

L'IA Agentique pour les opérations de sécurité : moins de bruit, plus d'impact

Agentic SOC by Splunk

Digital Resilience



Moez Kamel
Global Security Specialist – EMEA

Nicolas Mayer
Security Solution Architect – EMEA

Unrelenting Pressure on SOC Teams



Gaps in coverage

Staggering data growth, workload complexity, and costs are compounding risk



Fragmented, manual tooling

Siloed solutions, manual and reactive capabilities wear on team effectiveness



Overwhelming attack surge

Attacks, increasingly AI-fueled, are increasing in velocity, frequency and sophistication

The result: a record 50%+ of security leaders¹ and practitioners likely plan to quit their role in the next 12 months².

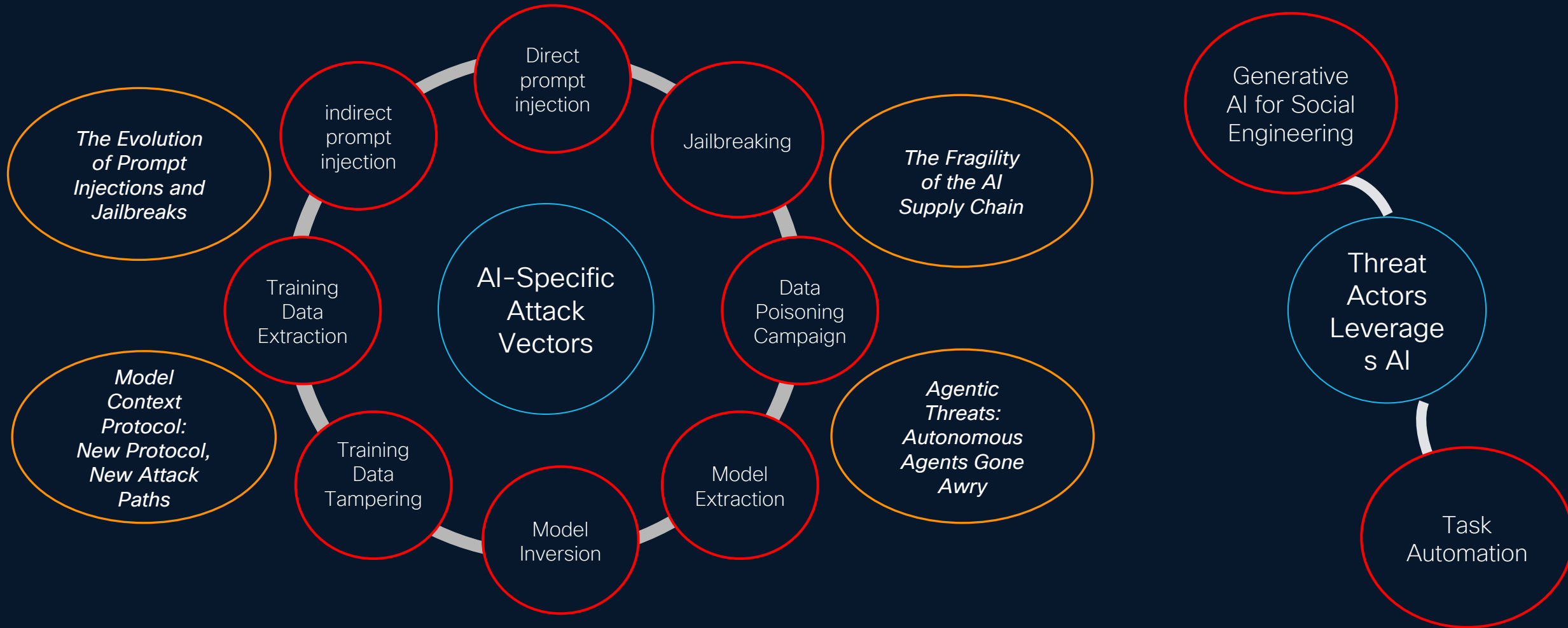


Security from the Agentic Frontier

The AI Transformation is here
and we must transform for it

State of AI Security

AI Threats Landscape



Your security team is stretched thin.

It's time for an agentic SOC platform that:

Automates the mundane

Clarifies the complex

Stops threats at machine speed



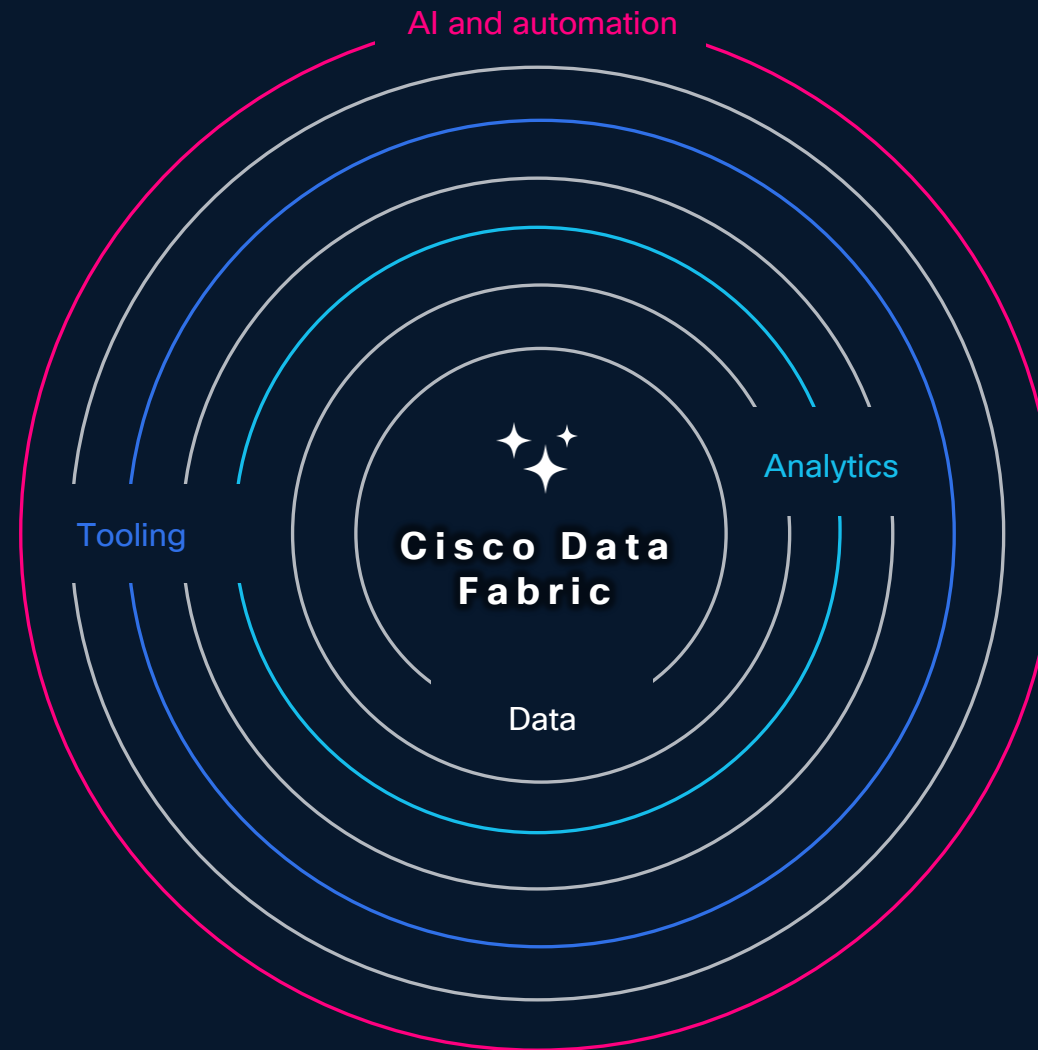
*It's time to Transform the
Analyst Experience and End
Analyst Fatigue*



The way forward **A New Operating Model**

An integrated system bringing together Data, Analytics, Tooling, and AI for a powerful analyst experience.

Agentic SOC



- Complete visibility
- Contextual understanding
- Intuitive analyst experience
- Machine speed & scale

A Foundation of High-Fidelity Data

Data fabric
Data management
Data pipelines

Analyzed at Machine Speed

TI enrichment & context
Correlated detections
Investigation & hunting

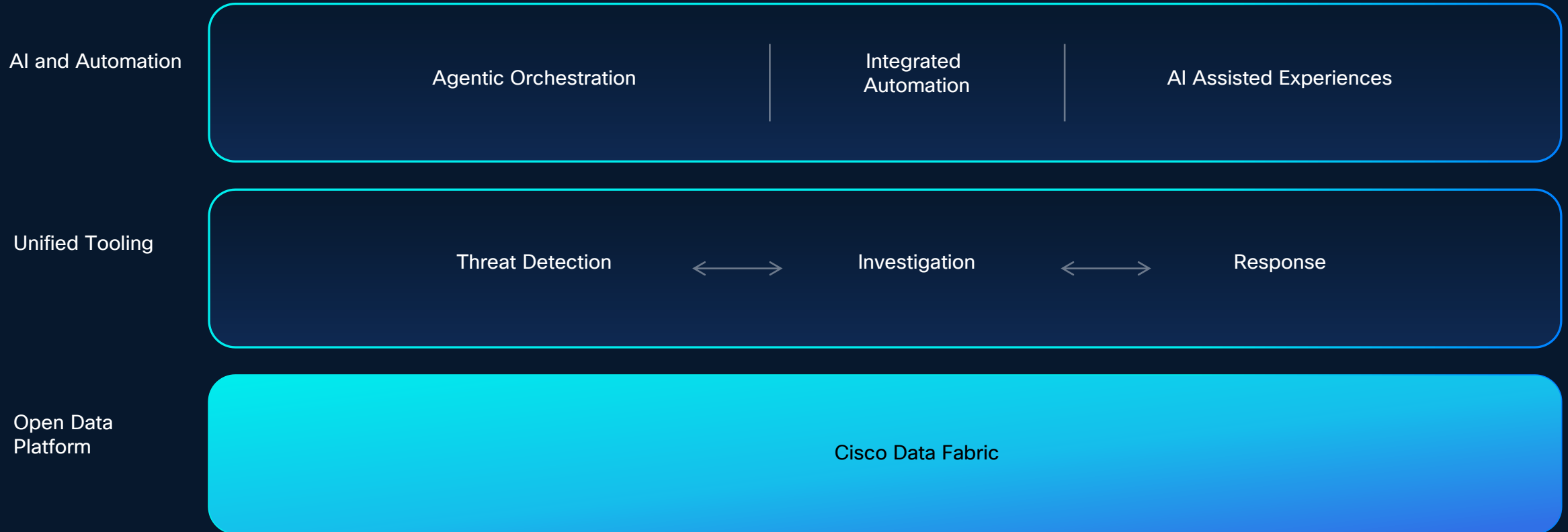
With Intuitive SOC Tooling

Single work surface for TDIR
Team coordination
Integrated workflows

And Human-led AI & Automation

Customizable agents
Reasons and acts
decisively
Prevents emerging threats

The new operating model for security in the Agentic era





Human-in-the Loop

Simplify and distill the analyst experience.

AI to maximize the human.



Domain-specific

AI to accomplish a specific security goal.

No AI for the sake of AI.



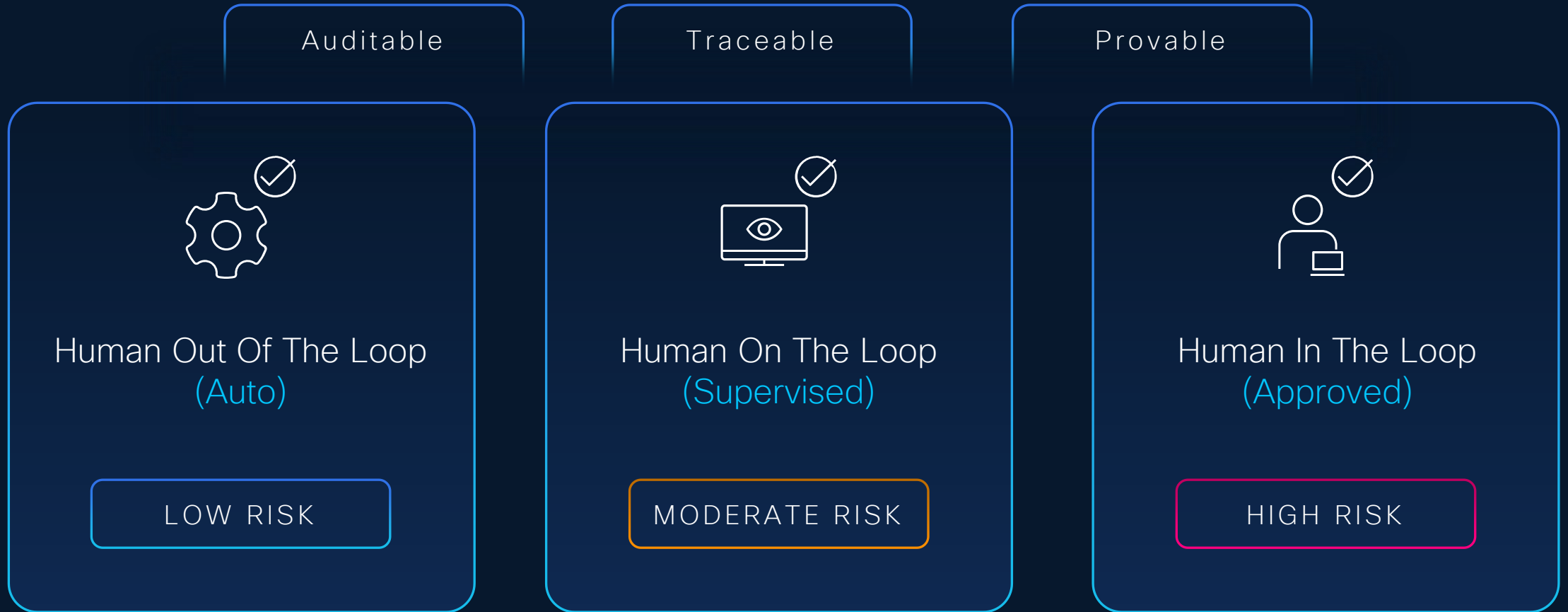
Open and Extensible

AI that is understandable and specific for each environment.

No closed boxes.

Human-AI Operating Model

How AI Trust is Earned : Evidence Packets



Enterprise Security

Now available in two editions



Dedicated and purpose-built Security AI Agents

Detection agent



Malware Reversing Agent



Triage Agent



Orchestration/SOP Agent



Guided Response + Automation Agents



SPEED

Detection

Triage

Investigation

Response

Augmenting Splunk with AI

Cisco Foundation Models

AI Toolkit
LLM Integrations

Data Science and Deep Learning
3rd Party Runtime Connectors

Splunk Native AI

Flexible and Customisable

Simplicity of Use

Custom AI/ML Platform

AI Toolkit
DSDL Toolkit

Native search commands

Human Guided AI Assistants

AI Assistant for SPL

AI Canvas

OOTB ML Analytics

AI Assistant in ES

UEBA

Detection Studio

Autonomous AI Agents

Triage Agent

Malware Reverse Engineering Agent

AI for Security

AI enhanced with Splunk

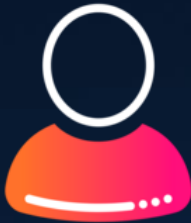
MCP Servers

The SOC Operation

Initial
Triage



Incident
Response



Advanced
Response



Engineering



Management



TDIR Platform

Triage Agent

ASK

Streamline alert prioritization and disposition

SEE

Automate insights to reduce MTTR

ACT

Plan and Execute investigations

The screenshot displays a security dashboard with a list of findings on the left and a detailed view of a specific finding on the right.

Title	ID	Entity	Risk	Fin...	Int...
Is this a Phish? - FW:Calling All Employees	ES-87199	administrator	97		25
Malicious PowerShell process with obfuscation techniques	FI-AB543	Entity name lorem ipsum si...	92		25
User access from unknown location tsmith2276621	ES-AB416	--	30	4	574
Geographically Improbable Access Detected 192.198.2.3	FI-AB410	--	80	4	98
24 hour risk threshold exceed for system=172.16.0.149	FI-AB293	172.16.0.149	84	3	4
Possible Phishing Attack	FI-AB198	Entity name	55		17
Threat Activity Detected from 10.163.194.46 to 8.108.191.101	FI-AB029	Entity name	35		247
3 failed login attempts within 24 hrs on device 10.34.56.354	FI-AB274	Entity name	96		17
Threat Activity Detected from 10.163.194.46 to 8.108.191.101	FI-AB558	Entity name	94		8
MITRE ATT&CK Tactic Threshold Exceeded For Object Over Previous 7 Days	FI-AB129	Entity name	89	4	17
AWS Cloud Provisioning From Previously Unseen IP Address	ES-AB992	Entity name	50	6	2
Email files written outside of the Outlook directory	FI-AB352	Entity name	50		6k
High or Critical Priority Individual Logging into Infected Machine	FI-AB225	Entity name	55		874
First Time Seen Running Windows Service	FI-AB002	Entity name	65		17
User access from unknown location tsmith2276621	ES-AB416	Entity name	30	5	3
Geographically Improbable Access Detected 192.198.2.3	FI-AB410	--	91	4	98
24 hour risk threshold exceed for system=172.16.0.149	FI-AB293	172.16.0.149	140	8	4
Unusual network activities detected from 52.218.245.82 to 52.216.133.181	FI-AB543	Entity name lorem ipsum si...	65		25
Possible Phishing Attack	FI-AB198	Entity name	55		17

The detailed view on the right shows the following information:

- Finding added by MS Graph O365**
- Owner:** Unassigned
- Status:** New
- Urgency:** Medium
- Sensitivity:** Unknown
- Disposition:** Undetermined
- Analysis:** True positive
- Info:** Event ID: ES-87199, Time: Nov 21st, 2024 5:57 PM, Last updated: Nov 21st, 2024 5:57 PM, Detection: Threat - MS Graph Office 365- Rule, Title: Is this a Phish? - FW:Calling All Employees, Reference ID: C4E8257A-9515-48E2-B1F8-E116C392323B@notable@21741..., Security domain: threat, Investigation type: Email
- Threat analysis:** Email analysis
- Verdict:** Phish (67)
- System tags:** Tag 01, Tag 02
- Phishkit families:** Zphisher, 16Shop, Kr3pto
- Phished brands:** Office365
- Resource analyzed:** qrcode → https://www.canva.com/design, otherRedirect → https://www.canva.com/design/DAFwH1htmSi/TzcAMPOnLBJ, click → https://www.canva.com/link?target=https%3A%2F%

Accelerate triage from signal → context → decision with an agent built to reduce noise and surface what matters.

Investigation Canvas

ASK

Type what you want to know

SEE

Investigation Canvas builds the visualization for you

ACT

Launch SOAR-powered actions right inside the workspace

splunk Search & Reporting

AI Canvas | Detected Anomalous Network Activity

2. Redis pool saturation — it shows pool utilization flatlined at max. Is it a root cause or a symptom of the traffic spike?

Let me know what you want to do.

You
Search on retry config change

AI Canvas 11:12 am
Generated a chart to break down outbound payment requests by retry attempt number and status code. Before `deploy-4281`, there's almost no retry traffic. The moment it lands at 01:38, the red band (retry 4-10) explodes from zero to ~750 requests per minute — that entire band is traffic that wouldn't exist under the old 3-retry config.

Ask AI Canvas a question

Recent Changes – api-prod-02

_time	deploy_id	description
08/09 01:38:02	deploy-4281	Payment gateway retry con...
08/08 15:20:14	deploy-4279	Logging format standardiz...
08/08 15:10:23	deploy-4268	Bug fix for timeout issue
08/08 11:08:41	config-auto-748	API update

Infrastructure Metrics – api-prod-02

Line chart showing Bytes Out and CPU % over time.

Payment Retry Volume Over Time

Line chart showing retry volume for different retry attempt numbers (0-1, 2-3, 4-10) over time.

Enable analysts to move from question → insight → response in a single generative workspace.

AI Assistant in Security

Guided security workflows

- ▶ Answer analyst questions to guide investigations
- ▶ Save time by addressing threats more rapidly
- ▶ Use natural language queries to get answers during investigations

The screenshot displays the Splunk Security Console interface. At the top, a navigation bar includes 'Mission Control', 'Analytics', 'Security content', 'Configure', and 'Search'. Below this, a queue entry for 'MC-00079' is highlighted with a red banner stating '24 hour risk threshold exceeded for system=win-svr1.acme.local'. The main area shows an 'Overview' section with a 'MITRE ATT&CK map' and a 'Timeline' view of intermediate findings. A chat window on the right, titled 'AI Assistant for Security', is highlighted with a blue border. The chat shows a user 'John Smith' asking to discover AI Assistant skills, and the AI responding with two main categories: 'SPL Generation based on the user's Splunk environment' and 'Summarizing security findings'. The chat also shows a previous message from John Smith regarding a 'Compromised user account' and the AI's response to recommend detecting Security Content Updates.

Queue: MC-00079 | 24 hour risk threshold exceeded for system=win-svr1.acme.local

Overview

MITRE ATT&CK map

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

Detections in Investigation: 4 | Detections in selected time range: 4 | Sub-Tec... (1) | L...

Initial Access (0 of 13 Techniques (0%)) | Execution (1 of 36 Techniques (3%)) | Persistence (0 of 71 Techniques (0%)) | Privilege Escalation (1 of 41 Techniques (2%)) | Defense Evasion (2 of 69 Techniques (3%)) | Credential Access (1 of 30 Techniques (3%)) | Discovery (0 of 33 Techniques (0%))

Intermediate findings

Entity: win-svr1.acme.local | Threshold: 100 | Intermediate findings count: 5 | Timeline | Threat topology

Asset: win-svr1.acme.local | Priority: Medium | DNS: win-svr1.acme.local | Business Unit: it services | Category: windows server

Timeline: May 2024 (Thu 30) | Fri 31 | Sat 1 | June 2024

Intermediate findings details

filter | Show 10

Time ↑ | Risk Message ↓

Yesterday... An instance of cmd.exe spawning procdump.exe was identified attempting to dump lsass.exe on endpoint...

AI Assistant for Security

MC-00079 - 24 hour risk threshold exceeded for system=win-svr1.acme.local

John Smith | May 31, 4:01 AM | Discover AI Assistant skills

AI | May 31, 4:01 AM | Sure, here are the AI Assistant skills that can be leveraged:

1. SPL Generation based on the user's Splunk environment:
 - This involves creating or generating Splunk Processing Language (SPL) queries according to the user's requirements and the available structure and data in the user's Splunk environment.
2. Summarizing security findings:

Reviewed all process activity for user bstoll

"parent_process_name","process_name","process,count,first Time,last Time

"svchost.exe","InstallAgent.exe","C:\Windows\System32\inst

John Smith | May 30, 8:31 PM | Compromised user account

user account bstoll appears compromised as that user is on leave. Have quarantined the machine pending further analysis, not other activity from this account on other

John Smith | May 30, 8:30 PM | Escalated to service owner

Contacted service owner to verify situation given IT user

4. Recommending detecti Security Content Updat

This involves sugge detections from E! various types of sr within the Splunk | environment.

These features enable efficient reporting of security events wit advanced analytics and AI cap

Ask me anything about security

AI Playbook Authoring

- Generative AI to build automation

- Interactive AI Building

Gen AI builds based on prompts that map to your exact use case

- Refine with AI

when creating advanced workflows, AI helps define, craft, and implement the next logical step

- Complete with Confidence

unlike other solutions Splunk's AI approach to playbook authoring optimizes on accuracy

01 Easily craft the most advanced and customized workflows

The screenshot displays the SOAR AI Assistant interface. On the left, a vertical toolbar contains various icons for workflow actions. The main workspace is divided into two panes. The top pane, titled 'Code', shows a Python script for listing and filtering users. The bottom pane shows the AI Assistant's response to a prompt, including a list of users and a follow-up question. A workflow diagram on the right side of the screen shows a sequence of steps: 'Start', 'ACTION list user', 'CODE Configuring...', and 'End'. Three callout boxes are overlaid on the image: '01 Easily craft the most advanced and customized workflows' at the top, '02 Increase confidence by verifying playbooks work while you build' on the right, and '03 Identify, craft, and implement content' at the bottom.

```
import json

# Simulate reading user data from a data path
data_path = "/path/to/user_data.json"
with open(data_path, 'r') as file:
    users = json.load(file)

def filter_users_no_password_change(users):
    return [user for user in users if not user["Password_Changed"]]

users_without_password_change =
filter_users_no_password_change(users)
```

Input: list users

Output 01

Extract the users who have not changed their password

I've extracted the following users for you:

admin, jane doe

Would you like to modify anything lorem ipsum?

Input prompt to test the output...

Results from GenAI can vary; review for accuracy. [View AI details](#)

02 Increase confidence by verifying playbooks work while you build

03 Identify, craft, and implement content

Detection Studio

Powered by SnapAttack

▶ AI Guided Detection Creation

▶ Detection Health, Coverage and Effectiveness Visibility

▶ Detection-as-code lifecycle management

The screenshot displays the Splunk Security content dashboard. The main view shows a list of detection rules with columns for Name, Priority, Health, Coverage, and Actions. A large circular callout highlights the 'Overall detection technique coverage' metric, which is 65% (up 5%). Another callout highlights the 'Highest priority detections' metric, which is 72. The right-hand panel shows the details for the 'ESCU - ICACLS Grant Command - Rule', including its priority (High), compatibility (High), and a list of detection logs.

Name	Priority	Health	Coverage	Deployed State	Actions		
Endpoint - Potential Automated File Collection	High	100	100	Off	👁️ 🗑️		
Endpoint - Potential Indicator Removal	High	100	100	Off	👁️ 🗑️		
Endpoint - Potential Text Based Data Exfiltration	High	100	100	Off	👁️ 🗑️		
ESCU - Any Powershell DownloadFile IF Only - Rule	High	100	15	98	Off	👁️ 🗑️	
ESCU - CMD Echo Pipe - Escalation IF Only - Rule	High	100	5	98	On	👁️ 🗑️	
ESCU - Detect RClone Command-Line Usage IF only - Rule - Rule	High	50	100	12	85	Off	👁️ 🗑️
ESCU - Disable Schedule Task IF Only - Rule - Rule	High	65	100	8	90	On	👁️ 🗑️
ESCU - Registry Keys Used For Persistence IF Only - Rule - Rule	High	70	100	10	80	On	👁️ 🗑️
ESCU - Windows Sensitive Registry Hive Dump Via CommandLine IF Only - Rule - Rule	High	68	100	14	90	Off	👁️ 🗑️
ESCU - ICACLS Grant Command - Rule	High	87	95	98	82	Off	👁️ 🗑️
ESCU - Network Discovery Using Route Windows App - Rule	High	55	100	11	85	Off	👁️ 🗑️
ESCU - PowerShell Get LocalGroup Discovery - Rule	High	78	100	7	95	Off	👁️ 🗑️
Cisco Network Interface Modifications	High	78	100	7	95	Off	👁️ 🗑️
Cisco Secure Firewall - Static Tundra Smart Install Abuse	High	78	100	7	95	Off	👁️ 🗑️

```
1 tstats `security_content_summariesonly`
2 min(_time) as firstTime max(_time)
3 as _lastTime from datamodel=Endpoint.Processes
4 where
5 Processes.process_name IN ( "icacls.exe",
6 "cacls.exe", "xcacls.exe") AND
7 Processes.process IN ("*/grant*", "*/g*", "*/g
8 ")
9 by Processes.action Processes.dest
10 Processes.original_file_name
11 Processes.parent_process
12 Processes.parent_process_exec
13 Processes.parent_process_guid
14 Processes.parent_process_id
15 Processes.parent_process_name
16 Processes.parent_process_path Processes.process
17 Processes.process_exec
18 Processes.process_guid Processes.process_hash
19 Processes.process_id
20 Processes.process_integrity_level
21 Processes.process_name Processes.process_path
22 Processes.user Processes.user_id
23 Processes.vendor_product
24 | `drop_de_object_name(Processes)`
25 | `security_content_ctime(firstTime)`
26 | `security_content_ctime(lastTime)`
27 | `icacls_grant_command_filter`
```

Detection Builder Agent

- Go from detection hypothesis to production in minutes with accuracy
- Quickly import, tune, and tag detections
- Personalize detections for your environment.

splunk> Cloud

Edit event-based detection

[Back to Content management](#)

1 Detection search
Create finding-based detections to create findings and finding groups in Splunk Enterprise Security for your specific security use case [Detection search documentation](#)

* Name

App

UI dispatch context

* Security domain

* Description

* Search

```

1 | rename object as user
2 | search NOT (user IN ("kennyb", "tommyj", "billym"))
3 | stats count min(_time) as firstTime max(_time) as lastTime by action actionlabel description user
4 | eval script=coalesce(process, "")
5 | `security_content_ctime(lastTime)`
6 | search *

```

Review

Last 24 hours

2 Analyst queue information

Enter optional note...

Status

AI Assist is successful
1 new line has been added

SOP Agent

- Import security standard operating procedures into Splunk Enterprise Security response plans so AI agents can act on them.

The screenshot displays the Splunk Cloud interface. At the top, the navigation bar includes 'splunk> Cloud', search, settings, and user profile (Splunk Administrator). The main content area is titled 'Edit event-based detection' with a 'Back to Content management' link. A modal window titled 'Import response plan' is centered, offering two options: 'Import and generate with AI' (upload security documentation for generative AI) and 'Import JSON' (import previously exported plans). Both options have a dashed box for file upload and support PDF, TXT, and JSON. A 'Close' button is at the bottom right of the modal. In the background, a table lists existing response plans.

Referen...	Name						
	Test file 1						
	Test file 2						
	Test file 3						
...7516	sad_v23321 dsa						
...1624	sad_v23aaa dsa						
...2236	Data Breach	Splunk	Feb 24th, 02:31 PM	Feb 24th, 02:31 PM	Splunk	published	
...d209	Network Indicator Enrichment Gather and analyze contextual information about URLs, hostnames, top level domain...	Splunk	Feb 24th, 02:31 PM	Feb 24th, 02:31 PM	Splunk	published	
...d210	Self-Replicating Malware This response template outlines a response to a potential infection by self-replicatin...	Splunk	Feb 24th, 02:31 PM	Feb 24th, 02:31 PM	Splunk	published	
...4a0e	Vulnerability Disclosure	Splunk	Feb 24th, 02:31 PM	Feb 24th, 02:31 PM	Splunk	published	
...334d	Suspicious Email There are many ways in which attackers can use email to gain a foothold in an ...	Splunk	Feb 24th, 02:31 PM	Feb 24th, 02:31 PM	Splunk	published	
...0de7	Generic Incident Response	Splunk	Feb 24th, 02:31 PM	Feb 24th, 02:31 PM	Splunk	published	
...e1ef1	arolscki-test_v3	admin	Feb 24th, 04:58 PM	Feb 24th, 04:58 PM	admin	published	

UEBA

Enterprise Security's UEBA capability

- CMP and Cloud enabled UEBA engines within ES
- Unsupervised AI and ML Behavioral baseline and detection
- Provide rich context for insider threats

The screenshot displays the Splunk Enterprise Security (ES) UEBA overview dashboard. The interface includes a navigation bar with 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', and 'Find'. Below the navigation, there are tabs for 'Mission Control', 'Analytics', 'Security content', 'Configure', and 'Search'. The main content area is titled 'UEBA overview' and provides a summary of top users and systems by risk over the past 7 days. It includes filters for 'Entity list: Identities', 'Entity list: Assets', 'Detection', and 'MITRE ATT&CK', along with 'Clear all' and 'Apply' buttons. The dashboard is divided into three main sections: 'Top risky users', 'Top risky assets', and 'Top risky entities detection activity'. Each section contains a table of entities with associated risk scores and trends, and a small line chart showing the risk score over time.

Top risky users 100

User	Entity list	Entity risk score (7d)	24h trend
TZ Taylor Zhang	Departing employee	85	+20
CG Charlie Garcia		80	-20
NA Nyah Aamadu	Admin, Departing employee, SOC	80	-5
SP Sasha Patel	Admin, SOC	75	-10
AT Kenji Tanaka	Admin, Contractor, SOC	50	-40
4 4afb3263\$	Service account	50	-20
AN Ava Nguyen		50	+40
AG Arjun Gupta	Admin, Contractor, Privileged account	48	-2
SR Sofia Rodriguez	Departing employee	48	-10

Top risky assets 100

System	Entity list	Entity risk score (7d)	24h trend
host-003		80	+20
DC1	Domain controller	80	+5
10.12.34.56		80	-5
app_database	Database server	80	+5
http://www.buttercupgames.com	Corporate web domain	80	+5
5.6.7.8		70	-50
2001:db8:85a3::8a2e:370:7334		70	-10
ops-sys-003		65	+5
ec2-54-183-247-244.us-west...		60	-40
192.168.12.9		60	-10

Top risky entities detection activity 150

Detections with findings or intermediate findings contributing to top risky entities.

Detection	Type	Source categories	Finding count	Unique entity count	Finding exclusion rul...	Actions
Unusual Volume of Admin Commands per User Model	ESCU	Database Activity	319	301	1	⌵ ⋮
Suspicious Privilege Escalation Model	ESCU	Windows Security Logs	312	238	9	⌵ ⋮
Protocol Impersonation	ESCU	Windows Security Logs	309	305	2	⌵ ⋮
Unusual Time of Badge Access Model	ML	Badge Access Logs	298	210	—	⌵ ⋮
Risk - 24 Hour Risk Threshold Exceeded - Rule	ESCU	Security Analytics	296	265	—	⌵ ⋮
Windows Screen Capture Via Powershell	ESCU	Windows Security Logs	290	156	—	⌵ ⋮
New Activity Type	ML	Behavioral Analytics	288	214	2	⌵ ⋮

Malware Threat Reversing Agent

- Autonomous reverse engineering of all inbound payloads
- Full disposition summary and integration with ES
- Remove all manual work from payload analysis

SAA Attack Analyzer Recent Search All Jobs Search Forensics caseyb@splunk.com

100 Email.zip

Verdict: Phish
 Malware Family: AgentTeslaXor
 Phished Brands: Microsoft, Microsoft O365
 Submitted: 7/9/2025, 11:06:47 AM by jcheckeye+show@splunk.com
 Tenant: splunk-show
 SHA256: 69e9a41020bee29616b9040081149e5...
 File Type: Zip archive data, at least v2.0 to extract
 File Size: 125 KB

View AI summary of this job

Resources Analyzed

- Email.zip
 - attachment → MobileLoginActiv...
 - decryption → MobileLoginActiv...
 - qrcode → https://sso.pecan-b...
 - click → https://signin.p...
 - click → https://pub-5652c...
 - download → 1...
 - 4625_76148

Summary

- Consolidated: 100
- Email.zip
 - Archive Extraction: 0
 - Static File Analysis: 0
 - ClamAV: 0
 - StaticAV: 0
 - YARA: 0
- MobileActivation.eml
 - Email Analyzer: 50
 - Static File Analysis: 0
 - ClamAV: 0
 - StaticAV: 0

Task Brands Impersonated

Initial Summary: This is a malware attack

Job Duration: [Duration]

Resources Analyzed: [Resources]

Verdict: Phish

Malware Family: AgentTeslaXor

Phished Brands: Microsoft, Microsoft O365

Detections (60)

Engine	Signature / Alert	Score
Web Analyzer	Detected Microsoft Phishing Attempt	100
Web Analyzer	Detected Phishing Attempt	100
StaticAV	StaticAV detected: Trojan.Ransom.Loki.BYX	100

The SOC Platform



Operations

Triage Agent

AI Assistant

AI Playbook
Authoring

Detection Studio

TDIR Platform

Detection

UEBA

AI Defense

Malware Threat
Reversing Agent

AI Toolkit

Data

Cisco Data Fabric



AI-powered
data management



Federated Search
and Analytics



AI-Native Experiences
and Platform for AI

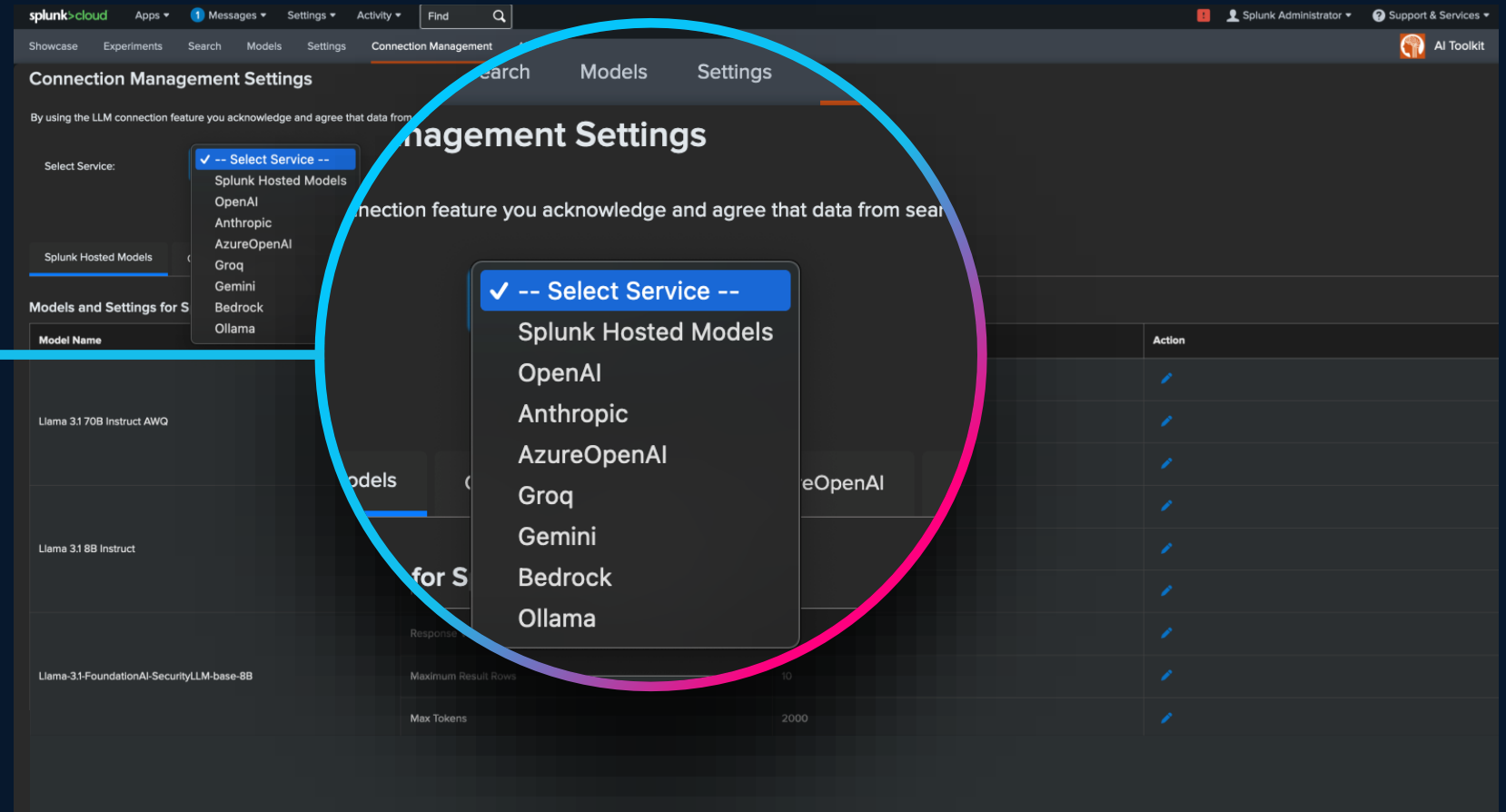


Machine Data Lake

Scaling AI Capabilities

Splunk AI Toolkit

- Build and deploy AI models
- Query Splunk with 3rd party LLMs
- Access Splunk hosted models, coming soon



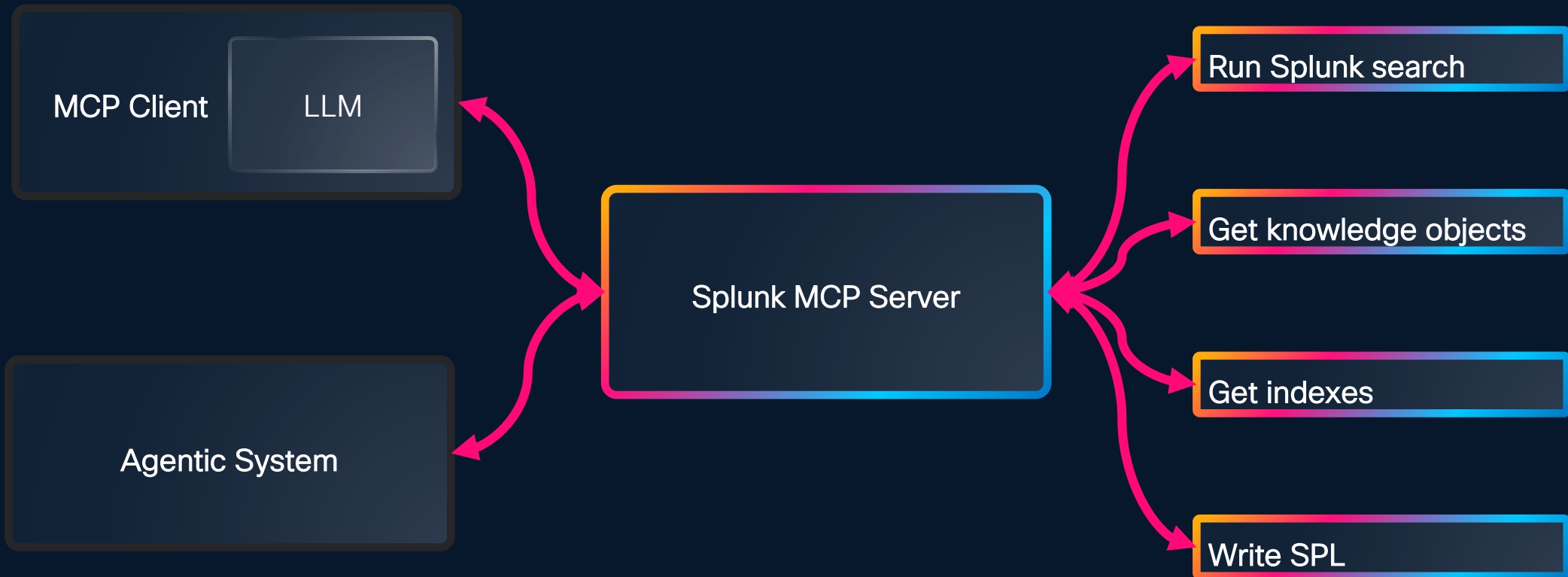
Splunk DSDL

Splunk App for Data Science and Deep Learning

- **35+ Code Examples:** Guided model building, testing, and deployment
- **Container Management:** productionized for scalability & optimization on CPU & GPU
- Flexible deployments and open source
- Extension to LLMs and VectorDB

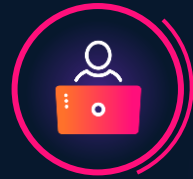
The screenshot displays the Splunk DSDL app interface. At the top, there is a navigation bar with 'splunk>enterprise' and 'Apps' on the left, and 'Administrator', 'Messages', 'Settings', and 'Activity' on the right. Below this is a secondary navigation bar with 'Content', 'Configuration', 'Examples', 'Assistants', 'Operations', 'Other', 'Documentation', and 'Search'. The main content area is titled 'Configuration' and features a central navigation menu with 'Configuration' (selected), 'Examples', 'Assistants', and 'Operations'. The main area is divided into two sections: 'Configuration' and 'Examples'. The 'Configuration' section includes three cards: 'Container Environment Setup' (Configure how the Splunk App for Data Science and Deep Learning connects to your Docker, Kubernetes or OpenShift environment), 'Container Management' (Controls to start and stop containers and check their status), and 'Container Image Builder' (Create custom container images for specific data science, machine learning or deep learning libraries). The 'Examples' section includes seven cards: 'Classifier' (Explore classification algorithm examples and use cases), 'Regressor' (Explore regression algorithm examples and use cases), 'Forecasting' (Explore forecasting algorithm examples and use cases), 'Clustering' (Explore clustering algorithm examples and use cases), 'Natural Language Processing' (Explore natural language processing (NLP) algorithm examples and use cases), 'Data Mining' (Explore various data mining algorithm examples and use cases), and 'Basic' (Explore some basic algorithm examples and use cases). A 'Graphs' card is also present, showing a network graph visualization.

Splunk MCP Server



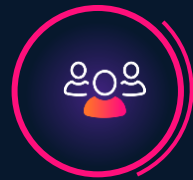
AI Defense with Cisco

Secure AI applications

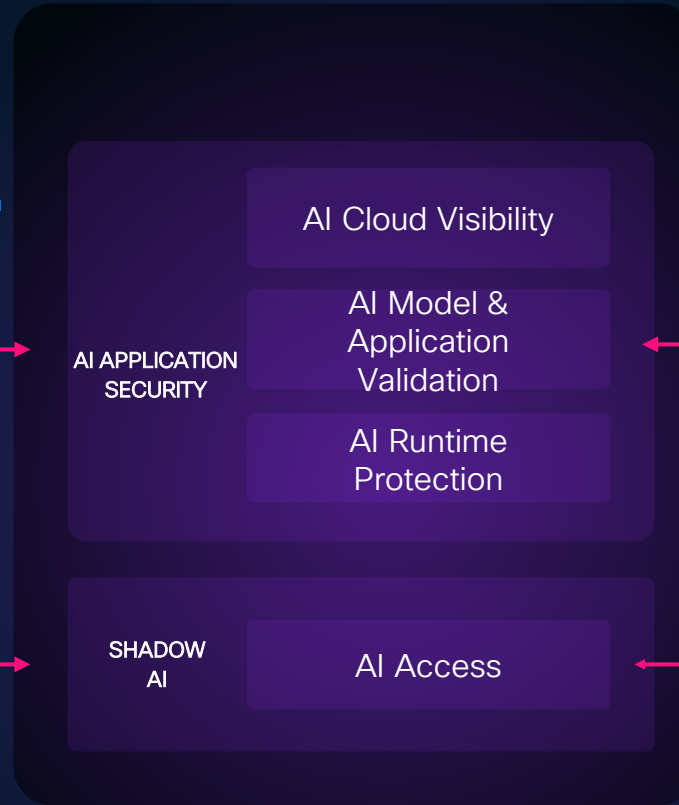


End User

Secure AI access




Employee





Model Providers  OpenAI
 Gemini

Custom AI Apps

App	·
Model	·
Data	·

Connected Data Sources 

Third-party Apps  Copilot




Splunk Enterprise Security + AI Defense

The integration between Splunk ES and Cisco AI Defense provides continuous monitoring to detect and reduce AI-based risk across your environment.

**Cisco
AI Defense**

AI Context
Events, Messages,
Actions, and Policy
names

AI Visibility
Network
Connections and
Applications

AI Governance
Guardrail entities and
Ruleset
types

**Splunk
Enterprise Security**

Splunk ES aggregates, normalizes, and maps Cisco AI Defense telemetry to the Common Information Model (CIM) to perform comprehensive analysis and enforce AI defensive governance that strengthens your overall security posture.

CISCO Connect

Thank you



