exabeam

Alert Triage

Publication date April 7, 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.

Table of Contents

1. Exabeam Alert Triage

Quickly and diligently identify, prioritize, and respond to important security alerts with Alert Triage on Exabeam Cloud Platform.

Alert Triage is an application on Exabeam Cloud Platform, available for users with a SaaS deployment of Advanced Analytics and Case Manager. It is your hub for incoming third-party or Exabeam Data Lake alerts, made smarter with machine learning, risk scores, and automatic context enrichment to help you efficiently investigate and triage alerts.

If you have administrator or manager permissions, you create a channel to gather alerts based on criteria you specify. If you're an analyst assigned to a channel, you investigate the alerts in these channels. Each alert provides the actionable insights you need to accurately assess the alert's potential impact and make an informed decision.

Where raw logs lack context, Alert Triage fills in the gaps. After it ingests alerts and the corresponding raw logs, it associates the alert to specific users and devices, calculates risk scores, connects alerts to related anomalies and ongoing sessions in Advanced Analytics Smart Timelines™, and enriches the alert with other contextual information so you have a complete picture of all users and devices involved.

After a quick investigation, you dismiss or escalate the alert. When you escalate the alert, you create a Case Manager incident with the Exabeam Alert Triage incident type, which includes alert-specific information like alert name, type, and severity.

2. Exabeam Cloud Platform Roles for Alert Triage

Understand how Advanced Analytics user permissions map to Exabeam Cloud Platform roles.

With Alert Triage, you are automatically enrolled in Exabeam Cloud Platform. In Exabeam Cloud Platform settings, you see **Exabeam IdP** in the **IDP** column for users who access Exabeam Cloud Platform through Advanced Analytics.

By default, Advanced Analytics users with out-of-the-box roles are automatically assigned out-of-the-box Exabeam Cloud Platform user roles:

- **Advanced Analytics Tier 1 Analyst** – Exabeam Cloud Platform Standard User
- **Advanced Analytics Tier 3 Analyst** – Exabeam Cloud Platform Standard User
- **Advanced Analytics Auditor** – Exabeam Cloud Platform Standard User
- **Advanced Analytics Data Privacy Officer** – Exabeam Cloud Platform Standard User
- **Advanced Analytics Administrator** – Exabeam Cloud Platform Administrator

If you are an Exabeam Cloud Platform administrator, you can change which Advanced Analytics roles are assigned to which Exabeam Cloud Platform roles.

Advanced Analytics users with custom user roles aren't automatically assigned Exabeam Cloud Platform roles. If you are an Exabeam Cloud Platform administrator, you must manually assign custom Advanced Analytics user roles to an Exabeam Cloud Platform role before these users can access Alert Triage.

For Alert Triage, the Exabeam Cloud Platform manager and administrator roles have the same permissions.

3. Alert Triage Channels

Organize a shared workload and get assigned to investigate certain alerts with Alert Triage channels.

An Alert Triage channel is a subset of alerts that analysts are assigned to investigate. If you have administrator or manager permissions, you curate the alerts in a channel based on certain criteria: source, severity, alert type, and alert name.

All channels you're assigned to appear on the All Channels tab. When you select a channel, it appears in another tab. On the tab, a number indicates how many new alerts have appeared in the channel since you last opened it. Select any alert in the channel to investigate, dismiss, or escalate it.

If you're an administrator or manager, you can create, edit, and delete a channel.

3.1. Create a Channel

Create and assign analysts to a channel so they can start triaging a specific subset of alerts. You can create a channel only if you have administrator or manager permissions.

1. On the All Channels tab, click **+ Create a Channel**.
2. To determine which alerts appear in the channel, filter the alerts by source, severity type, alert type, and alert name. The source you select narrows the possible values for the other criteria. These values have appeared at least once before in an existing alert.
   For an alert to appear in the channel, it must match all the criteria for a filter.
   a. After **show alerts where source is**, click the empty space, then select a vendor source. To search for a specific vendor source, start typing. You see the vendor sources for all your alerts, including Exabeam Data Lake you have it.
   b. (Optional) After **severity is**, click the empty space, then select a severity type from the list. To select all severity types in the list, select **Select All**.
   If you leave this blank, an alert appears in the channel if it has *any* severity type, including new severity types Alert Triage hasn't seen before.
   c. (Optional) After **alert type is**, click the empty space, then select an alert type from the list. To select all alert types in the list, select **Select All**.
   If you leave this blank, an alert appears in the channel if it has *any* alert type, including new alert types Alert Triage hasn't seen before.
   d. (Optional) After **alert name is**, click the empty space, then select an alert name from the list. To select all alert names in the list, select **Select All**.
   If you leave this blank, an alert appears in the channel if it has *any* alert name, including new alert names Alert Triage hasn't seen before.
3. To add another filter, click the add button. For an alert to appear in the channel, it must match all the criteria in at least one filter.
4. Under **Preview**, preview the alerts that match the filters you specified.
5. Click **Save Filters**.

6. Enter basic information about the channel:
   - **Channel Name** – Enter a name for the channel.
   - **Channel Assignment** – To assign people to investigate alerts in the channel, click the box, then select the people who can view the channel. To select all the people in the list, select **Select All**. Since you created the channel, you automatically have access.
   - (Optional) **Description** – Describe the channel.
7. Click **Create**.

3.2. Edit a Channel

Edit the filters that determine which alerts are curated in the channel, reassign people to the channel, or rename the channel. You can only edit channels you created.

1. Navigate to the All Channels tab.
2. Hover over a channel, then select edit.
3. Change the channel's filter criteria, name, access permissions, or description.
4. Click **Save**.

3.3. Delete a Channel

You can only delete channels you created.

1. Navigate to the All Channels tab.
2. Hover over a channel, then click the trash.
3. Click **Delete**. The channel is deleted for all users. If any users are currently viewing the channel, you may disrupt their workflow. Alert statuses remain the same.

4. Investigate Alerts

Understand the contextual information available in a channel and alert to determine which alerts are worth looking at, assess an alert's potential impact, and decide your next steps.

Although Alert Triage has already automated much of your workflow, there may still be hundreds of alerts in a channel. Use the contextual information provided with each alert to correlate alerts and build a complete picture of your organization's threat landscape. Once you understand this context, you can make informed decisions about what to investigate and how to respond.

4.1. 1. Identify where to start investigating

To get an overview of what's happening in a channel and identify where to start, review the list of all alerts in a channel. Alerts are sorted based on when they were created, from latest to oldest.

From the contextual information provided at a glance, learn about:

- When the alert was created
- The source that created the alert
- How severe the alert is, according to the alert source: low, medium, high, or critical
- The alert name
- Associated users and their risk score during the session when the alert occurred. If the session is ongoing, the risk score updates concurrently.
- Associated assets, whether it's a source or destination, and its risk score during the session when the alert occurred. If the session is ongoing, the risk score updates concurrently.
- Alert status:
  - **New** – By default, an alert has a **New** status. Once you change an alert to another status, you can't revert the status to **New**.
  - **In Progress** – Someone was assigned to investigate the alert and assess its impact. The alert is unassigned by default. If you ever reassign the alert to **Unassigned**, the alert status won't change.
  - **Escalated** – The alert is a potential true positive you want to report. This creates an incident in Case Manager.
  - **Dismissed** – The alert is a false positive.
  - **Resolved** – You resolved the alert without escalating it.
- Who has been assigned to investigate the alert

If an alert looks like it may be worth investigating further, click the alert to view more details.

4.2. 2. Assess an alert's potential impact

To better understand if an alert may be a true positive, view further details about the alert to further investigate it and assess its potential business impact.

1. From the list, select an alert.

2. To view the raw log, select the **View logs**. View details about time, date, alert type, severity, source IP, source host, or user.
3. Under **USER/DEVICE**, view the users and devices associated with the alert and whether they triggered other alerts in the past week. To learn more about the user or device, click on its name and view more details in Advanced Analytics. To understand the alert in the context of other anomalies, click **Go to Timeline**.
4. To understand what happened before this alert was triggered, under **NEARBY ANOMALIES**, view the five anomalies with the highest risk scores that occurred previously. To view all previous anomalies in the session, click **Show all**.

4.3. 3. Respond to the alert

After assessing this contextual information about the alert and associated users or devices, resolve, dismiss, or escalate it.

5. Respond to an Alert

After you investigate an alert, resolve, dismiss, or escalate it.

Resolve an alert if you took action to close the alert without escalating it.

Dismiss an alert if it's a false positive.

Escalate an alert if you determined that an alert is a true threat to move up your chain of command. When you change an alert's status to escalate, you create an incident in Case Manager. You can only create one incident for each alert. If you escalate an alert multiple times, you won't create multiple Case Manager incidents. If you change an alert's status in Alert Triage, the incident's status doesn't change in Case Manager.

1. To quickly dismiss an alert in a channel, hover over the alert, then click **Dismiss**.
   In the alert, click **Resolve**, **Dismiss**, or **Escalate**.
2. If you escalated the alert, select a priority for the incident created in Case Manager: low, medium, high, or critical.
   Click **Escalate**. In Case Manager, an alert is created in the Exabeam Alert Triage incident type, which includes alert-specific information like alert name, type, and severity.

6. What's New in Alert Triage

6.1. April 6, 2021

New	This is the General Availability release for Alert Triage.
Improved	Performance and stability improvements.
Fixed	Minor bugs and UI issues.
Known Issues	During a session, if no anomalies occurred before the security alert, you don't see any anomalies under the **Nearby Anomalies**, **Top <#>** tab. We're enhancing this tab and the **Show all** tab in the next release.