Manage Your Team

Exabeam Security Management Platform - Version SMP 2021.1 (CM I55)

Publication date April 3, 2021

Exabeam
1051 E. Hillsdale Blvd., 4th Floor
Foster City, CA 94404

650.209.8599

Have feedback on this guide? We'd love to hear from you!
Email us at docs@exabeam.com

Disclaimer: Please ensure you are viewing the most up-to-date version of this guide by visiting the Exabeam Documentation Portal.

Copyright

Trademarks

Patents

Exabeam owns, and reserves all rights for, patents for Exabeam products and services, which may be protected under registered patents as well as patents pending.

Other Policies

For information regarding Exabeam’s treatment of personally identifiable information, please review Exabeam’s current privacy policy at www.exabeam.com/privacy.

Table of Contents

1. Case Manager Queues

Effectively manage a shared workload and organize your investigation with queues.

A queue is a designated group responsible for investigating an incident. Every incident is assigned a queue. If you're in a queue assigned to an incident, you're responsible for working on the incident. Track the incidents your queue is assigned to with the **Incidents in My Queues** watchlist. The incident remains assigned to your queue until someone closes the incident or assigns it to another queue.

By default, everyone is in the Unassigned Queue. Create new queues that better fit your needs. You might create queues based on SOC tiers (tier 1, tier 2, and tier 3) or a 24-7 service model.

You can edit or delete a queue you created.

1.1. Create a Queue

To assign incidents to a group of people, create a queue.

1. In the navigation bar, click the menu ☰, select **Settings**, then select **Core**.
2. Under **QUEUES**, click **Queues**.
3. Click **Add a new queue** ⊕.
4. Enter a name for the queue.
5. (Optional) Describe the queue.
6. Add people to the queue:
   - To add specific people, click **+** next to the person's name. To quickly find and add a person, start typing in the search.
   - To add everyone in the system, click **ADD ALL**.
7. Click **CREATE QUEUE**.

1.2. Edit a Queue

Change the name, description, or people in a queue you created.

1. In the navigation bar, click the menu ☰, select **Settings**, then select **Core**.
2. Under **QUEUES**, click **Queues**.
3. Hover over a queue, then click **Edit Queue** ✎.
4. Edit the name, description or people in the queue.
5. Click **SAVE QUEUE**.

1.3. Delete a Queue

If you created a queue, you can delete it. Any people and incidents assigned to the queue are reassigned to the default Unassigned queue.

1. In the navigation bar, click the menu ☰, select **Settings**, then select **Core**.
2. Under **QUEUES**, click **Queues**.
3. Hover over a queue, then select **Delete Queue** 🗑.
4. Click **DELETE**.

2. Exabeam Phases

Organize your investigations and ensure everyone responds consistently using phases.

A phase is a general stage of your investigating process. It contains tasks that an analyst must complete in each phase.

Phases and tasks ensure everyone across your organization responds to different security scenarios consistently. A manager builds a set of standard scenarios and creates processes for each one. When analysts investigate an incident, they follow this process, working on separate items in parallel so their efforts don't overlap.

Exabeam provides five phases out of the box:

- Detection
- Containment
- Eradication & Mitigation
- Recovery
- Post-Incident Activity

Rename phases or create your own phase according to your needs. You can also delete and reorder phases.

2.1. Create a Phase

To standardize how you respond to incidents, break out your investigating process into phases and assign tasks to each one.

1. In the navigation bar, click the menu ☰, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **Tasks & Phases** tab.
4. Click **ADD PHASE**.
5. Enter a unique phase name, then click **SAVE**.
6. Click **PUBLISH**. The phase appears only in new incidents. It doesn't appear in existing incidents, open or closed.

2.2. Rename a Phase

Rename any phase to change how they appear in incidents.

1. In the navigation bar, click the menu ☰, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **TASKS & PHASES** tab.

4. Hover over a phase, then select edit ✎.
5. Change the phase name.
6. Click **SAVE**.
7. Click **PUBLISH**. Your changes are reflected in new incidents. They don't apply to existing incidents, open or closed.

3. Exabeam Tasks

Assign specific responsibilities and ensure everyone responds consistently using tasks.

A task is an action an analyst must complete when they investigate; for example, *confirm incident is contained*, *capture volatile data from systems as evidence*, *determine root cause.* Tasks are organized into phases of an investigation.

Phases and tasks ensure everyone across your organization responds to different security scenarios consistently. A manager builds a set of standard scenarios and creates processes for each one. When analysts investigate an incident, they follow this process, working on separate items in parallel so their efforts don't overlap.

3.1. Create a Task for a Phase or Incident Type

Create a task that always appears under a specific phase or incidents of a certain type.

You can create a task just for one specific incident. To automatically create a task depending on the conditions of an incident, set up a playbook.

1. In the navigation bar, click the menu ☰, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **Tasks & Phases** tab.
4. Click **ADD A TASK**.
5. Enter information about the task:
   - **Name** – Enter a name for the task.
   - **Instructions** – Enter instructions, details, or other information about the task.
   - **Phase** – Select the phase that the task appears under.
   - **(Optional) Incident type** – Select the incident type that the task appears under.
   - **Due date** – If there is no due date, select **None**. If there is a due date, select how many days after the task is initiated.
   - **(Optional) Required task** – If the task is required, select this box.
6. Click **SAVE**.
7. Click **PUBLISH**.

3.2. Delete a Task for a Phase or Incident Type

Delete a task that appears under a phase or for all incidents of a certain type.

1. In the navigation bar, click the menu ☰, select **Settings**, then select **Analytics**.
2. Under **Case Management**, select **Incident Configuration**.
3. Select the **Tasks & Phases** tab.

4. Hover over a task, then select the trash 🗑. A warning appears.
5. Click **DELETE**.
6. Click **PUBLISH**. Your changes are reflected in new incidents. They don't apply to existing incidents, open or closed.

3.3. Create a Task for a Specific Incident

Create a task that only appears under a specific incident to ensure that your team doesn't miss something when they respond to it.

Under each phase, create tasks to ensure your team complete certain duties. Assign the tasks to specific people so they know exactly what they should do to work in parallel. After they complete the task, they mark it as done.

You can create a task that always appears under a phase or for all incidents of a specific type. To automatically create a task depending on the conditions of an incident, set up a playbook.

1. In the navigation bar, click **INCIDENTS**, select an incident, then select the **Tasks** tab.
2. In a phase, click **ADD TASK**
3. Enter information about the task:
   - **Name** – Enter a name for the task.
   - **Instructions** – Enter instructions, details, or other information about the task.
   - **Assignee** – Assign the task to a person.
   - **Due Date** – Select a date that this task should be closed by.
4. Click **SAVE**.

3.4. Manage a Task in an Incident

View, reassign, change the due date, update the status, and add notes to any task, just for that specific incident.

1. In the navigation bar, click **INCIDENTS**, select an incident, then select the **Tasks** tab.
2. Select a phase to expand it and view associated tasks, assignee(s), and due date. Hover over the task to view further details.
3. Edit the task:
   - To re-assign the task to another analyst, click the task assignee and select another analyst from the list.
   - To change the due date, click the task due date and select another date on the calendar. If a task is not closed before the due date, the due date appears in red text with a warning icon.
   - To view additional details or update the task status, select the task name. Review the due date, add notes about the conclusion, or mark the task as done.

- To close a task, select the task name to view additional details, then click **MARK AS DONE**
  OR
  On the **Task** tab, select the checkbox.