Cisco Secure Cloud Analytics

Attack Chain Guide
# Table of Contents

**Introduction** .............................................................................................................. 3  
**Overview** .................................................................................................................. 3  
  - How We Build Attack Chains .................................................................................. 3  
  - How We Prioritize and Rank Attack Chains .............................................................. 3  
**Reviewing Your Alert Settings** ................................................................................... 5  
  - Configuring Subnet Sensitivity Settings ................................................................ 5  
  - Configuring Alert Priority Settings .......................................................................... 7  
**Accessing the Attack Chains Page** ............................................................................ 9  
**Managing Attack Chains** .......................................................................................... 12  
  - Renaming an Attack Chain .................................................................................... 12  
  - Assigning an Attack Chain ..................................................................................... 13  
  - Closing an Attack Chain ......................................................................................... 14  
  - Opening an Attack Chain ....................................................................................... 16  
  - Posting an Attack Chain as an Incident ................................................................. 17  
**Contacting Support** .................................................................................................. 18  
**Change History** ......................................................................................................... 19
Introduction

Overview

This guide provides information about attack chains in Cisco Secure Cloud Analytics. By correlating alerts which could be part of a larger threat into an "attack chain," this feature reduces the time typically required when investigating individual alerts. The attack chains are ranked to help you prioritize your investigation.

How We Build Attack Chains

We use extracted alert meta data to determine what the alerts have in common, which we refer to as common indicators. Common indicators include devices, IP addresses, host names, and user names. We then follow the MITRE ATT&CK® framework to further identify the tactics, techniques, and procedures (TTPs) to model the sequencing of actions and threat behaviors which could be early indications of an attack.

Not all alerts will share common indicators. Alerts that don’t share common indicators should be analyzed on an individual basis.

How We Prioritize and Rank Attack Chains

The attack chain rankings allow you to prioritize which attack chains should be investigated right-away. Depending on assessed threat levels, each attack chain is assigned a severity ranking based on the following:

- MITRE ATT&CK tactics identified
- subnet sensitivity of the devices involved
- alert priority (Low/Medium/High) of the alerts in the attack chain
- number of alerts in the attack chain

Make sure to review your Subnet Sensitivity and Alert Priority settings for your unique environment. For more information, refer to Reviewing Your Alert Settings.
The ranking process is refined using the following:

- **Norm Alert Score**: This is a normalized score that’s calculated using the subnet sensitivity of the device identified in the alert along with the alert priority.

- **Norm Tactic Score**: This is a normalized score that’s calculated using the MITRE ATT&CK Tactic priorities of the alerts within the chain and the corresponding subnet sensitivity of the devices. This score examines the progression of the MITRE ATT&CK Tactics in the chain to evaluate the intention of an attack as it is moves across the different stages of a possible cyber kill chain.

Each attack chain is ranked as Low, Medium, or High, as follows.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW Yellow</td>
<td>An attack chain ranked as LOW poses the <em>least</em> potential risk to your environment in relation to the other attack chains. When there are multiple attack chains, prioritization is based on a combination of factors such as alert priorities, device and subnet sensitivity, and MITRE ATT&amp;CK Tactic priorities.</td>
</tr>
<tr>
<td>MEDIUM Orange</td>
<td>An attack chain ranked as MEDIUM poses a <em>moderate</em> risk to your environment in relation to the other attack chains. When there are multiple attack chains, prioritization is based on a combination of factors such as alert priorities, device and subnet sensitivity, and MITRE ATT&amp;CK Tactic priorities.</td>
</tr>
<tr>
<td>HIGH Red</td>
<td>An attack chain ranked as HIGH poses the <em>most</em> potential risk to your environment in relation to the other attack chains. When there are multiple attack chains, prioritization is based on a combination of factors such as alert priorities, device and subnet sensitivity, and MITRE ATT&amp;CK Tactic priorities.</td>
</tr>
</tbody>
</table>

Attack chains that are ranked as High are automatically posted to Cisco XDR or Cisco SecureX to expedite remediation (if you have Cisco XDR or SecureX installed).
Reviewing Your Alert Settings

The Subnet Sensitivity and Alert Priority settings affect the alerts that can become part of an attack chain. A subnet’s sensitivity influences the alerts that can be generated, and the alert priority influences the degree to which subnet traffic is monitored.

For information about how subnet sensitivity and alert priorities affect alerts, click the Subnet Sensitivity Matrix link on the Priorities page during the configuring process.

Configuring Subnet Sensitivity Settings

To configure the Subnet Sensitivity settings, do the following:

1. Select Monitor > Alerts.

2. Click Related Config Links on the Alerts page.

To view more details about how the alert is included within an attack chain, click the (Link) icon.
3. Select **Subnet Sensitivity** to configure the sensitivity of subnets for alert generation.

4. Select **Low**, **Normal**, or **High** in the **Sensitivity** field.

Alerts closed with **Merit AUTO_IGNORED** are not included in attack chains. Make sure to review whether to specify **Low** for an alert.
Configuring Alert Priority Settings

To configure the Alert Priorities settings, do the following:

1. Select Monitor > Alerts.

   ![Monitor Screen Screenshot](image1)

2. Click Related Config Links on the Alerts page.

   ![Alerts Page Screenshot](image2)

3. Select Alert Priorities to configure alert priority levels.

   ![Alert Priorities Screen Screenshot](image3)
4. On the Priorities page, select **Low**, **Normal**, or **High** in the **Priority** field.

Alerts closed with Merit **AUTO_IGNORED** are not included in attack chains. Make sure to review whether to specify **Low** for an alert.
Accessing the Attack Chains Page

The Attack Chains page displays attack chains, which are sorted by rank to provide a visual indication of those posing the highest risk to your environment.

To access the Attack Chains page, do the following:

1. From the Dashboard, select **Monitor > Attack Chains**.

   ![Dashboard Screenshot](image)

   The Attack Chains page displays, defaulting to **Open** in the **See by status** field. **Click Closed** to view attack chains that have been closed.

2. Click a column title to sort how you’d like the attack chains to display. The following table shows the description for each column:

<table>
<thead>
<tr>
<th>Column Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>name used to identify a specific attack chain</td>
</tr>
<tr>
<td>Total Alerts</td>
<td>total number of alerts in the attack chain</td>
</tr>
<tr>
<td>Rank</td>
<td><strong>Yellow</strong> = LOW, <strong>Orange</strong> = MEDIUM, or <strong>Red</strong> = HIGH</td>
</tr>
<tr>
<td>Tactic Chain Pattern</td>
<td>pattern sequence of the MITRE ATT&amp;CK tactics showing the behavior of the attack chain</td>
</tr>
</tbody>
</table>
### Column Title | Description
---|---
Last Active Time | last time an observation was updated for an alert in the attack chain
Created Time | time when the first alert in the attack chain was created

3. Click the (Right Arrow) icon located next to an Attack Chain ID to display additional information about the attack chain, including the common indicators, all sources involved, alert counts, devices and IPs involved, MITRE ATT&CK, and time range. To close the additional information display, click the (Down Arrow) icon.
4. Select an Attack Chain ID to view the details page for the specific attack chain.

![Attack Chain at a Glance](image)

The details page for the specific attack chain provides more details about the attack chain, including when the attack chain was created or updated, the status of the attack chain, and the totals for the number of:

- devices identified in the attack chain
- days the attack chain has been active
- alerts (highlighting any unique alerts in the attack chain
- MITRE ATT& CK tactics and techniques) in the attack chain

5. Select one of these tabs for more details:

- **Alert Timeline**: displays a summary view of the alerts within a timeline
- **Connection Graph**: presents a connected network graph of alerts and common indicators for better visualization
- **Alerts Breakdown**: provides more details about the alerts within the attack chain
- **Devices and Roles**: displays a summary view of all the internal devices in the chain and their corresponding roles
- **All Hosts and Endpoints**: provides a summary of all the hosts in the chain view of all hosts participating in the chain, detailing attributes (source, indicator), the count of associated alerts, and the count of MITRE ATT&CK tactics and techniques
Managing Attack Chains

An attack chain remains available for one year after the most recent alert activity. If an attack chain is automatically closed and then merged into a new attack chain, we retain the original attack chain for 90 days after the most recent alert activity.

After an attack chain is created, you can rename it, assign it to someone to resolve, close and open it, and post it to Cisco XDR or SecureX.

The following tasks help you manage attack chains:

- Renaming an Attack Chain
- Assigning an Attack Chain
- Closing an Attack Chain
- Opening an Attack Chain
- Posting an Attack Chain as an Incident

Renaming an Attack Chain

To rename an attack chain, do the following:

1. Select Monitor > Attack Chains to access the Attack Chains page.
2. From the Attack Chains page, select an Attack Chain ID to view the details page for the specific attack chain.
4. Type the new name of the attack chain.
5. Click Save.
Assigning an Attack Chain

To assign or reassign an attack chain, do the following:

1. Select Monitor > Attack Chains to access the Attack Chains page.
2. From the Attack Chains page, select an Attack Chain ID to view the details page for the specific attack chain.

4. Select a name from the Assign this attack chain to drop-down list.

   - Click the x next to the Assign this attack chain to: field to clear the current assignee. This removes the current assignee when you're not reassigning the attack chain.

5. Click Assign.

6. Review the Assignee field to confirm the attack chain was assigned or cleared successfully.
Closing an Attack Chain

When you close an attack chain, you can open it using the instructions in the Opening an Attack Chain section.

Attack chains with a High rank are posted to Cisco XDR or SecureX automatically if you have Cisco XDR or SecureX installed. Once the incident is closed in Cisco XDR or SecureX, the attack chain in SCA is automatically closed.

Make sure to open an attack chain before attempting to post to Cisco XDR or SecureX. If an attack chain is closed, it can't be posted to Cisco XDR or SecureX.

To close an attack chain, do the following:

1. Select Monitor > Attack Chains to access the Attack Chains page.
2. From the Attack Chains page, select an Attack Chain ID to view the details page for the specific attack chain.

The Close this Attack Chain dialog box displays.

4. Choose whether to close the attack chain with alerts or without, then click Submit.

When you choose to close the attack chain without its alerts, a message displays in the lower right confirming you've successfully closed the attack chain.
When you choose to close the attack chain with its alerts, the Close Alerts dialog box displays.

5. Click Yes or No to indicate whether the alerts were helpful to you.

6. Select whether to snooze alerts; and if so, for how long.

7. Click Submit.
   A message displays in the lower right confirming you've successfully closed the attack chain.

When you toggle to Closed on the Attack Chains page, only the attack chains you've closed are shown. If an attack chain was automatically closed or merged, it won't be displayed.
Opening an Attack Chain

Only the attack chains you’ve closed, not those which were automatically closed, are available to be opened.

Opening an attack chain does not affect the status of any alerts within the attack chain. To change the status of an alert, go to the Alerts page.

To open an attack chain, do the following:

1. Select Monitor > Attack Chains to access the Attack Chains page.
2. From the Attack Chains page, select an Attack Chain ID to view the details page for the specific attack chain.
3. Select More Actions > Open.

The Open Attack Chain dialog box displays.

4. Click Submit if you’d like to open the attack chain.
Posting an Attack Chain as an Incident

Attack chains that are ranked as High are automatically posted to Cisco XDR or SecureX if you have Cisco XDR or SecureX installed.

To post a Low or Medium ranked attack chain to Cisco XDR or SecureX, do the following:

1. Select **Monitor > Attack Chains** to access the Attack Chains page.
2. From the Attack Chains page, select an Attack Chain ID to view the details page for the specific attack chain.
3. Click the **Post as Incident** button.

4. Go to Cisco XDR or SecureX to confirm the attack chain has successfully posted.

   If you don't have Cisco XDR or SecureX installed, the **Post as Incident** button will be dimmed and unusable.
Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by email: [tac@cisco.com](mailto:tac@cisco.com)
- For phone support: 1-800-553-2447 (U.S.)
## Change History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Revision Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>July 31, 2023</td>
<td>Initial Version</td>
</tr>
<tr>
<td>1.1</td>
<td>September 26, 2023</td>
<td>Updated content related to Cisco XDR.</td>
</tr>
</tbody>
</table>
Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)