

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Simplify the Analyst Experience by Harnessing AI and Machine Learning

Using AI for SecOps Efficiency

Jay Kripalani, Senior Security Solution Architect - Splunk
@jkripala
BRKSEC-2586

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2586>



Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on May 21, 2024 and its most recent report on Form 10-K filed on September 7, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

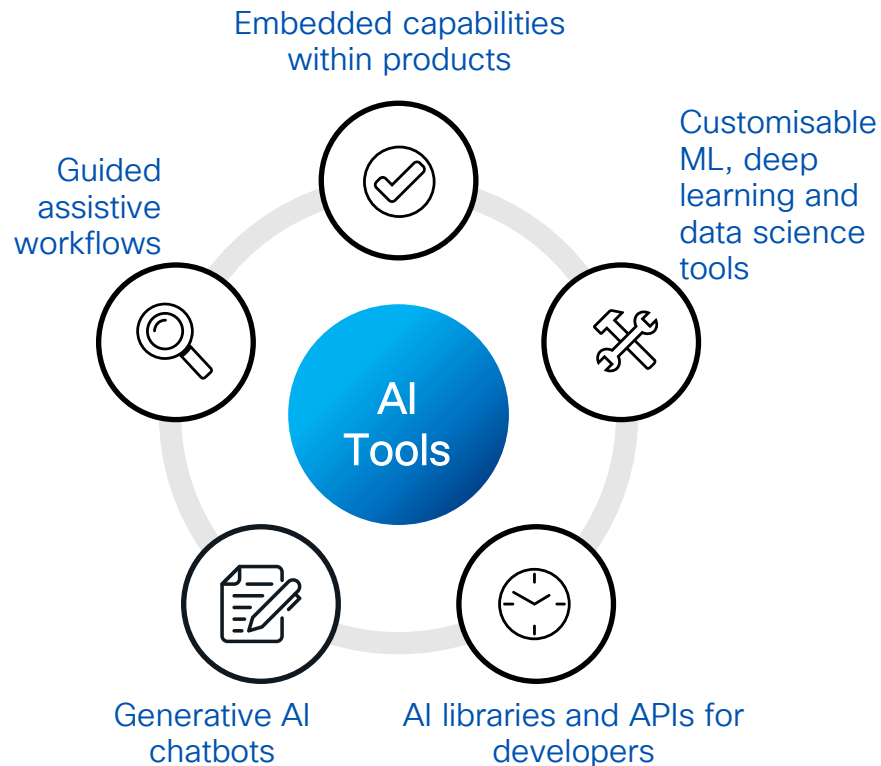
Splunk and Splunk> are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.

CISCO *Live!*



*The Next ~~10~~ Years Will
Be Defined By AI
Adoption*

Splunk's Secret AI-Super Power is Data!



Our AI Product Philosophy

Domain Specific

Human in the Loop

Open and Extensible

Focused on Security and
Observability

Human-assisted AI for
detection, investigation,
and response

Easily integrated with third
party frameworks

How can Splunk help you in your AI journey?

Building AI Models



Help build AI models
on the highest data
quality

Securing and monitoring
AI



Monitor and secure AI
data, infrastructure and
governance

Leveraging AI in Splunk



Improve security and
observability outcomes
with AI

Where are we investing?

Accelerate detection,
investigation and response

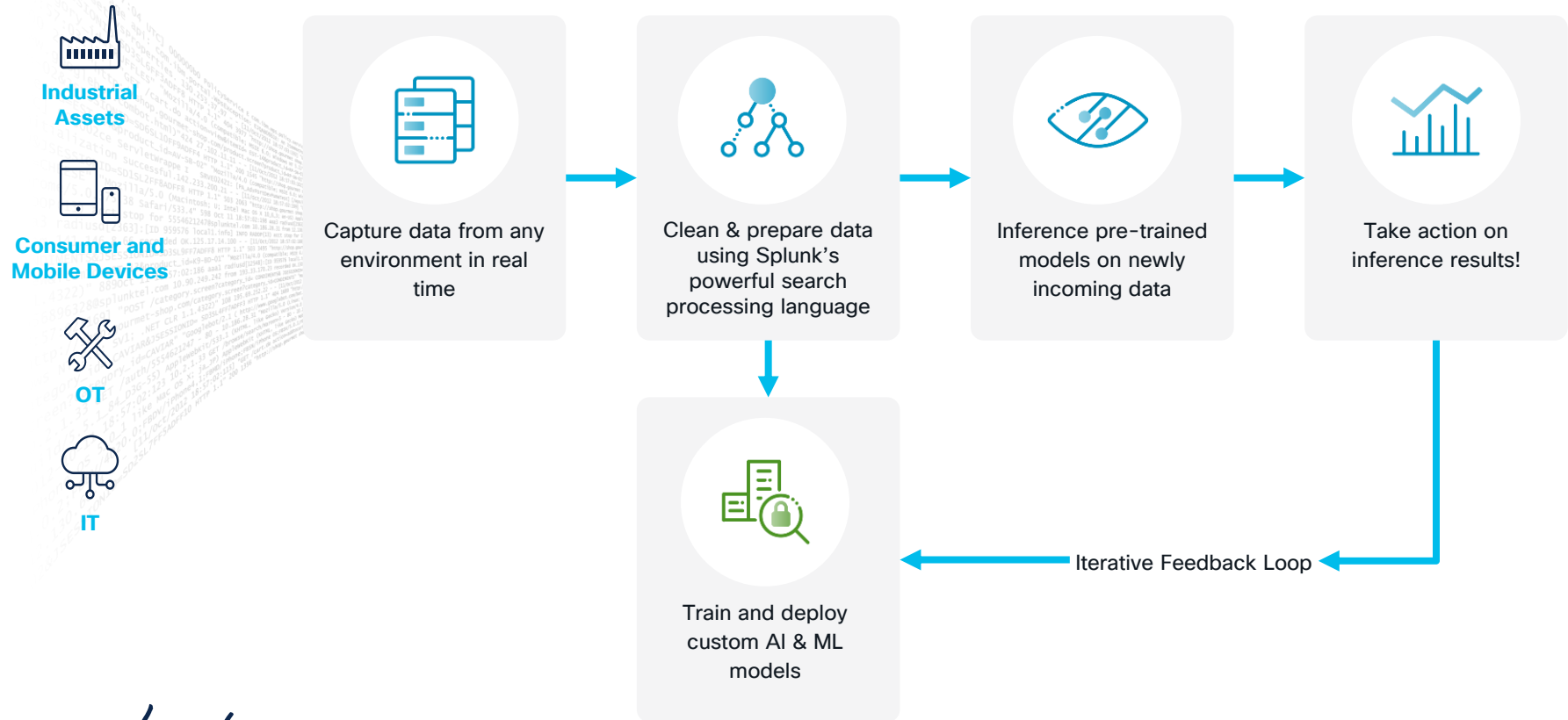
Sense Making

Make sense of the signal to
improve user productivity and
outcomes.

Finding Signals

Find the signal from the noise in
vast amounts of data.

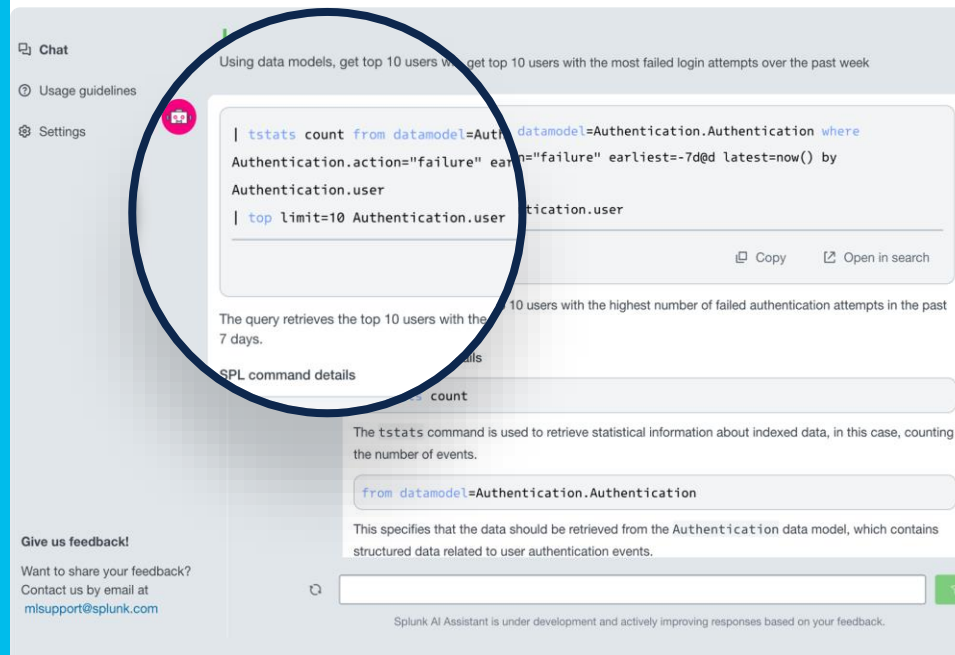
Splunk's Customizable AI & ML Pipeline



New AI Assistant for SPL

Preview in Q1 & GA in Q2

- Upskill new and advanced Splunk users quickly.
- Translate bi-directionally between NL and SPL.



New AI Assistant in Enterprise Security

Coming Soon

- Investigate faster.
- Answer analyst questions to speed up daily workflows.
- Save time while addressing threats more rapidly.
- Access natively within Splunk ES.

CISCO *Live!*

Geographically Improbable Access Detected 392.398.23

Overview

Custom Fields

Basic Info

Events

MITRE ATT&CK

AI Assistant

Geographically Improbable Access Detected 392.398.23

Source Host: workstation-478.internal.domain

Destination Host: server-932.internal.domain

Source IP Address: 192.168.10.47

Destination IP Address: 192.168.10.123

Protocol: SMB

Event Information

Files accessed and transferred: \\server-932\share\payroll_data.xlsx, \\server-932\share\config.says

Additional Context

1. The source workstation ("workstation-478") typically does not initiate SMB connections to this server.

Sara Jones: 2:04 PM

Which host downloaded the files?

AI assistant: 2:04 PM

Sure, I can help with that. The following query can download the files?"

SPL

| tstats count WHERE index=index_01 sourcetype=... action="download" by host

Sara Jones: 2:04 PM

Run query



SEC1928 - SURGe Minicon: LLM Lifeguard: Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications



OWASP Top 10 for LLM Applications v1.1

OWASP Top 10 for LLM Applications

LLM01

Prompt Injection

This manipulates a large language model (LLM) through crafty inputs, causing unintended actions by the LLM. Direct injections overwrite system prompts, while indirect ones manipulate inputs from external sources.

LLM02

Insecure Output Handling

This vulnerability occurs when an LLM output is accepted without scrutiny, exposing backend systems. Misuse may lead to severe consequences like XSS, CSRF, SSRF, privilege escalation, or remote code execution.

LLM03

Training Data Poisoning

This occurs when LLM training data is tampered, introducing vulnerabilities or biases that compromise security, effectiveness, or ethical behavior. Sources include Common Crawl, WebText, OpenWebText, & books.

LLM04

Model Denial of Service

Attackers cause resource-heavy operations on LLMs, leading to service degradation or high costs. The vulnerability is magnified due to the resource-intensive nature of LLMs and unpredictability of user inputs.

LLM05

Supply Chain Vulnerabilities

LLM application lifecycle can be compromised by vulnerable components or services, leading to security attacks. Using third-party datasets, pre-trained models, and plugins can add vulnerabilities.

LLM06

Sensitive Information Disclosure

LLMs may inadvertently reveal confidential data in its responses, leading to unauthorized data access, privacy violations, and security breaches. It's crucial to implement data sanitization and strict user policies to mitigate this.

LLM07

Insecure Plugin Design

LLM plugins can have insecure inputs and insufficient access control. This lack of application control makes them easier to exploit and can result in consequences like remote code execution.

LLM08

Excessive Agency

LLM-based systems may undertake actions leading to unintended consequences. The issue arises from excessive functionality, permissions, or autonomy granted to the LLM-based systems.

LLM09

Overreliance

Systems or people overly depending on LLMs without oversight may face misinformation, miscommunication, legal issues, and security vulnerabilities due to incorrect or inappropriate content generated by LLMs.

LLM10

Model Theft

This involves unauthorized access, copying, or exfiltration of proprietary LLM models. The impact includes economic losses, compromised competitive advantage, and potential access to sensitive information.

Cisco + Splunk

Power and protect the AI revolution

Infrastructure for AI

Networking and compute solutions for training AI models at scale

Data for AI

Massive breadth and depth of data across domains is the foundation for AI models

Observability for AI

Observability supports trustworthy, performant, and reliable AI deployment

AI for Security

AI solutions improve efficiency, efficacy, and economics of defending against security threats

Security for AI

Cisco's Identity Intelligence and User Protection and Splunk's analytics help protect enterprises in their use of AI from within

What's next for security assistive AI @ Splunk

- Continue to augment the analyst experience
 - Incident Prioritization
 - Incident Response
 - Automation Guidance
 - Guided → Assisted
 - Prompts → Functions
- Empower the security engineer
 - Detection engineering support
 - Automation engineering support

Demo – AI Assistant in Splunk Enterprise Security



QueueMC-0007924 hour risk threshold exceeded for system=win-svr1.acme.local

OverviewResponseEventsSearch

Overview

MITRE ATT&CK map

The highlighted techniques were detected on the entity (in a finding)win-svr1.acme.local

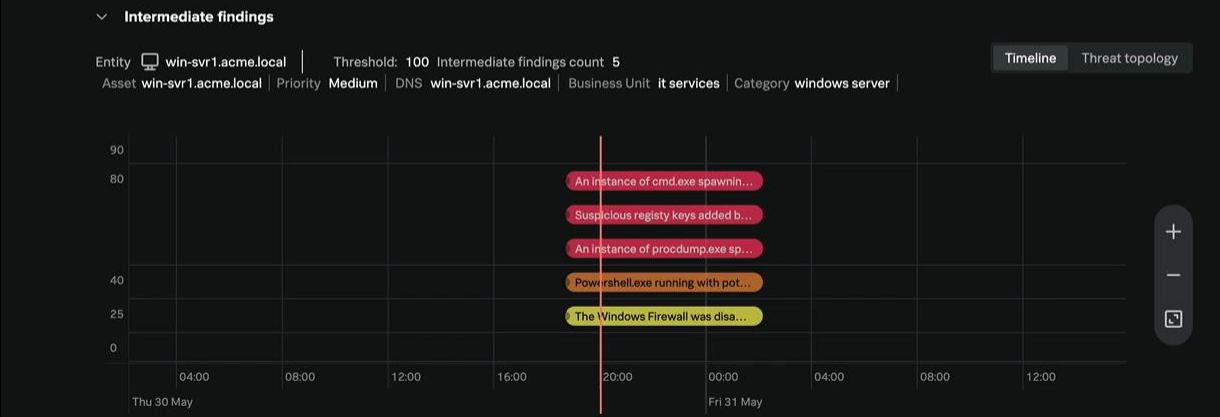
Detections in investigation4

Detections in selected time range0

Sub-Techniques(1)

Last 30 days

ent	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
(%)	0 of 13 Techniques (0%)	1 of 36 Techniques (3%)	0 of 71 Techniques (0%)	1 of 41 Techniques (2%)	2 of 89 Techniques (2%)	1 of 30 Techniques (3%)	0 of 33 Techniques (0%)	0 of 20 Techniques (0%)	0 of 17 Techniques
		Command and Scripting Interpreter PowerShell		Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism Impair Defenses	OS Credential Dumping			



Intermediate findings details

filter

Show 10

>	Time ↓	Risk Message ↑	Risk Rule
>	Today, 18:42	An instance of cmd.exe spawning procdump.exe was identified attempting to dump lsass.exe on endpoint win-svr1.acme.local by user bstoll.	AdHoc R
>	Today,	An instance of procdump.exe spawning procdump64.exe was identified attempting to dump lsass.exe on endpoint win-svr1.acme.local by user bstoll.	AdHoc R

INFO

OwnerJohn SmithStatusIn Progress

UrgencyMediumSensitivityAmber

DispositionUndetermined

IDMC-00079

TypeINVESTIGATION

TimeMay 30th, 2024 6:57 PM

Last updatedMay 30th, 2024 7:04 PM

Reference IDC7202D4D-59CC-4C26-AE51-76D4D4A81862@notable@ac12e48b01ebaf1959b504853aae11d7

Investigation typedefault

DescriptionRisk Threshold Exceeded for an object over a 24 hour period

Notes3

Show all

John SmithMay 30, 7:04 PMAssigned to L1 QueueInitial triage indicates something serious, please investigate.

splunk-system-userMay 30, 7:03 PMES CommentUpdating ES fields from Mission Control

splunk-system-userMay 30, 7:03 PMES CommentUpdating ES fields from Mission Control

FILES0

Complete Your Session Evaluations



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



Complete your surveys in the **Cisco Live mobile 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 DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: jkripalani@splunk.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC