


ExtraHop Quarterly Detection Updates

Published: 2024-01-12

This guide provides information about new and enhanced detections that were released to all sensors over the course of the previous quarter.

Detections are continuously developed and released to [cloud-connected](#) ExtraHop systems to ensure that your environment is covered against performance issues and the latest network-based attack techniques. Without a connection to Cloud Services, [detection updates are delayed](#) until the firmware is upgraded.

Learn more about [detections](#) or navigate to the [Detection Catalog](#) on your ExtraHop system to search for detection types and view detection details.

 **Important:** It is important to understand that the status of any given detection in the ExtraHop system is subject to change: we are continuously refining detections and a detection can be added, changed, or removed at any time throughout the quarter.


Q4 2023

New Detections

Detection Type	Requirements
CVE-2023-27350 Papercut Exploit Attempt	SSL/TLS decryption
CVE-2023-24489 Citrix ShareFile Storage Zones Controller Exploit Attempt	SSL/TLS decryption
Windows Saved Search File Phishing Attempt	<ul style="list-style-type: none"> Active Directory decryption SSL/TLS decryption
Poor VoIP Call Quality (MOS)	N/A
Poor VoIP Call Quality (Jitter)	N/A
CVE-2023-28771 Zyxel Networks Exploit Attempt	N/A
CVE-2023-46747 F5 BIG-IP Exploit Attempt	SSL/TLS decryption
Mimikatz MS-RPC Activity	<ul style="list-style-type: none"> Active Directory decryption ExtraHop System 9.4
Remote Service Launch Attempt to Run a LOLBAS	Active Directory decryption
CVE-2023-20198 Cisco IOS XE Exploit	N/A
AD Database File Transfer over SMB/CIFS	Active Directory decryption
CVE-2023-3519 Citrix NetScaler ADC and Gateway Exploit Attempt	SSL/TLS decryption
CVE-2023-29357 Microsoft SharePoint Exploit	N/A

Enhanced Detections

 **Note:** These detection enhancements might result in new detection events.

Detection Type	Change	Requirements
New Remote Access Software Activity	Added support for AnyDesk software	N/A
Kerberos Attack Tool Activity	Added support for Orpheus and Impacket Kerberoasting techniques	Active Directory decryption 
New Remote Access Software Activity	Added support for TeamViewer and Splashtop software	N/A
Suspicious SMB/CIFS Named Pipe	Added new malware and threat group indicators	N/A