Qualys Context XDR v1.x

Release Notes

Version 1.0.3

April 14, 2022

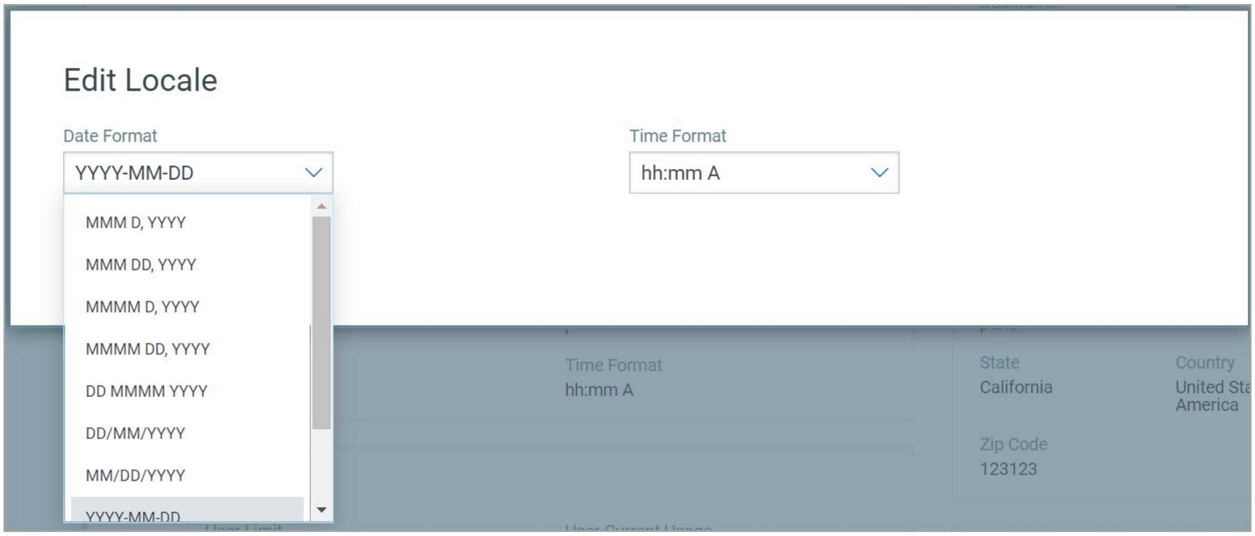
Here’s what’s new in Qualys Context XDR 1.0.3!

Context XDR 1.0.3 brings you more improvements and updates!

Set Date and Time Format

We have now introduced settings to configure the date and time in a required format. The date format you configure will then be applicable to all the dates and time stamps in the application.

Let us consider the example the current date format of Event Time on the Events tab is DD/MM/YYYY. To change this format, click the Profile icon and select View Profile from the menu. Click the edit icon in the Locale section of the Profile Information tab. Choose the required date and time format from the drop-down options and click **Save**. Now you can view the updated date and time format on the Events tab.



Edit Locale

Date Format: YYYY-MM-DD

Time Format: hh:mm A

Time Format: hh:mm A

State: California

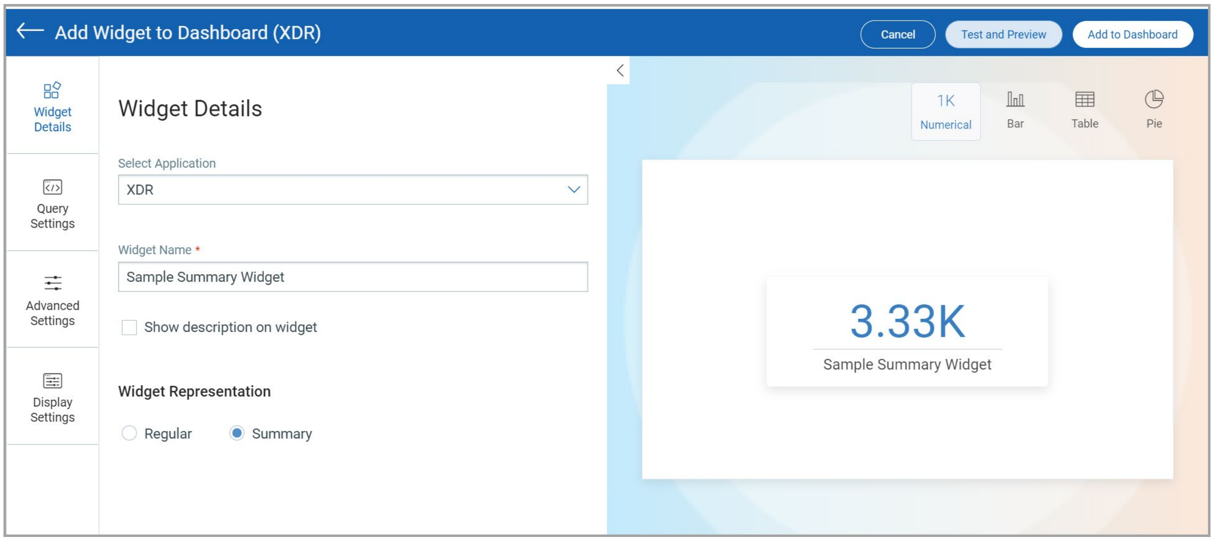
Country: United Sta America

Zip Code: 123123

Summary Card for Widgets on Dashboards

We have now introduced a new widget representation: Summary option only for Numerical type (Count) of widgets. You can view data in a summarized format to accommodate more number of widgets and data on a dashboard.

Navigate to the widget template library from your dashboard, click **Build Your Widget** and select **XDR** as the application. Choose **Numerical** as the widget type. Define the other required fields such as name and description.



Widget Details

Select Application: XDR

Widget Name *: Sample Summary Widget

□ Show description on widget

Widget Representation

○ Regular ● Summary

3.33K

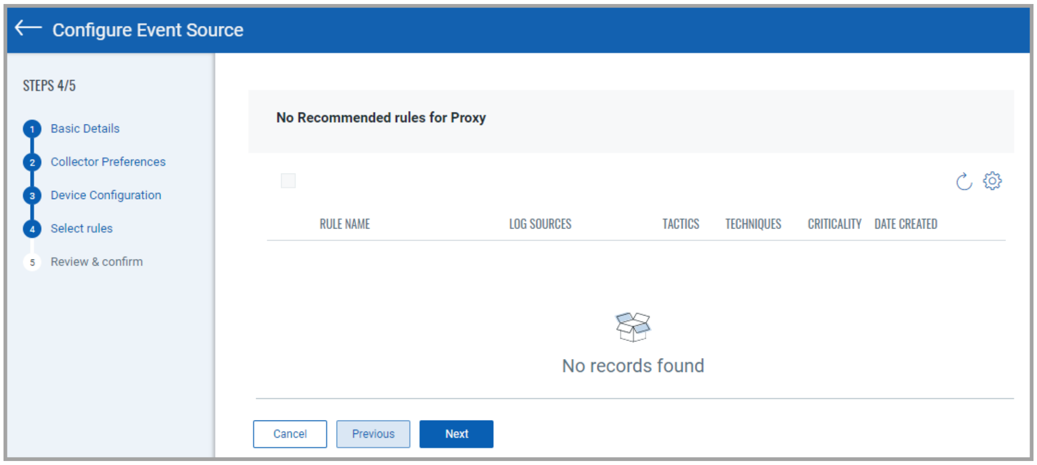
Sample Summary Widget

You can now choose Widget Representation to decide if the information to be presented in the count widget should be Regular or Summary.
- **Regular**: Choose to create the regular-sized numerical widget.
- **Summary**: Choose to create a small-sized compact numerical widget. You can use compact widgets to accommodate more number of widgets and data in a dashboard. Because the widgets are compact, you cannot resize the widget.

Out-of-the-box Experience - Default Rules

With this release, Context XDR provides you with the list of recommended default rules associated with the log source while configuration. You can view and select the rules to quickly activate them when the source is configured.

You can select the default rules from **Configuration** > **Data Collection** > **Catalog** and select any source from the list for configuration. You can view and select the default/recommended rules listed on the **Select rules** step and proceed to next steps for configuration.



Configure Event Source

STEPS 4/5

1. Basic Details
2. Collector Preferences
3. Device Configuration
4. Select rules
5. Review & confirm

No Recommended rules for Proxy

RULE NAME	LOG SOURCES	TACTICS	TECHNIQUES	CRITICALITY	DATE CREATED

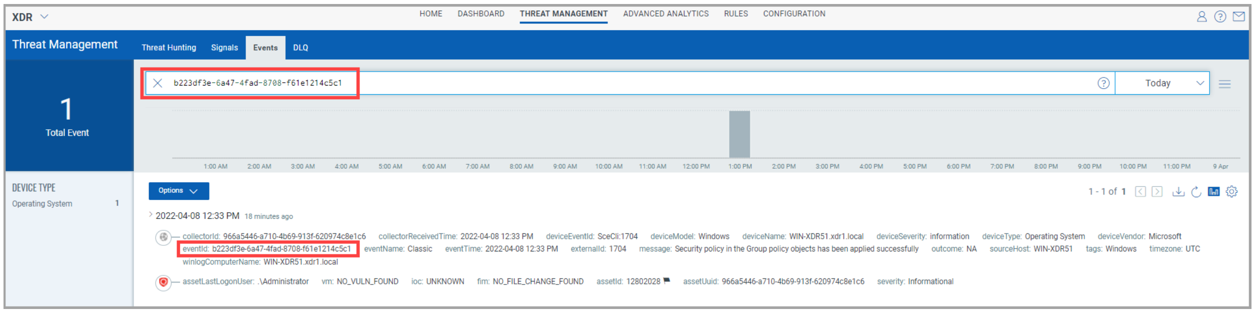
No records found

You can either access the default rules configuration step while configuring a new profile from the cloud agent profiles section.

Freeform Search for Raw Log Ingestion

We have newly introduced a freeform search that defines a way of searching events data in which we do not provide tokens as we do in QQL search. Freeform search will take only text and search across all the applicable fields in the event's index.

Navigate to **Threat Management** > **Events**. For example, you want to search the eventId with result '**b223df3e-6a47-4fad-8708-f61e1214c5c1'**, simply enter the value in search bar and you view the below results.



b223df3e-6a47-4fad-8708-f61e1214c5c1

1
Total Event

DEVICE TYPE
Operating System 1

2022-04-08 12:33 PM 18 minutes ago

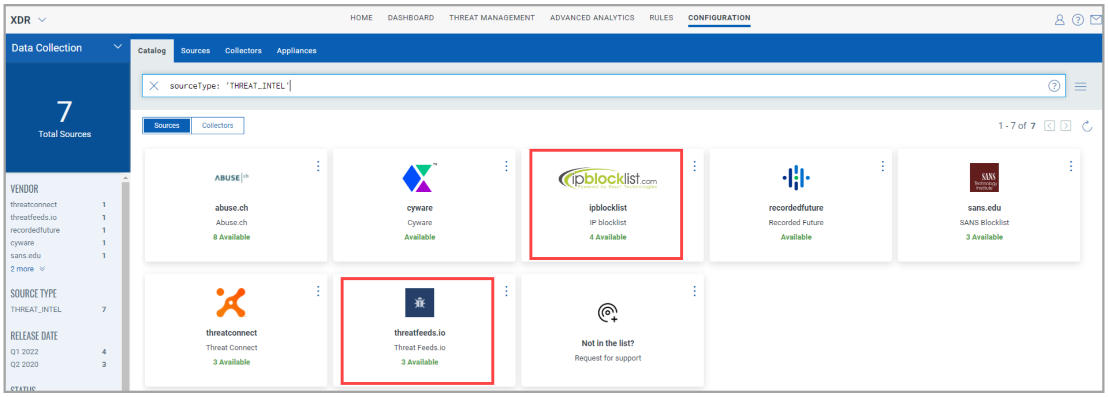
collectorId: 966a5446-a710-4b69-913f-620974c8e1c6 collectorReceivedTime: 2022-04-08 12:33 PM deviceEventId: SceCli:1704 deviceModel: Windows deviceName: WIN-XDR51.xdr1.local deviceSeverity: information deviceType: Operating System deviceVendor: Microsoft eventId: b223df3e-6a47-4fad-8708-f61e1214c5c1 eventName: Classic eventTime: 2022-04-08 12:33 PM externalId: 1704 message: Security policy in the Group policy objects has been applied successfully outcome: NA sourceHost: WIN-XDR51 tags: Windows timezone: UTC winlogComputerName: WIN-XDR51.xdr1.local

assetLastLogonUser: .\Administrator vm: NO_VULN_FOUND ioc: UNKNOWN fim: NO_FILE_CHANGE_FOUND assetId: 12802028 assetUuid: 966a5446-a710-4b69-913f-620974c8e1c6 severity: Informational

New Sources for Threat Intel Feeds

With this release, we have enhanced our threat intelligence with the support of two new threat sources that are added: Threatfeeds.io and Ipblocklist.

Navigate to **Configuration** > **Data Collection** > **Catalog** > and select source type as 'Threat Intel' from the left pane filters. You can locate the newly added threat sources in the Sources sub-tab.



sourceType: 'THREAT_INTEL'

7 Total Sources

VENDOR	
threatconnect	1
threatfeeds.io	1
recordedfuture	1
cyware	1
sans.edu	1
2 more	
SOURCE TYPE	
THREAT_INTEL	7
RELEASE DATE	
Q1 2022	4
Q2 2020	3
STATUS	

abuse.ch
Abuse.ch
8 Available

cyware
Cyware
Available

ipblocklist
IP blocklist
4 Available

recordedfuture
Recorded Future
Available

sans.edu
SANS Blocklist
3 Available

threatconnect
Threat Connect
3 Available

threatfeeds.io
Threat Feeds.io
3 Available

Not in the list?
Request for support

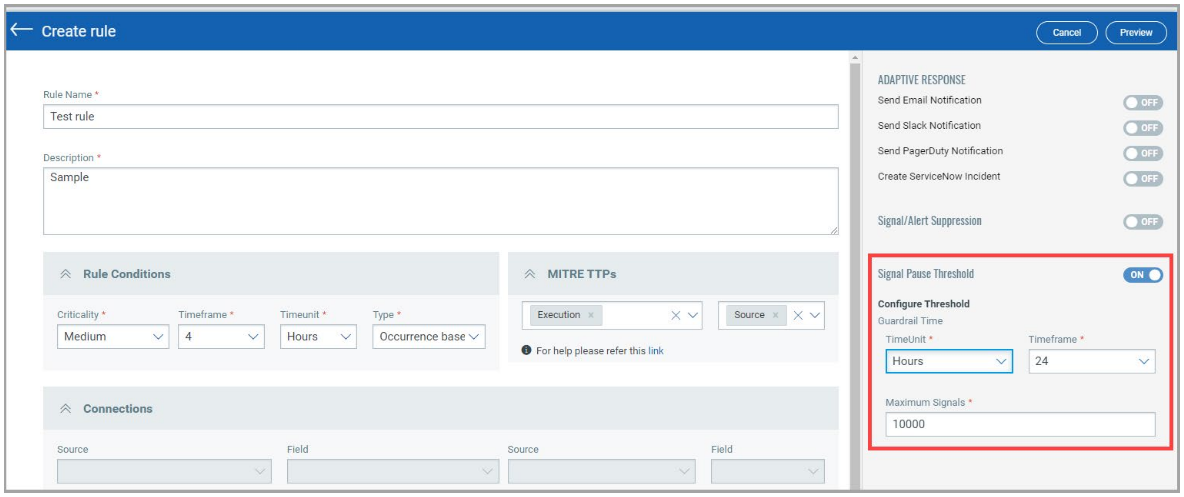
Threshold Settings to Pause Signals

We have newly introduced a **Signal Pause Threshold** feature. For every rule, the "**Signal Pause Threshold**" is enabled with the following defined values.

- Max count: 10k
- Time Unit: 24Hours

The **Maximum Signals** is applied for every rule and when a single rule generates the configured maximum in the defined time period (10k in 24 hours by default), that rule/signal stops producing signals until the defined **Timeframe** expires.

An alert is generated to the administrator, when this condition is triggered to ensure the administrator is notified that the threshold is reached. Then, you able to edit/change the threshold values for continuing generating signals. kindly note that the updated settings will get activated in the next schedule.



Rule Name *: Test rule

Description *: Sample

Criticality *: Medium | Timeframe *: 4 | Timeunit *: Hours | Type *: Occurrence base

MITRE TTPs: Execution | Source

ADAPTIVE RESPONSE
Send Email Notification: OFF
Send Slack Notification: OFF
Send PagerDuty Notification: OFF
Create ServiceNow Incident: OFF

Signal/Alert Suppression: OFF

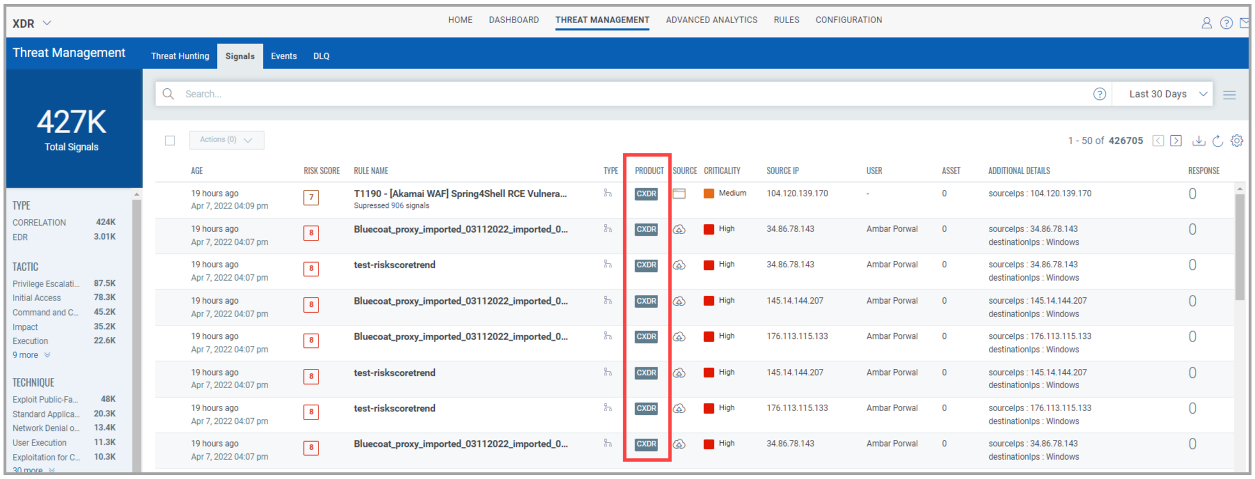
Signal Pause Threshold: ON
Configure Threshold
Guardrail Time
TimeUnit *: Hours
Timeframe *: 24
Maximum Signals *: 10000

You can override this with Admin activate option from the quick actions drop-down menu for each rule that are in Threshold paused Status.

Integration with EDR

We have now integrated EDR with XDR, where we can now view signals from Qualys EDR, if you have active Qualys EDR subscription.

Navigate to **Threat Management** > **Signals** and filter the **Product** column for **EDR** to view the signals coming from Qualys EDR.



427K
Total Signals

TYPE	
CORRELATION	424K
EDR	3.01K

TACTIC	
Privilege Escalati...	87.5K
Initial Access	78.3K
Command and C...	45.2K
Impact	35.2K
Execution	22.6K
9 more	

TECHNIQUE	
Exploit Public-Fa...	48K
Standard Applica...	20.3K
Network Denial o...	13.4K
User Execution	11.3K
Exploitation for C...	10.3K
30 more	

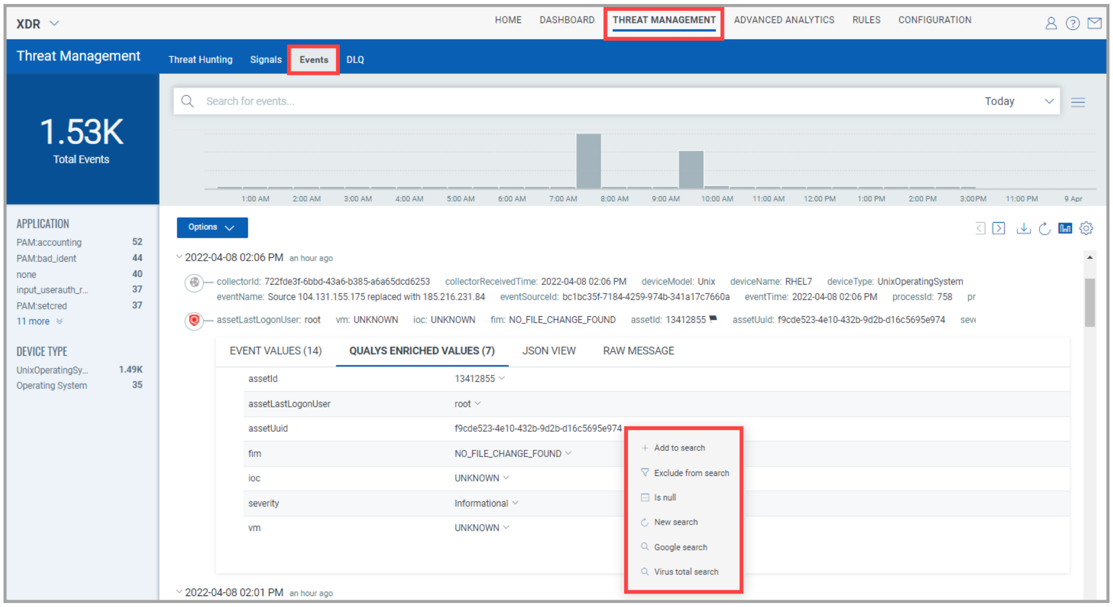
AGE	RISK SCORE	RULE NAME	TYPE	PRODUCT	SOURCE	CRITICALITY	SOURCE IP	USER	ASSET	ADDITIONAL DETAILS	RESPONSE
19 hours ago Apr 7, 2022 04:09 pm	7	T1190 - [Akamai WAF] Spring4Shell RCE Vulnera... Supressed 906 signals		CXDR		Medium	104.120.139.170	-	0	sourceIps : 104.120.139.170	
19 hours ago Apr 7, 2022 04:07 pm	8	Bluecoat_proxy_imported_03112022_imported_0...		CXDR		High	34.86.78.143	Ambar Porwal	0	sourceIps : 34.86.78.143 destinationIps : Windows	
19 hours ago Apr 7, 2022 04:07 pm	8	test-riskscoretrend		CXDR		High	34.86.78.143	Ambar Porwal	0	sourceIps : 34.86.78.143 destinationIps : Windows	
19 hours ago Apr 7, 2022 04:07 pm	8	Bluecoat_proxy_imported_03112022_imported_0...		CXDR		High	145.14.144.207	Ambar Porwal	0	sourceIps : 145.14.144.207 destinationIps : Windows	
19 hours ago Apr 7, 2022 04:07 pm	8	Bluecoat_proxy_imported_03112022_imported_0...		CXDR		High	176.113.115.133	Ambar Porwal	0	sourceIps : 176.113.115.133 destinationIps : Windows	
19 hours ago Apr 7, 2022 04:07 pm	8	test-riskscoretrend		CXDR		High	145.14.144.207	Ambar Porwal	0	sourceIps : 145.14.144.207 destinationIps : Windows	
19 hours ago Apr 7, 2022 04:07 pm	8	test-riskscoretrend		CXDR		High	176.113.115.133	Ambar Porwal	0	sourceIps : 176.113.115.133 destinationIps : Windows	
19 hours ago Apr 7, 2022 04:07 pm	8	Bluecoat_proxy_imported_03112022_imported_0...		CXDR		High	34.86.78.143	Ambar Porwal	0	sourceIps : 34.86.78.143 destinationIps : Windows	

New Improvements Added for Drilldown on Event Details

We have introduced new **drilldown** search menu options in the **Events** tab of **Threat Management**.

In the **Events** tab, you can run a drilldown search when you click on these parts of an event. The drilldown searches can perform the following actions for fields, tags, and event segments.

Simply, click **Threat Management** > **Events** and click on any of the parts of an event to see the drilldown search options.



APPLICATION	
PAM:accounting	52
PAM:bad_ident	44
none	40
input_userauth_r...	37
PAM:setcred	37
11 more	

DEVICE TYPE	
UnixOperatingSy...	1.49K
Operating System	35

2022-04-08 02:06 PM an hour ago

collectorId: 722fde3f-6bbd-43a6-b385-a6a65dcd6253 collectorReceivedTime: 2022-04-08 02:06 PM deviceModel: Unix deviceName: RHEL7 deviceType: UnixOperatingSystem eventName: Source 104.131.155.175 replaced with 185.216.231.84 eventSourceId: bc1bc35f-7184-4259-974b-341a17c7660a eventTime: 2022-04-08 02:06 PM processId: 758 pr

assetLastLogonUser: root vm: UNKNOWN ioc: UNKNOWN fim: NO_FILE_CHANGE_FOUND assetId: 13412855 assetUuid: f9cde523-4e10-432b-9d2b-d16c5695e974 sev

assetId	13412855
assetLastLogonUser	root
assetUuid	f9cde523-4e10-432b-9d2b-d16c5695e974
fim	NO_FILE_CHANGE_FOUND
ioc	UNKNOWN
severity	Informational
vm	UNKNOWN

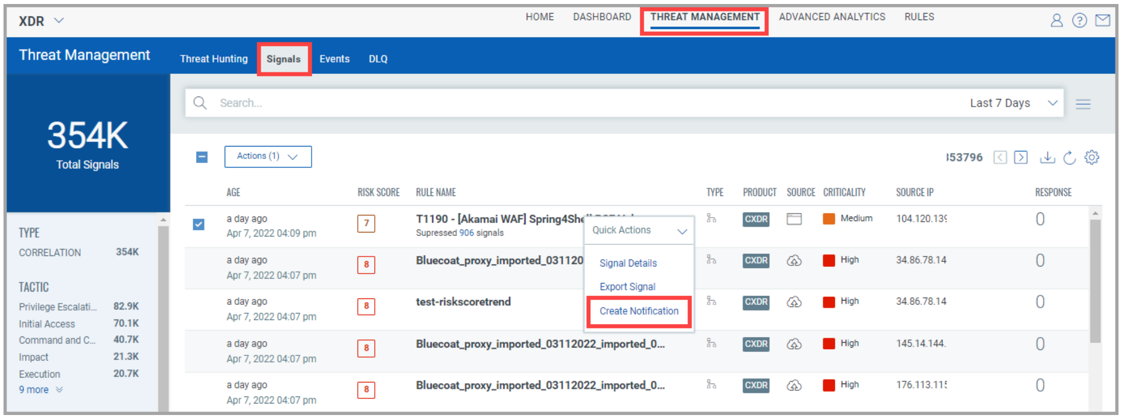
2022-04-08 02:01 PM an hour ago

- **New Search** - Create and populate a new QQL search on the search bar for that specific item.
- **Exclude from Search** - Update the current QQL search bar with an exclusion statement for the selected item.
- **Add to Search** - Update the current QQL search bar with this as a criteria statement for the selected item.
- **Google Search** - Launch a new tab and perform a google search for that item.
- **Virus Total Search** - Limited to hashes, domains, file names, host names and IP addresses - Launch a new tab and perform a Virus Total search for the item.
- **Asset Information** - Get Qualys Cloud agent information.

Configure Notification for Signals

We have newly added **Create Notification** option in the quick action menu of Signals tab under threat management.

You can set up notifications for each signal manually to send out notification. You can create new notification templates for Email, Slack, Pager, and ServiceNow. Navigate to **Threat Management** > **Signals** and select any of the event for Quick Actions menu click **Create Notification**.



TYPE

CORRELATION	354K

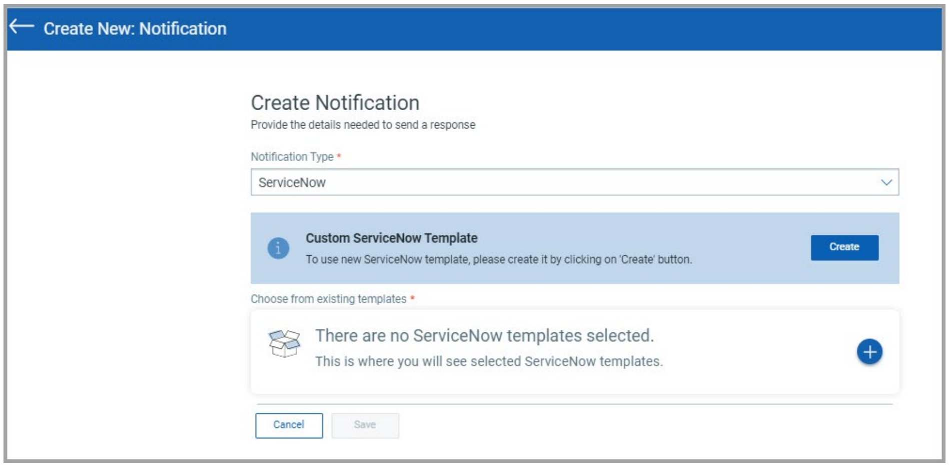
TACTIC

Privilege Escalati...	82.9K
Initial Access	70.1K
Command and C...	40.7K
Impact	21.3K
Execution	20.7K

9 more

	AGE	RISK SCORE	RULE NAME	TYPE	PRODUCT	SOURCE	CRITICALITY	SOURCE IP	RESPONSE
☑	a day ago Apr 7, 2022 04:09 pm	7	T1190 - [Akamai WAF] Spring4She... Supressed 906 signals		CXDR		Medium	104.120.139	0
	a day ago Apr 7, 2022 04:07 pm	8	Bluecoat_proxy_imported_031120...		CXDR		High	34.86.78.14	0
	a day ago Apr 7, 2022 04:07 pm	8	test-riskscoretrend		CXDR		High	34.86.78.14	0
	a day ago Apr 7, 2022 04:07 pm	8	Bluecoat_proxy_imported_03112022_imported_0...		CXDR		High	145.14.144.	0
	a day ago Apr 7, 2022 04:07 pm	8	Bluecoat_proxy_imported_03112022_imported_0...		CXDR		High	176.113.115	0

Select the **Notification Type** and click **Create** to create a new response template or you can choose from the existing templates and click **Save**, and the notification is triggered.



Create Notification

Provide the details needed to send a response

Notification Type *: ServiceNow

Custom ServiceNow Template
To use new ServiceNow template, please create it by clicking on 'Create' button.

Choose from existing templates *

There are no ServiceNow templates selected.
This is where you will see selected ServiceNow templates.