# IntSights App for QRadar v7.4.3 GA+

App Specification Guide

# Table of Contents

Table of Contents	2
App functionality	4
IOC/Alert Data Collection	4
IOC Correlation	4
Whitelist IOC	4
Enrich IntSights Platform	4
Investigate IOC	4
Correlation Alerts	4
App Installation & Configuration	5
Prerequisites	5
Upgrade	5
v.2.0.0	5
v.1.2.0	5
v.1.1.0	5
v.1.0.2	5
v.1.0.1	5
Installation	6
App Configuration	8
Uninstalling the Application	11
Steps to check application logs	11
Steps to generate the Authorization token on QRoC	12
Access application docker	12
Configuring app for correlation	14
Steps to enable rules	14
Steps for changing selected property of rules	14
Creating rules	15
Configuring app for generating alert on correlation	20
Configuring Email Server	20
Creating custom email template for IntSights Correlation e-mail	21
Adding email templates to Rules	22
Adding filter in Rules	24
Adding new field in Email	26
Whitelisting	27
Whitelisting an IOC	27
Retiring of data in reference set	28
Changing Time to Leave	28
Dashboard	29
IOC Overview	29
Correlation Overview	31
Correlation Details	32
Alert Overview	33

Alert Details	36
Email XML Template	37
XML Template for Email	37
Release notes	39
v2.0.0	39
v1.2.0	39
v1.1.0	39
v1.0.2	39
v1.0.1	39
Troubleshooting	39
Case #1 – App configuration fails with various error messages	39
Case #2 – UI related issues in the app	41
Case #3 – Error while initiating socket connection with IBM QRadar,	
while using QRadar v7.5.0 UP4 with encrypted Apphost deployment	41
Case #4 – Error while initiating socket connection with IBM QRadar	42
Case #5 – Events are parsed as Unknown or IntSights Message	42
Case #6 – IntSights events are shown up as "IntSights Message"	43
Case #7 – Internal Server Error while opening configuration page	44
Case #8 – All other issues which are not a part of the Document	44

# App functionality

### **IOC/Alert Data Collection**

QRadar admin/user can collect the information regarding IOCs and alerts from IntSights and ingest into QRadar as events by configuring the inputs from Input Config page of IntSights App for QRadar.

### **IOC Correlation**

QRadar will monitor all the incoming events and if any of those events have IOCs that are fetched from IntSights then it will correlate it and provide alerts to the user.

### Whitelist IOC

QRadar admin/user would be able to mark IOCs as whitelisted for false-positives or excluding certain IOCs. IOCs whitelisted for the configured account from any other app/platform will also be whitelisted and removed from the IntSights App for QRadar.

### **Enrich IntSights Platform**

The IntSights App for QRadar will add tags and comments to the IOC values that get matched with any of the QRadar events.

### **Investigate IOC**

QRadar admin/user can get enriched information about a correlated IOC value from IntSights.

### **Correlation Alerts**

QRadar admin/user will be able to get alerts as QRadar notification and emails whenever any of the users' QRadar events gets correlated with IOCs fetched from IntSights.

# App Installation & Configuration

# Prerequisites

Below is a list of requirements needed to run the app (v2.0.0) on QRadar:

- IntSights App for QRadar (v2.0.0)
- QRadar version: 7.4.3 GA+
- IntSights account credentials with IOC & Discovery module enabled.

# Upgrade

### v.2.0.0

- *NOTE:* Users will be able to upgrade from v1.x.x to v2.0.0 only if the app is installed on QRadar v7.4.3 GA+.
- Follow the same steps for Installation.
- Clear the browser cache and refresh the QRadar page.

### v.1.2.0

- Follow the same steps for <u>Installation</u>.
- Clear the browser cache and refresh the QRadar page.

### v.1.1.0

- Follow the same steps for Installation.
- Clear the browser cache and refresh the QRadar page.

### v.1.0.2

• Before upgrading the IntSight App make sure that you don't have <u>IoC Type</u> and <u>IoC</u> <u>Value</u> CEPs in the QRadar instance.

### Steps to delete Custom Event Properties:

- 1. Navigate to Custom Event Properties via the Admin panel.
- 2. In the search box enter the keyword "IntSights".
- 3. Select the custom property named "loC Type". Verify that the associated log source type is IntSights and click on the delete button.
- 4. Repeat the above step for property "IoC Value".
- 5. Go to the Admin Panel and click on Deploy Changes.
- After deleting CEPs successfully, Follow the same steps for Installation.
- Clear the browser cache and refresh the QRadar page.

### v.1.0.1

- *NOTE:* Users will be able to upgrade from v1.0.0 to v1.0.1 only if the app is installed on QRadar v7.4.1 FP2+ (app framework V2).
- Follow the same steps for Installation
- Clear the browser cache and refresh the QRadar page.

### Installation

The application installation requires access to the QRadar console machine via a web interface. The web interface can be accessed via <u>https://<<QRadarconsoleIP>>/</u>. The installation process is as follows: a. Login to QRadar console.

IBM QRadar Secure the Cloud Lucrans Lucrans Lucrans Lucrans Lucrans Lucrans

Figure 1: IBM QRadar login screen

- b. Go to Admin  $\rightarrow$  Extension Management.
- c. Click on Add button then choose the downloaded zip file by clicking on **Browse** and then, click **Add**.

Extensions Management	Search by extension name	Q		IBM Security App Exchange
ALL ITEMS INSTALLED NOT INSTALL	ED			Add
Name		Status	Author	Added On 🔻
QRadar Use Case Manager - QRadar 7.3.3 FP6+/7.4	.1 FP2+	Installed	IBM QRadar	July 5, 2023
QRadar Assistant - QRadar 7.3.3 FP6+/7.4.1 FP2+		Installed	IBM QRadar	July 5, 2023
IBM QRadar Baseline Maintenance Content Exte	Add a New Extension		IBM QRadar	July 5, 2023
IBM QRadar Baseline Maintenance Content Exte	From local storage: IntSightsAppForQradar.zip	Browse	IBM QRadar	July 5, 2023
QRadar Log Source Management	Install immediately		IBM QRadar	July 5, 2023
L	Add	Cancel		
4 Total: 8	4 <b>1</b> 5			10   25   50   All ♦

Figure 2: Add IntSights App for QRadar extension

d. QRadar will prompt a list of changes being made by the app. Click on the install button.

IntSights App For QRadar - QRadar v7.4.3 GA+ By: IntSights The extension contains 22 items which are already on the system and marked the versions in the extension that you are about to install, or you can preserve d Application items that are marked with REPLACE are upgraded but internal dat to system Custom Rule items are preserved. Any other item types marked with will be lost. How would you like to proceed? © Replace existing items. (Application data is preserved) © Preserve existing items. (Not recommended for applications)	with REPLACE. You can replace these items with existing items as-is and add only new items. Is and configuration is preserved. Customizations REPLACE will be replaced and customizations
By installing this extension, the following changes will occur in the system:	
Log Source Extensions (1)	A
IntSightsCustom_ext	REPLACE
Log Source Types (1)	
IntSights	REPLACE
QID Records (3)	
IntSights IOC	REPLACE
IntSights Correlated Event	REPLACE
IntSights Alert	REPLACE
Custom Extraction Properties (34)	
IOC Value	ADD
Start a default instance of each app 1	Install Cancel

#### Figure 3: Install IntSights app for QRadar

- e. Thereafter, it will show a window that the App is installed successfully along with lists of different components of the App.
- f. Clear the cache and refresh the browser window.
- g. Navigate to Extensions Management via the Admin panel. After successful installation, it will show "Installed" status against "IntSights App For QRadar".

Extensions Management	Search by extension name	Q	IBM	Security App Exchange
ALL ITEMS INSTALLED NOT INSTALLED				Add
Name		Status	Author	Added On
IntSights App For QRadar - QRadar v7.4 The IntSights App arms QRadar users with curated externa prioritize, and respond to security incidents with ease and c data enrichment, SOC analysts can perform real-time threa within their QRadar device.	* .3 GA+ I threat intelligence as they detect, onfidence. Leveraging bi-directional t correlation and analysis—all from (More Details)	Installed	IntSights	July 25, 2023
QRadar Use Case Manager		Installed	IBM QRadar	July 17, 2023
QRadar Assistant App		Installed	IBM QRadar	July 17, 2023
IBM QRadar Baseline Maintenance Content Extension v7.3.3	P4+	Installed	IBM QRadar	July 17, 2023
QRadar Log Source Management		Installed	IBM QRadar	July 17, 2023

Figure 4: Installation successful

### App Configuration

After completing the installation, users have to complete the configuration to use IntSights App functionality.

The setup process for configuring the app is as follows:

• Find the installed app on the Admin Panel under Apps as shown in the figure.

≡ IBM QRadar		(II)	Ċ	<u> </u>
Dashboard Offenses L	Log Activity Network Activity Assets Reports Risks Valmerabilities Admin	Sj	rstern Time: I	6:48 PM
Admin	🕲 Deploy Changes Advanced 🔻			0
System Configuration	😵 Checking for undeployed changes			
Data Sources	Apps			
P Data Sources	Risk Manager			
Remote Networks and Services Configuration	4. 4.			
Try it out	Configuration Source Device Import Management			
► Apps				
	QRadar Log Source Management			
	ul,			
	QRadar Log Source Management			
	QRadar App Editor			
	uk.			
	Develop Applications			
				- 1
	IntSights App for QRadar			- 1
	©			
	IntSights App for QRadar			
	Contiguration Page			-

Figure 5: Installed app's configuration page

• Click on the "IntSights App For QRadar Configuration Page", the configuration page will open as shown in the figure below.

Account Config	Input Config		
			Add IntSights Account
		No account configured.	

*Figure 6: IntSights app configuration page* 

• Configure IntSights Account in the "Account Config" tab and IOC/Alert related configurations from the "Input Config" tab. After configuring both tabs successfully, it will start collecting IOC and alert data.

### Configure IntSights Account configuration:

- For the "Account Config" tab, enter all the details related to the IntSights account. Enter proxy configuration, if needed.
   Note: Users will not be able to configure the inputs until an IntSights account is configured. Also, users would not be able to delete a configured IntSights account, until all inputs are disabled.
- For the field "Protocol", User can specify the transfer protocol to forward collected events to QRadar instance. By default, TCP protocol would be considered.
- For the field "Authorized Service Token" value first go to the Admin panel and then select "Authorized Services" in the User Management section. When the window opens, there should be one default service there, if not use this link to make an authorized service (Note: The created token should have "User Role" and "Security Profile" as Admin). Then, select a token from there and copy it, paste it into the "Account Config" page.

- For creating authorization tokens on QRoC follow steps mentioned below <u>Steps to</u> <u>generate the Authorization token on QRoC</u>
- The user is also provided with an option to enable/disable the functionality of adding tags and comments to IntSights platform for matched IOCs. By default, the functionality is enabled. If a user wishes to not enrich IntSights platform with tags and comments for matched IOCs, they can uncheck the checkbox "Add IOC tags and comments" in the Account Config tab.
- Saved account configurations would be stored in "config.conf" file.

#### **Configure IOC input configuration:**

- The default value for IOC input configuration should be as follows:
  - o All the IOC types should be unchecked for "Enable".
  - Fetch Retired IOCs should be enabled for all the IOC Types.
  - Interval time should be 14400 seconds.
  - IOC Severity should be Medium and High.
  - Reporting Feeds should be All.
  - Start Time for the IOC type are as follows:
    - IP Address: Last 14 days
    - URL, Email Address: Last 60 days
    - Domain, File Hash: Last 90 days
- The "Fetch Retired IOCs", if set to enabled will collect all the IOCs from IntSights, whereas if set to disabled, it won't add retired indicators to the QRadar instance and will remove IOCs that are retired after being ingested into QRadar.
- The "IOC Severity" and "Reporting Feeds" fields are multi-select dropdowns, so users would be able to select multiple values.
   Note: If "All" value is selected for either of the mentioned fields, even with other selected values, then the data would be collected for "All" values, ignoring the other selected values.
- For the "Start Time" field, users would not be able to select a time earlier than six months or a future time.
- After modifying the fields for desired IOC Types on the Input Config page, click on the "Enable" checkbox and save the input configurations.
- After the successful configuration of IntSights account and IOC input, background process will start fetching IOC data from the IntSights and will be ingested in the Log activity and Reference sets.
- Saved IOC input configurations would be stored in "inputs.conf" file.
- To enable the correlation feature, follow the steps mentioned under "<u>Configuring app</u> for correlation feature".

### Configure Alert input configuration:

- The default value for Alert input configuration should be as follows:
  - All the Alert types should be unchecked for "Enable".
  - Alert Status should be "Open".
  - Interval time should be 14400 seconds.
  - Alert Severity should be All.
  - Report Date should be "Last 30 Days".
- The "Alert Severity" field is a multi-select dropdown, so users would be able to select multiple values.

**Note:** If "All" value is selected, even with other selected values, then the data would be collected for "All" values, ignoring the other selected values.

- For "Alert Status" field, users would be able to select either "Open" or "Closed" status value.
- After modifying the fields for desired Alert types on the Input Config page, click on the "Enable" checkbox and save the input configurations.
- After successful configuration of IntSights account and Alert input, background process will start fetching Alert data from the IntSights and will ingest it in the Log activity.
- Saved alert input configurations would be stored in "alerts.conf" file.

# Uninstalling the Application

To uninstall the application, the user needs to perform the following steps.

- 1. Go to the Admin Page.
- 2. Open Extension Management.
- 3. Select IntSights App For QRadar application.
- 4. Click on Uninstall.

NOTE:

- On uninstalling the app, all the Custom Event Properties, and Dashboards will be removed.
- On uninstalling the app, only the log sources which are provided in the bundle will get uninstalled (i.e. IntSights Log Source).
- On uninstalling the app, removal of reference sets, Log source type, Log source extension, DSM event mappings (including QIDs) is not supported by QRadar yet.
- To remove IntSights App for QRadar's reference sets, navigate to Admin -> Reference Set Management -> Select reference sets with below name one-by-one:
  - IntSights\_IOC\_IpAddresses
  - IntSights\_IOC\_Domains
  - IntSights\_IOC\_Hashes
  - IntSights\_IOC\_Emails
  - IntSights\_IOC\_Urls

and then click "Delete". A prompt will open up, click the "Delete" button. (Note: Make sure no rules are associated with the reference set, if there is any rule which is using the reference set then we need to first delete that rule inorder to delete the reference set.)

- To remove IntSights App for QRadar's event mappings, navigate to Admin -> DSM Editor -> Select the "IntSights" log source type and click the "Select" button -> "Event Mappings" tab -> Select each event mapping and click the delete icon.
- To remove IntSights App for QRadar's log source type, navigate to Admin -> DSM Editor -> Select the log source type to be deleted in the pop-up menu in this case "IntSights", and click on the delete icon.

### **Steps to check application logs**

Users can go inside the application docker container. In the docker container user can see logs.

- Follow the steps for accessing the docker container of the IntSights App. <u>"Access application docker"</u>
- cd /opt/app-root/store/log (For navigating to log directory)
- Is (For getting list of all logs files)

<b>F</b> ile	Description
File	Description

app.log	Contains logs of configuration page and all the Dashboards(except IOC Overview dashboard), Manual Whitelisting, Investigate
<ul> <li>indicators_data_collection.log</li> <li>ioc_lpAddresses_data_collection.log</li> <li>ioc_Domains_data_collection.log</li> <li>ioc_Emails_data_collection.log</li> <li>ioc_Hashes_data_collection.log</li> <li>ioc_Urls_data_collection.log</li> </ul>	Logs for data collection of IOCs from IntSights
<ul> <li>alerts_data_collection.log</li> <li>alert_AttackIndication_data_collection.log</li> <li>alert_DataLeakage_data_collection.log</li> <li>alert_Phishing_data_collection.log</li> <li>alert_BrandSecurity_data_collection.log</li> <li>alert_ExploitableData_data_collection.log</li> <li>alert_vip_data_collection.log</li> </ul>	Logs for data collection of Alerts from IntSights
ioc_correlation.log	Logs for correlation of IntSights IOCs with QRadar events
ioc_whitelisting.log	Logs for whitelisting of an IOC
dashboard_population.log	Logs for fetching IOC Overview dashboard data

# Steps to generate the Authorization token on QRoC

- Login to QRadar console.
- Navigate to Admin Panel then click on "QRoc Self Serve" app
- Click on "Authorized Services Management"
- Click on "Add"
- Select User role as "Security Administrator" and "Security Profile" as "Admin" & then click on Save.
- Navigate to the Admin panel and deploy the changes.

# Access application docker

A user can go inside the application docker container. In the docker container, the user can see logs and configure some parameters.

Perform the below command on your QRadar instance via SSH.

- Run /opt/qradar/support/recon ps
- Above command will list all the applications installed in QRadar, then find the app with the name "IntSights App For QRadar" and copy the App-ID of that.
- Now run /opt/qradar/support/recon connect App-ID(That is copied in the above step)

Now the user is in the docker container.

# Configuring app for correlation

The IntSights QRadar app collects IOCs from the IntSights server and stores them into 5 different QRadar reference sets.

- 1. IntSights\_IOC\_IpAddresses
- 2. IntSights\_IOC\_Hashes
- 3. IntSights\_IOC\_Domains
- 4. IntSights\_IOC\_Emails
- 5. IntSights\_IOC\_Urls

The application contains default 6 rules named "IntSights Source IP Rule", "IntSights Destination IP Rule", "IntSights File Hash Rule", "IntSights Email Address Rule", "IntSights URL Rule" and "IntSights Domain Rule" which will check whether the respective property of all the incoming events are present in the respective reference set or not. If yes, it will create offenses. Users have to change the CEP as per their environments for File Hash, Domain, Email Address and URL. Follow the steps mentioned in "Steps for changing selected property of rules".

**Note:** By default, these rules are disabled. Users need to manually enable it from the rule window for correlation otherwise correlation will not happen. Follow the below steps for enabling rules.

### Steps to enable rules

The rules provided within the app bundle are disabled by default. To enable a rule in QRadar, follow below steps:

- Log into QRadar Console.
- Navigate to the offense tab.
- Go to Rules in the left panel.
- Select the rule to be enabled, then click on the Action button in the top panel.
- From the drop-down menu of the Action button, click the "Enable/Disable" option.
- A prompt will appear asking users if they are sure about enabling the rule. Click "Ok" and the rule would be enabled.

### Steps for changing selected property of rules

There are four rules that need to be updated as per the user's environment, namely "IntSights Email Address Rule", "IntSights URL Rule", "IntSights File Hash Rule" and "IntSights Domain Rule". By default IntSights Email Address Rule & IntSights Domain Rule have "File Hash" Property selected in Rule condition & in rule response, so users need to change it to with the CEP which extracts "Email Addresses/Domains" in their QRadar environment.

Note: If "File Hash" & "URL" CEPs are not present in the user's environment, then users need to change those CEPs in "IntSights File Hash Rule" and "IntSights URL Rule" to those CEPs which will extract the value from the event. To change the CEP in these rule follow below steps:

- Log into QRadar Console.
- Navigate to the offense tab.
- Go to Rules in the left panel.
- Open the rule in which we have to change the CEP.
- Rule wizard will be open as shown in figure 11.
- The filter "when any of <u>these event properties</u> are contained in any of <u>these</u> reference set(s)". matches the value of the selected properties against the selected reference sets. For example for IntSights Email Address Rule user needs to change the "<u>these event properties</u>" from "File Hash" to Emails(CEP) which user needs to create for email extraction from the events. Same thing user needs to do in the

"IntSights Domain Rule", where. Once the rule conditions are configured, click "Next" from the bottom panel.

**Note:** For custom properties to be selected in "**these event properties**", it must be "enabled for use in Rules, Forwarding Profiles and Search Indexing". Users can enable it from the Admin Panel -> Custom Event Properties -> Property Name -> Select the checkbox "Enable for use in Rules, Forwarding Profiles and Search Indexing") as shown in the figure 12.

- Under the Rule Action section, select the "Ensure the detected event is part of an offense" checkbox. In the dropdown for "Index offense based on", select the event property that was selected in the previous step. For example: If the user has selected the "Hash" event property in the rule conditions, then the "Hash" event property should also be selected in the Rule Action section for "Ensure the detected event is part of an offense" as shown in Figure 13.
- This action would create/update an offense indexed over the selected event property whenever the rule gets triggered. The user may select any other response or action from the given options if needed. Once the necessary rule actions are selected, click "Finish" from the bottom panel.
- After the rule is created, if any new event arrives, which matches the criteria of the rule then the rule will be triggered, and it will create an offense. Make sure the rule is enabled.

### **Creating rules**

A user can create different types of rules for the correlation. A user can create a rule to generate offense and it will be listed in the offense tab. Follow the below steps for creating a rule.

- Navigate to the offense tab.
- To create an offense rule, go to Rules in the left panel.

des         Display:         Twee         Group:         Select a group:         The Corup         Actions *         Prevent Rule         Search Rules:         Verve the IBM App Exchange for more           Offernoes:         All Exclosion E.         Asset Reconciliati.         Custom Rule         Event True         ReferenceSet         0         0         System         Mar 2,2014, 128         Ord         Creation Date         If           Category         AssetExclusion: E.         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 127         Oc           Category         AssetExclusion: E.         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 127         Oc           Source IP         AssetExclusion: E.         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 128         Oc           Source IP         AssetExclusion: E.         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 123         Oc	Group         Actions ¥ ₹ Revert Rule         Search Rules         Verr the IBM App Exchange for more           Rule Type         Enabled         Response         Event/Flow Count         Offense Count         Origin         Creation Date         Modification           True         ReferenceSet         0         0         System         Jan 7, 2014, 125         Oct 10, 2019, 2017         Oct 10, 2019,	Display:         New Me IDM App Exchange for more           Opes         Action V         Cencep         Action V         Cencep         Event/Flow Count         Offense Count         Of	ard Offenses	Log Activity Network Ac	tivity Assets	Reports Risks	Vulnerabilities							System Time:
Rule Name ▲         Group         Rule Category         Rule Type         Enabled         Response         Event/Flow Count         Offense Count         Origin         Creation Date         I           LOffenses         AssetExclusion: E.         Asset Reconciliat.         Custom Rule         Event         False         0         0         System         Mar 7, 2006, 434 (D)           Category         AssetExclusion: E.         Asset Reconciliat.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 125 Op         AssetExclusion: E.         Asset Reconciliat.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 127 Op         AssetExclusion: E.         <	Rule Type         Enabled         Response         Event/Flow Count         Offense Count         Origin         Creation Date         Modification           False         0         0         System         Mar 22,2006,434.         Oct 10,2019, Mar 7,2014,125.         Oct 10,2019, Mar 7,2014,125.         Oct 10,2019, Mar 7,2014,127.         Oct 10,2019, Mar 7,2014,127.         Oct 10,2019, Mar 7,2014,128.         O	Notes     Rule Name →     Group     Rule Category     Rule Type     Enabled     Response     Event#Tow Count     Offense Count     Origin     Creation Date     Modification       All Exploits Becom     Intrusion Detection     Custom Rule     Event     False     0     0     System     Mar 22,006,434.     Oct 10,2019, AssetExclusion       ory     AssetExclusion     E. Asset Reconciliat     Custom Rule     Event     True     ReferenceSet     0     0     System     Jan 7,2014,127.     Oct 10,2019, AssetExclusion:       e IP     AssetExclusion:     E. Asset Reconciliat     Custom Rule     Event     True     ReferenceSet     0     0     System     Jan 7,2014, 127.     Oct 10,2019, AssetExclusion:     Custom Rule     Event     True     ReferenceSet     0     0     System     Jan 7,2014, 120.     Oct 10,2019, AssetExclusion:     Custom Rule     Event     True     ReferenceSet     0     0     System     Jan 7,2014, 120.     Oct 10,2019, AssetExclusion:     Custom Rule     Event     True     ReferenceSet     0     0     System     Jan 7,2014, 120.     Oct 10,2019, AssetExclusion:     Custom Rule     Event     True     ReferenceSet     0     0     System     Jan 7,2014, 120.     Oct 10,2019, AssetExclusion:     Saster Reconciliat<	ies	Display: Rules	Group: Select	a group	Groups	Actions 🔻 🧭 Rever	t Rule Search Rules	9	View the IBM App Exch	ange for more		
All Exploits Becom.         Intrusion Detection         Custom Rule         Event         False         0         0         System         Mar 27, 2006, 43.4.         Oc           Category         AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 127.         Oc           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 127.         Oc           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 127.         Oc           Source IP         AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oc           Otheration IP         AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oc           AssetExclusion E         Asset Reconciliati.         Custom R	False         0         0         System         Mar 27 2008, 424.         Oct 10 2019, Oct 10 2019, True         Number 2008, 424.         Oct 10 2019, Oct 10 2019, True         Number 2008, 424.         Oct 10 2019, Oct 10 2019, Oct 10 2019, True         Number 2008, 424.         Oct 10 2019, Oct 10 2019, True         Number 2008, 426.         Oct 10 2019, Oct 10 2019, True         Number 2008, 426.         Oct 10 2019, Oct 10 2019, True         Number 2008, 426.         Oct 10 2019, True         Number 2008, 426.         Number 2008, True         Number 2008, True         Number	Alf Explois Bacom.         Intrusion Detection         Ustain Rule         Event         False         0         0         System         Mar 27, 2006, 434.         Oct 10, 2019,	Offenses	Rule Name 🔺	Group	Rule Category	Rule Type	Enabled	Response	Event/Flow Count	Offense Count	Origin	Creation Date	Modificatio
Interest         Asset Exclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         System         Jan 7, 2014, 125.         OC           tegory         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 125.         OC           assetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 125.         OC           unce IP         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 125.         OC           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 125.         OC           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 125.         OC           AssetExclusion E         Asset Reconcilati.         Custom Rule <td>True         ReferenceSet         0         0         System         Jan 7, 2014, 125.         Oct 10, 2019, Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oct 10, 2019,           True         &lt;</td> <td>des         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 125.         Oct 10. 2019           ory         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 125.         Oct 10. 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 125.         Oct 10. 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 123.         Oct 10. 2019           atton IP         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 123.         Oct 10. 2019           atton IP         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 133.         Oct 10. 2019</td> <td></td> <td>All Exploits Becom</td> <td>Intrusion Detection</td> <td>Custom Rule</td> <td>Event</td> <td>False</td> <td></td> <td>0</td> <td>0</td> <td>System</td> <td>Mar 27, 2006, 4:34</td> <td>Oct 10, 2019,</td>	True         ReferenceSet         0         0         System         Jan 7, 2014, 125.         Oct 10, 2019, Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019,           True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oct 10, 2019,           True         <	des         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 125.         Oct 10. 2019           ory         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 125.         Oct 10. 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 125.         Oct 10. 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 123.         Oct 10. 2019           atton IP         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 123.         Oct 10. 2019           atton IP         AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014, 133.         Oct 10. 2019		All Exploits Becom	Intrusion Detection	Custom Rule	Event	False		0	0	System	Mar 27, 2006, 4:34	Oct 10, 2019,
desetExclusion E         Asset Reconcilat.         Custom Rule         Event         Tue         ReferenceSet         0         System         Jan 7, 2014, 127         Ox           urce IP         AssetExclusion E         Asset Reconcilat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 127         Ox           urce IP         AssetExclusion E         Asset Reconcilat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 120         OX           stination IP         AssetExclusion E         Asset Reconcilat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 123         OX           stination IP         AssetExclusion E         Asset Reconcilat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 123         OX           twork         AssetExclusion E         Asset Reconcilat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 137         OX           AssetExclusion E         Asset Reconc	True         ReferenceSet         0         0         System         Jan 7, 2014, 127.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 137.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 137.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 137.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 138.         Oct 10, 2019           True         ReferenceSet	ory         AssetE Acutation E         Asset Reconciliat.         Outmon Tue         Vent         Tue         ReferenceSet         0         0         System         Jan 7. 2014, 128.         Oct 10. 2019           e IP         AssetExclusion E         Asset Reconciliat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014, 128.         Oct 10. 2019           AssetExclusion E         Asset Reconciliat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014, 128.         Oct 10. 2019           AssetExclusion E         Asset Reconciliat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014, 128.         Oct 10. 2019           AssetExclusion E         Asset Reconciliat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014, 123.         Oct 10. 2019           AssetExclusion E         Asset Reconciliat.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014, 133.         Oct 10. 2019           AssetExclusion E         Asset Recon	fenses	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:25	Oct 10, 2019.
AssetExclusion E         Asset Reconcilat.         Custom Rule         Event         True         ReferenceSet         0         System         Jan 7, 2014, 128.         Or           urce IP         AssetExclusion E         Asset Reconcilat         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Or           stant2         AssetExclusion E         Asset Reconcilat         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Or           AssetExclusion E         Asset Reconcilat         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Or           AssetExclusion E         Asset Reconcilat         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Or           Avork         AssetExclusion E         AssetExclusion Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 133.         Or           Avork         AssetExclusion E         Asset Reconcilat         Custom Rule	True         ReferenceSet         0         0         System         Jan 7, 2014, 128         Oct 10, 2019.           True         ReferenceSet         0         0         System         Jan 7, 2014, 128         Oct 10, 2019.           True         ReferenceSet         0         0         System         Jan 7, 2014, 128         Oct 10, 2019.           True         ReferenceSet         0         0         System         Jan 7, 2014, 123         Oct 10, 2019.           True         ReferenceSet         0         0         System         Jan 7, 2014, 123         Oct 10, 2019.           True         ReferenceSet         0         0         System         Jan 7, 2014, 123         Oct 10, 2019.           True         ReferenceSet         0         System         Jan 7, 2014, 135         Oct 10, 2019.           True         ReferenceSet         0         System         Jan 7, 2014, 135         Oct 10, 2019.           True         ReferenceSet         0         System         Jan 7, 2014, 135         Oct 10, 2019.           True         ReferenceSet         0         System         Jan 7, 2014, 138         Oct 10, 2019.	AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 128.         Oct 10, 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oct 10, 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule	iterion/	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:27	Oct 10, 2019
Unce IP         AssetE-bulsion E         Asset Reconciliat.         Custom Rule         Event         Tue         ReferenceSet         0         System         Jan 7,2014,120         OC           stinistion IP         AssetE-bulsion E         Asset Reconciliat.         Custom Rule         Event         Tue         ReferenceSet         0         O         System         Jan 7,2014,120         OC           stinistion IP         AssetE-bulsion E         Asset Reconciliat.         Custom Rule         Event         Tue         ReferenceSet         0         O         System         Jan 7, 2014, 123<.	True         ReferenceSet         0         0         System         Jan 7, 2014, 120.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 138.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 138.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 138.         Oct 10, 2019	IP         AssetExclusion E         Asset Reconcilat.         Custom Tule         Event         Tule         ReferenceSet         0         0         System         Jan 7. 2014 120.         Ord 10. 2019           nation IP         AssetExclusion E         Asset Reconcilat.         Custom Tule         Event         Tule         ReferenceSet         0         0         System         Jan 7. 2014 120.         Ord 10. 2019           nation IP         AssetExclusion E         Asset Reconcilat.         Custom Tule         Event         True         ReferenceSet         0         0         System         Jan 7. 2014 123.         Oc 10. 2019           AssetExclusion E         Asset Reconcilat.         Custom Tule         Event         Tule         ReferenceSet         0         0         System         Jan 7. 2014 123.         Oc 10. 2019           AssetExclusion E         Asset Reconcilat.         Custom Tule         Event         Tule         ReferenceSet         0         0         System         Jan 7. 2014 133.         Oc 10. 2019           AssetExclusion E         Asset Reconcilat.         Custom Rule         Event         Tule         ReferenceSet         0         0         System         Jan 7. 2014 138.         Oc 10. 2019           AssetExclusion E	cegory.	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:28	Oct 10, 2019
AssetExclusion E         Asset Reconcilati         Costom Rule         Event         Tue         ReferenceSet         0         System         Jan 7, 2014, 123         Or.           twork         AssetExclusion E         Asset Reconcilati         Costom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7, 2014, 123         Or.           twork         AssetExclusion E	True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oct 10, 2019	Matter IP         Asset Reconciliati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014.123.         Oct 10. 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014.123.         Oct 10. 2019           ork         AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014.123.         Oct 10. 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014.135.         Oct 10. 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014.135.         Oct 10. 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014.135.         Oct 10. 2019           AssetExclusion E         Asset Reconciliati         Custo	urce IP	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:20	Oct 10, 2019,
Utination IP         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         System         Jan 7, 2014, 123.         Oc           Work         AssetEchusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 123.         Oc           Work         AssetEchusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oc           AssetEchusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oc           AssetEchusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 135.         Oc	True         ReferenceSet         0         0         System         Jan 7, 2014, 123         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 137         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 137         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 133         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 133         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 133         Oct 10, 2019	Victor         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 132.         Oct 10, 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 132.         Oct 10, 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 133.         Oct 10, 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 133.         Oct 10, 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 133.         Oct 10, 2019           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 133.         Oct 10, 2019           Rule         Event         True         ReferenceSet		AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:23	Oct 10, 2019
AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 137         Or           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 135         Or           AssetExclusion E         Asset Reconciliati.         Custom Rule         Event         True         ReferenceSet         0         0         System         Jan 7, 2014, 135         Or           AssetExclusion E         AssetExclusic         AssetExclusion E         Asset	True         ReferenceSet         0         0         System         Jan. 7 2014, 132.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan. 7 2014, 135.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan. 7, 2014, 135.         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan. 7, 2014, 138         Oct 10, 2019	AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014. 137.         Oct 10. 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014. 137.         Oct 10. 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014. 135.         Oct 10. 2019           AssetExclusion E         Asset Reconcilati.         Custom Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014. 138.         Oct 10. 2019           Rule         Event         Tue         ReferenceSet         0         0         System         Jan 7. 2014. 138.         Oct 10. 2019	stination IP	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:23	Oct 10, 2019
AssetEsclusion E Asset Reconcilati. Custom Rule Event True ReferenceSet 0 0 System Jan 7, 2014, 135. Oc AssetEsclusion E Asset Reconcilati. Custom Rule Event True ReferenceSet 0 0 System Jan 7, 2014, 135. Oc	True         ReferenceSet         0         0         System         Jan 7, 2014, 135         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 138         Oct 10, 2019           True         ReferenceSet         0         0         System         Jan 7, 2014, 138         Oct 10, 2019	AssetExclusion E Asset Reconcilat. Custom Rule Event True ReferenceSet 0 0 System Jan 7, 2014, 135. O Cd 10, 2019 AssetExclusion E Asset Reconcilat. Custom Rule Event True ReferenceSet 0 0 System Jan 7, 2014, 138. O Cd 10, 2019 Rule	a construction of the second se	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:37	Oct 10, 2019
AssetExclusion: E Asset Reconciliati Custom Rule Event True ReferenceSet 0 0 0 System Jan 7, 2014, 1:38 Ot	True         ReferenceSet         0         0         System         Jan 7, 2014, 1:38         Oct 10, 2019	AssetEconolitati Custom Rule Event True ReferenceSet 0 0 System Jan 7, 2014, 138 Oct 10, 2019 Rule	twork	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:35	Oct 10, 2019
a en el composition de la		Rule		AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	True	ReferenceSet	0	0	System	Jan 7, 2014, 1:38	Oct 10, 2019
		Rie		• • • • • •	1			-			•		1 7 0044 4 00	
Rule				Rule										

Figure	7:	QRadar	offense	rules
--------	----	--------	---------	-------

• A user can add different types of rules by clicking on the Action button as shown below (Figure 8). Select "New Event Rule" from the dropdown menu.

	Log Activity Network Ac	tivity Assets	Reports Risks	Vulnerabilities Adm	lin						System Time: 1
es	Display: Rules	Group: Select	a group	Groups	Actions V Revert Rule S	arch Rules	Q	View the IBM App Exch	ange for more		
Offenses	Rule Name 📥	Group	Rule Category	Rule Type	New Event Rule	ponse	Event/Flow Count	Offense Count	Origin	Creation Date	Modification
	All Exploits Becom	Intrusion Detection	Custom Rule	Event	New Flow Rule		0	0	System	Mar 27, 2006, 4:34	Nov 7, 2019, 5
Offenses	Anomaly: Excessiv	Recon	Custom Rule	Event	New Common Rule	New Event	0	0	System	Nov 30, 2005, 5:4	Nov 7, 2019, 5
ategony	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	New Offense Rule	Set	0	0	System	Jan 7, 2014, 1:25	Nov 7, 2019, 5
acceory	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	Enable/Disable	Set	0	0	System	Jan 7, 2014, 1:27	Nov 7, 2019, 5
ource IP	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	In Duplicate	Set	0	0	System	Jan 7, 2014, 1:28	Nov 7, 2019, 5
	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	Ex Onen	Set	0	0	System	Jan 7, 2014, 1:20	Nov 7, 2019, 5
estination IP	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	C Deluis	Set	0	0	System	Jan 7, 2014, 1:23	Nov 7, 2019, 5
- house to	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	Delete	Set	0	0	System	Jan 7, 2014, 1:23	Nov 7, 2019, 5
PLWOIK	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	Assign Groups	Set	0	0	System	Jan 7, 2014, 1:37	Nov 7, 2019, 5
15	AssetExclusion: E	Asset Reconciliati	Custom Rule	Event	Historical Correlation	Set	0	0	System	Jan 7, 2014, 1:35	Nov 7, 2019, 5
201	1	A 10 2.0	A 1 A 1		ir in c	- · ·	A	^	- ·	1 7 0044 4 00	11 7 0040 5
	Pule										
	Notes										

Figure 8: New Event Rule

• On selecting any of the rules, a Rule wizard will be opened as shown in Figure 9. Click next from the bottom panel.

≡ IBM OBadar		Rule Wizard	0		4	Q
		Welcome to the Custom Rules Wizard!				
Dashboard Offenses	Log Activity Network Activity A	This wizard guides you through the process of creating security processing rules to detect specific events, flows, or offenses of interest. Matched rules allow for a number of responses, including Email, Syslog, or automatic response to threats.			System Time:	5:49 PM
Offenses	Display: Rules V Gro	The wizard guides you through the following steps:	ge for more			0
My Offenses	Rule Name 📥 🛛 G	1. Choose the tests to perform.	Origin	Creation Date	Modification	-
All Offenses	All Exploits Becom Intrusion	<ol> <li>Customize the parameters for your chosen tests.</li> <li>Decide the appropriate actions once an event or flow (or both) has been detected.</li> </ol>	System	Mar 27, 2006, 4:34	Nov 7, 2019, 5	-
All Offendes	Anomaly: Excessiv Recon	4. Review and save your rule.	System	Nov 30, 2005, 5:4	Nov 7, 2019, 5	
By Category	AssetExclusion: E Asset Re		System	Jan 7, 2014, 1:25	Nov 7, 2019, 5	
	AssetExclusion: E Asset Re		System	Jan 7, 2014, 1:27	Nov 7, 2019, 5	
By Source IP	AssetExclusion: E Asset Re	Click Next to continue, or click Gancel to exit the wizard.	System	Jan 7, 2014, 1:28	Nov 7, 2019, 5	
0.0.11.11.10	AssetExclusion: E Asset Re		System	Jan 7, 2014, 1:20	Nov 7, 2019, 5	
By Destination IP	AssetExclusion: E Asset Re		System	Jan 7, 2014, 1:23	Nov 7, 2019, 5	
By Network	AssetExclusion: E Asset Re	Skip this page when running this rules wizard.	System	Jan 7, 2014, 1:23	Nov 7, 2019, 5	
by needoric	AssetExclusion: E Asset Re		System	Jan 7, 2014, 1:37	Nov 7, 2019, 5	
Rules	AssetExclusion: E Asset Re		System	Jan 7, 2014, 1:35	Nov 7, 2019, 5	
			o	1 7 0044 4 00		
	Pulo					
	Notes					
						-
		- Part Mater - Parts Press				
		<< Back Next >> Finish Candel				

Figure 9: Rule Wizard

• On the next page, there will be radio buttons from which we have to choose the source from which the rules are generated. Events will be selected. Click on next.

≡ IBM QRadar	Rule W	izard				Ċ.	0
Dashboard Offenses	Log Activity Network Activity A	Welcome to the Custom Rules Wizard!				System Time:	5:50 PM
Offenses	Display: Rules V Grc	Choose the source from which you want this rule to generate:		ge for more			0
Ny Offenses All Offenses By Category By Source IP By Destination IP By Network Rules	Rule Name → C Al Exploite Secon	<ul> <li>Flows</li> <li>This tule type performs tests on fields that are unique to flow records</li> <li>Events or Flows</li> <li>Thore type performs tests on fields that are common to both event or flow records</li> <li>This fulle type tests for when changes are made to existing offenses</li> <li>Click Next to continue, or click Cancel to exit the wizard.</li> </ul>		Origin System System System System System System System System	Creation Date Mar 27, 2006, 4:34. Nov 30, 2005, 5:4. Jan 7, 2014, 125. Jan 7, 2014, 127. Jan 7, 2014, 128. Jan 7, 2014, 128. Jan 7, 2014, 123. Jan 7, 2014, 123. Jan 7, 2014, 123.	Modificatio Nov 7, 2019, Nov 7,	n * 50 50 50 50 50 50 50 50 50 50 50 50 50
	Notes						·
		<< Back 1	Next>> Finish Cancel				

Figure 10: Rule Wizard

• As shown in Figure 11, the Rule wizard opens up and there are many options to generate a rule.

= IBM OPadar		Rule Wizard			$^{\circ}$	0
		·			÷	-
Dashboard Offenses	Log Activity Netwo	Rule Wizard: Rule Test Stack Editor		Sy	stem Time: 3:20	PM
		Which tests do you wish to perform on incoming events?				_
Offenses	Display: Rules	Test Group All 🗸	he IBM App Exch	ange for more		0
My Offenses	Rule Name	event properties	ense Count	Origin	Ci ^	
	All Exploits Bec	✤ when any of these event properties are contained in any of these reference set(s)		System	Mar 2	
All Offenses	Anomaly: Exce	when any of these event properties is the key and any of these event properties is the value in any of these reference		System	Nov 3	
By Category	AssetExclusion	maps		System	Jan 7,	
by category	AssetExclusion	map of sets		System	Jan 7,	
By Source IP	AssetExclusion	when any of these event properties is the key of the first map and any of these event properties is the key of the second		System	Jan 7,	
	AssetExclusion	map and any or mese event properties is the value in any or mese reference map or maps		System	Jan 7,	
By Destination IP	AssetExclusion	operator the value of selected event property		System	Jan 7,	
	AssetExclusion	when at least this many events are seen with the same event properties in this many minutes		System	Jan 7,	
By Network	AssetExclusion	A when at losst this many events are seen with the same event prenerties and different event prenerties in this many		System	Jan 7,	
Pulor	AssetExclusion	Rule (Click on an underlined value to edit it)		System	Jan 7, 🖕	
nules	4	invand tests are nignighted and must be lixed before rule can be saved.		0		
	Rule	Apply (enter rule name here) on events which are detected by the Local v system				
	Kuic	C and when any of these event properties are contained in any of these reference set(s)				i
		Please select any groups you would like this rule to be a member of:				
		r 🗁 🗆 Anomaly				
		Asset Reconciliation Exclusion				
		Hard Authentication				
	Notes	Botnet				
		<< Back Next>>> Finish Canoel				

Figure 11: Rule Wizard: Rule Test Stack Editor

- Rule name must start with "IntSights". For example: If a user wants to create a rule to correlate Hashes then the rule name could be "IntSights Hash Rule".
   Note: Rule names must start with "IntSights", or else the offenses created/updated by such rules would not be considered as IntSights offenses and they won't be visible on IntSights QRadar App Dashboard.
- From these options select the filter: "when any of <u>these event properties</u> are contained in any of <u>these reference set(s)</u>". This condition will match the value of the selected properties against the selected reference sets. For example: If a user wants to create a rule to correlate Hashes then the user has to select the appropriate Custom event property which extracts Hash value from the events, and "IntSights\_IOC\_Hashes" as the reference set. Once the rule conditions are configured, click "Next" from the bottom panel.
   Note: For custom properties to be selected in "these event properties", it must be "enabled for use in Rules, Forwarding Profiles and Search Indexing". Users can

enable it from the Admin Panel -> Custom Event Properties -> Property Name -> Select the checkbox "Enable for use in Rules, Forwarding Profiles and Search Indexing") as shown in the below figure.

Custom Event Proper	ty Definition - Google Chrome	-		×			
A Not secure   htt	es://10.50.3.133/console/do/qradar/arielProperties?appName=qradar&pageId=ArielPropertiesList&disp	atch=e	dit&id	=5			
Custom Event Prop	erties			8			
You can define custom properties. If you naviga	properties from an event payload. Using the below options, you can test your RegEx entry that you wish to use to define you ted to this window from an event details window, the below options are populated with the payload of the event you were	our cust viewing	om				
Test Field	Note: Oustain neus are non indexed and could increase the time for reports, and/or searches to complete.			d			
LEEF:2.0 IntSights IntSights 1.0.0 intsights_ioc json={"value": "192.168.0.6", "type": "IpAddresses", " severity": "Low", "score": 7, "lastDpdateDate": "2021-01-28T12:00:00.0102", "lastBeen": "2021-01- 29T19:18:02.1152", "firstBeen": "2020-12-12T18:08:32.2252", "geolocation": "country", "relatedMalware": ["Malwarel"], "relatedCampaigna": ["Campaign1"], "relatedThreatActors": ["ThreatActor1"], "reportedFeeds": *							
Property Definition							
Existing Property:     Onew Property:     Enable for use in Ru Field Type:	IOC Value  les, Forwarding Profiles and Search Indexing AlphaNumeric						
Description:	Value of an IoC		11				
Property Expression	Definition						
Enabled:							
Selection Log Source Type Log Source: OEvent Name: ©Category:	IntSights  All Please browse for an event Browse High Level Category Any Low Level Category Any						

Figure 12: Custom Event Property: Enable for use in Rules, Forwarding Profiles and Search Indexing

Under the Rule Action section, select the "Ensure the detected event is part of an offense" checkbox. In the dropdown for "Index offense based on", select the event property that was selected in the earlier step. For example: If the user has selected the "Hash" event property in the rule conditions, then the "Hash" event property should also be selected in the Rule Action section for "Ensure the detected event is part of an offense" as shown below.

≡ IBM QRadar		Rule Wizard		ŧ	<u>_</u> _
Dashboard Offenses Lo	og Activity Netwo	Rule Wizard: Rule Response		Sy	stern Time: 3:45 PM
Offenses	Display: Rules	Rule Action Choose the action(s) to take when an event occurs that triggers this rule	he IBM App Exc	nange for more	0
My Offenses	Rule Name	Severity Set to V 0 V	ense Count	Origin	Ct ^
	All Exploits Bec	Credibility Set to V 0 V		System	Mar 2
All Offenses	Anomaly: Excer			System	Nov 3
Py Category	AssetExclusion	Relevance Set to V 0 V		System	Jan 7,
by category	AssetExclusion	Ensure the detected event is part of an offense		System	Jan 7,
By Source IP	AssetExclusion			System	Jan 7,
	AssetExclusion	Index offense based on Source IP -		System	Jan 7,
By Destination IP	AssetExclusion	Annotate this offense:		System	Jan 7,
	AssetExclusion	Include detected events by Source IP from this point forward, in the offense, for : 300 second(s)		System	Jan 7,
By Network	AssetExclusion			System	Jan 7,
Rules	AssetExclusion	Annotate event		System	Jan 7, 🖕
Rules	4	Bypass further rule correlation event		A	
	Rule	Rule Response Choose the response(s) to make when an event triggers this rule			^
	Notes	Dispatch New Event Email Send to Local Syslog Send to Forwarding Destinations Notify Add to a Reference Set Add to a Reference Data Destinations	·		
		<< Back Next>>> Finish C	anoel		

Figure 13: Rule Wizard: Rule Response

• This action would create/update an offense indexed over the selected event property

whenever the rule gets triggered. The user may select any other response or action from the given options if needed. Once the necessary rule actions are selected, click "Finish" from the bottom panel.

• After the rule is created, if any new event arrives, which matches the criteria of the rule then the rule will be triggered, and it will create an offense.

# Configuring app for generating alert on correlation

In the application, there is one rule named "IntSights Correlation Alert" that will monitor correlated events and will notify the users via notifications on the QRadar console and email. By default only "notify" is selected in the rule response, so it will send notifications only. For the email, users have to manually modify the rule.

Follow the below steps to receive an email whenever any IntSights rules get triggered.

- 1. Configure Email Server into QRadar
- 2. Configure IntSights Email Template
- 3. Update rules

**Note:** By default, the "IntSights Correlation Alert" is disabled. Users need to manually enable it from the rule window to receive email and notification on the QRadar console.

By default, the "IntSights Correlation Alert" will send notifications and emails for all correlations. If users want to notify based on the filters, then they have to modify the "IntSights Correlation Alert" rule. Follow the steps mentioned under "Adding filter in Rules" to add filters in the rule.

### **Configuring Email Server**

Follow the below steps to configure the email server into QRadar for receiving emails on the correlation.

- 1. Click the Admin tab.
- 2. Click Email Server Management.
- 3. Click the Other Settings (1) icon for the server that you are editing.

Em	ail Server Management					?
	Search O					Add
	Hostname	Description	Port	Username	TLS	
	localhost 🕕	LocalHost Email Server	25	-	disabled	
					Edit	
		Figure 14, Edit	ina Email	Comicon		
		rigure 14: Editi	ng Email	Server.		

4. Add email server details and save it.

Refer to the link below for more information. <u>https://www.ibm.com/docs/en/qsip/7.3.2?topic=hosts-configuring-email</u>

# Creating custom email template for IntSights Correlation e-mail

IntSights QRadar app provides a custom template for IntSights Correlation email. Follow below mentioned steps to add a custom email template.

- 1. Use SSH to log in to the QRadar Console as the root user.
- 2. Create a new temporary directory to use to safely edit copies of the default files.
- 3. To copy the files that are stored in the custom\_alerts directory to the temporary directory, type the following command:

cp /store/configservices/staging/globalconfig/templates/custom\_alerts/\*.\* <directory\_name>

The <directory\_name> is the name of the temporary directory that you created.

- 4. Confirm that the files were copied successfully:
  - a. To list the files in the directory, type Is -lah.
  - b. Verify that the alert-config.xml file is listed.
- 5. Open the alert-config.xml file for editing.
- 6. Copy and paste the provided email template from "<u>XML Template for Email</u>" in the alert-config.xml file in the "<templates>" XML tag. (Note: Make sure the indentation and spaces are appropriate). An image is attached below for reference, to see what the alert-config.xml file should look like after adding the template.



Figure 15: email template file (alert-config.xml)

- 7. Save and close the alert-config.xml file.
- 8. Type "cd .." to move out of the directory and then run the below command.
- 9. Validate the changes by typing the following command.

/opt/qradar/bin/runCustAlertValidator.sh <directory\_name>

The <directory\_name> parameter is the name of the temporary directory that you created.

If the script validates the changes successfully, the following message is displayed: "File alert-config.xml was deployed successfully to staging!"

- 10. Deploy the changes in QRadar.
  - a. Log in to QRadar.

- b. Navigate to the Admin tab.
- c. Click Advanced, and then Deploy Full Configuration.

For more information refer:

https://www.ibm.com/docs/en/qsip/7.4?topic=notifications-configuring-event-flow-custom-email

Users can modify this email template file to receive any extra fields in the email. Follow steps of "Adding new field in Email".

### Adding email templates to Rules

After successfully adding a custom template, follow the below steps to use the created template in the Email

- 1. Click on rules in the Log Activity tab.
- 2. Find the "IntSights Correlation Alert" rule, and open it.



Figure 16: Rule Wizard.

3. Click next and in the rule response select the checkbox with email and add the email address in which you wish to receive emails. Make sure that in templates "IntSights Email Template" is selected.

≡ IBM QRadar		Rule Wizard Contraction Contra	-	(li	Ļ	<u> </u>
Dashboard Offenses	Log Activity Netw				System Time: 1	12:11 PM
Offenses	Display: Rules	Rule Action Choose the action(s) to take when an event occurs that triggers this rule	the IBM	App Exchange for more		0
My Offenses All Offenses By Category By Source IP By Destination IP By Network <b>Rules</b>	Ruit FalsePositive I. Frist-Time Use State Host Port Scan Increase Magn Increase Magn Insights Courc Large Outbound Ruie Apply Insights Caurc Large Outbound Ruie Apply Insights Caurc Apply Insights	Severity       Set to       0         Credibility       Set to       0         Belevance       Set to       0         Ensure the detected event is part of an offense       0       0         Bypass further rule correlation event       Set to       0         Bypass further rule correlation event       Choose the response(s) to make when an event triggers this rule         Choose the response(s) to make when an event triggers this rule       Choose the response(s) to make when an event triggers this rule         Dispatch New Event       Enter email addresses to notify:       Select event email template:         Select event email template:       IntSights Email Template        Select event find the propagated to the 'System Notifications' item in the dashboard         Send to Local Syslog       Send to Forwarding Destinations       And to a Response Lumiter when using this response         And to a Reference Set       Add to a Reference Set       Set Set Set Set Set Set Set Set Set Set	Count	Offense Count           0           0           0           0           0           0           0           0           0           0           0           0           0           0           0	System System System System System User User User System	
			el			

Figure 17: Adding email template in Rule Response.

- 4. The selected "notify" checkbox is for receiving the notifications on the QRadar console at the right top corner.
- 5. Make sure that in Response Limiter the checkbox is unselected, as it will limit the number of responses users get with the rule. If users add a limit, then it will send only that number of emails/notifications in the provided time.

≡ IBM QRadar	Rule Wizard Consection	<b>-</b>	()	Ļ	0
Dashboard Offenses Log Activity Netw	Dispatch New Event			System Time:	12:11 PM
Offenses Display: Rules	Enter email addresses to notify:	the IBM Ap	p Exchange for more		0
My Offenses Rul	Select event email template: IntSights Email Template 🗸	Count	Offense Count	Ori	gii 🔶
All Offenses FalsePositive: F First-Time User	Send to Local Syslog		0	System System	
By Category Flow Source St Host Port Scan	Notify		0	System System	
By Source IP Increase Magni	This event / flow will be propagated to the 'System Notifications' item in the dashboard		0	System	_
By Destination IP IntSights Corre	✓ Use event severity for notification severity		0	User	
By Network IntSights Destir IntSights Sourc	Add to a Reference Set		0 0	User User	
Rules Large Outboun	Remove from a Reference Set		0	System	
Rule Apply IntSights C and when the ev	Execute Custom Action	-			^
and when any of	Response Limiter Use this section to configure the frequency with which you want this rule response to respond				
	Respond no more than time(s) per second(s) v per Rule v				ι.
Notes	Enable Rule				
	Enable this rule if you want it to begin watching events right away.	•			-
	<< Back Next>> Finish Cancel				

Figure 18: Unchecking Response Limiter.

6. Now save the rule and enable it. For enabling the rule click on the action tab and then click on Enable/Disable.

hboard Offenses L	Log Activity Network Activity Asset:	s Repo				OK	cel ashboard		v	System Time: 12:
fenses	Display: Rules V Group:	Select a group		Groups	Acti	ons 🔻 🧬 Revert Rule Searc	h Rules	View the IBM A	pp Exchange for more	
My Offenses	Rule Name A	Group	Rule Category	R		New Event Rule New Flow Rule	Response	Event/Flow Count	Offense Count	Origi
All Offenses	FalsePositive: False Positive Rul	False Positive	Custom Rule	Comm		New Common Rule		0	0	System
	First-Time User Access to Critical	Anomaly, Authenti	Custom Rule	Event	6	New Offense Rule	Dispatch New Eve	0	0	System
By Category	Flow Source Stopped Sending Fl	System	Custom Rule	Flow		Enchie/Dischie	Dispatch New Event	0	0	System
	Host Port Scan Detected by Rem	Recon	Custom Rule	Comm		Enable/Disable	Dispatch New Event	0	0	System
By Source IP	Increase Magnitude of High Rate	Recon	Custom Rule	Event	D	Duplicate		0	0	System
D. D. Handler ID	Increase Magnitude of Medium R	Recon	Custom Rule	Event	Ľ	Open		0	0	System
By Destination IP	IntSights Correlation Alert	IntSights	Custom Rule	Event	0	Delete	Email, Notification	0	0	User
By Network	IntSights Destination IP Rule	IntSights	Custom Rule	Event	10	Assign Groups		0	0	User
-,	IntSights Source IP Rule	IntSights	Custom Rule	Event	6	Historical Correlation		0	0	User
Rules	Large Outbound Transfer High R	Compliance, Exfiltr	Custom Rule	Flow	0		Dispatch New Event	0	0	System
	Rule Appy IntSights Correlation Alert on ee and when the event QID is one of the and when any of Whitelisted (custom)	vents which are detect following (100250000) match false	ad by the Local system 3) IntSights Correlated	Event						

Figure 19: Enabling the Rule.

# Adding filter in Rules

Users can modify the rule for receiving emails and notifications based on specific conditions. Refer to the below example.

In this example, we will notify the users only when the severity of the correlated IOC is High. Follow the below steps for modifying the rule.

- 1. Click on rules in the Log Activity tab.
- 2. Find the rule in which you want to add a filter for severity, and open it. For example, IntSights Correlation Alert.
- 3. When the rule wizard opens, in the search filter, search "when any of these properties match this regular expression".

= IBM ORadar		Rule Wizard				0
Dashboard Offenses	Log Activity Netwo	Rule Wizard: Rule Test Stack Editor	Î		System Time: 1:	2:19 PM
Offenses	Display: Rules	Which tests do you wish to perform on incoming events? Test Group All   Export as Building Block	he IBI	App Exchange for more		0
My Offenses All Offenses By Category By Source IP By Destination IP By Network <b>Rules</b>	Rul FalsePositive: I First-Time User Flow Source St Host Port Scan Increase Magn Increase Magn Insights Boarc IntSights Destr IntSights Destr IntSights Destr IntSights Destr IntSights Destr IntSights Destr IntSights Courc Arge Outboan Carge Outboan Rule Ropy IntSights C And when the ev and when any of	when any of these properties match this regular expression         Image: the any of these properties match this regular expression         Image: the any of these properties match this regular expression         Image: the any of these properties match this regular expression         Image: the any of these properties match this regular expression         Image: the any of these properties match this regular expression         Image: the any of these properties match this regular expression         Image: the any of the any of the angle		I         Offense Count           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0           0         0	System System System System System User User User System	
	Notes	Calegory Definitions  Votes (Enter your notes about this rule)	•			*
		<< Back Next>> Finish Ca	oel			

Figure 20: Adding Rule filter.

- 4. Add this rule filter and click on "these properties" and select "IOC severity (Custom)" in the pop-up.
- 5. Now click on "this regular expression", and type a regular expression as below:

- a. To receive mail only for High severity, type. Eg. "High"
- b. For receiving mail in case of either of two severity. For High and Medium severity, type "**High|Medium**" (without quotes). For medium and low severity type "**Low|Medium**".

Dashboard Offenses Log Adivity Network Offenses Display: Rules Ny Offenses Rul when	Rule Wizard: Rule Test Stack Editor hich tests do you wish to perform on incoming events? at Group All v en any of these properties match this regular expression	Not secure   10.0.9.182/console/do/rulewizard/customizeCondition Enter a value Low/Medum	Parameter?test=2 P Submit Cancel	4
Dashboard         Offenses         Log Activity         Network           Offenses         Display:         Rules         Test           My Offenses         Rul         whether         White	nich tests do you wish to perform on incoming events? st Group All  any of these properties match this regular expression	Enter a value Low/Medium	Submit Cancel	M
All Offenses FalsePositive I First-Time User By Category Flow Source St Host Pot Scan By Source IP Increase Magn	<ul> <li>when any of these properties match this regular expression</li> </ul>			
By Destination IP Increase Magni Insights Corre Insights Corre Ins	le (Click on an underlined value to edit it) alid tests are highlighted and must be fixed before rule can be saved. pply [intSights Correlation Alert on events which ar and when the event OLD is one of the following (1002500003) IntSight and when any of VMIhelisted (custom) match this regular expression and when any of [IoC_Severity (custom) match this regular expression			
Notes	ase select any groups you would like this rule to be a member of:			

Figure 21: Adding IoC Severity Regular Expression.

Rule Wizard						
🗾 Rul	e Wizard: Rule Te	st Stack Edit	tor			·····
Which test	s do you wish to perform on i	coming events?				
Test Group	All 🗸				Export as Bu	uilding Block
when any of	these properties match this regu	lar expression				
🔅 when	any of these properties mal	ch this regular exp	pression			
Rule (Click	on an underlined value to ed	it it)				
Invalid test	s are highlighted and must be	fixed before rule c	an be saved.			
Apply Ints	ights Correlation Alert		on events which are detected by the	Local 🗸	system	
	nd when the event QID is one	e of the following (1	002500003) IntSights Correlated Ever	nt	-	
	nd when any of Whitelisted (o	custom) match false				
	nd when any of loc Severity	( <u>custom)</u> match <u>Lov</u>	<u>v Medium</u>			
Please sel	ect any groups you would like	this rule to be a me	ember of:			
	nomaly					<u>^</u>
	Asset Reconciliation Exclusion	ו				
	Authentication					
	Botnet					•
	Jatedory Definitions					
Notes (Ent	er your notes about this rule)					
					<< Back Next >>	Finish Cancel

Figure 22: Final Rule would look like this.

c. Now click on Finish and Enable the rule.

**NOTE:** As we have to write regular expressions in this filter, type carefully as any spelling mistake could result in rules not being triggered.

### Adding new field in Email

- 1. First, check if the new field you want to add exists or not. To check perform the following steps:
  - a. Click the **Admin** tab.
  - b. Click Custom Event Properties.
  - c. Search for your property.
- 2. If the property exists then double click on it to open the property.
- 3. Make sure the checkbox for "Enable for use in Rules, Forwarding Profiles, and Search Indexing" is selected, otherwise users won't receive the property in Email.

Custom Event Prop	erties
'ou can define custom properties. If you naviga	properties from an event payload. Using the below options, you can test your RegEx entry that you wish to use to define your custom ated to this window from an event details window, the below options are populated with the payload of the event you were viewing.
M	lote: Custom fields are not indexed and therefore, could increase the time for reports, and/or searches to complete.
est Field	
LEEF:2.0 IntSid "IpAddresses", "2021-01-29T19 "relatedThreat	ghts IntSights 1.0.0 intsights_correlated_event json={"value": "192.168.0.0", "type": "severity": "Low", "score": 7, "lastDpdateDate": "2021-01-28712:00:00.0102", "lastBeen": 118:02.1152", "firstBeen": "2020-12-12718:08:32.2252", "relatedMalware": "Malwarel, Malware2", Actors": "ThreatActor1. ThreatActor2", "reportedFeeds": "ABC, XYZ", "swstemTags": "SwsTag1.
roperty Definition	
Existing Property:	Whitelisted 🗸
ONew Property:	
Enable for use in Ru	iles, Forwarding Profiles and Search Indexing
ield Type:	AlphaNumeric 🗸
Description:	Shows whether the IOC is whitelisted or not
roperty Expression I	Definition
Enabled: 🗹	
Selection	
Log Source Type	IntSights
Log Source:	All
OEvent Name:	Please browse for an event Browse
	High Level Category Any
Category:	

Figure 23: Enabling property for Rule

4. Add the below line in the email template (alert-config.xml) file under the <body> tag. Label> : \${body.CustomProperty("property-name>")}

```
For e.g, the User wants to add "Property 1" in the email then
add the below line in the alert-config.xml file under <body>
tag.
```

```
Property 1 : ${body.CustomProperty("Property 1")}
```

5. Follow the steps mentioned in the link below for deploying this email template. <u>https://www.ibm.com/docs/en/qsip/7.4?topic=notifications-configuring-event-flow-cust</u> <u>om-email</u>

# Whitelisting

# Whitelisting an IOC

User can follow the below steps to whitelist an IOC:

- Navigate to the Log Activity tab in QRadar.
- Open up an IntSights IOC event for the IOC value user wishes to whitelist.
- Click on the "Whitelist IOC" button in the top panel.

IBM QRada	ır						
Dashboard Offenses	Log Activity Network Act	ivity Assets	Reports Ris	ks Vulnerabilities	Admin	Use Case Manager	IntSights Dashboard
12 Return to Event List	Offense 🕜 Map Event 🔸 False F	ositive 🛛 🏠 Extract P	Property 🕜 Previou	s 🔮 Next 👌 Print	Obfuscation	<ul> <li>Whitelist IOC</li> </ul>	
Event Information							
Event Name	IntSights IOC						
Low Level Category	Misc System Event						
Event Description	IOCs from IntSights						
Magnitude			(2)	Relevance	1		
Username	N/A						
Start Time	Jun 7, 2022, 1:16:56 PM			Storage Time	Jun 7, 20	022, 1:16:56 PM	
File Hash (custom)	voohnyqdinl.com						
First Seen Date (custom)	Jan 5, 2020, 1:32:00 AM						
Geo Location (custom)	N/A						
IOC Type (custom)	Domains						
IOC Value (custom)	voohnyqdinl.com						
IoC Match Count (custom)	N/A						
IoC Score (custom)	50						
IoC Severity (custom)	Medium						
IoC Tags (custom)	0						

Figure 24 Whitelisting an IOC

• A prompt will be displayed stating that the IOC is whitelisted successfully.

# Retiring of data in reference set

### **Changing Time to Leave**

Users can change the time after which a reference set will be retired. By default the data retiring times are:

- File hash 180 days
- Domain 90 days
- Email 90 days
- URL 60 days
- IP address 14 days

To change the retiring time follow below steps:

- Navigate to the admin tab in QRadar.
- Open Reference Set Management.
- Click on the reference set for which you want to change the retiring time.
- Click on edit on the top bar of the pop up window.
- Now change the time under "Time to Leave of elements"
- Click on submit to apply the changes.

# Dashboard

### **IOC Overview**

The IOC Overview dashboard provides the details regarding the fetched IOCs from IntSights. It is populated by a background python script that fetches the data for the dashboard every 30 minutes and stores the data into a file named "dashboard\_data.json" under the "Store" folder. The dashboard would be populated with the data from the file whenever the user loads the IOC Overview dashboard.

A "Last updated time" label is provided in the top-right corner of the dashboard, it represents the time the dashboard data was updated last. This dashboard also provides the user to drill down to QRadar's Log Activity tab from each panel. It consists of twelve panels. Users can also export the dashboard into a PDF, by clicking on the "Export as PDF" button.

Each panel is described briefly below:

- **Total IOCs:** The "Total IOCs" panel provides the count of IOCs fetched from IntSights over the last 180 days. Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- New IOCs in Last 7 Days: The "New IOCs in Last 7 Days" panel provides the count of IOCs fetched from IntSights over the last 7 days. Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- New IOCs in Last 24 Hours: The "New IOCs in Last 24 Hours" panel provides the count of IOCs fetched from IntSights over the last 24 hours. Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- **Total IOCs by Type:** The "Total IOCs by Type" panel is a bar-chart panel, it will represent the counts of IOCs fetched within the last 180 days with a bar for each IOC Type. Upon clicking on any bar, the user is redirected to QRadar's Log Activity tab populated with events contributing to the respective IOC Type's bar-count on the panel.
- **Domain IOCs in Last 24 Hours:** The "Domain IOCs in Last 24 Hours" panel provides the count of IOCs fetched in the last 24 hours with IOC Type as "Domains". This panel also provides users with insights into the data flow for Domain IOCs in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched Domain IOCs. Trend will be shown in percentage and trend arrow will be green if the data collected in last 24 hours is less then the data collected in previous 24 hours and red if the data collected in last 24 hours is more then the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- Email Address IOCs in Last 24 Hours: The "Email Address IOCs in Last 24 Hours" panel provides the count of IOCs fetched in the last 24 hours with IOC Type as "Emails". This panel also provides users with insights into the data flow for Email Address IOCs in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched Email Address IOCs. Trend will be shown in percentage and trend arrow will be green if the data collected in last 24 hours is less then the data collected in previous 24 hours and red if the

data collected in last 24 hours is more then the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.

- File Hash IOCs in Last 24 Hours: The "File Hash IOCs in Last 24 Hours" panel provides the count of IOCs fetched in the last 24 hours with IOC Type as "Hashes". This panel also provides users with insights into the data flow for File Hash IOCs in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched File Hash IOCs. Trend will be shown in percentage and trend arrow will be green if the data collected in last 24 hours is less then the data collected in previous 24 hours and red if the data collected in last 24 hours is more then the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- IP Address IOCs in Last 24 Hours: The "IP Address IOCs in Last 24 Hours" panel provides the count of IOCs fetched in the last 24 hours with IOC Type as "IpAddresses". This panel also provides users with insights into the data flow for IP Address IOCs in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched IP Address IOCs. Trend will be shown in percentage and trend arrow will be green if the data collected in last 24 hours is less then the data collected in previous 24 hours and red if the data collected in last 24 hours is more then the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- URL IOCs in Last 24 Hours: The "URL IOCs in Last 24 Hours" panel provides the count of IOCs fetched in the last 24 hours with IOC Type as "Urls". This panel also provides users with insights into the data flow for URL IOCs in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched URL IOCs. Trend will be shown in percentage and trend arrow will be green if the data collected in last 24 hours is less then the data collected in previous 24 hours and red if the data collected in last 24 hours is more then the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- **Total High Severity IOCs:** The "Total High Severity IOCs" panel provides the count of IOCs fetched in the last 180 days with IOC Severity as "High". Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- **Total Medium Severity IOCs:** The "Total Medium Severity IOCs" panel provides the count of IOCs fetched in the last 180 days with IOC Severity as "Medium". Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.
- Total Low Severity IOCs: The "Total Low Severity IOCs" panel provides the count of IOCs fetched in the last 180 days with IOC Severity as "Low". Upon clicking on the panel, the user is redirected to QRadar's Log Activity tab populated with events contributing to the displayed count on the panel.



Figure 25: IOC Overview dashboard

# **Correlation Overview**

The Correlation Overview dashboard provides the details regarding the IOCs matched with the user's QRadar events. It consists of five panels and four filters. The filters available are: IOC Severity, Reporting Feeds, Correlated Log Sources, and Last Correlated Time. The dashboard data is updated as per the selected filter values after clicking the "Go" button. This dashboard also provides the user to drill down to the Correlation Details dashboard from each panel. Users can also export the dashboard into a PDF, by clicking on the "Export as PDF" button. The panels are described briefly below:

- **Total Matched IOCs:** The "Total Matched IOCs" panel provides the count of the number of IOCs correlated with the user's QRadar events(except IntSights log source) within the provided time-range filter value. Upon clicking on the panel, the user is redirected to the Correlation Details dashboard, populated with the details of IOCs that contribute to the count displayed on the panel.
- Total Matched IOCs by Type: The "Total Matched IOCs by Type" is a bar-chart panel. It will represent the count of Matched IOCs with a bar for each type. The user would be able to see the IOC details for each type by clicking on the bar representing respective IOC Type values. Upon clicking on any bar of the panel, the user would be redirected to the Correlation Details dashboard populated with details of IOCs contributing to the bar count displayed on the panel.
- Top 10 Tags Linked with Matched IOCs: The "Top 10 Tags Linked with Matched IOCs" panel provides the top 10 tags linked to the matched IOCs and its count in a tabular format. If values in the Count column are the same then the sorting will happen based on the last Correlated time. The user would be able to see the IOC details for each tag value by clicking on the displayed tag values. Upon clicking on the displayed tag values, the user would be redirected to the Correlation Details dashboard populated with details of IOCs linked to the selected tag value.
- **Top 10 Malwares Linked with Matched IOCs:** The "Top 10 Malwares Linked with Matched IOCs" panel provides the top 10 malwares linked to the matched IOCs and

its count in a tabular format. If values in the Count column are the same then the sorting will happen based on the last Correlated time. The user would be able to see the IOC details for each malware value by clicking on the displayed malware values. Upon clicking on the displayed malware values, the user would be redirected to the Correlation Details dashboard populated with details of IOCs linked to the selected malware value.

• **Top 10 Threat Actors Linked with Matched IOCs:** The "Top 10 Threat Actors Linked with Matched IOCs" panel provides the top 10 threat actors linked to the matched IOCs and their count in a tabular format. If values in the Count column are the same then the sorting will happen based on the last Correlated time. The user would be able to see the IOC details for each threat actor value by clicking on the displayed threat actor values. Upon clicking on threat actor value, the user would be redirected to the Correlation Details dashboard populated with details of IOCs linked to the selected threat actor value.

≡ IBM QRadar											i Ç	<u>0</u>
Dashboard Offenses	Log Activity 1	Network Activity	Assets Rep	orts Ris	sks Vulnerabilities Admin F	Pulse Use Case Manager	IntSights Dashb	ard			System Time:	12:13 PM
IOC Overview Corre	lation Overview	/ Correlati	on Details 🛛 🖌	Alert Over	view Alert Details					6		SHTS
IOC Severity		Reporting F	eeds		Correlated Log Sources	Last Correl	lated Time ays		Go	l	Export as	PDF
Total Matched IOCs					Total Matched IOCs by Type							
	1	5			15 12 9 6 3 0			IP	P Address OC Type			
Top 10 Tags Linked w	th Matched IO	Ēs.			Top 10 Malwares Linked with	Matched IOCs			Top 10 Threat Actors Linked with Match	ed IOCs		
	Tags	÷	Count	÷	Malware	s 🔶	Count	÷	Threat Actors	÷	Count	÷
			15				13				8	
transferrer (			15		100000		7					
			12		-		5					

Figure 26: Correlation Overview dashboard

# **Correlation Details**

The Correlation Details dashboard provides the user with eight filters and one panel. The available filters are IOC Type, IOC Severity, Tags, Malware, Threat Actors, Reporting Feeds, Correlated Log Sources, and Last Correlated Time. The dashboard data is updated as per the selected filter values after clicking the "Go" button. On clicking "View in Log Activity" button, users can view the IOC events in the Log Activity tab, for all the IOCs displayed in the Correlation Details dashboard. Users can export the dashboard into a PDF, by clicking on the "Export as PDF" button (Note: filter values will not be displayed in the exported PDF). The provided panel is described briefly below:

Top 1000 Matched IOCs: The "Top 1000 Matched IOCs" panel provides the details
of the top 1000 most recent Matched IOCs. The user can get enriched information
about an IOC value by clicking on the "Investigate" button (Note: the configured
IntSights account should have the subscription to IntSights Investigate API). On
clicking the "View" button, the user would be redirected to the IntSights portal
displaying information regarding the IOC value. The user can view the events(except

events from IntSights log source) containing the IOC value in their payload by clicking on any IOC value in the table panel.

IBM QRad	ar										() Ç	
oard Offenses	s Log Ac	tivity Netwo	ork Activity A	ssets Reports Risks	Vulnerabilities A	udmin Pulse Use Case Manager	IntSights Dashboard				System Tim	ne: 1
Overview C	Correlation	Overview	Correlation	Details Alert Overview	Alert Details							G
Гуре			OC Severity		Tags	Malware		Threat Actors				
AII			×AII		×AII	×AII		×AII				
rting Feeds		C	Correlated Log	Sources	Last Correlated Tin	ne						
di			×AII		Last 30 Days	Go				Vi	ew in Log A	.cti
o 1000 Matche	d IOCs											
kport as PDF										Search:		
					Last							
∲	¢ Type	Severity	Match Count	Correlated Log	Correlated Time	Reporting Feeds	♦ ♦ Tags Ma	+ Threat +	Last Seen  🍦 Time	∲ Investigate	Redirect to IntSights	þ
100000	IP Address	(40) Medium	1		2023-07-24 17:51:01	Constitution Robins Research Robins (per Your Class	- Care		2023-07-18 00:00:54	Investigate	View	
10000	IP Address	(40) Medium	1		2023-07-24 17:51:01	Losse Constraint States Research States (per Vers March	-		2023-07-18 00:00:54	Investigate	View	
	IP Address	(40) Medium	1		2023-07-24 17:51:01		Sec.		2023-07-18 00:00:54	Investigate	View	
0.00000-09	IP Address	(40) Medium	1	Construction of the later	2023-07-24 17:51:01				2023-07-18 00:00:54	Investigate	View	
	IP Address	(40) Medium	1		2023-07-24 17:51:01	Constantion Rolling Strength Strength Strength			2023-07-18 00:00:54	Investigate	View	
	IP Address	(40) Medium	1		2023-07-24 17:51:01	And American Contra-	il.		2023-07-18 00:00:54	Investigate	View	
	IP Address	(40) Medium	1		2023-07-24 17:51:01	And Design and the Party of the	-		2023-07-18 00:00:54	Investigate	View	
	IP Address	(40) Medium	1		2023-07-24 17:51:01	Contraction States			2023-07-18 00:00:54	Investigate	View	
	IP Address	(40) Medium	1	Constant of Street, or other the street, or other t	2023-07-24 17:51:01	Loss Decision (in the second	See.		2023-07-18 00:00:54	Investigate	View	
-	IP Address	(40) Medium	1		2023-07-24 17:51:01	Course Searching Models Robbinsk Robbinsk (plan Treat Observ	Care .		2023-07-18 00:00:54	Investigate	View	
owing 1 to 10 c	of 15 entries	5				1000				Previous	1 2	_

Figure 27: Correlation Details dashboard

### **Alert Overview**

The Alert Overview dashboard provides the details regarding the fetched Alerts from IntSights.

"Tags" and "Assignee" filters are populated dynamically whenever the user loads this dashboard. The "Flagged Alert" filter is rendered with static values. By default, all the dashboard filters are set to "All".

The checkbox filter "Show only alerts with related IOCs" would be present in the dashboard. Users can check this field and click the Go button. when they want to visualize the dashboard with only alerts that contain related IOC values.

It consists of fourteen panels. Users can also export the dashboard into a PDF, by clicking on the "Export as PDF" button.

Each panel is described briefly below:

- **Total Alerts:** The "Total Alerts" panel provides the count of alerts fetched from IntSights over the last 180 days. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of the recent 1000 alerts ingested over the past 180 days.
- New Alerts in Last 30 Days: The "New Alerts in Last 30 Days" panel provides the count of alerts fetched from IntSights over the last 30 days. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of the recent 1000 alerts ingested over the past 30 days.
- New Alerts in Last 7 Days: The "New Alerts in Last 7 Days" panel provides the count of alerts fetched from IntSights over the last 7 days. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of the recent 1000 alerts ingested over the past 7 days.
- New Alerts in Last 24 Hours: The "New Alerts in Last 24 Hours" panel provides the count of alerts fetched from IntSights over the last 24 hours. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of the recent 1000 alerts ingested over the past 24 Hours.
- **Total Alerts by Type:** The "Total Alerts by Type" panel is a bar-chart panel, it will represent the counts of alerts fetched within the last 180 days with a bar for each Alert Type. Upon clicking on any bar, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the respective Alert Type's bar-count on the panel.
- Attack Indication Alerts in Last 24 Hours: The "Attack Indication Alerts in Last 24 Hours" panel provides the count of alerts fetched in the last 24 hours with Alert Type value "AttackIndication". This panel also provides users with insights into the data flow for Attack Indication alerts in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched Attack Indication alerts. The trend will be shown in percentage and trend arrow will be green if the data collected in the last 24 hours is less than the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.

- Data Leakage Alerts in Last 24 Hours: The "Data Leakage Alerts in Last 24 Hours" panel provides the count of alerts fetched in the last 24 hours with Alert Type value "DataLeakage". This panel also provides users with insights into the data flow for Data Leakage alerts in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched Data Leakage alerts. The trend will be shown in percentage and trend arrow will be green if the data collected in the last 24 hours is less than the data collected in previous 24 hours and red if the data collected in last 24 hours is more than the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.
- Phishing Alerts in Last 24 Hours: The "Phishing Alerts in Last 24 Hours" panel provides the count of alerts fetched in the last 24 hours with Alert Type value "Phishing". This panel also provides users with insights into the data flow for Phishing alerts in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched Phishing alerts. The trend will be shown in percentage and trend arrow will be green if the data collected in the last 24 hours is less than the data collected in previous 24 hours and red if the data collected in last 24 hours is more than the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.
- Brand Security Alerts in Last 24 Hours: The "Brand Security Alerts in Last 24 Hours" panel provides the count of alerts fetched in the last 24 hours with Alert Type value "BrandSecurity". This panel also provides users with insights into the data flow for Brand Security alerts in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched Brand Security alerts. The trend will be shown in percentage and trend arrow will be green if the data collected in the last 24 hours is less than the data collected in previous 24 hours and red if the data collected in last 24 hours is more than the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.
- Exploitable Data Alerts in Last 24 Hours: The "Exploitable Data Alerts in Last 24 Hours" panel provides the count of alerts fetched in the last 24 hours with Alert Type value "ExploitableData". This panel also provides users with insights into the data flow for Exploitable Data alerts in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched Exploitable Data alerts. The trend will be shown in percentage and trend arrow will be green if the data collected in the last 24 hours is less than the data collected in previous 24 hours. Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.
- VIP Alerts in Last 24 Hours: The "VIP Alerts in Last 24 Hours" panel provides the count of alerts fetched in the last 24 hours with Alert Type value "vip". This panel also provides users with insights into the data flow for VIP alerts in the last 24 hours, over the previous 24 hour-cycle. A trend arrow is also provided that represents the change in data flow of fetched VIP alerts. The trend will be shown in percentage and trend arrow will be green if the data collected in the last 24 hours is less than the data collected in previous 24 hours and red if the data collected in last 24 hours is more than the data collected in previous 24 hours 24 hours. Upon clicking on the panel, the user is

redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.

- **Total High Severity Alerts:** The "Total High Severity Alerts" panel provides the count of alerts fetched in the last 180 days with Alert Severity as "High". Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.
- **Total Medium Severity Alerts:** The "Total Medium Severity Alerts" panel provides the count of alerts fetched in the last 180 days with Alert Severity as "Medium". Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.
- **Total Low Severity Alerts:** The "Total Low Severity Alerts" panel provides the count of alerts fetched in the last 180 days with Alert Severity as "Low". Upon clicking on the panel, the user is redirected to the Alert Details dashboard to display the details of alerts contributing to the displayed count on the panel.

≡ IBM QRadar					¢ º
Dashboard Offenses Log Activity	Network Activity Assets Reports	Risks Vulnerabilities Admin Use Ca	se Manager IntSights Dashboard		System Time: 2:52 PM
IOC Overview Correlation Overvi	ew Correlation Details Alert C	verview Alert Details			
Tags	Assignee 🔍 🗐	Flagged Alert	□ Show only alerts with related IOCs	Go	Export as PDF
Total Alerts	New Alerts in	Last 30 Days	New Alerts in Last 7 Days	New Alerts in La	st 24 Hours
12,32	0	12,320	12,32	0 1	2,320
Total Alerts by Type					
14,000 12,000 0,000 0,000 4,000 2,000 2,000 0 	5-15-16-10-14-		Dastadas		
	ExploitableData		Alert Type	Attackingication	
Attack Indication Alerts in Last 24 Hours 12,230	Data Leakage Alerts in Last 24 Hours <b>86</b>	Phishing Alerts in Last 24 Hours	Brand Security Alerts in Last 24 Hours	Exploitable Data Alerts in Last 24 Hours 4	VIP Alerts in Last 24 Hours
→ N/A	→ N/A	→ N/A	→ N/A	→ N/A	→ N/A
Total High Severity Alerts		Total Medium Severity Alerts		Total Low Severity Alerts	
5	5	12,	265		D

Figure 28: Alert Overview dashboard

### **Alert Details**

The Alert Details dashboard provides the user with seven filters and two panels. The available filters are Time Range, Tags, Assignee, Type, Severity, Flagged Alert, and Show only alerts with related IOCs. The dashboard data is updated as per the selected filter values after clicking the "Go" button. On clicking "View in Log Activity" button, users can view the displayed alerts in the Log Activity tab, for all the alerts displayed in the Alert Details dashboard. Users can export the tabular panel into a PDF, by clicking on the "Export as PDF" button (Note: filter values will not be displayed in the exported PDF.). The provided panel is described briefly below:

• **Top 1000 Alerts:** The "Top 1000 Alerts" panel provides the details of the top 1000 most recently ingested alerts. To visualize the image of a specific alert, users have to click on the respective image ID of the alert displayed under the Images column. On clicking the "View" button, the user would be redirected to the IntSights portal displaying information regarding the particular alert. The user can view the particular alert and its parsed properties by clicking on the value of the Alert ID column in the table panel.

∃ IBM QRadar													<b>€</b>
ishboard Offenses Log Act	ivity Netw	rork Activity	Assets Reports Risk	s Vulnerabilities	Admin Pulse	Use Case	Manager IntS	ights Dashboar					System Time: 11:1
OC Overview Correlation	Overview	Correlatio	n Details Alert Overv	iew Alert Deta	ails							(	
me Range	I	Tags		Assignee		Тур	De			Severity			
ast 30 Days	•	×All		×AII			All			×All			
agged Alert	(	Show onl	y alerts with									_	
	<b>`</b> '	elated IOC	s	Go								V	iew in Log Activity
Top 1000 Alerts													
Export as PDF													
												Search:	
Alert ID	Alert Title	Related	mages	Alert Type	Alert Subtype	Alert Severity	Assignees	Found Date	Update Date	Source Type	Source	Source URL	Redirect to
	-												
								2023-07-	2023-07-		2023-07-		
				Attackindication		Medium		28 10:18:26	10:18:26		09:29:46		View
	2												
				AttackIndication		Medium		2023-07-	2023-07-		2023-07-		View
				rational				10:18:15	10:18:15		01:50:00		
				AttackIndication		Madium		2023-07-	2023-07-		2023-07-		Mow
				Attackingication		Wedium		10:18:03	10:18:03		03:23:00		View
			-	AttackIndication		Medium		2023-07- 28	2023-07- 28		2023-07- 28		View
								10:17:50	10:17:50		08:02:00		
								2022.07	2022.07		2022 07		
	and the second s							2023-07-	2023-07-	in mail	2023-07-	And in case of the local data of	and the second s

Figure 29: Alert Details dashboard

# Email XML Template

# XML Template for Email

<template>

<templatename>IntSights Email Template</templatename> <templatetype>event</templatetype> <active>true</active> <filename></filename> <subject>QRadar Correlation Alert: IntSights App for QRadar</subject> <body> Details of Correlated IOC:

Rule Name: \${RuleName} IOC Value: \${body.CustomProperty("IOC Value")} IOC Type: \${body.CustomProperty("IOC Type")} IOC Severity: \${body.CustomProperty("IoC Severity")} Correlated Log Sources: \${body.CustomProperty("Matched Log Sources")} IOC Match Count: \${body.CustomProperty("IoC Match Count")} Last Seen Time: \${body.CustomProperty("Last Seen Date")} IOC Tags: \${body.CustomProperty("IoC Tags")} Related Malware: \${body.CustomProperty("Related Malware")} Threat Actors: \${body.CustomProperty("Related Threat Actors")} Reporting Feeds: \${body.CustomProperty("Reporting Feeds")} </body> <from></from> <to></to> <cc></cc> <bcc></bcc> </template>

# Release notes

### v2.0.0

- Added the configuration page to configure the Alert inputs for collecting alerts.
- Added Alert overview and Alert Details dashboards to visualize ingested alerts.
- Added CEPs and event mappings for alerts data.
- Upgraded QRadar minimum supported version to 7.4.3 GA.

#### v1.2.0

• Added a configurable option "Protocol" on Account Config page to support TCP/UDP protocol for forwarding events.

#### v1.1.0

- Migrated IntSights API endpoints to v2.
- Added a configurable option "Fetch Retired IOCs" on the Input Config page for each IOC Type.

#### v1.0.2

• Resolved the issue of CEPs conflict for "IOC Value" and "IOC Type".

v1.0.1

• Resolved the issue of Internal Server Error on configuration page in QRadar instances with version 7.4.3 FP3 or higher.

# Troubleshooting

This section describes the common issues that might happen during the deployment or the running of the app and the steps to resolve the issues.

### Case #1 – App configuration fails with various error messages

• **Problem:** New configuration fails with error message "401 - Authorized service token is not valid.". Below is a screenshot for quick reference.

Account Config	Input Config	S INTSIGHTS
	Add IntSights Account	×
	Account ID* 63232e1ea479504bfeb3519d API Key* Protocol TCP QRadar Authorization Token* 	dd IntSights Account  PHostname (Without http or https)*  Port*  Require Authentication for Proxy
	401 - Author	rized service token is not valid. Cancel Save

#### Figure 30: Authorization Token error

**Troubleshooting Steps:** This happens when the user has entered the wrong authorization service token, so authentication failed while saving the configuration. Users are recommended to provide the valid authorization service token. For checking logs <u>"Steps to check logs"</u>.

• **Problem:** New configuration fails with error message "IOC Module is not enabled for entered account credentials.". Below is a screenshot for quick reference.

Account Config	Input Config		S
	Add IntSights Account	×	
	Account ID* 63232e1ea479504bfeb3519d API Key* Protocol • TCP ~ QRadar Authorization Token* • • • • • • • • • • • • •	dd IntSights Account IP/Hostname (Without http or https)* Port* Require Authentication for Proxy	
	Support for IOC module or QRadar int credentials.	egration is not enabled for entered account Cancel Save	

Figure 31: IOC Module not enabled Error

**Troubleshooting Steps:** This happens when the user doesn't have a subscription for the IOC module which helps in data collection. So either use credentials which have IOC modules enabled or enable the IOC module and QRadar integration from the IntSights portal. For checking logs <u>"Steps to check logs"</u>.

• **Problem:** New configuration fails with error message "Authentication failed: Invalid credentials". Below is a screenshot for quick reference.

Account Config	Input Config	
	Add IntSights Account	×
	Account ID* 63232e1ea479504bfeb3519d API Key* Protocol • TCP · QRadar Authorization Token* ····································	dd IntSights Account ble Proxy t http or https)* tion for Proxy
	Authentication failed: Invalid credentials.	Cancel Save

Figure 32: Invalid IntSights credentials

**Troubleshooting Steps:** This happens when a user has entered the wrong Account ID/API key for IntSights. Please verify the Account ID and API key. For checking logs <u>"Steps to check logs"</u>

### Case #2 – UI related issues in the app

• **Problem:** Configuration page or dashboard, shows error or unintended behavior.

**Troubleshooting Steps:** Clear the browser cache and reload the webpage.

# Case #3 – Error while initiating socket connection with IBM QRadar, while using QRadar v7.5.0 UP4 with encrypted Apphost deployment

- **Problem:** "Error while initiating socket connection with IBM QRadar. Error = [Errno 111] Connection refused" log message found in log files.
  - While using QRadar v7.5.0 UP4 with an encrypted app host, events wouldn't be forwarded to QRadar via the TCP socket channel.
  - Follow the below steps to check app host connection is encrypted or not?
    - Click on System and License Management in the Admin Panel.
    - Select the host on which the IntSights app for Qradar v7.4.3 GA+ is installed.
    - Click on Deployment Actions in the top panel and select the option Edit Host.
    - A pop-up named Edit Managed Host will open.
    - If "Encrypt Host Connections" field is checked which means apphost connection is encrypted.

#### Troubleshooting Steps:

To prevent this issue users need to make sure that they are using the latest version (v1.2.0) of IntSights QRadar app. Or else users should <u>upgrade the app to v1.2.0</u>.

After upgrading the app to latest version, Users have to modify existing app configurations and specify the UDP protocol for the "Protocol" configurable field in the "Account Config" section.

### Case #4 – Error while initiating socket connection with IBM QRadar

• **Problem:** "Error while initiating socket connection with IBM QRadar" observed in log files.

#### **Troubleshooting Steps:**

This issue might be observed in the QRadar v2 app framework (< v7.4.2 P2). To resolve it, please refer to the following link: <u>https://www.ibm.com/support/pages/node/6395080</u>

### Case #5 – Events are parsed as Unknown or IntSights Message

• Problem: IntSights events are parsed as "Unknown" or "IntSights Message".

#### **Troubleshooting Steps:**

- 1. Go to the Log Source Extensions tab under the Admin section.
- 2. Confirm that "Default for Log Source Types" is "IntSights". If it is not "IntSights" then perform the below steps.

🜔 Log Source Extensions - Google Chrome			-		$\times$
A Not secure   10.0.8.112/console/do	/core/genericsearchlist?appName=event	viewer&pageId=DeviceExtensionList			
Add Fedit Copy Solete Eable	e/Disable 🛛 🛃 Log Sources				0
Extension Name	Description	Enabled	Default for Log Source	Types	
IntSightsCustom_ext		true	IntSights		

#### Figure 33: Log Source Extensions List

- 3. Click on IntSightsCustom\_ext which will download an XML file.
- 4. Log into QRadar console view SSH and execute the following command: /opt/gradar/bin/contentManagement.pl -a search -c 24 -r .\*IntSights
- 5. Copy the ID corresponding to IntSights. If the ID copied is **4002**, then in the XML file, change device-type-id-override="4001" to device-type-id-override="**4002**"
- 6. Click on Upload and select the modified XML file. Select default Log Source Type as "IntSights".
- 7. Click on Save.

8. After clicking on Save, confirm that the value of device-type-id-override is correct for all the extensions. Refer below screenshot:

Log Source Extension - Google Chrome	-	$\rightarrow$
Not secure   10.0.8.112/console/do/sem/mai	tain Device Extension? dispatch = edit & app Name = event viewer & page Id = Device Extension List & id = 51	
dit a Log Source Extension		0
Name           Description           Log Source Types           Available           3Com 8800 Series Switch           APC UPS           AhnLab Policy Center APC           Akamai KONA           Amazon AWS Application Load Balance           Amazon AWS Substic Kubernetes Servi           Amazon AWS Static Kubernetes Servi           Amazon AWS Security Hub           Amazon AWS WAF           Upload Extension:           Choose File           No file ch           Extension Document <ns2: <="" device-extension="" td="" xmlns:ns2="event">           valtern id="EventCategory-Pattern-1" type          valtern id="EventCategory-Pattern-1" type           valtern id="EventCategory-Pattern-1" type           valtern id="EventStrutions="tri           valtern id="AllEvents" type="JavaPattern"           vent-matcher enable-substitutions="tri           vent-matcher enable-substitutions="tri           vent-matcher group-</ns2:>	set to default for set to default for f Access Log r Access Log parsing/device_extension"> parsing/device_extension"> perlLeefKey?SeventdS "LeefKey?SeventdS "LeefKey?SeventdS "LeefKey?SeventdS "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate" "JoonKeypath">/"lastUpdateDate"	

Figure 34: Edit a Log Source Extension

### Case #6 – IntSights events are shown up as "IntSights Message"

• **Problem:** IntSights events will show up as IntSights Message rather than getting identified as the right QRadar category. This will be seen in the "Log Activity" tab in QRadar when a user might be searching for an event of IntSights log source type.

#### Troubleshooting Steps:

This issue is caused when the required field is not present in the raw event or the event payload size is more than 4096 bytes which leads to the breaking of the event payload. If the payload is getting truncated, users can increase the maximum payload size. 4096 is the default size configured in the QRadar platform. Follow the below steps to increase max payload size in QRadar:

- 1. Navigate to System settings by going to the Admin panel.
- 2. Click on the button under Switch To  $\rightarrow$  **Advanced**.
- 3. There are two options: Max TCP Syslog Payload Length and Max UDP Syslog Payload Length. Below is a screenshot for quick reference:

System Settings		
Quelers Quellana	<ul> <li>System Settings</li> </ul>	
system settings	Administrative Email Address	root@localhost
Database Settings	Alert Email From Address	QRADAR@localhost.localdomain
Ariel Database Settings	Email Locale	English ·
Custom Rule Settings	Max Email Attachment Size (KB)	15,360
	Delete Root Mail	Yes *
ransaction Sentry Settings	Temporary Files Retention Period	6 hours *
NMP Settings	Asset Profile Query Period	1 day(default)
mbedded SNMP Daemon	Coalescing Events	Yes 👻
ettings	Store Event Payload	Yes *
sset Profile Settings	Global Iptables Access (comma separated)	
console Settings	Syslog Event Timeout (minutes)	720
	Partition Testers Timeout (seconds)	30
uthentication Settings	Max UDP Syslog Payload Length	1,024
NS Settings	Max TCP Syslog Payload Length	4,096
VINS Settings	The maximum payload length (characters) displayed for TCP systoms.	2,500
enorting Cattings	HIGA TOF SYSIOD OFFICIOUST BETTOST	10 *
reporting actungs	Timeout for Idle TCP Syslog Connections (seconds)	900
ata Export Settings	Log and Network Activity Data Export Temporary Directory	/store/exports
Flow Settings	Display Country/Region Flags	Yes *
Dadar Makuark Ineiakte Cattinae	<ul> <li>Display Embedded Maps in IP Address Tooltips</li> </ul>	Yes *
	Enable X-Force Threat Intelligence Feed	No *
Switch to:	Lag time to remove expired reference data (minutes)	5
Basic	Database Settings	
	User Data Files	/store/users/
	Accumulator Retention - Minute-by-Minute	1 week (default) *

Figure 35: System Settings

- 4. Increase the value of these fields according to need (Recommended: 32000)
- 5. Click on Deploy Changes. It is recommended to choose the full deploy option.

### Case #7 – Internal Server Error while opening configuration page

• **Problem:** "Internal Server Error: the server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application. Refer to the below screenshot



Figure 36: Internal server error in IntSights app configuration page

**Troubleshooting Steps:** This issue is caused when a user tries to open a configuration page in QRadar instances with version 7.4.3FP3 or higher. To resolve this issue upgrade to IntSights App For QRadar(v1.0.2+)

### Case #8 – All other issues which are not a part of the Document

• **Problem:** If the problem is not listed in the document, please follow below steps.

Troubleshooting Steps: Please follow below steps to generate log files:

1. Click on System and License Management in the Admin Panel.

- 2. Select the host on which the tab IntSights app for Qradar v7.4.3 GA+ is installed.
- 3. Click on Actions in the top panel and select the option Collect Log Files.
- 4. A pop-up named Log File Collection will open.
- 5. Click on Advance Options.
- 6. Select the checkbox to Include Debug Logs, Application Extension Log, Setup Log (Current Version).
- 7. Click on Collect Log Files Button after selecting 5 days as data input.
- 8. Click on "Click here to download files".
- 9. This will download all the log files in a single zip on your local machine.