exabeam

Respond to Security Incidents

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.

Table of Contents

1. Turnkey Playbooks

Fully pre-configured turnkey playbooks are ready to run out of the box.

Turnkey playbooks are pre-configured playbooks that are ready for you to run, without having to purchase additional services to get the actions you need.

They are listed along other playbooks you created on the **PLAYBOOKS** page. Like a playbook you created yourself, you can run them manually or automatically with a playbook trigger.

These playbooks leverage an in-house service, Exabeam Actions, that is available out-of-the-box and free to use. The service supports basic actions, including:

- Get Domain Reputation
- Get URL Reputation
- Get Email Reputation
- Get IP Reputation
- Get File Reputation

To customize a turnkey playbook, you can also use it as a template.

1.1. Threat Intelligence Reputation Lookup Turnkey Playbook

Learn about the Threat Intelligence Reputation Lookup turnkey playbook and how it works.

The Threat Intelligence Reputation Lookup turnkey playbook helps you analyze and triage suspicious emails, like potential spam and phishing emails. It changes a Case Manager incident's priority based on the reputation of an email entity and its artifacts.

First, the playbook assesses the reputation of the incident's entities and artifacts, including:

- Files attached to the email
- IP addresses
- Domains of any URLs in the email body
- Domain of the sender's email address

If the playbook finds any IP addresses with a malicious reputation, it searches for other incidents that has the same IP address entity or artifact. View the output in the incident's workbench.

If any entity or artifact has a malicious reputation, the playbook escalates the incident's priority to critical. If none of the artifacts have a malicious reputation, the playbook de-escalates the incident's priority to low.

2. Create a Playbook

Create a playbook to automate your workflow, and respond more quickly and efficiently to attacks.

1. Ensure you're familiar with the logic of compound, relational, and conditional operators.
2. Navigate to the **PLAYBOOKS** page.
3. Click **Add a new playbook** .
4. Enter information about the playbook:
   - **Playbook template** – Choose a template from the list. To create an empty playbook, select **New Playbook**.
   - **Name** – Give your playbook a unique name.
   - **(Optional) Description** – Describe your playbook, what it does, and when it should be used.
5. Click **Create**. The playbook contains a start node and end node. If you selected a template, the playbook contains other nodes based on the template.
6. Define the logic of your playbook: add a node, and configure action, decision, or filter nodes. As you design your playbook, keep in mind:
   - All nodes must be linked in some way to the start and end node; otherwise, you can't run the playbook.
   - You can only use the output from the previous node as an input for the next node.
   - You can use the output of one node in another only if the latter node takes in data of the same type. For example, if one node outputs a list of URLs, you can't link it to a node that takes in a list of IP addresses.
   - You must configure all necessary input fields for a given node. If you haven't configured one or more necessary fields, the node is outlined in red.
7. Click **Save** . You may save your playbook at any time, but if it contains an error, it won't run and is disabled by default. Your playbook appears in the list on the **PLAYBOOKS** page.

2.1. Add a Node

When you create or edit a playbook, add nodes to define or change its logic.

1. Click on the outbound port of the existing node you are connecting to the new node.
2. Click anywhere in the interface.
3. To add an action node, select **ACTION**. To add a decision node, select **DECISION**. To add a filter node, select **FILTER**.

2.2. Add an Action Node

When you create a playbook, you add action, decision, and filter nodes. Add an action node to call and use the results from a service.

1. From a node, add another node, then select **ACTION**.
2. Select a **Service**. These services are available for you to use; they either come out-of-the-box or have been configured by your organization. You might find the descriptions helpful in choosing the appropriate service to use.
3. Select the action type the node performs.
4. Select an input source. You can select between the fields, entities, or artifacts in the incident or the output from a previous node.
5. To close the panel, click anywhere in the interface. If there is a red border around the node, you have not configured one or more necessary fields.

2.3. Add a Decision Node

When you create a playbook, you create action, decision, and filter nodes. Create a decision node to make a boolean (if/else) decision.

A decision node evaluates whether the input is true or false. Based on this evaluation, the next node in the playbook executes an action.

1. From the node you wish to make a decision on, add a node and select **DECISION**. If you add the node straight from the start node, it operates on all the fields and raw data in the incident.
2. Select an input source. You can select between the fields, entities, or artifacts in the incident or the output from a previous node.
3. Select an operator:
   - **Equals** – Checks if values are equal.
   - **Not Equal To** – Checks if values are not equal.
   - **Contains** – Checks if values partially match.
   - **Not Contains** – Checks if values do not match.
   - **Is Empty** – Checks if incident field doesn't have an assigned value.
   - **Exists** – Checks if incident field has an assigned value.
   - **Starts With** – Checks if string data type starts with a specified value.
   - **Not Starts With** – Checks if string data type doesn't start with a specified value.
   - **Ends With** – Checks if string data type ends with a specified value.
   - **Not Ends With** – Checks if string value doesn't end with a specified value.
   - **In** – Checks if value is in a specified list.
   - **Not In** – Checks if value is not in a specified list.
   - **Matches** – Checks if values match exactly.
   - **Not Matches** – Checks if values don't match exactly.

- **Greater Than** – Checks if value is greater than a specified value.

4. (Optional) If relevant, enter or select a value.
5. Click **SAVE**.
6. (Optional) Add additional conditions to the decision node.
   - To add an *or* condition, select **+OR**.
   - To add an *and* condition, select **+AND**.
7. From the decision node's outbound ports, add a node that executes depending on how the input was evaluated:
   - To execute a node if the input is evaluated as true, add a node from the outbound port on the side.
   - To execute a node if the input is evaluated as false, add a node from the top or bottom outbound ports.
8. To close the panel, click anywhere in the interface. If there is a red border around the node, you have not configured one or more necessary fields.

2.4. Add a Filter Node

When you create a playbook, you add action, decision, and filter nodes. Add a filter node to narrow down multiple input values to a specific subset.

You use a filter node to filter out a subset of the input source, based on conditions you specify when you configure the node. The filter node outputs the remaining subset and passes it on to the next node. The next node only evaluates this remaining subset. For example, you can use a filter node to remove:

- Normal domains, so the next node evaluates malicious domains only.
- Allow listed URLs, so the next node evaluates block listed URLs only.
- Email attachments with a risk score below 90, so the next node evaluates attachments with a risk score above 90 only.
- IP addresses from other countries, so the next node evaluates IP addresses from a specific country only.

To evaluate a single value, add a decision node.

1. From one node, add another node, then select **FILTER**.
2. Select an input source. You can select between the fields, entities, or artifacts in the incident or the output from a previous node.
3. Select an operator:
   - **Equals** – Checks if values are equal.
   - **Not Equal To** – Checks if values are not equal.

- **Contains** – Checks if values partially match.
- **Not Contains** – Checks if values do not match.
- **Is Empty** – Checks if incident field doesn't have an assigned value.
- **Exists** – Checks if incident field has an assigned value.
- **Starts With** – Checks if string data type starts with a specified value.
- **Not Starts With** – Checks if string data type doesn't start with a specified value.
- **Ends With** – Checks if string data type ends with a specified value.
- **Not Ends With** – Checks if string value doesn't end with a specified value.
- **In** – Checks if value is in a specified list.
- **Not In** – Checks if value is not in a specified list.
- **Matches** – Checks if values match exactly.
- **Not Matches** – Checks if values don't match exactly.
- **Greater Than** – Checks if value is greater than a specified value.

4. (Optional) If relevant, enter or select a value.
5. Click **SAVE**.
6. (Optional) Add an additional condition to the filter node. You can't use both in one filter node; you must choose one or the other.
   - To add an *or* condition, select **+OR**.
   - To add an *and* condition, select **+AND**.
   - To change a condition from one to the other, select the down arrow next to it, then select the appropriate condition.
7. To close the panel, click anywhere in the interface. If there is a red border around the node, you have not configured one or more necessary fields.

3. Playbook Templates

If you don't want to create a playbook from scratch, use a template. These templates come out-of-the-box or you can import your own from an existing playbook.

Playbook templates are frameworks that are already designed and ready for you to use; you just indicate the service you want to use.

There are 16 templates available out of the box, including ones for malware and phishing. You can also use turnkey playbooks as templates.

You can't delete these out-of-the-box templates.

To modify a template, export an existing playbook, then import it back into the system as a template. You can also create a new playbook from scratch.

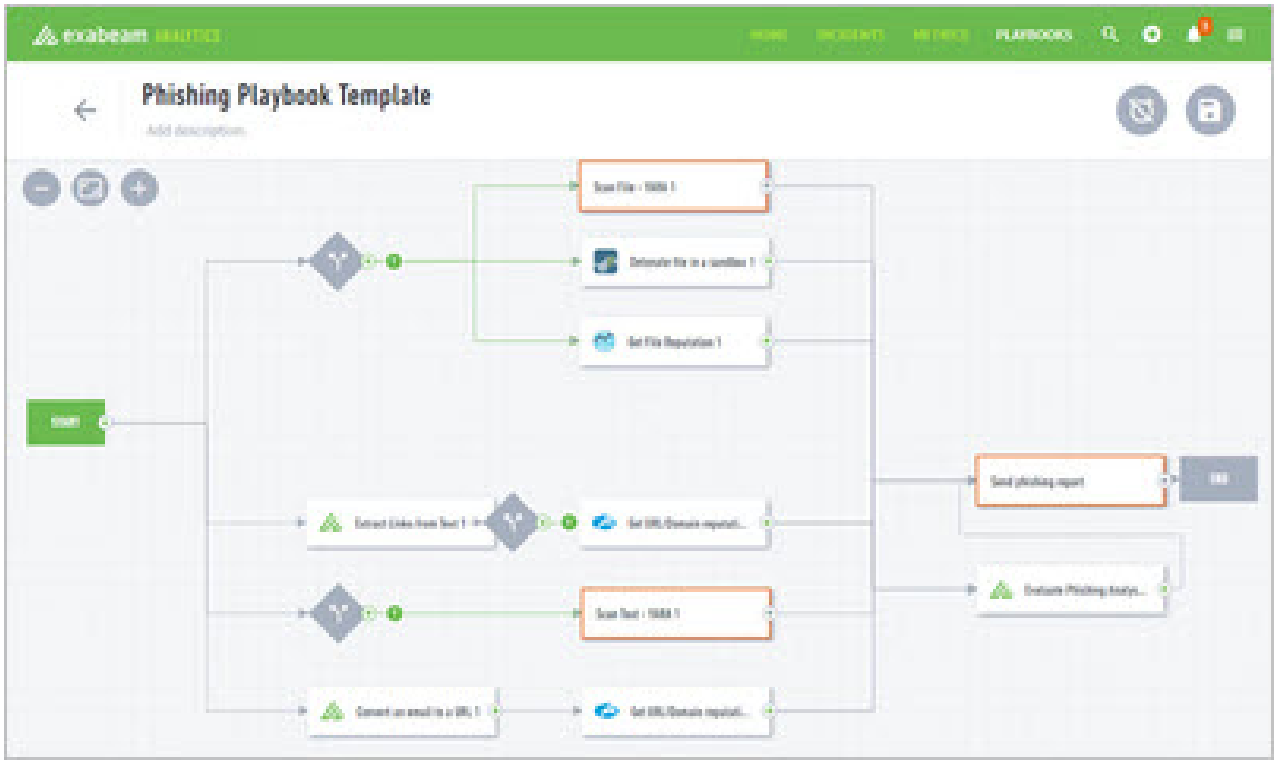
3.1. Import a Playbook Template

When you export a playbook, import it back into the system or another system as a template. It can only import as a template, not a playbook.

1. Ensure that your template file is in a valid JSON format. If you created and exported the playbook from Incident Responder, it is already in a valid format.
2. In the navigation bar, click **PLAYBOOKS**.
3. Click **Import template**  .
4. Click **CHOOSE TEMPLATE FILE**, then select a valid JSON file to upload.
   The playbook is imported as a template. To use the playbook, create a new playbook using the template.

3.2. Phishing Playbook Template

Break down the logic flow of the out-of-the-box phishing playbook template.



Phishing emails imitate reputable senders to fool recipients into installing malicious software or revealing personal information.

The phishing playbook sources emails into Case Manager. It checks the reputation of the domain that sent the email; extracts any files, URLs, or links; and checks the reputation of these entities. Then, the playbook checks if the email recipient has any web activity related to the URL.

Based on the sender's email address, the playbook searches for other recipients. If it finds other recipients, the playbook alerts you.

4. Create a Playbook Trigger

For a playbook to run automatically, define which circumstances and conditions trigger the playbook. You define a playbook trigger from the **PLAYBOOKS** page, or when you create or edit a playbook.

If you manually create an incident, playbooks aren't triggered.

1. In the navigation bar, click **PLAYBOOKS**, or create or edit a playbook.
2. Click **Add trigger to playbook.**:
   - On the **PLAYBOOKS** page, select the clock for an existing playbook in the list.
   - If you're creating or editing a playbook, select the clock.
3. Click **+ Trigger**.
4. Select the situation that triggers the playbook:
   - **Incident Created** – When you create a new incident.
   - **Status Changed** – When you change the the state of an incident.
   - **Priority Changed** – When you change the priority of an incident.
5. To add a condition to the situation, select **+ Condition**. If the situation occurs and the condition is met, the playbook runs. These conditions are based on incident fields, default or custom.
6. (Optional) To add another condition, click **+ ADD**.
7. Click **SAVE**.

5. Manually Run an Action

Instead of automating an action using a playbook, run an action manually from an incident's workbench.

1. In the navigation bar, click **INCIDENTS**.
2. Select an incident, then select **View Workbench**.
3. Select **RUN ACTION**.
4. Select an action from the list and enter the relevant information.
5. Click **LAUNCH**.

   If the action runs successfully, it appears in the workbench **ACTIONS** tab with a ✓ check mark, and you see its output in the workbench.

6. Manually Run a Playbook

Instead of triggering a playbook with an event, run a playbook manually on an incident from its workbench.

1. In the navigation bar, click **INCIDENTS**
2. Select an incident, then select **View Workbench**.
3. Select **RUN PLAYBOOK**.
4. Select a playbook from the list.
5. Click **LAUNCH**.
   If the actions in your playbook run successfully, they appear in the workbench **ACTIONS** tab with a ✓ check mark, and you see their outputs in the workbench.
   If your playbook has finished running successfully, it appears in the workbench **PLAYBOOKS** tab with a ✓ check mark.