Vierteljährliche Erkennungsupdates von ExtraHop

Veröffentlicht: 2024-01-22

Dieser Leitfaden enthält Informationen zu neuen und verbesserten Erkennungen, die im Laufe des vorangegangenen Quartals für alle Sensoren veröffentlicht wurden.

Erkennungen werden kontinuierlich weiterentwickelt und veröffentlicht an mit der Cloud verbunden ExtraHop-Systeme, um sicherzustellen, dass Ihre Umgebung vor Leistungsproblemen und den neuesten netzwerkbasierten Angriffstechniken geschützt ist. Ohne eine Verbindung zu Cloud Services Erkennungsupdates werden verzögert bis die Firmware aktualisiert ist.

Erfahre mehr über Erkennungen oder navigieren Sie zum Erkennungskatalog auf Ihrem ExtraHop-System, um nach Erkennungstypen zu suchen und Erkennungsdetails anzuzeigen.

Wichtig: Es ist wichtig zu verstehen, dass sich der Status einer bestimmten Entdeckung im ExtraHop-System ändern kann: Wir verfeinern kontinuierlich die Erkennungen und eine Erkennung kann jederzeit während des Quartals hinzugefügt, geändert oder entfernt werden.

VIERTES QUARTAL 2023

Neue Entdeckungen

Entdeckungstyp	Anforderungen
CVE-2023-27350 Papercut-Exploit-Versuch	SSL/TLS-Entschlüsselung
CVE-2023-24489 Versuch, den Citrix ShareFile Storage Zones Controller auszunutzen	SSL/TLS-Entschlüsselung
Phishing-Versuch, eine gespeicherte Suchdatei von Windows zu speichern	• Active Directory Directory-Entschlüsselung • SSL/TLS-Entschlüsselung
Schlechte VoIP-Anrufqualität (MOS)	N/A
Schlechte VoIP-Anrufqualität (Jitter)	N/A
CVE-2023-28771 Exploit-Versuch von Zyxel Networks	N/A
CVE-2023-46747 F5 BIG-IP-Exploitversuch	SSL/TLS-Entschlüsselung
Mimikatz MS-RPC-Aktivität	• Active Directory Directory-Entschlüsselung • ExtraHop-System 9.4
Versuch, einen LOLBAS auszuführen, per Fernzugriff zu starten	Active Directory Directory-Entschlüsselung
CVE-2023-20198 Cisco IOS XE-Exploit	N/A
AD-Datenbankdateiübertragung über SMB/CIFS	Active Directory Directory-Entschlüsselung
CVE-2023-3519 Citrix NetScaler ADC- und Gateway-Exploit-Versuch	SSL/TLS-Entschlüsselung
CVE-2023-29357 Microsoft SharePoint-Exploit	N/A

Verbesserte Erkennungen

Hinweis: Diese Erkennungsverbesserungen können zu neuen Erkennungsereignissen führen.

Entdeckungstyp	Änderung	Anforderungen
Neue Aktivität für Fernzugriffssoftware	Unterstützung für AnyDesk-Software hinzugefügt	N/A
Aktivität des Kerberos-Angriffstools	Unterstützung für Orpheus- und Impacket-Kerberoasting-Techniken hinzugefügt	Active Directory Directory-Entschlüsselung
Neue Aktivität für Fernzugriffssoftware	Unterstützung für TeamViewer- und Splashtop-Software hinzugefügt	N/A
Verdächtige SMB/CIFS Named Pipe	Neue Malware- und Bedrohungsgruppenindikatoren hinzugefügt	N/A