

# What's New

Published: 2024-01-17

While [release notes](#) provide a comprehensive view of our release updates, here is a preview of our most exciting features in ExtraHop 9.5.

## Detections

The [Detection Catalog](#) now identifies whether a detection type is currently available in your environment.

The screenshot displays the 'Detection Catalog' interface in ExtraHop. The main area shows a table of detection types with 389 results. The table has columns for Name, Author, Detection Type ID, Status, and Category. One row is selected, showing 'CVE-2022-36804 Atlassian Bitbucket Exploit Attempt' with a status of 'In Review' and a category of 'Exploitation'. The right sidebar shows the 'Detection Type Settings' for this item, including its display name, ID, author (ExtraHop), status (In Review), release date (2023-08-28), last updated date (2023-08-28), and category (Security: Exploitation).

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

You can also [create notifications for the Detection Catalog](#), which lets you know when detection types are added or updated.

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

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

We have also added a [Detection Updates guide](#) where you can see when a detection is added or updated. You can now create [tuning rules](#) that hide participants by hostname or domain.

## 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

## Threat Intelligence

[Curated threat collections](#) from CrowdStrike Falcon are now available by default in your ExtraHop system. CrowdStrike threat collections no longer require a CrowdStrike license and can be managed with other ExtraHop built-in collections on the [Threat Intelligence page](#).

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	<a href="#">Disable</a>
CrowdStrike Falcon: IP Addresses	Enabled	<a href="#">Disable</a>
Malicious Botnet Host Names and URIs	Enabled	<a href="#">Disable</a>
Malicious Botnet IP Addresses	Enabled	<a href="#">Disable</a>
Malicious Brute Force IP Addresses	Enabled	<a href="#">Disable</a>
Malicious C2 IP Addresses	Enabled	<a href="#">Disable</a>
Malicious Cobalt Strike C2 IP Addresses	Enabled	<a href="#">Disable</a>
Malicious Host Names and URIs (I)	Enabled	<a href="#">Disable</a>
Malicious Host Names and URIs (II)	Enabled	<a href="#">Disable</a>
Malicious IP Addresses	Enabled	<a href="#">Disable</a>
Sensitive Information Patterns	Disabled	<a href="#">Enable</a>

Detections can now [be recommended for triage](#) when a participant hostname or IP address is [referenced in a threat collection](#) that is enabled on your system.

Detection participants that are associated with suspicious IP addresses or hostnames according to [threat intelligence](#) are now labeled in detections and detection type summaries. Matches to high confidence indicators of compromise from built-in CrowdStrike threat collections are labeled as Malicious.

Last 2 months just now (UTC-3.5) Detections / SUNBURST C&C Activity

### SUNBURST C&C Activity

**94** RISK  
COMMAND & CONTROL  
Dec 12 15:04 • lasting a few seconds

west.example attempted to access a host associated with the backdoor known as SUNBURST or Solorigate, indicating comm (C&C) activity. The SUNBURST backdoor affects SolarWinds Orion Platform versions 2019.4 through 2020.2 HF 1.

**59 Offenders**  
 27.226.40.82 **SUSPICIOUS**  
 206.87.153.126  
 143.58.100.52  
 177.82.221.79 **SUSPICIOUS**  
 125.80.192.93

**OFFENDER**

IP 34.223.124.45  
suspicious-example.com  
**MALICIOUS**

**VICTIM**

west.example

#### Threat Intelligence

**SUSPICIOUS** Threat Intelligence Indicator for suspicious-example.com

Type SUNBURST Backdoor  
Type ExtraHop Threat Intelligence

## For Administrators

You can now [enable CrowdStrike Falcon LogScale](#) as the recordstore. (Requires Reveal(x) Enterprise and an ExtraHop license for the 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**

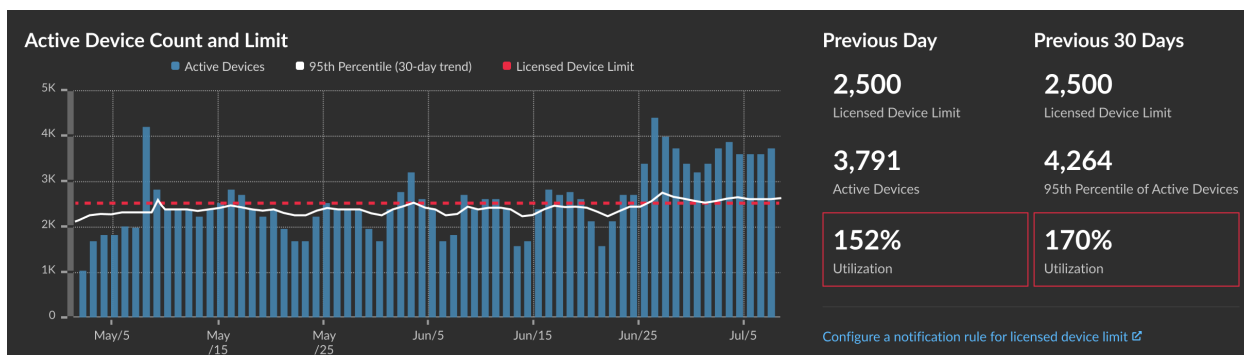
[Change Query Settings](#)

**Advanced Options**

Compress outgoing record payloads with gZIP

Save

We added new charts to the Administration page for [Reveal\(x\) Enterprise](#) and [Reveal\(x\) 360](#) that enable you to monitor active device counts and compare them to your licensed limit. You can [create a system notification rule](#) to notify Administrators when the active device count reaches a specified threshold.



You can now [upload a custom set of IDS rules to IDS sensors](#) that the ExtraHop system converts to detections that you can view and investigate.

# 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. <a href="#">Learn more</a>
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. <a href="#">Learn more</a>
2200007	MALWARE-BACKDOOR MISC Solaris 2.5 attempt	● Rejected. <a href="#">Learn more</a>
2200008	Malware Signature: Win32.Bancos.DI Reporting Infection via Email	● Accepted
2200009	MALWARE-BACKDOOR MISC r00t attempt	● Rejected. <a href="#">Learn more</a>
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. <a href="#">Learn more</a>

We [added System Health charts](#) where you can monitor metrics for throughput, packet rate, and packet errors by interface.

