# Detections

Published: 2024-10-15

The ExtraHop system applies machine learning techniques and rule-based monitoring to your wire data to identify unusual behaviors and potential risks to the security and performance of your network.

**Before you begin**
Users must be granted privileges ⬀ to view detections.

When anomalous behavior is identified, the ExtraHop system generates a detection and displays the available data and options. Controls on the Detections page surface detections that are recommended for triage and help you filter and sort your views, so you can quickly focus on detections related to critical systems first.

With NPM module access, detections can help you maintain your network in the following ways:

- Collect high-quality, actionable data to find the root causes behind network issues.
- Find unknown issues with performance or infrastructure.

With NDR module access, detections can help you defend your network in the following ways:

- Identify malicious behavior that is associated with different attack categories or MITRE techniques.
- View related detections or create your own investigation to group detections and track potential attack campaigns.
- Flag suspicious IP addresses, hostnames, and URIs identified by threat intelligence.
- Highlight security hardening best practices.

Learn more about optimizing detections ⬀.

> ⚠ **Important:** Although detections can inform you about security risks and performance issues, detections do not replace decision-making or expertise about your network. Always review security ⬀ and performance ⬀ detections to determine the root cause of unusual behavior and when to take action.

> ▶ **Video** See the related trainings:
> - Security Detections ⬀
> - Performance Detections ⬀

## Viewing detections

In the upper left corner of the Detections page, there are four options for viewing detections: Summary, Triage, MITRE Map, and Investigations. These options each provide a unique view of your detections list.

## Summary

By default, detections on the Detections page appear in Summary view, which aggregates information about detections to highlight patterns of activity in your environment. You can sort and group your detections list in Summary view to focus on frequently appearing detection types and the most active participants.

> 🗒 **Note:** By default, the **Open** status filter is applied to the Detections page. Click the **Open** filter to access other filter options.

**Sorting detections in Summary view**
You can sort detections by either the highest risk score or most recent occurrence.

When sorted by Risk Score, detections that are recommended for triage appear first, followed by detections with the highest risk score.

When sorted by **Most Recent**, detections with the most recent end time appear first. If two detections are still ongoing, the detection with the most recent update time appears first. Click the sort icon ⬛ above the detections list to select an option.

**Grouping detections in Summary view**
You can group detections by the type of detection (such as Spike in SSH Sessions) or by detection source (such as offender IP address), or you can choose to not group your detections list at all.



**Group by Type**

When grouping the Summary view by **Type**, you can view lists of values associated with detections that occurred during the selected time interval, such as participants, detection properties, or network localities.

You can click participant values to learn more about that device or IP address. Click any value to view only detections associated with that value, or track all associated detections ⬈.

**Participants**

Lists all offenders and victims in the selected detection type. The Offender and Victim lists are ordered by the number of detections in which the participant appears.

**Property Values**

Lists the property values associated with the detection type. The Property Values list is ordered by the number of detections in which the property value appears.

**Network Localities**

Lists the network localities that contain detections of the selected type. The Network Localities list is ordered by the number of detections in the network locality.

At the bottom of the summary panel are links that enable you to track all detections ⧉ included in the summary. You can create a tuning rule ⧉ to hide all detections included in the summary or view hidden detections of that detection type.

You can scroll past the summary panel to view individual detection cards. Detections that are recommended for triage appear first.

**Group by Source**

When grouping the Summary view by Source, you can view participants that are the source of a detection, with the number of detections displayed next to the participant name. Click on a source to display the detections the device appeared in as either an offender or victim. Click **Details** under the device name to view a list of the detection types that the device appeared in, then click a detection type to filter by that detection type.



**Group by None**

When grouping by **None** on the Detections page, you can view a timeline chart of the total number of detections identified within the selected time interval. Each horizontal bar in the chart represents the duration of a single detection and is color-coded according to the risk score.

- Click and drag to highlight an area on the chart to zoom in on a specific time range. Detections are listed for the new time interval.
- Hover over a bar to view the detection risk score.
- Click a bar to navigate directly to the detection detail page.

Beneath the timeline, a flow chart displays the number of detections that are associated with each attack category. Categories are assembled into an attack chain that characterizes the progression of steps an attacker takes to ultimately achieve their objective, such as stealing sensitive data. Click an attack category to only display detections in that category.

## Triage

(NDR module only) The Triage view surfaces detections that ExtraHop recommends for triage based on contextual analysis of factors in your environment.

Detection cards that are recommended for triage are marked with a yellow tag and list the factors that led to the recommendation.

**Involves a high value asset**

The asset provides authentication or essential services, or an asset that was manually identified as high value ⤢.

**Involves a top offender**

The device or IP address has participated in numerous detections and a variety of detection types.

**Involves a rare detection type**

The detection type has no recent history of appearing in your environment. Uncommon detection types can indicate unique, malicious behavior.

**Involves a suspicious hostname or IP address**

The hostname or IP address is referenced in a threat collection ⤢ that is enabled on your system.

**Involves a recommended investigation**

The detection is part of a potential attack chain in a recommended investigation.

Detections recommended for triage are prioritized in Summary view and appear at the top of your detections list regardless of sorting.

You can filter detections to display only detections that are recommended for triage and include Recommended for Triage as criteria for a notification rule ⤢.

Here are some considerations about recommendations for triage:

- Recommendations based on high value assets are limited to a maximum of five detections of the same detection type over a two week period.
- Two weeks of sensor data is required before recommendations are made based on top offender or rare detection type factors.
- Recommendations based on threat intelligence ⤢ are limited to two detections of the same detection type, for the same indicator of compromise, over a thirty day period.

## MITRE map

Click the **MITRE Map** view if you want to display your detections by attack technique.

Each tile in the matrix represents an attack technique from the MITRE ATT&CK® Matrix for Enterprise. If a tile is highlighted, the detection associated with that technique occurred during the selected time interval. Click any tile to see detections that match that technique.

## Investigations Table

The Investigations view displays all user-created and recommended investigations that were created during the selected time interval.

Click an investigation name to open the investigation. Learn more about Investigations.

## Filtering detections

You can filter the Detections page to display only the detections that match your specified criteria. For example, you might only be interested in exfiltration detections that occur over HTTP, or detections associated with participants that are important servers.

### Status

You can filter detections with a specific detection status, such as Acknowledged, In Progress, or Closed. By default, the **Open** status filter is applied to the Detections page. Click the **Open** filter to access other filter options.

You can select the **Hidden** status to only show detections that are currently hidden ⧉ by tuning rules ⧉.

### Category

You can filter by Attack or Performance detections, or you can select a more specific category to further refine your view of the Detections page. When you click the Category filter, most categories listed under the **All Attack Categories** and **All Performance Categories** options are sorted by the number of detections in the category. Hardening detections always appear at the end of the list.

Attack detections include the following categories that match phases of the attack chain.

### Command & Control

An external server that has established and maintained connection to a compromised device on your network. C&C servers can send malware, commands, and payloads to support the attack. These detections identify when an internal device is communicating with a remote system that appears to be acting as a C&C server.

**Reconnaissance**

An attacker is seeking high-value targets and weaknesses to exploit. These detections identify scans and enumeration techniques.

> **Note:** Detections might identify a known vulnerability scanner such as Nessus and Qualys. Click the device name to confirm if the device is already assigned a Vulnerability Scanner role in the ExtraHop system. To learn how to hide detections related to these devices, see Tune detections ⤴.

**Exploitation**

An attacker is taking advantage of a known vulnerability on your network to actively exploit your assets. These detections identify unusual and suspicious behaviors associated with exploitation techniques.

**Lateral Movement**

An attacker has infiltrated your network and is moving from device to device in search of higher-value targets. These detections identify unusual device behavior associated with east-west corridor data transfers and connections.

**Actions on Objective**

The attacker is close to achieving their objective, which can vary from stealing sensitive data to encrypting files to ransom. These detections identify when an attacker is close to completing a campaign objective.

**Caution**

Highlight activity that does not present an imminent threat to operations, but should be addressed to sustain a healthy security posture. These detections also identify activity by suspicious participants that are associated with threat intelligence.

**Performance** detections include the following categories.

**Authentication & Access Control**

Highlight unsuccessful attempts by users, clients, and servers to log in or access resources. These detections identify potential WiFi issues over authentication, authorization, and audit (AAA) protocols, excessive LDAP errors, or uncover resource-constrained devices.

**Database**

Highlight access problems for applications or users based on analysis of database protocols. These detections identify database issues, such as database servers that are sending an excessive number of response errors that might cause slow or failed transactions.

**Desktop & App Virtualization**

Highlight long load times or poor quality sessions for end users. These detections identify application issues, such as an excessive number of Zero Windows, which indicates that a Citrix server is overwhelmed.

**Network Infrastructure**

Highlight unusual events over the TCP, DNS, and DHCP protocols. These detections might show DHCP issues that are preventing clients from obtaining an IP address from the server, or reveal that services were unable to resolve hostnames due to excessive DNS response errors.

**Service Degradation**

Highlight service issues or performance degradation associated with Voice over IP (VoIP), file transfer, and email communications protocols. These detections might show service degradations where VoIP calls have failed and provide the related SIP status code, or show that unauthorized callers have attempted to make several call requests.

**Storage**

Highlight problems with user access to specific files and shares found when evaluating network file system traffic. These detections might show that users were prevented from accessing files on

Windows servers due to SMB/CIFS issues, or that network-attached storage (NAS) servers could not be reached due to NFS errors.

**Web Application**

Highlight poor web server performance or issues observed during traffic analysis over the HTTP protocol. These detections might show that internal server issues are causing an excessive number of 500-level errors, preventing users from reaching the applications and services they need.

**Hardening** detections identify security risks and opportunities to improve your security posture.

**Hardening**

Highlight security hardening best practices that should be enforced to mitigate the risk of exploitation. These detections identify opportunities to improve the security posture of your network, such as preventing credential exposure and removing expired SSL/TLS certificates from servers. After you click a hardening detection, you can apply additional filters to view specific detections within that hardening detection type. Learn more about filtering and tuning hardening detections ⤤.

**Intrusion Detection System (IDS)** detections identify security risks and malicious behavior.

**Intrusion Detection**

Highlight network traffic that matches known signatures of unsafe practices, exploit attempts, and indicators of compromise related to malware and command-and-control activity.

> ⓘ **Important:** While IDS detections include links to packets for all protocol types, links to records are only available for L7 protocols.

**Type**

Filter your detection list by a specific detection type, such as Data Exfiltration or Expired SSL Server Certificates. You can also type a CVE identification number into this filter to only show detections for a specific public security vulnerability.

**MITRE Technique**

Highlight detections that match specific MITRE technique IDs. The MITRE framework is a widely recognized knowledgebase of attacks.

**Offender and Victim**

The offender and victim endpoints associated with a detection are known as participants. You can filter your detection list to only show detections for a specific participant, such as an offender that is an unknown remote IP address, or a victim that is an important server. Gateway or load balancer devices that are associated with external endpoint participants can also be specified in these filters.

**Assignee**

Filter detections by the user assigned to the detection.

**More Filters**

You can also filter your detections by the following criteria:

- Recommended for Triage
- Device roles ⤤
- Source
- Site (console only)
- Ticket ID filter (third-party ticket tracking ⤤ only)
- Minimum Risk Score

# Navigating detections

After you select how to view, group, and filter your detections list, click any detection card to navigate to the detection detail page.

### Detection cards

Each detection card identifies the cause of the detection, the detection category, when the detection occurred, and the victim and offender participants. Security detections include a risk score.



### Risk score

Measures the likelihood, complexity, and business impact ⧉ of a security detection. This score provides an estimate based on factors about the frequency and availability of certain attack vectors against the necessary skill levels of a potential hacker and the consequences of a successful attack. The icon is color coded by severity as red (80-99), orange (31-79), or yellow (1-30).

### Participants

Identifies each participant (offender and victim) involved in the detection by hostname or IP address. Click on a participant to view basic details and access links. Internal endpoints display a link to the Device Overview page; external endpoints display the geolocation of the IP address, endpoint lookup links ⧉ such as ARIN Whois and a link to the IP address detail page. If a participant has passed through another device like a load balancer or gateway, both the participant and the device are displayed on the participant card, but only the origin endpoint is considered a participant.

> **Note:** SSL/TLS decryption is required to display origin endpoints if HTTPS is enabled. Learn more about SSL/TLS decryption ⧉.

When grouping by **Type**, a summary panel appears under the detection type that breaks down detections by offender and victim and enables you to quickly apply participant filters.

When grouping by **Source**, internal device role icons are highlighted red if the device was an offender in a detection and teal if the device was a victim. You can click **Details** under the source name to view a summary of detections where that source was a participant. These device details are displayed next to the detection card on wide screens (1900 pixels or greater).

**Duration**

Identifies how long the unusual behavior was detected or displays ONGOING if the behavior is currently occurring.

Detections that highlight security hardening best practices display two dates: the first time and the most recent time that the violation was identified.

**Metric data**

Identifies additional metric data when the unusual behavior is associated with a specific metric or key. If metric data is unavailable for the detection, the type of anomalous protocol activity appears.
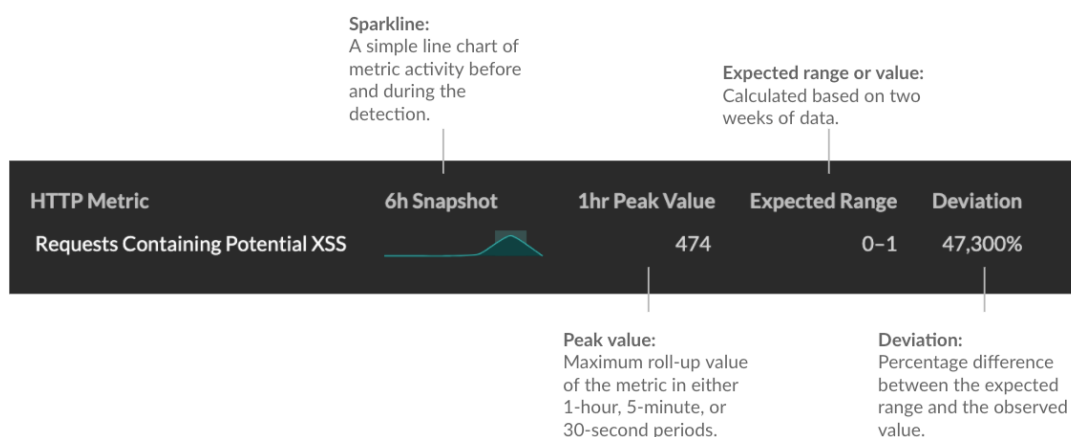


**Detection management**

You can track ⧉ or tune ⧉ the detection from the Actions dropdown list, or click **View Detection Details** to navigate to the detection detail page.

**Detection detail page**

Most of the data that you need to understand and validate a detection appears on the detection detail page: tables of relevant metric data, record transactions, and links to raw packets.

The detection card information is followed by all available sections for the detection. These sections vary depending on the type of the detection.

**Track Detection**

You can track ⧉ or tune ⧉ the detection, or click **Add to an Investigation** to include the detection in a new or existing investigation.

If you have configured a CrowdStrike integration ⧉ on your ExtraHop system, you can initiate containment of CrowdStrike devices ⧉ that are participants in the detection. (Reveal(x) 360 only.)

**Decryption badge**

When the ExtraHop system identifies suspicious behavior or a potential attack in decrypted traffic records, the detection detail page displays a decryption badge to the right of the detection name.

**CVE-2021-34527 Windows Print Spooler Exploit Attempt**

83 RISK

🔒 DETECTED WITH DECRYPTION ⓘ

EXPLOITATION

Dec 8 12:17 • lasting a few seconds

dc05-west received a malicious request that matches an attempt to exploit PrintNightmare, a privilege escalation and remote code execution (RCE) vulnerability in the Windows Print Spooler service. Refer to this Microsoft Security Update Guide for patch and mitigation information

☠ OFFENDER

externalVM
192.168.226.68

🎯 VICTIM

dc05-west
192.168.77.175

**Track Detection**

Status
No Status ✎

Assignee
Unassigned ✎

Actions
Add to an Investigation
Tune Detection

Learn more about SSL/TLS decryption ⧉ and decrypting traffic with a Windows domain controller ⧉.

**Detection properties**

Provides a list of properties that are relevant to the detection. For example, detection properties can include a query, URI, or hacking tool that is central to the detection.



**Activity map**

Provides an activity map ⧉ that highlights the participants involved in the detection. The activity map displays east-west traffic of the protocol associated with the detection to help you assess the scope of malicious activity. Click the victim or offender to access a drop-down menu with links to the Device Overview page and other detections where the device is a participant.
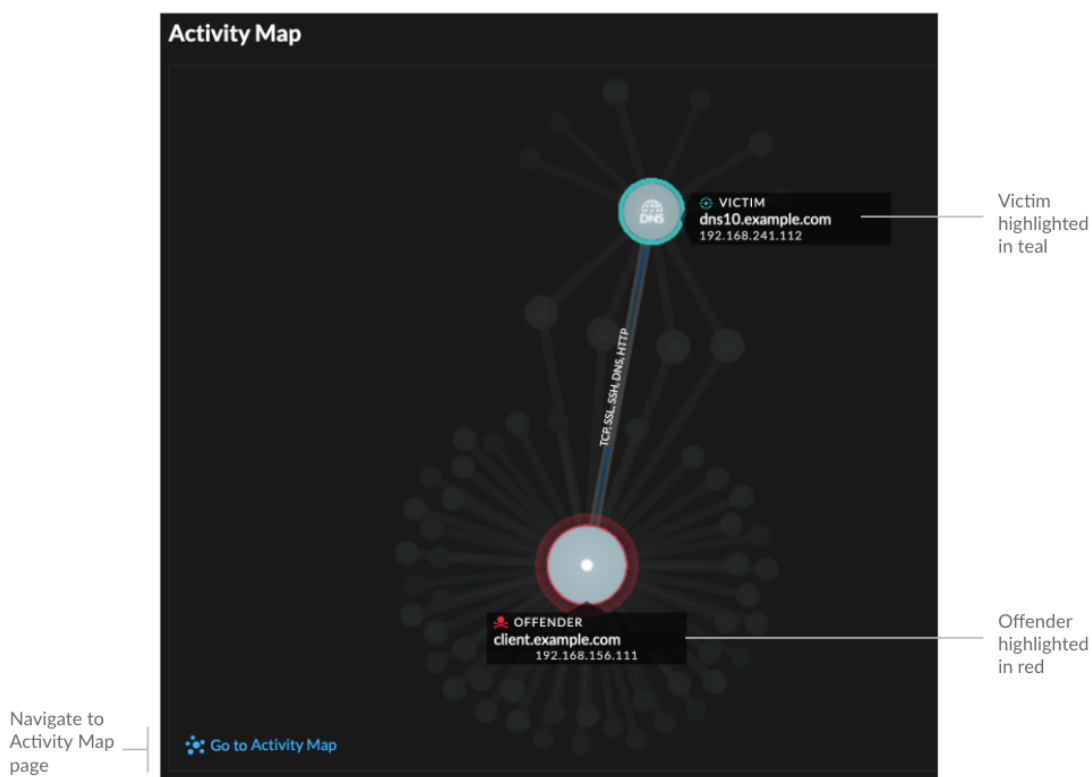
**Detection data and links**

Provides additional data associated with the detection to investigate. The types of data can include related metrics, links to record ⬀ transaction queries, and a link to a general packets ⬀ query. The availability of metrics, records, and packets vary by detection. For example, IDS detections include links to packets for all protocol types, but links to records are only available for L7 protocols.

Metric data and record transactions are displayed in tables. In a metrics table, click the icon 🔍 to view related record transactions. In a records table, click the icon ◎ to view the related packet query for a transaction.

> 📄 **Note:** A recordstore ⬀ must be configured to view transactions and continuous packet capture ⬀ must be configured to download packets.

**Compare behaviors**

Provides a chart that displays the activity of the offender next to the activity of similar devices over the time period when the detection occurred. The chart appears for detections related to unconventional activity by a device, and highlights unexpected behavior by displaying it next to the behavior of devices on the network with similar properties.

Unconventional activity

Time period prior to detection

Expected activity

Devices compared in the chart

## Related detections

Provides a timeline of detections related to the current detection that can help you identify a larger attack campaign. Related detections include the participant role, duration, timestamp, and any role changes if the offender in one detection becomes the victim in a different detection. Click any related detection in the timeline to view the details page for that detection.



Times each detection occurred relative to the current detection

Click the detection name to view the detail page

Roles of the participants in each related detection
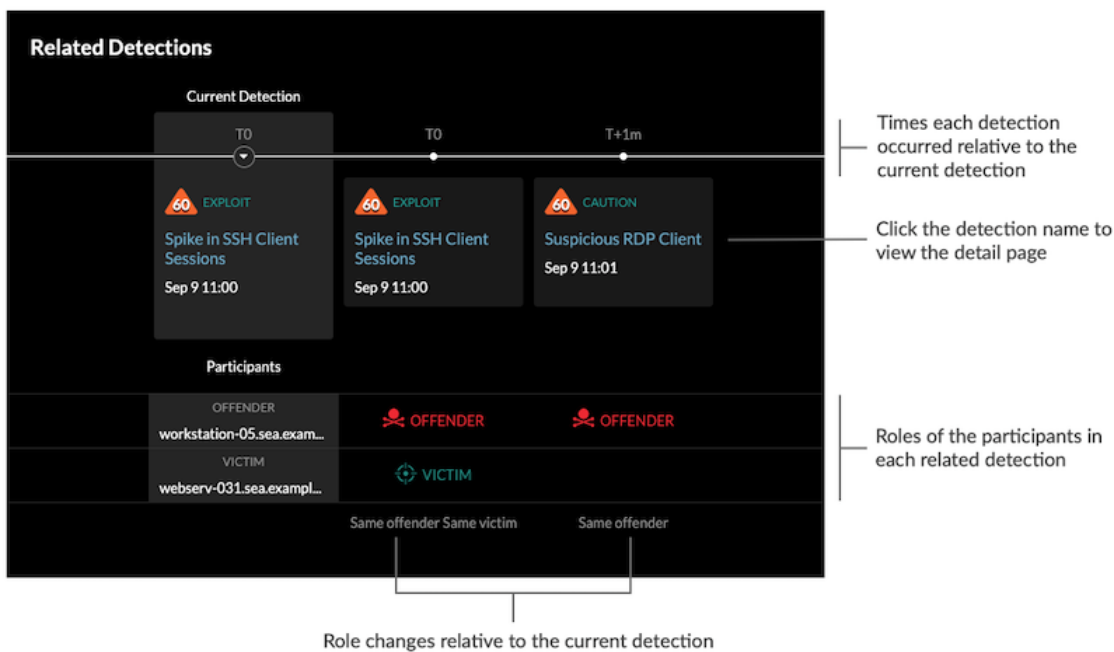
Related detections that are included in a recommended investigation are marked with gold links and can be clicked to navigate to the investigation page.

**Detection details**

Provides an expanded description of the detection, such as associated MITRE techniques, risk factors, attack backgrounds and diagrams, mitigation options, and reference links to security organizations such as MITRE.

These details are displayed next to the detection card on wide screens (1900 pixels or greater), or you can access them by clicking **Details** under the detection title when grouping the Detection page by **Types**.
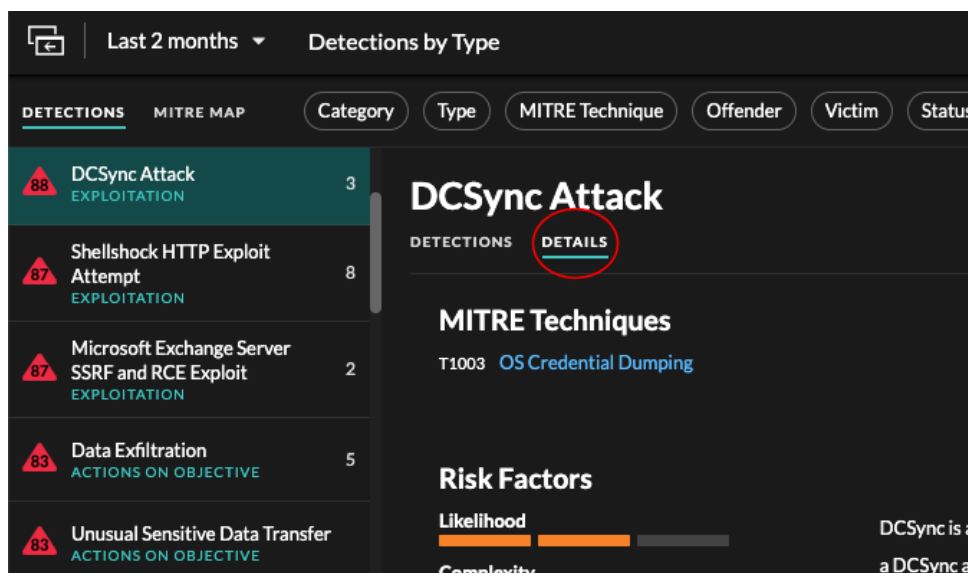


💡 **Tip:** You can share detection ↗ detail pages with other ExtraHop users.

# Detection Catalog

The Detection Catalog provides a complete list of all detection types in the ExtraHop system, including detection types that are currently inactive or in review. You can also manage custom detection types from the Detection Catalog page.

You can access the Detection Catalog page by clicking the System Settings icon ⚙.



In addition to the display name and author, you can filter the detection type list by ID, status, category, MITRE techniques associated with the detection type, and detection types that support data from flow sensors.

Click an ExtraHop-authored detection to view the Detection Type Settings panel, which displays the detection type name, ID, author, current status of the detection type, the date that the detection type was first released to production (when available), and associated categories. To learn more about the detection, click **Detection Type Details**.

**Detection type status**

This status identifies whether a detection is available in your environment.

**Active**

Active detection types are available for all sensors and can generate detections in your environment.

**Inactive**

Inactive detection types have been removed from all sensors and will no longer generate detections. When a detection type becomes Inactive, existing detections of that type will continue to display.

**In Review**

In Review detection types are evaluated on a limited number of ExtraHop systems before they are available for all sensors. These detection types pass a thorough review for efficiency and accuracy before they are made available to an increasing number of sensors. The review period can last up to several weeks. After review is complete, the detection type status is updated to Active.

Here are some important considerations about whether detections of a certain type are visible in your environment:

- If you do not see Active detections as expected, the detection type might require decryption ⧉ or might not support flow sensors (Reveal(x) 360 only).
- Reveal(x) Enterprise systems must be connected to Cloud Services ⧉ to receive frequent updates to the Detection Catalog. Without a connection to Cloud Services, updates are delayed ⧉ until firmware is upgraded.

**Custom detections**

You can view and manage custom detections from the Detection Catalog page.

- To create a custom detection type, click **Create** in the upper right corner of the page. The detection type ID for the new detection type must match the ID included in the custom detection trigger. Learn more about creating a custom detection ⧉.

- To edit a custom detection, click the detection and edit the display name, author, detection categories, and associated MITRE techniques in the Edit Detection Type panel. You cannot edit detections where ExtraHop is listed as the author.
- To delete a custom detection, click the detection, and then click **Delete** from the Detection Type Settings panel.
- Custom detections always display a dash (-) under Status.

## Investigations

(NDR module only) Investigations enable you to add and view multiple detections in a single timeline and map. Viewing a summary of connected detections can help you determine whether suspicious behavior is a valid threat and if a threat is from a single attack, or part of a larger attack campaign.

You can create and add to investigations from a detection detail page or from the **Actions** menu on each detection card. Your ExtraHop system will also create recommended investigations in response to potentially malicious activity.

Each investigation page includes the following tools:

**Investigation Timeline**

The investigation timeline appears on the left side of the page and lists the added detections, beginning with the most recent detection. New detections that are added to the investigation appear in the timeline according to the time and date the detection occurred. Detection participants are displayed under the detection title and detection tracking information, such as assignee and status, is displayed next to the participants.

**Attack Categories**

The categories of the added detections are displayed across the top of the investigation page.

The attack category chain displays the number of detections in each category, not the order in which the detections occurred. Refer to the investigation timeline for an accurate view of how the detections occurred over time.

## Viewing investigations

At the top of the investigation page, there are two options for viewing the investigation: Summary and Attack Map. Both options provide a unique view of your investigation.

**Summary**

By default, investigations open in **Summary** view, which includes the detection timeline, an aggregated list of participants, and a panel for tracking the status and response actions for the investigation.

You can click a detection in the investigation timeline to view detection details, then click the x icon to close the detection details and return to the investigation summary. You can also click the go to ⬈ icon in the upper right corner to view the detection details page in a new tab.

In the Participants panel, participants in the investigation are grouped by external endpoints, high value devices, and recurring participants, which are participants that appear in multiple detections in the investigation. Click on a participant to view details and access links.

In the Status and Response Actions panel, click **Edit Investigation** to change the investigation name, set the status or final assessment of the investigation, specify an assignee, or add notes.

You can continue to track individual detections ↗ after you add them to an investigation.

**Attack Map**

In **Attack Map** view, the offender and victim from every detection in the investigation are displayed in an interactive map next to the investigation timeline.



The participants are connected by lines that are labeled with the detection type, and device roles are represented by an icon.

- Click a detection in the investigation timeline to highlight participants. Circles are highlighted in red if the device has appeared as an offender in at least one detection in the investigation and

are highlighted in teal if the device is a victim. Highlights are updated when you click a different detection to help you identify when a participant changes from victim to offender.

- Click a circle to view details such as the device hostname, IP address, or MAC address, or to navigate to associated detections or the Device Overview page ⬀.
- Hover over any circle or line to display the label.

## Recommended investigations

The ExtraHop Machine Learning Service monitors network activity for combinations of attack techniques that might indicate malicious behavior. When a combination is identified, the ExtraHop system will create a recommended investigation, enabling your security teams to assess the situation and respond quickly if malicious behavior is confirmed.

For example, if a device is the victim in a detection in the Command-and-Control category, but becomes the offender in an Exfiltration detection, the ExtraHop system will recommend a C&C with Exfiltration investigation.



You can interact with recommended investigations in the same way as user-created investigations, such as adding or removing detections, specifying an assignee, and setting a status and assessment.

Recommended investigations can be found in the investigations table. You can sort the Created By column to find investigations that were created by ExtraHop.

## Navigating investigations

After a detection is added to an investigation, a link to the investigation appears at the bottom of the detection card and on the detection detail page.

Click the name to open the investigation and then click the name of the detection on the investigation page to return to the detection detail page.

Learn how to create an investigation ⬈.

## Finding detections in the ExtraHop system

While the Detections page provides quick access to all detections, there are indicators and links to detections throughout the ExtraHop system.

> **Note:** Detections remain in the system according to your system lookback capacity ⬈ for 1-hour metrics, with a minimum storage time of five weeks. Detections will remain in the system without supporting metrics if your system lookback capacity is less than five weeks.

- From a Device Overview page, click Detections to view a list of associated detections. Click the link for an individual detection to view the detection details page.
- From a Device Group Overview page, click the Detections link to go to the Detections page. The detections list is filtered to the device group as the source.
- From a device or device group protocol page, click the Detections link to go to the Detections page. The detections list is filtered to the source and protocol.
- On an activity map, click a device that displays animated pulses around the circle label to view a list of associated detections ⬈. Click the link for an individual detection to view detection details.
- From a chart on a dashboard or protocol page, hover over a detection marker ⬈ to display the title of the associated detection or click the marker to view detection details.