



# Qualys Context XDR v1.x

## Release Notes

Version 1.0.6

June 29, 2022

Here's what's new in Qualys Context XDR 1.0.6!

[Enhancements to the Rules Criticality Rating](#)  
[Support for Microsoft Sysmon Source](#)  
[DLQ Events Moved to Events Tab](#)  
[Newly Introduced Log Source Monitoring/Storage Management Notes](#)

Context XDR 1.0.6 brings you more improvements and updates!

## Enhancements to Rules Criticality Rating

We have now enhanced the rule criticality rating from low, med, and high to **Rule Score** rating from level 1 to level 5 based on the Common Vulnerability Scoring System (CVSS).

When creating a new rule, you need to select the rule score from 1 to 10. Based on the selected rule score, the **Risk score** rating is displayed on the UI.

The screenshot shows the 'Create Rule' interface. The 'Rule Conditions' section has 'Rule Score' set to 5, 'Timeframe' to 2, 'Timeunit' to Hours, and 'Type' to Occurrence base. The 'MITRE TTPs' section has 'Tactics' and 'Techniques' dropdowns. The 'Connections' section has source and field dropdowns. On the right, the 'ADAPTIVE RESPONSE' section has several notification options (Send Email, Slack, PagerDuty, ServiceNow) set to OFF, and 'Signal/Alert Suppression' set to OFF. The 'Signal Pause Threshold' is set to ON. The 'Configure Threshold' section has 'TimeUnit' set to Hours and 'Timeframe' set to 24. The 'Maximum Signals' field is set to 10000.

Simply, navigate to **Rules** tab and you can view the newly added **Rule Score** column on the **Rules** sub-tab.

The screenshot shows the 'Rules' tab in the XDR console. The table displays a list of rules with columns for 'LAST UPDATED', 'RULE NAME', 'LOG SOURCES', 'STATUS', 'RULE SCORE', 'TACTICS', 'TECHNIQUES', and 'SIGNALS'. The 'RULE SCORE' column is highlighted with a red box and shows a visual representation of the score (e.g., 5 out of 10 red squares). The 'SIGNALS' column shows the number of signals for each rule, ranging from 0 to 10.2K.

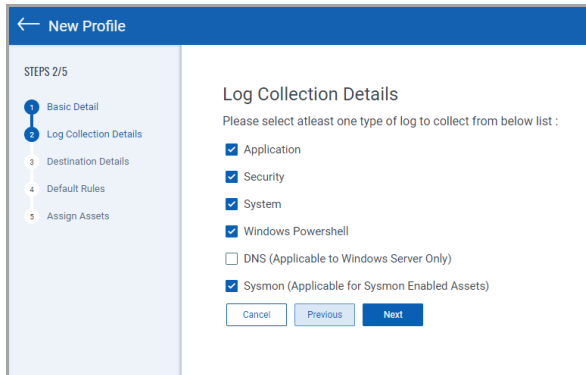
LAST UPDATED	RULE NAME	LOG SOURCES	STATUS	RULE SCORE	TACTICS	TECHNIQUES	SIGNALS
21 hours ago	TippingPoint-Sample Rule Jun 8, 2022 01:39 pm	ips	Inactive	5	-	-	0
a day ago	T1190 - [Cisco Sourcefire] F5 BIG-IP IContr... May 31, 2022 11:38 am	ips	Threshold paused	5	Initial Access	Exploit Public-Facing Applicati...	10K
a day ago	T1498.002 - [Cisco Sourcefire] NTP Amplif... May 31, 2022 11:38 am	ips	Threshold paused	5	Impact	Network Denial of Service	10K
a day ago	TA0002 - Cisco Sourcefire: Executable Cod... Dec 15, 2021 03:06 pm	ips	Threshold paused	5	Execution	-	10.2K
a day ago	Cisco Sourcefire: Executable Code Detecte... Dec 10, 2021 01:33 pm	ips	Threshold paused	5	Execution	-	10.2K
a day ago	destinationzone May 24, 2022 03:25 pm	ips	Threshold paused	5	-	-	10.2K
a day ago	Rule IPS SourceFire DSO May 23, 2022 06:50 pm	ips	Threshold paused	5	-	-	10.2K
2 days ago	T1484.001 - Cisco ISE, Multiple Configur... Jun 21, 2022 08:59 pm	iam	Active	5	Defense Evasion	Group Policy Modification	0
2 days ago	T1484.002 - Windows_Domain Trust Chan... Jun 21, 2022 08:36 pm	Windows	Active	5	Privilege Escalation,I	-	0

## Support for Microsoft Sysmon Source

With this release, we now support **Sysmon** source to ingest the event logs into context XDR for enriched data.

To configure the sysmon source, navigate to **Configuration > Cloud Agent Profiles > Profiles** and click **New Profile**. Enter the basic details such as Name and Description of profile, select **Windows** as the Operating System, and click **Next**. Then, select Sysmon (applicable for Sysmon Enabled Assets) and proceed to the next steps for configuration.

Note: you can ingest the event logs only from the Sysmon-enabled assets.

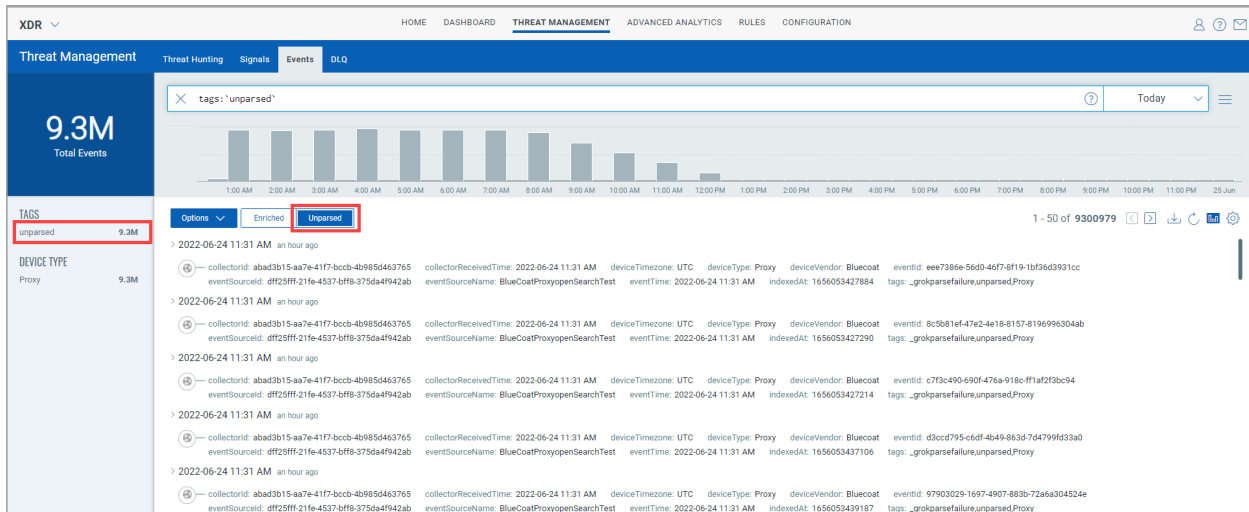


After the profile is successfully saved, Qualys Cloud Agents starts to collect logs from the assets you selected and forwards them to the destination you configured.

## DLQ Events Moved to Events Tab

With this release, you can view the unparsed events under the **Events** tab directly. The DLQ feature is deprecated and will be available for older logs.

Navigate to **Threat Management > Events** tab, and click **Unparsed** to view to the unparsed events.



## Newly Introduced Log Source Monitoring/Storage Management

We have now introduced a new feature for monitoring, alerting, and limiting the data storage utilization of various device types. As Context XDR is licensed on a per asset basis with storage guardrails to ensure that you do not overuse the storage and explode back-end cloud storage costs for Hadoop. The storage guardrail is now set to 50 GB per asset with a historical retention period of 6 months.

- **Monitoring:**– Allows you to view the amount of allocated data and usage of consumed data.
- **Alerting:**– Notifies to the user when the allocated data usage has reached/crossed over 80%, and data is being aged-out.
- **Limiting:**– Limit the age-out data (first-in and first-out) to ensure the data remains within applied guardrails.

### Notes

- Cloud agent XDR filebeat and QGS proxy works with https\_proxy=http://<ip>:Port format.  
Example: https\_proxy=<http://10.114.252.191:8080>