

Was ist neu

Veröffentlicht: 2024-01-22

Während [Versionshinweise](#) geben Sie einen umfassenden Überblick über unsere Release-Updates. Hier finden Sie eine Vorschau auf unsere aufregendsten Funktionen in ExtraHop 9.5.

Erkennungen

Das [Erkennungskatalog](#) identifiziert jetzt, ob ein Erkennungstyp derzeit in Ihrer Umgebung verfügbar ist.

The screenshot displays the 'Detection Catalog' in the ExtraHop interface. The main table lists various detection types, with the following data extracted from the visible rows:

Name	Author	Detection Type ID	Status	Category
PaperCut MF/NG RCE Exploit Attempt	ExtraHop	unpac_the_hash	In Review	Command & Control
UnPAC-the-Hash Activity	ExtraHop	cve_2023_27350	In Review	Command & Control
CVE-2023-27350 PaperCut MF/NG Exploit	ExtraHop	cve_2022_36804	In Review	Exploitation
CVE-2022-36804 Atlassian Bitbucket Exploit Attempt	ExtraHop	cve_2023_29357	In Review	Exploitation
CVE-2023-29357 Microsoft SharePoint Exploit	ExtraHop	suspicious_nfs_file_reads	Active	Reconnaissance
Suspicious NFS File Reads	ExtraHop	suspicious_cifs_file_reads	Active	Caution
Suspicious SMB/CIFS File Reads	ExtraHop	cifs_file_transfers	Inactive	Caution
Increase in Internal SMB/CIFS File Transfers	ExtraHop	nfs_file_transfers	Active	Exploitation
Increase in Internal NFS File Transfers	ExtraHop	ftp_file_transfers	Active	Hardening
Increase in Internal FTP File Transfers	ExtraHop	db_file_transfers	Active	Actions on Objective, Ex
Increase in Internal Database Data Transfers	ExtraHop	sepernova_webshell	Active	Exploitation
SUPERNOVA Webshell	ExtraHop	unusual_port	Inactive	Lateral Movement
New Protocol Activity on an Unusual Port	ExtraHop	wmi_process	Active	Exploitation
New WMI Process Creation	ExtraHop	ldap_user_enum	Active	Exploitation
LDAP User Enumeration	ExtraHop	cifs_brute_force	Active	Actions on Objective, Ex
SMB/CIFS Brute Force Attack Kerberos Brute Force	ExtraHop	wmi_method_launch	Active	Actions on Objective, Bc
New WMI Method Launch	ExtraHop	dat_exfil_azure	Inactive	Command & Control
Data Exfiltration to an Azure Resource	ExtraHop	unusual_protocol_enterprise	Active	Reconnaissance
Unusual Protocol for Enterprise Software	ExtraHop	user_session_enum	Inactive	Reconnaissance
User Session Enumeration	ExtraHop	kerberos_attack_tool	Active	Actions on Objective, Ex
Kerberos Attack Tool Activity	ExtraHop	kerberos_attack_tool	Active	Actions on Objective, Ex

The right-hand sidebar shows the 'Detection Type Settings' for 'ldap_object_enum':

- Display Name:** All Object Enumeration
- Detection Type ID:** ldap_object_enum
- Author:** ExtraHop
- Status:** In Review (Reviewing before release. This review can take several days or weeks.)
- Released:** 2023-08-28
- Last Updated:** 2023-08-28
- Category:** Security: Exploitation
- Go To:** [Detection Type Details](#)

Du kannst auch [Benachrichtigungen für den Erkennungskatalog erstellen](#), das Sie darüber informiert, wenn Erkennungstypen hinzugefügt oder aktualisiert werden.

ExtraHop | Reveal(x) 360 | Overview | Dashboards | Detections | Alerts | Assets | Records | Packets | Search...

Last 6 hours | Settings / Notification Rules

Notification Rules

Notification rules enable you to send notifications about detections through email and external services.

Name Create

<input type="checkbox"/>	Name	Event Type	Actions
<input checked="" type="checkbox"/>	New Notification Rule	System	Email
<input type="checkbox"/>	Priority Detection Email	Security Detection	Email
<input type="checkbox"/>	Record Capacity Watch	System	Email
<input type="checkbox"/>	ServiceNow Tickets	Security Detection	Webhook
<input type="checkbox"/>	Slack Notifications	Security Detection	Email, Webhook
<input type="checkbox"/>	SNOC Queue	Security Detection	Webhook

Create Notification Rule

Properties

Name * Author: angle

Description

Event

- Security Detection
- Performance Detection
- Security Detection Catalog
- Performance Detection Catalog
- Threat Briefing
- System

Criteria

Notifications are automatically sent when a new detection type becomes active and is released to all sensors.

Actions

Specify how notifications are sent when the criteria is met.

Send Email ✕

Email Recipients

Cancel Save

Wir haben auch eine hinzugefügt [Leitfaden zu Erkennungsaktualisierungen](#) wo Sie sehen können, wann eine Erkennung hinzugefügt oder aktualisiert wird.

Sie können jetzt erstellen [Tuning-Regeln](#) die Teilnehmer nach Hostname oder Domain verstecken.

Tune Detection

Create a rule to hide future detections that match the following criteria. Matching detections are hidden from view and do not have notifications or trigger events.

Criteria

Detection Type

- Data Exfiltration
- All detections types

Offender

Device: AccountingLaptop

Victim

Hostname or Domain

Victim Hostname or Domain ⓘ

Type hostnames or domains, separated by a comma...

✖ At least one hostname or SNI required.

Rule Options

Expiration

8 hours from now

Rule expires at 21:05 on May 9, 2022

Description

Cancel

Save

Bedrohungsinformationen

[Kuratierte Bedrohungssammlungen](#) von CrowdStrike Falcon sind jetzt standardmäßig in Ihrem ExtraHop-System verfügbar. CrowdStrike-Bedrohungssammlungen benötigen keine CrowdStrike-Lizenz mehr und können mit anderen integrierten ExtraHop-Sammlungen auf dem [Seite „Threat Intelligence“](#).

☰ | Last 5 minutes (UTC-3.5) ▾ | Settings / Threat Intelligence

Threat Intelligence

Threat intelligence is a collection of information about malicious IP addresses, threat actor techniques, and other indicators of compromise that can help your organization detect attacks.

Custom Threat Collections

Upload a collection that you have obtained from a reputable source.

ID	Name	Observables	Last Updated
BitNodes	BitNodes Collection	6,680	2021-04-13 19:37:24

[Manage custom collections](#)

Note
Custom collections must be uploaded to each sensor.

Built-In Threat Collections

Built-in threat intelligence collections are available by default on your Reveal(x) system. This console manages shared settings for 3 of 3 connected sensors.

Name	Status	Actions
CrowdStrike Falcon: Hostnames and URIs	● Enabled	Disable
CrowdStrike Falcon: IP Addresses	● Enabled	Disable
Malicious Botnet Host Names and URIs	● Enabled	Disable
Malicious Botnet IP Addresses	● Enabled	Disable
Malicious Brute Force IP Addresses	● Enabled	Disable
Malicious C2 IP Addresses	● Enabled	Disable
Malicious Cobalt Strike C2 IP Addresses	● Enabled	Disable
Malicious Host Names and URIs (I)	● Enabled	Disable
Malicious Host Names and URIs (II)	● Enabled	Disable
Malicious IP Addresses	● Enabled	Disable
Sensitive Information Patterns	● Disabled	Enable

Erkennungen können jetzt [für die Triage empfohlen werden](#) wenn der Hostname oder die IP-Adresse eines Teilnehmer [in einer Bedrohungsammlung referenziert](#) das ist auf Ihrem System aktiviert.

Erkennungsteilnehmer, die mit verdächtigen IP-Adressen oder Hostnamen verknüpft sind, gemäß [Bedrohungsinformationen](#) sind jetzt in Erkennungen und Zusammenfassungen der Erkennungstypen gekennzeichnet. Übereinstimmungen mit Bedrohungsindikatoren mit hoher Konfidenz aus den integrierten CrowdStrike-Bedrohungsammlungen werden als böse eingestuft.

The screenshot displays the ExtraHop interface for detecting SUNBURST C&C activity. At the top, it shows a risk level of 94 and a time range of 'Last 2 months just now (UTC-3.5)'. The main section is titled 'SUNBURST C&C Activity' and includes a description: 'west.example attempted to access a host associated with the backdoor known as SUNBURST or Solorigate, indicating command (C&C) activity. The SUNBURST backdoor affects SolarWinds Orion Platform versions 2019.4 through 2020.2 HF 1.' Below this, an 'OFFENDER' card shows IP 34.223.124.45 from suspicious-example.com with a 'MALICIOUS' tag. A 'VICTIM' card shows west.example. A '59 Offenders' list on the right includes IP addresses like 27.226.40.82 (SUSPICIOUS), 206.87.153.126, 143.58.100.52, 177.82.221.79 (SUSPICIOUS), and 125.80.192.93. A 'Threat Intelligence' popup shows a 'SUSPICIOUS' indicator for suspicious-example.com, with a type of 'SUNBURST Backdoor' and source 'ExtraHop Threat Intelligence'.

Für Administratoren

Du kannst jetzt [aktiviere CrowdStrike Falcon LogScale](#) wie der Recordstore. (Erfordert Reveal (x) Enterprise und eine ExtraHop-Lizenz für den LogScale Recordstore.)

Recordstore

Configure these settings to send transaction data to a recordstore. These settings override any connected ExtraHop recordstores. To configure an ExtraHop recordstore, disable these settings and go to [Connect ExtraHop Recordstore](#).

- Disable recordstore settings
- Enable LogScale as the recordstore
- Enable Splunk as the recordstore
- Enable BigQuery as the recordstore

LogScale Settings

Ingest

Ingest Hostname

Ingest Port

[Change Ingest Settings](#)

Query

API Hostname

API Port

View Name

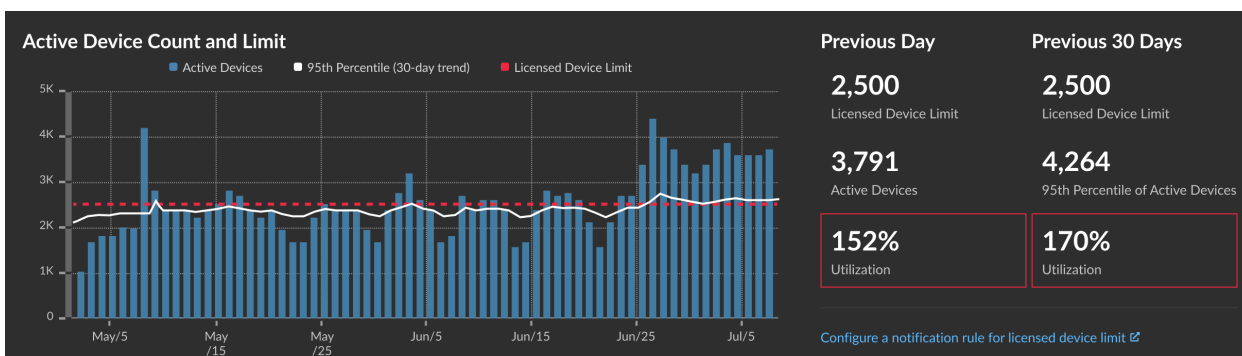
[Change Query Settings](#)

Advanced Options

Compress outgoing record payloads with gZIP

Save

Wir haben der Administrationsseite neue Charts hinzugefügt für [Enthülle \(x\) Enterprise](#) und [Zeige \(x\) 360](#) die es Ihnen ermöglichen, die Anzahl der aktiven Gerät zu überwachen und sie mit Ihrem Lizenzlimit zu vergleichen. Du kannst [eine Regel für Systembenachrichtigungen erstellen](#) um Administratoren zu benachrichtigen, wenn die Anzahl der aktiven Gerät einen bestimmten Schwellenwert erreicht.



Du kannst jetzt [Laden Sie einen benutzerdefinierten Satz von IDS-Regeln auf IDS-Sensoren hoch](#) die das ExtraHop-System in Erkennungen umwandelt, die Sie einsehen und untersuchen können.

Custom IDS Rules

Suricata Rules File

Uploaded By: jsu

Uploaded On: 2023-10-26 13:34

Last Processed On: 2023-10-26 14:05

[Replace File](#)

[Delete File](#)

Processed Rules

Rule SID 3,083 results

Rule SID ↓	Rule Name	Rule Status
2200000	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	Accepted
2200001	MALWARE-BACKDOOR MISC r00t attempt	Accepted
2200002	MALWARE-BACKDOOR MISC sm4ck attempt	Accepted
2200003	MALWARE-BACKDOOR MISC Solaris 2.5 attempt	ExtraHop 9.5 required. Learn more
2200004	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	Accepted
2200005	MALWARE-BACKDOOR MISC r00t attempt	Accepted
2200006	MALWARE-BACKDOOR MISC sm4ck attempt	Rejected. Learn more
2200007	MALWARE-BACKDOOR MISC Solaris 2.5 attempt	Rejected. Learn more
2200008	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	Accepted
2200009	MALWARE-BACKDOOR MISC r00t attempt	Rejected. Learn more
2200010	MALWARE-BACKDOOR MISC sm4ck attempt	Accepted
2200011	MALWARE-BACKDOOR MISC Solaris 2.5 attempt	Accepted
2200012	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	Rejected. Learn more

Wir [Diagramme zum Systemzustand hinzugefügt](#) wo Sie Metriken für Durchsatz, Paketrate und Paketfehler nach Schnittstelle überwachen können.

