

# Quoi de neuf

Publié: 2024-01-23

Alors que [notes de version](#) pour un aperçu complet de nos mises à jour de versions, voici un aperçu des fonctionnalités les plus intéressantes d'ExtraHop 9.5.

## Détections

Le [Catalogue de détection](#) identifie désormais si un type de détection est actuellement disponible dans votre environnement.

The detection catalog enables you to browse all detection types and manage custom detection types.

Name  389 results Create

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

**Detection Type Settings**

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](#)

Done

Vous pouvez également [créer des notifications pour le catalogue de détection](#), qui vous permet de savoir quand des types de détection sont ajoutés ou mis à jour.

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

Type email addresses, separated by a comma

Cancel Save

Nous avons également ajouté un [Guide des mises à jour de détection](#) où vous pouvez voir quand une détection est ajoutée ou mise à jour.

Vous pouvez désormais créer [règles d'exceptions](#) qui masquent les participants par nom d'hôte ou domaine.

## 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

### Renseignements sur les menaces

[Collections de menaces sélectionnées](#) de CrowdStrike Falcon sont désormais disponibles par défaut dans votre système ExtraHop. Les collections de menaces CrowdStrike ne nécessitent plus de licence CrowdStrike et peuvent être gérées à l'aide d'autres collections intégrées d'ExtraHop sur [Page relative au renseignement sur les menaces](#).

☰ 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>

Les détections peuvent désormais être recommandé pour le triage [☑](#) lorsque le nom d'hôte ou l'adresse IP d'un participant est référencé dans une collecte des menaces [☑](#) qui est activé sur votre système.

Détection des participants associés à des adresses IP ou à des noms d'hôte suspects selon renseignements sur les menaces [☑](#) sont désormais étiquetés dans les détections et les résumés des types de détection. Les correspondances avec des indicateurs de compromission à haut niveau de confiance provenant des collections de menaces intégrées à CrowdStrike sont qualifiées de malveillantes.

📄 🔄 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.

**OFFENDER**

IP 34.223.124.45  
 suspicious-example.com  
MALICIOUS

**VICTIM**

west.example

### 59 Offenders

- 27.226.40.82 SUSPICIOUS
- 206.87.153.126
- 143.58.100.52
- 177.82.221.79 SUSPICIOUS
- 125.80.192.93

### Threat Intelligence

SUSPICIOUS Threat Intelligence Indicator for suspicious-example.com

Type	SUNBURST Backdoor
Type	ExtraHop Threat Intelligence

### Pour les administrateurs

Tu peux maintenant [activer CrowdStrike Falcon LogScale](#) comme espace de stockage des enregistrements. (Nécessite Reveal (x) Enterprise et une licence ExtraHop pour l'espace de stockage des enregistrements LogScale.)

## 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**

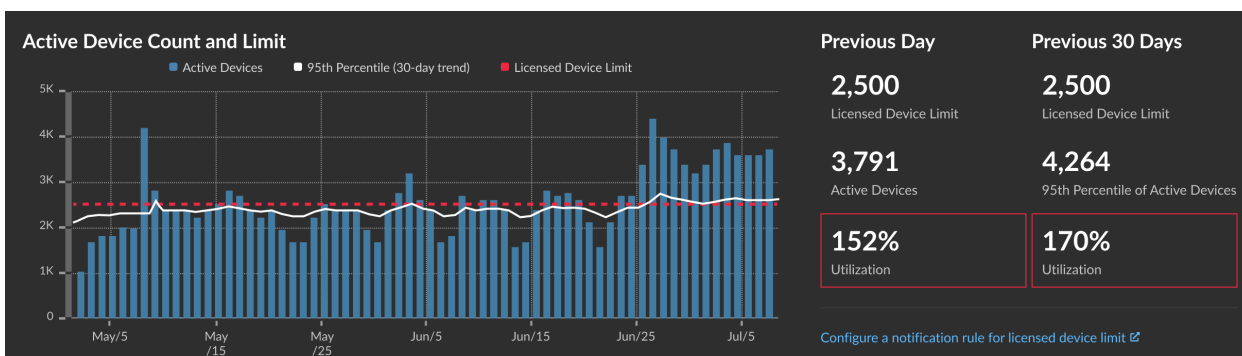
**View Name**

[Change Query Settings](#)

**Advanced Options**

Compress outgoing record payloads with gZIP

Nous avons ajouté de nouveaux graphiques à la page Administration pour [Reveal \(x\) Enterprise](#) et [Révéler \(x\) 360](#) qui vous permettent de surveiller le nombre d'équipements actifs et de le comparer à la limite de votre licence. Tu peux [créer une règle de notification système](#) pour avertir les administrateurs lorsque le nombre d'équipements actifs atteint un seuil défini.



Tu peux maintenant [télécharger un ensemble personnalisé de règles IDS vers les capteurs IDS](#) que le système ExtraHop convertit en détections que vous pouvez consulter et examiner.

## 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>

Nous [graphiques de santé du système ajoutés](#) où vous pouvez surveiller les mesures relatives au débit, au débit de paquets et aux erreurs de paquets par interface.

