Qualys Context XDR v1.x

Release Notes

Version 1.0.1

March 14, 2022

Here’s what’s new in Qualys Context XDR 1.0.1!

Enhancement of Palo Alto GlobalProtect VPN Device Fields

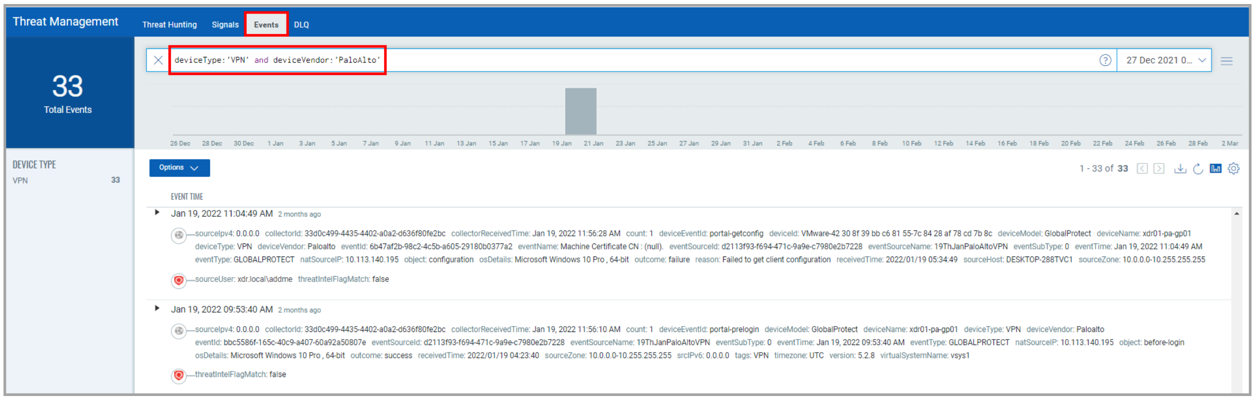
Quick Filters Added on the Signals Tab

Onboarded Forcepoint Proxy Source

Delete Option for Response Templates

Enhancement of Palo Alto GlobalProtect VPN Device Fields

You can now view the newly added enhanced fields for Global Protect VPN. Simply, click **Threat Management > Events** tab to view the detected history of event logs. Then, use search tokens filter with ‘`deviceType`’ and ‘`deviceVendor`’ to view the most recent events.

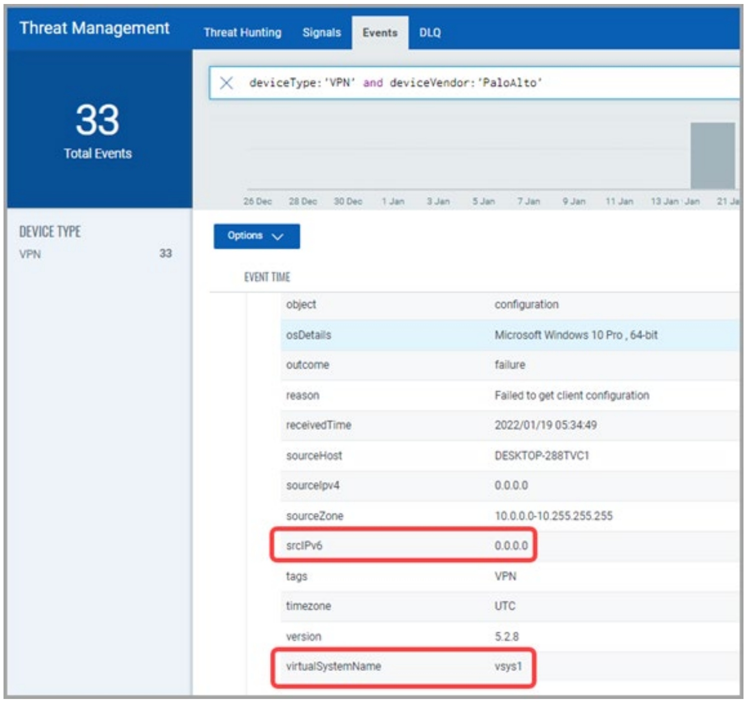


```
deviceType:'VPN' and deviceVendor:'PaloAlto'
```

```
EVENT TIME
Jan 19, 2022 11:04:49 AM 2 months ago
sourceIpv4: 0.0.0.0  collectorId: 33d0c499-4435-4402-a0a2-d636f80fe2bc  collectorReceivedTime: Jan 19, 2022 11:56:28 AM  count: 1  deviceEventId: portal-getconfig  deviceId: VMware-42 30 8f 39 bb c6 81 55-7c 84 28 af 78 cd 7b 8c  deviceModel: GlobalProtect  deviceName: xdr01-pa-gp01
deviceType: VPN  deviceVendor: Paloalto  eventId: 6b47af2b-98c2-4c5b-a605-29180b0377a2  eventName: Machine Certificate CN : (null).  eventSourceId: d2113f93-f694-471c-9a9e-c7980e2b7228  eventSourceName: 19ThJanPaloAltoVPN  eventSubType: 0  eventTime: Jan 19, 2022 11:04:49 AM
eventType: GLOBALPROTECT  natSourceIP: 10.113.140.195  object: configuration  osDetails: Microsoft Windows 10 Pro , 64-bit  outcome: failure  reason: Failed to get client configuration  receivedTime: 2022/01/19 05:34:49  sourceHost: DESKTOP-288TVC1  sourceZone: 10.0.0.0-10.255.255.255
sourceUser: xdr.local\addme  threatIntelFlagMatch: false

Jan 19, 2022 09:53:40 AM 2 months ago
sourceIpv4: 0.0.0.0  collectorId: 33d0c499-4435-4402-a0a2-d636f80fe2bc  collectorReceivedTime: Jan 19, 2022 11:56:10 AM  count: 1  deviceEventId: portal-prelogin  deviceModel: GlobalProtect  deviceName: xdr01-pa-gp01  deviceType: VPN  deviceVendor: Paloalto
eventId: bbc5586f-165c-40c9-a407-60a92a50807e  eventSourceId: d2113f93-f694-471c-9a9e-c7980e2b7228  eventSourceName: 19ThJanPaloAltoVPN  eventSubType: 0  eventTime: Jan 19, 2022 09:53:40 AM  eventType: GLOBALPROTECT  natSourceIP: 10.113.140.195  object: before-login
osDetails: Microsoft Windows 10 Pro , 64-bit  outcome: success  receivedTime: 2022/01/19 04:23:40  sourceZone: 10.0.0.0-10.255.255.255  srcIPv6: 0.0.0.0  tags: VPN  timezone: UTC  version: 5.2.8  virtualSystemName: vsys1
threatIntelFlagMatch: false
```

Click on any event to view the enhanced fields. The newly added fields are method, natSourceIP, sourceIpv6, deviceId, count, module, and virtualSystemName.



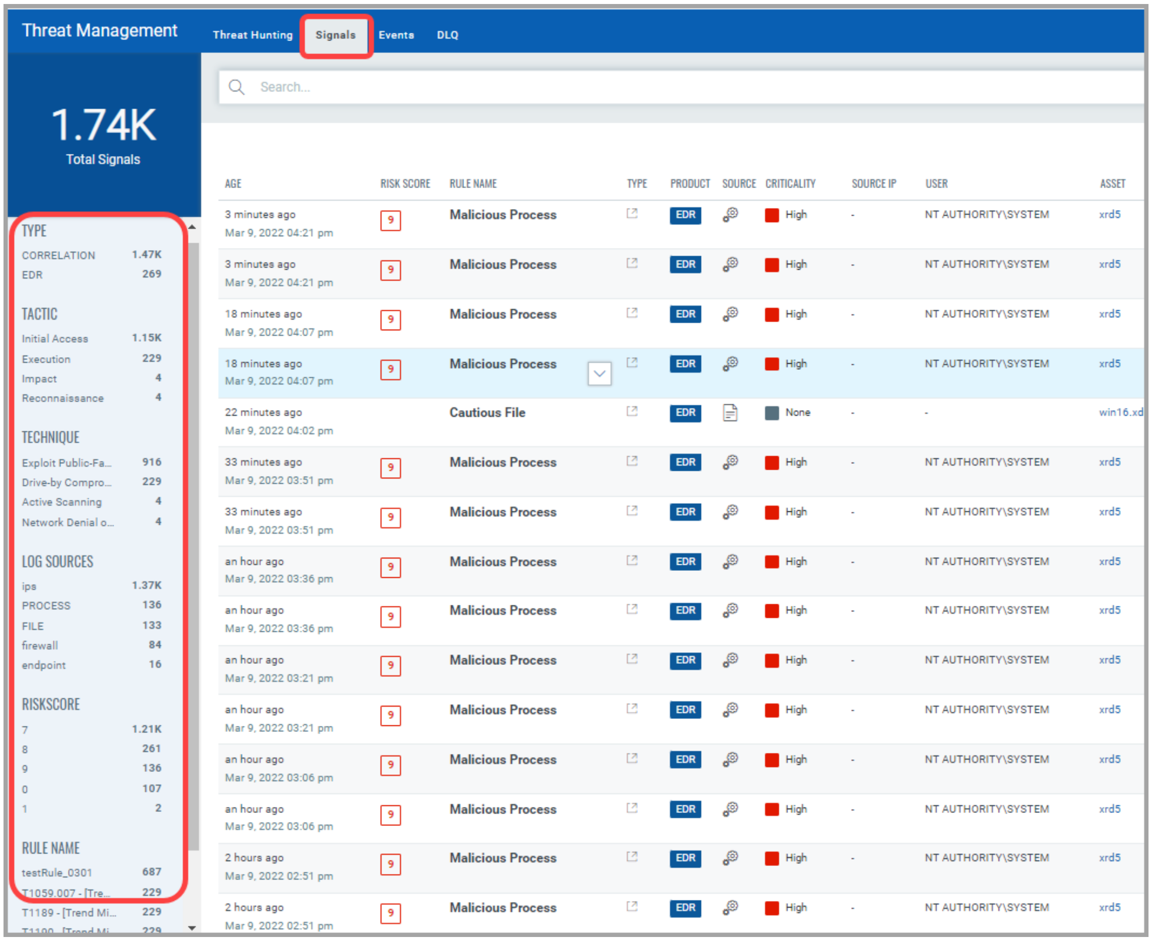
```
deviceType:'VPN' and deviceVendor:'PaloAlto'
```

object	configuration
osDetails	Microsoft Windows 10 Pro , 64-bit
outcome	failure
reason	Failed to get client configuration
receivedTime	2022/01/19 05:34:49
sourceHost	DESKTOP-288TVC1
sourceIpv4	0.0.0.0
sourceZone	10.0.0.0-10.255.255.255
srcIPv6	0.0.0.0
tags	VPN
timezone	UTC
version	5.2.8
virtualSystemName	vsys1

Quick Filters Added on the Signals Tab

We have introduced new quick filters on the **Signals** tab of **Threat Management**. You can now view the newly added quick filters **Type**, **Tactic**, **Technique**, **Log sources**, **Riskscore**, and **Rule name** in the left pane.

Now, you can easily use the above-mentioned filters to view various details you are looking out for. For example, if you need to view all logs sources from firewall, just click **firewall** under **Log Sources** to view all logs from firewall.



1.74K
Total Signals

TYPE	
CORRELATION	1.47K
EDR	269

TACTIC	
Initial Access	1.15K
Execution	229
Impact	4
Reconnaissance	4

TECHNIQUE	
Exploit Public-Fa...	916
Drive-by Compro...	229
Active Scanning	4
Network Denial o...	4

LOG SOURCES	
ips	1.37K
PROCESS	136
FILE	133
firewall	84
endpoint	16

RISKSCORE	
7	1.21K
8	261
9	136
0	107
1	2

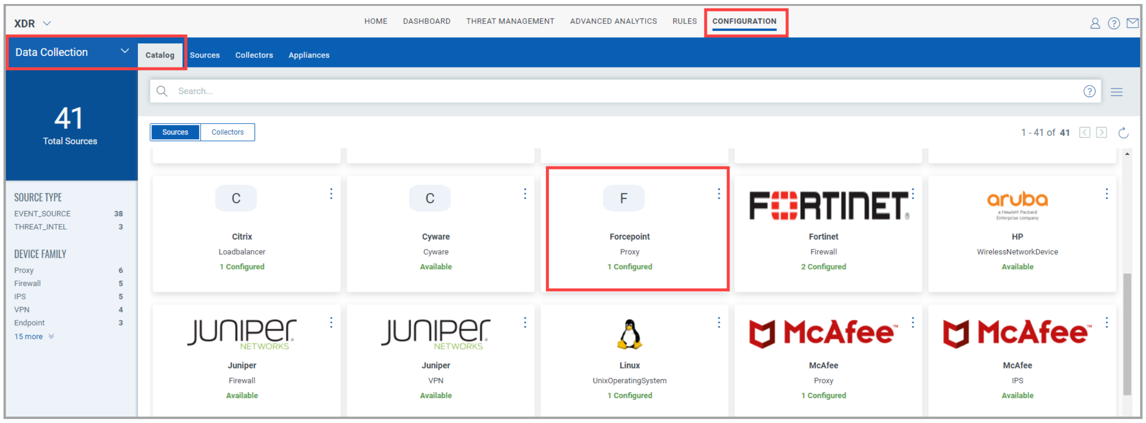
RULE NAME	
testRule_0301	687
T1059.007 - [Tre...	229
T1189 - [Trend Mi...	229
T1190 - [Trend Mi...	229

AGE	RISK SCORE	RULE NAME	TYPE	PRODUCT	SOURCE	CRITICALITY	SOURCE IP	USER	ASSET
3 minutes ago Mar 9, 2022 04:21 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
3 minutes ago Mar 9, 2022 04:21 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
18 minutes ago Mar 9, 2022 04:07 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
18 minutes ago Mar 9, 2022 04:07 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
22 minutes ago Mar 9, 2022 04:02 pm		Cautious File	↗	EDR	🗎	■ None	-	-	win16.xd
33 minutes ago Mar 9, 2022 03:51 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
33 minutes ago Mar 9, 2022 03:51 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
an hour ago Mar 9, 2022 03:36 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
an hour ago Mar 9, 2022 03:36 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
an hour ago Mar 9, 2022 03:21 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
an hour ago Mar 9, 2022 03:21 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
an hour ago Mar 9, 2022 03:06 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
an hour ago Mar 9, 2022 03:06 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
2 hours ago Mar 9, 2022 02:51 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5
2 hours ago Mar 9, 2022 02:51 pm	9	Malicious Process	↗	EDR	⚙	🟥 High	-	NT AUTHORITY\SYSTEM	xrd5

Onboarded Forcepoint Proxy Source

We now support **Forcepoint Proxy** data source to ingest the event logs. You can configure Forcepoint proxy source by simply clicking on **Configuration** > **Data Collection** > **Catalog** > **Forcepoint Proxy**.

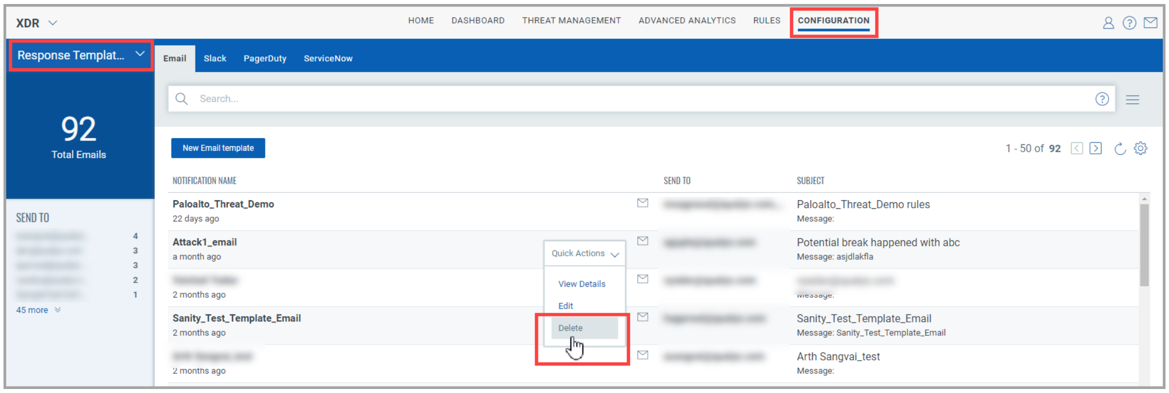
To know the detailed steps for configuration, refer to Collect logs from 3rd party data sources section in the online help.



Delete Option for Response Templates

We have introduced a quick action menu to delete the existing response notification templates for **Email**, **Slack**, **PagerDuty**, and **ServiceNow**.

Simply, click **Configuration** > **Response Templates** > **Email** to view all the existing notification templates. Then select any of the existing notification template and click the **Quick Actions** menu, and click **Delete** to delete the selected notification template. You can delete a template only if it is not used in any rule. If you attempt to delete a template that is used in a rule, you will be prompted to remove the template from any associated rules before you delete.



NOTIFICATION NAME	SEND TO	SUBJECT
Paloalto_Threat_Demo 22 days ago	[redacted]	Paloalto_Threat_Demo rules Message:
Attack1_email a month ago	[redacted]	Potential break happened with abc Message: asjdlakfla
[redacted] 2 months ago	[redacted]	[redacted] Message:
Sanity_Test_Template_Email 2 months ago	[redacted]	Sanity_Test_Template_Email Message: Sanity_Test_Template_Email
[redacted] 2 months ago	[redacted]	Arth Sangvai_test Message: