Qualys Context XDR v1.x

Release Notes

Version 1.0.6

June 29, 2022

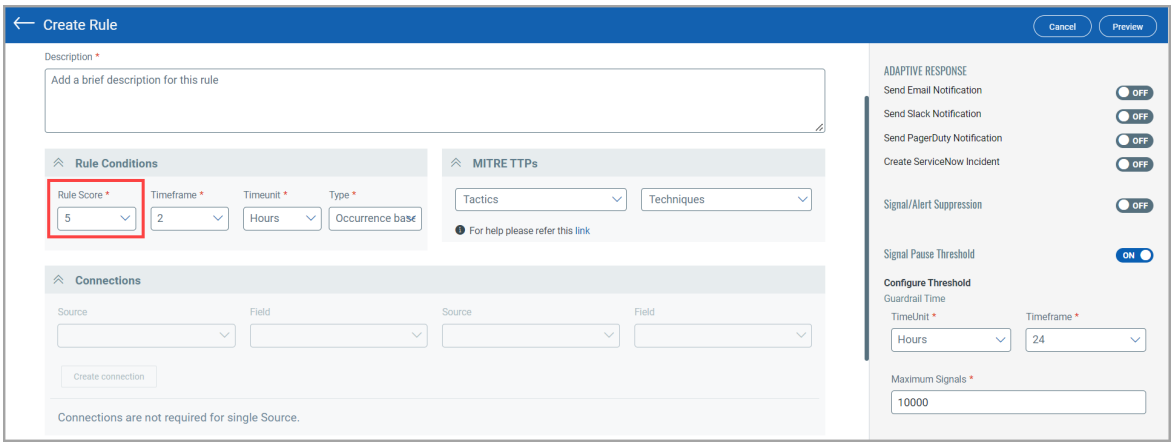
Here's what's new in Qualys Context XDR 1.0.6!

Context XDR 1.0.6 brings you more improvements and updates!

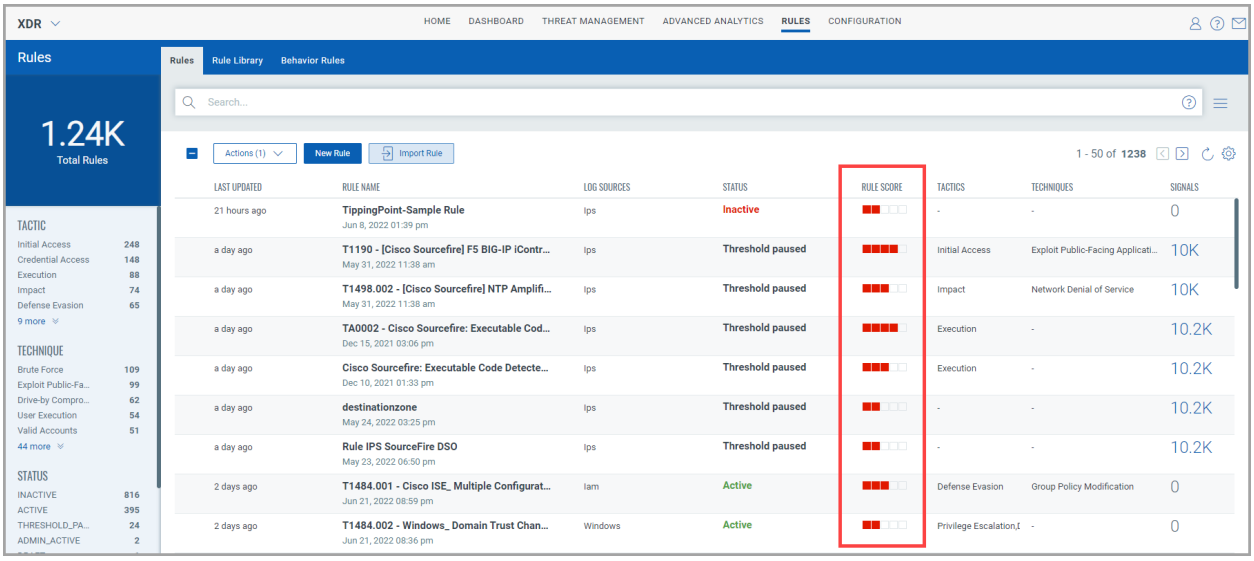
Enhancements to Rules Criticality Rating

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.



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

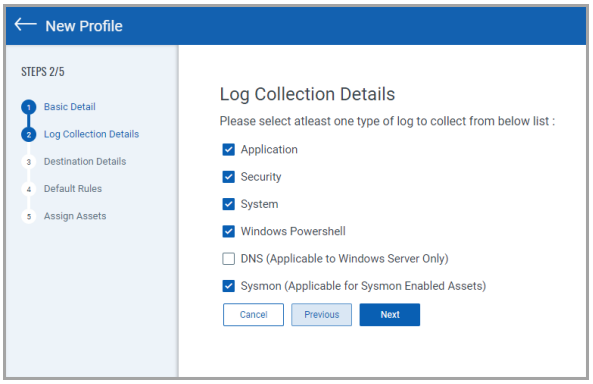


Support for Microsoft Sysmon Source

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.

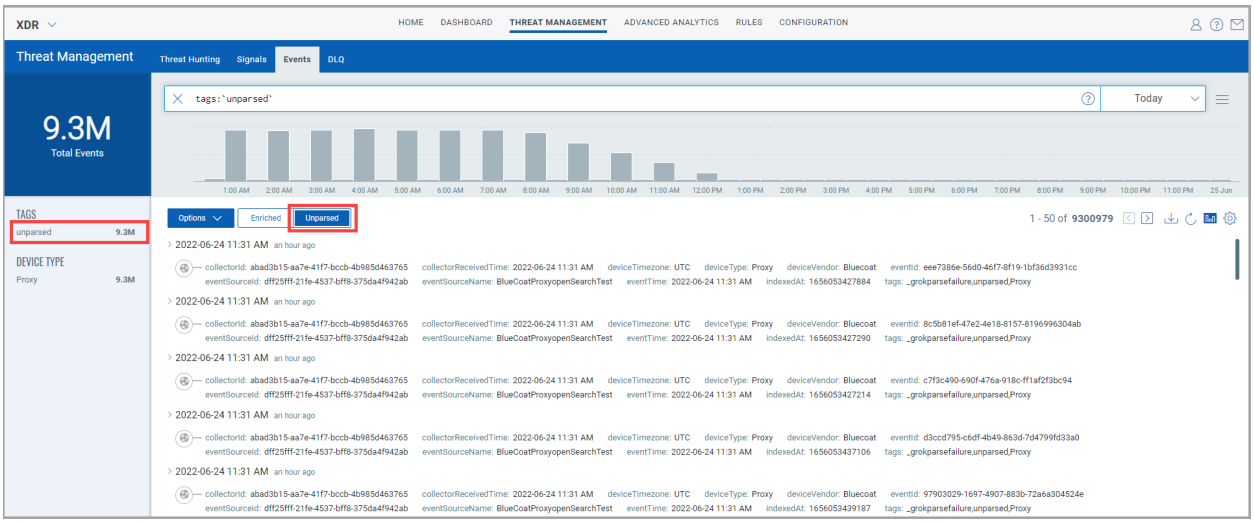


After the profile is successfully saved, Qualys Cloud Agents starts to collect logs from the assets you selected and forwards them to the destination you configured.

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