Get Started With Incident Responder

Publication date August 19, 2020
# Table of Contents

1. Incident Responder ................................................................................................................. 3  
2. Network Prerequisites For Deploying Incident Responder ......................................................... 4  
   2.1. Open Ports .................................................................................................................... 4  
   2.2. Whitelist URLs ............................................................................................................. 4  
3. Exabeam Actions ..................................................................................................................... 5  
4. Playbooks ............................................................................................................................... 6  
   4.1. Playbook Terminology ................................................................................................. 6  
   4.2. Playbook Triggers ....................................................................................................... 8  
5. Services ................................................................................................................................... 9  
   5.1. Exabeam Actions Service ............................................................................................... 9
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 are an overburdened analyst, integrated services and automated workflows help you avoid repetitive tasks and switch between security tools.

If you are a SOC manager, Incident Responder helps you deal with talent shortage. You create and maintain playbooks using a simple drag-and-drop editor—you don’t need to know how to code. You can even use playbook templates 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

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

2.2. Whitelist URLs

You must whitelist URLs to use some services and actions.

<table>
<thead>
<tr>
<th>Service</th>
<th>URL</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxMind</td>
<td>maxmind.com / geopip.maxmind.com</td>
<td>Geolocate IP</td>
</tr>
<tr>
<td>VirusTotal</td>
<td>virustotal.com</td>
<td>Get URL Reputation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Get IP Reputation</td>
</tr>
<tr>
<td>IP-API</td>
<td>ip-api.com</td>
<td>Geolocate IP</td>
</tr>
<tr>
<td>GoogleSafe Browsing</td>
<td>googleapis.com</td>
<td>Get URL Reputation</td>
</tr>
<tr>
<td></td>
<td>safebrowsing.googleapis.com</td>
<td>Get IP Reputation</td>
</tr>
<tr>
<td>Microsoft Trace</td>
<td><a href="https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace">https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace</a></td>
<td>Microsoft Outlook Message Track</td>
</tr>
</tbody>
</table>
3. 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 IP address artifact. 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.
4. Playbooks

Automate your tasks, immediately neutralize attacks, and mitigate damages with Exabeam 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.

4.1. 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 node, 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.

4.2. Playbook Triggers

Automatically run playbooks using triggers.

Playbooks automatically run when 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 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.
5. 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 central environment.

You configure each service differently. Once you add a service, you can edit or delete 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 you’ve 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.

5.1. 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.