Leverage the Power of Splunk Using the Latest Cisco Security Integrations

Digital Resilience

David Gamer
Principal Global Security Product Specialist

Session ID: BRKSEC-1800

Agenda

01 One Cisco

02 Integrations Overview

03 Available Today

04 Cisco Security Cloud App

05 Cisco AI Defense

06 Cisco XDR

07 Value Across Integrations

08 Talos Integrations

09 Duo, Kenna, etc.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Webex App

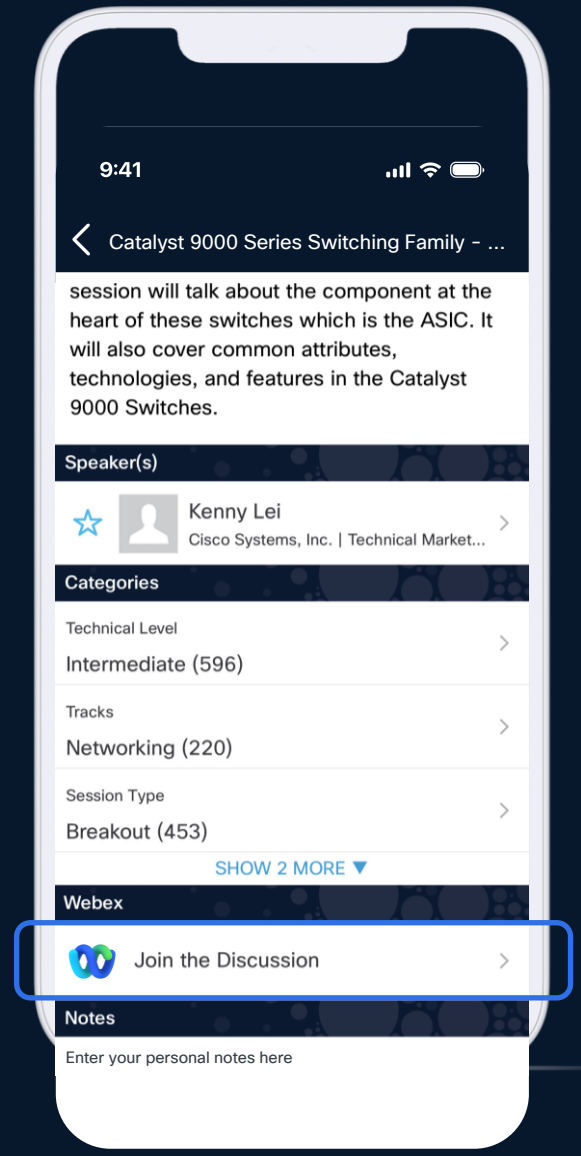
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKSEC-1800**

© 2025 Cisco and/or its affiliates. All rights reserved.

We deliver mission critical outcomes as One Cisco.

AI-ready data centers

Future-proofed workplaces

Digital resilience

Accelerated by Cisco AI

© 2025 Cisco and/or its affiliates. All rights reserved.

Game changing security to protect your entire digital footprint

Access the right data

Cisco data is being made accessible to Splunk users through technology add-ons*.

**now available on Splunkbase via Cisco Security Cloud App.*

Apply the right analytics

Cisco adds deep telemetry to detect lateral movement through the network.

Accelerate the right action

Cisco adds rich context and detections from Talos threat intelligence.

**now available in Splunk ES, SOAR and Attack Analyzer.*

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Integrations to protect your entire digital footprint

Threat intelligence

Enhance defense against known and unknown threats

Splunk +
Cisco Talos

Security alerts and context

Accelerate detection, investigation and response

Splunk +
Cisco Security Cloud App

Secure AI

Detect and reduce AI-based risks

Splunk +
Cisco AI Defense

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco integrations made seamless

The Cisco Security Cloud app enables easier integration of your Cisco data sources within Splunk

Available Today:

- AI Defense
- Secure Network analytics
- XDR (Incident Reporting)
- Email Threat Defense
- Multi Cloud Defense
- Secure Firewall (FTD, Estreamer, ASA)
- Malware Analytics
- Secure Endpoint
- Kenna Vulnerability Intelligence
- Identity Intelligence
- Duo

Next Up:

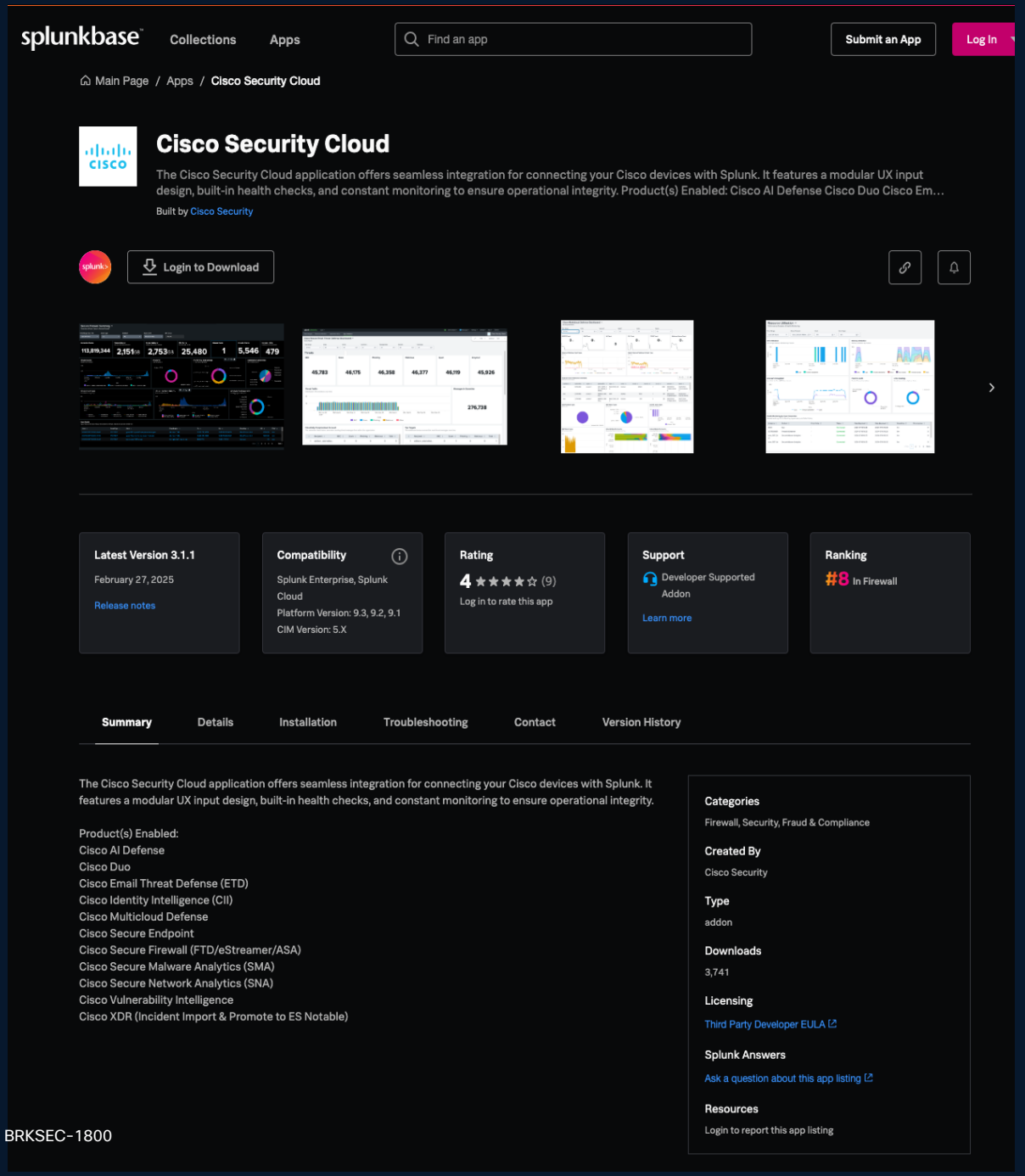
- Isovalent (Hypershield)
- Secure Workload
- Crosswork Cloud

© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

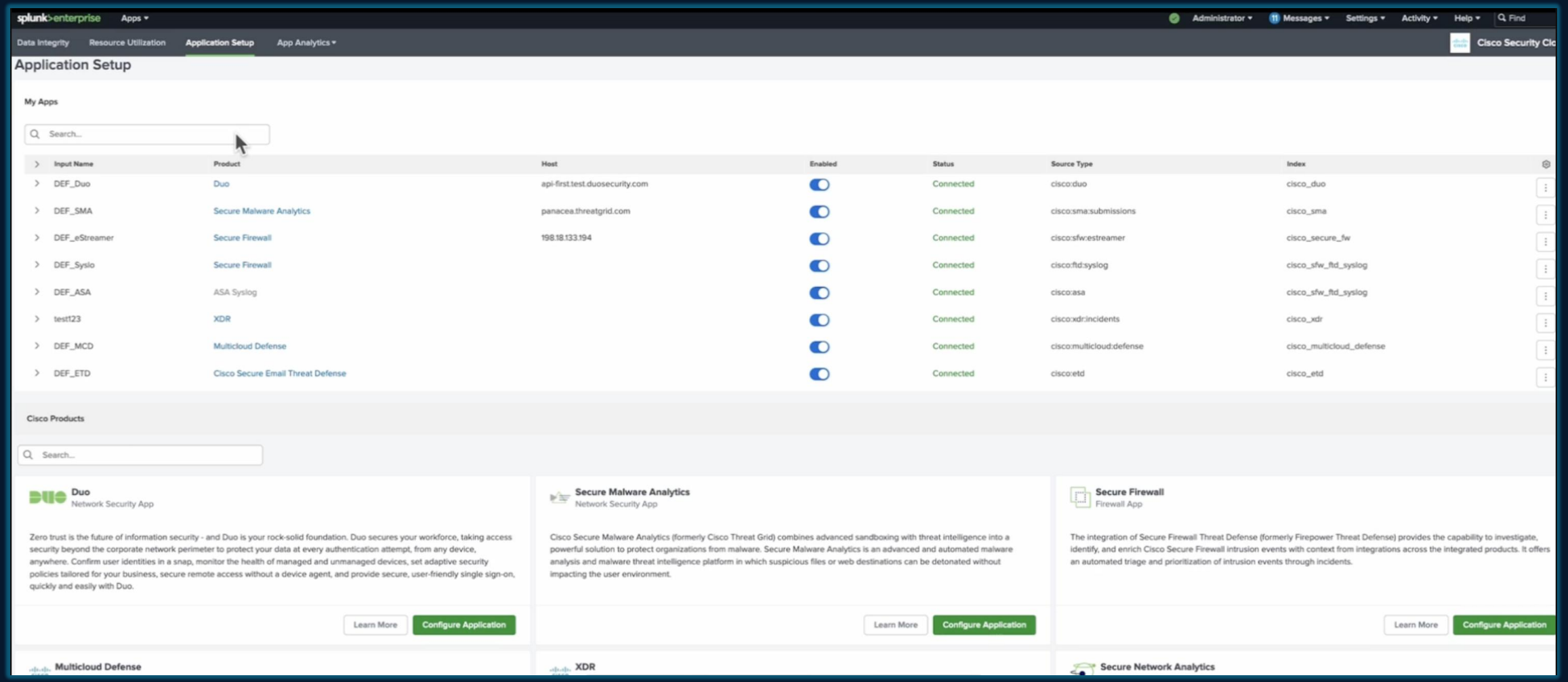
Cisco Security Cloud App

- Single application that packages all Cisco Security integrations in a single offering based on “gold standard” best practices
- Replaces the older individual Cisco TA's and Apps that are now archived
- Includes these Cisco Security products:
  - **AI Defense (NEW)**
  - Secure Network Analytics (SNA)
  - XDR
  - Duo
  - Email Threat Defense
  - Multi Cloud Defense
  - Secure Firewall (FTD, Estreamer, ASA)
  - Malware Analytics
  - Secure Endpoint
  - Kenna VI
  - Identity Intelligence



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Security Cloud – Application Setup



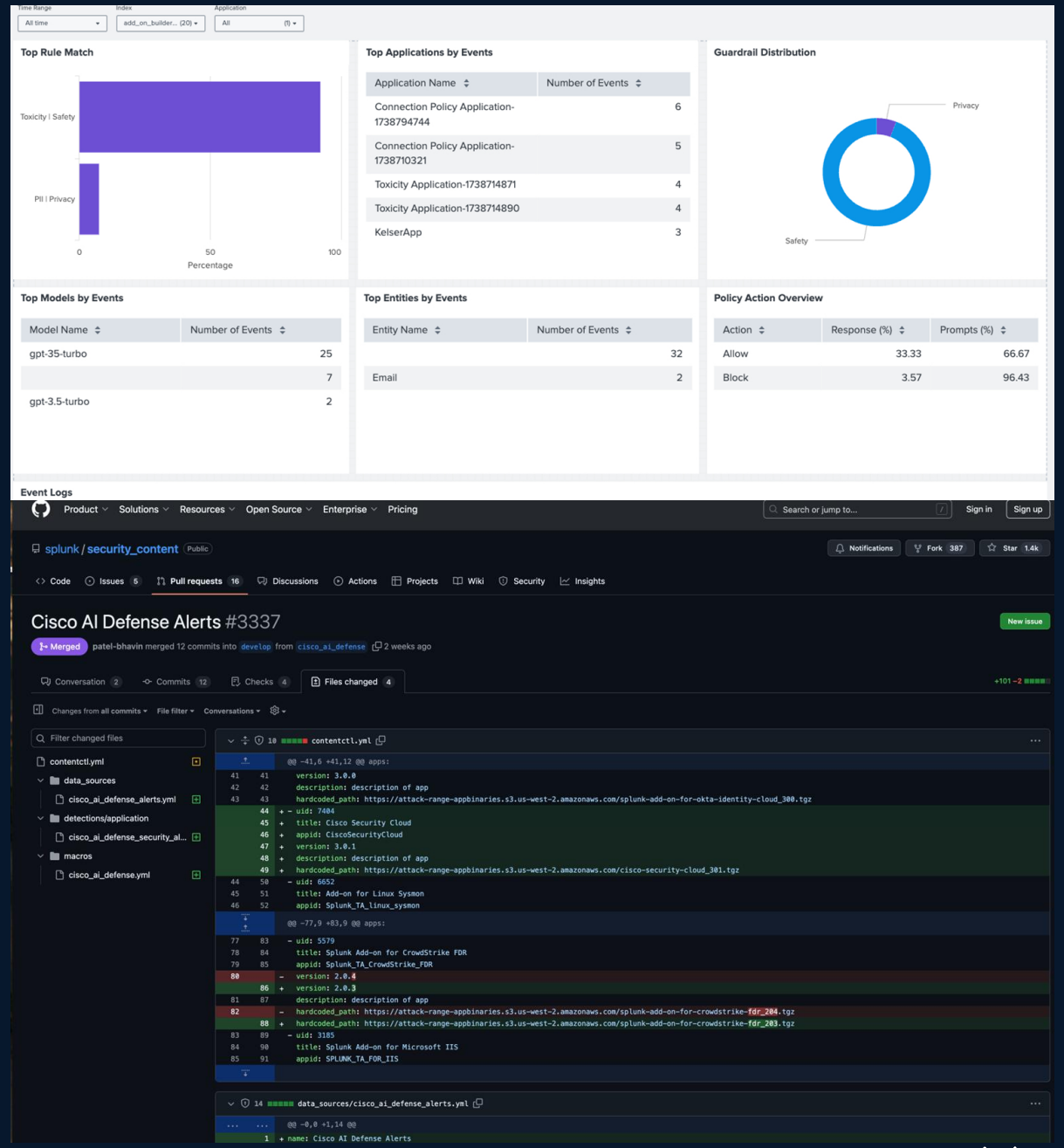
© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Cisco AI Defense

Gain visibility into emerging AI risks with Splunk

- Pulls in alerts from AI Defense and maps them to the Common Information Model (CIM), visualized in a dashboard.
- Gain visibility into risks associated with LLM models, AI apps and entities.
- Includes an out-of-the-box Enterprise Security detection that creates a search and surfaces potential attacks against the AI models running in your environment.



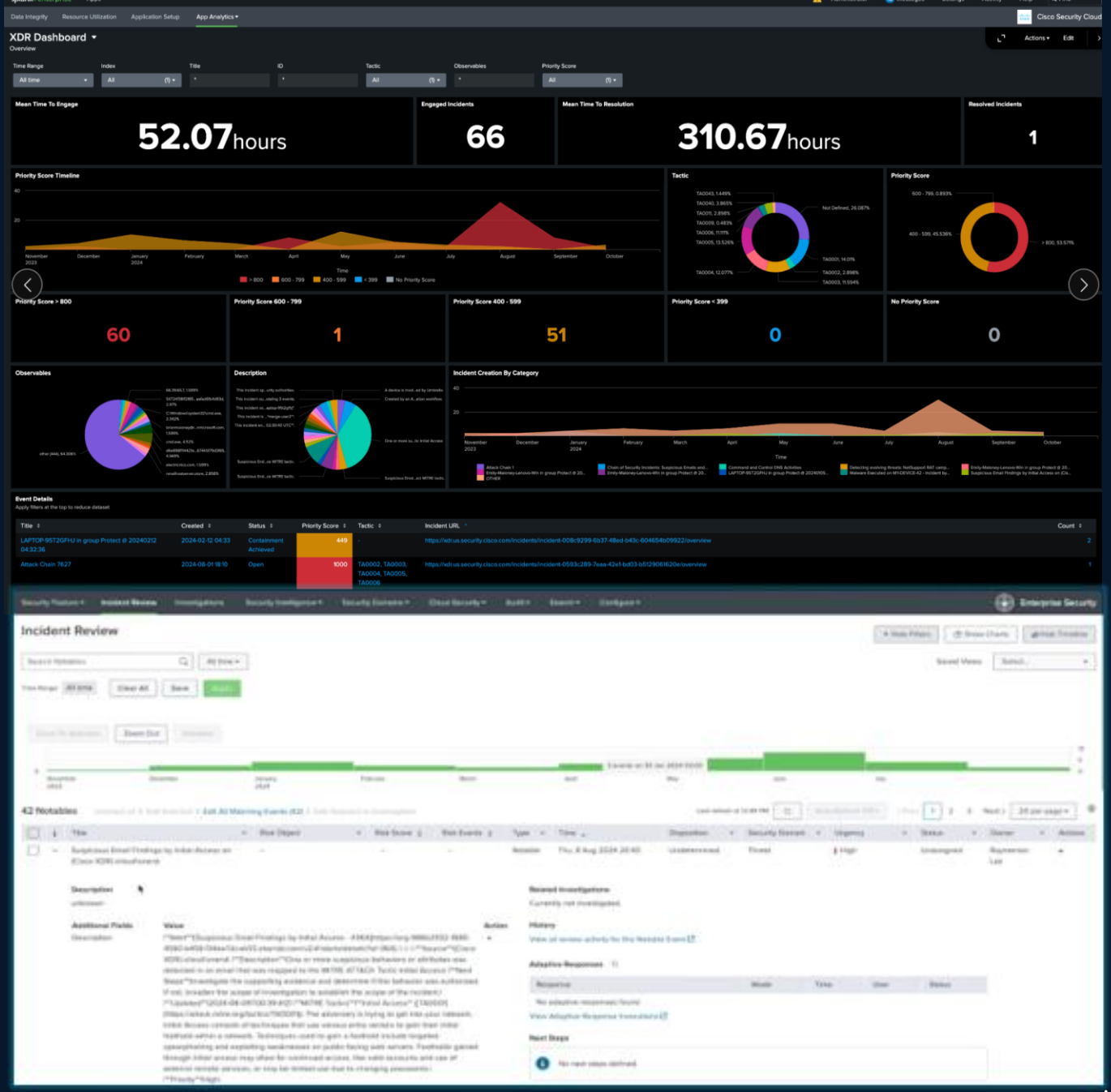
© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Cisco XDR

Splunk Integration

- Provides a comprehensive view of security-related threats targeting your environment across multiple security control points
- The Splunk integration ingests and maps XDR Incidents to the Alert CIM data model
- The XDR incident that is ingested contains all of the observables that were correlated together from various XDR sources
- The XDR incident can be promoted to an ES finding that will contain all of the observables and context from XDR automatically, manually or both.



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Security Integrations | Now Available

How Cisco data can be used in Splunk to drive Unified TDIR

Cisco XDR

- Analyzes and enriches alerts and data from Cisco and third-party products
- Performs analysis on Netflow data to look for suspicious behavior
- Sends outcome of analysis in the form of an Incident to Splunk to be elevated into an ES finding

Cisco DUO

- Verifies user and endpoints connecting to the user network to look for security access related threats
- Alerts / events triggered by suspicious activity are sent to Splunk mapped to the authentication CIM model
- Customers can take the alerts generated by Duo

Cisco Email Threat Defense

- Analyzes emails looking for phishing attempts and malicious IOC in the email
- Alerts are sent to Splunk and mapped to the email data model
- OOTB ES content to detect suspicious or malicious emails can be used to trigger an ES finding

Cisco Multi-cloud Defense

- Detects and blocks lateral movement and exfiltration of data
- Alerts and events are sent to Splunk and mapped to CIM
- OOTB ES content to detect suspicious or malicious network attacks and data exfiltration can be used to trigger an ES finding

Cisco Secure Firewall

- Network security device that monitors / filters incoming & outgoing network traffic
- Alerts and events are sent to Splunk and mapped to CIM
- OOTB ES content to detect suspicious or malicious network attacks and malicious communication

So What?

Integrate XDR incidents into ES findings for seamless threat detection and investigation, ensuring comprehensive security coverage.	Incorporate Duo events into Splunk ES findings to detect and respond to suspicious user activities, enhancing user security.	Add phishing detections and email context into Splunk ES findings for enriched investigations, improving threat response accuracy.	Integrate lateral movement detection incidents into ES findings for cloud incident management, ensuring robust cloud security.	Include firewall incidents into ES findings for seamless network incident management, enhancing network security visibility.

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Cisco Security Integrations | Now Available

How Cisco data can be used in Splunk to drive Unified TDIR

Cisco Secure Network Analytics

- Analyzes network traffic looking for malicious communications and anomalies
- The Splunk integration ingests and maps SNA events and alerts to the Alert, Network, Web CIM data models
- Customers can take the alerts generated by SNA and elevate them into an ES finding or turn into RBA findings

Cisco Secure Malware Analytics

- Analyzes artifacts like files and URLs to look for malicious behavior
- Outcome of analysis is sent to Splunk and mapped to CIM
- Customers can use OOTB ES content for detecting malware

Cisco Secure Endpoint

- Analyzes endpoint behavior looking for suspicious or malicious activity that that is an indication of a compromised host
- Outcome of analysis is sent to Splunk and mapped to various CIM models
- Customers can use OOTB ES content for detecting endpoint activities

Cisco Kenna VI Feed

- Vulnerability intelligence feed that helps prioritize CVE vulnerabilities based on severity, likelihood of being exploited and other factors
- Threat intelligence feed is sent to Splunk and stored in lookup tables
- Customers can use the intelligence to match CVE's against in Enterprise Security

Cisco Secure Firewall

- Analyzes human identities and associates risk based on users' behavior, access activity, resources they have access to and privileges
- Outcome of analysis is sent to Splunk and mapped to various CIM models
- Customers can use the information to trigger findings in ES

So What?

Incorporate SNA incidents into Splunk ES findings for deep network visibility and seamless threat detection and investigation.

Add malware events into Splunk ES findings to correlate findings on related URLs and artifacts, streamlining malware investigations.

Integrate endpoint detections into Splunk ES findings for enriched investigations and event correlation, improving endpoint security.

Incorporate vulnerabilities and threat intelligence into Splunk ES findings to enrich investigations with context, enhancing threat intelligence.

Add data on suspicious user activity into Splunk ES findings for added identity context during investigations, improving user activity monitoring.

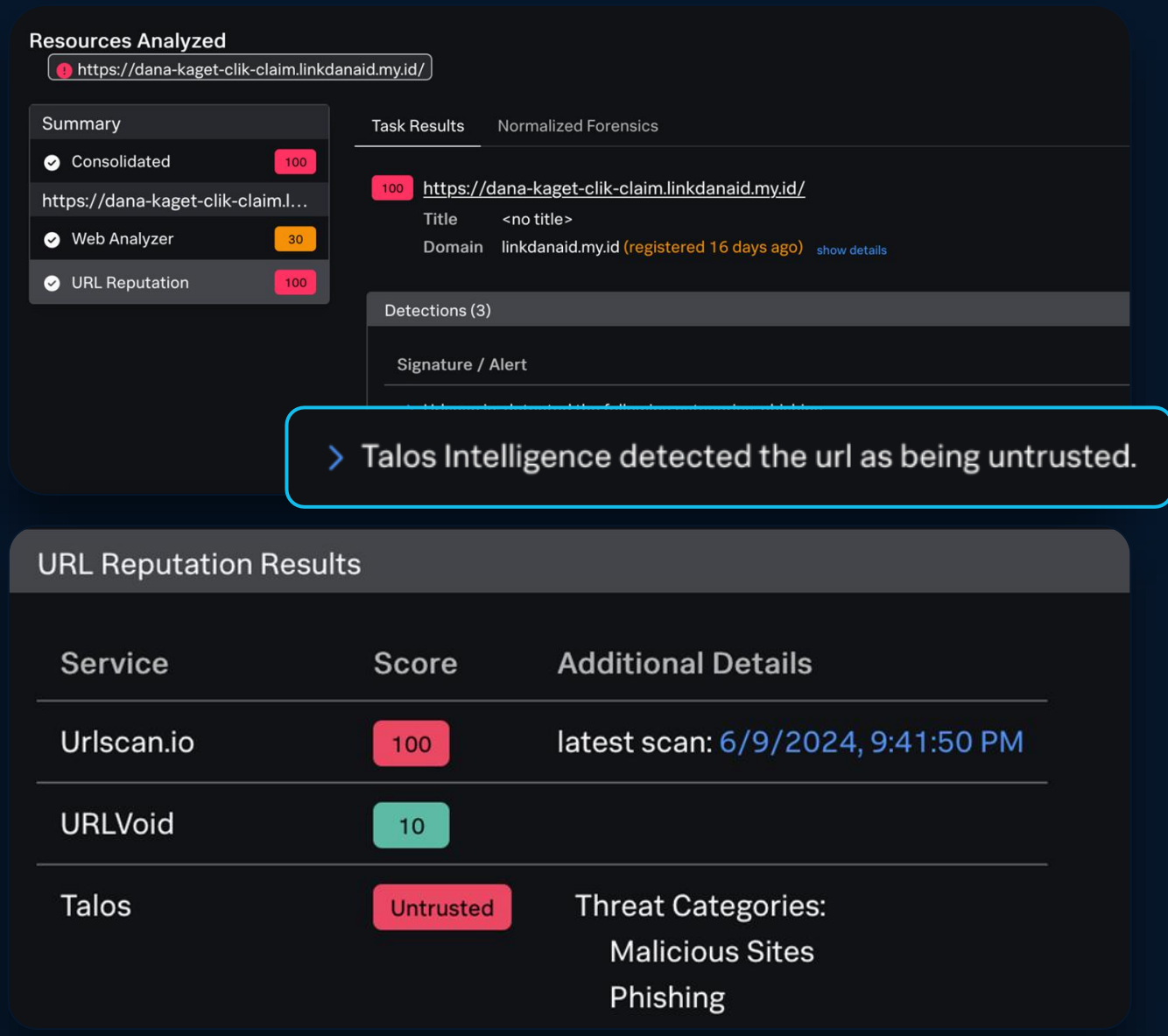
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Now Available

Talos Threat Intelligence for Splunk Attack Analyzer

- Enabled for all Splunk Attack Analyzer customers – no additional configuration required
- Empowers detection of net new threats, particularly those that are ephemeral in nature
- Enriches URLs discovered in attack chain with reputation results

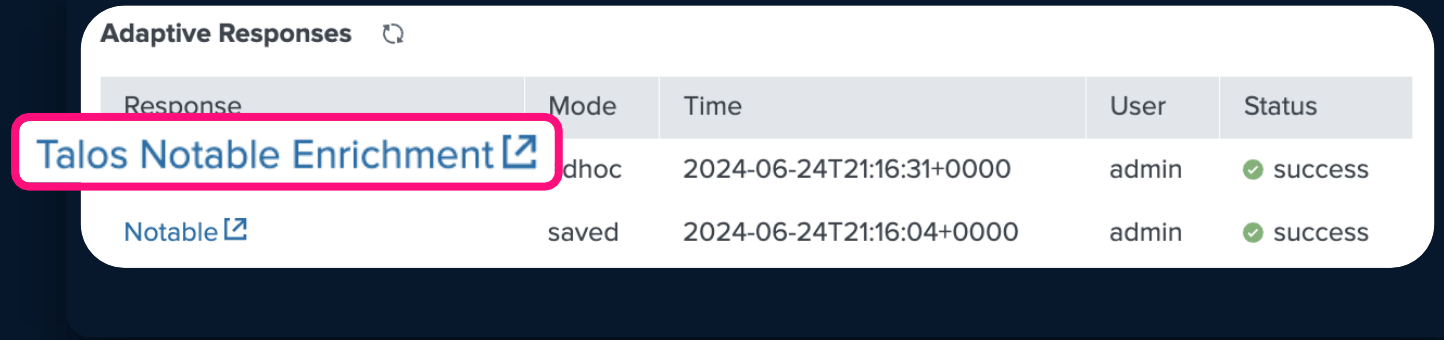


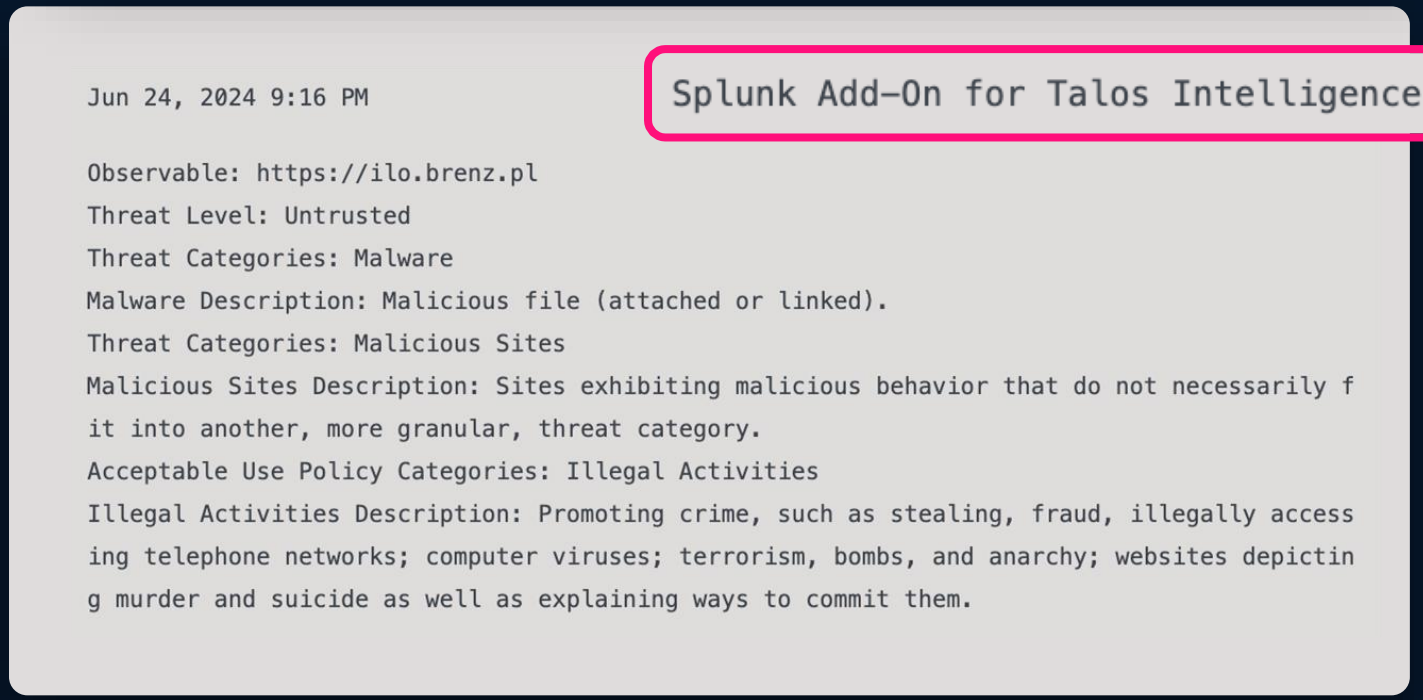
© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Splunk Add-on for Talos Intelligence

- Out-of-the-box adaptive response action
- All Splunk Enterprise Security customers have access
- Delivers rich enrichment for common IOCs



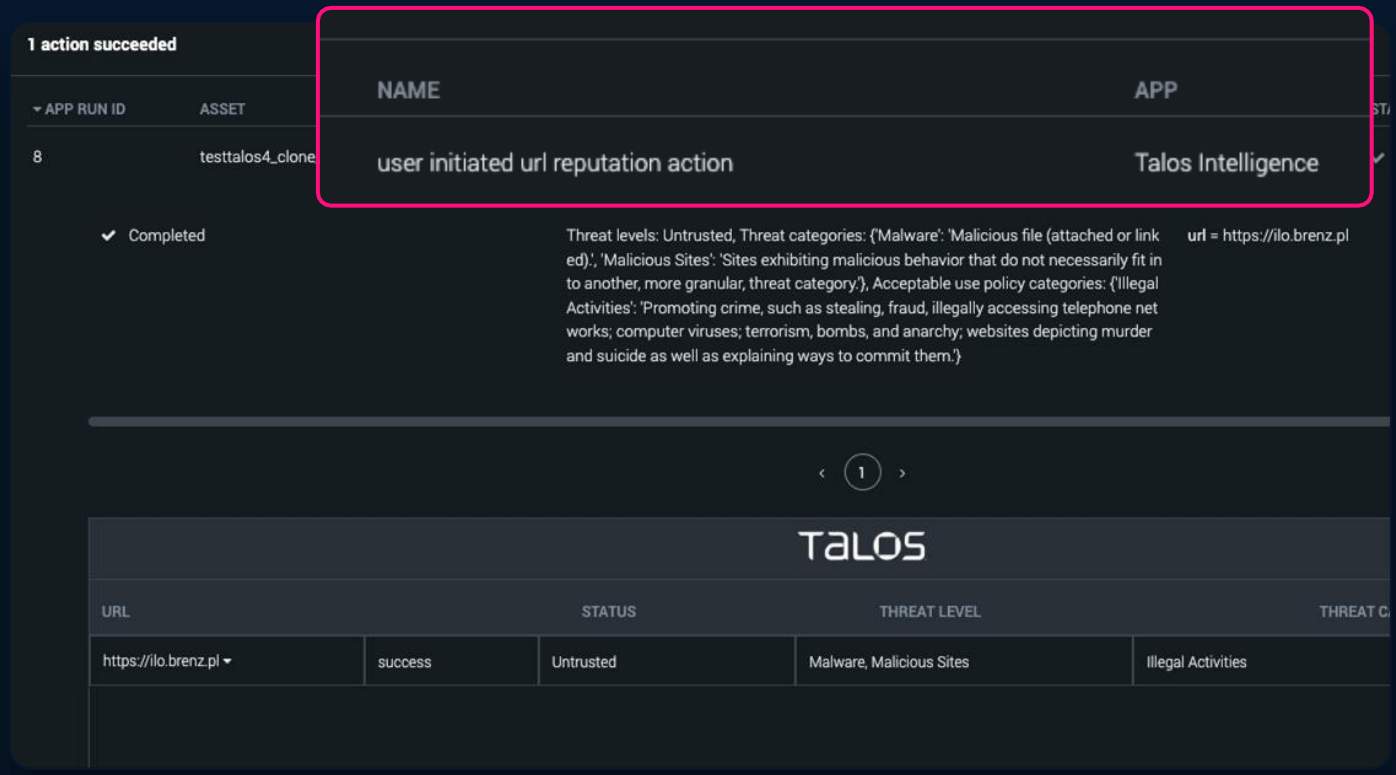


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Talos Intelligence Connector

- Out-of-the-box connector for Splunk SOAR
- All Splunk SOAR customers have access
- Infuses Talos threat intelligence directly into incident res



© 2025 Cisco and/or its affiliates. All rights reserved.

Splunk + Cisco Talos Incident Response Services

Combine the best of Splunk Security and Cisco Talos

Splunk's industry-leading SecOps solutions

+

Cisco Talos' incident response expertise

=

A holistic approach to fortify digital resilience

Proactive Defense for Your Security Operations

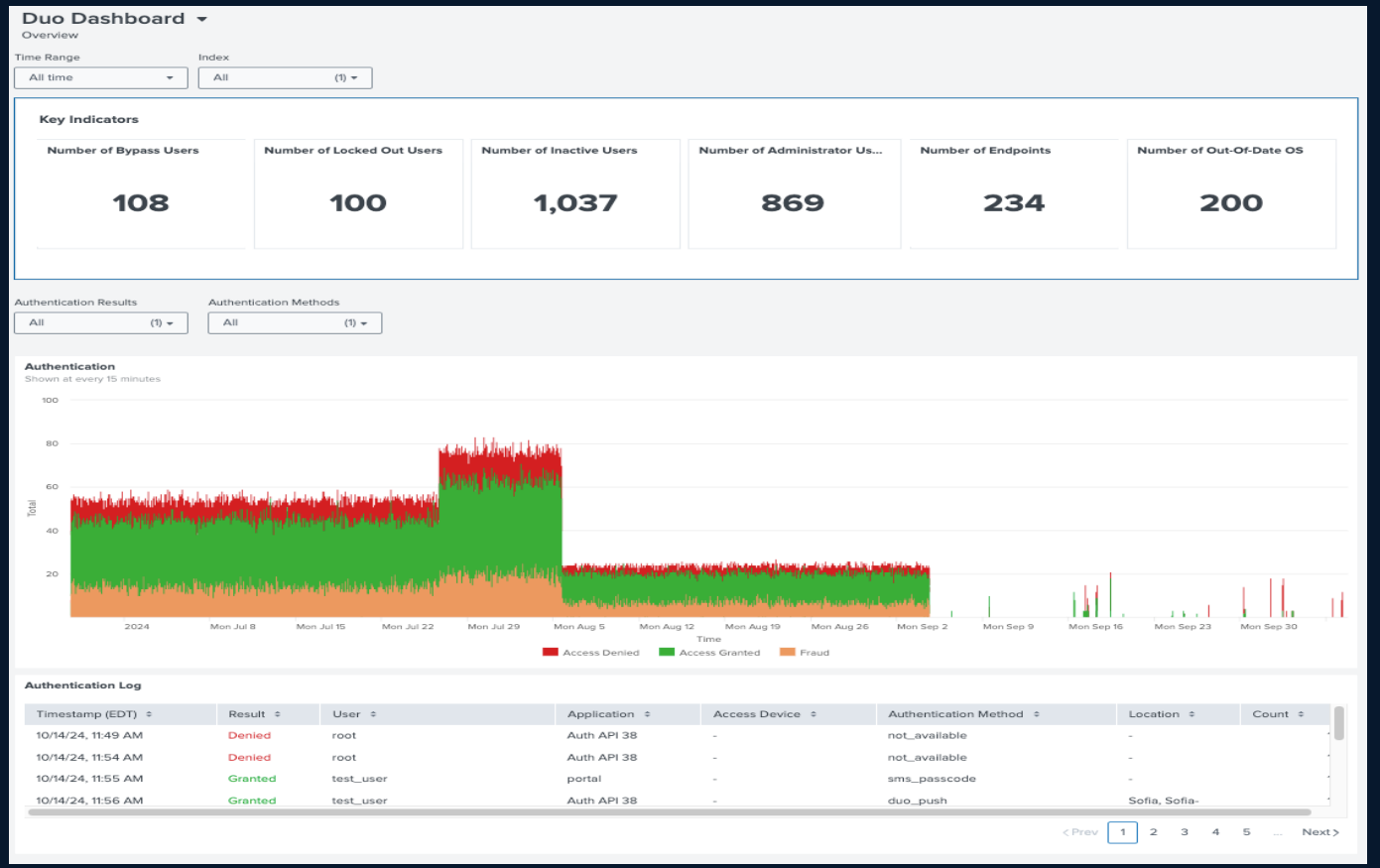
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Now Available

Cisco Duo

- Cisco Duo is a multi-factor authentication and secure remote access
- The Splunk integration ingests and maps Duo system log events to the Authentication CIM model
- **Common DUO Detections and alerts sent to Splunk**
  - Fraudulent Duo user
  - High number of MFA request
  - User authentication
  - User set to bypass status
  - User set to disable
  - User accessing for new location
  - New admin account created
  - Authentication policy changed
  - Security keys presented in plain text
  - Delete an integration

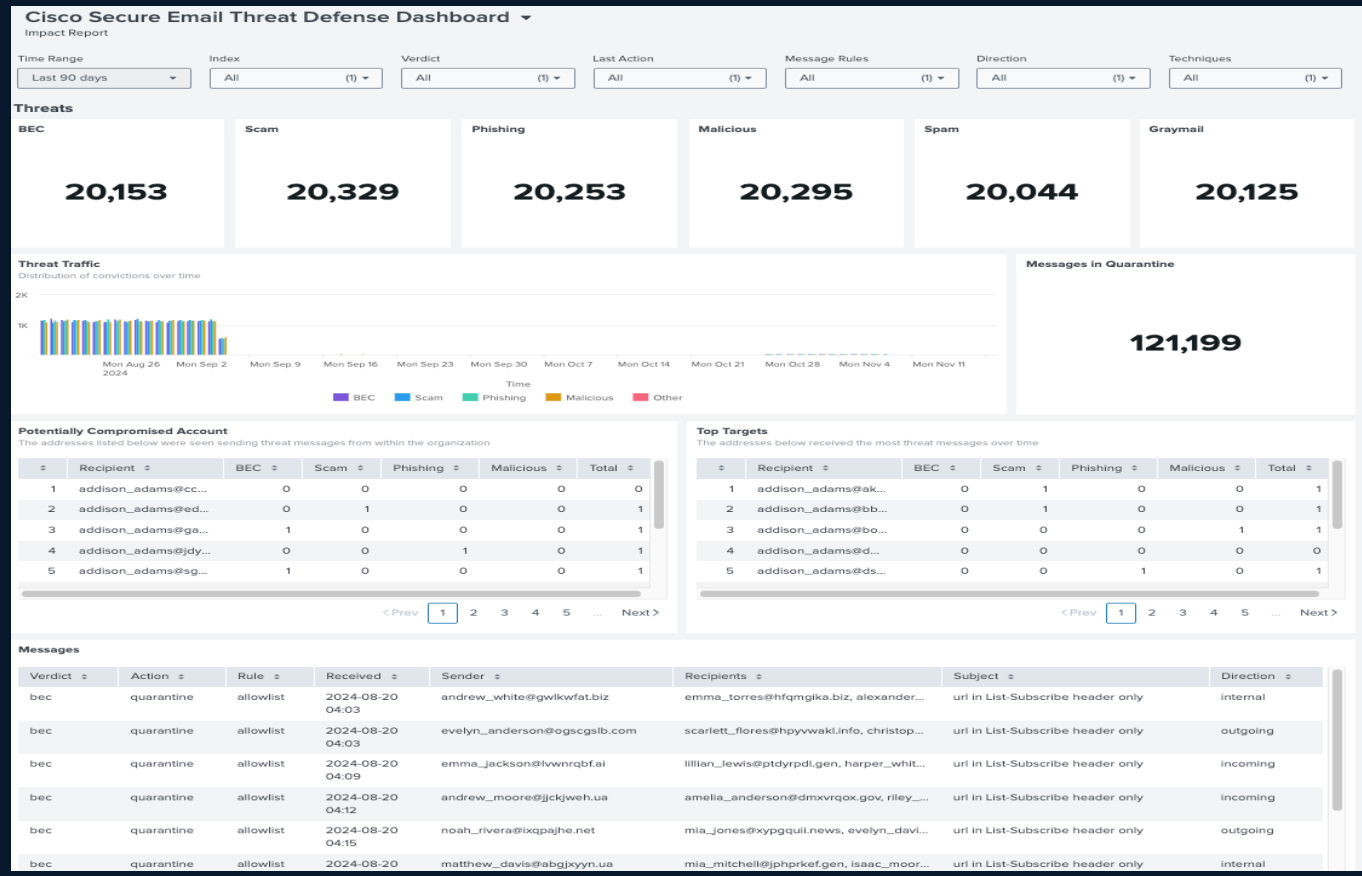


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Cisco Email Threat Defense

- Email Threat Defense Addresses gaps in Microsoft 365 email security by detecting and blocking advanced email threats
- The Splunk integration ingests threat messages found and convicted by Cisco's Email Threat Defense solution. It will include all the IOCs that led to the message conviction by ETD.
- Events and alerts are mapped to the Email CIM data model

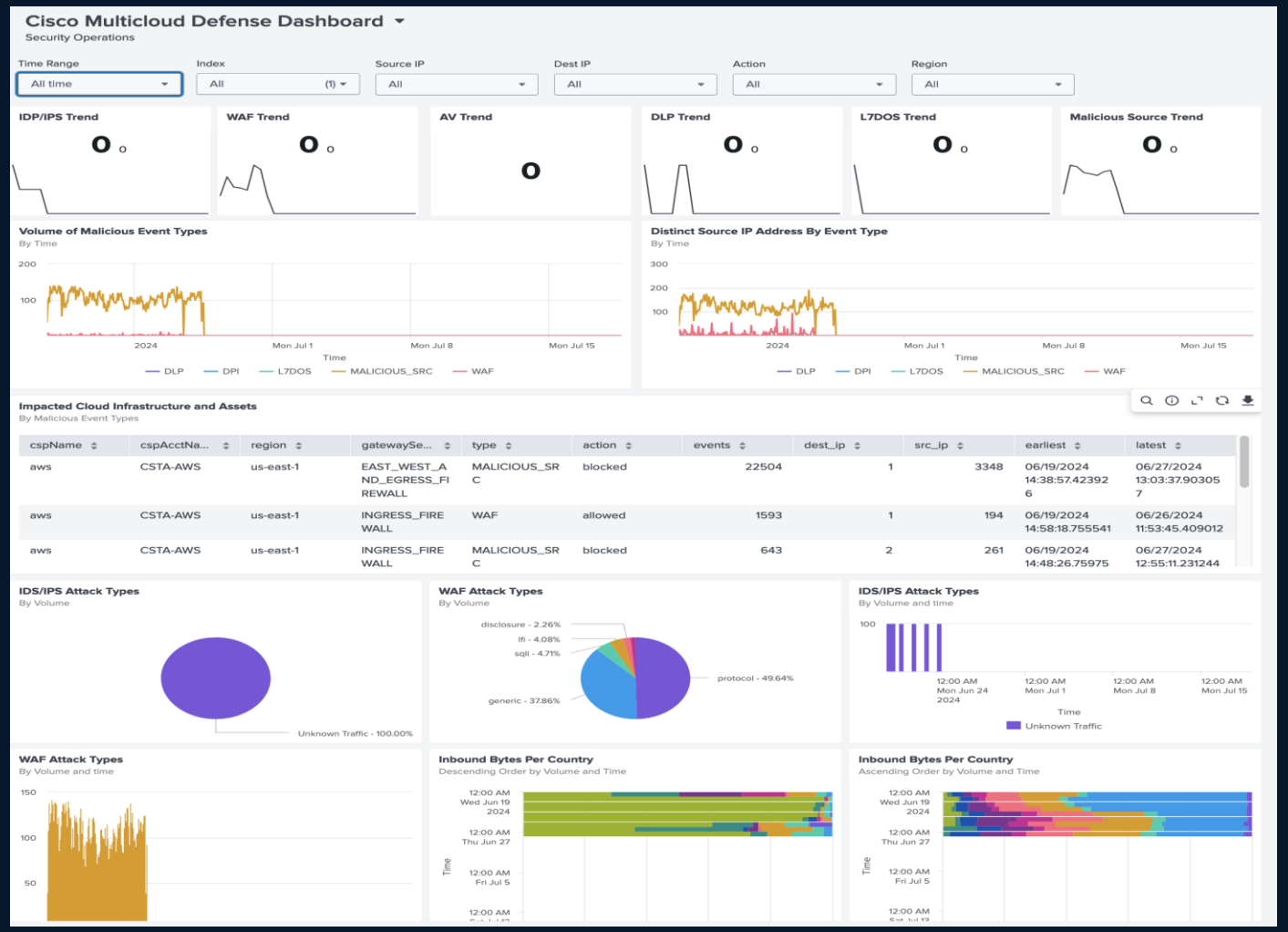


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Cisco Multicloud Defense

- Multi-cloud defense protects customer environments to block inbound, lateral movement attacks and exfiltration of data
- The Splunk integration ingests and maps events and alerts from their different modules (Waf, AV, DLP, DDOS, Errors, Malware, FQDN) into the Network, Malware, IDS, Web and communicate CIM models
- Dashboards cover malicious communications, GEO location data, prevention and asset inventory

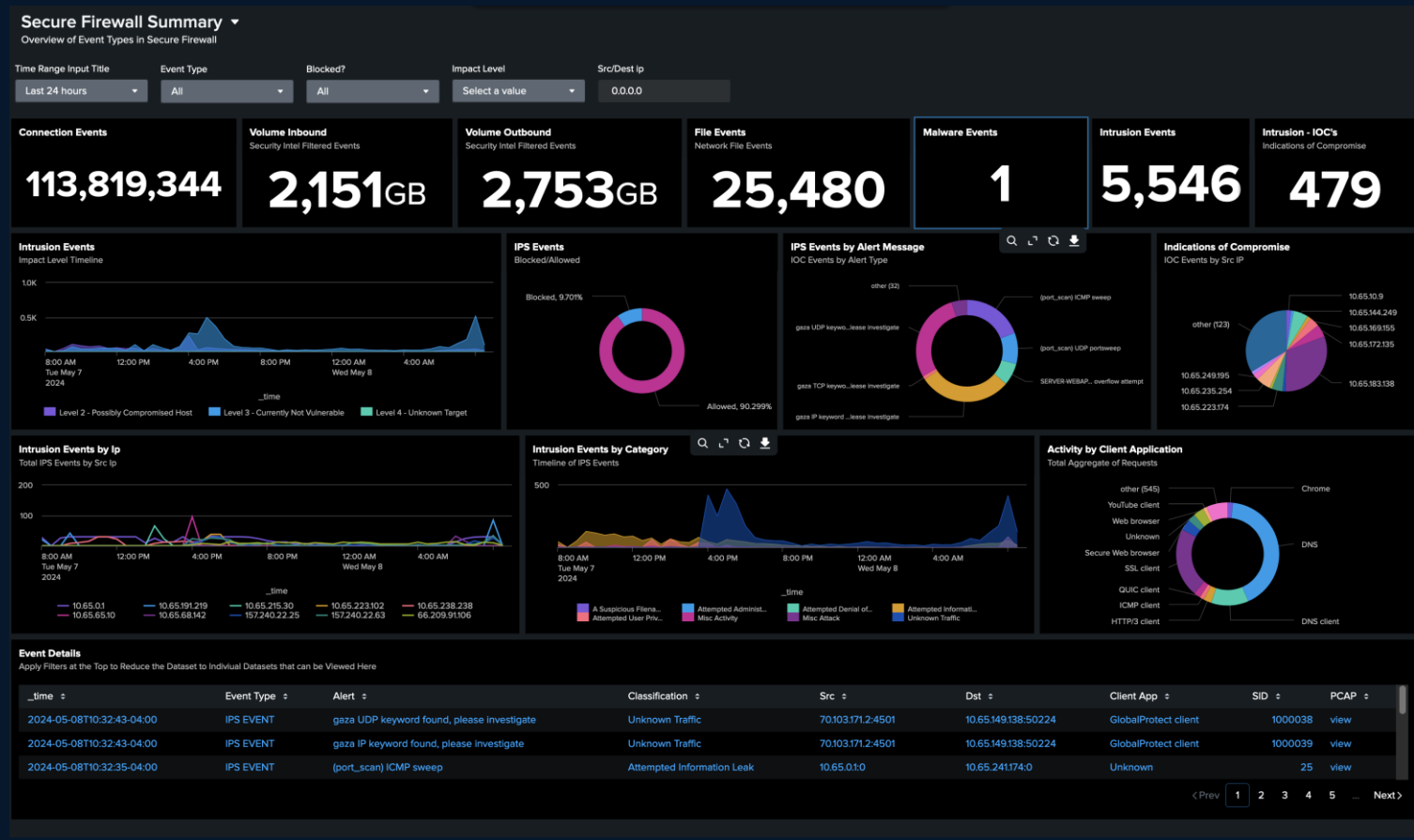


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Secure Firewall

- Secure Firewall helps protect customer networks
- The Splunk integration spans Secure Firewall IDS, Connection and Malware event types and ingests and maps them to IDS, Endpoint, Attack, Network CIM models
- Dashboards profile IOC's and details for connection and malware events.
- Ability to filter high fidelity events in the app

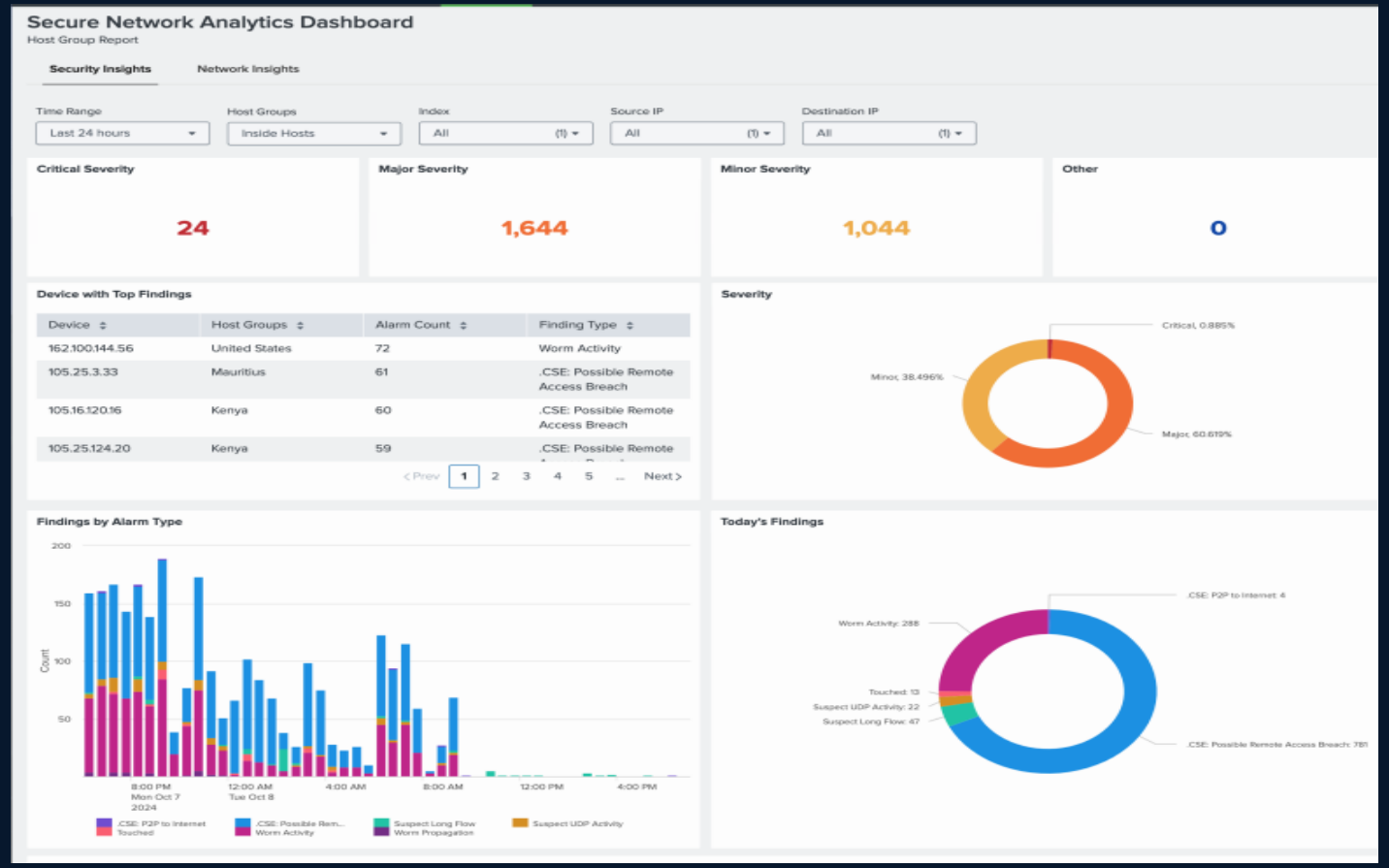


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Cisco Secure Network Analytics

- Secure Network Analytics analyzes network traffic to detect threats
- The Splunk integration ingests and maps SNA events and alerts to the Alert, Network, Web CIM data model
- Ability to promote an SNA alert into an ES finding or RBA event-based criteria set by the end user on severity of alert
- Ability to filter high fidelity events in the app

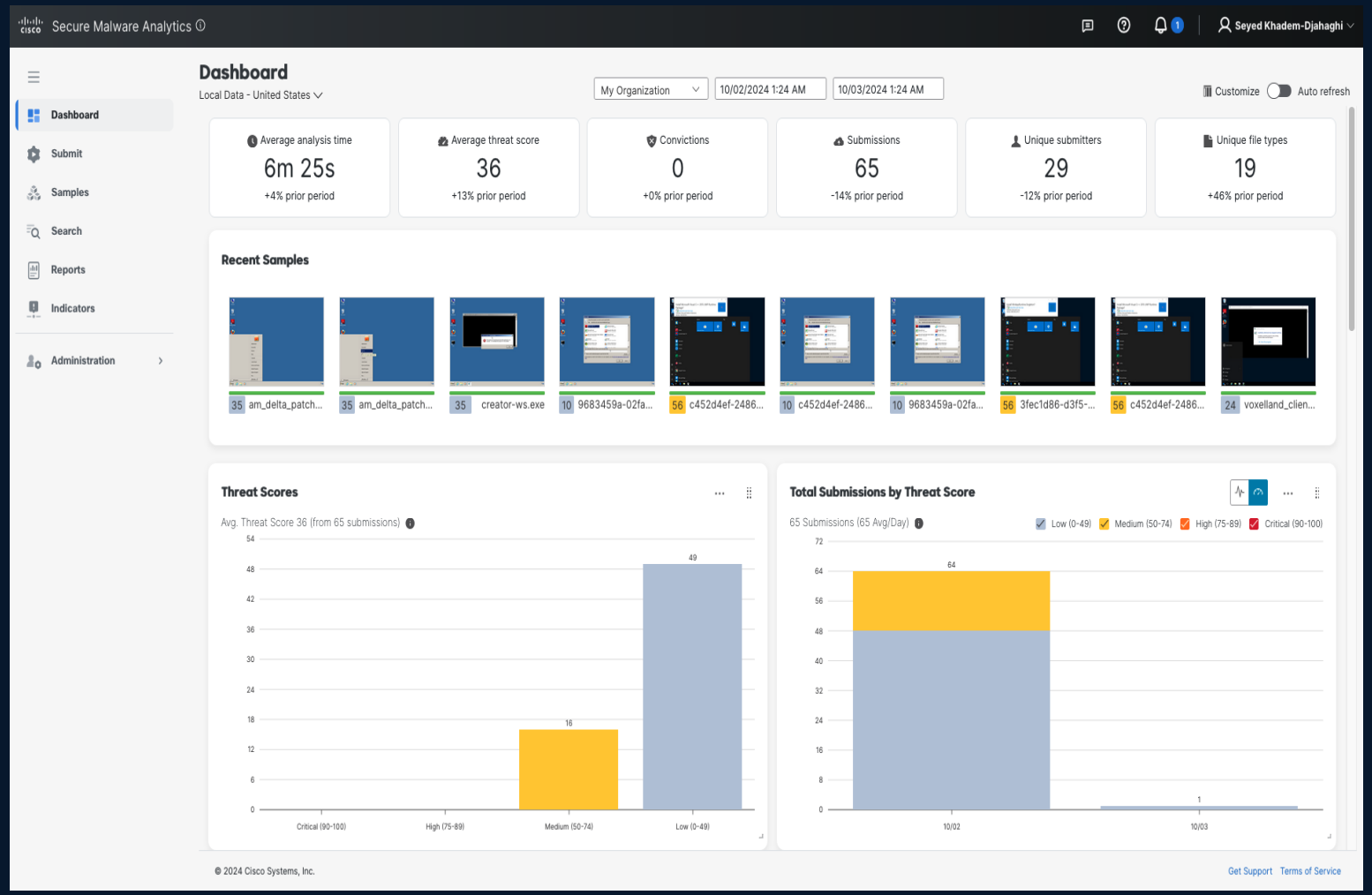


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Cisco Malware Analytics

- Malware analytics analyzes files and URLs in a sandbox to identify malicious IOC's
- The Splunk integration ingests and maps that output of the analysis done by the submission to the sandbox to the Malware CIM data model

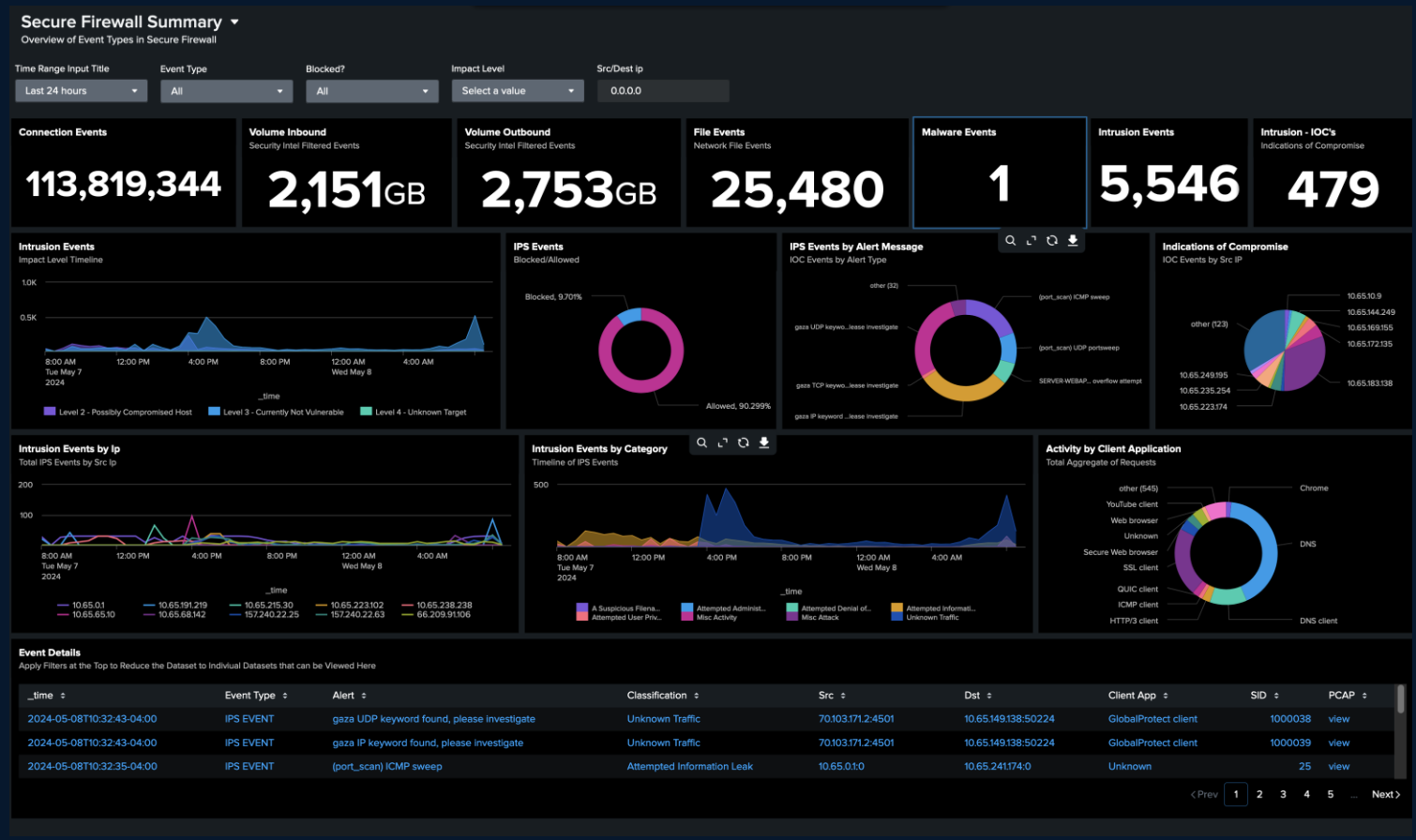


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Secure Endpoint

- Secure Endpoint helps protect customers systems from getting infected my malware
- The Splunk integration maps the alerts generated by Secure Endpoint to the Alert CIM model malware related activity is mapped to the Malware and other CIM models
- Ability to filter high fidelity events in the app

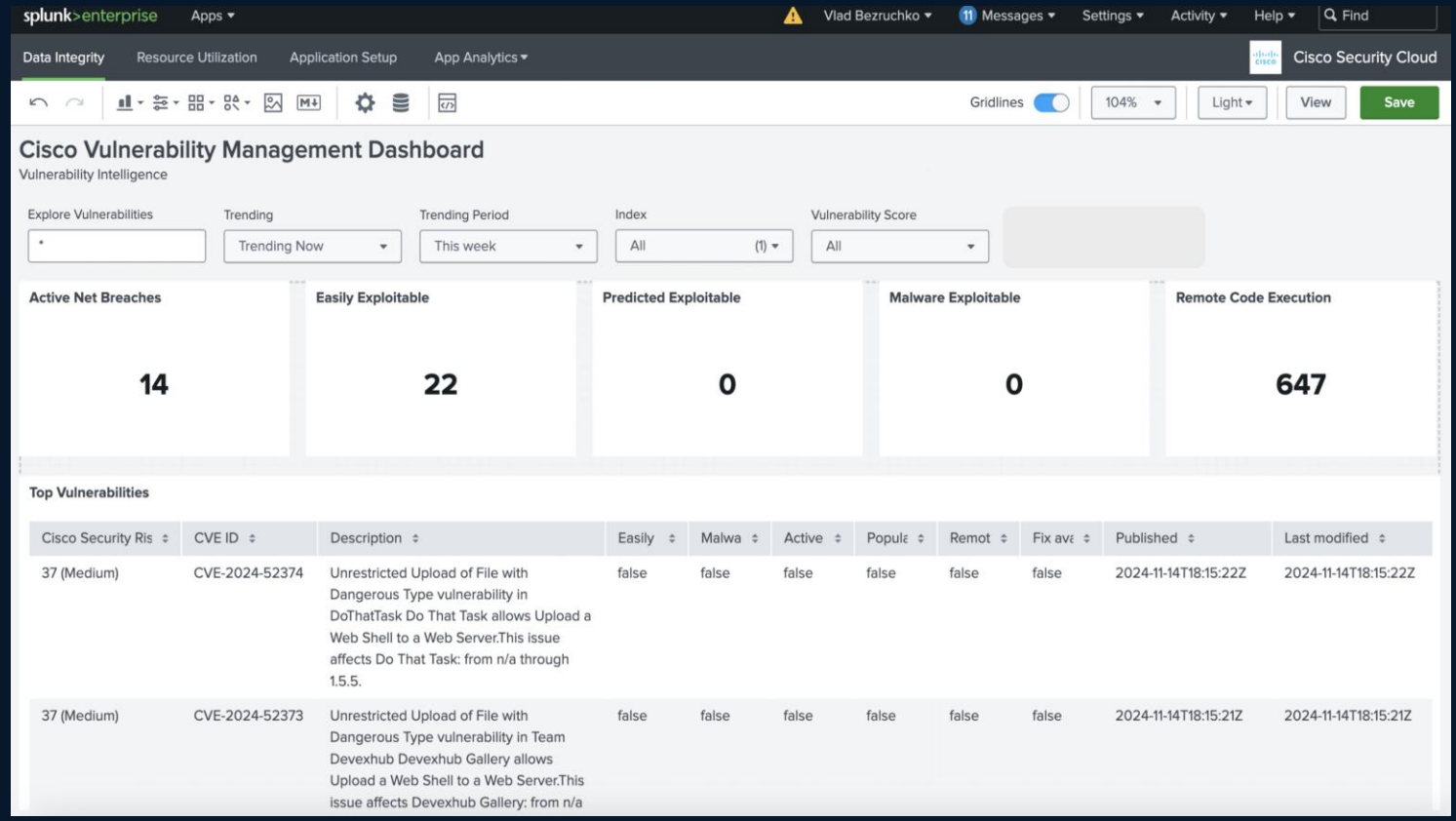


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Kenna VI

- Kenna Vulnerability Intelligence provides context to CVE about their risk
- The Splunk integration ingest vulnerability intelligence into Splunk and maps it to the Vulnerability CIM model
- Dashboards provide a list of vulnerabilities and their score that are being chatted, researched or in the new
- Ability to browse the vulnerabilities being reported and search on the ones that you want more information on

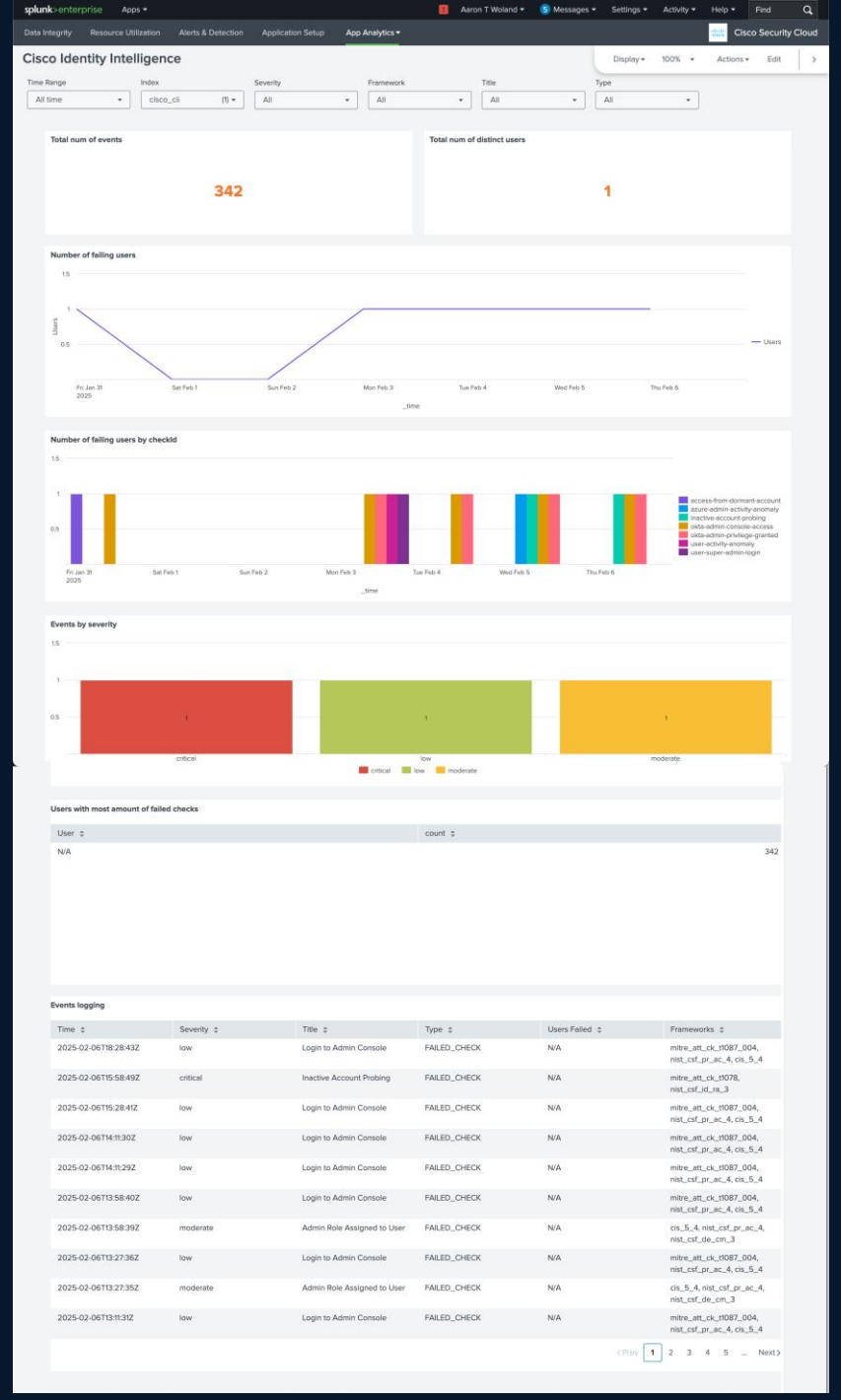


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Identity Intelligence

- Identity Intelligence provides a full picture of identity activity identifying risky accounts
- Identity high-risk access attempts and resources and privileges that are associated with users
- The Splunk integration ingest alerts from Identity Intelligence into Splunk and maps it to the CIM model

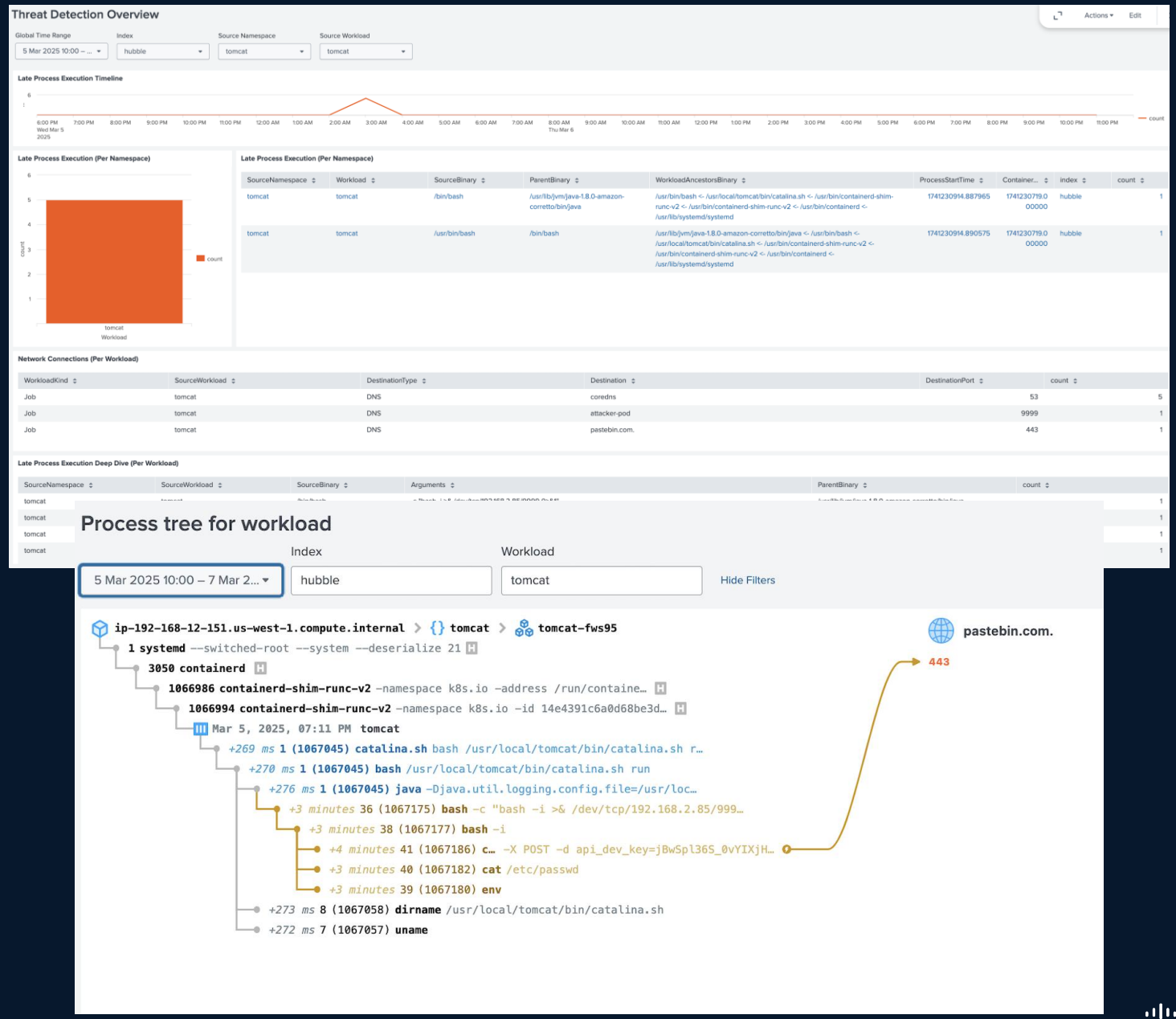


© 2025 Cisco and/or its affiliates. All rights reserved.

Now Available

Isovalent Runtime Security

- Isovalent provides deep, kernel level runtime and network visibility into any system where the eBPF-based Tetragon agent is running on:
  - Kubernetes workloads, Linux VMs, Windows VMs
- This data supports Threat Detection and Incident Investigation Workflows via Splunk dashboards:
  - Late Process Executions
  - Shell Executions
  - Container Escapes
  - Detecting new external DNS names
- The data will be mapped to CIM Endpoint model



© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Continue your education

Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you


CISCO