



Qualys Context XDR v1.x

Release Notes

Version 1.0.7

July 27, 2022

Here's what's new in Qualys Context XDR 1.0.7!

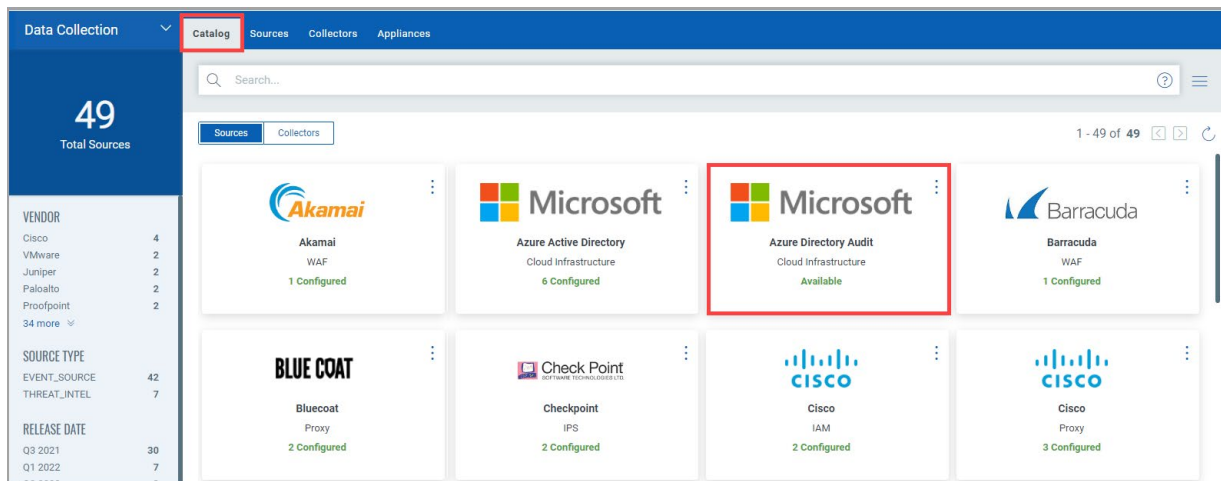
- [Onboarded Azure Active Directory Audit Collector](#)
- [New Improvement for Assets Details](#)
- [Enhancements to Assets Tab](#)
- [Removal of DLQ Tab](#)

Context XDR 1.0.7 brings you more improvements and updates!

Onboarded Azure Directory Audit Collector

We now support Azure Directory Audit cloud collector that allows you to ingest the audit logs/events into Context XDR to enrich data from other log sources.

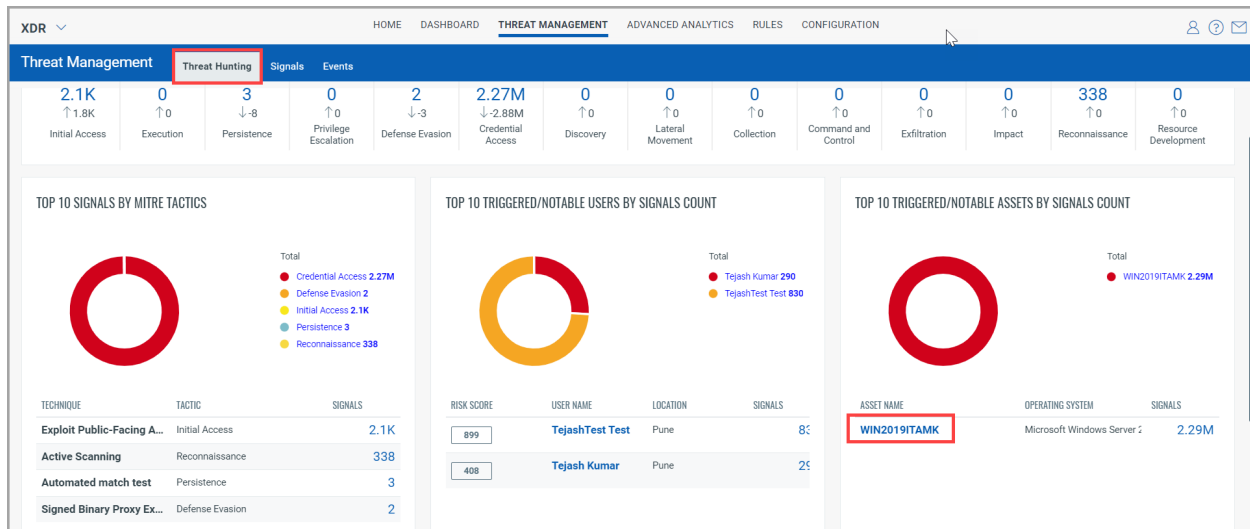
Navigate to **Configuration > Data Collection > Catalog**. Navigate to the **Microsoft Azure Directory Audit** tile and click **Configure Cloud Azure Directory Audit**. Enter the required details to configure the Azure Directory Audit collector and click **Save**. Once the collector binds successfully, the collector status appears as **Configured** under the **Sources** tab.



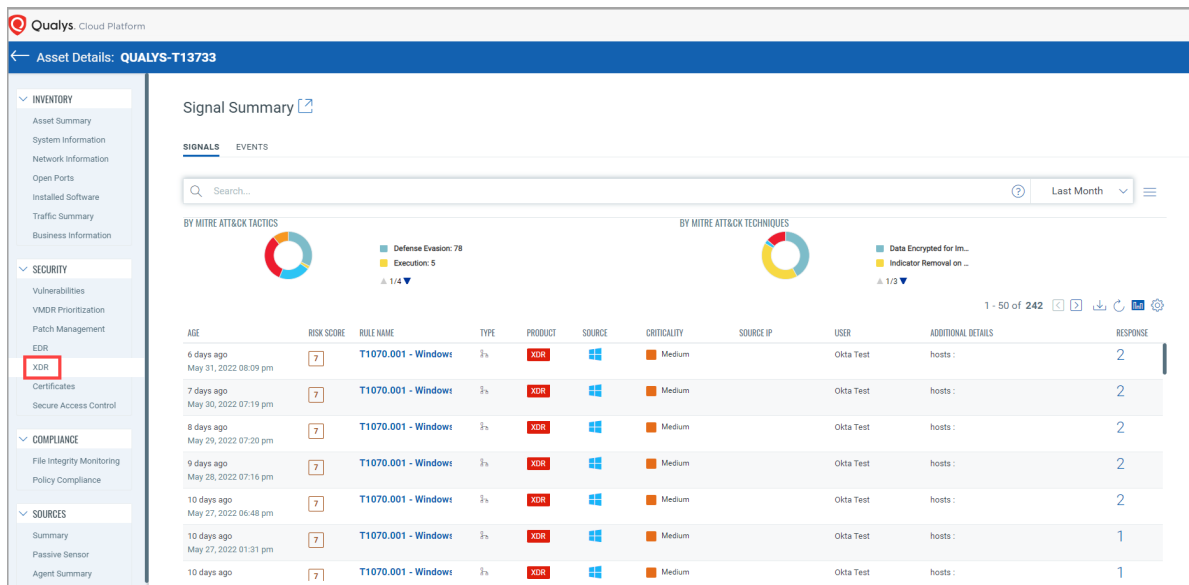
New Improvement for Assets Details

With this release, we have newly added 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.



Enhancements to Assets Tab

We have newly added the **Asset Name**, **Events**, **Agent Version**, and **Last Agent Status** columns on the Assets Tab.

Asset Name – Displays the name and details of an Asset.

Events – Displays if the events are streaming or not.

Agent Version – Displays the agent version associated with the asset.

Last Agent status – Displays the last agent status of an asset.

Note that the Last Agent Status is currently displayed only for Windows OS and for Linux OS - it is displayed as Not available.

Navigate to **Configuration > Cloud Agent Profiles > Assets** to view the newly added details.

Cloud Agent Profiles ▾ Profiles Assets									
35 Total Assets		Search...							
1 - 35 of 35									
XDR STATUS	ASSET NAME	EVENTS	AGENT VERSION	MANIFEST STATUS	LAST AGENT STATUS	OS	PROFILES	TAGS	
✓	WIN2019ITAMK 10.115.139.69	✓	4.9.17.2	Manifest Assigned 6 days ago	Streaming 16 minutes ago	Microsoft Windows Server...	18Jul22_Windows	Cloud Agent	
✓	DESKTOP-V3RH7I2 10.115.127.92	✓	4.9.0.11	Manifest Assigned 7 days ago	Streaming 16 minutes ago	Windows Microsoft Windo...	18Jul22_Windows	Cloud Agent	
⚠	ubuntu-2124 10.113.107.201	✓	-	Deactivation 7 days ago	Not Applicable	Ubuntu Linux 20.04.4	-	-	
⚠	DESKTOP-2KJTVJO 10.115.126.122	✓	4.9.0.11	- 25 days ago	Not available	Windows Microsoft Windo...	-	Cloud Agent	
⚠	d5eb2a6c-ef49-4bbf-be6f-ct	✓	-	- a month ago	Not available	Windows Microsoft Windo...	-	Cloud Agent	
⚠	Win7Patch69-85 10.115.74.210	✓	4.9.0.11	- a month ago	Not available	Windows Microsoft Windo...	-	Deepak_Tag	Cloud Agen
⚠	DESKTOP-9QP1UDI 10.115.138.119	✓	4.7.0.30	- 2 months ago	Not available	Microsoft Windows 10 Pro...	-	Cloud Agent	
⚠	DESKTOP-QGDR0OC 10.115.126.123	✓	4.8.0.31	- 2 months ago	Not available	Microsoft Windows 10 Ent...	-	IOC_ASSET_TAG	Cloud /
⚠	log4j-node04 10.113.107.171	✓	-	- 3 months ago	Not available	Windows Microsoft Windo...	-	Cloud Agent	

Removal of DLQ Tab

With this release, we have removed the **DLQ** tab from the **Threat management**. You can directly view the unparsed events under the **Events** tab.

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

