# Table of Contents

1. Case Manager On The Home Page .................................................................................................................. 3
   1.1. My Incidents Watchlist ....................................................................................................................... 3
   1.2. Incidents In My Queues Watchlist ........................................................................................................ 3
   1.3. Notable Users Watchlist ...................................................................................................................... 3
2. The Incidents Page ........................................................................................................................................... 5
3. Get To Know An Incident ................................................................................................................................ 6
4. The Workbench ................................................................................................................................................. 8
5. The Case Manager Metrics Page ..................................................................................................................... 9
6. Configure Case Manager Settings .................................................................................................................. 11
1. Case Manager on the Home Page

On the home page, get a snapshot of the most pressing and important Case Manager incidents. The **Home** page alerts you to incidents, users, or entities you might want to investigate and organizes them into watchlists:

- **My Incidents** – View new and active incidents you're assigned to.
- **Notable Users** – View risky, increasingly suspicious users that have become threats.
- **Incidents In My Queues** – Manage incidents your queue is assigned to.

1.1. My Incidents Watchlist

On the **HOME** page, the **My Incidents** watchlist displays your new and active incidents. Sort the incidents, navigate to their profiles or timelines, or view their details.

The **My Incidents** watchlist displays new and active incidents you're assigned to.

To sort incidents by the date it was created, priority, or status, click the **Sort By** menu.

To view the details of an incident, click the incident's name.

1.2. Incidents In My Queues Watchlist

On the **HOME** page, the **Incidents In My Queues** watchlist displays incidents assigned to a queue you're in. Sort the incidents, reassign the incidents, or view their details.

Use the **Incidents In My Queues** watchlist to manage incidents assigned to queues you're in.

To sort incidents by date created, priority or status, click the **Sort By** menu.

To reassign an incident to an assignee or queue, click the name of the queue, edit the **Queue** and **Assignee** fields, then click **SAVE**.

To view further details about an incident, click its name.

1.3. Notable Users Watchlist

On the **HOME** page, the **Notable Users** watchlist displays increasingly risky users that are potential threats.

If a user is involved in increasingly risky activities, they become a threat. Advanced Analytics marks them as a "notable user" once they cross a configured risk threshold. The default risk threshold is a risk score greater than or equal to 90 points. To modify this threshold, contact customer success.

When a user becomes notable, Case Manager creates an incident and they are listed in the **Notable Users** watchlist.

If a user is associated with any open incidents, they are marked with a folder icon and the number of open incidents. Click the folder icon to view the incidents and the priority, status, and assignee for each. To go to a specific incident, select the incident's name.
To filter notable users by when they became notable, select the time filter. When you select the folder icon for these filtered users, you see just the open incidents that were created within that time frame.

To view all incidents in Case Manager, select the folder icon, then click View all incidents.
2. The Incidents Page

View, create, manage, and find incidents in the **Incidents** page.

In the navigation bar, select **INCIDENTS**.

The **Incidents** page lists all the incidents you have access to. After you view which incidents might be threats on the **HOME** page, you navigate to the **Incidents** page to begin investigating and gathering further information.

![Incidents Page](image)

Use **filters** to find incidents that match frequently used criteria, or adjust each filter input. To further narrow the list of incidents, you can also **sort them** or **search for a keyword**.

To view the **details** of an incident, select an incident from the list.

You can **manually create a new incident**, and also **reassign incidents** to new queues, assignees, status, and priorities.
3. Get to Know an Incident

Break down an incident into its components, and learn about the information and functionality available in an incident.

On the INCIDENTS page, select an incident to view its information and take steps to review and manage it.

1. Edit the incident; change its name, type, start and end time, restrict who can access the incident, and reassign the incident to a different priority, status, queue, or assignee.

2. Delete the incident.

3. Create an entity or artifact.

4. Reassign the incident to a different priority, status, queue, or assignee.

5. Access the workbench to run actions and playbooks, and view the results.

6. View information about the incident. The fields vary based on the type of incident and from where it was ingested. You can customize these fields and how they are organized in the incident.

7. View entities associated with the incident and manually add an entity.

8. View the results of actions and playbooks you've run on the incident.
9 View the tasks that must be completed for this incident.
10 View artifacts associated with the incident and manually add an artifact.
11 Send messages, like case notes and emails, directly from the incident.
12 View the incident’s history.
4. The Workbench

View all Incident Responder actions and playbooks you've run on an incident and their outputs, and run more actions and playbooks at an incident's workbench.

To navigate to an incident's workbench, go to the INCIDENTS page, select an incident to view its details, then click the View Workbench button.

View all Incident Responder actions and playbooks you've run on this incident and what the outputs are. The number on each action or playbook indicates how many input parameters it processed. To view the output for an input, select the menu.

To run single actions or full playbooks, select RUN ACTION or RUN PLAYBOOK.
5. The Case Manager Metrics Page

View graphs, charts, and diagrams about how Case Manager is performing in the Metrics page.

The **Metrics** page is a dashboard of visualizations—graphs, charts, and diagrams—that reflect Case Manager’s current state and environment. It measures and assesses how security operations and events are performing.

Filter the **Metrics** dashboard by incident assignee and time period. If you select a time period, it is applied across all charts.

Every time you refresh the page, the metrics also refresh.

View visualizations about:

- **Open Incidents** - The number of incidents currently open.
- **Mean Time to Resolution** - The current mean (average) time to resolve all closed incidents in the environment.
- **Mean Time To Close** - The current mean (average) time taken to close all of the currently closed incidents in the environment.
- **Mean Dwell Time** - The current mean (average) dwell time for all incidents. Measured by incident start date to incident create date.
- **False Positives** - The percentage of false positive incidents found in Incident Responder.

- **Hours Saved** - Approximates how much Incident Responder worked equivalent to manual people hours based on the type of incident, average response time, and number of incidents processed.

- **New vs Closed Incidents** - A timeline view of how many incidents were created vs closed on a given day.

- **Incidents by Type** - A grid that breaks down incidents by their type. Hover over a date to view data specific to that date.

- **Work Distribution** - Total incidents assigned to each team member, reflects how incidents and workload are allocated across the SOC team.

- **Incidents by Status** - A percentage pie chart that breaks down the total incidents by their current status - New, In Progress, Pending, Resolved, Closed.

- **Mean Time to Resolution Table** - Mean time to resolution based on incident type, as measured from the time an incident is marked In Progress to when it is marked Resolved.

- **Incident Breakdown** - The number of open incidents, created incidents, closed incidents, and the average time that an incident remains unassigned to a user.

To download the current dashboard as a PDF, select the download button. The PDF contains data for all visualizations.
6. Configure Case Manager Settings

Ingest data, create rules to triage incidents, customize incidents, create or edit queues, and configure a proxy in Case Manager settings.

In the navigation bar, click the Menu ☰, select Settings, then navigate to Case Management.

In Incident Ingestion, add sources that feed data into Case Manager, specify which type of log to ingest from your incident source, configure email ingest, and configure an email account to send emails directly from an incident.

In Incident Rules, create rules to automatically triage incidents after they’re created.

In Incident Configuration, create incident types, incident fields, tasks, and phases.

In Queues, create or edit a queue.

In Proxy, configure a proxy connection, if your organization uses one.