

AI-Powered SOC: Cisco Sec-8b and AIPOD in Action

cisco Live !

Daria Margherita Maggi
Consulting Engineer
Cisco

Stefano Gioia
EMEA Solution Architect
Cisco

Webex App

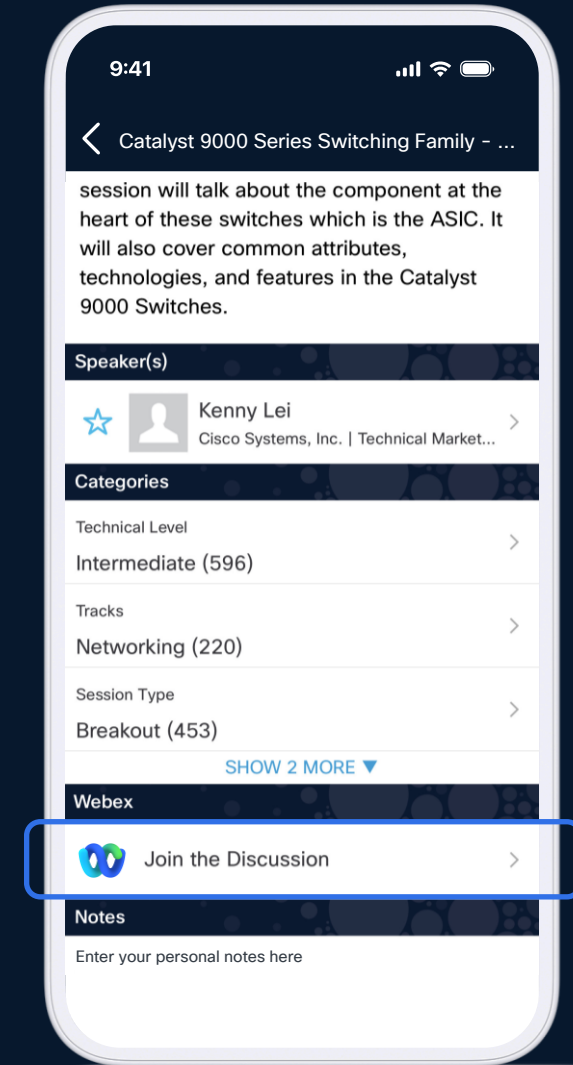
Questions?

Use Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events 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 February 27, 2026.



Daria Margherita Maggi

Adversarial Machine Learning with generative AI researcher (before it was cool :))

CX Security Consulting Engineer, specialized in military and highly regulated sectors.

Cat mom.



Stefano Gioia

25+ experience in Industry:
Ericsson, Oracle, Cisco since 2017

Observability, AI and
Virtualization expert.

BBQ Judge



Agenda

- 01 Introduction
- 02 LLMs and SOC troubles
- 03 Meet the Sec-8B Model
- 04 Sec-8B Model Use Cases
- 05 Meet the Cisco AI POD
- 06 Sec-8B in Action: Demo
- 07 Closing and Q&A

"Safe Harbor" Statement

This session is not...

Level 200, 300

It is Level 100 so it will be introducing concepts and practices.

Big Model Discussion

Mostly on-premise or air-gapped scenarios, with limited computing power – small language models only.

Vendor comparison

We are not comparing us versus other.

What you will get from this session ...

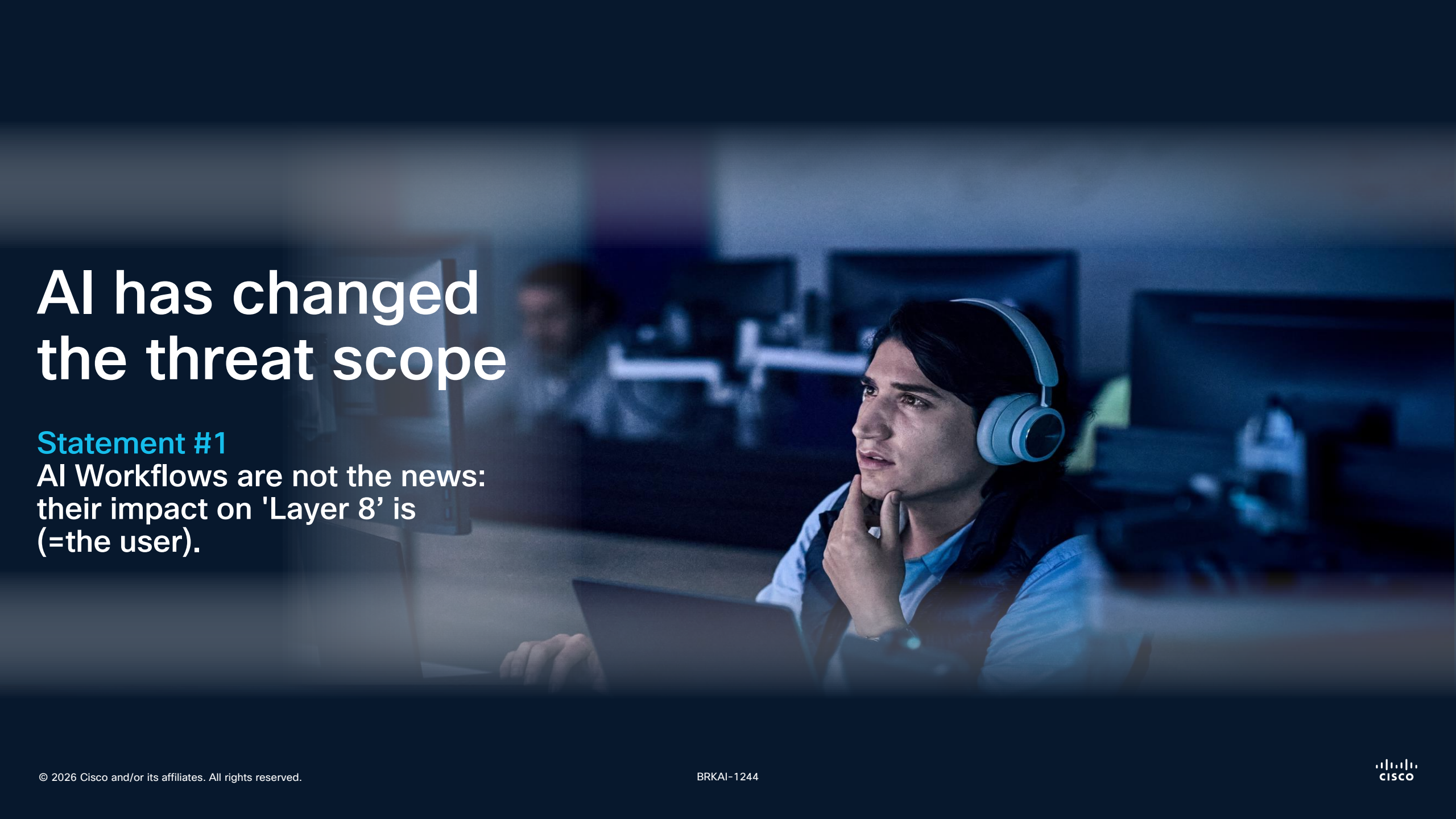
How has AI transformed the way SOC manage and respond to threats.

How you can accelerate SOC process with Cisco Foundation AI model(s).

Cisco AI POD as the perfect platform to host Cisco Sec-8B Security Model.



LLMs and SOC troubles

A man with dark hair, wearing a light blue shirt and a dark vest, is seated at a desk in a dimly lit office. He is wearing large, light blue over-ear headphones and is looking intently at a laptop screen. His right hand is resting on his chin, suggesting deep thought or concentration. In the background, other office desks and monitors are visible but out of focus, creating a sense of a busy, modern workspace.

AI has changed the threat scope

Statement #1

AI Workflows are not the news:
their impact on 'Layer 8' is
(=the user).

AI has changed the threat scope

Statement #2

LLM security capabilities are comparable to, or exceeding, the reactive reflexes of a typical Tier 1 SOC analyst.

AI has changed the threat scope

Statement #3

Mindset shift from adversarial to
offensive security.

What AI Can do today?

Statement #1

Task summarization, prioritization, follow up action suggestion (hindered by lack of internet access).

What AI Can do today?

Statement #2

Mislead the user (model sycophancy).

And SOC?

Statement #1

Generale purpose LLMs make mistakes due to largeness.



And SOC?

Statement #2

SOC requires specific skills – among which hierarchical thinking, with a low margin for hallucinations.

Hierarchical thinking = cause-> effect chains on multiple levels of depth.



And SOC?

Statement #3

Fine tuning a large language model is less efficient than having more agents cooperating.



AI in the SOC: Powerful Tool – Risky if Misplaced



Allow internet browsing:

SLM might leak data or download malware



Retrieval Augmented Generation (RAG)

Expensive, and difficult, you need somewhere to host it.



Vendor lock-in:

Models differ, cloud hosting might be expensive, unpredictable, or outright impossible

Meet the Foundation-Sec-8B Model



“Cisco’s acquisition of Robust Intelligence may be one of its best buys in recent years. It provides the automated red-teaming capability in the company’s AI Defense platform, and it supports the newly launched **Foundation AI open-source reasoning model** that is **purpose-built for enhancing security applications.**”

<https://www.forbes.com/sites/moorinsights/2025/05/07/rsa-conference-2025-highlights-insights-and-companies-to-watch/>

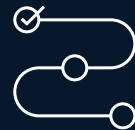
Foundation AI Background



Spun out from the **Robust Intelligence** team



Established in **March 2025** with a newly defined charter



Core mission: build **bleeding edge** AI for cybersecurity and cybersecurity for AI



Highly experienced team with decades of combined AI and security expertise

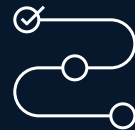
Foundation AI OSS Security Model Background



Open-weight, **8B parameter** model, Cisco's first domain-specific LLM for cybersecurity



Pre-trained on **Llama-3.1 8B**



Designed from the ground up for security workflows



Trained on a curated corpus of **CVEs, CWEs, MITRE ATT&CK**, threat-intel reports, red-team playbooks, tooling docs and compliance standards, delivering analyst-ready context with fewer hallucination

Development Highlights

Building infrastructure for model pre-training, finetuning, and model evaluation



Building a novel data collection system

- Web scrapers visited over 160 million domains and 60 large security specific sources, yielding over 4 TiB of raw unfiltered data.
- Raw data is then passed through language, quality, and relevancy filters before being deduplicated and undergoing PII removal.
- Pre-training on 7B high-quality cybersecurity tokens.



Handpicked special sources from trusted security and research domains:

- Cyber Threat Intel: MITRE ATT&CK, CVE, CWE, NVD, OWASP, GitHub Advisories
- Incident Response: NIST CSRC guides, SOC/IR playbooks, RFCs, PRs, postmortems
- Cloud & Tooling Docs: GCP, Azure, Kubernetes
- Research & Textbooks: ArXiv, Open Textbooks
- Standards & Policy: HIPAA, SOC2, public regulations

Cisco Foundation-AI: Built in 3 Forms, Designed for Every Need



Foundation-Sec-8B



**Foundation-Sec-8B
Instruct**



**Foundation-Sec-8B
Reasoning**

Understanding Foundation AI Models: Instruct and Reasoning Overview

Models Everywhere

Foundation Model

Large, pre-trained AI on diverse data;

Flexible for many tasks.

Instruct Model

Fine-tunes foundation models to follow user instructions better, improving task-specific responses.

Reasoning Model

Enables complex, multi-step logical thinking for advanced analysis and decision-making in specialized domains.

Ok, where to get the Foundation AI Sec-8b models?

 **Hugging Face**

Models

Datasets

Spaces

Community

Docs

Enterprise

Pricing

Log In

Sign Up

 **Cisco Foundation AI** Team Company

<https://fdtn.ai/>

[fdtn_ai](#)

Activity Feed

Follow 472

AI & ML interests

Cybersecurity x AI

Recent Activity

 anuvellore published a model about 13 hours ago

[fdtn-ai/Foundation-Sec-8B-Reasoning-Q8_0-GGUF](#)

 anuvellore published a model about 13 hours ago

[fdtn-ai/Foundation-Sec-8B-Reasoning-Q4_K_M-GGUF](#)

 edli authored a paper 2 days ago

[Llama-3.1-FoundationAI-SecurityLLM-Reasoning-8B Technical...](#)

View all activity

Papers

 Llama-3.1-FoundationAI-SecurityLLM-Reasoning-8B Technical Report

< fdtn-ai's models 11 >

Sort: Recently updated

 fdtn-ai/Foundation-Sec-8B-Reasoning

Text Generation • ... 8B • Updated 5 days ago • 553 • 13

 fdtn-ai/Foundation-Sec-8B-Reasoning-Q8_0-GGUF

Text Generation • ... 8B • Updated 7 days ago

 fdtn-ai/Foundation-Sec-1.1-8B-Instruct

Text Generation • ... 8B • Updated Nov 20, 2025 • 2.51k • 13

 fdtn-ai/Foundation-Sec-8B-Instruct-Q8_0-GGUF

Text Generation • ... 8B • Updated Aug 26, 2025 • 444 • 5

 fdtn-ai/Foundation-Sec-8B-Q8_0-GGUF

 fdtn-ai/Foundation-Sec-8B-Reasoning-Q4_K_M-GGUF

Text Generation • ... 8B • Updated 7 days ago • 1

 fdtn-ai/Foundation-Sec-1.1-8B-Instruct-Q4_K_M-GGUF

Text Generation • ... 8B • Updated Dec 3, 2025 • 145

 fdtn-ai/Foundation-Sec-1.1-8B-Instruct-Q8_0-GGUF

Text Generation • ... 8B • Updated Nov 19, 2025 • 167 • 3

 fdtn-ai/Foundation-Sec-8B-Q4_K_M-GGUF

Text Generation • ... 8B • Updated Aug 26, 2025 • 166 • 2

 fdtn-ai/Foundation-Sec-8B-Instruct

© 2026 Cisco and/or its affiliates. All rights reserved.

BRKAI-1244



Sec-8B Model Use Cases

Foundation security models enable the SOC



SOC Teams are overwhelmed by:

- False Positives
- Manual Repetitive Triage
- Fragmented Tools



Model is ready to embed across the SOC lifecycle:

- Advance Threat Detection & Investigation
- Adversary Behavior & Threat Intelligence
- Security Posture & Vulnerability Management
- Proactive Defense & Engineering Enablement



Model is being adopted in Pilots across Cisco:

- Splunk
- Cisco CSIRT
- Cisco XDR

What's difference with other models?

You are a senior SOC analyst assisting with incident triage. Your task is to read the incident metadata and alert logs, and provide a clear summary of what occurred. Instructions:

- Highlight the sequence of events (inferred from timestamps).
- Think deeply about cause and effect and how artifacts relate to one another
- Mention key attack techniques used (if inferable from logs)
- Describe how the attack began and progressed
- Use clear and concise language appropriate for L1/L2 analysts

incident_id: INC-1024,

type: Unauthorized Access,

severity: High

timestamp: 2025-04-09T10:30:00Z

2025-04-09 10:00:23 - Alert: 5 failed login attempts for user 'alice' on host 'WS123'

2025-04-09 10:05:10 - Alert: Suspicious PowerShell execution on 'WS123' by 'alice' (malicious script blocked)

2025-04-09 10:10:45 - Alert: Process dumping LSASS memory on 'WS123' (possible credential theft)

2025-04-09 10:15:00 - Alert: Successful login of 'alice' to server 'DC1' from host 'WS123'

Summarize what happened in this incident in a few sentences

What's difference with other models?



mistral

Temporary Chat

Here's a summary of the incident **INC-1024**:

Sequence of Events:

1. **2025-04-09 10:00:23**: Suspect made 5 failed login attempts for user 'alice' on host 'WS123'.
2. **2025-04-09 10:05:10**: With failed login attempts complete, the suspect executed a malicious powershell script.
3. **2025-04-09 10:10:45**: The suspect attempted to dump LSASS memory on 'WS123', likely trying to steal credentials.
4. **2025-04-09 10:15:00**: The suspect successfully logged into the domain controller 'DC1' using 'alice's credentials'.

Key Attack Techniques Used:

- Credential dumping. The attack started with brute force login attempts. After failing, the attacker tried to execute a malware but caused it to be blocked.
- Credential Access: Attempted to dump LSASS memory to extract credentials which may have worked for the moment since they successfully used the account.

Incident Progression:

- The attacker began with a brute-force attempt to gain access to the account. They then executed a suspicious PowerShell script, likely to bypass security measures. After likely failing to get credentials using brute force the attacker used a credential access method to get credentials. Using those, the attacker successfully accessed the domain controller 'DC1'.
The potential motive: Domain Admin access. Patching the access any server using Alice's account would be essential.

Suspicious behaviors that may have indicated an attacker:

- 5 failed login attempts for the same user
- Suspicious PowerShell execution in a timeframe to security logs.
- Using a legitimate account to attempt additional escalation.
- Unusual remote logins for a user immediately after credible access.

Likely the attacker wanted to get an initial foothold into the system and quickly tried credential-based exploits to elevate their access to administrative-level controls in a timeframe of about 15 minutes



What's difference with other models?

ChatGPT ▾

✦ Get Plus ✕

incident_id: INC-1024,
type: Unauthorized Access,
severity: High
timestamp: 2025-04-09T10:30:00Z
2025-04-09 10:00:23 - Alert: 5 failed login attempts for user 'alice' on host 'WS123'
2025-04-09 10:05:10 - Alert: Suspicious PowerShell execution on 'WS123' by 'alice' (malicious script blocked)
2025-04-09 10:10:45 - Alert: Process dumping LSASS memory on 'WS123' (possible credential theft)
2025-04-09 10:15:00 - Alert: Successful login of 'alice' to server 'DC1' from host 'WS123'
Summarize what happened in this incident in a few sentences

📄 ✎

Incident Summary (INC-1024 – Unauthorized Access, High Severity)

The incident began on **2025-04-09 at 10:00:23** with **multiple failed login attempts** against user **alice** on workstation **WS123**, suggesting a possible **brute-force or credential-guessing attempt**. Shortly after (**10:05:10**), **suspicious PowerShell activity** was detected and blocked on the same host, indicating an attempted **malicious script execution**. At **10:10:45**, the system logged **LSASS memory dumping** on WS123, a strong indicator of **credential dumping** (e.g., MITRE T1003).

By **10:15:00**, the attacker appears to have successfully obtained valid credentials, as **alice successfully authenticated to domain controller DC1 from WS123**, indicating **credential compromise followed by lateral movement**. Overall, the attack likely progressed from initial credential access attempts to post-exploitation activity and unauthorized access to a critical server.

📄 👍 💬 ↗️ ↺ ⋮

⬇️

What's difference with other models?

foundation-sec-8b-reasoning

Eject

2025-04-09 10:15:00 - Alert: Successful login of 'alice' to server 'DC1' from host 'WS123'
Summarize what happened in this incident in a few sentences

foundation-sec-8b-reasoning

Analyze Incident Details

Incident ID: INC-1024

Type: Unauthorized Access

Severity: High

Timeline Summary:

The attack initiated with **failed login attempts** for user 'alice' at 2025-04-09 10:00:23, indicating a brute-force or credential-guessing effort. This was followed by **suspicious PowerShell execution** on host 'WS123' by 'alice' at 10:05:10, suggesting an attempt to execute malicious code. At 10:10:45, the attacker performed a process dump of LSASS memory—a common technique for credential theft—which was blocked by security controls. Finally, successful authentication occurred at 2025-04-09 10:15:00 when 'alice' logged into server 'DC1' from host 'WS123', confirming initial access compromise.

Key Attack Techniques:

1. Credential Access (T1552)

- LSASS dumping to steal credentials.

2. Execution (T1059.001)

- PowerShell for malicious script execution.

3. Initial Access

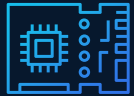
- Successful login after repeated failed attempts implies credential compromise or phishing.

Send a message to the model...

Meet the Cisco AI POD

What's Needed to Run Foundation-AI Sec-8b LLM?

Sec-8B can run on laptop, but we want centralized access and carrier grade reliability



GPU Acceleration

Enables simultaneous inferencing for many users through optimized GPU partitioning and orchestration.



Infrastructure Essential

Modular systems to enable independent scaling of CPUs, GPUs, memory, and storage.



Software and Management

Cloud-based approach that manages multi-tenant AI Workloads with integrated management tools.



Security and Compliance

Compliance frameworks and observability tools ensure secure, resilient operations across all users.

Robust, flexible infrastructure to meet your needs

Data center building blocks



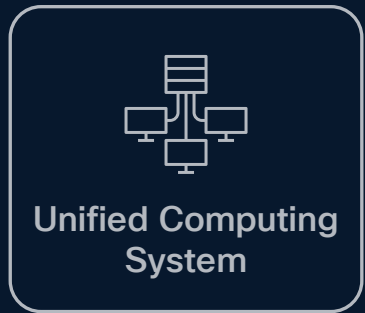
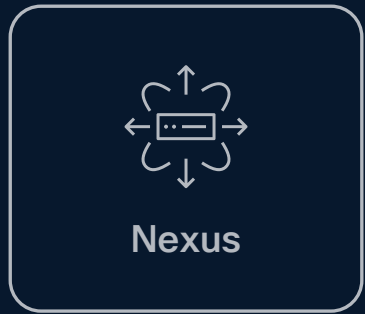
Nexus



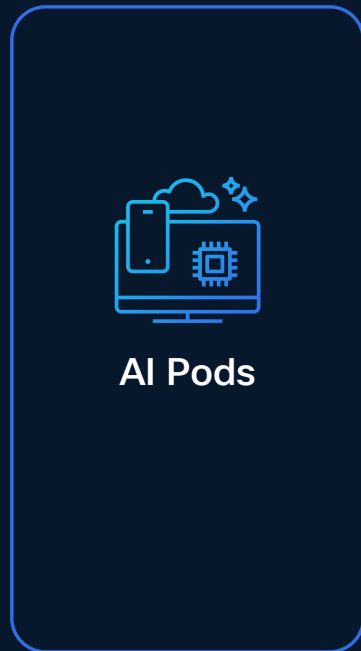
**Unified Computing
System**

Robust, flexible infrastructure to meet your needs

Data center building blocks

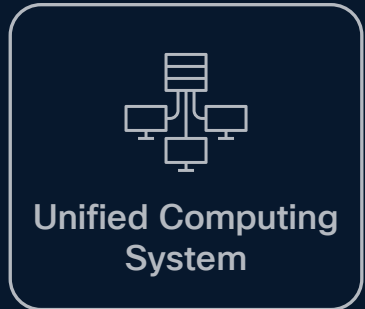
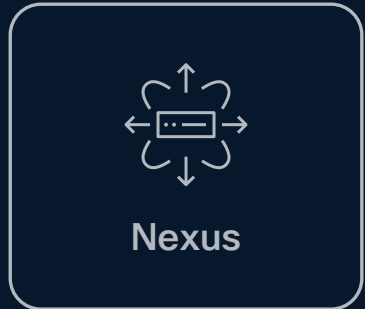


Full stack systems

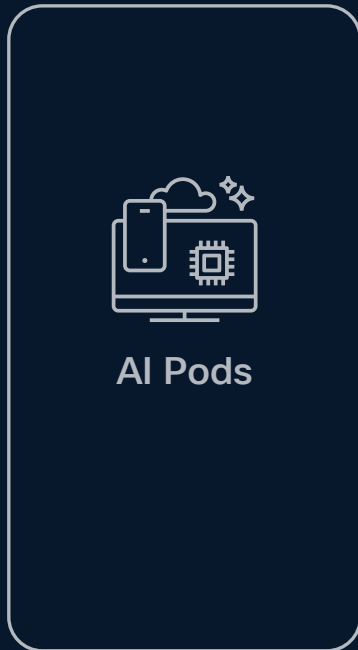


Robust, flexible infrastructure to meet your needs

Data center building blocks



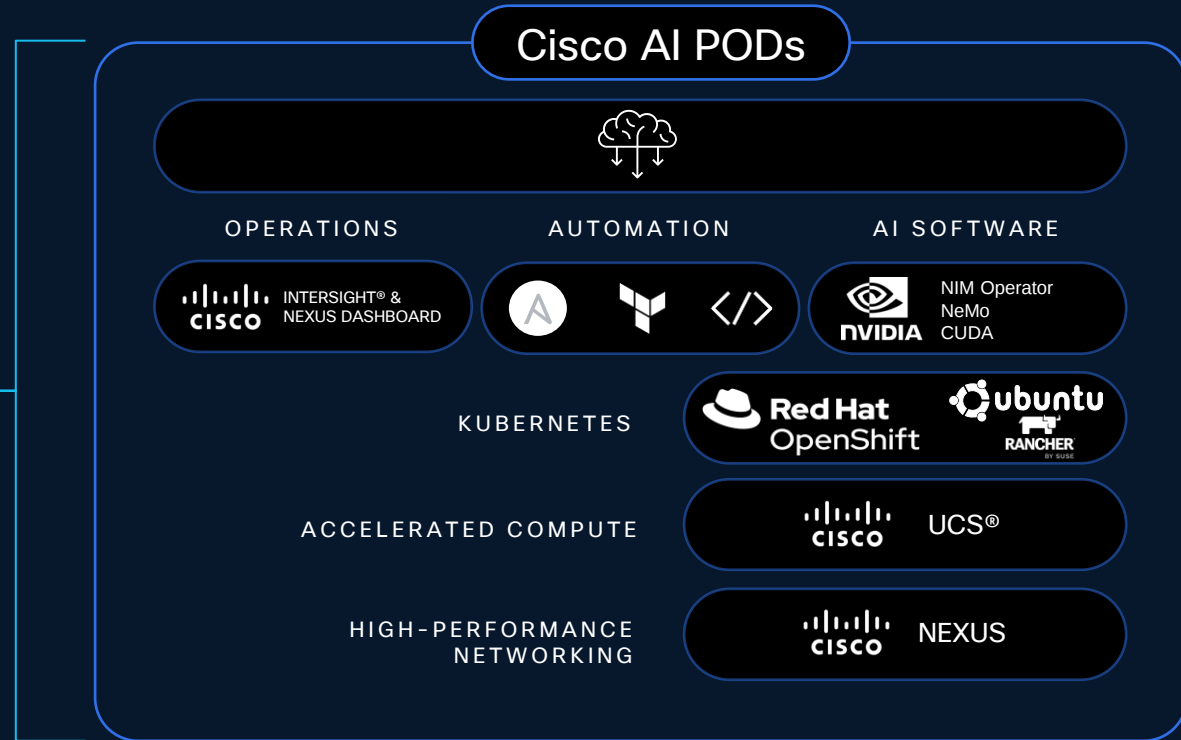
Full stack systems



Training

Optimization

Inferencing



Cisco AI Pod Full Stack System

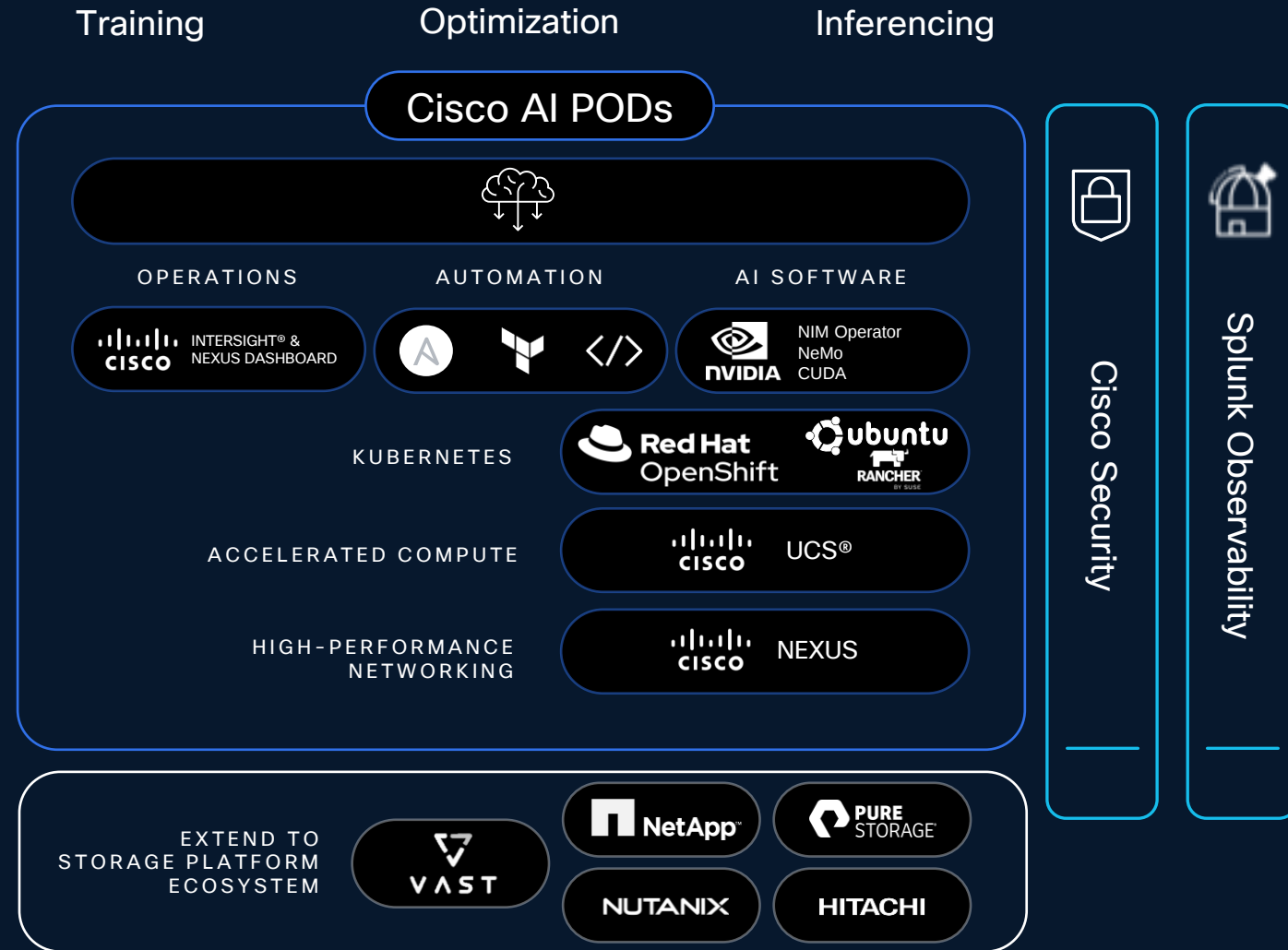
What is an AI POD?

Modular components for flexible adoption

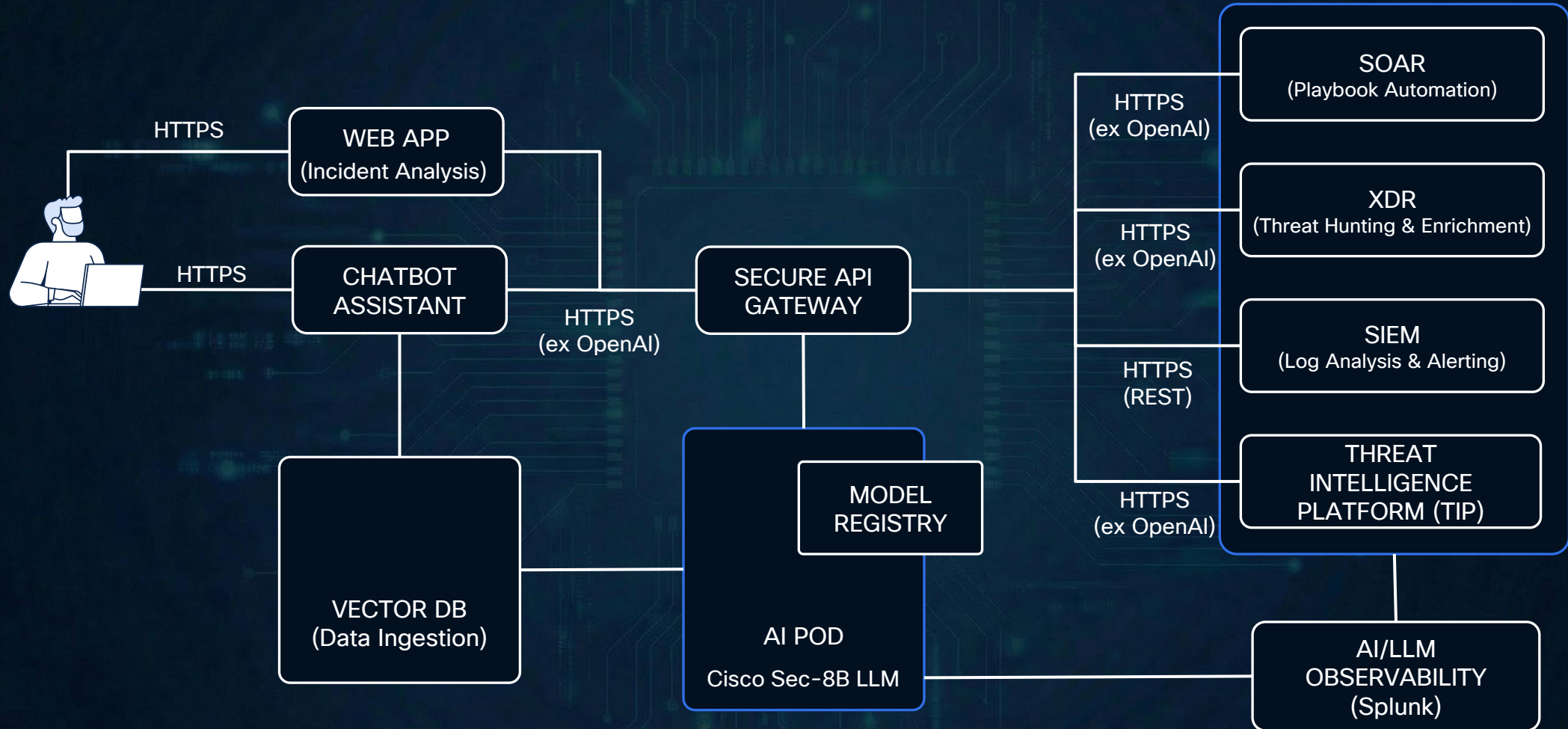
Deploy AI with confidence: CVD

Sizing tools for predictability

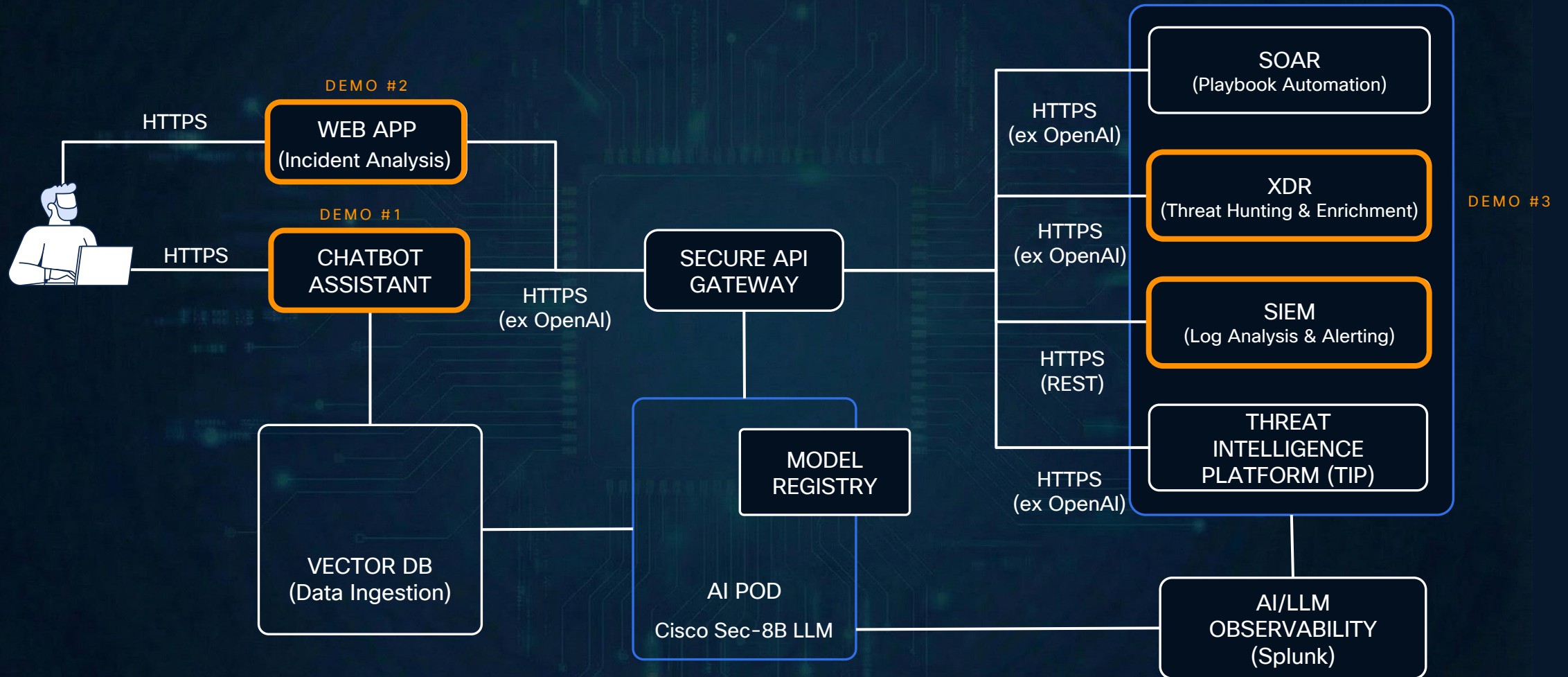
Fully stack by Cisco, including 3rd Party



LLM for SOC: Sample Executive Architecture



LLM for SOC: Sample Executive Architecture

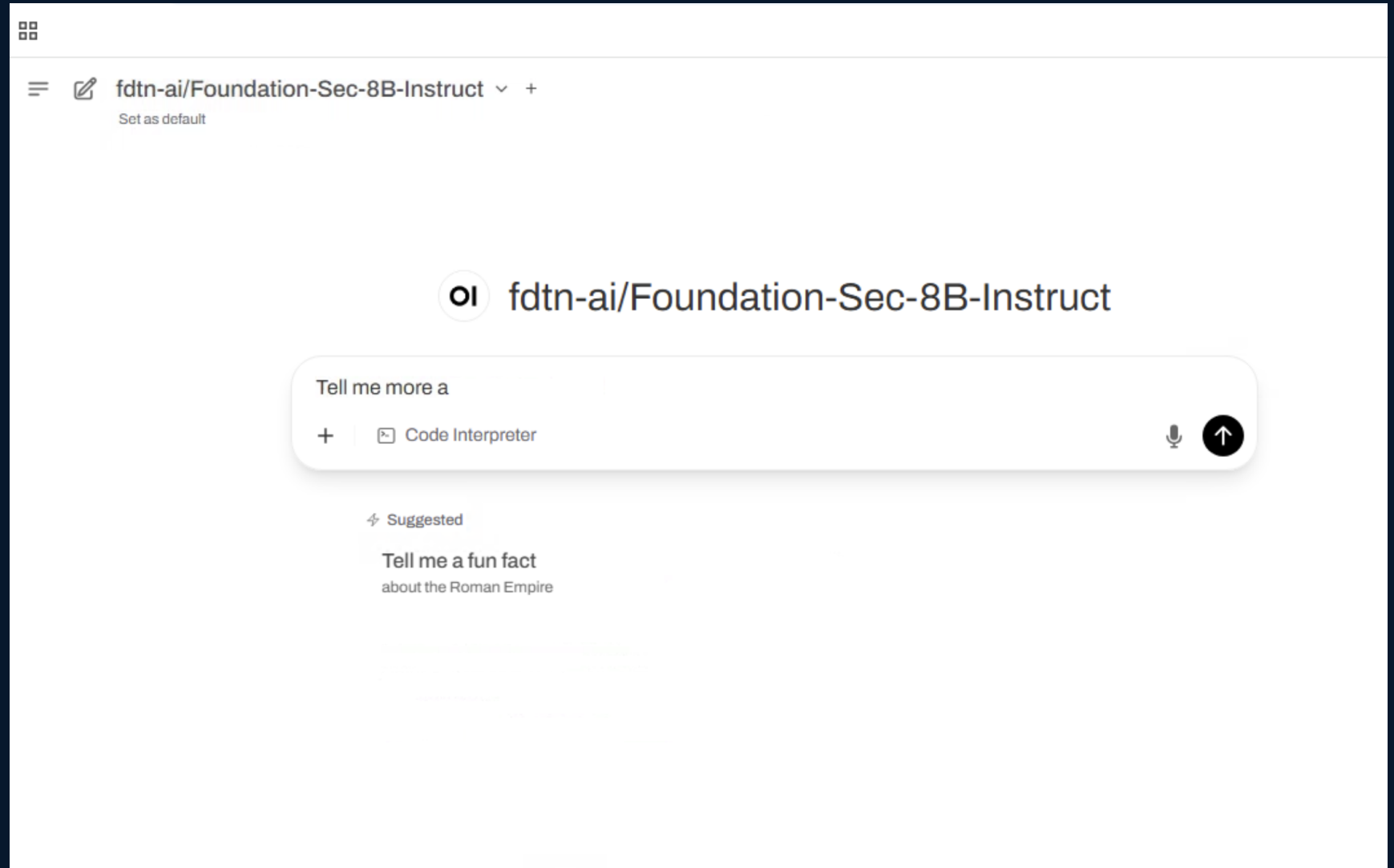


Use Case #1 Demo

Simple Chatbot

Simple Chatbot

More than just a Chatbot: A Security-Native Interface. Unlike general-purpose LLMs, Sec-8b is pre-loaded with the 'DNA' of cybersecurity.



Use Case #2 Demo

Incident Summarization

Incident Summarization

Critical cybersecurity incidents often result in lengthy, complex documentation that is difficult to digest, slowing triage, handoffs, and leadership visibility. The goal is to automatically condense these incident reports into concise summaries tailored to analysts or executives – enabling faster response, clearer communication, and more effective decision-making

Select Incident to Investigate

INC-1024
Domain Controller Compromise

INC-1025
Malicious Email Attack

INC-1026
Cryptomining Attack

CUSTOM Try Your Own!
Try Your Own Incident

Security Alert Timeline

2025-05-12 08:22:11 - Alert: Malicious email attachment 'invoice.docm' delivered to user 'bob' on host 'WS456' (macros disabled)

2025-05-12 08:25:37 - Alert: Word macro executed by 'bob' on 'WS456' (PowerShell download cradle attempted)

2025-05-12 08:26:05 - Alert: Outbound connection from 'WS456' to C2 IP 45.77.12.34 over port 443 (beaconing)

2025-05-12 08:28:45 - Alert: New scheduled task 'Updater' created on 'WS456' launching PowerShell for persistence

2025-05-12 08:31:12 - Alert: LSASS memory read attempt on 'WS456' by 'powershell.exe' (possible credential theft)

Investigation Actions

Note: The first AI request may take up to 60 seconds as the model wakes up from an idle state. Subsequent requests will be much faster.

Generating Summary...

Extract Entities & Tactics

Generate Recommendations

Generate Final Report

© 2026 Cisco and/or its affiliates. All rights reserved.

BRKAI-1244

 cisco

Blackhat Demo - Cybersecurity Incident Analysis

INC-1024

INC-1025

INC-1026

CUSTOM Try Your Own!

Note: The first AI request may take up to 60 seconds as the model wakes up from an idle state. Subsequent requests will be much faster.

Incident Investigation Dashboard

Blackhat Demo - Cybersecurity Incident Analysis

Select Incident to Investigate

INC-1024

Domain Controller Compromise

INC-1025

Malicious Email Attack

INC-1026

Cryptomining Attack

CUSTOM Try Your Own!

Try Your Own Incident

• Security Alert Timeline

2025-04-09 10:00:23 - Alert: 5 failed login attempts for user 'alice' on host 'WS123'

2025-04-09 10:05:10 - Alert: Suspicious PowerShell execution on 'WS123' by 'alice' (malicious script blocked)

2025-04-09 10:10:45 - Alert: Process dumping LSASS memory on 'WS123' (possible credential theft)

2025-04-09 10:15:00 - Alert: Successful login of 'alice' to server 'DC1' from host 'WS123'

Investigation Actions

Note: The first AI request may take up to 60 seconds as the model wakes up from an idle state. Subsequent requests will be much faster.

Use Case #3 Demo

Cisco XDR Integration Example

Enhancing Security Operations with Cisco XDR and Sec-8b-Instruct LLM

Workflow Integration: dedicated XDR workflow to facilitate API queries to Sec-8B running on Cisco AI POD Foundation-sec compute server, transmitting incident content for analysis.

The screenshot displays the Cisco XDR incident response interface. At the top, it shows the incident title "Malicious activity by [redacted]" with a status of "Open: Investigating" and a count of "570". Below this, it indicates the incident was "Reported by Cisco XDR Analytics on [redacted]". A brief description states: "The incident occurred on [redacted], however, the progression through the kill-chain **could not be determined**. The incident included **16 IP Addresses, 1 Device** and **2 Hostnames**. AI-generated".

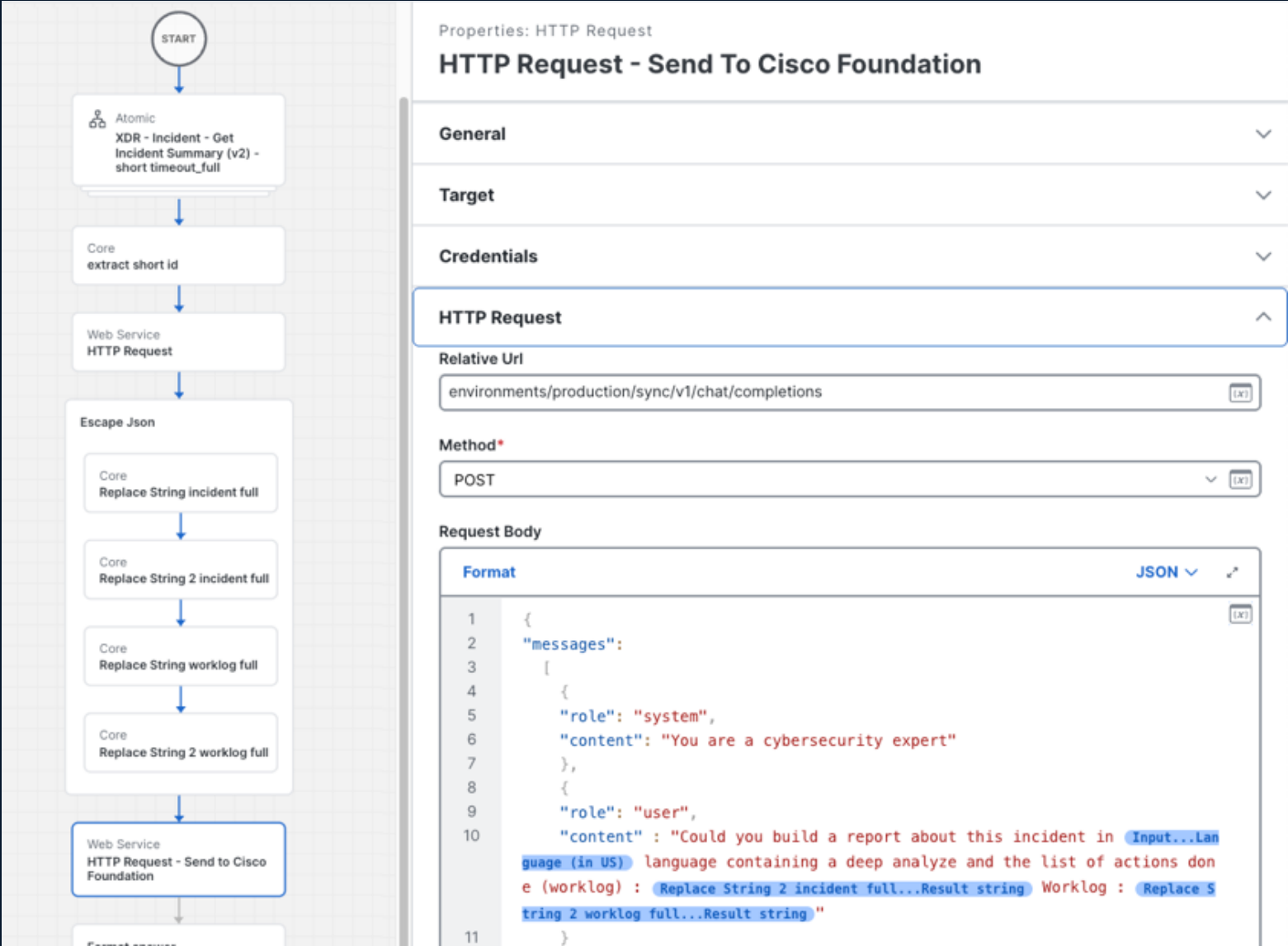
The interface includes a navigation bar with tabs: Overview, Detection, **Response**, Evidence, Worklog, and Report. On the left, a sidebar lists response stages: Identification, Containment, Eradication, and Recovery. The main content area under the "Response" tab shows a list of tasks:

- Identify the domain for IPs (DNS logs)** (Status: Complete) - Identify the domain for IPs by querying DNS log in splunk.
- Identify Location and Purpose** - Identify in which room or avenue endpoints are located and the lab name.
- Confirm Incident** - Update the incident status to "Incident Reported" and, if the incident has assignees start a chat room for triage and collaboration.
- Document and Notify** - Create an incident ticket with the appropriate parameters and contextual incident information.
- Endace PCAP Enrichment** - Fetch a PCAP of specified IP address. Automation workflow will add a link to the PCAP in the worklog note.
- Cisco Foundation AI - Analyze the incident** (Status: Running) - Ask Cisco Foundation AI to Analyze the incident.
- Cisco Foundation AI - Custom Question about Incident** - Ask Cisco Foundation AI a custom question about the incident.

At the bottom right, there is a "Back" button and a blue circular icon.

Workflow Setup

Workflow Integration: A dedicated XDR workflow was established to facilitate API queries to our Foundation-sec model running on Cisco AI POD, transmitting incident content for analysis



Playbook Integration

Playbook Integration: The model was further integrated into XDR as an identification playbook. This allowed security analysts to initiate an immediate analysis of any incident by selecting "Ask Cisco Foundation AI to Analyze the incident" directly from the incident view

The screenshot displays the Cisco XDR incident response interface. At the top, it shows the incident title "Malicious activity by [redacted]" with a status of "Open: Investigating" and a progress indicator of 57%. Below the title, it states "Reported by Cisco XDR Analytics on [redacted]" and provides a "View detailed description" link. The description mentions that the incident occurred on [redacted] and that the progression through the kill-chain could not be determined, including 16 IP addresses, 1 device, and 2 hostnames. The interface includes tabs for Overview, Detection, Response (selected), Evidence, Worklog, and Report. On the left, a sidebar lists the playbook stages: Identification, Containment, Eradication, and Recovery. The main content area shows the "Response" stage with a list of tasks: "Identify the domain for IPs (DNS logs)" (Completed), "Identify Location and Purpose" (Pending), "Confirm Incident" (Pending), "Document and Notify" (Pending), "Enforce PCAP Enrichment" (Pending), "Cisco Foundation AI - Analyze the incident" (Running), and "Cisco Foundation AI - Custom Question about Incident" (Pending). Each task has a brief description of its purpose. A "Back" button is visible at the bottom right.

- ☰
- Control Center

>
- Incidents

>
- Investigate

>
- Intelligence

>
- Automate

>
- Assets

>
- Client Management

>
- Administration

>

Incidents

197 Incidents

11 New Incidents

1 Open Incident

15 Unassigned Incidents

🔍 Search

🕒 Last year ▼

☐ Hide closed incidents

🏷️ Filters

5 results

[Reset all](#)

▼ 1 Applied Filter

☐	Priority	Name	Sources	Created ↕	Assigned	Status	⚙️
☐	210	Malicious IP activity by 10[.]220[.]250[.]37	Cisco Secure Firewall via Splunk	2025-12-10T09:33:22.010Z	IB JB	Closed: Confirmed Threat ▼	...
☐	210	Malicious activity associated with 195[.]58[.]49[.]249	Cisco Secure Firewall via Splunk	2025-12-10T08:37:11.303Z	JB	Closed: Confirmed Threat ▼	...
☐	210	Cisco SFW - IP Malicious	Cisco Secure Firewall via Splunk	2025-12-10T08:27:14.803Z	JB	Closed: Confirmed Threat ▼	...
☐	210	Malicious IP activity by 195[.]58[.]49[.]249	Cisco Secure Firewall via Splunk	2025-12-10T07:37:22.694Z	JB	Closed: Confirmed Threat ▼	...
☐	680	Secure client overflow attempt by SERVER-MYSQL	Cisco Secure Firewall via Splunk	2025-12-08T09:57:41.769Z	JB	Closed: Confirmed Threat ▼	...

Use Case #4 Demo

Zero-Shot Security Classification

Filter on labels: {Malware Activity, Data Exfiltration Attempt, Phishing/Social Engineering, Unauthorized Access, Denial of Service (DoS), Insider Threat, Vulnerability Scans}					
Filter on labels="Malware Activity&&Data Exfiltration Attempt&&Phishing/Social Engineering&&Unauthorized Access&&Denial of Service (DoS)&&Insider Threat&&Vulnerability Scans"					
10 PM)	No Event Sampling ▾				
					predicted_Label ▲
ess,192.168.1.75,,file_system,medium,"User 'mary.smith' accessed a highly restricted HR salary spreadsheet (salary_data.q4.xlsx) outside of ours."					Data Exfiltration Attempt
113.10,10.0.0.50,web_access,high,"Unusually high number of HTTP GET requests (5000 req/sec) from single external IP 203.0.113.10 targeting our website."					Denial of Service (DoS)
rt,192.168.1.100,,system,high,"New executable 'cryptominer.exe' detected and launched from a temporary directory by 'admin_svc' account."					Malware Activity
200,intrusion_detection,critical,"IDS alert: ET POLICY Outbound SSL to self-signed certificate. Possible malicious encrypted tunnel."					Malware Activity
10.0.0.150,172.217.160.142,network,critical,"High volume of outbound connections from internal server 10.0.0.150 to external IP address 172.217.160.142 (Google Cloud). Affected services include database replication and backup agents."					Malware Activity
,192.168.1.80,,email,medium,"Internal user 'jane.doe' sent an email with subject 'Urgent: Payroll Update' containing a link to an external site (http://example.com/payroll-update.php) to 200 internal recipients."					Phishing/Social Engineering
.168.1.90,,web_proxy,medium,"User 'bob.jones' attempted to access a gambling website (www.gamblingsite.com) which is explicitly blocked by corporate policy."					Policy Violation
d,192.168.1.50,,authentication,high,"Multiple failed login attempts for user 'john doe' from IP 192.168.1.50 within 60 seconds. Brute force attack suspected."					Unauthorized Access
connect,8.8.8.8,,vpn_access,high,"VPN connection from 'external_user' using a compromised credential from an unusual geographic location (Russia)."					Unauthorized Access
.1.200,10.0.0.0/24,network_scan,low,"Automated network scanner (Nessus) initiated a full port scan across the entire production subnet 10.0.0.0/24. No vulnerabilities detected."					Vulnerability Scan

Closing and Q&A

Empower Your SOC with AI-Driven Security



Experience Sec-8b:

- Free to try, easy to run on your laptop, or at scale



Enterprise-Ready Deployment:

- Run on Cisco Secure AI Factory; delivers unmatched reliability and security
- Flexible GPU support—NVIDIA or AMD



Partner with Cisco:

- Experiment, innovate and strengthen your defense
- Cisco experts are ready to support your AI security journey

Stay ahead—secure your future with Cisco AI-first solutions

Where to go next?

This cookbook repository helps you get started with using models developed by Cisco Foundation AI team.

It will cover many security related use cases, deployment options, practical adaption approaches like finetuning and so forth.



Complete your session surveys



Complete your surveys in the Cisco Events App.



Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions



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



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

Contact us at: damaggi@cisco.com, sgioia@cisco.com

Thank you

CISCO Live !

