Cisco Talos Threat Hunting Portal User Guide

Contents

Overview

The Cisco Talos Threat Hunting Portal is a central console in Security Cloud Control for participating customers to:

- Review threat hunt notification details, including:
  - Threat summary
  - MITRE ATT&CK mappings
  - Incident timelines
  - Remediation guidance
- Close notifications after remediation is complete or the activity is declared non-malicious
- Communicate with the Cisco Talos Threat Hunting team
- Review threat hunting and MITRE metrics based on network activity

The portal is organization-specific. Users will see only the threat hunt notifications and metrics for the Security Cloud Control organization they are currently signed in to.

Access Requirements

You must have ordered Threat Hunting Services through the Cisco Commerce web site, received your welcome claim code, and set up a Security Cloud Sign On Account to access the Threat Hunting portal.

For more information about getting started with Security Cloud Control see our help docs here: https://securitydocs.cisco.com/

The person who initiates the set-up for your organization will be automatically assigned the role of Administrator. This role allows that user to perform all permission-based actions within the Threat Hunting Portal, in addition to managing users and user roles within your organization.

To add more users to your organization's Threat Hunting Portal, an administrator must invite users to join.

Other roles available include Read-Only and Operations. Users with Operations level permissions can close open notifications as well as send messages within the portal to the Threat Hunting Team.

To provision the portal with your claim code: https://securitydocs.cisco.com/docs/scc/admin/95947.dita

To assign roles to users: https://securitydocs.cisco.com/docs/scc/admin/95952.dita

Role	View notifications	View metrics	Send messages	Close notifications	Invite users	Adjust user roles
Administrator	✓	✓	✓	✓	✓	✓
Operations	✓	✓	✓	✓	✗	✗
Read only	✓	✓	✗	✗	✗	✗

If the portal does not show a page or action you expect, ask your Security Cloud Control administrator to verify your Talos Threat Hunting role.

Opening the Portal

1. Sign into Security Cloud Control
2. Select Talos Threat Intel Center

The Talos Threat Intel Center opens the Cisco Talos Threat Hunting portal to the Threat Notifications page by default. The top navigation contains these views:

- Threat Notifications
- Hunt Metrics
- MITRE Metrics

Threat Notifications

The Threat Notifications page lists threat hunt notifications for your organization.

Open notifications require review, response, or remediation. Closed notifications have been completed, remediated, or determined not to require further action.

Users with Administrator or Operations access can send messages from an open notification to ask for clarification, share findings, provide remediation status, or contact the Threat Hunting team with other concerns. Read Only users can view message history but cannot send new messages.

Messages are text-only. File attachments are not supported. The portal does not send email notifications when new messages are added, so users must return to the notification detail page to check for updates.

Notifications may be labeled as Confirmed Threat if the Threat Hunting team has validated the activity as malicious. If a notification is labeled as Needs Information, the Threat Hunting team needs more context from your organization before making a final assessment. A False Positive notification indicates that the activity was reviewed and determined to not be malicious. It is possible for a Needs Information notification to become either a Confirmed Threat or a False Positive once additional information has been reviewed and the notification is closed.

Users can view a notification's details page by clicking on the notification title. This page provides details regarding the activity including a summary of the activity, mapped MITRE ATT&CK tactics and techniques, an incident timeline, and remediation steps.

Close a Notification

Users with Administrator or Operations access can close open notifications.

Close a notification when:

- Recommended remediation is complete.
- The threat has been contained.
- Your investigation confirms the activity was not malicious.
- The notification no longer requires action from your organization or the Threat Hunting team.

If the current threat assessment is Needs Information, you can optionally update the final threat type to Confirmed Threat or False Positive before closing.

Open notifications will automatically close after 30 days, and tcan also be closed by the Threat Hunting team.

After a notification is closed, you can no longer send messages from that notification.

Hunt Metrics

The Hunt Metrics page summarizes threat hunting activity for your organization within a selected time period. Available metrics include total proactive threat hunts run by the Cisco Talos Threat Hunting team, comparisons of confirmed threats to potential threats and confirmed false positives, and breakdowns of top MITRE ATT&CK activity by tactic and technique.

MITRE Metrics

The MITRE Metrics page shows how all tagged threat hunts map to MITRE ATT&CK tactics, techniques, and subtechniques.

Use MITRE Metrics to understand which adversary behaviors have appeared most often in your organization's threat hunting results and where hunt coverage is concentrated.

Troubleshooting

I cannot see the Threat Hunting Portal

Confirm that you are signed in to the correct Security Cloud Control organization and that your account has a Talos Threat Hunting role.

I see "You do not have access to this page"

Your assigned role does not include permission for that page. Ask your Security Cloud Control administrator to review your role assignment.

Notifications or metrics fail to load

Refresh the page and try again. If the issue continues, confirm that your Security Cloud Control session is still active and that your organization is provisioned for Threat Hunting.

I cannot send a message

Messages can only be sent from open notifications by users with Administrator or Operations access. Closed notifications and Read Only access do not allow new messages.

I cannot close a notification

Only Administrator and Operations users can close notifications. If you have the correct role and the close action still fails, retry after refreshing the page.

Legal information

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.