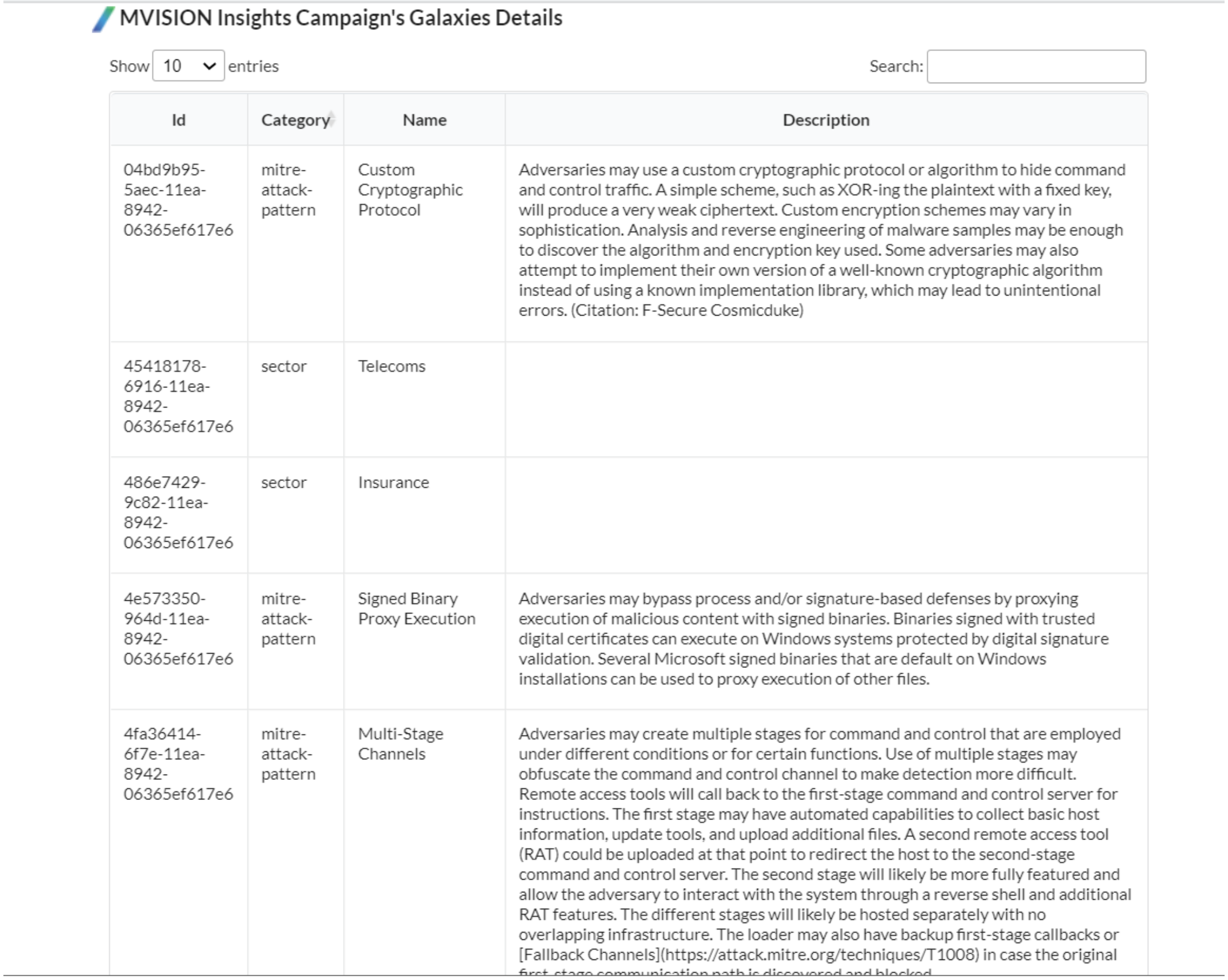
View: Select An Option: Display: Custom Results Limit 1,000

Current Filters:
Log Source is MVISION Insights Events (Clear Filter)

▸ Current Statistics

Event Name	Log Source	Event Count	Start Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude	Campaign Id (custom)
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 5:42:38...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 4:32:46...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 4:32:37...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 12:22:3...	Alert	10.254.41.30	0	10.254.41.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 6, 2022, 12:22:3...	Alert	10.254.41.30	0	10.254.41.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 5, 2022, 10:24:3...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...
MVISION Insights Ev...	MVISION Insights Events	1	May 5, 2022, 10:24:3...	Alert	10.254.46.95	0	10.254.46.				2a7e9-caf5-11ea-...

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

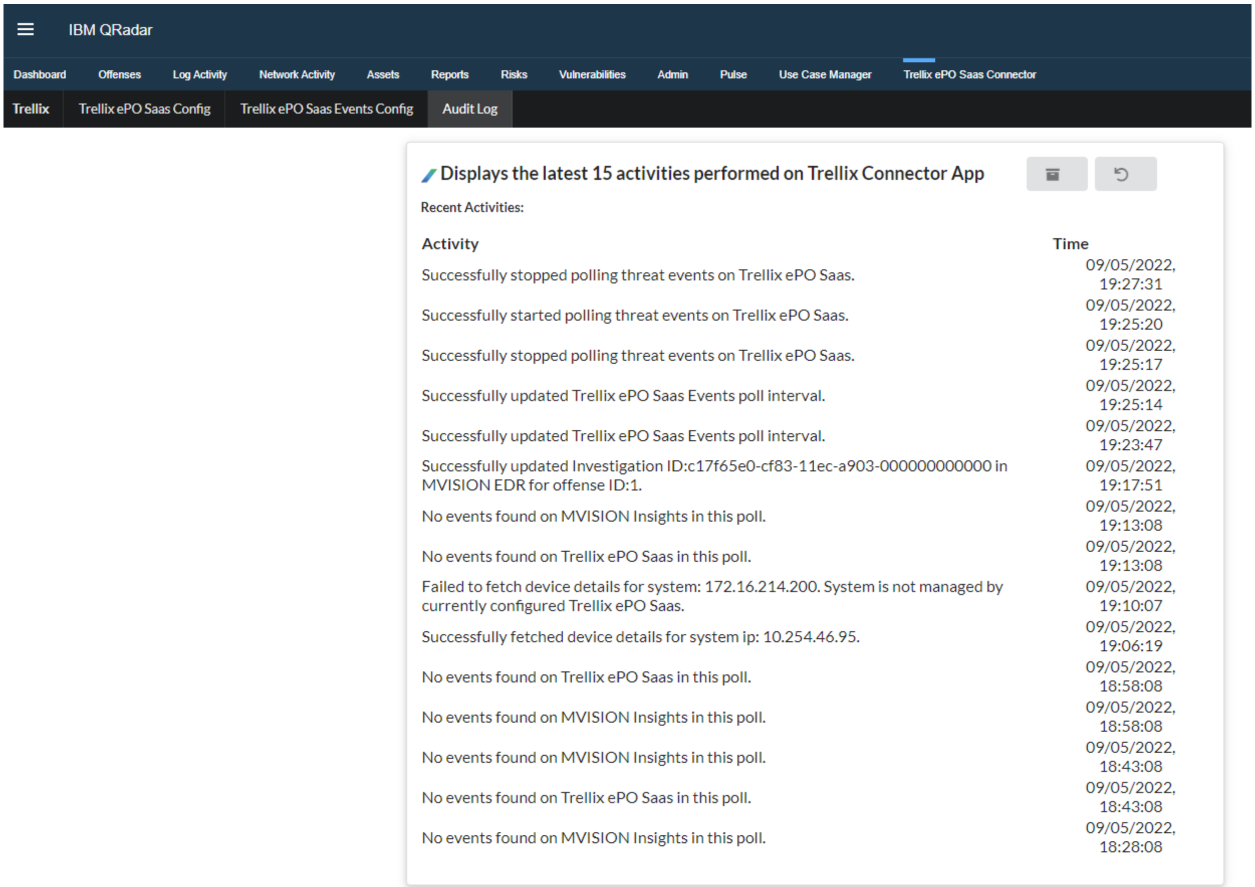


MVISION Insights Campaign's Galaxies Details

Id	Category	Name	Description
04bd9b95-5aec-11ea-8942-06365ef617e6	mitre-attack-pattern	Custom Cryptographic Protocol	Adversaries may use a custom cryptographic protocol or algorithm to hide command 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 enough 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-8942-06365ef617e6	sector	Insurance	
4e573350-964d-11ea-8942-06365ef617e6	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.
4fa36414-6f7e-11ea-8942-06365ef617e6	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 additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

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:



Displays the latest 15 activities performed on Trellix Connector App

Recent Activities:

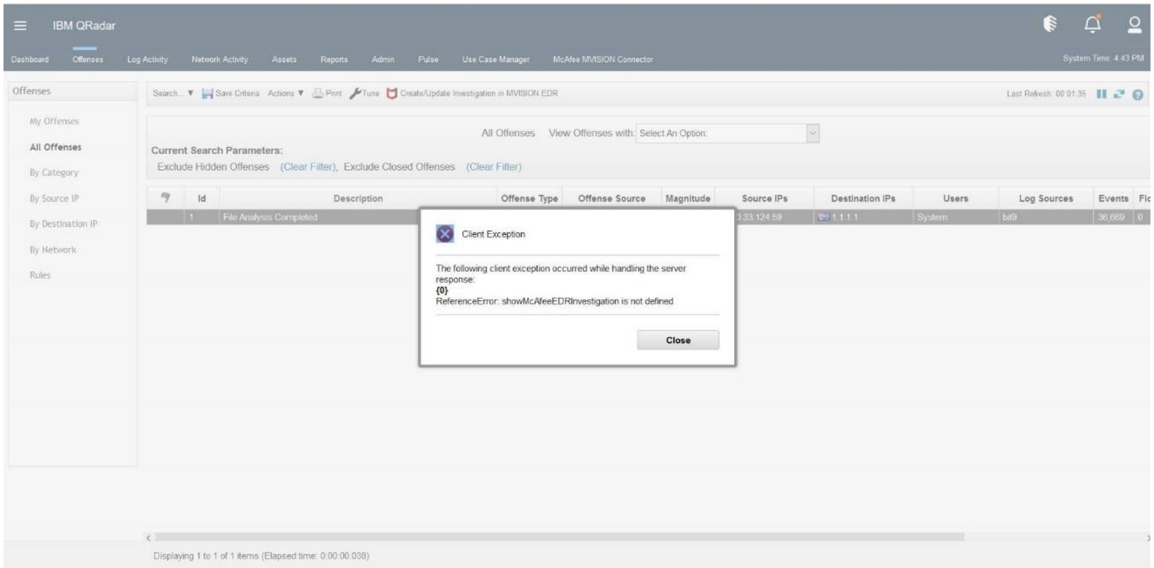
Activity	Time
Successfully stopped polling threat events on Trellix ePO Saas.	09/05/2022, 19:27:31
Successfully started polling threat events on Trellix ePO Saas.	09/05/2022, 19:25:20
Successfully stopped polling threat events on Trellix ePO Saas.	09/05/2022, 19:25:17
Successfully updated Trellix ePO Saas Events poll interval.	09/05/2022, 19:25:14
Successfully updated Trellix ePO Saas Events poll interval.	09/05/2022, 19:23:47
Successfully updated Investigation ID:c17f65e0-cf83-11ec-a903-000000000000 in MVISION EDR for offense ID:1.	09/05/2022, 19:17:51
No events found on MVISION Insights in this poll.	09/05/2022, 19:13:08
No events found on Trellix ePO Saas in this poll.	09/05/2022, 19:13:08
Failed to fetch device details for system: 172.16.214.200. System is not managed by currently configured Trellix ePO Saas.	09/05/2022, 19:10:07
Successfully fetched device details for system ip: 10.254.46.95.	09/05/2022, 19:06:19
No events found on Trellix ePO Saas in this poll.	09/05/2022, 18:58:08
No events found on MVISION Insights in this poll.	09/05/2022, 18:58:08
No events found on MVISION Insights in this poll.	09/05/2022, 18:43:08
No events found on Trellix ePO Saas in this poll.	09/05/2022, 18:43:08
No events found on MVISION Insights in this poll.	09/05/2022, 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.



Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources	Events	Flo
1	File Analysis Completed				33.124.59	1.1.1.1	System	bit9	36,669	0

Client Exception

The following client exception occurred while handling the server response:
{0}
ReferenceError: showMcAfeeEDRInvestigation is not defined

Displaying 1 to 1 of 1 items (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.