Mises à jour trimestrielles de détection ExtraHo

Publié: 2024-01-22

Ce guide fournit des informations sur les détections nouvelles et améliorées qui ont été publiées pour tous les capteurs au cours du trimestre précédent.

Les détections sont continuellement développées et diffusées à connecté au cloud Des systèmes ExtraHop pour garantir que votre environnement est protégé contre les problèmes de performances et les dernières techniques d'attaque basées sur le réseau. Sans connexion aux services cloud, les mises à jour de détection sont retardées jusqu'à ce que le firmware soit mis à jour.

En savoir plus sur détections ou naviguez jusqu' à Catalogue de détection sur votre système ExtraHop pour rechercher les types de détection et afficher les détails de détection.

Important: Il est important de comprendre que l'état d'une détection donnée dans le système ExtraHop est susceptible de changer : nous affinons continuellement les détections et une détection peut être ajoutée, modifiée ou supprimée à tout moment au cours du trimestre.

QUATRIÈME TRIMESTRE 2023

Nouvelles détections

Type de détection	Exigences
Tentative d'exploit CVE-2023-27350 Papercut	Décryptage SSL/TLS
CVE-2023-24489 Tentative d'exploitation du contrôleur de zones de stockage Citrix ShareFile	Décryptage SSL/TLS
Tentative de phishing avec un fichier de recherche enregistré sous Windows	• Décryptage Active Directory • Décryptage SSL/TLS
Mauvaise qualité des appels VoIP (MOS)	N/A
Mauvaise qualité des appels VoIP (gigue)	N/A
CVE-2023-28771 Tentative d'exploitation de Zyxel Networks	N/A
Tentative d'exploit CVE-2023-46747 F5 BIG-IP	Décryptage SSL/TLS
Activité Mimikatz MS-RPC	• Décryptage Active Directory • Système ExtraHop 9.4
Tentative de lancement du service à distance pour exécuter un LOLBAS	Décryptage Active Directory
Exploitation de Cisco IOS XE CVE-2023-20198	N/A
Transfert de fichiers de base de données AD via SMB/CIFS	Décryptage Active Directory
CVE-2023-3519 Tentative d'exploitation de Citrix NetScaler ADC et Gateway	Décryptage SSL/TLS

Type de détection	Exigences
Exploitation de Microsoft SharePoint CVE-2023-29357	N/A

Détections améliorées

Note: Ces améliorations de détection peuvent entraîner de nouveaux événements de détection.

Type de détection	Changement	Exigences
Nouvelle activité logicielle d'accès à distance	Ajout du support pour le logiciel AnyDesk	N/A
Activité de l'outil d'attaque Kerberos	Ajout de la prise en charge des techniques de Kerberoasting d'Orpheus et d'Impacket	Décryptage Active Directory
Nouvelle activité logicielle d'accès à distance	Ajout du support pour les logiciels TeamViewer et Splashtop	N/A
Canalisation nommée SMB/CIFS suspecte	Ajout de nouveaux indicateurs de programmes malveillants et de groupes de menaces	N/A