Qualys Context XDR v1.x

Release Notes

Version 1.3.7

February 17, 2023

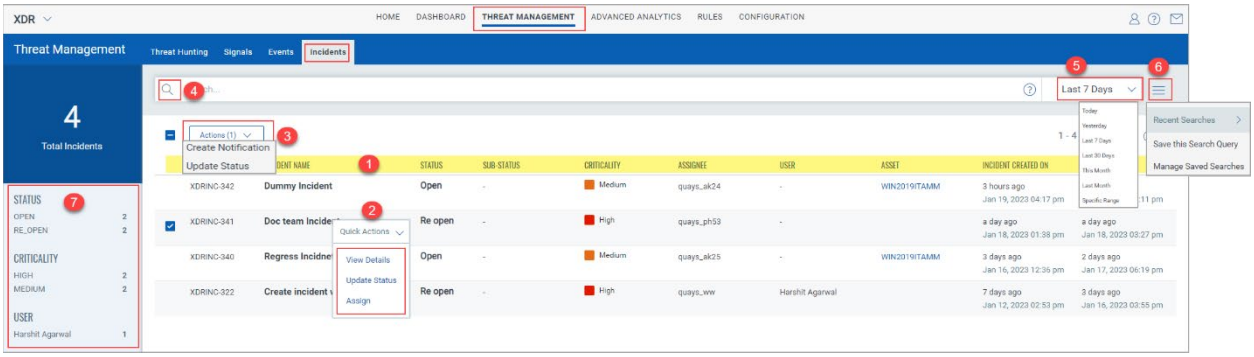
Here's what's new in Qualys Context XDR 1.3.7!

Enhancements

Context XDR 1.3.7 brings you more improvements and updates!

New Sub-Tab Introduced: Incidents

With this release, we've added a new Sub-Tab called **Incidents** under the tab **Threat Management**. The incidents tab allows you to view details, update the status and change the assignee of your incidents. Also, it offers you to review the signals associated with your incidents. Refer to the following screenshot and the numbers on it.



(1) The following are the columns under which you can see the details of your incidents.

- **INCIDENT ID:** This column shows a unique Id of your incident.
- **INCIDENT NAME:** This column shows the name of your incident.
- **STATUS:** This column shows the current status of your incident.
- **SUB-STATUS:** This column shows the sub-status of your incident. It is visible only if sub-status is available.
- **CRITICALITY:** This column shows the selected criticality of your incident.
- **ASSIGNEE:** This column shows the current assignee of your incident.
- **USER:** This column lists all the users associated with the signals of the incident
- **ASSET:** This column lists all the assets associated with the signals of the incident
- **INCIDENT CREATED ON:** This column shows the incident created date and time.
- **LAST UPDATED:** This column shows the incident's last updated details.

(2) This is a **Quick Actions** menu; it appears when you hover over any incidents. Under the quick actions menu, you can see **View Details**, **Update Status**, and **Assign** options. To know more details and functionality of these options, kindly refer to the Qualys Context XDR Online Help.

(3) This is an **Actions** menu; select the incident or bulk incidents and click **Actions**, under which you can see **Create Notification** and **Update Status** options. To know more details and functionality of these options, kindly refer to the Qualys Context XDR Online Help.

(4) This is the **Search** bar where you can use Qualys QQL to search for specific incidents on this page.

(5) This is the **Time Filter** dropdown, which you can use to view the incidents that occurred within a time range. You can define your own time range or choose a pre-defined time frame.

(6) This is the **Search Actions** menu; you can always save a search query and make it readily available. You can view the frequently used QQL queries, save, and manage them with ease.

(7) This is a **Quick Filters**; here you can view the newly added quick filters such as **STATUS**, **CRITICALITY**, and **USER** on the left pane. Use these filters to quickly look for incident details you are interested in.

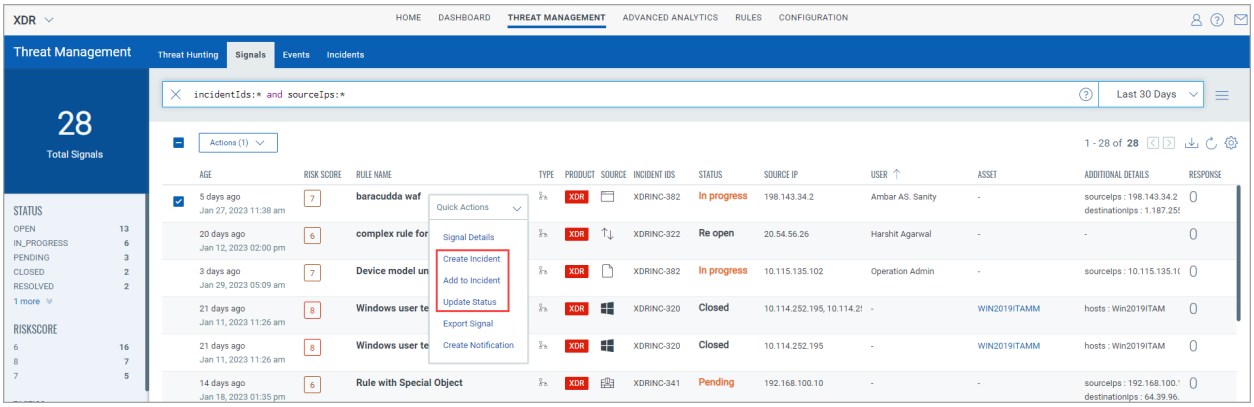
Enhancements to Signals Tab

With this release, we have added a capability to configure incidents out of signals. This can be achieved through the newly added options under the **Quick Actions** menu for each signal, such as **Create Incident**, **Add to Incident**, and **Update Status**.

You can manually create a new incident, add signals to the existing Incidents and update the incident's status.

Hover over the signal and choose one of these options from the Quick Actions menu to create, add the signal to the incident, or update individual signal status. Refer to the following screenshot.

To know more details about how to create, add and update the status of your incidents, kindly refer to the Qualys Context XDR Online Help.

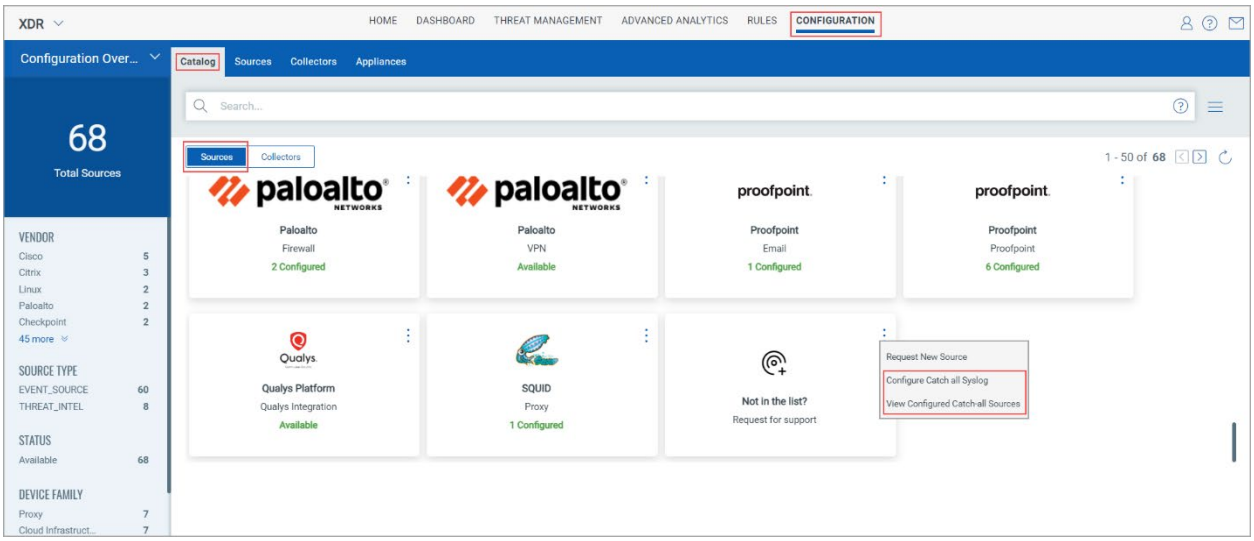


New Improvement 'Catchall Syslog Source' for Catalog

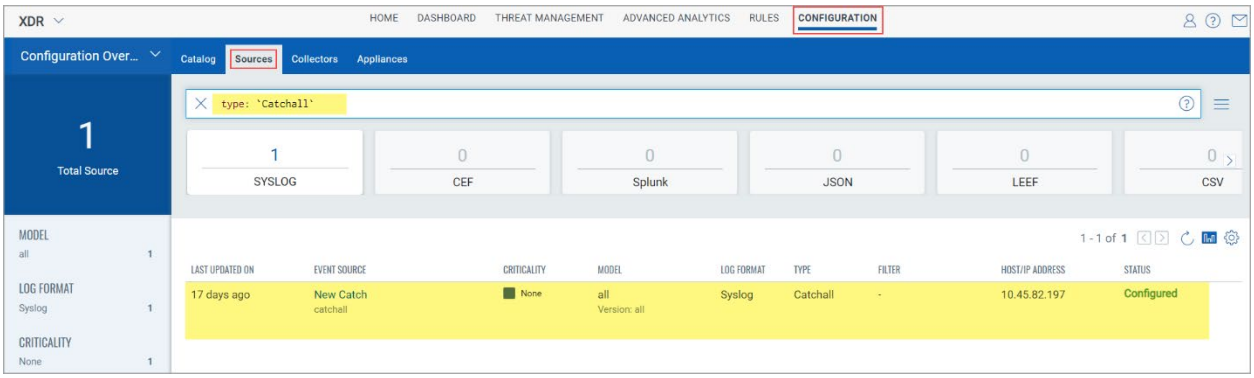
With this release, we have added an option under **Configuration** > **Catalog** > **Sources**, called **Configure Catch all Syslog**.

Using this option, you can configure the collector to store unknown source data in its raw message format for a specified period. You can use this to configure it as a Catch all Syslog collector. Also, you can configure one or more devices to send to the syslog collector without configuring it in XDR.

It enables you to deal with unexpected/unwanted data from old sources that must be adequately decommissioned on the source side.



You can view the configured catch-all sources under the **Configuration** > **Sources** Tab.

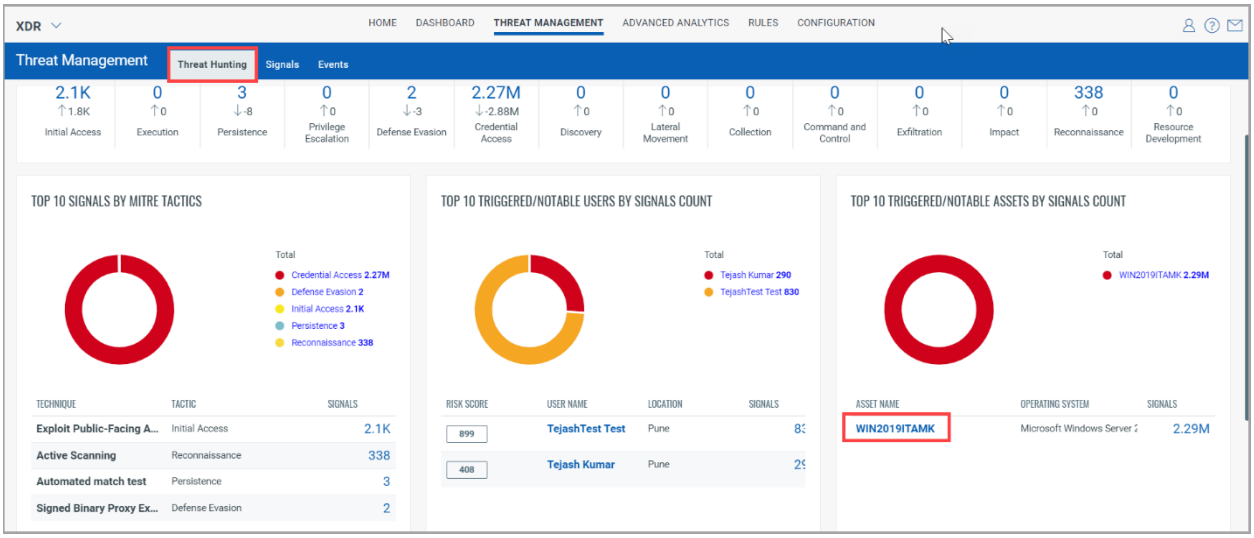


To know more details about how to configure catch all syslog, kindly refer to the Qualys Context XDR Online Help.

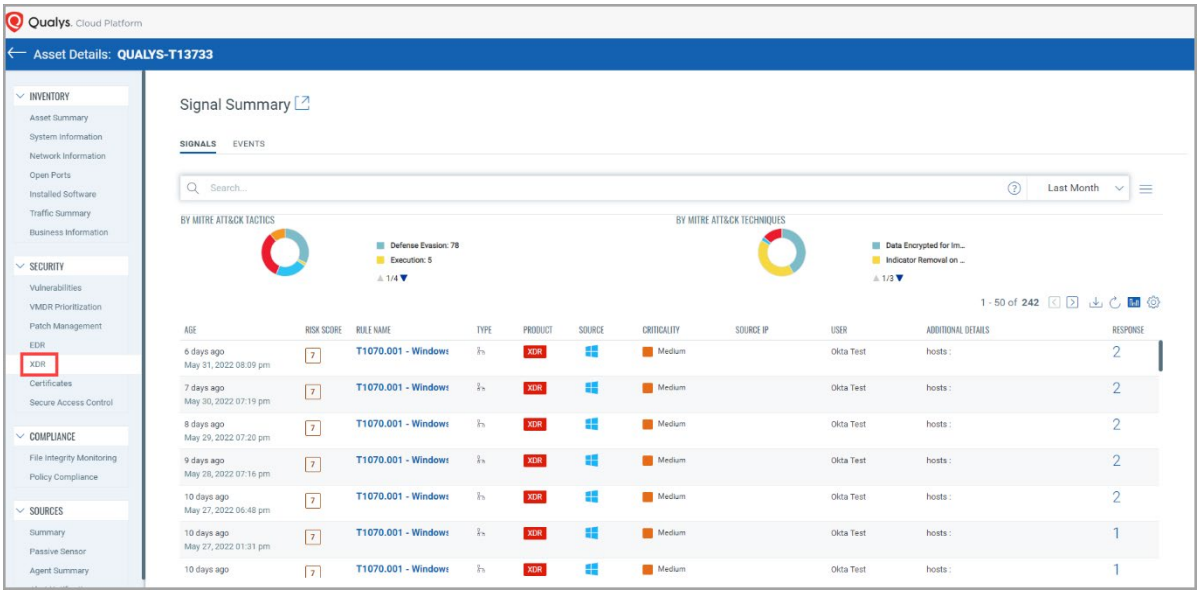
Enhancement to the Assets Details Page

With this release, we have newly added an XDR section on the **Assets Details** page. Now, you can view the complete summary details of an asset, such as signals, events, and Mitre tactics, etc.

Navigate to **Threat Management** > **Threat Hunting** and click the Asset to view the **Asset Details** page.



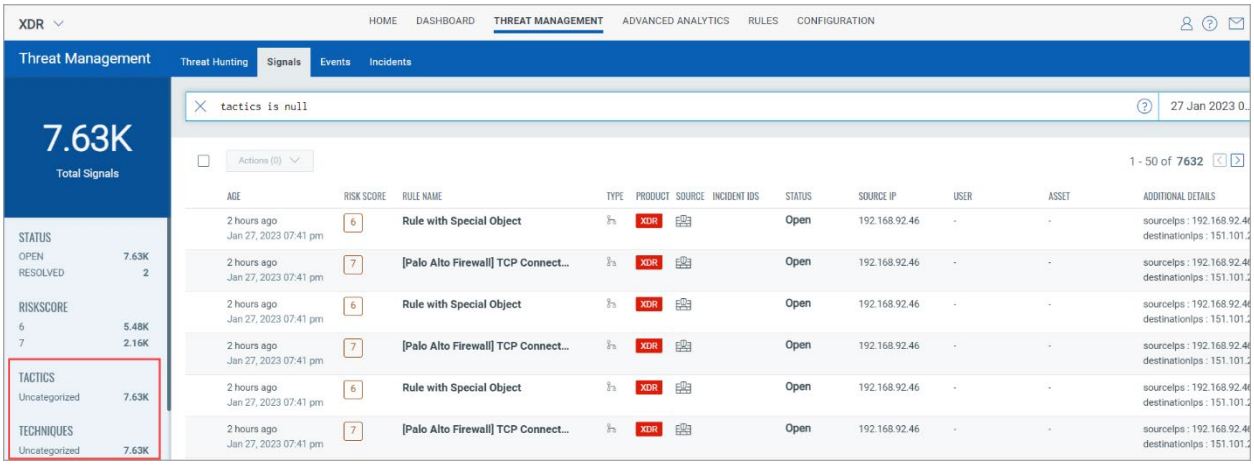
You can view the newly added **XDR** tab under the **Security** drop-down menu. Also, you can view the asset details from the Events tab or wherever there is AssetId involved.



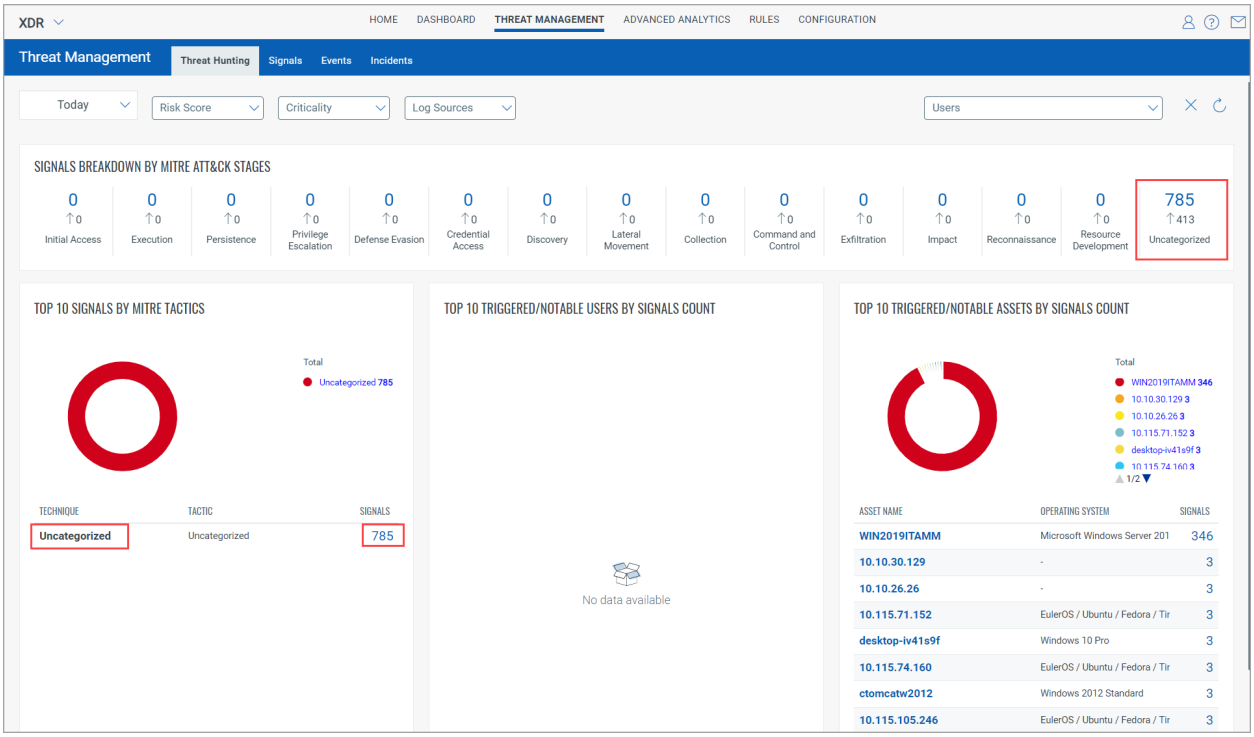
Enhanced Signal tab Quick Filters

With this release, we have added a new category called **Uncategorized** for quick filters Tactics & Techniques under the **Threat Management** > **Signals** tab.

This helps you to address/highlight/categorize those signals which do not have tactics & techniques defined. Refer to the following screenshot.

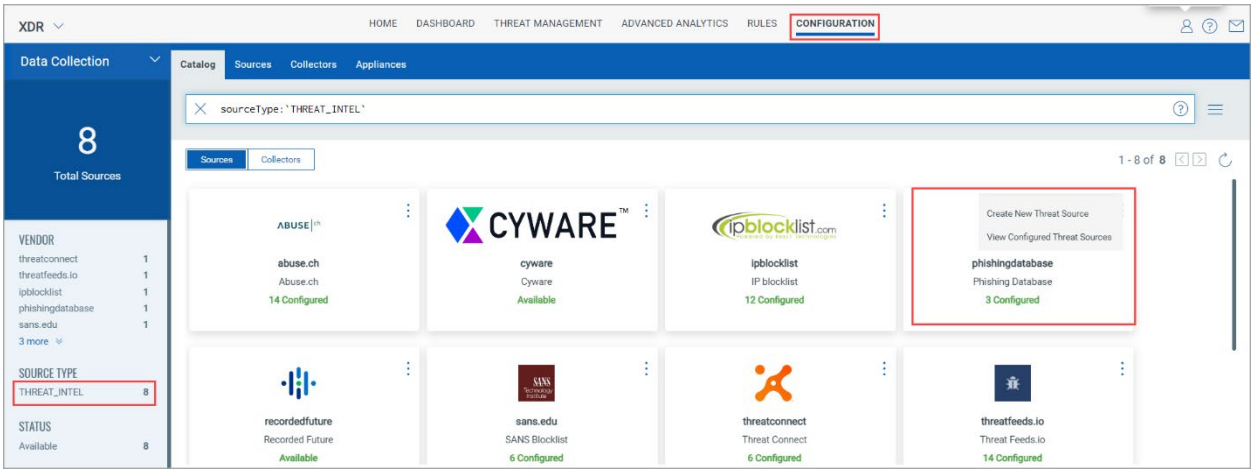


Also, you can view them under the tab **Threat Management** > **Threat Hunting**.



New Catalog Introduced: 'phishingdatabase'

With this release, under the tab **CONFIGURATION** > **Data Collection** > **Catalog**, we have added a new catalog called '**phishingdatabase**'. Using this catalog, you can create a new threat source.



Under this catalog, you can configure malicious, harmful phishing domains, URLs, websites, and threats databases.

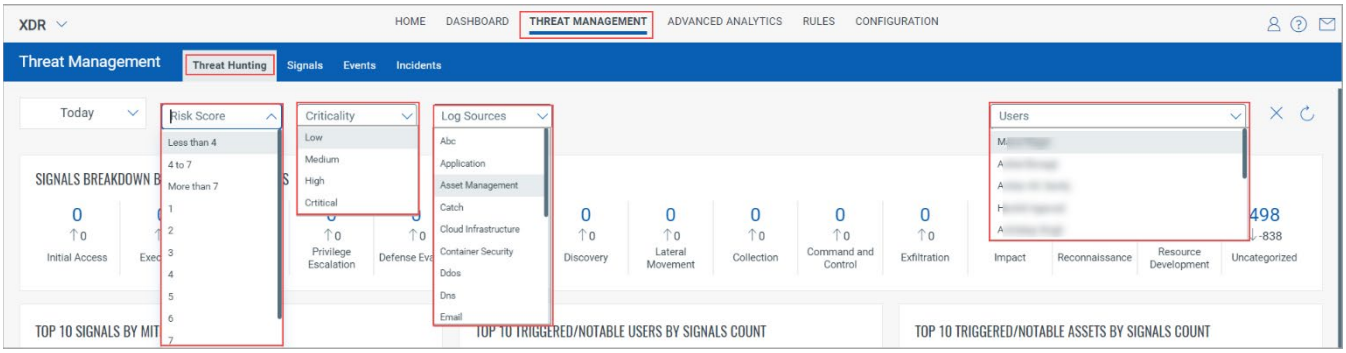
The following are the new threat intel sources introduced; you can use these sources while creating a new threat source.

- Active Domains
- Inactive Domains
- Invalid Domains
- Active Links
- Inactive Links
- Invalid Links
- Active IPs
- Inactive IPs
- Invalid IPs

Enhanced the Sub-Tab: Threat Hunting

With this release, under the tab **THREAT MANAGEMENT** > **Threat Hunting**, we have added new filters called **Risk Score**, **Criticality**, **Log Sources**, and **Users** to enhance your search results.

You can search or break-down your signals using these filters by selecting multiple risk score values, criticality, log sources, and users to view the signal breakdown on the threat intel dashboard.



Added a New Log Sources and Collectors

With this release, the following are the newly added log sources along with collectors:

- Azure Directory Audit
- Azure SignIn
- Oracle Cloud Infrastructure OCI Audit
- Netbox
- Atlassian Confluence Cloud
- Atlassian Jira Cloud
- Oracle OCI VCN
- Oracle OCI Loadbalancer
- Azure Defender for Identity
- Cloudflare Audit
- **Qualys Platform Integrations:** Knowledge Base, VMDR, Endpoint Detection and Response, File Integrity Monitoring, VMDR Mobile, Container Security, Cyber Security Asset Management.

New Tokens

We have introduced the following new search tokens for XDR tabs to enhance your search results:

Signals Tab (Threat Management > Signals)

- **ruleVersion:** This token helps you search the rule's version.
- **ruleDescription:** This token helps you search the rule's description.
- **customerId:** This token helps you to search results based on the customer ID of the signal generated.
- **id:** This token helps you to search results based on the ID of the signal generated.
- **signalType:** This token helps you to search results based on the type of signal.
- **outlier:** This token helps you to search results based on the outlier for the UEBA signal.
- **baseline:** This token helps you to search results based on the baseline of the UEBA signal.
- **eventProcessedTime:** This token helps you to search results based on the time of the UEBA signal batch.
- **companyCode:** This token helps you to search results based on the company code of the user.
- **sourceGeoIps:** This token helps you to search results based on the source geo IPs of the signals.
- **tiFeeds.tpiFlagMatch:** This token helps you to search results based on the threat intel.
- **tiFeeds.tpiDescription:** This token helps you to search results based on the description of the threat intel.
- **tiFeeds.tpiType:** This token helps you to search results based on the type that matches the threat intel.
- **tiFeeds.tpiMalware:** This token helps you to search results based on the threat intel malware.
- **tiFeeds.tpiScore:** This token helps you to search results based on the threat intel score.
- **tiFeeds.tpiUrl:** This token helps you to search results based on the threat intel url.

- **tiFeeds.tpiReason:** This token helps you to search results based on the reason for the threat intel.
- **tiFeeds.tpiAddressIP:** This token helps you to search results based on the IP address of the threat intel.
- **tiFeeds.tpiHashType:** This token helps you to search results based on the hash type of the threat intel.
- **tiFeeds.tpiField:** This token helps you to search results based on the event field that matches the threat intel.
- **tiFeeds.tpiSrc:** This token helps you to search results based on the threat intel source.
- **tiFeeds.tpiHashValue:** This token helps you to search results based on the value of the threat intel hash.
- **tiFeeds.tpiDomain:** This token helps you to search results based on the domain of the threat intel.
- **tiFeeds.tpiId:** This token helps you to search results based on the ID of the threat intel.
- **tiFeeds.tpiRepo:** This token helps you to search results based on the repo of the threat intel.
- **destinationGeoIps:** This token helps you to search results with the destination Geo IPs.

Events Tab (Threat Management > Events)

- **deviceType:** This token helps you search all results based on the type of device producing the audit events.
- **collectorId:** This token helps you search all results based on the collector ID.
- **eventSourceName:** This token helps you to search all results based on the event source name.
- **vm:** This token helps you to search all results based on the Qualys product enrichment reserved for VM.
- **fim:** This token helps you to search all results based on the Qualys product enrichment reserved for FIM.
- **ioc:** This token helps you to search all results based on the Qualys product enrichment reserved for IOC.
- **userDivision:** This token helps you to search all results based on the user division.
- **userEmployeeType:** This token helps you to search all results based on the user employee type.
- **threatIntelField:** This token helps you to search all results based on the new field of event that matches with the TI.
- **threatIntelCustom1:** This token helps you to search all results that match the existing threat intel custom 1.
- **threatIntelCustom2:** This token helps you to search all results that match the existing threat intel custom 2.

Users Tab (Advanced Analytics > Users)

- **deviceType:** This token helps you search all results by the user's title.
- **riskScore:** This token helps you search all results based on the user's risk score.

Sources Tab (Configuration > Threat Intel > Sources)

- **collectionNames:** This token helps you search all results based on collections names fetched from the TI feed source.

Incidents Tab (Threat Management > Incidents)

- **signalCount:** This token helps you to search all results based on the count of signals associated with an incident.
- **assignee:** This token helps you to search the results by the name of the incident assignee.
- **userDetails.companyCode:** This token helps you search all results based on the user details associated with an incident by company code.
- **userDetails.country:** This token helps you search all results based on the user details associated with an incident by country.
- **userDetails.firstName:** This token helps you to search results based on the list of user details associated with an incident by their first name.
- **userDetails.lastName:** This token helps you to search all results based on the list of user details associated with an incident by their last name.
- **userDetails.managerEmployeeId:** This token helps you to search all results based on the list of user details associated with an incident by their managerEmployeeId.
- **userDetails.department:** This token helps you to search all results based on the list of user details associated with an incident by their department.
- **userDetails.preferredName:** This token helps you to search all results based on the list of user details associated with an incident by their preferredName.
- **userDetails.title:** This token helps you to search all results based on the list of user details associated with an incident by their title.
- **userDetails.userGroup:** This token helps you search the results based on the list of user details associated with an incident by their user group.
- **userDetails.workEmail:** This token helps you search all results based on the user details associated with an incident by their work email.
- **userDetails.userId:** This token helps you to search all results based on the list of user details associated with an incident by their userId.
- **assetDetails.assetId:** This token helps you search all results based on the asset details associated with an incident by their assetId.
- **assetDetails.assetUuid:** This token helps you search all results based on the asset details associated with an incident by their asset UUIDss.
- **assetDetails.assetName:** This token helps you to search all results based on the list of asset details associated with an incident by their asset name.
- **logSources:** This token helps you to search all results based on the list of log sources associated with an incident.
- **criticality:** This token helps you select the incident's criticality as configured in the signal.
- **incidentName:** This token helps you to search the results by the name of the incident generated.
- **updatedOn:** This token helps you to use a date range or specific date to define the date on which the incident was updated.

- **createdOn:** This token helps you to use a date range or specific date to define the date on which the incident was created.
- **status:** This token helps you to search all results based on the status of the incident.

Behavior Changes

There are no behavioral changes observed in this release.

Known Limitations and Workarounds

There are no reported and notable issues open in this release.