exabeam

Investigate a Security Incident

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

All content in this document, including text, graphics, logos, icons, images, and video clips, is the exclusive property of Exabeam or its content suppliers and is protected by U.S. and international copyright laws. The compilation (meaning the collection, arrangement, and assembly) of all content in this document is the exclusive property of Exabeam and is also protected by U.S. and international copyright laws. The content in this document may be used as a resource. Any other use, including the reproduction, modification, distribution, transmission, republication, display, or performance, of the content in this document is strictly prohibited.

Copyright ©2021 Exabeam, Inc. All Rights Reserved.

Trademarks

Exabeam, the Exabeam logo, Threat Hunter, Smarter SIEM, Smart Timelines and Security Management Platform are service marks, trademarks or registered marks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. The marks and logos displayed in this document may not be used without the prior written consent of Exabeam or their respective owners.

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. Edit an Incident

Change an incident's details, and reassign the incident to different people, priority, or status.

1. On the **INCIDENTS** page, select an incident.
2. Select edit .
3. Change the incident details:
   - **Incident name** – Enter an incident name.
   - **Incident type** – Select an incident type.
   - **Event start time** – Indicate when the incident started.
   - **Event end time** – Indicate when the incident ended, if known.
   - **Queue** – Assign the incident to a queue. If not, the incident is assigned to the default Unassigned queue.
   - **Assignee** – Assign the incident to someone on your team. If not, it is assigned to "unassigned" by default.
   - **Priority** – Low, medium, high, or critical.
   - **Status** – Select the status of the incident: **New**, **In Progress**, **Pending**, **Resolved**, or **Closed**. Feel free to use these statuses according to your organization's workflow and needs.
   - **Restrict to** – Restrict who can access this incident. These people or groups can't see or search for this incident.
   - **Description** – Provide context about the incident.
4. Select **SAVE**.

2. Assign an Incident to a Queue, Assignee, Priority, or Status

When you create an incident, it is assigned the unassigned queue, unassigned assignee, medium priority, and new status by default. Reassign an incident to better fit your needs.

1. On the **INCIDENTS** page, hover over an incident, then select edit .
2. Edit the **Queue**, **Assignee**, **Status**, or **Priority**.
3. Click **SAVE**.
   If you reassign the incident to a new assignee, that assignee is notified via email if their email is in the system. If you reassign the incident to a new queue, no one is notified.

3. Manually Add an Entity

Add the primary objects you're investigating to the incident.

3.1. Add a File Entity

1. Navigate to an incident or its workbench:
   - To start from an incident, in the navigation bar, click **INCIDENTS**, then select an incident.
   - To start from an incident's workbench, in the navigation bar, click **INCIDENTS**, select an incident, then select **View Workbench**
2. Click **Add a new entity**.

   In an incident, you may also locate the **Entities** panel and click **Add a new entity**.
3. Under **Entity type**, select **File**.
4. To extract a file's name, hash, and size, select **Upload file**. To manually fill all fields, select **Manually enter file details**.
   - If you selected **Upload file**:
     1. Click **UPLOAD FILE**, then select a file from your system.
     2. Under **File path**, enter where the file is located in your file system.
   - If you selected **Manually enter file details**, fill in the fields:
     - **File name** – Enter the name used to uniquely identify the file in the file system.
     - **Hash type** – Enter at least one hash value from a MD5, SHA256, SHA1, or SHA512 function.
5. Click **SAVE**. The entity appears in the incident under the **Entities** panel.

3.2. Add a Device Entity

1. Navigate to an incident or its workbench:
   - To start from an incident, in the navigation bar, click **INCIDENTS**, then select an incident.
   - To start from an incident's workbench, in the navigation bar, click **INCIDENTS**, select an incident, then select **View Workbench**
2. Click **Add a new entity**.

   In an incident, you may also locate the **Entities** panel and click **Add a new entity**.
3. Under **Entity type**, select **Device**.
4. To extract data from an existing host, IP or URL asset in Advanced Analytics, select **Select from AA**. To manually enter all details, select **Custom**.
   - If you selected **Select from AA**, start typing to search for a host or IP, select a result, then enter an associated URL. Fill in the fields:

- **Type** – Select an operating system, Windows, Linux, or Mac.
- **Zone** – Enter the internal network location the device last connected from. This may be a city, business unit, building, or room.
- **Location** – Enter the city, U.S. state (if applicable), and country the device last connected from.

- If you selected **Custom**, enter at least one **Host**, **IP**, or **URL**, then fill in the fields:
  - **Type** – Select an operating system, Windows, Linux, or Mac.
  - **Zone** – Enter the internal network location the device last connected from. This may be a city, business unit, building, or room.
  - **Location** – Enter the city, U.S. state (if applicable), and country the device last connected from.

5. Click **SAVE**. The entity appears in the incident under the **Entities** panel.

3.3. Add a User Entity

1. Navigate to an incident or its workbench:
   - To start from an incident, in the navigation bar, click **INCIDENTS**, then select an incident.
   - To start from an incident's workbench, in the navigation bar, click **INCIDENTS**, select an incident, then select **View Workbench**
2. Click **Add a new entity** .
   In an incident, you may also locate the **Entities** panel and click **Add a new entity** .
3. Under the **Entity type**, select **User**.
4. To extract data from an existing user in Advanced Analytics, select **Select from AA**. To manually enter all details, select **Custom**.
   - If you selected **Select from AA**, start typing to search for a user, then select from the results. Case Manager extracts all data available in Advanced Analytics.
   - If you selected **Custom**, enter the user's **Full Name** or **Username**, then fill in the fields:
     - **Account ID** – Enter the account ID associated with the user's login credentials.
     - **User email** – Enter the user's work email address
     - **User title** – Enter the user's job title.
     - **User department** – Enter the corporate department the user works in.
     - **Employee type** – Indicate the user's employee type; for example, full-time, part-time, or contractor.
     - **Zone** – Enter the internal network zone within your organization the user last connected from. This may be a city, business unit, building, or room.

- **User office phone** – Enter the phone number the user uses at their office location.
- **User cell phone** – Enter the user's personal cell phone number.
- **Manager name** – Enter the full name of the user's manager.
- **Manager email** – Enter the manager's work email address/
- **Manager title** – Enter the manager's job title.
- **Manager office phone** – Enter the phone number the manager uses at their office location.
- **Manager cell phone** – Enter the manager's personal cell phone number.

5. Click **SAVE**. The entity appears in the incident under the **Entities** panel.

4. Manually Add an Artifact

Provide external evidence to your investigation. You can choose from five artifact types.

4.1. Add a File Artifact

1. Navigate to an incident or its workbench:
   - To start from an incident, in the navigation bar, click **INCIDENTS**, then select an incident.
   - To start from an incident's workbench, in the navigation bar, click **INCIDENTS**, select an incident, then select **View Workbench**
2. Click **Add a new artifact**  .
3. Under **Artifact type**, select **File**.
4. To extract a file's name, hash value, and size, select **Upload file**. To manually enter all details, select **Manually enter file details**.
   - If you selected **Upload file**, click **UPLOAD FILE**, then select a file from your file system. Fill in the fields:
     - **File path** – Enter where in the file system this file is located.
     - **Threat status** – Indicate if the artifact is a malicious, benign, or unknown threat, or a false positive.
     - **Role** – Specify if the artifact describes a victim, attacker, or unknown.
     - **Related entity** – Indicate which entity the artifact is related to.
   - If you selected **Manually enter file details**, fill in the fields:
     - **File name** – Enter the name used to uniquely identify the file in the file system.
     - **Hash type** – Enter at least one hash value from a MD5, SHA256, SHA1, or SHA512 function.
     - **Threat status** – Indicate if the artifact is a malicious, benign, or unknown threat, or a false positive.
     - **Role** – Specify if the artifact describes a victim, attacker, or unknown.
     - **Related entity** – Indicate which entity the artifact is related to.
5. Click **SAVE**. The artifact appears in the incident under the **Artifact** tab.

4.2. Add an IP Artifact

1. Navigate to an incident or its workbench:
   - To start from an incident, in the navigation bar, click **INCIDENTS**, then select an incident.
   - To start from an incident's workbench, in the navigation bar, click **INCIDENTS**, select an incident, then select **View Workbench**

2. Click **Add a new artifact** .
3. Under **Artifact type**, select **IP**.
4. Fill in the fields:
   - **IP** – Enter the IP address this artifact describes.
   - **Location** – Enter the city, U.S. state (if applicable), and country this IP last connected from.
   - **Threat status** – Indicate if the artifact is a malicious, benign, or unknown threat, or a false positive.
   - **Role** – Specify if the artifact describes a victim, attacker, or unknown.
   - **Related entity** – Indicate which entity the artifact is related to.
5. Click **SAVE**. The artifact appears in the incident under the **Artifact** tab.

4.3. Add a Process Artifact

1. Navigate to an incident or its workbench:
   - To start from an incident, in the navigation bar, click **INCIDENTS**, then select an incident.
   - To start from an incident's workbench, in the navigation bar, click **INCIDENTS**, select an incident, then select **View Workbench**
2. Select the fingerprint button.
3. Under **Artifact type**, select **Process**.
4. Fill in the fields:
   - **Process name** – Enter the file name of the program that executed the process.
   - **Process path** – Enter where in the file system the program file was located.
   - **Process ID** – Enter the ID of the process the artifact describes.
   - **UID** – Enter process's user ID, available in Unix-like operating systems.
   - **Start time** – Enter the date and time the process started running. You may also select the calendar and clock icons to enter a date and time.
   - **End time** – Enter the date and time the process stopped running. You may also select the calendar and clock icons to enter a date and time.
   - **Threat status** – Indicate if the artifact is a malicious, benign, or unknown threat, or a false positive.
   - **Role** – Specify if the artifact describes a victim, attacker, or unknown.
   - **Related entity** – Indicate which entity the artifact is related to.
5. Click **SAVE**. The artifact appears in the incident under the **Artifact** tab.

4.4. Add a URL Artifact

1. Navigate to an incident or its workbench:
   - To start from an incident, in the navigation bar, click **INCIDENTS**, then select an incident.
   - To start from an incident's workbench, in the navigation bar, click **INCIDENTS**, select an incident, then select **View Workbench**
2. Click **Add a new artifact**  .
3. Under **Artifact type**, select **URL**.
4. Fill in the fields:
   - **URL** – Enter the URL the artifact describes.
   - **IP** – Enter the the URL's corresponding IP address.
   - **Location** – Enter the city, U.S. state (if applicable), and country the URL was last accessed from.
   - **Threat status** – Indicate if the artifact is a malicious, benign, or unknown threat, or a false positive.
   - **Role** – Specify if the artifact describes a victim, attacker, or unknown.
   - **Related entity** – Indicate which entity the artifact is related to.
5. Click **SAVE**. The artifact appears in the incident under the **Artifact** tab.

4.5. Add an Email Address Artifact

1. Navigate to an incident or its workbench:
   - To start from an incident, in the navigation bar, click **INCIDENTS**, then select an incident.
   - To start from an incident's workbench, in the navigation bar, click **INCIDENTS**, select an incident, then select **View Workbench**
2. Click **Add a new artifact**  .
3. Under **Artifact type**, select **Email Address**.
4. Fill in the fields:
   - **Email address** – Enter the email address the artifact describes.
   - **Threat status** – Indicate if the artifact is a malicious, benign, or unknown threat, or a false positive.
   - **Role** – Specify if the artifact describes a victim, attacker, or unknown.
   - **Related entity** – Indicate which entity the artifact is related to.
5. Click **SAVE**. The artifact appears in the incident under the **Artifact** tab.

5. Entity Types

When you add an entity to an incident, they fall under three types. Each type contains a unique set of data, which you can input to action nodes in Incident Responder playbooks.

File – Any electronic file; for example, Word and Excel documents, Windows or Linux executables.

Device – A computer, either on an internal network or the internet.

User – A person identified by a corporate directory account ID, email address, or other means (app login ID, full name, etc.).

5.1. File Entity Data

Every entity type contains data a unique set of data fields. The file entity contains data about the file path, size, hash, and more. In Incident Responder, you can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

File created time	Date and time this file was created. **Example:** *2019-05-06 15:56*
File name	Name used to uniquely identify the file in the file system. **Example:** *barbarian.jar*
File path	Where in the file system this file was located. If you add a hash, the entity will not contain this information. **Example:** *c:\user\windows\XXX*
File size	How much space the file takes up in storage, in MB. If you add a hash, the entity will not contain this information. **Example:** *1.7 MB*
MD5	MD5 hash value. **Example:** *b1d64dfbc73158114f20dee14b994755*
SHA1	SHA1 hash value. **Example:** *aed420a76e730364ca8d804873a7f3c6ca2ff4f4*
SHA256	SHA256 hash value.

	Example: *ee424b6d4657808c1c634fcaa7fc52e2ec9f30b1cb8ed457178559d5f840b40b*
SHA512	SHA512 hash value. **Example**: *20a5ab43c7106846e4954adec2c2c1348d157beb686fbbb0f23a5efcf89cb49c4ab6c6c369869e05da7661d1386b5f439dfad9e6d60b11cac599be83b0146200*
Source	Link to the file asset's Advanced Analytics notable session timeline. If you manually uploaded the file, there is no link.

5.2. Device Entity Data

Every entity type contains a unique set of data. The device entity contains data about the device's host, IP address, top user, and more. In Incident Responder, you can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

Alerts	Number of third-party security alerts this device has triggered. **Example:** *2*
City	City the device last connected from. **Example:** *San Francisco*
Country	Country the device last connected from. **Example:** *United States*
Data insights	Link to the device's Data Insights page in Advanced Analytics.
Entity frequency	Number of incidents that contain this entity. Click to view a list of all these incidents. **Example:** *2*
First seen	Date Advanced Analytics first detected the device in the network. **Example:** *1 Apr 2018*
IP	IP address assigned to the device. **Example:** *10.78.121.42*

Last seen	Date of the most recent sequence that involved this device. **Example:** *4 May 2018*
Risk score	The device's Advanced Analytics risk score at the time Case Manager created the incident. The risk score doesn't update as the notable session continues or when it closes. Click to return to the session and view the final risk score. **Example:** *299*
Source	Link to the device asset's Advanced Analytics notable session timeline.
State	U.S. state the device last connected from. If the device connected from outside the U.S., the artifact will not contain this information. **Example:** *California*
Top user	Full name of the Advanced Analytics user that logs into this device most frequently. Click to view the user's profile in Advanced Analytics. **Example:** *Barbara Salazar*
Type	Operating system; Windows, Linux, or Mac.
URL	URL associated with the IP address. **Example:** *www.ddddd.com*
Watchlists	Number of watchlists the device appears on in the home page. **Example:** *2*
Zone	Internal network zone within your organization the device last connected from. This may be a city, business unit, building, or room. **Example:** *Atlanta office*

5.3. User Entity Data

Every entity type contains a unique set of data. The user entity type contains data about the user's employment, contact information, manager, and more. In Incident Responder, you can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

Account ID	Corporate directory account ID, typically corresponds to a set of login credentials.

	Example: *bsalazar*
Alerts	Number of third-party security alerts this user has triggered. **Example:** *3*
Data insights	Link to the user's Data Insights page in Advanced Analytics.
Employee type	Type of employee, as defined in the Advanced Analytics user_employee_type context table; for example, full-time, part-time, or contractor. **Example:** *full-time*
Entity frequency	Number of incidents that contain this entity. Click to view a list of all these incidents. **Example:** *2*
First seen	Date when Exabeam first detected the the user in the IT environment. **Example:** *1 April 2018*
Full name	First name and last name. Click to navigate to the user's profile in Advanced Analytics. **Example:** *Barbara Salazar*
Last seen	Date the user last logged in to a device or network; the user's most recent Advanced Analytics login event. **Example:** *4 May 2018*
Manager cell phone	Manager's personal cell phone number. **Example:** *212-408-5108*
Manager email	Manager's work email address. Click to start writing an incident email to the manager. **Example:** *tu.peterson@example.com*
Manager name	Full name of the user's manager. Click to navigate to the manager's user profile in Advanced Analytics. **Example:** *Tu Peterson*
Manager office phone	Phone number the manager uses at their office location. **Example:** *494-512-5019*

Manager title	Manager's job title. **Example:** *VP of Human Resources*
Photo	User's display picture in Advanced Analytics.
Risk score	The device's Advanced Analytics risk score at the time Case Manager created the incident. The risk score doesn't update as the notable session continues or when it closes. Click to return to the session and view the final risk score. **Example:** *299*
Source	Link to the user's Advanced Analytics notable session timeline.
Top device	Device the user logs into most frequently. **Example:** *srv_143lm_us*
User cell phone	A private cell phone number. **Example:** *274-557-3374*
User department	Corporate department the user works in. **Example:** *HR*
User email	User's work email address. Click to start writing an incident email to the user. **Example:** *barbara.salazar@example.com*
User office phone	Phone number they use at their office location. **Example:** *212-408-8076*
User title	User's job title. **Example:** *Human Resources Coordinator*
Username	Username in Advanced Analytics. **Example:** *Barb S.*
Watchlist	Number of watchlists the user appears on in the home page. **Example:** *2*
Zone	Internal network zone within your organization the user last connected from. This may be a city, business unit, building, or room.

Example: *Chicago*

6. Artifact Types

When you add an artifact to an incident, they fall under five types. Each type contains its own unique set of data, which you can input to action nodes in Incident Responder playbooks.

Email Address – An email address observed on an email client or server.

File - A file observed on a device. It may or may not have a payload. You may retrieve the file, but not download, display, or execute it because it may be malicious.

IP - An IP address in IPv4 or IPv6 format.

Process - A process executed by a program observed on an operating system.

URL – A URL associated with an IP address.

6.1. Email Address Artifact Data

Every artifact type contains a unique set of data. The email address artifact contains data about the email address's role, threat status, and more. In Incident Responder, you can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

Artifact frequency	Number of open incidents that contain this artifact. Click to view a list of these incidents. **Example:** *2*
Email address	Email address the artifact describes. **Example:** *alerts@microsft.com*
Related entity	The entity this artifact is related to. **Example:** *fweber*
Role	Whether the email is a victim, was attacked, or unknown.
Source	Link to the email asset's Advanced Analytics notable session timeline.
Threat status	Whether the email is a malicious, benign, or unknown threat, or a false positive.

6.2. File Artifact Data

Every artifact type contains a unique set of data. The email artifact contains data about the file's path, size, hash, and more. In Incident Responder, you can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

Artifact frequency	Number of open incidents that contain this artifact. Click to view a list of these incidents. **Example:** *2*
File created time	Date and time this file was created. **Example:** *2019-05-06 15:56*
File name	Name used to uniquely identify the file in the file system. **Example:** *barbarian.jar*
File path	Where in the file system the file was located. If you add a hash, the artifact will not contain this information. **Example:** *c:\user\windows\XXX*
File size	How much space the file takes up in storage, in MB. If you add a hash, the artifact will not contain this information. **Example:** *1.7 MB*
MD5	MD5 hash value. **Example:** *b1d64dfbc73158114f20dee14b994755*
Role	Whether the file is a victim, was attacked, or unknown.
SHA1	SHA1 hash value. **Example:** *aed420a76e730364ca8d804873a7f3c6ca2ff4f4*
SHA256	SHA256 hash value. **Example:** *ee424b6d4657808c1c634fcaa7fc52e2ec9f30b1cb8ed457178559d5f840b40b*
SHA512	SHA512 hash value. **Example**: *20a5ab43c7106846e4954adec2c2c1348d157beb686fbbb0f23a5efcf89cb49c4ab6c6c369869e05da7661d1386b5f439dfad9e6d60b11cac599be83b0146200*

Source	Link to the file asset's Advanced Analytics notable session time. If you manually uploaded the file, there is no link.
Threat status	Whether the file is a malicious, benign, or unknown threat, or a false positive.

6.3. IP Artifact Data

Every artifact type contains a unique set of data. The IP artifact contains data about the IP's geolocation, role, threat status, and more. In Incident Responder, you can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

Artifact frequency	Number of open incidents that contain this artifact. Click to view a list of these incidents. **Example:** *2*
City	City this IP address last connected from. **Example:** *San Francisco*
Country	Country this IP address last connected from. **Example:** *United States*
IP	IP address the artifact describes. **Example:** *8.8.8.8*
Related entity	The entity this artifact is related to. **Example:** *fweber*
Role	Whether the IP address is a victim, was attacked, or unknown.
Source	Link to the IP asset's Advanced Analytics notable session timeline.
State	U.S. state this IP address last connected from. If the IP address connected from outside the U.S., the artifact doesn't contain this information. **Example:** *California*
Threat status	Whether the IP address is malicious, benign, or unknown threat.

6.4. Process Artifact Data

Every artifact type contains a unique set of data. The process artifact contains data about the process's run time, ID, parent process, and more. In Incident Responder, you can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

Artifact frequency	Number of open incidents that contain this artifact. Click to view a list of these incidents. **Example:** *2*
End time	Date and time the process stopped running. **Example:** *2019-05-06 18:56*
Parent PID	Parent process ID. **Example:** *2130*
Parent process name	Program filename of the parent process. **Example:** *explorer.exe*
Process ID	ID of the process the artifact describes. **Example:** *4109*
Process name	File name of the program that executed the process. **Example**: a.exe
Process path	Where in the file system the program file was located. **Example**: *C:\Users\Developer\Exabeam\Test\...*
Process UID	Process's user ID, available in Unix-like operating systems. **Example:** *39569*
Related entity	The entity this artifact is related to. **Example:** *fweber*
Role	Whether the process is a victim, was attacked, or unknown.
Source	Link to the process asset's Advanced Analytics notable session timeline.

Start time	Date and time the process started running. **Example:** *2019-05-06 15:56*
Threat status	Whether the process is a malicious, benign, or unknown threat, or a false positive.

6.5. URL Artifact Data

Every artifact type contains a unique set of data. The URL artifact type contains data about the URL geolocation, IP, and more. You can input this data to a playbook action node.

When you click on a link that redirects you from Case Manager to Advanced Analytics, you must have View Unmasked Data (PII) privileges to view the data in Advanced Analytics if you've turned on data masking in Advanced Analytics settings.

Artifact frequency	Number of open incidents that contain this artifact. Click to view a list of these incidents. **Example:** *2*
City	City this URL was last accessed from. **Example:** *San Francisco*
Country	Country this URL was last accessed from. **Example:** United States
IP	URL's corresponding IP address. **Example:** *8.8.8.8*
Related entity	The entity this artifact is related to. **Example:** *fweber*
Role	Whether the URL is a victim, was attacked, or unknown.
Source	Link to the URL asset's Advanced Analytics notable session timeline.
State	U.S. state this URL was last accessed from. If the URL was accessed outside the U.S., the entity doesn't contain this information. **Example:** *California*
Threat status	Whether the URL is a malicious, benign, or unknown threat, or a false positive.
URL	URL the artifact describes.

Example: *https://www.exabeam.com*

7. Add Advanced Analytics Evidence to a Case Manager Incident

If an Advanced Analytics-generated incident doesn't include all the entities or artifacts you need, add them to the incident directly from Advanced Analytics.

When an Advanced Analytics user or asset session crosses a configured risk threshold, Case Manager automatically creates an incident. By default, Advanced Analytics adds some evidence from notable events to the incident as entities or artifacts. If it misses any entities and artifact you need, or if you discover more relevant entities or artifacts as you investigate the timeline, add these entities or artifacts to the incident directly from the notable session.

When you update an incident with the relevant entities and artifacts, you can use them in playbooks to effectively triage, investigate, and respond to incidents.

You can only add Advanced Analytics evidence to an existing incident. You can't create a new incident directly from a notable session.

1. Navigate to an Advanced Analytics asset or user Smart Timeline:
   - To navigate from a Case Manager incident: navigate to the incident, find the **Timeline Page** incident field, then select **Go to page**.
   - To navigate to an asset Smart Timeline in Advanced Analytics: On the **HOME** page, find the **NOTABLE ASSETS** watchlist or other watchlist you created, then select an asset's risk score. Or, from a watchlist, select the asset's name, then under **RISK REASONS** click **GO TO TIMELINE**.
   - To navigate to a user Smart Timeline in Advanced Analytics: On the **HOME** page, find the **NOTABLE USERS**, **Account Lockouts**, **Executive Users**, or other watchlist you created, then select a user's risk score. Or, from a watchlist, select the user's name, then under **RISK REASONS** click **GO TO TIMELINE**.
   - Search for a user or asset, select from the results, then under **RISK REASONS** click **GO TO TIMELINE**.
2. Select an event in the Smart Timeline. The event expands to review further details.
3. Click the More ⋮ menu, then click **Add to Incident**.
4. Select a Case Manager incident from your list of most recent assigned incidents, or to search for a specific incident, start typing. If you navigated directly from a Case Manager incident, this field is automatically populated.
5. Select the entities and/or artifacts. To create all the entities or artifacts, select the first checkbox.
6. Select **ADD TO INCIDENT**.

8. Send Messages from an Incident

Send messages, collaborate, and track information right from within an incident.

From an incident's details, under the **Messages** tab, send messages and securely distribute information about an incident to your team members or those outside your SOC.

There are two types of messages:

1. **Case Notes** - Comments added directly to and contained within an incident. Case Notes are enabled by default.
2. **Incident Emails** - Messages to those in your organization who can't access Case Manager or are external to your SOC. You send, receive, and track emails directly from an incident. You can add an email attachment to an incident as an artifact.

You can sort, filter, and restrict views to both types of messages.

8.1. Case Notes

Add findings or data to your investigation and communicate with people from directly within an incident using case notes.

A case note is free-form text you use to add descriptions, observations, and artifacts to your incident. Use case notes when your findings or data points are relevant to your investigation but do not fit in the generic incident fields and categories, or Case Manager can't measure or filter them.

Case notes are one way you message people directly from an incident. You can view an incident's case notes if you can access Case Manager and the incident. To collaborate with people who can't access Case Manager and still track the conversation within the incident, send an email.

8.1.1. ADD A CASE NOTE TO AN INCIDENT

Add descriptions, observations, and artifacts to your incident using case notes.

1. On the **INCIDENTS** page, select an incident.
2. On the **Messages** tab, click **NEW CASE NOTE**.
3. Enter the case findings, like descriptions, observations, and artifacts.
4. Click **ADD CASE NOTE**.

8.2. Incident Emails

To collaborate with people who can't access Case Manager, send an email directly from an incident.

Email people who can't access Case Manager, like non-SOC staff in your organization, to exchange questions, instructions, and feedback about an investigation.

Case Manager transports emails using your organization's email servers. Your email server or service policies may restrict your email size and who you can send emails to.

8.2.1. SEND AN EMAIL FROM AN INCIDENT

Send emails directly from an incident to communicate with people who can't access Case Manager.

1. From the navigation bar, click **INCIDENTS**, then select an incident.
2. On the **Messages** tab, click **NEW EMAIL MESSAGE**.
3. Compose the email and attach evidence.
4. Click **SEND**.

8.2.2. SEND ATTACHMENTS WITH YOUR INCIDENT EMAIL

To add evidence to an incident, send and receive attachments directly from an incident. When you receive an attachment, safely preview it, view attribute details, and download it.

Your internal mailbox and email policies may limit and restrict the attachments, like size and file type.

1. In the navigation bar, click **INCIDENTS**, select an incident, then select the **Messages** tab.
2. Create a new email, then click **INSERT ATTACHMENT**. The attachment appears as an icon in the email body.
3. Click **SEND**. The attachment is added to the incident.
   After 60 days, the attachment is purged, but the email text is not. To add the attachment to the incident indefinitely so you can run actions and playbooks on it, convert it into an artifact.

8.2.3. CONVERT AN EMAIL ATTACHMENT TO AN ARTIFACT

When you receive an email attachment, convert it to an artifact to investigate it further.

1. On the **INCIDENTS** page, select an incident, then select the **Messages** tab.
2. Ensure that the artifact doesn't already exist. You may duplicate an existing artifact you've already created.
3. Find the email that contains the attachment.
4. On the attachment, click the More ⋮ menu, then select **Add to Artifacts List**.

8.2.4. DOWNLOAD AN EMAIL ATTACHMENT

Download an attachment you received in an incident email.

1. On the **INCIDENTS** page, select an incident, then select the **Messages** tab.
2. Find the email that contains the attachment.
3. On the attachment, click the More ⋮ menu, then select **Download**.