Detection Monitoring

Last updated: Jun. 25, 2025

Overview

See all available detections consolidated in a single view. View detections that originate from CrowdStrike alongside detections that originate from integrated third-party security products.

Customize your view to focus on the items that are the most relevant to your investigation, save custom filters to share with colleagues, and create incidents from selected detections.

The types of CrowdStrike-generated detections shown depend on your active Falcon subscriptions. The types of third-party detections shown depend on your integrated third-party products.

Requirements

- **Subscription:**
  - Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB
  - Optional additional subscriptions:
    - **For mobile detections:** Falcon for Mobile
    - **For identity-based detections:** Falcon Identity Threat Detection or Falcon Identity Threat Protection
- **Default roles:**
  - Falcon Administrator
  - All roles that can view and manage relevant detections
- **CrowdStrike clouds:** Available in US-1, US-2, EU-1, and US-GOV-1.
- **Additional requirements for third-party integrations:**
  - Your CID must have the required connector for each integrated third-party data source.
  - For more info about third-party integration requirements, see the CrowdStrike documentation for your applicable integrations: Third-Party Data Sources [/documentation/category/je6a45b3/next-gen-siem/third-party-integration-and-data-connectors/third-party-integrations]

Understanding the unified detections view

The unified view provides a consolidated interface for viewing and working with multiple types of detections. The unified detections view contains the same data and pivots that are available in the separate, module-specific views.

You can also get to module-specific detections in their respective dedicated views:

- Get to endpoint detections at **Endpoint security > Monitor > Endpoint detections [/activity-v2/detections]**.
- Get to mobile detections at **Endpoint security > Monitor > Mobile detections [/mobile/detections]**.
- Get to identity-based detections at **Identity protection > Monitor > Identity-based detections [/identity-protection/detections]**.
- Get to cloud runtime detections by going to **Cloud security > Detections > Containers [/cloud-security-v2/detections/containers/dashboard]** and then clicking **Container detections**.

> **Note:** Cloud runtime detections are also available at **Endpoint security > Monitor > Endpoint detections [/activity-v2/detections]**.

CrowdStrike-generated detections

The following CrowdStrike-generated detections are available in the unified view:

- Endpoint detections
- Mobile detections
- Identity-based detections
- Cloud runtime detections

Third-party detections

In the unified view, monitor and manage detections that originate from integrated third-party security products alongside CrowdStrike-generated detections.

- Corelight [/documentation/page/ba489c63/corelight-zeek]
- ExtraHop RevealX 360 [/documentation/page/d724e73b/extrahop-revealx]
- Data Connector built for Microsoft Graph API [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api]
- Mimecast [/documentation/page/reb45714/mimecast-email-security-v2]

- Netskope [/documentation/page/gd894c25/netskope-sse-v2]
- Okta Identity Management [/documentation/page/cc573d83/okta-identity-management]
- Palo Alto Next Gen Firewall [/documentation/page/bb227624/paloalto-next-gen-firewall]
- Skyhigh Security [/documentation/page/e09515f2/skyhigh-security-secure-web-gateway]

The specific data fields that appear in a given detection depend on the source product.

All available data fields and values are included in detections, but some fields are consolidated under a general **Details** heading instead of under separate field-specific headings.

Detection filters and groupings

Customize your view to focus on the items that are the most relevant to your investigation by filtering and grouping detections. For more info, see Filter, sort, and group unified detections [/documentation/page/ke886083/unified-detections-monitoring#i2215a79].

Improve efficiency and collaboration in your workflows by saving frequently used filter combinations in the unified detections view. Saved filters are accessible to all other users who have access to the unified detections view in your CID. For more info, see Managing saved filters [/documentation/page/ke886083/unified-detections-monitoring#j4c6c5a9] and Apply a saved filter [/documentation/page/ke886083/unified-detections-monitoring#sab98a5c].

Incident creation

Accelerate triage and investigation by creating an incident from selected detections in the unified view. You can include up to 200 detections in an incident.

> **Note:** Currently, a given detection can be included in only one incident.

Incidents that you create are available in the incident workbench, where they can be triaged, assigned, or investigated more deeply. You can also automate follow-up actions through Falcon Fusion SOAR workflows as you would with any CrowdStrike-generated incident. For more info, see Incident Investigation [/documentation/page/r2f1bac9/xdr-incident-investigation].

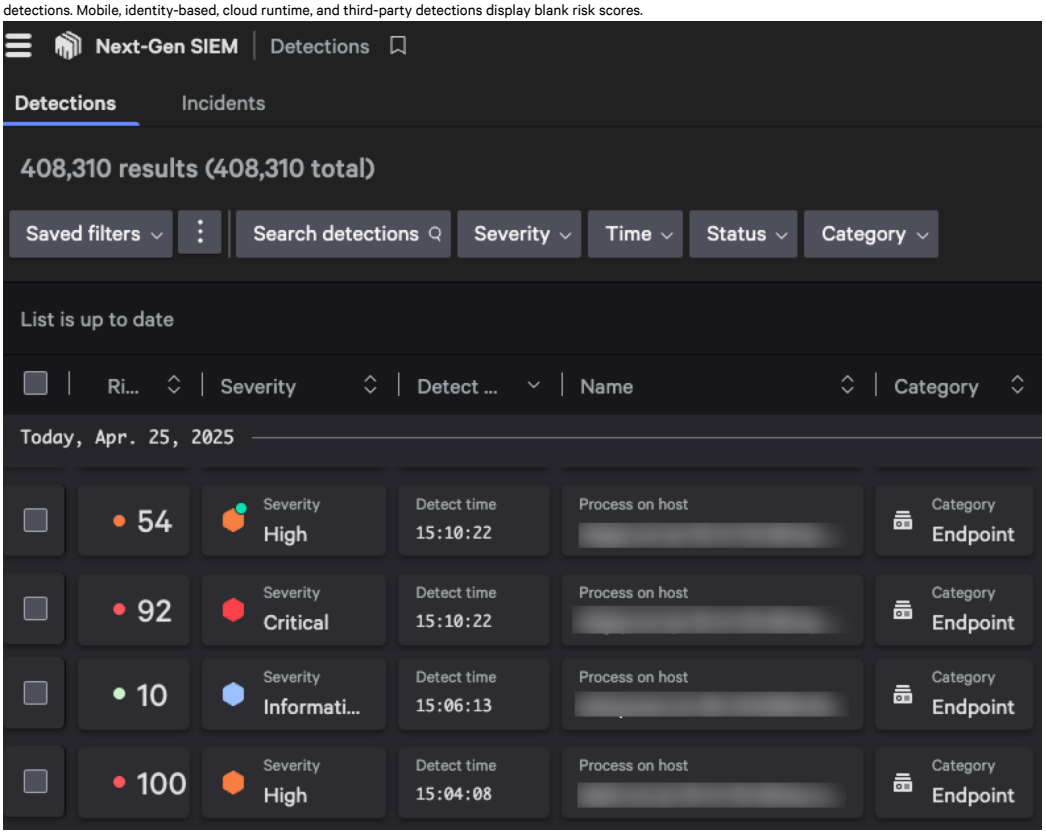
After you create an incident, a link to the incident is included in each relevant detection.

If you later edit an incident's assignee or status value, the changes are propagated to the related detections.

> **Important:** When a detection or prevention is triggered for an IOA or IOC, CrowdStrike recommends reviewing the host and process tree for events that may show additional context. Events can occur both before and after the detection that may suggest related adversary activity, such as credential access, lateral movement, data exfiltration, or file encryption. Adversaries often attempt to perform many activities on a host, so CrowdStrike recommends that your organization perform additional review and risk mitigation when detections and preventions occur.

Risk score

Detection risk scores are numerical values that indicate the potential severity and impact of a security event. Use risk scores to help prioritize your response efforts by identifying which endpoint detections require immediate attention, based on their potential impact to your organization. Risk scores are only applied to endpoint detections. Mobile, identity-based, cloud runtime, and third-party detections display blank risk scores.

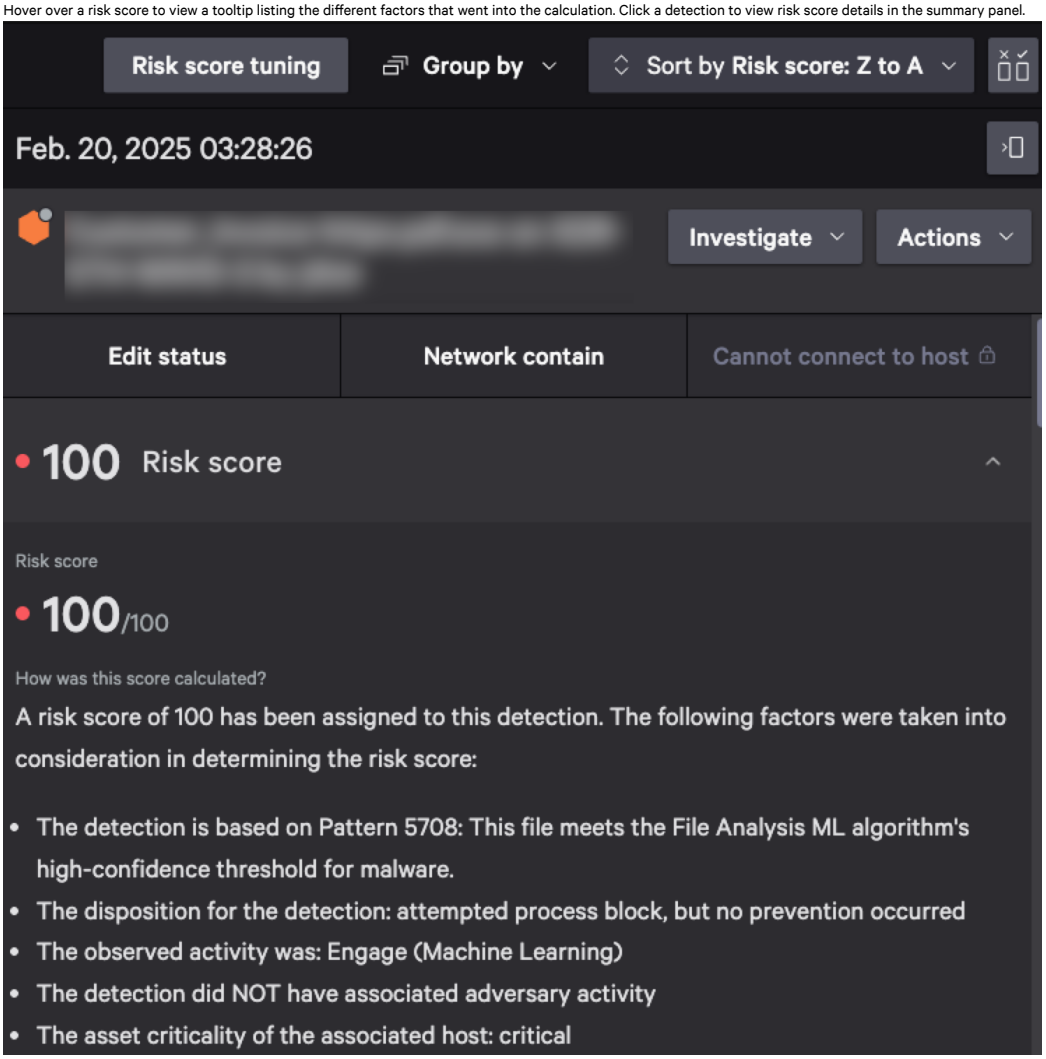


Risk scores range from 0-100. There are several factors that are calculated into a risk score. These factors include:

- Actual observed activity

- Attack technique sophistication
- Historical behavior
- Presence of preventative or response actions
- The criticality of the associated host
- The process and its parent process
- Threat intelligence context
- Type of detected activity

Hover over a risk score to view a tooltip listing the different factors that went into the calculation. Click a detection to view risk score details in the summary panel.



You can customize how risk scores are calculated by giving more or less weight to different factors, based on your unique security concerns. For more info, see Adjust risk score weighting [/documentation/page/ke886083/unified-detections-monitoring#bf8f9a04].

Example scenario: Two different risk scores

Here is an example scenario showing how risk score can change depending on context.

Next-Gen SIEM detects a suspicious PowerShell command. However, it only has a risk score of 40, because the detection occurred on a test system with no sensitive data. If the same PowerShell command occurs on a domain controller, the risk score increases to 90. This is because the asset is critical and can connect to many endpoints on the network.

For more info on asset criticality, see Asset Management: Asset Criticality [/documentation/page/ld9d1e7c/asset-management-asset-criticality].

Customize risk scoring

You can customize risk scoring sensitivity to different business impacts by adjusting weight values. This customization creates tailored threat prioritization based on your organization's specific security concerns and risk profile.

There are 4 categories: Observed activity, adversary association, prevention activity, and entity criticality. The total weight in each category must equal 100. If you increase the number of one control in a category, you must decrease a number in a control in that same category. If a control has a higher number, then Next-Gen SIEM considers it more important than related controls and therefore increases the risk score score when this control or factor is detected.

If the weight is raised above the default, the score is increased proportionally if that criteria is met, and similarly lowered if the weight is below the default.

Within each category, at most, one of the items is true for any given detection. For example, if yes is true, then no cannot be true. On the other hand, each category can apply or not apply for a given detection.The result is the combination of the individual upward and downward adjustments.

Observed activity

Observed activity describes what is known about threat actor activity on the host reporting the detection. These controls are mapped to tactics in the MITRE ATT&CK framework. There are 4 controls, listed in increasing order of severity:

- **Prepare**: The initial planning phase where adversaries gather information and build capabilities. Includes reconnaissance activities to identify targets and resource development to establish infrastructure. MITRE tactics: Reconnaissance and resource development.
- **Engage**: The initial compromise phase where adversaries gain their first foothold in the environment. Involves gaining access to systems and executing malicious code. MITRE tactics: Initial access and execution.
- **Presence**: The establishment and expansion phase where adversaries maintain access, elevate privileges, and move throughout the environment while avoiding detection. MITRE tactics: Persistence, privilege escalation, defence evasion, credential access, discovery, and lateral movement.
- **Effect**: The objective achievement phase where adversaries gather and transmit data, maintain remote control, and achieve their ultimate goals. MITRE tactics: Collection, command and control, exfiltration, and impact.

To learn more about MITRE, see MITRE-Based Falcon Detections Framework [/documentation/page/ac6e065a/mitre-based-falcon-detections-framework].

Adversary association

Adversary association refers to whether a detection has been tied to a known adversary based on behavior or indicators of compromise (IOC). There are 2 controls:

- **Yes**: Higher **Yes** weight increases score when a known adversary or IOC is detected.
- **No**: Lower **No** weight means a lower score when no adversary is detected.

Prevention activity

Prevention activity relates to mitigation actions. There are 2 controls:

- **Yes**: Higher **Yes** weight increases score when prevention activity is detected.
- **No**: Higher **No** weight increases the score when there is no prevention activity. If no mitigation actions are taken the detection becomes more urgent.

Entity criticality

Entity criticality refers to the business criticality of the entity that is part of the detection. An entity is a user, asset, or host. There are 4 controls:

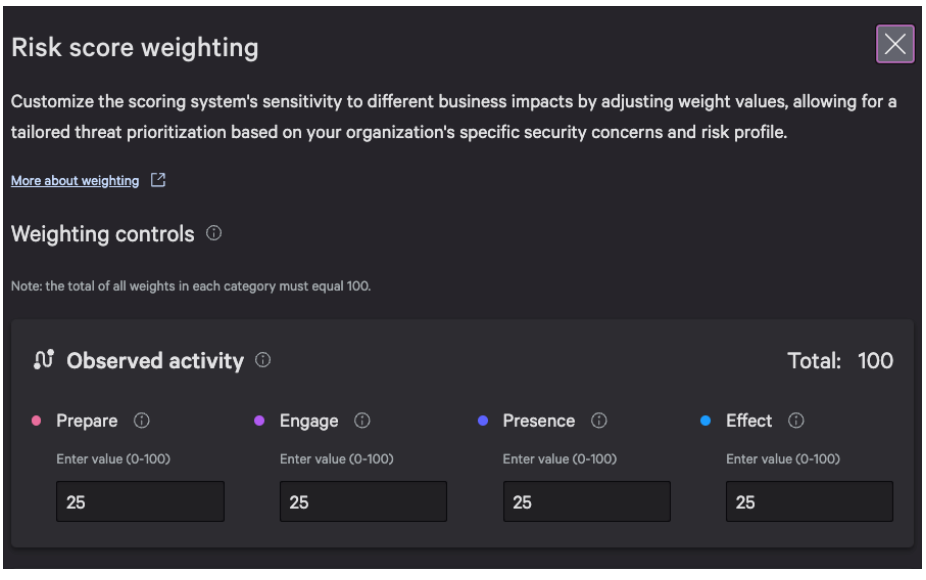
- **Critical**
- **High**
- **Non-critical**
- **Unassigned**

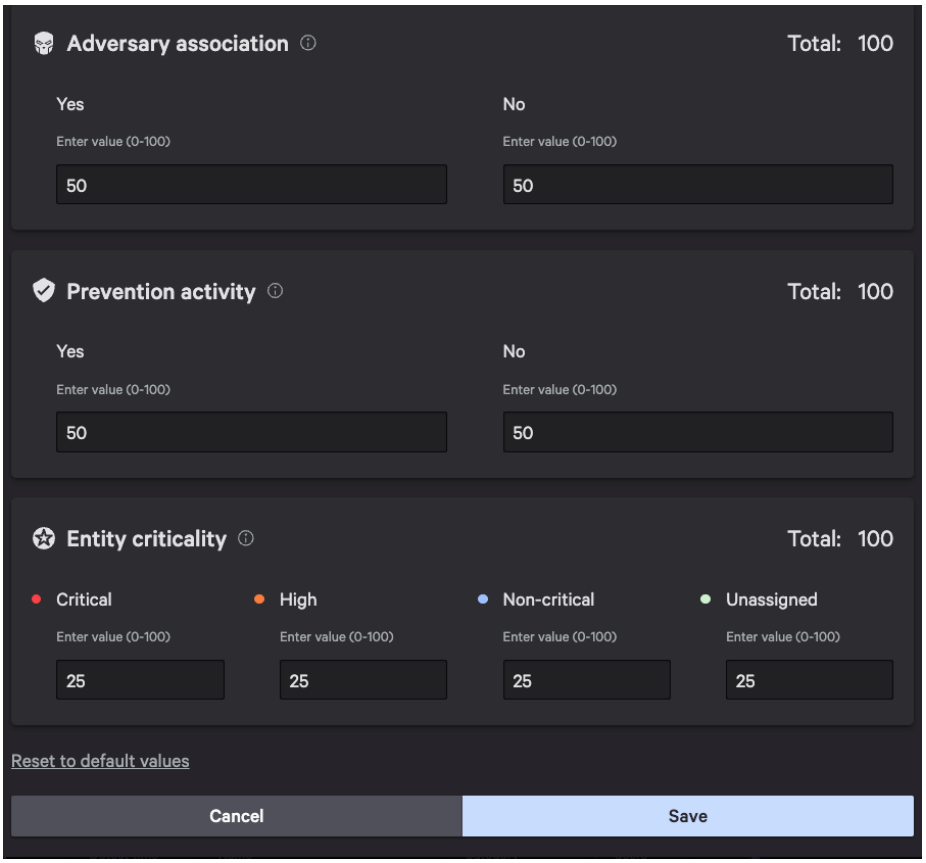
By default, each host where a detection occurs has equal weight. This means no adjustment is done. To increase the priority of detections on critical assets:

1. Increase the weight value of the Critical control.
2. Set Unassigned to a neutral weight.
3. Lower the weight of the Non-critical control.

Adjust risk score weighting

1. Go to **Next-Gen SIEM > Monitor and investigate > Detections [/unified-detections]**.
2. Click the **Risk score tuning** button.
3. Adjust the numbers in the text boxes according to your needs. The total combined weight in each category must equal 100. If you increase a number in one text box in a category, you must decrease a number in a text box in that same category.
4. To reset all of your risk weights, click **Reset to default values**.
5. Click **Save**.





Working with detections in the unified view

Get to unified detections

- Go to **Next-Gen SIEM > Monitor and investigate > Detections [/unified-detections]**.

Filter, sort, and group unified detections

By default, all available detections are shown and are sorted by time, from newest to oldest.

Refine your view by filtering, sorting, and grouping detections. The specific filtering options available depend on your Falcon subscriptions and the detection type.

In most cases, filters in the unified detections view behave identically to filters in the respective module-specific views. Exceptions:

- **Detection name:** In the module-specific view for mobile detections, the equivalent filter is **Name**. Other module-specific views don't include an equivalent filter.
- **Vendor:** For first-party detections that originate from CrowdStrike, this value is **CrowdStrike**. For third-party detections, this value is the name of the vendor that the detection originated from.
- **Platform:** This filter reflects the family of operating system that's running on the endpoint. For identity detections that involve both source and destination endpoints, this filter reflects the operating system of the source endpoint.

  > **Note:** The **Platform** filter reflects data from newly added fields; therefore, any detections that were generated before the new fields were added contain inaccurate platform information. After those detections in your CID reach their retention limit of 90 days, the **Platform** filter will show accurate information. During the 90-day transition period, you can get accurate platform information for endpoint and mobile detections that originate from CrowdStrike by filtering on the legacy **Endpoint platform** and **Mobile platform** filters. After the 90-day retention period ends, the **Platform** filter will provide accurate platform data for endpoint, mobile, and identity detections that originate from CrowdStrike.

- **IOA name:**
  - In the module-specific view for endpoint detections, the equivalent filter is **IOA name**.
  - In the module-specific view for identity-based detections, the equivalent filter is **Detection name**.
  - You can filter by **IOA name** for mobile detections in the unified view. However, the module-specific view for mobile detections doesn't include an equivalent filter.

Additionally, the unified detections view includes these unique filtering options that aren't available in the module-specific views:

- **Source product:** For third-party detections, this value is the name of the product that the detection originated from. Supported values for first-party detections that originate from CrowdStrike:
  - **Falcon Insight:** Includes both endpoint and cloud runtime detections
  - **Falcon Identity Protection**
  - **Falcon for Mobile**
- **Category:** Filter detections by specific data domains. Supported **Category** values:

- **Endpoint:** Includes both endpoint and mobile detections
- **Identity**
- **Cloud**
- **Email**
- **Web**
- **Network**

Options for grouping detections can vary by detection type. For example, some grouping options might not apply to third-party detections.

> **Note:** Some grouping options provide aggregate counts for affected users or hosts. These counts are based on newly added fields; therefore, any detections that were generated before the new fields were added reflect inaccurate aggregate counts. After the affected earlier detections in your CID reach their retention limit of 90 days, the aggregate counts will be accurate.

You can group detections by host or user across endpoint, mobile, and—when the relevant data is available—identity detections.

Show attribute-specific quick actions by hovering over a detection attribute.

Show or hide table columns by clicking **Configure table columns**.

Filter with the MITRE ATT&CK Matrix

Get a more detailed view of your environment by filtering detections based on the MITRE ATT&CK Matrix tactics and techniques. Techniques are categorized by severity and display the number of detections identified for each method.

1. In the unified detections view, enable the **MITRE ATT&CK Matrix** toggle.
2. Select which matrix you want to filter by:
   - **ATT&CK Matrix for Enterprise**
   - **ATT&CK Matrix for Mobile**
   - **ATT&CK Matrix for ICS**
   - **Falcon Detection Methods for Enterprise**
   - **Falcon Detection Methods for Mobile**
3. In the matrix view, select which tactics and techniques you want to filter by. Techniques are categorized by severity and display the number of detections identified for each method. Severity levels include: **Critical**, **High**, **Medium**, **Low**, and **Informational**.
4. Click **Apply filters** .

Tip: Clear an applied filter by clicking **Cancel** for the relevant tactic or technique in the quick filters bar.

Apply a saved filter

- In the unified detections view, from the **Saved filters** list, click the saved filter that you want to apply.

Configure detection attributes

Customize detection attributes to adjust what information appears in the list of detections, helping you triage detections more quickly and easily. For more info, see Detection Attribute Management [/documentation/page/b6c2f67b/detection-attribute-management].

Investigate detections triggered by correlation rules

From a detection's details, use the **Investigate** menu to get additional context about the detection.

- **Rule trigger event search:** View the event that corresponds to this detection being triggered.
- **Related event search:** View all the events that are part of this detection.
- **Correlation rule details:** View the **Rules** page with the correlation rule that triggered this detection selected.

Incident involvement

If a detection is part of an incident, the detection's **Related incident** attribute includes a link to the full incident.

Create an incident from selected detections

1. Go to **Next-Gen SIEM > Monitor and investigate > Detections [/unified-detections]**.
2. Filter detections as needed, and then select the checkboxes for the detections that you want to include in the incident.
3. Click **Add to incident**.
4. Select **Create a new incident** to add the detections to a new incident.
5. Enter a **Name** and optional **Description**.
6. Select a **Severity** for the incident.
7. Optional. Assign a MITRE ATT&CK tactic and technique to the incident.

8. Click **Add to incident**. After a few minutes, the incident is visible in **Next-Gen SIEM > Monitor and investigate > Incidents [/xdr/incidents]**.

Add detections to an existing incident

1. Go to **Next-Gen SIEM > Monitor and investigate > Detections [/unified-detections]**.
2. Filter detections as needed, and then select the checkboxes for one or more detections that you want to add to an incident.
3. Click **Add to incident**.
4. Select **Add to an existing incident** to add the detections to an incident that already exists.
5. Click **Select an incident** to select an incident from the list. You can also start typing to narrow the list.
6. Optional. Review the details of the incident you selected.
7. Click **Add to incident**.

Export detections

Export one or more detections in CSV or JSON format. You can include up to 200 detections in an export file.

1. Go to **Next-Gen SIEM > Monitor and investigate > Detections [/unified-detections]**.
2. Filter detections as needed, and then select the checkboxes for the detections that you want to export.
3. Click **Export**, and then click either **CSV** or **JSON**. The file preparation process begins.

   Note: The file preparation process can take up to 15 minutes to complete.
4. Click **Download**, and then save the file to your local computer.

Managing saved filters

Create a saved filter

1. In the unified detections view, apply the combination of filters that you want to save.
2. In the filter bar, click **Add or remove saved filters** ⋮ , and then click **Save**.
3. Enter a name for the filter, and then click **Save**.

Duplicate a saved filter

As an alternative method for creating a filter, you can duplicate a saved filter and then modify the duplicated filter's settings as needed.

1. In the unified detections view, from the **Saved filters** list, click the saved filter that you want to duplicate.
2. Click **Add or remove saved filters** ⋮ , and then click **Save as**.
3. Enter a name for the new filter, and then click **Save**.
4. Modify the new filter's settings as needed.

Rename a saved filter

1. In the unified detections view, from the **Saved filters** list, click the saved filter that you want to rename.
2. Click **Add or remove saved filters** ⋮ , and then click **Rename**.
3. Enter a name for the filter, and then click **Save**.

Delete a saved filter

Delete saved filters with caution. A deleted filter cannot be recovered.

1. In the unified detections view, from the **Saved filters** list, click the saved filter that you want to delete.
2. Click **Add or remove saved filters** ⋮ , click **Delete**, and then click **Delete** again.