ExtraHop Quarterly Detection and Smart Investigation Updates

Published: 2025-01-04

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

Detections and Smart Investigations 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, Smart Investigations are not available and detection updates are delayed until the firmware is upgraded.

Important: It is important to understand that the status for a detection can change at any time as we refine or retire detections. Navigate to the Detection Catalog on your ExtraHop system to search for detection types and verify if any specific detection is currently available on your system. (Requires ExtraHop 9.5)

Q3 2024

New Detections

Detection Type	Requirements
Mythic C&C HTTP Connection	TLS decryption
Mythic C&C SSL/TLS Connection	N/A
Mythic C&C WebUI Connection	N/A
Havoc C&C Beaconing	TLS decryption
PingCastle Scan	Active Directory decryption
BackConnect Protocol Activity	N/A
BackConnect XOR Protocol Activity	N/A

Enhanced Detections

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

Detection Type	Change	Requirements
Log4Shell JNDI Injection Attempt	Improved performance, now supports a maximum of 250 unique JNDI strings	TLS decryption

New Smart Investigation Types

Your ExtraHop system will recommend an investigation when your network traffic matches the required criteria for that investigation type.

No new Smart Investigation types were added this quarter.

Enhanced Smart Investigation Types

Note: These enhancements might result in new recommended investigations.

No enhancements were made to Smart Investigations this quarter.

Q2 2024

New Detections

Detection Type	Requirements
Responder HTTP Activity	TLS decryption
Responder NTLM Activity	N/A
Merlin C&C HTTP Connection	TLS decryption
Impacket PSExec Activity	Active Directory decryption
CVE-2023-46604 Apache ActiveMQ Exploit	TLS decryption
CVE-2024-3400 Palo Alto Networks PAN-OS File Creation	TLS decryption
CVE-2024-3400 Palo Alto Networks PAN-OS Command Injection Attempt	TLS decryption
Rubeus Kerberos Diamond Ticket Activity	Active Directory decryption

Enhanced Detections

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

Detection Type	Change	Requirements
Overlapping IP Fragmentation	Improved performance	N/A
Remote Service Launch Attempt to Run a LOLBAS	Added new LOLBAS executable files	Active Directory decryption
Impacket SMBExec Activity	Added new indicators	N/A
Sudden Decrease in High Value Device Bandwidth	Added support for all high value devices	9.5 or earlier includes customer-specified high value devices 9.6 or later includes all high value devices
CVE-2021-22205 Gitlab CE and EE Exploit Attempt	Added a filter for devices running Gitlab CE/EE	TLS decryption

New Smart Investigation Types

Your ExtraHop system will recommend an investigation when your network traffic matches the required criteria for that investigation type.

Detection Type	Requirements
Network Recon with Lateral Movement	A device on your network ran network scans, performed enumeration techniques, and attempted

Detection Type	Requirements
	to remotely control another internal device. This detection sequence has been observed in known attack campaigns that led to ransomware.
Suspicious Software Usage	A device on your network was an offender that accessed a combination of software and cloud services that are often abused by attackers. Malware and threat groups have been known to leverage publicly available software such as AdFind, Rclone, PingCastle, BloodHound, and Impacket to carry out attack objectives.
Executable File Download with Lateral Movement	A device on your network was the offender in executable file download, transfer, and lateral movement detections. This detection sequence can be associated with early steps of network compromise, where an attacker pivots from an initial foothold to compromise other devices on the network.
Active Directory Enumeration	A device on your network was an offender in enumeration detections, attempting to discover Active Directory (AD) information such as privileged users, groups, and policies.

Enhanced Smart Investigation Types

Note: These enhancements might result in new recommended investigations.

No enhancements were made to Smart Investigations this quarter.

Q1 2024

New Detections

Detection Type	Requirements
Unusual Decrease in Inbound TCP Connections to High Value Devices	N/A
Sudden Decrease in High Value Device Bandwidth	N/A
CVE-2023-22518 Atlassian Confluence Exploit	TLS decryption
BadCandy Web Shell Activity	TLS decryption
CVE-2022-36804 Atlassian Bitbucket Server and Data Center Exploit	TLS decryption
CVE-2024-21887 Ivanti Connect Secure and Policy Secure Exploit	TLS decryption
Data Exfiltration to Slack	TLS decryption (for TLS 1.3)
Data Exfiltration to Discord	TLS decryption (for TLS 1.3)
Data Exfiltration to GitHub	TLS decryption (for TLS 1.3)

Detection Type	Requirements
Data Exfiltration to Dropbox	TLS decryption (for TLS 1.3)
HTTP/2 Rapid Reset DoS Attempt	TLS decryption
Unusual Archive File Upload	TLS decryption (depending on protocol)
CVE-2023-38035 Ivanti Sentry Exploit	TLS decryption

Enhanced Detections

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

Detection Type	Change	Requirements
Suspicious User Agent	Added new indicators	N/A
New WMI Enumeration Query	Improved performance	N/A
New External Connection (for RDP, SSH, FTP, NFS, Database, IIOP, LDAP, CIFS, Java RMI, and Cryptomining protocols)	Improved performance	N/A

New Smart Investigation Types

Your ExtraHop system will recommend an investigation when your network traffic matches the required criteria for that investigation type.

Detection Type	Requirements
Sustained C&C Activity	A device on your network was the victim in multiple command-and-control (C&C) detections.
Frequent Offender	A device on your network was the offender in a combination of lateral movement and exfiltration techniques
C&C with Exfiltration	A device on your network was the victim in a command-and-control (C&C) detection, then became the offender in an exfiltration detection.

Q4 2023

New Detections

Detection Type	Requirements
CVE-2023-27350 Papercut Exploit Attempt	TLS decryption
CVE-2023-24489 Citrix ShareFile Storage Zones Controller Exploit Attempt	TLS decryption
Windows Saved Search File Phishing Attempt	• Active Directory decryption • TLS decryption
Poor VoIP Call Quality (MOS)	N/A

Detection Type	Requirements
Poor VoIP Call Quality (Jitter)	N/A
CVE-2023-28771 Zyxel Networks Exploit Attempt	N/A
CVE-2023-46747 F5 BIG-IP Exploit Attempt	TLS decryption
Mimikatz MS-RPC Activity	• 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	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