



**HORIZON**

08 June 2023

# **HORIZON XDR/XPR**

Administration Guide



# Check Point Copyright Notice

© 2023 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

## RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c) (1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

## TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

# Important Information



## Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



## Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



## Latest Version of this Document in English

Open the latest version of this [document in a Web browser](#).  
Download the latest version of this [document in PDF format](#).



## Feedback

Check Point is engaged in a continuous effort to improve its documentation.  
[Please help us by sending your comments](#).

## Revision History

| Date             | Description  |
|------------------|--|
| 01 June 2023     | Added information about "API Support" on page 8.                                   |
| 15 March 2023    | Updated "Getting Started" on page 9.   |
| 06 March 2023    | Added the Take number for on-boarding Quantum Security Gateway on-premises R81.10. |
| 24 February 2023 | First release of this document   |

# Table of Contents

---

|  |    |
|--|----|
| Introduction to Horizon XDR/XPR .....                    | 7  |
| Benefits .....   | 7  |
| Use Case .....   | 8  |
| Supported Products .....                                 | 8  |
| API Support .....  | 8  |
| Horizon XDR/XPR API .....                                | 8  |
| Horizon Threat Hunting API .....                         | 8  |
| Getting Started .....                                    | 9  |
| Creating an Account in the Infinity Portal .....         | 9  |
| Accessing the Horizon XDR/XPR Administrator Portal ..... | 9  |
| Licensing the Product .....                              | 10 |
| On-boarding Products .....                               | 10 |
| Adding Users .....                                       | 12 |
| How to Address an Incident .....                         | 13 |
| Overview .....   | 14 |
| Sources .....  | 14 |
| XDR/XPR Prevention Status .....                          | 15 |
| Prevention by Sources .....                              | 15 |
| Open Incidents by Assignee .....                         | 15 |
| Incidents .....  | 16 |
| Incidents Over Time .....                                | 16 |
| News .....   | 17 |
| Incidents .....  | 18 |
| Top Banner .....   | 21 |
| Incidents - Overview .....                               | 22 |
| Incident Summary .....                                   | 23 |
| MITRE .....  | 24 |
| Assets and Indicators .....                              | 24 |
| Managing Assets and Indicators .....                     | 25 |
| Prevention .....   | 26 |
| Insights Timeline .....                                  | 27 |
| Comments .....   | 27 |
| Adding a Comment .....                                   | 27 |

---



---

|  |    |
|--|----|
| Incidents - Affected Assets .....                                  | 27 |
| Managing Affected Assets .....                                     | 29 |
| Creating an Exclusion for an Asset from an Incident .....          | 30 |
| Incidents - Indicators & Artifacts .....                           | 31 |
| Managing Indicators and Artifacts .....                            | 34 |
| Adding or Editing an Indicator or Artifact in IoC Management ..... | 34 |
| Removing an Indicator from IoC Management .....                    | 35 |
| Incidents - MITRE .....  | 35 |
| Incidents - Insights & Forensics .....                             | 36 |
| Incidents - Attack Tree .....                                      | 37 |
| Policy .....   | 38 |
| Automations .....  | 38 |
| Exclusions .....   | 38 |
| Configuring an Exclusion .....                                     | 38 |
| Editing an Exclusion .....   | 39 |
| Exporting Exclusions .....   | 39 |
| Notifications .....  | 39 |
| Sending Email, Slack, and Microsoft Teams Notifications .....      | 40 |
| Testing the Notifications .....                                    | 41 |
| Events .....   | 42 |
| Statistics .....   | 42 |
| Events Table .....   | 42 |
| Managing the Events Table .....                                    | 44 |
| Viewing Events for a Time Period .....                             | 45 |
| Searching for Events .....   | 45 |
| Exporting Events .....   | 45 |
| Card .....   | 46 |
| Intelligence .....   | 48 |
| Viewing Intelligence for Indicators .....                          | 48 |
| Intelligence Dashboard .....                                       | 50 |
| Indicator Information .....  | 50 |
| Research .....   | 51 |
| Check Point Traffic Analysis .....                                 | 52 |
| Open Source Intelligence Tools .....                               | 52 |
| Managing Indicators in IoC Management .....                        | 53 |

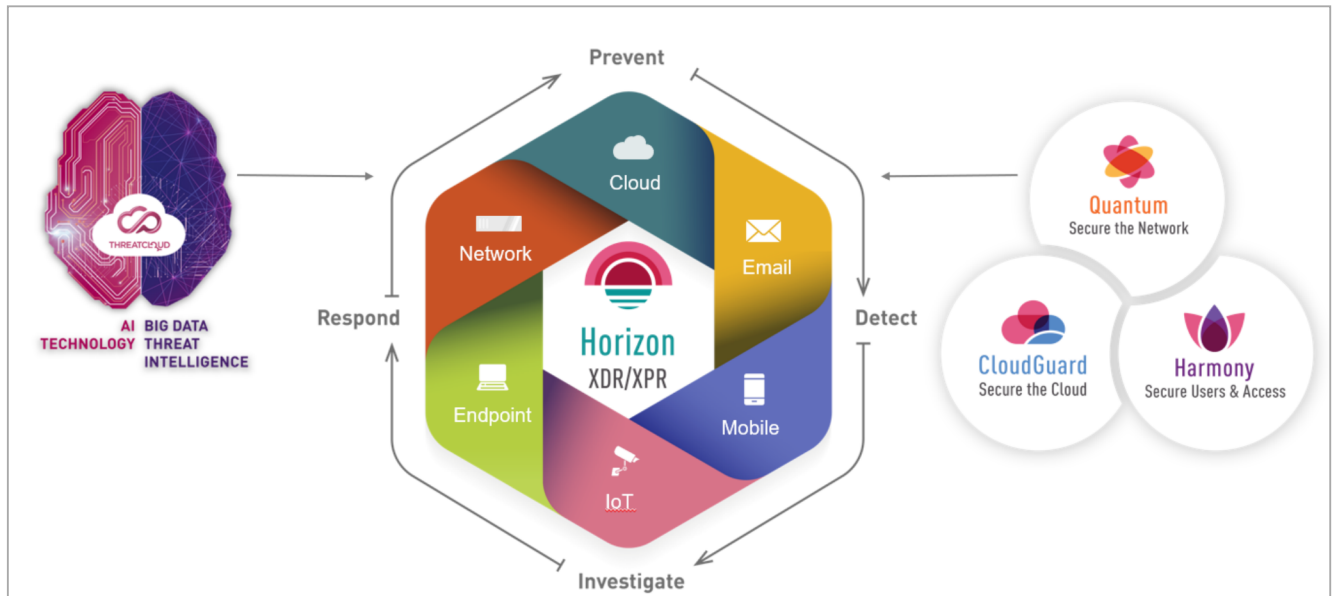
---

---

|   |    |
|---|----|
| Exporting the Search Summary to a CSV .....                     | 54 |
| Copying and Removing an Indicator from the Search Summary ..... | 54 |
| Analyzing a File .....  | 54 |
| Investigating a File .....                                      | 56 |
| Adding a File to IoC Management .....                           | 56 |
| IoC Management .....  | 58 |
| IOC Management Overview .....                                   | 58 |
| Working with IoC Management .....                               | 58 |
| Creating a New IoC .....  | 59 |
| Adding IoCs by Uploading a CSV File .....                       | 61 |
| Editing and Deleting an IoC .....                               | 61 |
| Filtering IoCs .....  | 62 |
| Exporting IoCs .....  | 62 |
| Configuring IoC Management .....                                | 62 |
| Testing IoC Management .....                                    | 66 |
| Threat Hunting .....  | 67 |
| Supported Versions .....  | 67 |
| Enabling Threat Hunting .....                                   | 67 |
| Using Threat Hunting .....                                      | 68 |
| Use Case - Maze Ransomware Threat Hunting .....                 | 71 |

# Introduction to Horizon XDR/XPR

Check Point Horizon XDR/XPR is an Extended Detection Response (XDR) and Extended Prevention Response (XPR) tool that provides a unified view of all the security operations across onboarded products and helps you detect, respond to and prevent cyber attacks.



**i** Note - Check Point CloudGuard is not supported currently.

Horizon XDR/XPR uses Check Point ThreatCloud's Artificial Intelligence (AI) and Machine Learning (ML) to analyze security events across the products to identify security risks in your organization. If a security risk is detected, it generates an [incident](#) (alert) with an appropriate priority based on the severity and confidence level of the detection, and provides mitigation to the incident. Incidents are also fully mapped to the MITRE ATT&CK framework and also allows you to view the internal and external intelligence available for an indicator and analyze files for threats.

## Benefits

- Unified view for all the security operations across products.
- Correlates multiple logs across products to a single security incident.
- Early automatic detection and response to security events across your products.
- Eliminates false positives.
- Provides a comprehensive understanding of your organization's security posture, which allows you to take more confident and effective actions to mitigate and prevent attacks.
- Advanced User Entity Behavioral Analytics (UEBA) detections.

# Use Case

You are subscribed to multiple products and you want a single application to prevent, detect, investigate, and respond to security attacks.

## Supported Products

Horizon XDR/XPR is supported with these products:

- Check Point Quantum Security Gateway Management
  - On-premises R81.10 with the [R81.10 Jumbo Hotfix Accumulator](#) Take 93 and higher.
  - Smart-1 Cloud
- Check Point Harmony Endpoint (EPMaaS)
- Check Point Harmony Email & Collaboration

## API Support

### Horizon XDR/XPR API

You can use the Horizon XDR/XPR REST APIs to query incidents and forensic data in Horizon XDR/XPR.

To access Horizon XDR/XPR API:

1. Go to [https://sc1.checkpoint.com/documents/latest/api\\_reference/index.html](https://sc1.checkpoint.com/documents/latest/api_reference/index.html).
2. Click Horizon.
3. In the Horizon XDR/XPR API widget, click Open.

### Horizon Threat Hunting API

You can use the Horizon Threat Hunting GraphQL APIs to query Horizon Threat Hunting and retrieve information about events reported by your devices.

To access Horizon Threat Hunting API:

1. Go to [https://sc1.checkpoint.com/documents/latest/api\\_reference/index.html](https://sc1.checkpoint.com/documents/latest/api_reference/index.html).
2. Click Horizon.
3. In the Horizon Threat Hunting API widget, click Open.

# Getting Started

To get started with Horizon XDR/XPR:

1. [Create an Account in the Infinity Portal](#)
2. [Access the Horizon XDR/XPR Administrator Portal](#)
3. [License the product](#)
4. [On-board Applications](#)
5. [Add Users](#)
6. [Address an Incident](#)

## Creating an Account in the Infinity Portal

Check Point Infinity Portal is a web-based interface that hosts the Check Point security SaaS services. With Infinity Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

To create an Infinity Portal account, see the [Infinity Portal Administration Guide](#).

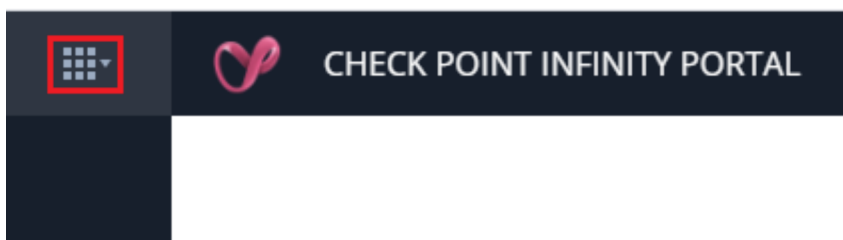
## Accessing the Horizon XDR/XPR Administrator Portal



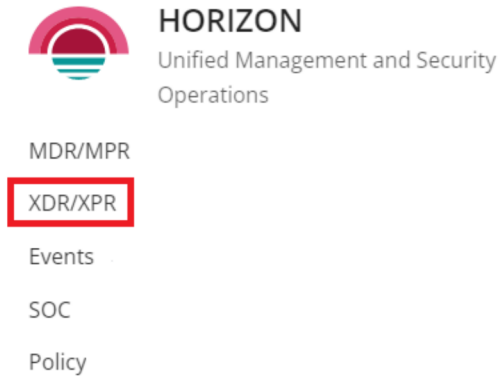
Note - The recommended browser is Google Chrome.

To access the Horizon XDR/XPR Administrator Portal:

1. Sign in to [Check Point Infinity Portal](#).
2. Click the Menu button in the top left corner.



- Under Horizon, click XDR/XPR.



The "Overview" on page 14 page appears.

## Licensing the Product

When you create an account in the Infinity Portal and access the service, you get a free 30-day trial. After the 30-day trial period, you must purchase a software license to use the product. To purchase a license, you must create a Check Point User Center account. For instructions, see [sk22716](#).

After you create a User Center account, contact your Check Point sales representative to purchase a license.

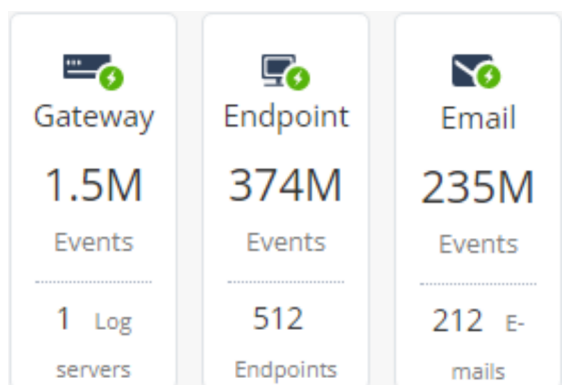
If you have licensed the product, you can view your current contract (license) information from the Infinity Portal > Global Settings > Contracts page.


## On-boarding Products

This table provides the on-boarding process for the supported products:

| Product Family | Product Name                  | On-boarding Process   |
|----------------|-------------------------------|---|
| Check Point    | Quantum Security Gateway      | <ul style="list-style-type: none"> <li>■ On premises               <ul style="list-style-type: none"> <li>• For R81.10 with the <a href="#">R81.10 Jumbo Hotfix Accumulator Take 93</a> and higher, see <a href="#">Sharing SmartConsole Configuration and Logs with Infinity Portal</a> &gt; To share your on-premises Management Server log information with the Infinity Portal in the <a href="#">R81.10 Security Management Administration Guide</a>.</li> <li>• For R81.20, see <a href="#">Sharing SmartConsole Configuration and Logs with Infinity Portal</a> &gt; To share your on-premises Management Server log information with the Infinity Portal in the <a href="#">R81.20 Security Management Administration Guide</a>.</li> </ul> </li> <li>📘 Note - You can on-board only one Security Management Server. Multi-Domain Security Management Server is not supported.</li> <li>■ Smart-1 Cloud - Automatic if you subscribe to Horizon XDR/XPR.</li> </ul> |
|                | Harmony Endpoint (EPMaaS)     | <p>Automatic if you subscribe to Horizon XDR/XPR. Ensure that you enable Threat Hunting in Harmony Endpoint. To enable, see <a href="#">"Enabling Threat Hunting" on page 67</a>.</p> <p>📘 Note - You can on-board only one account (tenant) of Harmony Endpoint.</p>   |
|                | Harmony Email & Collaboration | <p>Automatic if you subscribe to Horizon XDR/XPR.</p> <p>Note - You can on-board only one account (tenant) of Harmony Email &amp; Collaboration.</p>  |

After you successfully on-board,  appears for the product in the Source widget.



If  does not appear after 45 minutes of on-boarding, contact Check Point [Support](#).

# Adding Users

To address incidents, you must assign it to a Security Operations Center (SOC) analyst (assignee) in your organization. To assign, you must add SOC analysts as users with **Operator** service specific role in the Horizon XDR/XPR portal. The specific service roles are in addition to the global rules and do not override them. For more information, see [Specific Service Rules](#) in the Infinity Portal Administration Guide.

To access Specific Service Roles, go to **Global Settings > Users > New > Add User** and expand **Specific Service Roles**.

| Role           | Description  |
|----------------|--|
| Admin          | Full Read & Write access to all system aspects.  |
| Operator       | Has full access to handle incidents, including taking prevention actions, and read-only access to the Policy menu.<br>Typically, your SOC analyst. |
| Read-Only User | Has read-only access to the application.   |

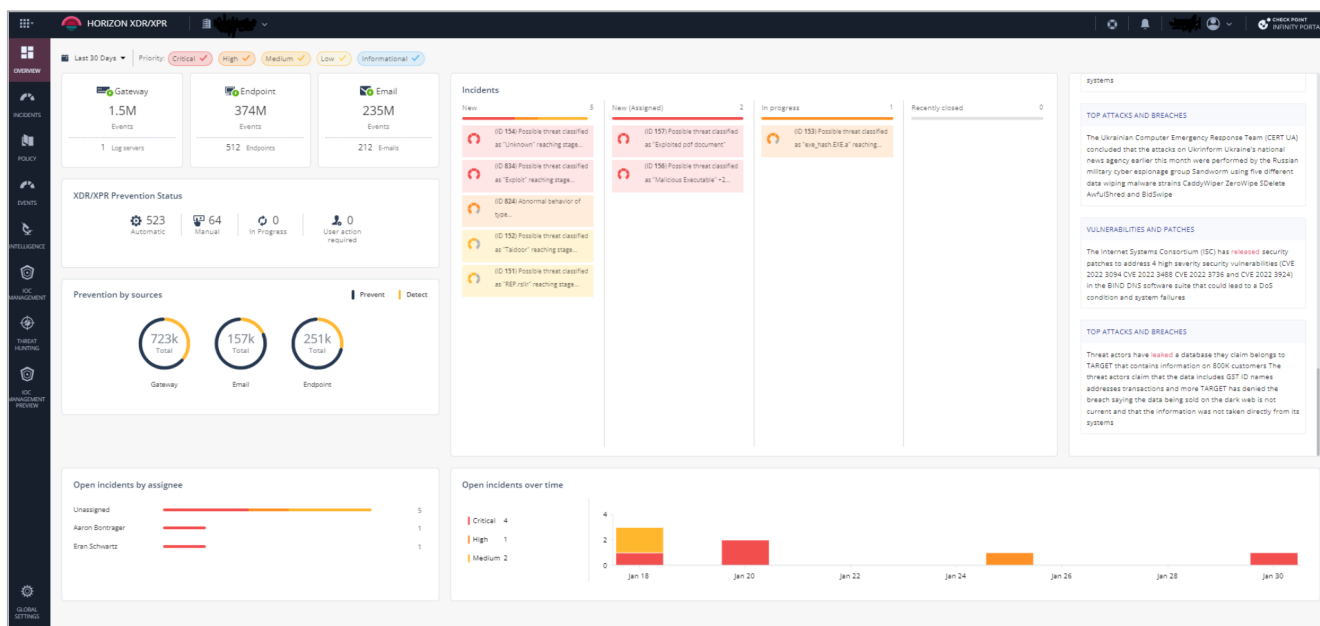


# How to Address an Incident

| Step | Owner           | Action  |
|------|-----------------|---|
| 1    | Horizon XDR/XPR | Horizon XDR/XPR generates an incident.  |
| 2    | Administrator   | Assign the incident to a Security Operations Center (SOC) analyst.  |
| 3    | SOC Analyst     | In the <a href="#">"Incidents" on page 18</a> page, review these information on the incident: <ul style="list-style-type: none"> <li>▪ Description</li> <li>▪ Priority level</li> <li>▪ Sources</li> <li>▪ MITRE ATT&amp;CK tactics involved.</li> <li>▪ Assets involved.</li> <li>▪ Identified Indicators of Compromise.</li> <li>▪ Prevention actions taken and recommended prevention actions.</li> <li>▪ Timeline of the incident</li> </ul>  |
| 4    | SOC Analyst     | For further investigation on the incident: <ul style="list-style-type: none"> <li>▪ See <a href="#">"Incidents - Insights &amp; Forensics" on page 36</a> to view insights and forensics (processes, files, URL, domains and Registry involved in the insight) related to the incident.</li> <li>▪ See <a href="#">"Incidents - Affected Assets" on page 27</a> to view the assets involved in the incident.</li> <li>▪ See <a href="#">"Incidents - Indicators &amp; Artifacts" on page 31</a> to view the indicators and artifacts involved the incident.</li> <li>▪ See <a href="#">"Incidents - Attack Tree" on page 37</a> to view a graphical representation of the forensic report generated by Harmony Endpoint for each detection in an insight.</li> <li>▪ See <a href="#">"Incidents - MITRE" on page 35</a> to know the MITRE ATT&amp;CK tactics used in the incident.</li> </ul> |
| 5    | SOC Analyst     | To investigate the Indicator of Compromise involved in the incident and analyze a file, see <a href="#">"Intelligence" on page 48</a> .   |
| 6    | SOC Analyst     | To investigate the logs further, see <a href="#">"Threat Hunting" on page 67</a> .  |
| 7    | SOC Analyst     | Take the recommended prevention actions. See <a href="#">"Prevention" on page 26</a> .  |

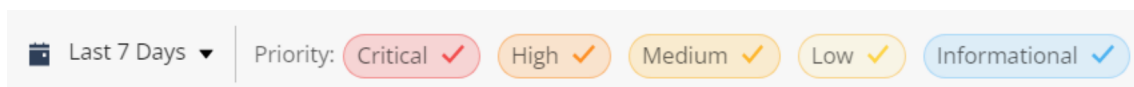
# Overview

The Overview page shows a summary of the security operations of the on-boarded applications.



To view the Overview page, access Horizon XDR/XPR and click Overview.

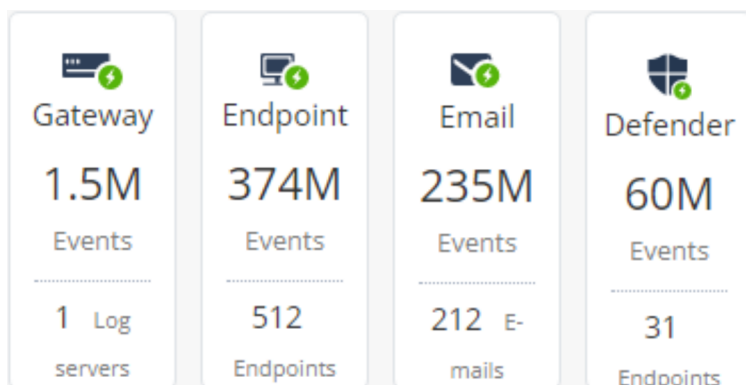
By default, the Overview page shows the data (all priorities) from the last 7 days.



To filter the data by priority:

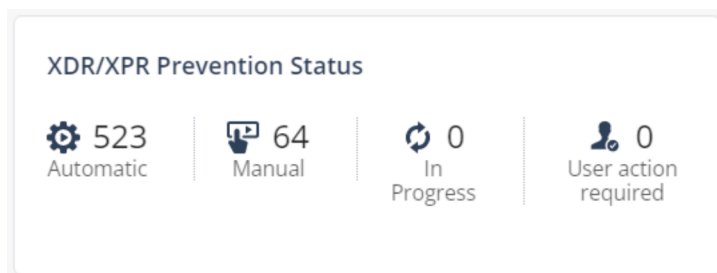
1. Select the time period. By default, it lists from the last 7 days.
2. Select the Priority. By default, all priority levels are selected.

## Sources



The Sources widget shows the number of logs and devices for the connected products.

## XDR/XPR Prevention Status



The XDR/XPR Prevention Status widget displays the prevention status in Horizon XDR/XPR.

- Automatic - The number of prevention steps taken automatically by Horizon XDR/XPR.
- Manual - The number of prevention steps taken manually by the users.
- In Progress - The number of prevention steps that are in progress.
- User action required - The number of prevention steps that require user action.

## Prevention by Sources



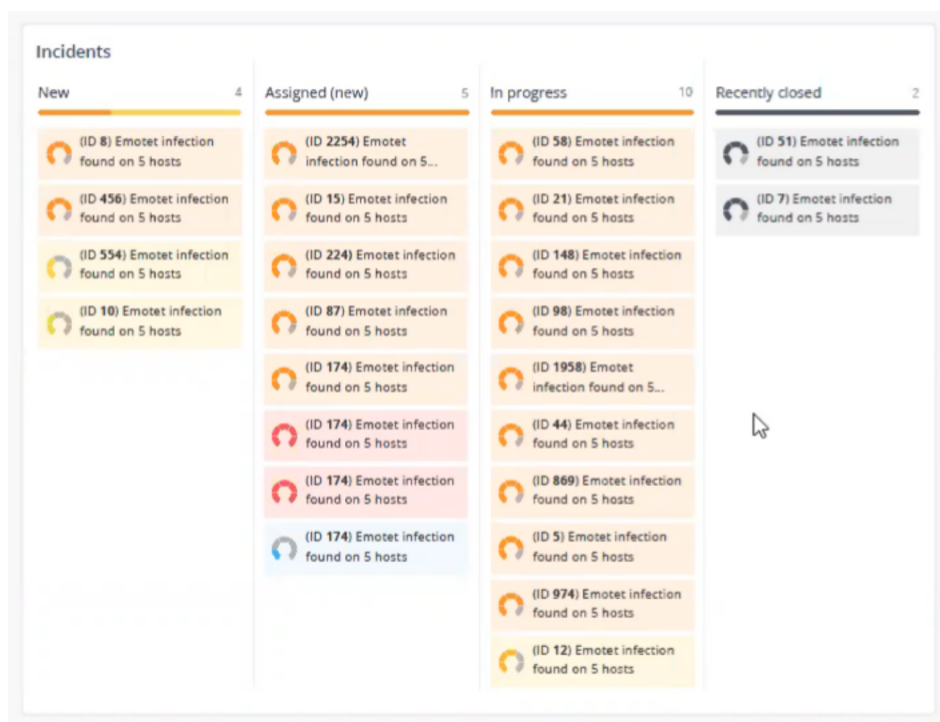
The Prevention by sources widget shows the number of security events analyzed for each on-boarded application and the respective security risk (detect/prevent) action.

## Open Incidents by Assignee



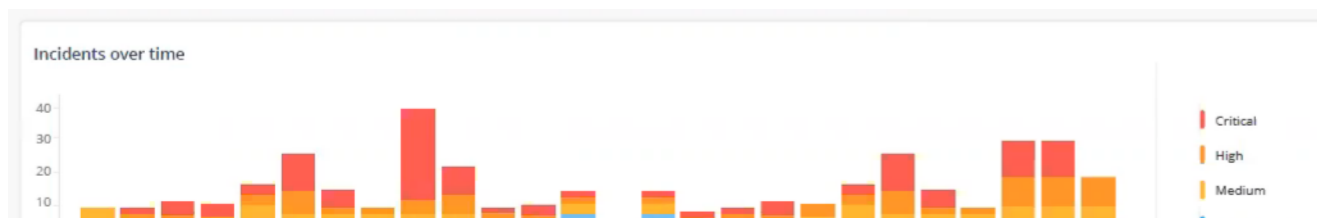
The Open incidents by Assignee widget lists the number of open incidents for each assignee. Incidents are color-coded based on the priority levels.

# Incidents



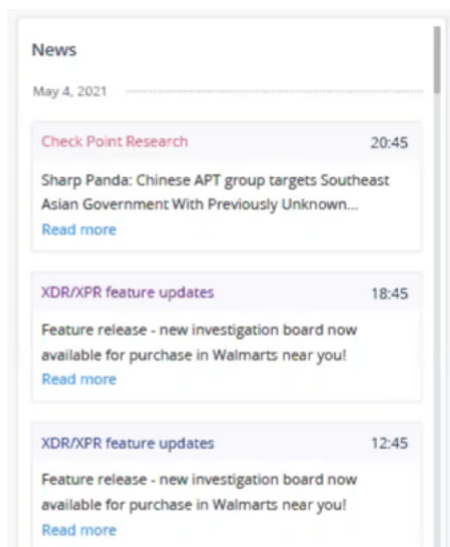
The Incidents widget lists incidents by status. Hover over the incident for more information. Incidents are color-coded based on the priority levels.

# Incidents Over Time



The Incidents over time widget shows the timeline of incidents by priority. Incidents are color-coded based on the priority levels.

# News



The News widget shows the latest cyber security news provided by Check Point Research.

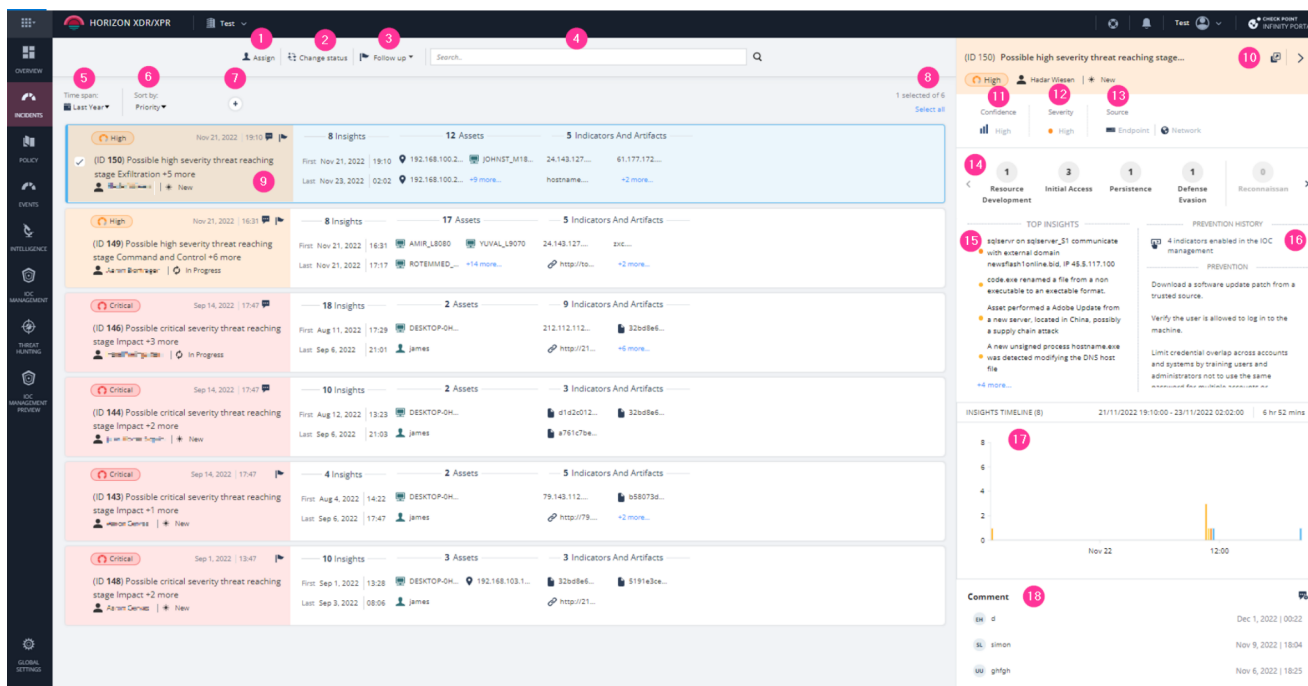
# Incidents

An incident is a collection of events from one or more products that together represent an attack story. Horizon XDR/XPR utilizes ThreatCloud's Artificial Intelligence (AI) and applies Machine Learning (ML) models to correlate between the events from on-boarded products (both benign and security events) into unified incidents. The incident's priority level is calculated based on the artifacts of the incident, including the confidence and severity levels of the detection. Incidents are actionable with prevention steps that can be taken within the Horizon XDR/XPR application.



The Incidents page shows the list of incidents and its details that includes:

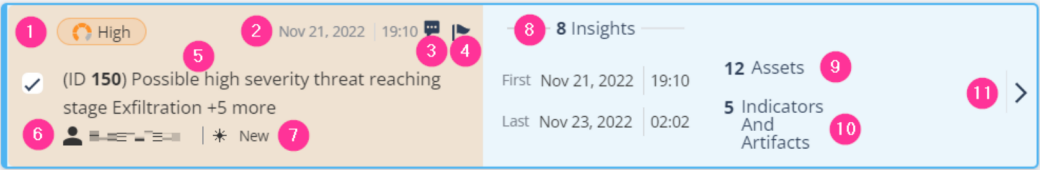
- Insights that triggered the incident and its timeline
- Impacted assets and users
- Indicators
- Prevention history and recommended prevention actions. You can automate some of these actions. For more information, see "Automations" on page 38.

To view the Incidents page, access Horizon XDR/XPR and click Incidents.





| Legend | Item          | Description  |
|--------|---------------|--|
| 1      | Assign        | Assign a security expert to address the incident.  |
| 2      | Change status | Change the status of the incident. <ul style="list-style-type: none"> <li>■ New</li> <li>■ In Progress</li> <li>■ Close - Handled</li> <li>■ Close - False Positive</li> <li>■ Close - Known Activity</li> </ul> |

| Legend | Item   | Description   |
|--------|--|---|
| 3      | Follow up  | Indicates that the incident requires a follow-up.<br> Note - Horizon XDR/XPR does not send automatic reminders for follow-up.            |
| 4      | Search   | Search for the an asset, incident or a user.  |
| 5      | Time span  | Select the duration for which you want to view the incidents. <ul style="list-style-type: none"> <li>▪ Last 24 hours</li> <li>▪ Last week</li> <li>▪ Last two weeks</li> <li>▪ Last month</li> <li>▪ Last year</li> </ul> |
| 6      | Sort by  | Select a criterion to sort the incidents. <ul style="list-style-type: none"> <li>▪ Priority</li> <li>▪ Creation date</li> <li>▪ Last update</li> <li>▪ Severity</li> </ul>  |
| 7      | <br>(Filter) | Filter the incidents by: <ul style="list-style-type: none"> <li>▪ Assignee</li> <li>▪ Status</li> <li>▪ Priority</li> </ul>   |
| 8      | Select all   | Select or clear all incidents.  |

| Legend | Item  | Description   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
|--------|---|---|--------|-------------|---|--|---|--|---|--|---|---|---|--|---|---|---|--|---|---|---|--|----|--|----|---|
| 9      | Incident  | <p>Shows incident details.</p>  <table border="1" data-bbox="416 465 1461 1883"> <thead> <tr> <th>Legend</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Priority of the incident:                             <ul style="list-style-type: none"> <li>Critical</li> <li>High</li> <li>Medium</li> <li>Low</li> <li>Informational</li> </ul> </td> </tr> <tr> <td>2</td> <td>Date and time when the incident was generated.</td> </tr> <tr> <td>3</td> <td>View the comments added related to the incident.</td> </tr> <tr> <td>4</td> <td>Add or remove the follow-up flag on the incident.</td> </tr> <tr> <td>5</td> <td>Incident ID and title. Click the title to open the <a href="#">"Incidents - Overview" on page 22</a> page.</td> </tr> <tr> <td>6</td> <td>Security Operations Center (SOC) analyst assigned to the incident. Shows Unassigned if an incident is unassigned.</td> </tr> <tr> <td>7</td> <td>Status of the incident. Click to set the status.                             <ul style="list-style-type: none"> <li>New</li> <li>In Progress</li> <li>Close - Handled</li> <li>Close - False Positive</li> <li>Close - Known Activity</li> </ul> </td> </tr> <tr> <td>8</td> <td>Number of insights involved in triggering the incident with date and time when the first and last insight was created. Click to view <a href="#">"Incidents - Insights &amp; Forensics" on page 36</a> page. An insight is an aggregation of one or more logs into valuable observations indicating the nature of the activity.</td> </tr> <tr> <td>9</td> <td>Number of assets involved in the incident.</td> </tr> <tr> <td>10</td> <td>Number of indicators and artifacts involved in the incident.</td> </tr> <tr> <td>11</td> <td>Opens the <a href="#">"Incidents - Overview" on page 22</a> page.</td> </tr> </tbody> </table> | Legend | Description | 1 | Priority of the incident: <ul style="list-style-type: none"> <li>Critical</li> <li>High</li> <li>Medium</li> <li>Low</li> <li>Informational</li> </ul> | 2 | Date and time when the incident was generated. | 3 | View the comments added related to the incident. | 4 | Add or remove the follow-up flag on the incident. | 5 | Incident ID and title. Click the title to open the <a href="#">"Incidents - Overview" on page 22</a> page. | 6 | Security Operations Center (SOC) analyst assigned to the incident. Shows Unassigned if an incident is unassigned. | 7 | Status of the incident. Click to set the status. <ul style="list-style-type: none"> <li>New</li> <li>In Progress</li> <li>Close - Handled</li> <li>Close - False Positive</li> <li>Close - Known Activity</li> </ul> | 8 | Number of insights involved in triggering the incident with date and time when the first and last insight was created. Click to view <a href="#">"Incidents - Insights &amp; Forensics" on page 36</a> page. An insight is an aggregation of one or more logs into valuable observations indicating the nature of the activity. | 9 | Number of assets involved in the incident. | 10 | Number of indicators and artifacts involved in the incident. | 11 | Opens the <a href="#">"Incidents - Overview" on page 22</a> page. |
| Legend | Description   |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 1      | Priority of the incident: <ul style="list-style-type: none"> <li>Critical</li> <li>High</li> <li>Medium</li> <li>Low</li> <li>Informational</li> </ul>  |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 2      | Date and time when the incident was generated.  |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 3      | View the comments added related to the incident.  |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 4      | Add or remove the follow-up flag on the incident.   |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 5      | Incident ID and title. Click the title to open the <a href="#">"Incidents - Overview" on page 22</a> page.  |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 6      | Security Operations Center (SOC) analyst assigned to the incident. Shows Unassigned if an incident is unassigned.   |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 7      | Status of the incident. Click to set the status. <ul style="list-style-type: none"> <li>New</li> <li>In Progress</li> <li>Close - Handled</li> <li>Close - False Positive</li> <li>Close - Known Activity</li> </ul>  |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 8      | Number of insights involved in triggering the incident with date and time when the first and last insight was created. Click to view <a href="#">"Incidents - Insights &amp; Forensics" on page 36</a> page. An insight is an aggregation of one or more logs into valuable observations indicating the nature of the activity. |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 9      | Number of assets involved in the incident.  |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 10     | Number of indicators and artifacts involved in the incident.  |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |
| 11     | Opens the <a href="#">"Incidents - Overview" on page 22</a> page.   |   |        |             |   |  |   |  |   |  |   |   |   |  |   |   |   |  |   |   |   |  |    |  |    |   |



| Legend | Item  | Description  |
|--------|---|--|
| 10     |  | Opens the incident " <a href="#">Incidents - Overview</a> " on the next page in a new tab.   |
| 11     | Confidence  | Confidence level of the detection: <ul style="list-style-type: none"> <li>High</li> <li>Medium</li> <li>Low</li> </ul>   |
| 12     | Severity  | Priority of the incident: <ul style="list-style-type: none"> <li>Critical</li> <li>High</li> <li>Medium</li> <li>Low</li> <li>Informational</li> </ul>   |
| 13     | Source  | The source of the events correlated into the incident. <ul style="list-style-type: none"> <li>Endpoint (Harmony Endpoint)</li> <li>Gateway (Quantum Security Gateway)</li> <li>Email (Harmony Email &amp; Collaboration)</li> </ul>  |
| 14     | MITRE ATT&CK  | <a href="#">MITRE ATT&amp;CK</a> tactics and techniques involved in the incident. The numbers represent the number of insights related to each tactic. Opens the " <a href="#">Incidents - Insights &amp; Forensics</a> " on page 36 page that shows the related insights. |
| 15     | Top Insights  | Top insights for the incident.   |
| 16     | Prevention  | Lists prevention actions taken and those that are recommended to be taken.   |
| 17     | Insights Timeline   | Shows the timeline of insights and the duration between the first and the last insight.  |
| 18     | Comments  | Shows the comments added for the incident. Click  to add a comment.   |

## Top Banner

The top banner is displayed in these pages:

- "[Incidents - Overview](#)" on the next page
- "[Incidents - Affected Assets](#)" on page 27
- "[Incidents - Indicators & Artifacts](#)" on page 31

- "Incidents - MITRE" on page 35
- "Incidents - Insights & Forensics" on page 36
- "Incidents - Attack Tree" on page 37.



You can see the incident title, priority of the incident and allows you to [add a comment](#) and [change incident status](#).

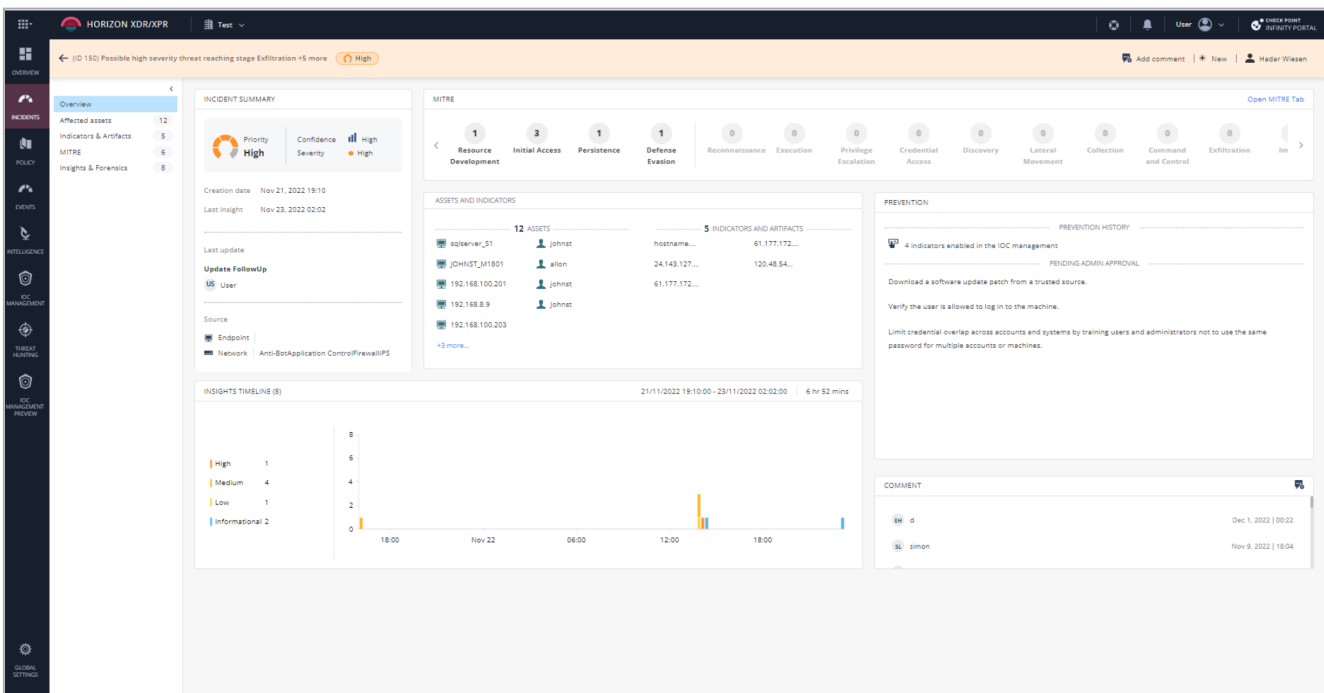
## Incidents - Overview

The Overview page shows the details of the incident and allows you to perform these actions:

- "Managing Assets and Indicators" on page 25
  - Copying an asset, indicator or artifact name to the clipboard
  - Viewing forensic details related to the chosen asset
  - Viewing intelligence for asset, indicator or an artifact
  - Searching for an asset, indicator or an artifact in an incident
- Execute prevention actions. See "Prevention" on page 26
- "Adding a Comment" on page 27


To view the Overview page, access Horizon XDR/XPR and click Incidents:

- Click the incident title.
- Hover over the incident and click >.




# Incident Summary

## INCIDENT SUMMARY



Priority  
**High**


Confidence



High

---

Severity



High


Creation date Nov 21, 2022 19:10

Last insight Nov 23, 2022 02:02

---

Last update


### Update FollowUp

 User

---

Source

 Endpoint

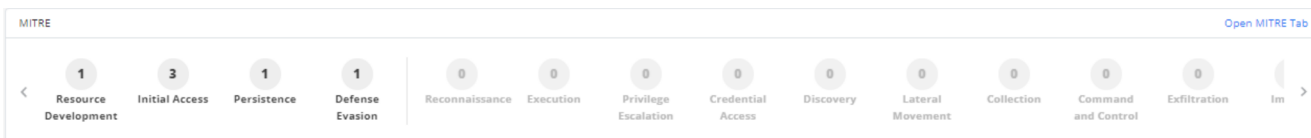
 Network | Anti-BotApplication ControlFirewallIPS

The Incident Summary widget shows:

- Priority of the incident:
  - Critical
  - High
  - Medium
  - Low
  - Informational
- Confidence level of the detection:
  - High
  - Medium
  - Low
- Severity of the incident:

- Critical
  - High
  - Medium
  - Low
  - Informational
- Creation date - Date and time when incident was created.
  - Last insight - Date and time when the last insight was added to the incident.
  - Last update on the incident
  - The source of the events correlated into the incident.
    - Endpoint (Harmony Endpoint)
    - Gateway (Quantum Security Gateway)
    - Email (Harmony Email & Collaboration)

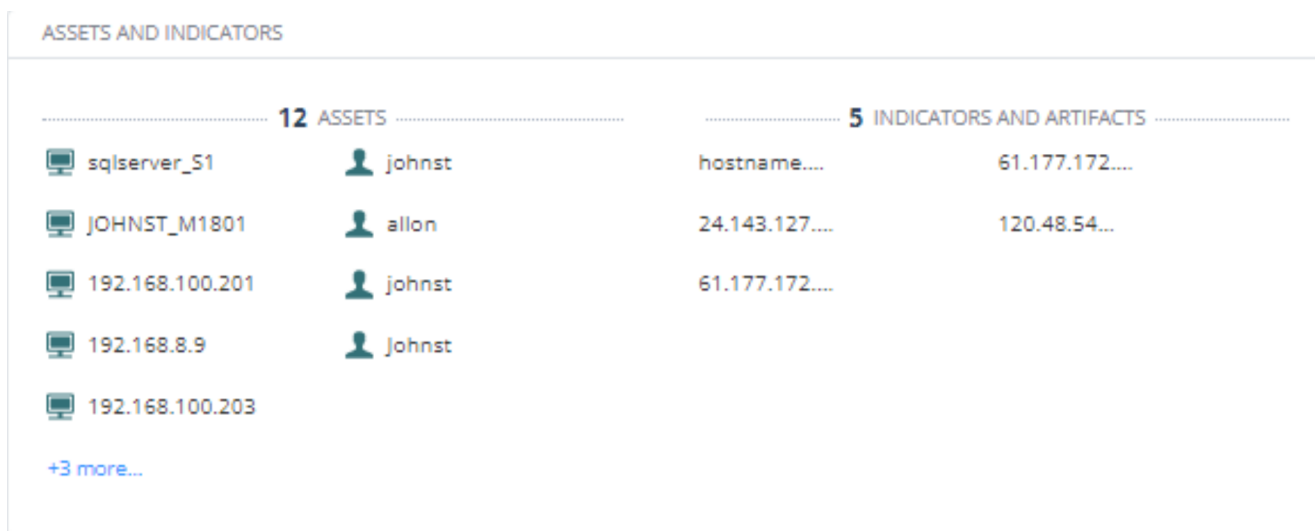
## MITRE



[MITRE ATT&CK](#) tactics and techniques involved in the incident. The numbers represent the number of insights related to each tactic.

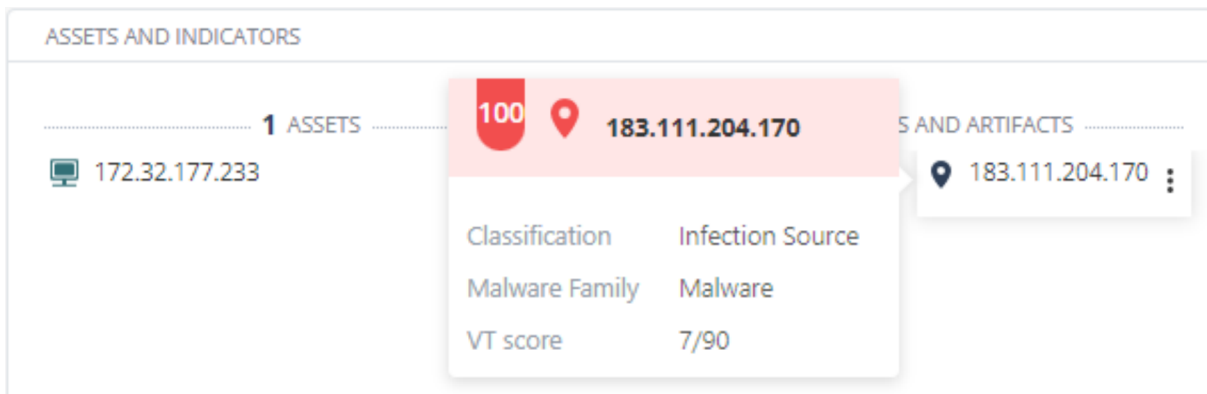
Click Open MITRE Tab to open the "Incidents - MITRE" on page 35 page.

## Assets and Indicators



The Assets and Indicators widget shows:

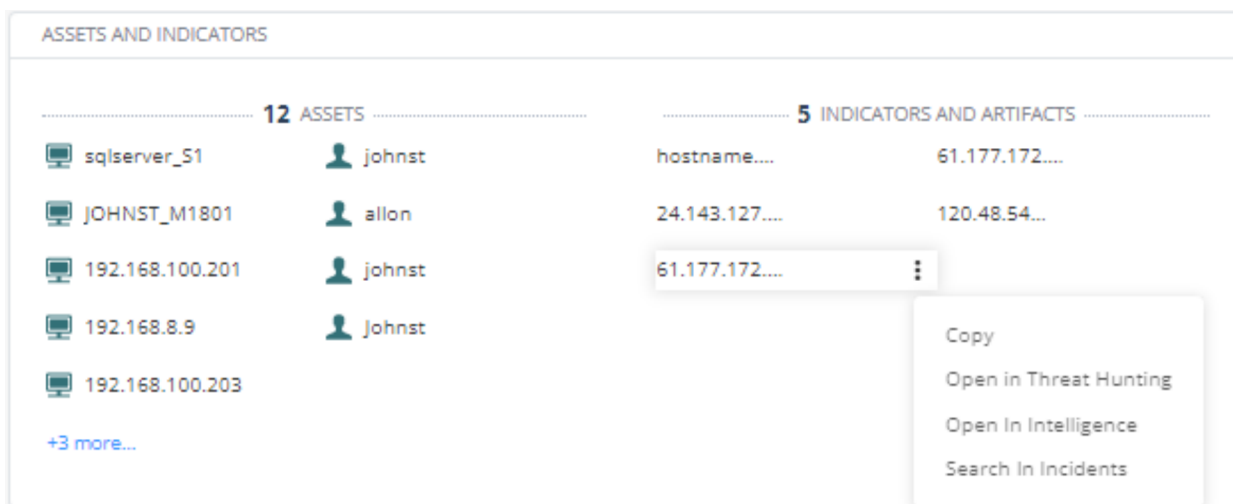
- Assets involved in the incident.
- Indicators and artifacts involved in the incident.




Hover over the indicator or artifact to view the risk level score (for example, 34), Classification, Malware Family and the VT score.

## Managing Assets and Indicators

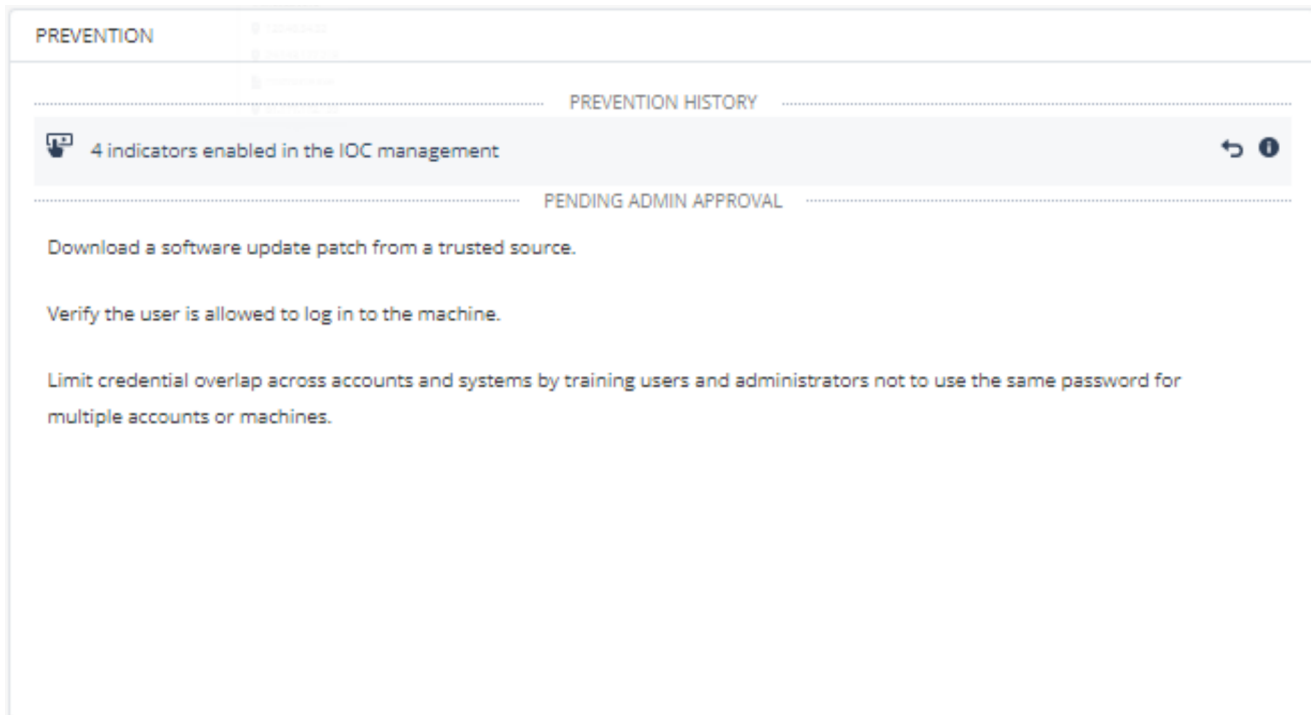
1. Click Incidents:
  - a. Click the incident title.
  - b. Hover over the incident and click >.
2. In the Assets and Indicators widget, hover over the asset, indicator or an artifact.





3. Hover over .
4. To copy an asset, indicator or artifact name to the clipboard, click Copy.  
Horizon XDR/XPR copies the name of the asset, indicator or the artifact to the clipboard.
5. To view forensic details related to the chosen asset, click Open in Threat Hunting.  
Horizon XDR/XPR opens the ["Threat Hunting" on page 67](#) page and shows the data for the asset, indicator or the artifact for the last seven days.
6. To view intelligence for an indicator or artifact, click Open in Intelligence.  
Horizon XDR/XPR opens the Intelligence page and shows the available intelligence for the asset, indicator or the artifact.
7. To search for asset, indicator or artifact in incidents, click Search in Incidents.

Horizon XDR/XPR opens the "Incidents" on page 18 page and shows the incidents with the searched asset, indicator or the artifact.

## Prevention



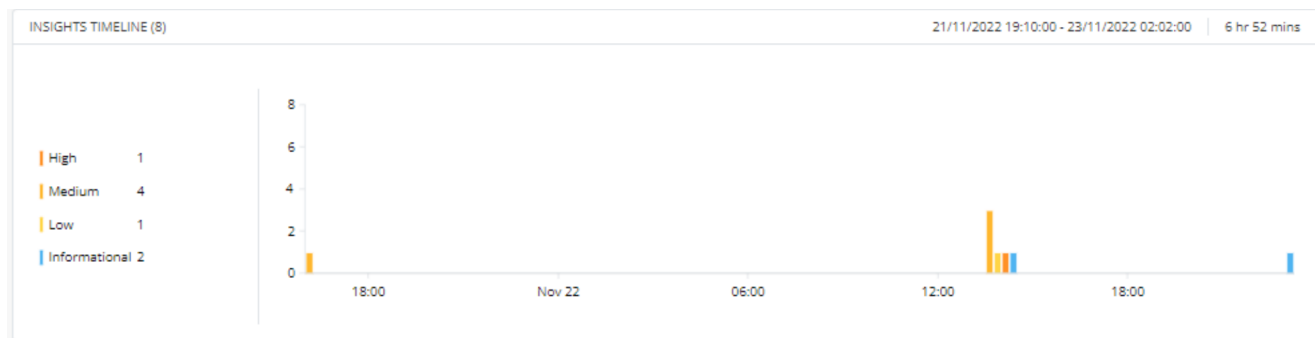
The Prevention widget shows:

- Prevention History - Automatic (  ) and manual (  ) prevention actions that Horizon XDR/XPR takes. The available prevention steps include:
    - Enable IoCs in the IoC Management
    - Isolate an asset in Harmony Endpoint
    - Quarantine a file in Harmony Endpoint
    - Killing a process in Harmony Endpoint.

For more information, see Push Operations in the [Harmony Endpoint Administration Guide](#).

  - Isolate IP addresses (hosts) in the Quantum Security Gateway.
- This is implemented using Check Point PlayBlocks that is currently available only to customers in the Early Availability (EA) program. To enroll to the EA program, contact [yaelci@checkpoint.com](mailto:yaelci@checkpoint.com).
- Pending Admin Approval - Recommended prevention actions that can be taken from Horizon XDR/XPR and those that should be taken outside of Horizon XDR/XPR, for example in one of the on-boarded products.

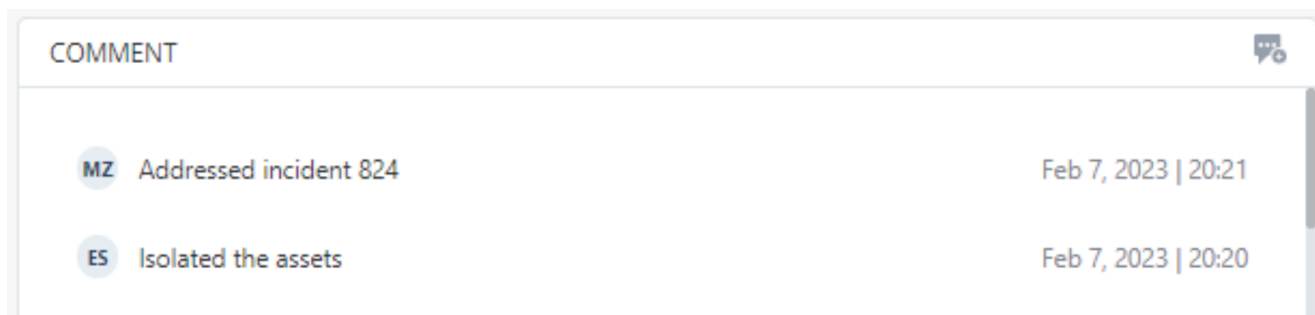
## Insights Timeline



The Insights Timeline widget shows the:


- Timeline of insights color-coded according to their severity.
- Date and time when the first and last insight was created.
- Duration between the first and last insight.

## Comments



The Comments widget shows the comments added by the SOC analysts to the incident.

## Adding a Comment

1. Click Incidents:
  - a. Click the incident title.
  - b. Hover over the incident and click >.
2. In the Comments widget, click  .
3. Enter a comment (maximum 150 characters) and click Save.

## Incidents - Affected Assets

The Affected Assets page shows the details of assets involved in the incident and allows you to perform these actions:

- ["Managing Indicators and Artifacts" on page 34](#)
  - Isolating an Asset
  - Isolating an IP Address
  - De-isolating an Asset
  - De-isolating an IP Address
  - Copying an Asset Name to Clipboard
  - Viewing Intelligence for an Asset
  - Searching for an Asset in Incidents
  - Viewing Threat Hunting for an Asset
- ["Creating an Exclusion for an Asset from an Incident" on page 30](#)

To view the **Affected Assets** page:

1. Access Horizon XDR/XPR and click **Incidents**:
  - Click the incident title.
  - Hover over the incident and click >.
2. Click **Affected assets**.

To edit the columns in the table, click **Edit columns** and select the columns.

To export the data to an excel in CSV format, click **Export All (CSV)**.

To search, in the **Search** field, enter the string. The table automatically filters and shows the content that matches with the string.


| Column                    | Description  |
|---------------------------|--|
| Type                      | Asset type: <ul style="list-style-type: none"> <li>▪ Machine</li> <li>▪ User</li> <li>▪ IP address</li> <li>▪ Email address</li> </ul> |
| Asset name                | Asset name.  |
| Endpoint Status           | Installation status of the Harmony Endpoint Security client on the machine.  |
| Endpoint Isolation Status | Isolation status of the machine. Applies only to machines with Harmony Endpoint Security client installed.                             |
| Gateway Status            | Isolation status of the asset on the gateway. Applies only to assets of type IP address.   |
| OS Name                   | Operating System of the machine.   |
| Last IP address           | Last associated IP address with the asset. Applies only to endpoints and IP address.   |
| OS Version                | Version of the Operating System.   |




| Column             | Description   |
|--------------------|---|
| Computer Last Seen | Date when the asset was last seen in the logs of the on-boarded products.   |
| GUID               | Global Unique Identifier of the asset.  |
| AD Domain          | Active Directory domain of the asset.   |
| Users              | Users related to the asset.   |
| Last IP Address    | Last IP address associated with the asset.  |
| Associated IPs     | IP addresses associated with the asset.   |
| Insights           | Number of insights related to the incident in which the asset is involved. Hover over to view the insights by severity.     |
| Indicators         | Number of indicators related to the incident in which the asset is involved. Hover over to view the indicators by severity. |
| Related Incidents  | Number of incidents where the asset was involved.   |

## Managing Affected Assets

1. Click **Incidents**:
  - Click the incident title.
  - Hover over the incident and click >.
2. Click **Affected assets**.
3. Select the asset.
4. To isolate an affected endpoint from the network. Horizon XDR/XPR enforces isolation through Harmony Endpoint's **Isolate Computer** push operation, at the top of the page, click **Isolate** and then click **Isolate on Endpoint**.  
A confirmation message appears. Click **Yes**.
5. To isolate an asset of the type IP address on the Quantum Security Gateway, at the top of the page, click **Isolate** and then click **Isolate on Gateway**.  
A confirmation message appears. Click **Yes**.
6. To de-isolate an isolated endpoint in the network. Horizon XDR/XPR enforces isolation through Harmony Endpoint's **Isolate Computer** push operation, at the top of the page, click **De-Isolate**.  
A confirmation message appears. Click **Yes**.
7. To de-isolate or unblock an isolated IP address in the network. Horizon XDR/XPR enforces isolation through the Quantum Security Gateway, at the top of the page, click **De-Isolate**.  
A confirmation message appears. Click **Yes**.

8. To copy an asset name to the clipboard, in the table, at the end of the row, hover over , and click **Copy Asset Name**.


Horizon XDR/XPR copies the name of the asset to the clipboard.

9. To view intelligence for an IP address, in the table, at the end of the row, hover over , and click **Open in Intelligence**.

Horizon XDR/XPR opens the Intelligence page and shows the available intelligence for the IP address.



Note - This applies only to assets of type IP address.


10. To isolate an IP address on the Quantum Security Gateway, in the table, at the end of the row, hover over , and click **Isolate on GW**.

A confirmation message appears. Click Yes.




Notes:

- This applies only to assets of type IP address.
- This is implemented using Check Point PlayBlocks that is currently available only to customers in the Early Availability (EA) program. To enroll to the EA program, contact [yaelci@checkpoint.com](mailto:yaelci@checkpoint.com).

11. To search for an asset in the incidents table, in the table, at the end of the row, hover over , and click **Search in Incidents**.

Horizon XDR/XPR opens the "[Incidents](#)" on page 18 page and shows the assets involved in the incidents.

12. To view Threat Hunting for an asset, in the table, at the end of the row, hover over , and click **Open in Threat Hunting**.

Horizon XDR/XPR opens the "[Threat Hunting](#)" on page 67 page searching for the chosen asset in the logs from the past seven days.

## Creating an Exclusion for an Asset from an Incident


You can create exclusions for assets so that they do not create new incidents. For example, an asset that represents an approved network scanner.



Note - You can create exclusions from the Policy menu also. See "[Exclusions](#)" on page 38

To create an exclusion for an asset from an incident:

1. Click **Incidents**:
  - Click the incident title.
  - Hover over the incident and click >.
2. Click **Affected assets**.

3. In the table, at the end of the row, hover over , and click Create Exclusion.  
The Asset type and Exclusion value are pre-filled.
4. From the Asset type drop-down:
  - If the asset type is an IP address, select IPv4.
    - Select an Exclusion value:
      - Single - Enter the IP address.
      - Range - Enter From and To IP addresses.
      - CIDR - Enter Subnet and Prefix.
5. (Optional) Select an Expiration date (UTC). After the expiration, the asset can create incidents.
6. (Optional) Enter Comments.
7. Click Submit.

## Incidents - Indicators & Artifacts

The Indicators & Artifacts page shows the indicators and artifacts in the incident.

An artifact of an incident is a domain, URL, IP address or a file affected in the incident. An indicator is a malicious artifact. For example, an artifact is a legitimate file involved in an incident and an indicator is a malicious domain.

You can use the Indicators & Artifacts page to perform these actions:

- ["Managing Indicators and Artifacts" on page 34](#)
  - Copying an Indicator or an Artifact Value to Clipboard
  - Copying HASH of an Indicator to Clipboard
  - Viewing Intelligence for an Indicator or Artifact
  - Viewing Threat Hunting for an Indicator or Artifact
- ["Adding or Editing an Indicator or Artifact in IoC Management" on page 34](#)
- ["Removing an Indicator from IoC Management" on page 35](#)

To view the Indicators & Artifacts page:

1. Access Horizon XDR/XPR and click Incidents:
  - Click the incident title.
  - Hover over the incident and click >.
2. Click Indicators & Artifacts.





























































To edit the columns in the table, click Edit columns and select the columns.











To export the data to an excel in CSV format, click Export All (CSV).

To search, in the Search field, enter the string. The table automatically filters and shows the content that matches with the string.

The Indicator & Artifacts tab shows a list of all indicators and artifacts involved in the incident. The Domains, URL, IP Address and Files tabs offer a drill-down view into their respective type and their related information:


| Column          | Description  | Indicators & Artifacts | Domains | URL | IP Address | Files |
|-----------------|--|------------------------|---------|-----|------------|-------|
| Type            | Indicator or an artifact.  |                        |         |     |            |       |
| Value           | Value of the indicator or artifact.  |                        |         |     |            |       |
| Status IOC Mgmt | Indicates whether the indicator was enabled or disabled in the IoC management.         |                        |         |     |            |       |
| XDR Confidence  | Confidence level of the indicator, calculated by Horizon XDR/XPR.                      |                        |         |     |            |       |
| XDR Severity    | Severity level of the indicator, calculated by Horizon XDR/XPR.                        |                        |         |     |            |       |
| Classification  | Threat classification of the indicator. For example, Malware or Benign.                |                        |         |     |            |       |
| Malware Family  | The malware family associated with the indicator. For example, Invader.                |                        |         |     |            |       |
| VT Score        | VirusTotal score reported by <a href="https://www.virustotal.com">virustotal.com</a> . |                        |         |     |            |       |
| Related Assets  | Assets related to the indicator or artifact.   |                        |         |     |            |       |

| Column                | Description   | Indicators & Artifacts  | Domains   | URL   | IP Address  | Files   |
|-----------------------|---|---|---|---|---|---|
| Related Incidents     | Incidents related to the indicator or artifact.                                     |    |    |    |    |    |
| Global Top country    | Top country where the indicator was seen in the Check Point telemetry.              |    |    |    |    |    |
| Global Top industry   | Top industry where the indicator was seen in the Check Point telemetry.             |    |    |    |    |    |
| Registrar name        | Name of the registrar.  |    |    |    |    |    |
| Country               | Country where the IP address is registered.   |    |    |    |    |    |
| Owner                 | Organization to which the IP address is registered.                                 |  |  |  |  |  |
| IP abuse              | Confidence of abuse reported by <a href="https://abuseipdb.com">abuseipdb.com</a> . |  |  |  |  |  |
| File type             | Type of file.   |  |  |  |  |  |
| File size             | Size of the file.   |  |  |  |  |  |
| Signer                | Authority that signed the certificate of the file.                                  |  |  |  |  |  |
| Additional file names | Other known names seen for the file's hash in the on-boarded product logs.          |  |  |  |  |  |
| File path             | Path of the file.   |  |  |  |  |  |

| Column                  | Description  | Indicators & Artifacts  | Domains   | URL   | IP Address  | Files   |
|-------------------------|--|---|---|---|---|---|
| File origin             | Source application of the file.                    |  |  |  |  |  |
| Threat Emulation report | Download the Threat Emulation report for the file. |  |  |  |  |  |


## Managing Indicators and Artifacts

### Copying an Indicator or an Artifact Value to the Clipboard

1. Click Incidents:
  - Click the incident title.
  - Hover over the incident and click >.
2. Click Indicators & Artifacts.
3. At the end of the row, hover over .
4. To copy the indicator or artifact (of the type file) file name, click Copy file name.  
Horizon XDR/XPR copies the file name to the clipboard.
5. To copy the indicator or artifact value, click Copy value.  
Horizon XDR/XPR copies the value to the clipboard.
6. To copy the indicator or artifact (of the type file) file name, click Copy HASH.  
Horizon XDR/XPR copies the HASH of the file to the clipboard.
7. To view the intelligence for indicators or artifacts, and click Open in Intelligence at the top of the table. You can select up to 20 indicators or artifacts.  
Horizon XDR/XPR opens the ["Intelligence" on page 48](#) page and shows the available intelligence for the indicator or artifact.
8. To view Threat Hunting for an indicator or artifact, click Open in Threat Hunting  
Horizon XDR/XPR opens the ["Threat Hunting" on page 67](#) page and shows the data for the indicator or artifact.


## Adding or Editing an Indicator or Artifact in IoC Management

1. Click Incidents:
  - Click the incident title.
  - Hover over the incident and click >.
2. Click Indicators & Artifacts.

- To add an artifact to IoC Management, in the table, at the end of the row, hover over , and click Add to IOC Management.




Note -Adding an artifact to IoC Management changes its type from artifact to indicator.

- To edit an indicator's setting in IoC Management, in the table, at the end of the row, hover over , and click Edit in IOC Management.

Horizon XDR/XPR automatically populates Status, Action and Name fields.

- Expand Advanced settings, and enter:
  - Confidence
  - Severity
  - Blade
  - Expiration date - After the expiration date, the IoC is disabled automatically
- Click Save.

## Removing an Indicator from IoC Management

- Click Incidents:
  - Click the incident title.
  - Hover over the incident and click >.
- Click Indicators & Artifacts.
- To remove an indicator from IoC Management, in the table, at the end of the row, hover over , and click Remove from IOC Management.



Note - If you remove an indicator from IoC Management, it changes its type from an indicator to an artifact.

- A confirmation message appears. click Yes.

## Incidents - MITRE

The [MITRE ATT&CK](#) is a framework that breaks down the cyber attack lifecycle into its component stages and provides in-depth information about how each stage was accomplished.

To view the MITRE page:

- Access Horizon XDR/XPR and click Incidents:
  - Click the incident title.
  - Hover over the incident and click >.
- Click MITRE.

|   | Reconnaissance                     | Resource Development                         | Initial Access                                     | Execution                                     | Persistence                                      | Privilege Escalation                       | Defense Evasion                             | Credential Access                         | Discovery                                    | Lateral Movement                            | Collection                                      | Command And Control                             | Exfiltration                        | Impact |
|---|------------------------------------|--|--|---|--|--|---|---|--|---|---|---|-------------------------------------|--------|
| Active Scanning<br>T1585                    | Acquire Infrastructure<br>T1583    | Drive By Compromise<br>T1183                 | Command And Scripting Interpreter<br>T1059         | Account Manipulation<br>T1038                 | Abuse Elevation Control Mechanism<br>T1548       | Abuse Elevation Control Mechanism<br>T1548 | Brute Force<br>T1110                        | Account Discovery<br>T1087                | Exploitation Of Remote Services<br>T1210     | Archive Collected Data<br>T1560             | Application Layer Protocol<br>T1071             | Automated Exfiltration<br>T1020                 | Account Access Removal<br>T1531     |        |
| Gather Victim Host Information<br>T1592     | Compromise Accounts<br>T1586       | Exploit Public Facing Application<br>T1190   | Container Administration Command<br>T1628          | BITS Jobs<br>T1197                            | Access Token Manipulation<br>T1194               | Access Token Manipulation<br>T1194         | Credentials From Password Stores<br>T1556   | Application Window Discovery<br>T1010     | Internal Spearphishing<br>T1294              | Audio Capture<br>T1123                      | Communication Through Removable Media<br>T1092  | Data Transfer Size Limits<br>T1038              | Data Destruction<br>T1485           |        |
| Gather Victim Identity Information<br>T1589 | Compromise Infrastructure<br>T1584 | External Remote Services<br>T1133            | Deploy Container<br>T1610                          | Boot Or Logon Autostart Execution<br>T1547    | Boot Or Logon Autostart Execution<br>T1547       | BITS jobs<br>T1197                         | Exploitation For Credential Access<br>T1212 | Browser Bookmark Discovery<br>T1217       | Lateral Tool Transfer<br>T1570               | Automated Collection<br>T1119               | Data Encoding<br>T1132                          | Exfiltration Over Alternative Protocol<br>T1046 | Data Encrypted For Impact<br>T1486  |        |
| Gather Victim Network Information<br>T1590  | Develop Capabilities<br>T1587      | Hardware Additions<br>T1200                  | Exploitation For Client Execution Scripts<br>T1287 | Boot Or Logon Initialization Scripts<br>T1527 | Build Image On Host<br>T1612                     | Force Authentication<br>T1187              | Cloud Infrastructure Discovery<br>T1589     | Remote Service Session Hijacking<br>T1563 | Clipboard Data<br>T1115                      | Data Obfuscation<br>T1001                   | Exfiltration Over C2 Channel<br>T1041           | Data Manipulation<br>T1545                      |                                     |        |
| Gather Victim Org Information<br>T1591      | Establish Accounts<br>T1585        | Phishing<br>T1566                            | Inter Process Communication<br>T1176               | Create Or Modify System Process<br>T1143      | Deobfuscate Decode Files Or Information<br>T1140 | Forge Web Credentials<br>T1606             | Cloud Service Dashboard<br>T1021            | Remote Services<br>T1530                  | Data From Cloud Storage Object<br>T1530      | Dynamic Resolution<br>T1568                 | Exfiltration Over Other Network Medium<br>T1011 | Defacement<br>T1491                             |                                     |        |
| Phishing For Information<br>T1598           | Obtain Capabilities<br>T1588       | Replication Through Removable Media<br>T1091 | Native API<br>T1136                                | Compromise Client Software Binary<br>T1554    | Domain Policy Modification<br>T1484              | Deploy Container<br>T1610                  | Input Capture<br>T1056                      | Cloud Service Discovery<br>T1526          | Replication Through Removable Media<br>T1002 | Data From Configuration Repository<br>T1573 | Encrypted Channel<br>T1573                      | Exfiltration Over Physical Medium<br>T1052      | Disk Wipe<br>T1561                  |        |
| Search Closed Sources<br>T1597              | Stage Capabilities<br>T1608        | Supply Chain Compromise<br>T1195             | Scheduled Task Job<br>T1053                        | Create Account<br>T1136                       | Escape To Host<br>T1611                          | Direct Volume Access<br>T1056              | Man In The Middle<br>T1537                  | Container And Resource Discovery<br>T1613 | Software Deployment Tools<br>T1072           | Data From Information Repositories<br>T1213 | Fatback Channels<br>T1058                       | Exfiltration Over Web Service<br>T1567          | Endpoint Denial Of Service<br>T1489 |        |
| Search Open Technical Databases<br>T1596    | Trusted Relationship<br>T1199      | Shared Modules<br>T1129                      | Create Or Modify System Process<br>T1543           | Event Triggered Execution<br>T1546            | Domain Policy Modification<br>T1484              | Modify Authentication Process<br>T1556     | Domain Trust Discovery<br>T1462             | Taint Shared Content<br>T1030             | Data From Local System<br>T1105              | Ingress Tool Transfer<br>T1105              | Scheduled Transfer<br>T1029                     | Firmware Corruption<br>T1455                    |                                     |        |
| Search Open                                 | Valid                              | Software                                     | Event Triggered                                    | Exploitation For Execution                    | Network Sniffing                                 | File And Use Alternate                     | Data From                                   | Multi Stage                               | Transfer Data To                             | Inhibit System                              |   |   |                                     |        |

MITRE ATT&CK organizes information into a hierarchy:

- Tactics: The column headers, represent adversaries' tactical goals in a cyber attack.
- Techniques: The cells under the tactic, represent the known methodologies available to achieve each tactic.

The number in a cell indicates the number of insights associated with the tactic or technique in the incident. Click the number to view the "Incidents - Insights & Forensics" below page searching for the chosen tactic or technique.

# Incidents - Insights & Forensics

The Insights & Forensics page shows the details of insights and forensics (processes, files, URL, domains and Registry involved in the insight) related to the incident.

To view the Indicators & Artifacts page:

1. Access Horizon XDR/XPR and click Incidents:
  - Click the incident title.
  - Hover over the incident and click >.
2. Click Indicators & Forensics.

To edit the columns in the table, click Edit columns and select the columns.

To export the data to an excel in CSV format, click Export All (CSV).

To search, in the Search field, enter the string. The table automatically filters and shows the content that matches with the string.



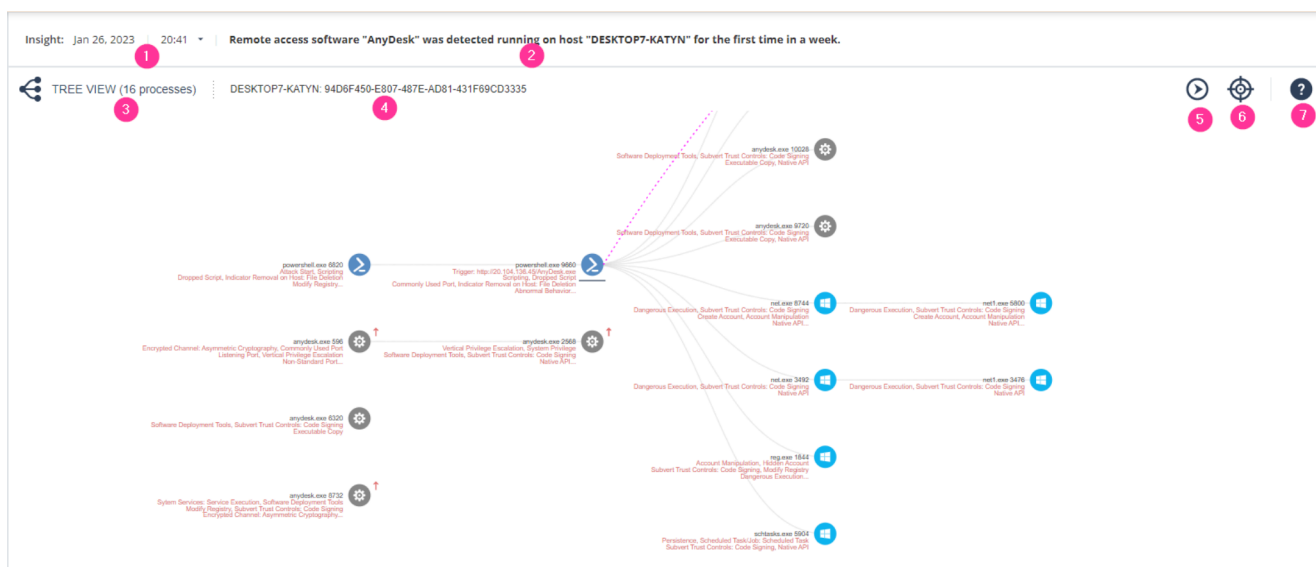
# Incidents - Attack Tree

The Attack Tree shows a graphical representation of the forensic report generated by Harmony Endpoint for each detection in an insight.

 Note - An insight can contain zero or multiple attack trees.

To view the Attack Tree page:

1. Access Horizon XDR/XPR and click Incidents:
  - Click the incident title.
  - Hover over the incident and click >.
2. Click Attack Tree.



| Legend | Description   |
|--------|---|
| 1      | Date and time when the insight was generated. Click to view the insights and attack trees available for the incident. Click the attack tree to view its graphical representation. |
| 2      | Insight summary.  |
| 3      | Process involved in the insight.  |
| 4      | Asset involved in the insight.  |
| 5      | Goes to that start of the tree.   |
| 6      | Goes through the processes in the tree.   |
| 7      | Opens the graph legends.  |

# Policy


On the Policy page, you can:

- Configure automatic response when Horizon XDR/XPR detects an IoC with a specified severity. See ["Automations" below](#).
- Configure exclusions for assets that are not malicious. See ["Exclusions" below](#).
- Send email, Slack and Microsoft Teams notifications when an incident with a specified priority is generated. See ["Notifications" on the next page](#).

## Automations


You can configure Horizon XDR/XPR to take prevention actions automatically when an incident is generated with a specified severity. Currently, the only automatic response supported is addition of indicator to ["IoC Management" on page 58](#).

For example, you can configure the automatic response that all IoCs with severity High must be added to ["IoC Management" on page 58](#) with the Enabled status.

 Note - By default, Horizon XDR/XPR automatically adds all the indicators to ["IoC Management" on page 58](#) with the Disabled status.


To configure an automatic response:

1. Click Policy > Automations.
2. Enable the toggle button.
3. Select the required threshold (Confidence and Severity level).

 Note - If the IoC is a file that matches the configured threshold, and if it is detected in a machine with Harmony Endpoint Security client installed, the file will be quarantined by Harmony Endpoint.

## Exclusions

You can create exclusions for assets, so that Horizon XDR/XPR will not create incidents for these assets in the future. For example, an asset that represents an approved network scanner.


 Note - These exclusions affect only the creation of incidents in Horizon XDR/XPR and do not affect the policies of the on-boarded products.

## Configuring an Exclusion

To configure an exclusion for the Horizon XDR/XPR incidents:

1. Click Policy > Exclusions.
2. Click New.

The New Exclusion window appears.

3. Under **Exclusion type**, select **Asset**.
4. Select the required **Asset type**.
  - To add the exclusion for a machine, select **Host**.
  - To add the exclusion for IP address, select **IPv4**.
5. Under **Exclusion value**, select the required machine name or IP address.
  - If you selected **Host**, enter the required machine name.
  - If you selected **IPv4**:
    - To add single IP address, select **Single** and enter the IP address.
    - To add a range of IP address, select **Range** and enter the **From** and **To** IP address.
    - To add the IP address in CIDR, select **CIDR** and enter the **Subnet** and **Prefix**.
6. (Optional) Under **Expiration date (UTC)**, select the date when the exclusion expires.
  -  **Note** - The default time zone is UTC.
7. (Optional) Under **Comment**, enter a description about the exclusion.
8. Click **Submit**.

## Editing an Exclusion

To edit an exclusion:

1. Click **Policy > Exclusions**.
2. Select the exclusion and click **Edit**.

The **Edit Exclusion** window appears.
3. Make the necessary changes for the exclusion and click **Submit**.

## Exporting Exclusions

To export the exclusions:

1. Click **Policy > Exclusions**.
2. Click **Export All (CSV)**.

The system downloads the report in the CSV format.

## Notifications

You can send email, Slack and Microsoft Teams notifications when an incident with a specified priority is generated.

# Sending Email, Slack, and Microsoft Teams Notifications

To send notifications for Horizon XDR/XPR incidents:

1. Click **Policy > Notifications**.
2. Enable the toggle button.
3. In the **Trigger** section, select the incident priority for which you need to send notifications.
  - Critical
  - High and above
  - Medium and above
  - Low and above
  - Informational and above
4. To send email notifications:
  - a. Enable the **Email** toggle button.
  - b. Enter the email addresses of users and/or distribution lists.
  - c. To view how the email subject and body appears, click **Preview Email**.
5. To send Slack notifications:
  - a. Enable the **Slack** toggle button.
  - b. Click **Edit**.  
Slack Channels pop-up appears.
  - c. Enter the **Channel name** and its **URL**.  
To add multiple channels, click **Add Channel** and enter the **Channel name** and its **URL**.
  - d. Click **Save**.
  - e. To view how the Slack notification appears, click **Preview Message**.
6. To send Microsoft Teams notifications:
  - a. Enable the **Microsoft Teams** toggle button.
  - b. Click **Edit**.  
Teams Channels pop-up appears.
  - c. Enter the **Channel name** and its **URL**.  
To add multiple channels, click **Add Channel** and enter the **Channel name** and its **URL**.
  - d. Click **Save**.
  - e. To view how the Microsoft Teams notification appears, click **Preview Message**.
7. Click **Save Changes**.

# Testing the Notifications

To test the configured email, Slack, and Microsoft Teams notifications:

1. Click **Policy > Notifications**.
2. Click **Test**.
3. Under **Test Platforms**, select the platforms you need to test (Email, Slack, Teams).
4. Under **Test**, select the users.
  - To send the notifications to all the configured email addresses or channels, click **All recipients**.
  - To send the notifications to specific users or channels, click **Specific** and enter the required **Recipients**.
5. Click **Send**.

# Events

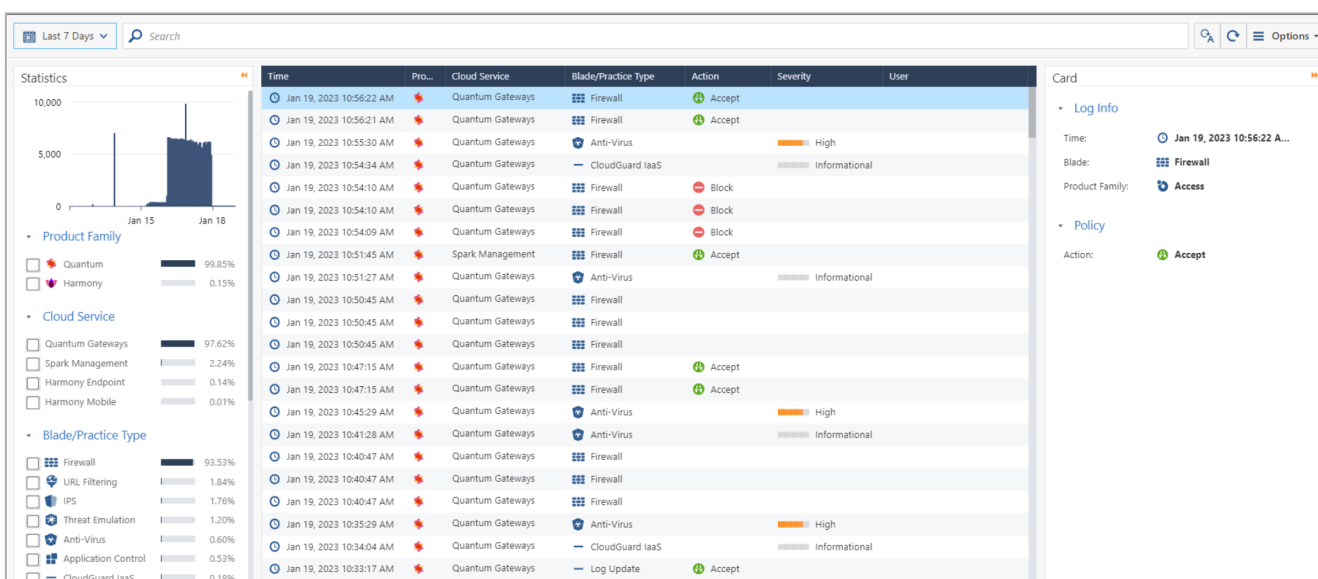
The Events page provides a unified interface to view security events of products supported by Horizon Events. For more information, see [Horizon Events Administration Guide](#).

**Note** - Corrective action for an event must be taken in the product that generated the event. For example, if a benign URL is blocked, then access the product and correct the policy.

This page shows:

- ["Statistics" below](#)
- ["Events Table" below](#)
- ["Card" on page 46](#)

To view the Events page, access Horizon XDR/XPR and click Events.



## Statistics

On the Statistics page, you can:

- See a bar graph of the number of events for the selected time frame.
- Filter the event data in ["Events Table" below](#).

For example, you can filter the events data for a product family, a Blade/Practice Type and more.

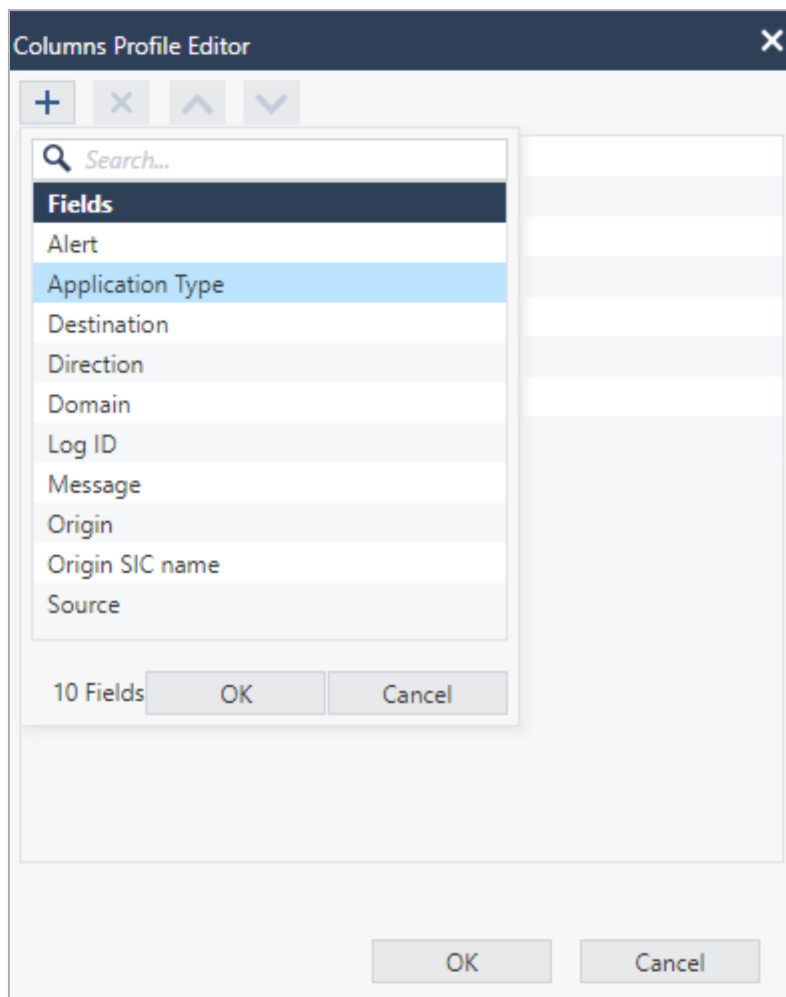
## Events Table

| Field Name     | Description        |
|----------------|--------------------|
| Default Fields |                    |
| Time           | Time of the event. |

| Field Name               | Description   |
|--------------------------|---|
| Product Family           | Check Point product family.<br>For example, Quantum, Harmony or CloudGuard.   |
| Cloud Service            | The cloud service used by the Check Point product.<br>For example, Quantum Gateways.  |
| Blade/Practice Type      | Software blade that triggered the event.<br>For example, Firewall, VPN, Syslog.   |
| Action                   | Action enforced on the event: <ul style="list-style-type: none"> <li>▪ Accept</li> <li>▪ Block</li> <li>▪ Detect</li> <li>▪ Other</li> </ul>                  |
| Severity                 | Severity of the event: <ul style="list-style-type: none"> <li>▪ Critical</li> <li>▪ Informational</li> <li>▪ Low</li> <li>▪ Medium</li> <li>▪ High</li> </ul> |
| User                     | User logged in at the time of the event.  |
| <b>Additional Fields</b> |   |
| Alert                    | Type of alert generated for the event.<br>For example, spoof alert, mail.   |
| Destination              | Destination IP address.   |
| Direction                | Direction of the network traffic: <ul style="list-style-type: none"> <li>▪ Inbound</li> <li>▪ Outbound</li> </ul>   |
| Domain                   | Domain name sent to DNS request.  |
| Log ID                   | Unique identity for logs.<br>Includes Type, Family, Product/Blade, Category.  |
| Message                  | Message displayed for the security event.<br>For example, remote access client IP address and port were changed.  |
| Origin                   | Name of the first Security Gateway that reported this event.  |
| Source                   | Source IP address.  |

## Managing the Events Table

1. To view the details of a specific log, double-click the row.
2. To view the default columns, right-click the table header row and click Default.
3. To modify the table columns, right-click the table header row and click Columns Profile Editor.
4. To add a new column to the table:
  - a. Click +.



- b. Select the column from the list and click OK.

The new column appears in the Events table and in the Statistics pane.



5. To remove a column from the table:
  - a. Select the column you want to delete and click X.
  - b. Click OK.

The selected column is deleted from the Events table and from the Statistics pane.

6. To sort the columns:



a. Select the column.

- To move the column higher in the order, click .
- To move the column lower in the order, click .

b. Click OK.

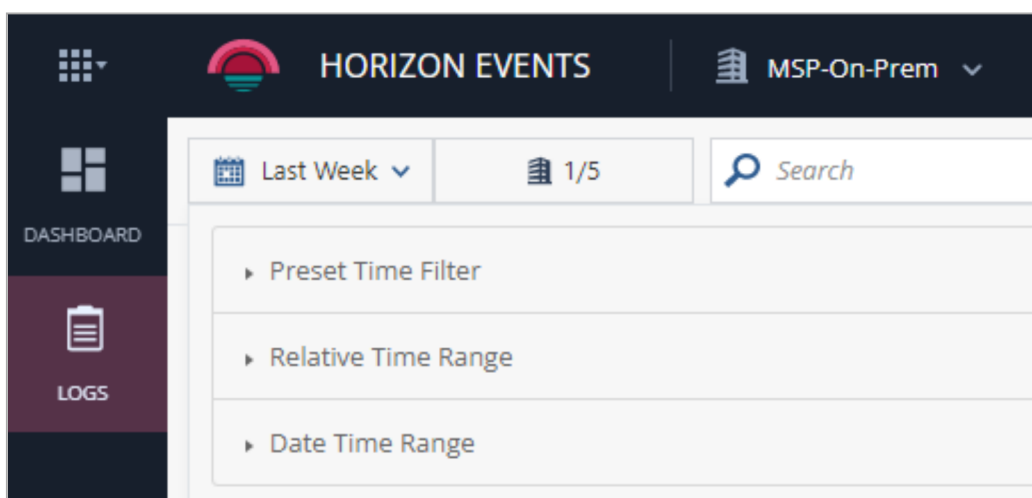
The column position is updated in the Events table and in the Statistics pane.

## Viewing Events for a Time Period

By default, the Events table shows events for the last 7 days.

To view Events table for a specified period, use one of these to set the time range:

- Preset Time Filter
- Relative Time Range
- Date Time Range



## Searching for Events

You can search for events using free text or a filter.

- To search using free text, in the **Search** field, enter the text and press **Enter**.  
For example, if you enter **Block**, the search results show all the blocked events.
- To search using a filter, click the **Search** field, select a filter and enter the text.  
For example, if the filter is **Blade/Practice Type** and text is **URL Filtering**, search as **Blade/Practice Type:"URL Filtering"**.  
The search results show all events with **Blade/Practice Type** as **URL Filtering**.



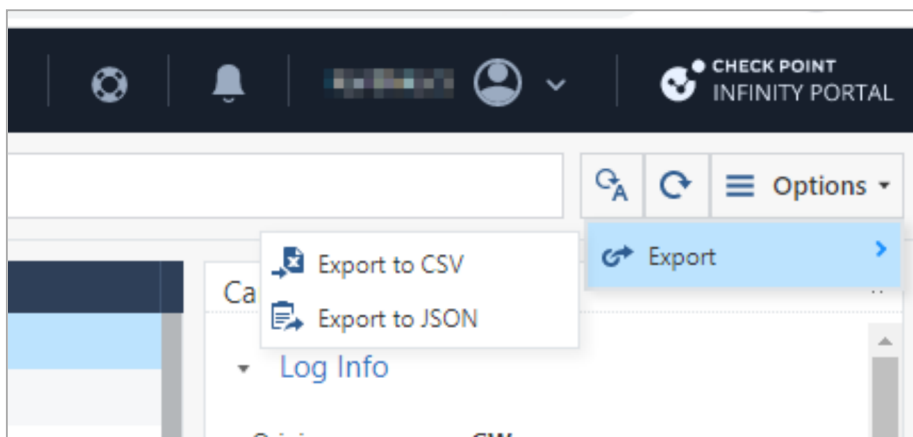
Note - You can use logical operations **AND**, **OR** and **NOT** in the search.

For example, **Block AND URL Filtering** shows the blocked events with **Blade/Practice Type** as **URL Filtering**.

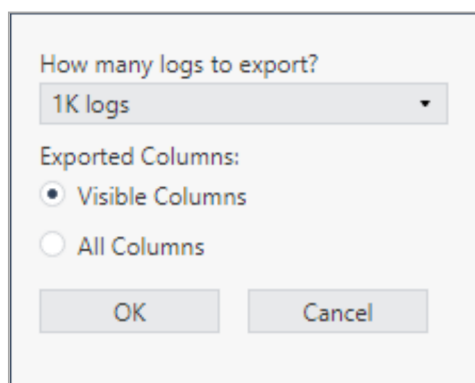
## Exporting Events

You can export events from the Events table to a CSV file or to a JSON file.

1. In the Events window, click Options > Export.



2. Select one of these output file formats:
  - Export to CSV
  - Export to JSON
3. Enter the information for these fields:
  - In How many logs to export drop-down, select the number of logs you want to export.
  - In Exported Columns, select whether to export event data from Visible Columns or from All Columns.



4. Click OK.

For CSV output, system generates an Excel sheet with the file name format: Events\_Logs\_Date\_Time.xls.

For JSON output, system generates a json file with name format: Events\_Logs\_Date\_Time.json.

Example, Events\_Logs\_Oct\_17\_2022\_01\_48\_24\_PM.

## Card

The Card pane shows the details for the event selected in the ["Events Table" on page 42](#).

Last 7 Days

Options

### Statistics

**Product Family**

- Quantum 99.85%
- Harmony 0.15%

**Cloud Service**

- Quantum Gateways 97.62%
- Spark Management 2.24%
- Harmony Endpoint 0.14%
- Harmony Mobile 0.01%

**Blade/Practice Type**

- Firewall 93.53%
- URL Filtering 1.84%
- IPS 1.76%
- Threat Emulation 1.20%
- Anti-Virus 0.60%
- Application Control 0.53%
- CloudGuard IaaS 0.18%
- Log Update 0.08%
- Mobile Access 0.06%

| Time                     | Product Family   | Cloud Service    | Blade/Practice Type | Action | Severity      | User |
|--------------------------|------------------|------------------|---------------------|--------|---------------|------|
| Jan 19, 2023 10:56:22 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:56:21 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:55:30 AM | Quantum Gateways | Quantum Gateways | Anti-Virus          | Accept | High          |      |
| Jan 19, 2023 10:54:34 AM | Quantum Gateways | Quantum Gateways | CloudGuard IaaS     | Accept | Informational |      |
| Jan 19, 2023 10:54:10 AM | Quantum Gateways | Quantum Gateways | Firewall            | Block  | High          |      |
| Jan 19, 2023 10:54:10 AM | Quantum Gateways | Quantum Gateways | Firewall            | Block  | High          |      |
| Jan 19, 2023 10:54:09 AM | Quantum Gateways | Quantum Gateways | Firewall            | Block  | High          |      |
| Jan 19, 2023 10:51:45 AM | Quantum Gateways | Spark Management | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:51:27 AM | Quantum Gateways | Quantum Gateways | Anti-Virus          | Accept | Informational |      |
| Jan 19, 2023 10:50:45 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:50:45 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:50:45 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:47:15 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:47:15 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:45:29 AM | Quantum Gateways | Quantum Gateways | Anti-Virus          | Accept | High          |      |
| Jan 19, 2023 10:41:28 AM | Quantum Gateways | Quantum Gateways | Anti-Virus          | Accept | Informational |      |
| Jan 19, 2023 10:40:47 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:40:47 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:40:47 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |
| Jan 19, 2023 10:35:29 AM | Quantum Gateways | Quantum Gateways | Anti-Virus          | Accept | High          |      |
| Jan 19, 2023 10:34:04 AM | Quantum Gateways | Quantum Gateways | CloudGuard IaaS     | Accept | Informational |      |
| Jan 19, 2023 10:33:17 AM | Quantum Gateways | Quantum Gateways | Log Update          | Accept | Informational |      |
| Jan 19, 2023 10:31:23 AM | Quantum Gateways | Quantum Gateways | Anti-Virus          | Accept | Informational |      |
| Jan 19, 2023 10:30:44 AM | Quantum Gateways | Quantum Gateways | Firewall            | Accept | Informational |      |

### Card

**Log Info**

Origin: SD-WAN-Branch-GW1

Time: Jan 19, 2023 10:54:10 A...

Blade: Firewall

Product Family: Access

Type: Connection

**Traffic**

Source: 172.28.28.119

Source Port: 49068

Destination: 88.221.154.122

Destination Count: Israel

**Policy**

Action: Drop

Policy Name: Management\_Service

Policy Name: SD-WAN-Policy

Policy Date: Jan 16, 2023 1:52:28 PM GM...

# Intelligence

The Intelligence page shows the intelligence available for an indicator derived from internal (Check Point's ThreatCloud, Research and Threat Emulation services) and external sources (reliable closed and open third-party feeds). On this page, you can also upload a file to Check Point's Threat Emulation Sandbox for analysis.

To view the Intelligence page, access Horizon XDR/XPR and click Intelligence.

The Sample attackers tab shows examples of the available intelligence. Click the tiles to view the intelligence data.

You can use the Intelligence page to perform these actions:

- ["Viewing Intelligence for Indicators" below.](#)
- ["Analyzing a File" on page 54.](#)

## Viewing Intelligence for Indicators

You can view the intelligence for a specific:

- URL
- Domain
- MD5, SHA1 or SHA256 hash of a file
- IP address

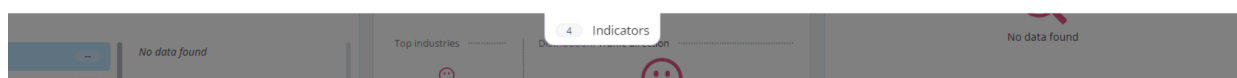
To view the intelligence for an indicator:

1. Click Intelligence.
2. Enter the indicator name(s) in the Search field and press Enter.

The search summary table is displayed. You can search for up to 20 indicators in a single search. The indicators can be of the same type or different types.

Response Remove Export to CSV Copy Indicator 4 of 4 selected

| Indicator                            | Source | Classification | Malware family | Confidence |
|--------------------------------------|--------|----------------|----------------|------------|
| 0 gmail.com 142.250.193.133          | Search | Benign         | N/A            | High       |
| 0 amazon.com 52.94.236.248           | Search | Benign         | N/A            | High       |
| 100 48056d41e62b91864ddf37780cdec8db | Search | Malware        | Invader        | High       |
| 192.168.100.201                      | Search | Local IP       |                |            |



| Item  | Description   |
|---|---|
| Risk  | The indicator's risk level based on the Check Point reputation engine. The higher the risk, higher the degree of maliciousness. Value ranges from 1 to 100, where 100 indicates a higher risk level and/or level of maliciousness.  |
| Indicator IP Address (For URLs and Domains) | IP address of the indicator.  |
| File Type (For files)                       | Type of the file. For example, .exe, .dll.  |
| Source                                      | Indicates the source where you searched for the indicator. Examples - <ul style="list-style-type: none"> <li>■ If you searched the indicator from the Search field, then the Source is displayed as Search.</li> <li>■ If you search for amazon.com and added an indicator from Research &gt; Communicating Files, the Source is displayed as amazon.com &gt; Communicating Files.</li> </ul> |
| Classification                              | Threat classification determined by Check Point engines. For example, Malware or Benign.  |
| Malware family                              | The malware family associated with the indicator, determined by Check Point engines. For example, Invader.  |
| Confidence                                  | The confidence level of the indicator's classification, determined by Check Point engines.  |

3. To view the [Intelligence Dashboard](#) for the indicator, click the indicator row.



Note - To view (silent search) only Check Point's intelligence information, click  .

## Intelligence Dashboard

The Intelligence dashboard shows:

- "Indicator Information" below
- "Research" on the next page
- "Check Point Traffic Analysis" on page 52
- "Open Source Intelligence Tools" on page 52

## Indicator Information

The Indicator Information widget displays a high level overview of the analyzed indicator.

- For domains and URLs, this widget shows a live screenshot of the website.
- For files, the widget shows:
  - File hash details - MD5, SHA1, and SHA256
  - Tags - The file tags from VirusTotal. Indicates the different characteristics about the file. For example, the signed tag indicates that the file is signed by a valid authority.
  - First seen - Date the file was first seen.
  - Last seen - Date the file was last seen.

- Report - Check Point Threat Emulation Report (if available).

Hash

**MD5:** 48056d41e62b91864ddf37780cdec8db

**SHA1:** e49968d886d6810dfce75e058c88a7203ceed493

**SHA256:** c449ab7272cc69d1131d565f52532059e7f69d12e8f2a2e9f917a5bfec965

revoked-cert
peexe
spreader
signed
...

First seen 27/09/2017 | Last seen 03/12/2020 No report available

## Research

The Research widget displays technical information about the indicator.

- For domain and URLs, the widget shows:

| Item                              | Description   |
|-----------------------------------|---|
| Whois data                        | Shows registered users or assignees of an Internet resource such as a domain name or IP address block.  |
| Indications                       | Summarized reputation data on this domain.  |
| Subdomains                        | Sub-domains for this domain.  |
| Related URLs                      | URLs under this domain.   |
| Communicating Files               | Files that were seen communicating with the searched domain.  |
| Downloaded Files                  | Files downloaded from this domain.  |
| Triggered Check Point Protections | Check Point protections triggered by the domain in: <ul style="list-style-type: none"> <li>• Anti-Virus</li> <li>• Anti-Bot</li> <li>• IPS</li> </ul> |
| User Agent                        | The user agent used to contact this domain during a malicious event.  |

- For files, the widget shows:

| Item             | Description   |
|------------------|---|
| File Names       | The file names observed by Check Point for this file.                     |
| Network Activity | The network traffic the file created during Check Point Threat Emulation. |

| Item            | Description  |
|-----------------|--|
| DNS Resolutions | DNS requests the file created during Check Point Threat Emulation. |
| Parent Process  | The process that created the file.                                 |
| Parent Archive  | The hash of the available file archive.                            |
| Source URLs     | URLs from which the file was downloaded.                           |
| Email Subjects  | Email subjects that contains this file as an attachment.           |

## Check Point Traffic Analysis

The Check Point Traffic Analysis widget shows a global view of the indicator's network traffic based on Check Point's global sensors. It gives a comparative view of the network traffic across different geographies. The widget shows:

| Item                         | Description   |
|------------------------------|---|
| Geolocation                  | <p>The indicator's usage in different geographic locations.</p> <ul style="list-style-type: none"> <li>▪ Highlights the top 3 countries that have the highest number of hits for this indicator.</li> <li>▪ To view the hits in a region, hover your mouse over that region.</li> <li>▪ You can also zoom in and zoom out the map.</li> </ul> |
| Top industries               | Top 3 industries where this indicator was seen.   |
| Distribution                 | Types of platforms that accessed the indicator.<br>For example, Web, Email.   |
| Events in-the-wild over time | The number of events over time for the indicator.   |

## Open Source Intelligence Tools

The Open Source Intelligence Tools widget shows the indicator information from Open Source Intelligence (OSINT). The widget has these tabs:

| Tab                  | Description   |
|----------------------|---|
| Check Point Research | Articles published by Check Point Research that mention this indicator and/or malware family. |
| Tweets               | Any tweets that mention the indicator, based on Check Point Research's social media crawler.  |
| Google               | Google Search results for the indicator.  |
| References           | Web page links that contains the indicator.   |



## Managing Indicators in IoC Management

Horizon XDR/XPR automatically classifies malicious artifacts as Indicators of Compromise (IoCs), and adds them to IOC Management according to the user-defined policy. From this screen, you can add, edit and remove indicators directly in IOC Management.

1. Click Intelligence.
2. Enter the indicator name in the Search field and press Enter.
3. To add the indicator to IoC Management, at the top, click Response > Add Selected to IOC Management.

The Update Indicators window appears.

4. Enter these:
  - Name - Enter a name for the indicator.
  - (Optional) Comment
 

The name and comment appear in the log created when the relevant blade detects or prevents the IoC.
  - Enable an Action - Detect or Prevent.

- Click **Advanced**:
  - Select a **Blade** that the IoC triggers.
  - Select **Confidence** and **Severity** levels for the trigger.
  - Select an **Expiration Date**. After the expiration date, the IoC is deleted automatically.

If the values for these fields are not defined, indicators are added with default values, as shown in the previous screen.

5. Click **Update**.
6. To edit an indicator that already exists in IoC Management, click **Response > Update Selected to IOC Management**.
7. Make the changes in **Update Indicators** window and click **Update**.
8. To delete an indicator from IoC Management, click **Response > Remove Selected to IOC Management**.

## Exporting the Search Summary to a CSV

1. Click **Intelligence**.
2. Enter the indicator name(s) in the **Search** field and press **Enter**.
3. In the **Search Summary** table, select the indicators you want to export.  
By default, all the searched indicators are selected.
4. At the top, click **Export to CSV**.

The system downloads a .csv file in the name format **Exported Summary Report Date Time**.

For example, **Exported Summary Report 2022-12-08 12-33-37.csv**

## Copying and Removing an Indicator from the Search Summary

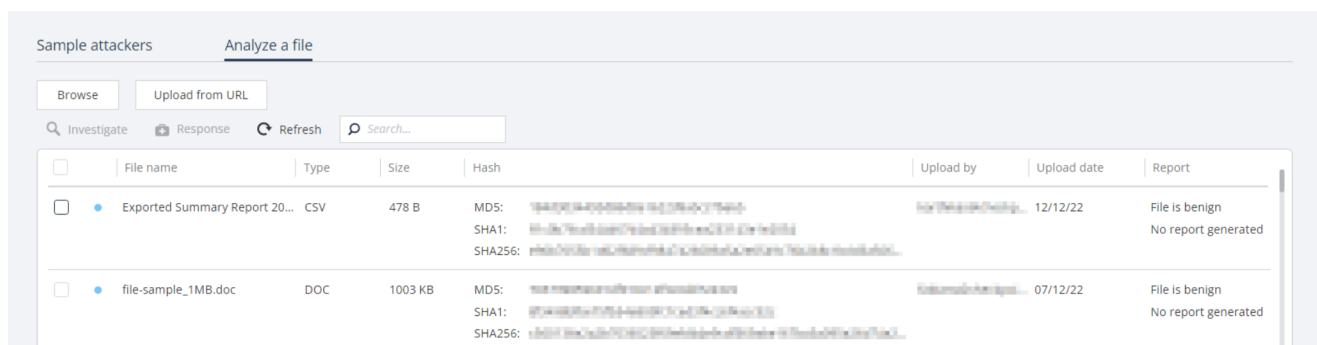
1. To copy an indicator, select the indicator in the **Search Summary** table and at the top, click **Copy Indicator**.

You can copy the indicator name and search for the indicator in any external or internal resources, or share the indicator name with other applications.

2. To remove an indicator, select the indicator in the **Search Summary** table and at the top, click **Remove**.

## Analyzing a File

You can upload a file to Check Point's Threat Emulation Sandbox for analysis.



To analyze a file:

1. Click **Intelligence > Analyze a file**.
2. To browse and upload a file:
  - a. Click **Browse**.
  - b. In the Explorer window, select the file and click **Open**.  
The file is added in the summary table.
3. To upload the file from a URL:
  - a. Click **Upload from URL**.
  - b. Enter the URL of the file and click **Upload**. For example, <https://databases.about.com/library/samples/address.xls>  
The file is added in the summary table.
4. To refresh the summary table, click **Refresh**.
5. To search for a file in the summary table, enter the file name in the **Search** field and press **Enter**.

The summary table shows these file parameters:

| Item        | Description  |
|-------------|--|
| File name   | Name of the file.  |
| Type        | Type of the file.<br>For example, EXE, DLL, CSV.   |
| Size        | File size.   |
| Hash        | File hash details: <ul style="list-style-type: none"> <li>■ MD5</li> <li>■ SHA1</li> <li>■ SHA256</li> </ul> |
| Upload by   | Email address of the user who uploaded the file.   |
| Upload date | The date on which the file was uploaded.   |

| Item   | Description   |
|--------|---|
| Report | The verdict returned by Check Point Threat Emulation analysis. If the file was determined as malicious, the Threat Emulation report is available to download. |

## Investigating a File

You can view the intelligence information for a file and investigate it from the Intelligence dashboard.

To investigate about a file:

1. Click **Intelligence > Analyze a file**.
2. [Upload](#) the file.
3. In the summary table, select the file to investigate. Click **Investigate**.

The [intelligence information](#) for the file is displayed.

## Adding a File to IoC Management

To add a file to IoC Management:

1. Click **Intelligence > Analyze a file**.
2. Upload the file.
3. In the summary table, select the file to add to IOC Management.

Click **Response > Add Selected to IOC Management**.

The **Update Indicators** window appears.

4. Enter these:

- Name - Enter a name for the indicator.

- (Optional) Comment

The name and comment appear in the log created when the relevant blade detects or prevents the IoC.

- Enable an Action - Detect or Prevent.

- Click Advanced:

- Select a Blade that the IoC triggers.
- Select Confidence and Severity levels for the trigger.
- Select an Expiration Date. After the expiration date, the IoC is deleted automatically.

If the values for these fields are not defined, indicators are added with default values, as shown in the previous screen.

5. Click Update.

# IoC Management

With IoC Management, you can view, create and edit Indicators of Compromise (IoCs) that apply to all the Check Point products on-boarded with Horizon XDR/XPR.

To view the IOC Management page, access Horizon XDR/XPR and click IOC Management.

## IOC Management Overview

During the Horizon XDR/XPR onboarding process, two separate feeds for Detect and Prevent actions are created. To configure these feeds on the Management Server, see ["Configuring IoC Management" on page 62](#).

Horizon XDR/XPR IoC management requires no new rules or policy installation. IoC management works directly on the Security Gateway. After configuration, the Security Gateway continually fetches intelligence data stored in a .csv file on the Check Point web server. You can use the CSV file link with other products that support intelligence feeds from external sources, such as cloud-based mail protection platforms.

## Working with IoC Management

The IoC Management table shows only the latest 30 IoCs added to IoC Management. To view the all IoCs, click Export > Export All. See ["Exporting IoCs" on page 62](#).

| Enabled                             | Action  | Blade | Name               | Type   | Value   | Comment          | Confidence | Severity | Created          | Modified         | Expires          |
|-------------------------------------|---------|-------|--------------------|--------|---|------------------|------------|----------|------------------|------------------|------------------|
| <input checked="" type="checkbox"/> | DETECT  | AV    | Phishing           | URL    | https://americafirst-2viewalerts0.com/DOM...  |                  | HIGH       | MEDIUM   | 2022-09-13 15:04 | 2022-09-13 15:04 | 2032-09-13 15:02 |
| <input checked="" type="checkbox"/> | DETECT  | AV    | test-vikas         | MD5    | abe0fb9cd0a6c72b280d15f62e09c776              | created by vikas | HIGH       | MEDIUM   | 2022-09-27 22:03 | 2022-09-27 22:03 | 2032-09-27 22:02 |
| <input checked="" type="checkbox"/> | DETECT  | AV    | PrivateIOC.XDRL... | IP     | 24.143.127.236                                |                  | LOW        | LOW      | 2022-10-23 18:29 | 2022-10-23 18:28 | 2032-10-23 18:28 |
| <input checked="" type="checkbox"/> | DETECT  | AV    | XDR.Backdoor...    | IP     | 24.143.127.201                                |                  | LOW        | MEDIUM   | 2022-10-23 18:27 | 2022-10-23 18:27 | 2032-10-23 18:26 |
| <input checked="" type="checkbox"/> | DETECT  | AV    | XDR.SMB            | IP     | 45.61.187.162                                 |                  | LOW        | MEDIUM   | 2022-10-23 18:25 | 2022-10-23 18:25 | 2032-10-23 18:25 |
| <input checked="" type="checkbox"/> | DETECT  | AV    | PrivateIOC.XDRL... | URL    | http://toptools100.com/cgi-bin-py/weather_... |                  | LOW        | MEDIUM   | 2022-10-23 18:23 | 2022-10-23 18:31 | 2032-10-23 18:21 |
| <input checked="" type="checkbox"/> | DETECT  | AV    | demo               | DOMAIN | omnator.com                                   |                  | HIGH       | MEDIUM   | 2022-12-18 19:49 | 2022-12-18 19:49 | 2032-12-18 19:48 |
| <input checked="" type="checkbox"/> | PREVENT | AV    | web                | DOMAIN | 2002.discussion.community                     |                  | HIGH       | HIGH     | 2021-03-03 00:03 | 2021-03-03 16:52 | 2031-03-03 16:52 |
| <input checked="" type="checkbox"/> | PREVENT | AV    | web                | DOMAIN | 3322.org                                      |                  | HIGH       | HIGH     | 2021-03-03 00:03 | 2021-03-03 16:52 | 2031-03-03 16:52 |
| <input checked="" type="checkbox"/> | PREVENT | AV    | web                | DOMAIN | 37765128d75u9m4mul1.z1.web.core.window...     |                  | HIGH       | HIGH     | 2021-03-02 22:03 | 2021-03-03 16:52 | 2031-03-03 16:52 |
| <input checked="" type="checkbox"/> | PREVENT | AV    | web                | DOMAIN | 7008.xg4ken.com                               |                  | HIGH       | HIGH     | 2021-03-02 22:03 | 2021-03-03 16:52 | 2031-03-03 16:52 |
| <input checked="" type="checkbox"/> | PREVENT | AV    | web                | DOMAIN | 8023f3c8.sibforms.com                         |                  | HIGH       | HIGH     | 2021-03-02 22:03 | 2021-03-03 16:52 | 2031-03-03 16:52 |
| <input checked="" type="checkbox"/> | PREVENT | AV    | web                | DOMAIN | 6631f33cf2a1032b.com                          |                  | HIGH       | HIGH     | 2021-03-02 22:03 | 2021-03-03 16:52 | 2031-03-03 16:52 |
| <input checked="" type="checkbox"/> | PREVENT | AV    | web                | DOMAIN | 5088.xg4ken.com                               |                  | HIGH       | HIGH     | 2021-03-02 22:03 | 2021-03-03 16:52 | 2031-03-03 16:52 |

| Item    | Description  |
|---------|--|
| Enabled | Indicates whether the Action is enabled (enforced) on the IoC.   |
| Action  | The action enforced on the IoC: <ul style="list-style-type: none"> <li>■ Detect</li> <li>■ Prevent</li> </ul>                        |
| Blade   | The software blade that the IoC triggers: <ul style="list-style-type: none"> <li>■ Anti-Bot(AB)</li> <li>■ Anti-Virus(AV)</li> </ul> |

| Item       | Description  |
|------------|--|
| Name       | Name of the IoC.   |
| Type       | IoC type: <ul style="list-style-type: none"> <li>▪ Domain</li> <li>▪ IP address</li> <li>▪ URL</li> <li>▪ File - MD5, SHA1 or SHA256 hash key</li> </ul> |
| Value      | Value of the IoC.  |
| Confidence | Confidence level of the IoC detection.   |
| Severity   | Severity of the IoC.   |
| Created    | Date and time on which the IoC was created.  |
| Modified   | Date and time on which the IoC was last modified.  |
| Expires    | Date and time when the IoC expires. After the IoC expires, it is deleted automatically.  |

## Creating a New IoC



Note - You can also add IoCs to IOC Management from:

- Intelligence tab. See "[Managing Indicators in IoC Management](#)" on page 53.
- Incidents tab. See "[Adding or Editing an Indicator or Artifact in IoC Management](#)" on page 34.

1. In the IoC Management menu bar, click **New**.

The Add Indicators window appears.

2. Enter these:

- **Indicator Type** - Select the IoC type.
- **Value** - Enter the value of the IoC.
- **Name** - Enter a name for the IoC.
- **(Optional) Comment**

This name and comment appears in the log created when the relevant blade detects or prevents the IoC.

- **Enable an Action** - Detect or Prevent.

3. Click Advanced.

- Select a **Blade** that the IoC triggers.
- Select **Confidence** and **Severity** levels for the trigger.
- Select an **Expiration Date**. After the expiration date, the IoC is deleted automatically.

If the values for these fields are not defined, indicators are added with default values, as shown in the previous screen.

4. Click Add.



## Adding IoCs by Uploading a CSV File

1. In the IoC Management menu bar, click Upload from File.

The Upload CSV File window appears.

UPLOAD CSV FILE
✕

Choose file

---

▼ Info

| Field Name | Required | Possible Values               | Default Value          |
|------------|----------|-------------------------------|------------------------|
| Value      | +        |                               | -                      |
| Name       | +        |                               | -                      |
| Type       | -        | SHA1/SHA256/MD5/DOMAIN/URL/IP | Auto detect            |
| Status     | -        | Enabled/Disabled              | Enabled                |
| Action     | -        | Detect/Prevent                | Detect                 |
| Blade      | -        | AV/AB                         | AV                     |
| Confidence | -        | LOW/MEDIUM/HIGH               | LOW                    |
| Severity   | -        | LOW/MEDIUM/HIGH               | LOW                    |
| Expires    | -        | YYYY/DD/MM Date Format        | 10 years from updating |
| Comment    | -        | String                        | -                      |

\* A file can have up to 100 indicators.  
\* Optional fields that are not filled will have default values.

Download CSV Format

UPLOAD

2. If you have the CSV file to upload:
  - a. Click Choose file.
  - b. Browse the select the file and click Upload.
3. If you do not know the format of the CSV file:
  - a. Click Info > Download CSV Format.  
The system downloads Upload\_Format.xls.
  - b. Enter the IoC information in Upload\_Format.xls and upload this file.

## Editing and Deleting an IoC

1. To edit an IoC, select the IoC in the IoC Management table.
2. In the IoC Management menu bar, click Edit.

In the Edit Indicators window, enter the details and click Update.

3. To delete an IoC, select the IoC and click Delete.

## Filtering IoCs

1. In the IoC Management menu bar, click .

The Filter pane appears.

2. Select the parameter to filter the IoCs.

The IoC Management table refreshes and shows only the IoCs relevant to the applied filter.

## Exporting IoCs

1. In the IoC Management menu bar, click Export.

2. Select one of these export options:

- Export All - To export information of all the IoCs in the IoC Management table.
- Export Filtered - To export information of the IoCs relevant to the applied filter.
- Export Selected - To export information of only the selected IoCs in the IoC Management table.

System downloads a CSV file with the IoC information.

## Configuring IoC Management

After you successfully onboard to Horizon XDR/XPR:

1. In the IoC Management menu bar, click Show feed URLs.

The Feed URLs window appears.



When you onboard to Horizon XDR/XPR, two feeds in .csv format are created for Prevent and Detect actions. To create these files again, click Regenerate URLs.

2. Copy the Prevent URL and the Detect URL to a text file.

For example:

```
https://feeds.now.checkpoint.com/public_feeds/xxxxxxxxxx.csv  
https://feeds.now.checkpoint.com/public_feeds/xxxxxxxxxx.csv
```

## 3. In SmartConsole:

- a. From the left navigation panel, click Security Policies.
- b. In the middle top pane, click Threat Prevention > Indicators.
- c. From the top toolbar, click New > External IOC Feed.

The Indicator window appears.

- d. In Feed URL, enter the Prevent URL from step 2.
- e. In Action, select Prevent and click OK.
- f. Create a new External IOC Feed (Follow steps a to c).
- g. In Feed URL, enter the Detect URL from step 2.
- h. In Action, select Detect and click OK.

You have now created IoC feeds for Prevent and Detect actions.

| Name           | Actions | File Name/Feed   |
|----------------|---------|--|
| XXXXXXXXXX_IOC | Prevent | https://feeds.now.checkpoint.com/public_feeds/xxxxxxxxxx.csv |
| XXXXXXXXXX_IOC | Detect  | https://feeds.now.checkpoint.com/public_feeds/xxxxxxxxxx.csv |

- i. Install the Threat Prevention policy on this Security Gateway.

For more information, see [Importing External Custom Intelligence Feeds in SmartConsole](#).

4. In Horizon XDR/XPR, go to IOC Management and click Show Feed URLs.

Copy the full Security Gateway commands for Prevent and Detect.

Example:

```
ioc_feeds add --feed_name InfinitySOCPrevent --transport https --  
resource "https://feeds.now.checkpoint.com/public_  
feeds/xxxxxxxxx1.csv" --feed_action Prevent
```

```
ioc_feeds add --feed_name InfinitySOCDetect --transport https --  
resource "https://feeds.now.checkpoint.com/public_  
feeds/xxxxxxxxx2.csv" --feed_action Detect
```

5. In SmartConsole:

- a. From the left navigation panel, click Gateways & Servers.
- b. Right-click the Security Gateway object and click Actions > Open Shell.

Alternatively, connect to the command line on the Security Gateway through a SSH client.

6. Run the commands you copied in step 4 from Horizon XDR/XPR:

Example:

```
ioc_feeds add --feed_name InfinitySOCPrevent --transport https --  
resource "https://feeds.now.checkpoint.com/public_  
feeds/xxxxxxxxx1.csv" --feed_action Prevent
```

```
ioc_feeds add --feed_name InfinitySOCDetect --transport https --  
resource "https://feeds.now.checkpoint.com/public_  
feeds/xxxxxxxxx2.csv" --feed_action Detect
```

7. Close the shell after the operation completes successfully.



Note - If you generate the URLs again, the old feeds are no longer accessible. You must update the feeds on the Security Gateway and the indicator URL in SmartConsole.

# Testing IoC Management

As a simple test, block access to a website.

If the site is still accessible after you update the IoC feed:

1. Connect to the command line on the Security Gateway for each Cluster Member.
2. Log in to the Expert mode.
3. Fetch feeds in debug mode:

```
$FWDIR/bin/ioc_feeder -d -f
```

4. Examine this configuration file:

```
$FWDIR/conf/ioc_feeder.conf
```

If the file is corrupt, delete the feed, make the required changes in the feed, and add the feed again.

5. Examine these files for errors:

- \$FWDIR/log/ioc\_feeder.elg

For example:

```
Feed log External IOC - External Indicators processing
failedInfinitySOCPrevent: Failed to fetch feed. Resource:
https://feeds.now.checkpoint.com/public_feeds/PersonalFeed.csv,
Reason: Peer certificate cannot be authenticated with given CA
certificates
```

```
InfinitySOCDetect: Failed to fetch feed. Resource:
https://feeds.now.checkpoint.com/public_feeds/PersonalFeed.csv,
Reason: Peer certificate cannot be authenticated with given CA
certificateshttps://supportcenter.checkpoint.com/supportcenter/por
tal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
```

- \$FWDIR/log/ext\_ioc\_push.elg

# Threat Hunting

Threat Hunting is an investigative tool which allows for advanced querying on all malicious and benign forensics events collected from the organization's endpoints with Harmony Endpoint installed.

The information collected lets you to:

- Investigate the full scope of an attack.
- Discover stealth attack by observation of a suspicious activity.
- Remediate the attack before it causes further damage.
- Proactively hunt for advanced attacks by searching for anomalies, and using hunting leads and enrichment.

Threat Hunting supports:

- Data collection and enrichment - All events are collected through multiple sensors on the Harmony Endpoint, sent to a unified repository and enhanced by ThreatCloud, MITRE mapping and alerts from all Harmony Endpoint prevention engines.
- Rich toolset for custom queries, drill down and pivoting to suspicious activity.
- Predefined queries and a MITRE dashboard which map all activity and allow a quick start to proactive hunting.
- Remediation actions per result or a bulk operation integrated in the Threat Hunting flow (such as file quarantine and kill process).

The data is saved for 7 days, unless you purchased an extended retention license.

## Supported Versions

- Endpoint Security Client version E84.10 and higher.

## Enabling Threat Hunting

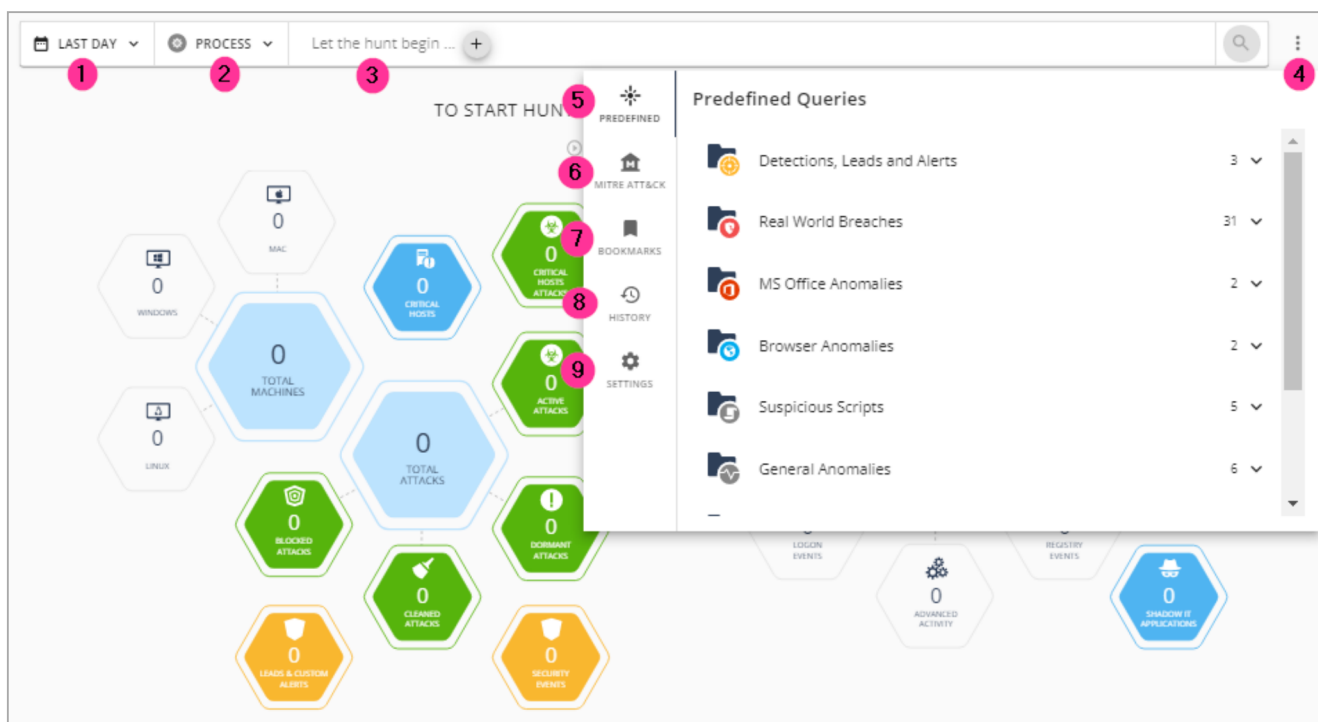
By default, Threat Hunting is disabled in Harmony Endpoint.

To enable Threat Hunting:

1. Go to Policy > Policy Capabilities.
2. Click the Analysis & Remediation tab.
3. From the Enable Threat Hunting list, select On.
4. Click Save & Install.
5. After the policy is pushed to the agents, wait a few minutes until data is sent by the agents.

Then you can go to the Threat Hunting view to start searching through events.

# Using Threat Hunting



| Item | Description   |
|------|---|
| 1    | Last Day - Time filter for the query. Users can choose between Last Day, Last 2 Days, Last Week and a Custom time period.   |
| 2    | Process - Refine your query results according to the activity type.   |
| 3    | Let the hunt begin - Click + and define the values to search in the logs. You can add multiple values and fields at a time.   |
| 4    | Menu for predefined queries.  |
| 5    | <p>Predefined - Check Point's predefined queries, divided by category.</p> <p><b>i</b> Note - Leads in Detections, Leads and Alerts are lead detections or signatures. If an incident is raised under this category, the term Lead. is prefixed to its protection name. For example, Lead.Win.BrwsrPassThft.B. It does NOT indicate an attack and we recommend that you ignore these incidents.</p> <p>This is used by Check Point to analyze if a protection has to be developed. For example, create a new signature.</p> |
| 6    | MITRE ATT&CK - Shows the MITRE ATT&CK framework of tactics and techniques. Each technique includes one or more queries, pre-defined by <a href="#">Check Point Research</a> .   |
| 7    | Bookmarks - Shows the custom queries saved as bookmarks, either as global (available for all users in the account) or private (available only for the user). Users can also define email notifications for these saved queries, currently limited to 10.  |
| 8    | History - See all the queries that you used.  |




| Item | Description                             |
|------|---|
| 9    | Settings - Change the UI look and feel. |

To hunt for threats, you can use predefined queries or by proactively creating your own queries.

- To use predefined queries:

1. Go to Predefined Hunting Queries or

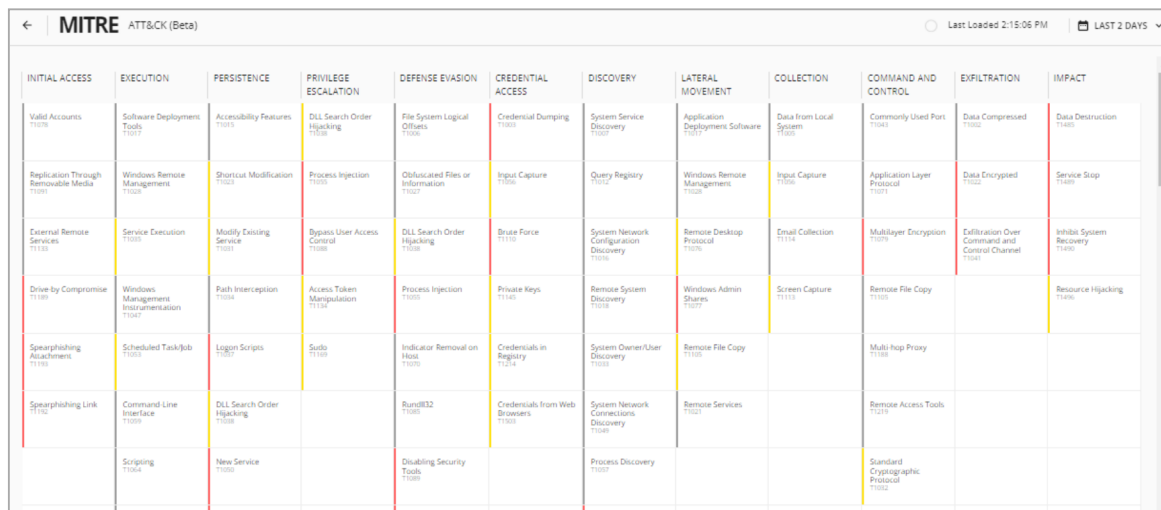
Click the  icon next to the search box and select **Predefined**.

You can quickly find all active attacks and browse through different malicious events detected by Endpoint clients.

- Click the  icon next to the search box and select MITRE ATT&CK.

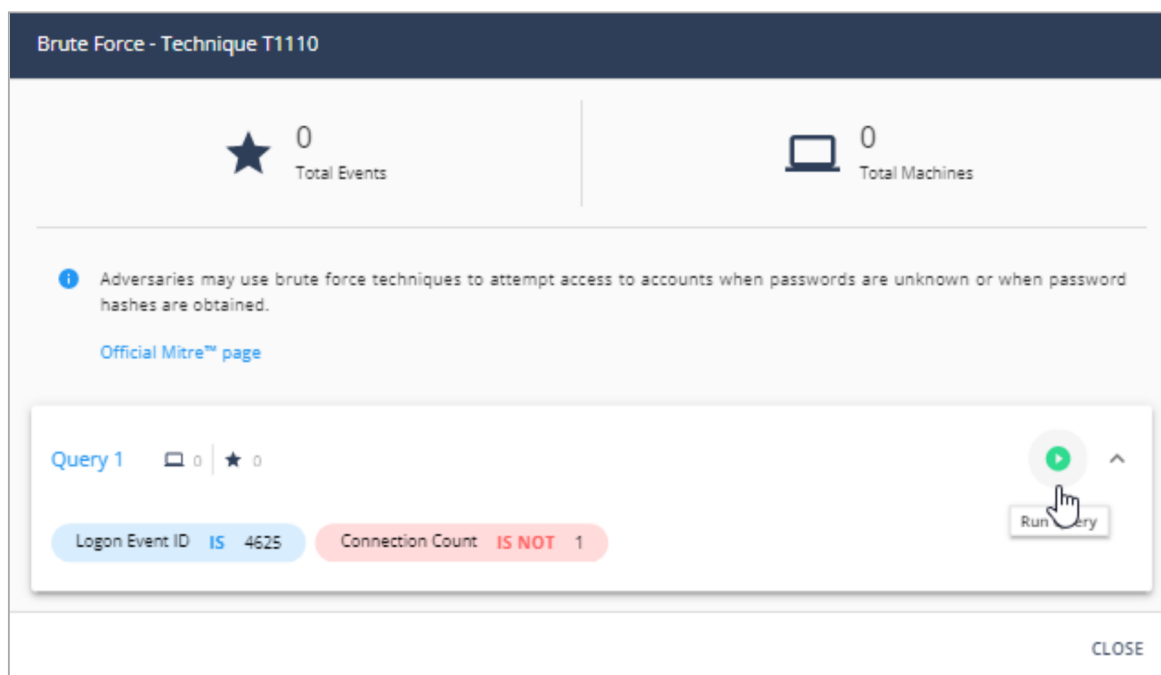
The MITRE ATT&CK dashboard provides real-time visibility on all the techniques observed by Harmony Endpoint across your endpoints. It maps all raw events to MITRE Tactics, Techniques, and Procedures (TTPs) regardless of status.

The MITRE ATT&CK dashboard is divided into 12 categories and each category is a stage in an attack. Each category includes multiple attack techniques.



| INITIAL ACCESS                               | EXECUTION                                   | PERSISTENCE                         | PRIVILEGE ESCALATION                | DEFENSE EVASION                          | CREDENTIAL ACCESS                      | DISCOVERY                                       | LATERAL MOVEMENT                         | COLLECTION                               | COMMAND AND CONTROL                 | EXFILTRATION   | IMPACT                           |
|--|---|-------------------------------------|-------------------------------------|--|--|---|--|--|-------------------------------------|--|----------------------------------|
| Valid Accounts<br>T1108                      | Software Deployment Tools<br>T1107          | Accessibility Features<br>T1103     | DLL Search Order Hijacking<br>T1106 | File System Logical Offsets<br>T1106     | Credential Dumping<br>T1103            | System Service Discovery<br>T1107               | Application Deployment Software<br>T1108 | Data from Local System<br>T1108          | Commonly Used Port<br>T1104         | Data Compressed<br>T1102                               | Data Destruction<br>T1105        |
| Replication Through Removable Media<br>T1109 | Windows Remote Management<br>T1102          | Shortcut Modification<br>T1103      | Process Injection<br>T1105          | Obfuscated Files or Information<br>T1102 | Input Capture<br>T1106                 | Query Registry<br>T1104                         | Windows Remote Management<br>T1102       | Input Capture<br>T1106                   | Application Layer Protocol<br>T1107 | Data Encrypted<br>T1102                                | Service Stop<br>T1108            |
| External Remote Services<br>T1102            | Service Detection Service<br>T1103          | Modify Existing Service<br>T1103    | Bypass User Access Control<br>T1106 | DLL Search Order Hijacking<br>T1106      | Brute Force<br>T1110                   | System Network Configuration Discovery<br>T1106 | Remote Desktop Protocol<br>T1102         | Email Collection<br>T1114                | Multi-layer Encryption<br>T1107     | Exfiltration Over Command and Control Channel<br>T1104 | Inhibit System Recovery<br>T1106 |
| Drive-by Compromise<br>T1109                 | Windows Management Instrumentation<br>T1104 | Path Interception<br>T1104          | Access Token Manipulation<br>T1114  | Process Injection<br>T1105               | Private Keys<br>T1140                  | Remote System Discovery<br>T1108                | Windows Admin Shares<br>T1107            | Screen Capture<br>T1114                  | Remote File Copy<br>T1107           |  | Resource Hijacking<br>T1106      |
| Spearphishing Attachment<br>T1190            | Scheduled Task/Job<br>T1105                 | Logon Scripts<br>T1107              | Sudo<br>T1109                       | Indicator Removal on Host<br>T1103       | Credentials in Registry<br>T1114       | System Owner/User Registry<br>T1103             | Remote File Copy<br>T1107                | Multi-hop Proxy<br>T1108                 |                                     |  |                                  |
| Spearphishing Link<br>T1102                  | Command Line Interface<br>T1109             | DLL Search Order Hijacking<br>T1106 |                                     | Bundled DLLs<br>T1103                    | Credentials from Web Browsers<br>T1106 | System Network Connections Discovery<br>T1106   | Remote Services<br>T1107                 | Remote Access Tools<br>T1107             |                                     |  |                                  |
|  | Scripting<br>T1104                          | New Service<br>T1103                |                                     | Disabling Security Tools<br>T1109        |  | Process Discovery<br>T1107                      |  | Standard Cryptographic Protocol<br>T1102 |                                     |  |                                  |

When you click a technique, a window opens with an explanation about the technique and a list of predefined queries. Run a query to get a list of the events in which the specific technique implementation was used.



**Brute Force - Technique T1110**

★ 0 Total Events | 🖥️ 0 Total Machines

Adversaries may use brute force techniques to attempt access to accounts when passwords are unknown or when password hashes are obtained.

[Official Mitre™ page](#)

Query 1 🗨️ 0 ★ 0

Logon Event ID IS 4625 | Connection Count IS NOT 1

Run Query

CLOSE

- To search for specific events by proactively creating your own queries:
  - Go to Let the hunt begin and click the + sign.
  - Select the required filters and enter the applicable information for the search.

3. Click Add.

It shows the search results in a timeline. The timeline provides behavioral insights that indicate anomalies or attacks.

4. To filter events based on the timeline, click the required hexagon.

It shows detailed information about the event, together with intelligent enrichment, such as attack classification, malware family and MITRE technique details.


5. To create bookmark for the custom queries, after selecting the filters, click the ☆ icon to the right of the search bar. You can choose to create the bookmark as global (available for all users in the account) or private (available only for the user).

6. You can also filter the results by date and process.

For the query results, you can choose to take remediation actions (Terminate Process, Quarantine File, Trigger Forensic Analysis, and Isolate Machine).

## Use Case - Maze Ransomware Threat Hunting

You want to investigate the maze ransomware attack. You read about it in the internet and you are afraid it may already have infiltrated your organization.

1. In the MITRE ATT&CK website: Search for Maze ransomware.
2. From the list of techniques that Maze ransomware uses, select the applicable technique. For example: Windows Management Instrumentation
3. From the Infinity Portal > Threat Hunting, click the  icon on the right side of the search box, and go to MITRE ATT&CK.
4. In the MITRE ATT&CK dashboard, search for the technique you copied from the Maze website.
5. Click the technique to see all the events in your organization in which this technique was used.