exabeam

Get Started With Incident Responder

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

Publication date April 6, 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

Table of Contents

1. Incident Responder

Incident Responder automates your repetitive and manual tasks, like looking up the reputation of an IP address. Respond quickly and efficiently to incidents using actions and playbooks.

Exabeam Incident Responder is a security orchestration, automation, and response (SOAR) solution that features playbooks and a visual editor. With Incident Responder, your SOC works more productively, makes less mistakes, and quickly resolves security incidents.

If you're an overburdened analyst, integrated services and automated workflows help you avoid repetitive tasks and switch between security tools.

If you're a SOC manager, Incident Responder helps you deal with a shortage of talent. You create and maintain playbooks using a simple drag-and-drop editor, no coding experience required. You can even use to teach junior analysts about your organization's best practices for common scenarios, like phishing and malware.

Incident Responder requires a separate license. To learn more, contact your technical account manager or watch product videos on the Exabeam Community.

2. Network Prerequisites for Deploying Incident Responder

Before you deploy Incident Responder, open ports and whitelist URLs.

2.1. Open Ports

NOTE
For IMAP and POP3, only open the ports that match the email server protocol you use.

From	To	Port	Protocol
User Network	Case Manager Node	22/TCP	SSH
Log Sources	Case Manager Node	9875/TCP/UDP	Syslog
Incident Responder Appliance	Internal Email Server	143/TCP	IMAP
Incident Responder Appliance	Internal Email Server	993/TCP	IMAPS
Incident Responder Appliance	Internal Email Server	25/TCP	SMTP
Incident Responder Appliance	Internal Email Server	587/TCP	SMTPS
Incident Responder Appliance	Internal Email Server	110/TCP	POP3
Incident Responder Appliance	Internal Email Server	995/TCP	Secure POP3
Incident Responder Appliance	External Internet	43/TPC	HTTP (whois)

2.2. Whitelist URLs

You must whitelist URLs to use some services and actions.

Service	URL	Actions
MaxMind	maxmind.com / geopip.maxmind.com	Geolocate IP
VirusTotal	virustotal.com	Get URL Reputation Get IP Reputation
IP-API	ip-api.com	Geolocate IP
GoogleSafe Browsing	googleapis.com safebrowsing.googleapis.com	Get URL Reputation Get IP Reputation
Microsoft Trace	https://reports.office365.com/ecp/reportingwebservice /reporting.svc/MessageTrace	Microsoft Outlook Message Track

3. Services

Integrate Incident Responder with a service to run actions and playbooks.

A service is a third-party product or vendor you integrate with Incident Responder to run actions and playbooks. This service is usually one your organization already uses, like Cisco Threatgrid or Palo Alto Networks Wildfire. Instead of leaving Incident Responder to use these services, integrate them so you access them in one location.

You configure each service differently. Once you configure a service, you can edit or disable it.

If you don't want to purchase additional services from third parties, you can use Exabeam's in-house service, Exabeam Actions. It is free to use and available out of the box. You can also upload a custom service. This custom service can be one you developed from scratch or one that customizes an out-of-the-box third-party service.

If you use a third-party service we don't yet support, contact your Sales Representative to request it.

3.1. Exabeam Actions Service

Get started using basic actions with the Exabeam Actions service.

Exabeam Actions is an in-house service that is free to use and available out-of-the-box. With the Exabeam Actions service, you can start using actions or playbooks, like turnkey playbooks, without purchasing additional services from third parties.

The service supports basic actions, including:

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

To assess the reputation of an entity, Exabeam Actions searches across various sources, like threat feeds and IP reputation lists, for evidence that the entity may be risky. Then, it compares the evidence against a set of conditions. Depending on which conditions the evidence matches, Exabeam Actions assigns the entity a severity level between 0 and 99. If the entity has a severity level of 50 and above, Exabeam Actions considers the entity to have a malicious reputation.

4. Exabeam Actions

Call a third-party service and gather data points manually or automatically using Exabeam actions.

An action is an API call to a service that gathers specific data points about an indicator of compromise (IOC) in an incident; for example, it can find the reputation of an . It is a Python script that you can edit or create on your own. You execute them manually, or automatically using a playbook. There are out-of-the-box actions, or you integrate Incident Responder with a service to run others.

5. Playbooks

Automate your tasks, immediately neutralize attacks, and mitigate damages with Incident Responder playbooks.

A playbook is a standard, repeatable sequence of actions that responds to specific incident types, like phishing or malware, based on your best practices. It automates your workflow and completes complex, manual, and repetitive tasks so you quickly identify and address incidents.

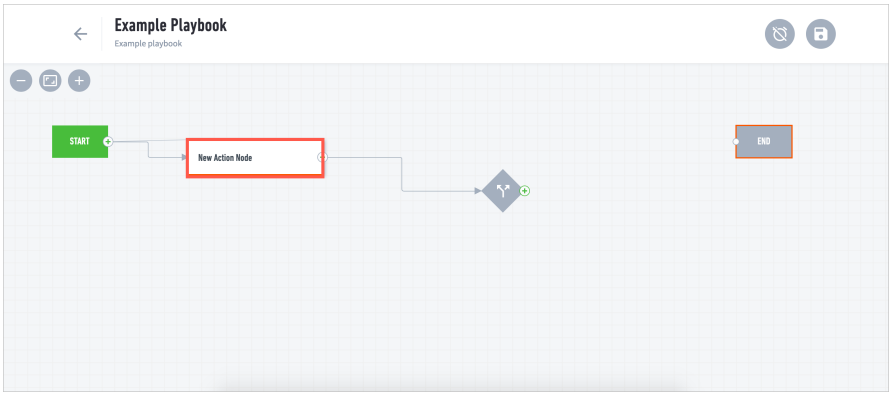
You design a logic flow that triggers the playbook under certain conditions. Then, the playbook automatically runs the relevant responses. You make workflows semi-automated so it runs at the push of a button, or fully automated so it runs without any human intervention.

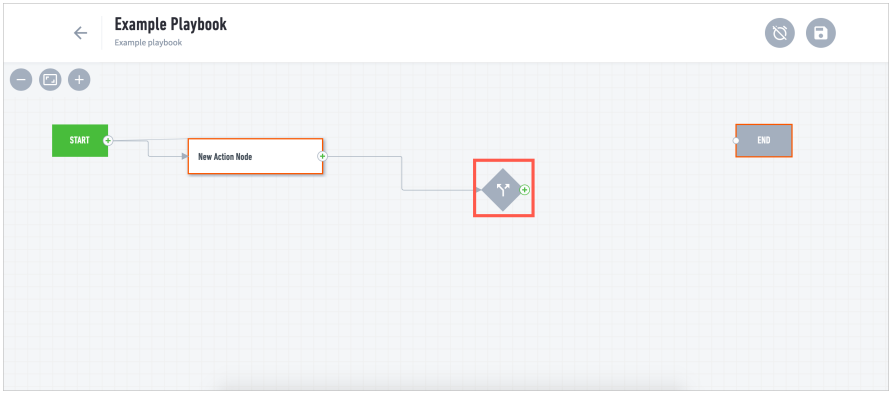
You manage a playbook and track its history in an incident's workbench.

You can create your own playbook from scratch, create a playbook from a per-designed template, or run a fully-configured turnkey playbook.

5.1. Playbook Terminology

Define all the terms you encounter when dealing with playbooks.

Action	A scripted task to call a third-party API service and gather data, executed manually or automatically using playbooks. For example: *retrieve the reputation information for a given URL* or *search emails by sender*. You use action nodes in playbooks. It has an inbound port on the left and an outbound on the right. 
Decision	A node that indicates a boolean (if/else) decision. It has one inbound node on the left, an if/true node on the right, and else/false nodes on the top and bottom.

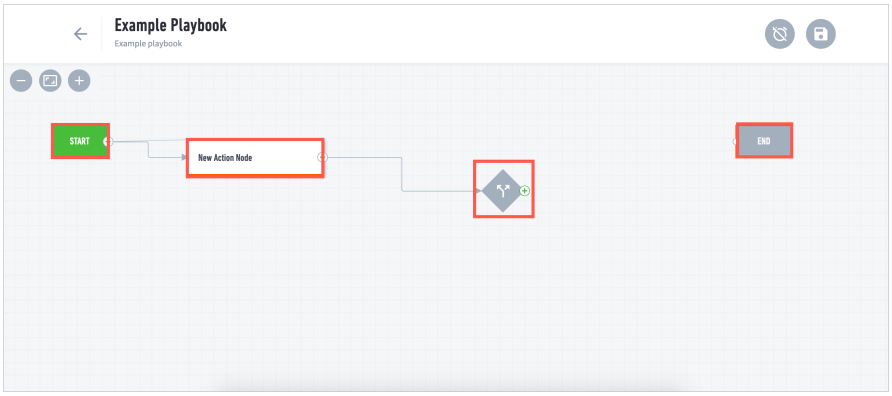


Input

Data passed from one node to another; data from a Case Manager incident, entity, or artifact.

Node

The fundamental building blocks of playbooks. Each one represents an action, decision, start, or end.

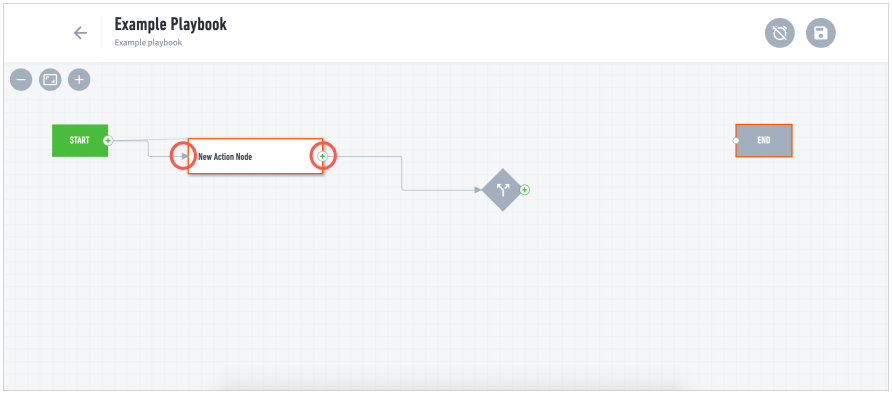


Operator

Compares operands and returns a logical value if the comparison is true. Operands may be numerical, string, logical, or object values. Strings are compared based on standard lexicographical ordering, using Unicode values.

Port

Each node has at least one inbound port and one outbound port that connects it to another node (except the start node and end node). An inbound port receives data from another note, and an outbound node sends data.



Service	A third-party product or vendor you integrate with Incident Responder to run actions and playbooks. For example: Cisco Threatgrid, Palo Alto Networks Wildfire. You interact with multiple instances of a service from within Incident Responder. Information about a service, like how to connect to it and which actions are defined, is stored in the Incident Responder server.

5.2. Playbook Triggers

Automatically run playbooks using triggers.

Playbooks run automatically if you prescribe it to run under a certain circumstance and that circumstance happens. This circumstance is called a trigger. There are three circumstances that trigger a 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.

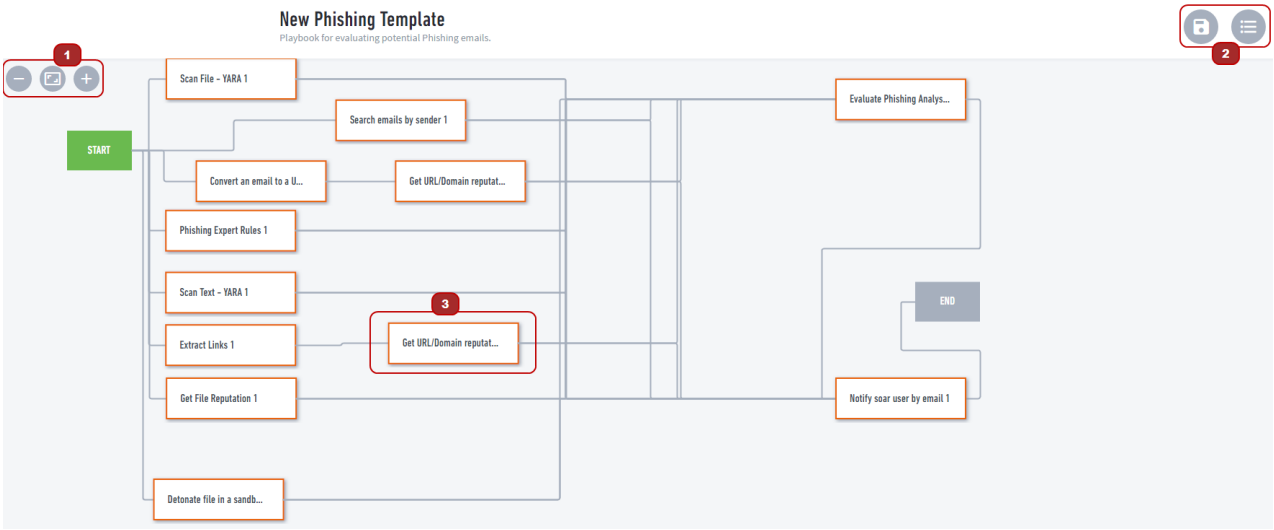
If you've already created an incident manually and the details match the conditions of a playbook trigger, the playbook will not trigger automatically.

6. Get to Know the Playbook Interface

Learn about the interface components you use to create and edit playbooks.

On the playbook interface, you and edit playbooks.

This is a new playbook created using the phishing template. Let's explore this playbook:



1 Control how you view the interface. Zoom in, out, or reset the view to the default.

2 Save your playbook and return to the **PLAYBOOKS** page. You can save your playbook even if it's incomplete, but if it contains any errors, it will not run.

3 A playbook is made of nodes. You connect each node to one or more other nodes. Each node has two or more ports, inbound and outbound. To view a node's ports, hover over the node.

Every playbook has a start node and end node that defines its logical boundaries—where the playbook starts and ends. You cannot change these two nodes.The start node has one outbound port; the end node has one inbound port.

To build the logic of your playbook, , and configure

If a node is outlined in red, it needs your attention. When you create a playbook using a template, all the nodes are initially outlined in red. You must click on the node and change how it's configured, or the playbook will not run.

7. Configure Incident Responder Settings

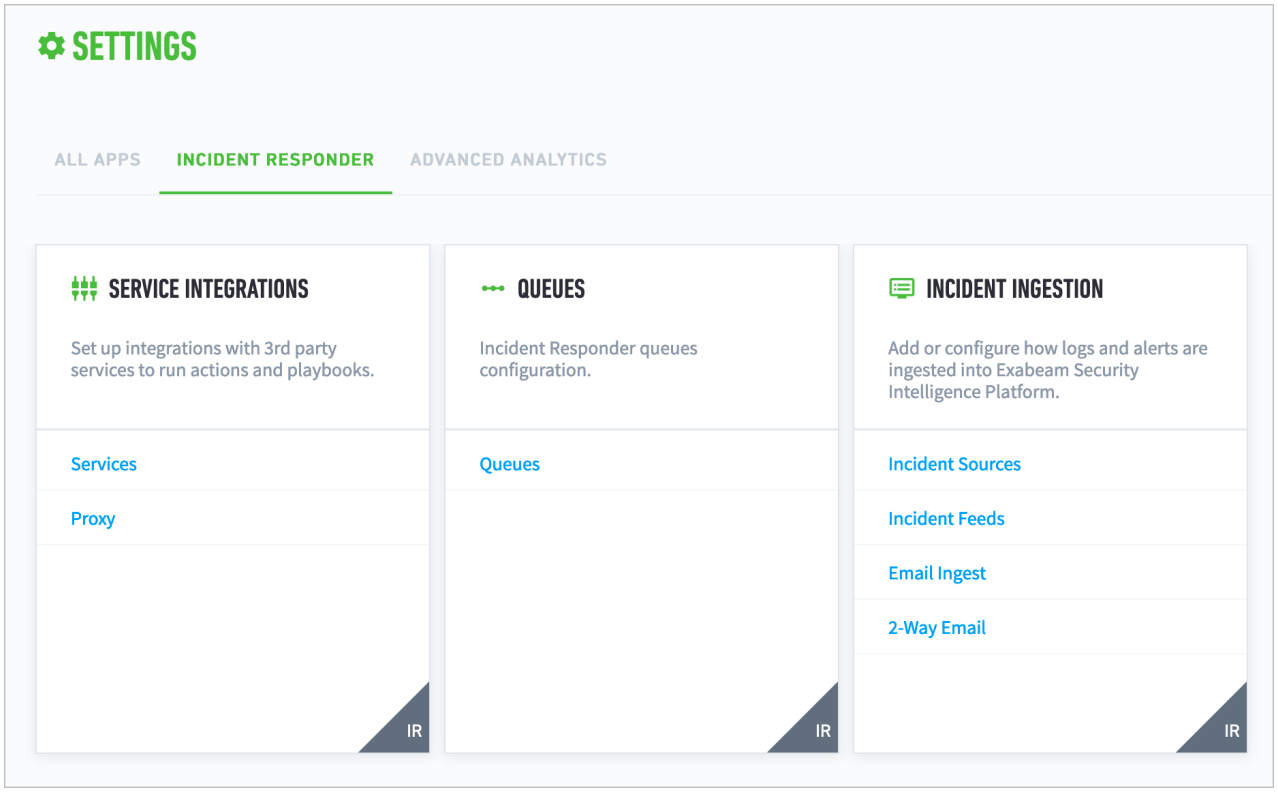
Integrate Incident Responder with services in Incident Responder settings.

In the navigation bar, click the menu , then select **Settings**. Depending on your permissions, select **Core** or **Analytics**:

- If you have Core *Manage Users and Context Sources* permissions, you can only access **Core** settings.
- If you have Advanced Analytics *All Admin Ops* permissions, you can access both **Core** and **Analytics** settings. In **Analytics** settings, you can configure and customize more settings than in **Core** settings.

7.1. Core Settings

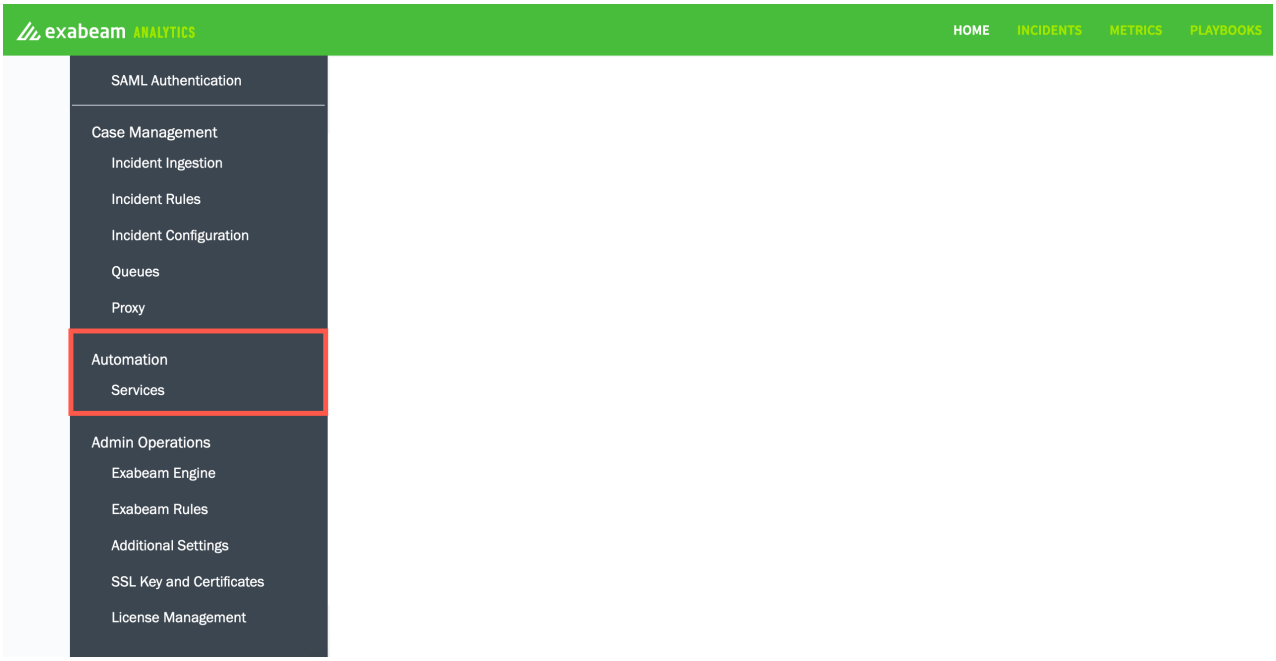
In **Core** settings, view all settings under **ALL APPS** or click the **INCIDENT RESPONDER** tab to view Case Manager and Incident Responder settings.



Under **SERVICE INTEGRATIONS**, select **Services** to configure a service, edit a service, disable a service, and upload or delete a custom service.

7.2. Analytics Settings

In the navigation bar, click the menu , select **Settings**, then navigate to **Automation**.



In **Services**, configure a service, edit a service, disable a service, and upload or delete a custom service.