Cisco Secure Cloud Analytics

Attack Chain Guide

Table of Contents

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.

Rank	**Description**
LOW **Yellow**	An attack chain ranked as LOW poses the *least* 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&CK Tactic priorities.
MEDIUM **Orange**	An attack chain ranked as MEDIUM poses a *moderate* 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&CK Tactic priorities.
HIGH **Red**	An attack chain ranked as HIGH poses the *most* 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&CK Tactic priorities.

> ⓘ 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

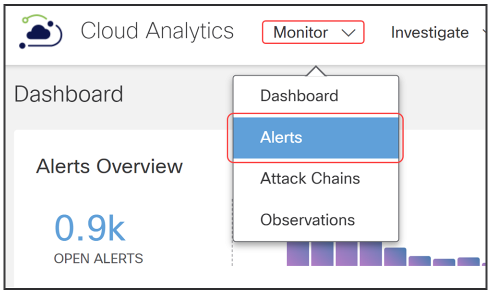
The Subnet Sensitivity and Alert Priority settings affect the alerts that can become part of an attack chain. A subnet's sensitivity influences the alerts that can be generated, and the alert priority influences the degree to which subnet traffic is monitored.

> 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.

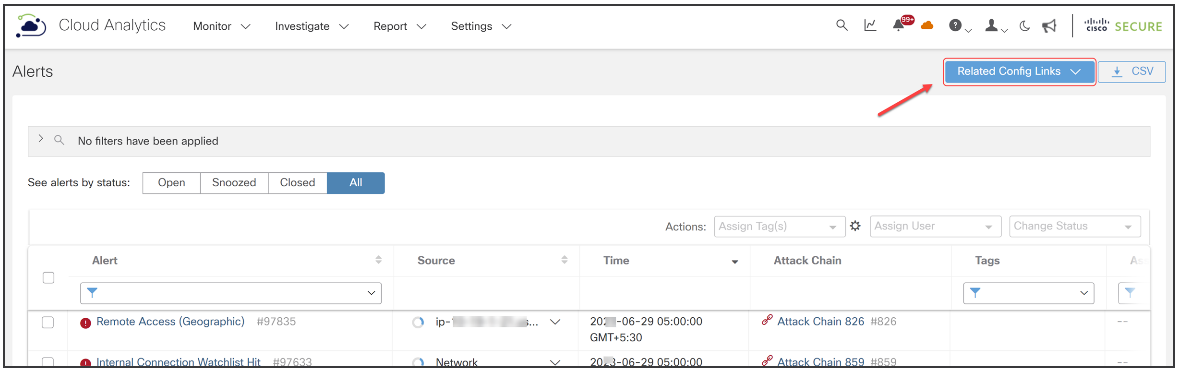
Configuring Subnet Sensitivity Settings

To configure the Subnet Sensitivity settings, do the following:

1. Select **Monitor** > **Alerts**.



2. Click **Related Config Links** on the Alerts page.



No filters have been applied

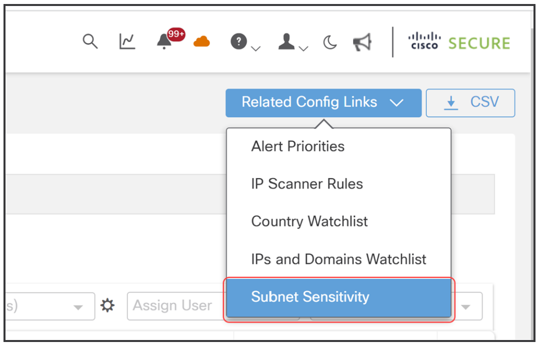
See alerts by status: Open | Snoozed | Closed | All

Actions:

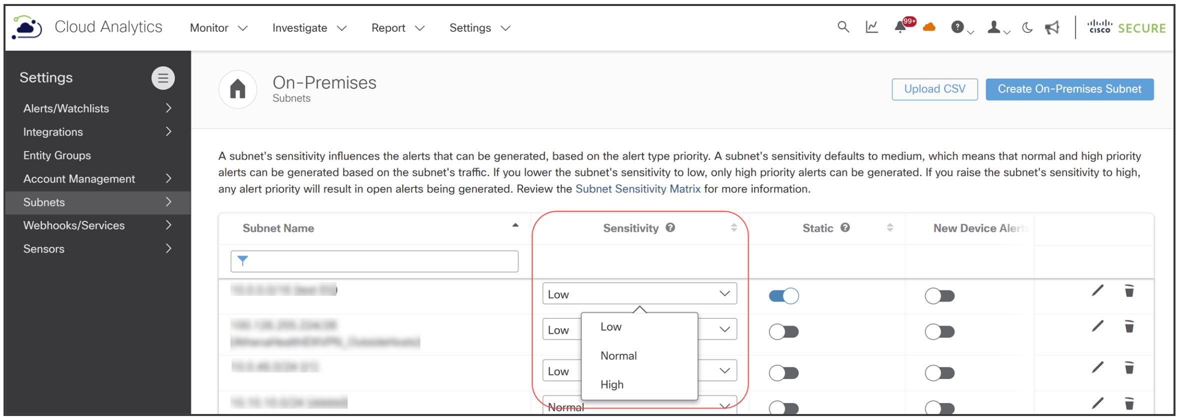
Alert	Source	Time	Attack Chain	Tags	As
Remote Access (Geographic) #97835	ip-[redacted]s...	20[redacted]-06-29 05:00:00 GMT+5:30	Attack Chain 826 #826		--
Internal Connection Watchlist Hit #97633	Network	20[redacted]3-06-29 05:00:00	Attack Chain 859 #859		--

> 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.



A subnet's sensitivity influences the alerts that can be generated, based on the alert type priority. A subnet's sensitivity defaults to medium, which means that normal and high priority alerts can be generated based on the subnet's traffic. If you lower the subnet's sensitivity to low, only high priority alerts can be generated. If you raise the subnet's sensitivity to high, any alert priority will result in open alerts being generated. Review the Subnet Sensitivity Matrix for more information.

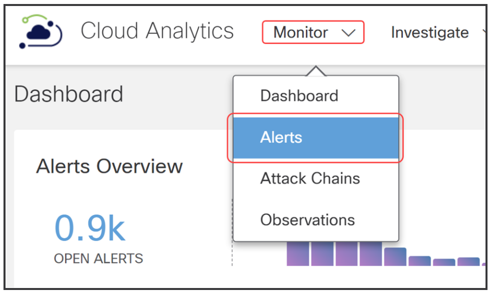
Subnet Name	Sensitivity	Static	New Device Alerts
[redacted]	Low	●	○
[redacted]	Low	○	○
[redacted]	Low	○	○
[redacted]	Normal	○	○

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

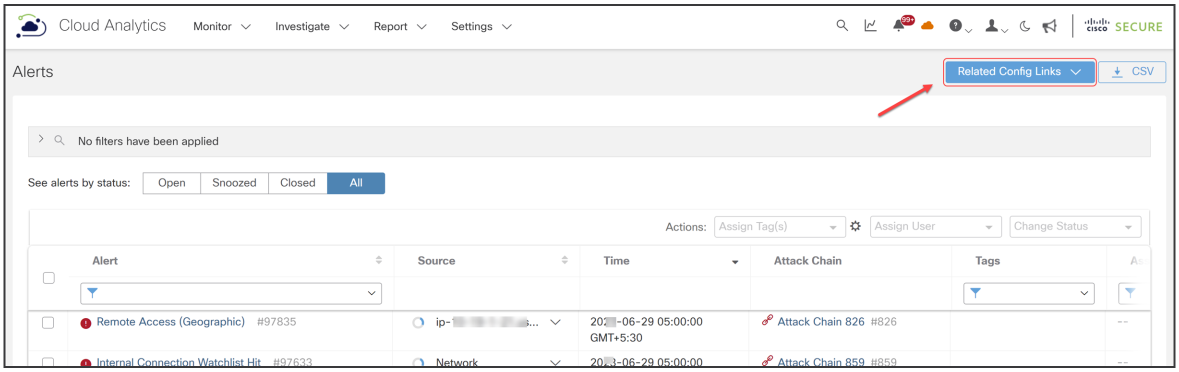
Configuring Alert Priority Settings

To configure the Alert Priorities settings, do the following:

1. Select **Monitor** > **Alerts**.

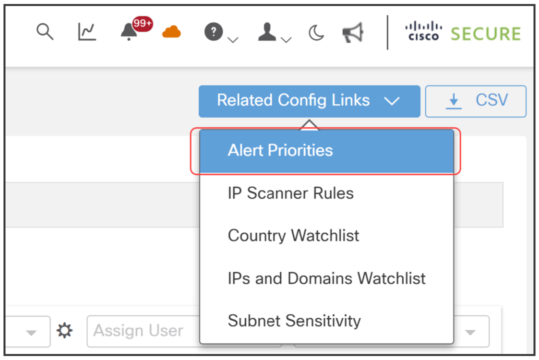


2. Click **Related Config Links** on the Alerts page.

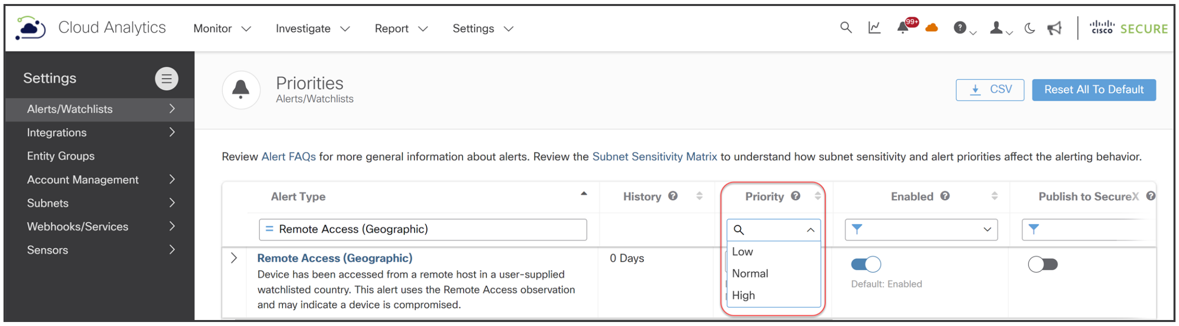


□	Alert	Source	Time	Attack Chain	Tags	As
□	Remote Access (Geographic) #97835	ip-[redacted]s...	20[redacted]-06-29 05:00:00 GMT+5:30	Attack Chain 826 #826		--
□	Internal Connection Watchlist Hit #97633	Network	20[redacted]3-06-29 05:00:00	Attack Chain 859 #859		--

3. Select **Alert Priorities** to configure alert priority levels.



4. On the Priorities page, select **Low**, **Normal**, or **High** in the **Priority** field.



Review Alert FAQs for more general information about alerts. Review the Subnet Sensitivity Matrix to understand how subnet sensitivity and alert priorities affect the alerting behavior.

Alert Type	History	Priority	Enabled	Publish to SecureX
= Remote Access (Geographic)				
Remote Access (Geographic) Device has been accessed from a remote host in a user-supplied watchlisted country. This alert uses the Remote Access observation and may indicate a device is compromised.	0 Days	Low Normal High	Default: Enabled	

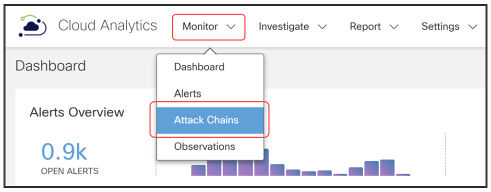
Alerts closed with `Merit AUTO_IGNORED` are not included in attack chains. Make sure to review whether to specify **Low** for an alert.

Accessing the Attack Chains Page

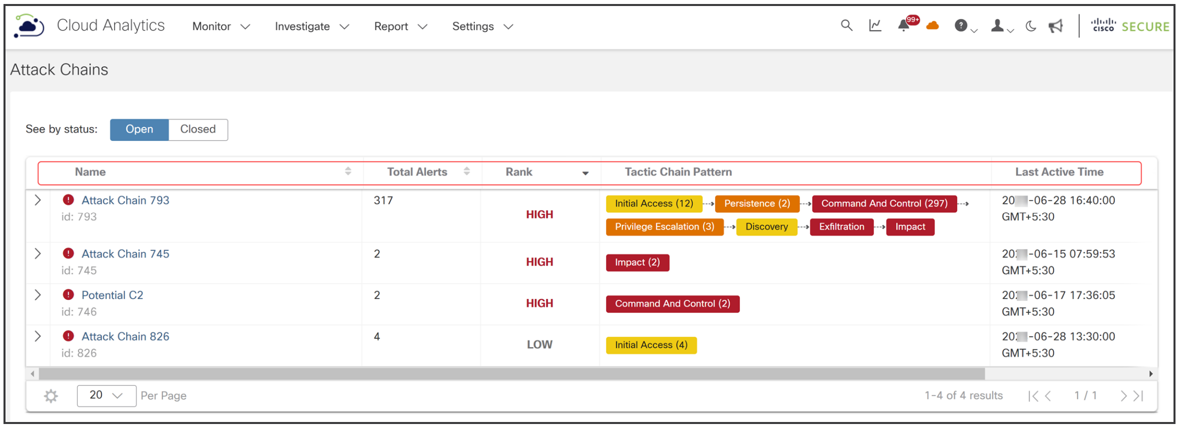
The Attack Chains page displays attack chains, which are sorted by rank to provide a visual indication of those posing the highest risk to your environment.

To access the Attack Chains page, do the following:

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



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



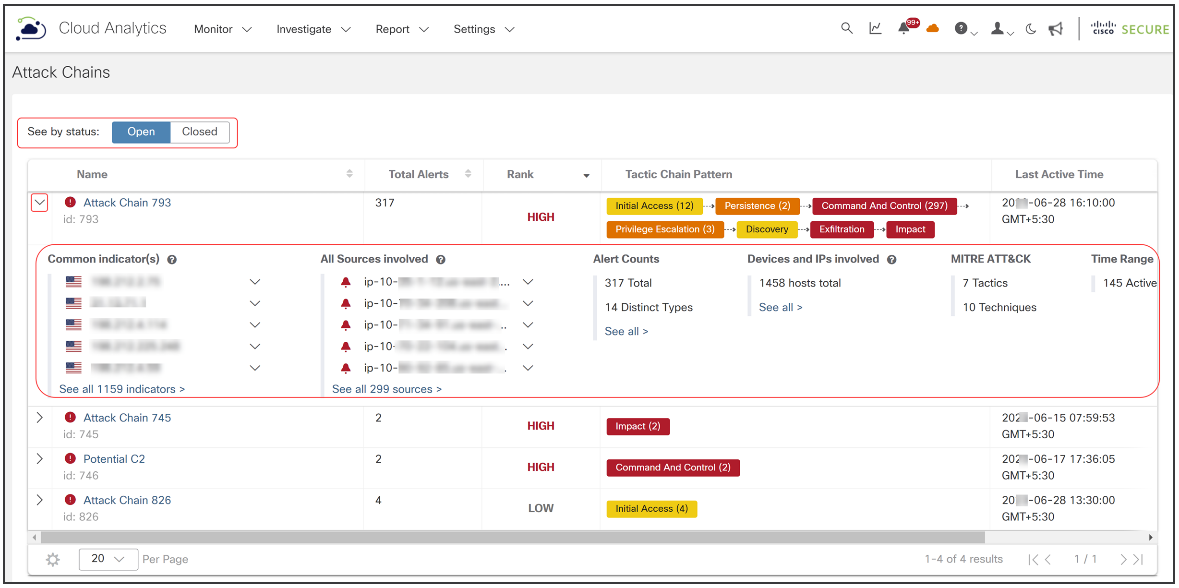
Name	Total Alerts	Rank	Tactic Chain Pattern	Last Active Time
Attack Chain 793 id: 793	317	HIGH	Initial Access (12) → Persistence (2) → Command And Control (297) → Privilege Escalation (3) → Discovery → Exfiltration → Impact	20[redacted]-06-28 16:40:00 GMT+5:30
Attack Chain 745 id: 745	2	HIGH	Impact (2)	20[redacted]-06-15 07:59:53 GMT+5:30
Potential C2 id: 746	2	HIGH	Command And Control (2)	20[redacted]-06-17 17:36:05 GMT+5:30
Attack Chain 826 id: 826	4	LOW	Initial Access (4)	20[redacted]-06-28 13:30:00 GMT+5:30

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:

Column Title	Description
Name	name used to identify a specific attack chain
Total Alerts	total number of alerts in the attack chain
Rank	Yellow = LOW, Orange = MEDIUM, or Red = HIGH
Tactic Chain Pattern	pattern sequence of the MITRE ATT&CK tactics showing the behavior of the attack chain

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.



Attack Chains

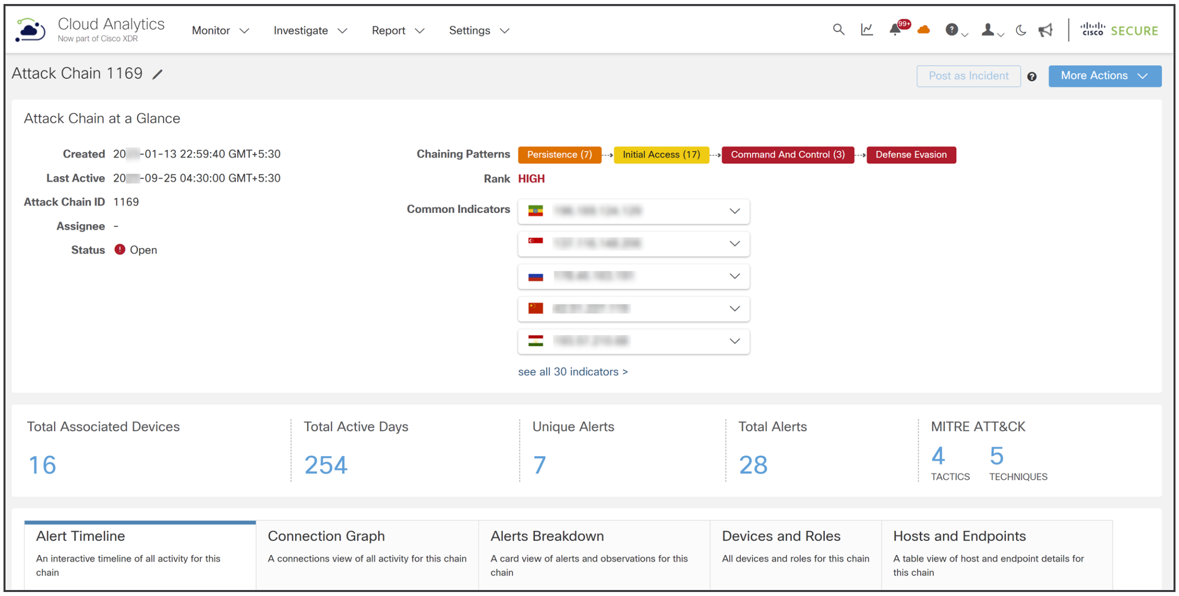
See by status: Open Closed

	Name	Total Alerts	Rank	Tactic Chain Pattern	Last Active Time
∨	Attack Chain 793 id: 793	317	HIGH	Initial Access (12) → Persistence (2) → Command And Control (297) → Privilege Escalation (3) → Discovery → Exfiltration → Impact	20[redacted]-06-28 16:10:00 GMT+5:30
>	Attack Chain 745 id: 745	2	HIGH	Impact (2)	202[redacted]-06-15 07:59:53 GMT+5:30
>	Potential C2 id: 746	2	HIGH	Command And Control (2)	202[redacted]-06-17 17:36:05 GMT+5:30
>	Attack Chain 826 id: 826	4	LOW	Initial Access (4)	20[redacted]-06-28 13:30:00 GMT+5:30

Common indicator(s)	All Sources involved	Alert Counts	Devices and IPs involved	MITRE ATT&CK	Time Range
[redacted]	ip-10-[redacted]...	317 Total	1458 hosts total	7 Tactics	145 Active
[redacted]	ip-10-[redacted]	14 Distinct Types	See all >	10 Techniques	
[redacted]	ip-10-[redacted] ..	See all >			
[redacted]	ip-10-[redacted] .				
[redacted]	ip-10-[redacted] .				
See all 1159 indicators >	See all 299 sources >				

20 Per Page 1-4 of 4 results 1 / 1

4. Select an Attack Chain ID to view the details page for the specific attack chain.



Attack Chain 1169

Attack Chain at a Glance

Created 20[redacted]-01-13 22:59:40 GMT+5:30
Last Active 20[redacted]-09-25 04:30:00 GMT+5:30
Attack Chain ID 1169
Assignee -
Status Open

Chaining Patterns Persistence (7) → Initial Access (17) → Command And Control (3) → Defense Evasion
Rank HIGH
Common Indicators [redacted]
[redacted]
[redacted]
[redacted]
[redacted]
see all 30 indicators >

Total Associated Devices	Total Active Days	Unique Alerts	Total Alerts	MITRE ATT&CK
16	254	7	28	4 TACTICS 5 TECHNIQUES

Alert Timeline	Connection Graph	Alerts Breakdown	Devices and Roles	Hosts and Endpoints
An interactive timeline of all activity for this chain	A connections view of all activity for this chain	A card view of alerts and observations for this chain	All devices and roles for this chain	A table view of host and endpoint details for this chain

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.

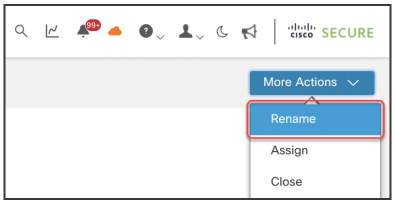
The following tasks help you manage attack chains:

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

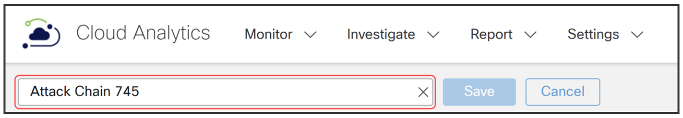
Renaming an Attack Chain

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.
3. Select **More Actions** > **Rename**.



4. Type the new name of the attack chain.



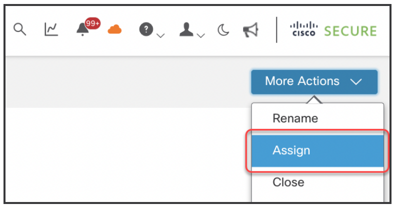
Attack Chain 745

5. Click **Save**.

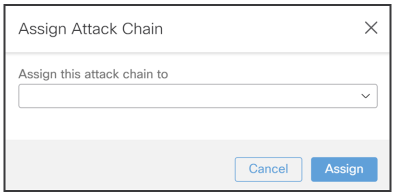
Assigning an Attack Chain

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.
3. Select **More Actions** > **Assign**.



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

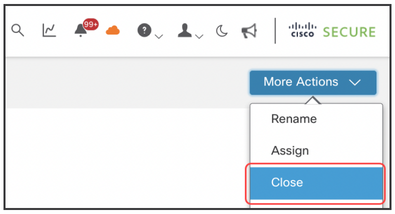
When you close an attack chain, you can open it using the instructions in the **Opening an Attack Chain** section.

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.

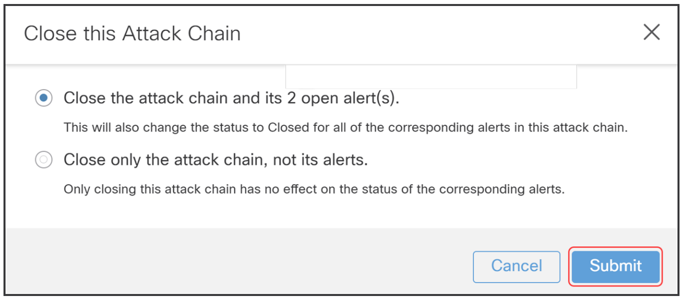
> Make sure to open an attack chain before attempting to post to Cisco XDR or SecureX. If an attack chain is closed, it can't be posted to Cisco XDR or SecureX.

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.
3. Select **More Actions** > **Close**.

   The Close this Attack Chain dialog box displays.

   
   Close this Attack Chain

   ● Close the attack chain and its 2 open alert(s).

   This will also change the status to Closed for all of the corresponding alerts in this attack chain.

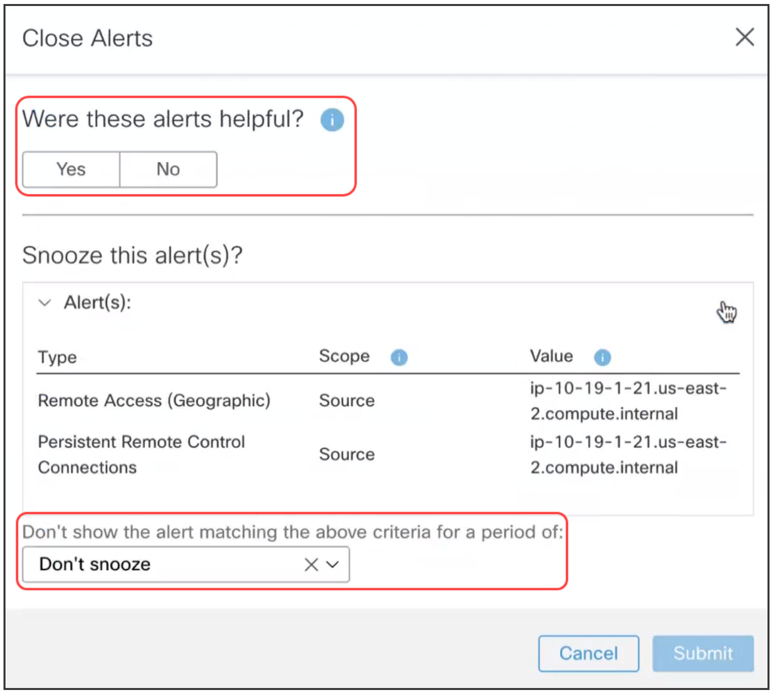
   ○ Close only the attack chain, not its alerts.

   Only closing this attack chain has no effect on the status of the corresponding alerts.

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.

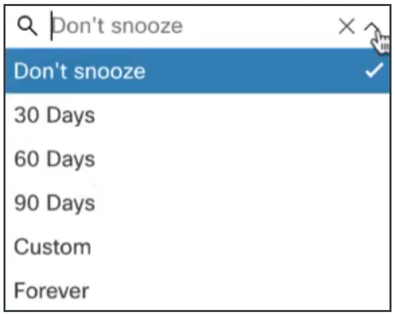
When you choose to close the attack chain *with* its alerts, the Close Alerts dialog box displays.



Type	Scope	Value
Remote Access (Geographic)	Source	ip-10-19-1-21.us-east-2.compute.internal
Persistent Remote Control Connections	Source	ip-10-19-1-21.us-east-2.compute.internal

Don't show the alert matching the above criteria for a period of: Don't snooze

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.

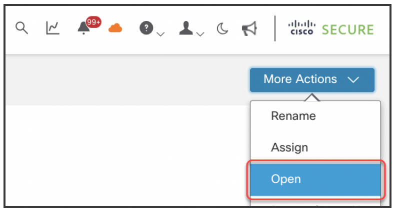
Opening an Attack Chain

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

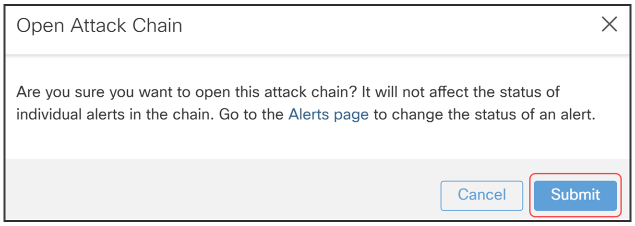
> Opening an attack chain does not affect the status of any alerts within the attack chain. To change the status of an alert, go to the Alerts page.

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.



Open Attack Chain

Are you sure you want to open this attack chain? It will not affect the status of individual alerts in the chain. Go to the Alerts page to change the status of an alert.

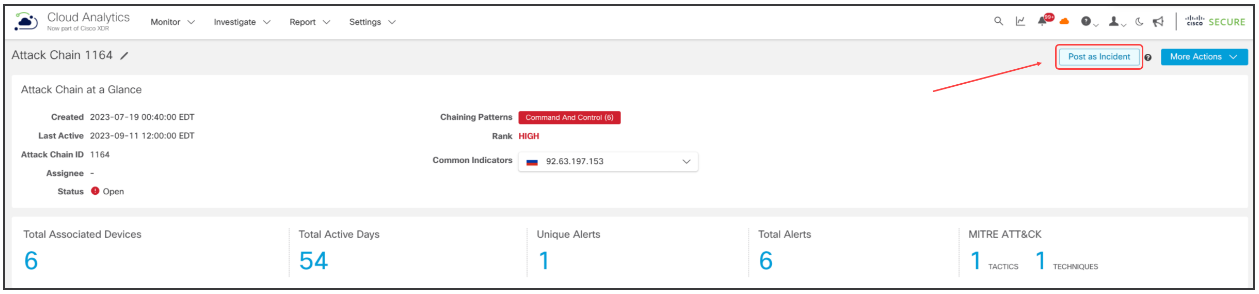
4. Click **Submit** if you'd like to open the attack chain.

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.



Attack Chain 1164

Attack Chain at a Glance

Created 2023-07-19 00:40:00 EDT
Last Active 2023-09-11 12:00:00 EDT
Attack Chain ID 1164
Assignee -
Status Open

Chaining Patterns Command And Control (6)
Rank HIGH
Common Indicators 92.63.197.153

Total Associated Devices 6
Total Active Days 54
Unique Alerts 1
Total Alerts 6
MITRE ATT&CK 1 TACTICS 1 TECHNIQUES

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 web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Revision	Revision Date	Description
1.0	July 31, 2023	Initial Version
1.1	September 26, 2023	Updated content related to Cisco XDR.

Copyright Information