

Power the Agentic SOC with Splunk TDIR (Threat Detection, Investigation & Response)

Caglar Dogan
Security Specialist MEATRC

7th October 2026 Istanbul





Caglar Dogan

Security Specialist & Advisory
MEA-TRC Splunk

Forward- looking statements

This document may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. 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 document.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this document, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Cisco Investor Relations website at <https://investor.cisco.com/home/default.aspx> or the SEC's website at www.sec.gov. The forward-looking statements made in this document are made as of the time and date of its drafting. If reviewed later in time, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about 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. We undertake no 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.

Four market forces

Inference is the new workload

Agents are the new workforce

Tokens are the new currency

Control is the new moat

On a laptop



In an enterprise smart switch



In a contact center



In a meeting room

Agents are going to be running everywhere

Every device, every room, every workflow — quietly, all at once.

In a branch router



In a SOC

In the data center



In a deskside device

Two megatrends build pressure across every organization

The rise of agentic AI + The post-Mythos cyber landscape

What shape should my workforce take?

What infrastructure do I need to modernize?

Can I trust what my AI is doing?

What needs to change in my security posture?

How do I manage token costs?

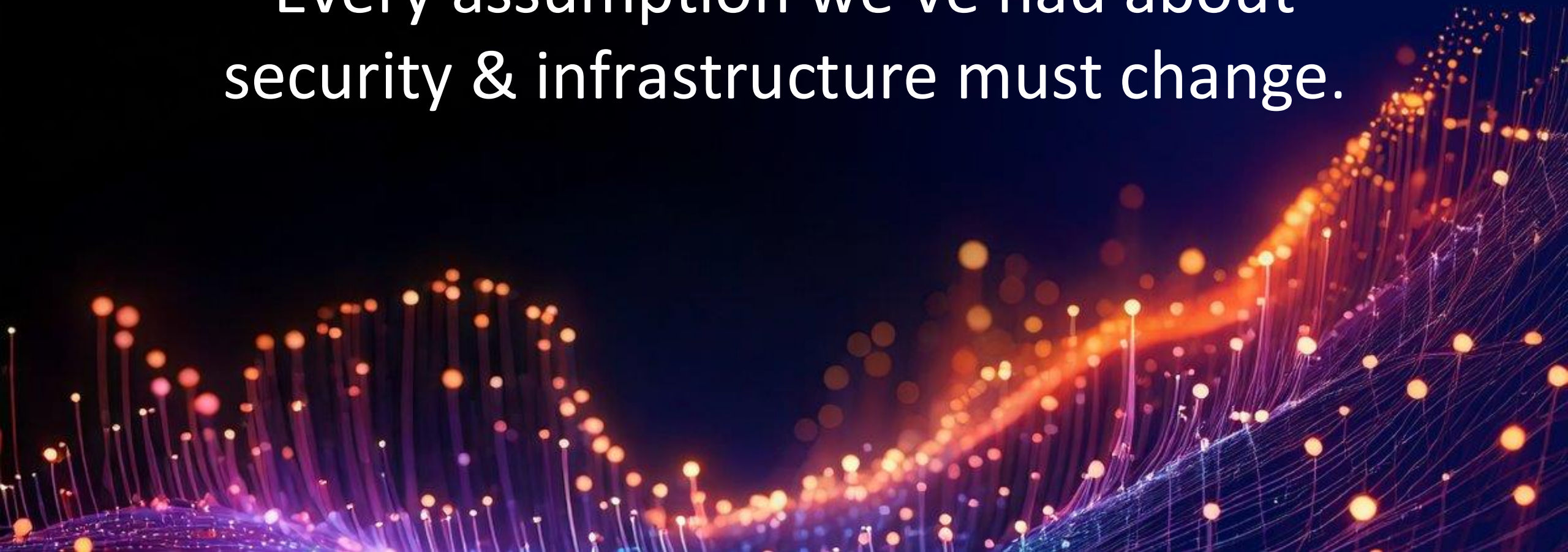
Where should I run my AI workloads?

How do I keep agents from going rogue?

Do I have the data I need in the right place?

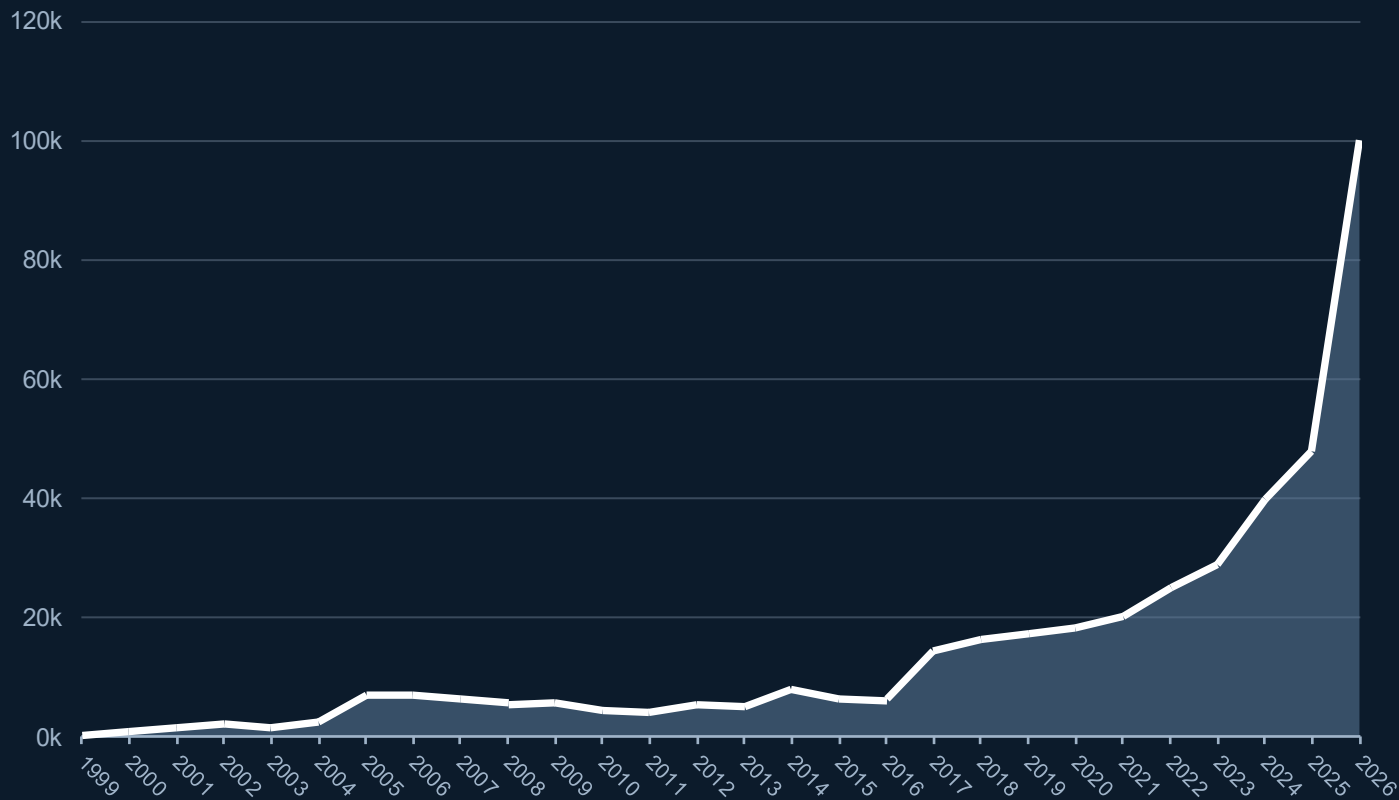
We live in the **Post-Mythos** world.

Every assumption we've had about
security & infrastructure must change.



Implication #1: CVE Growth

Annual CVE Growth (1999 - 2026)



CVE Volume Milestones

1999

300 CVEs

2005

~7,000 CVEs

2017

~14,600 CVEs

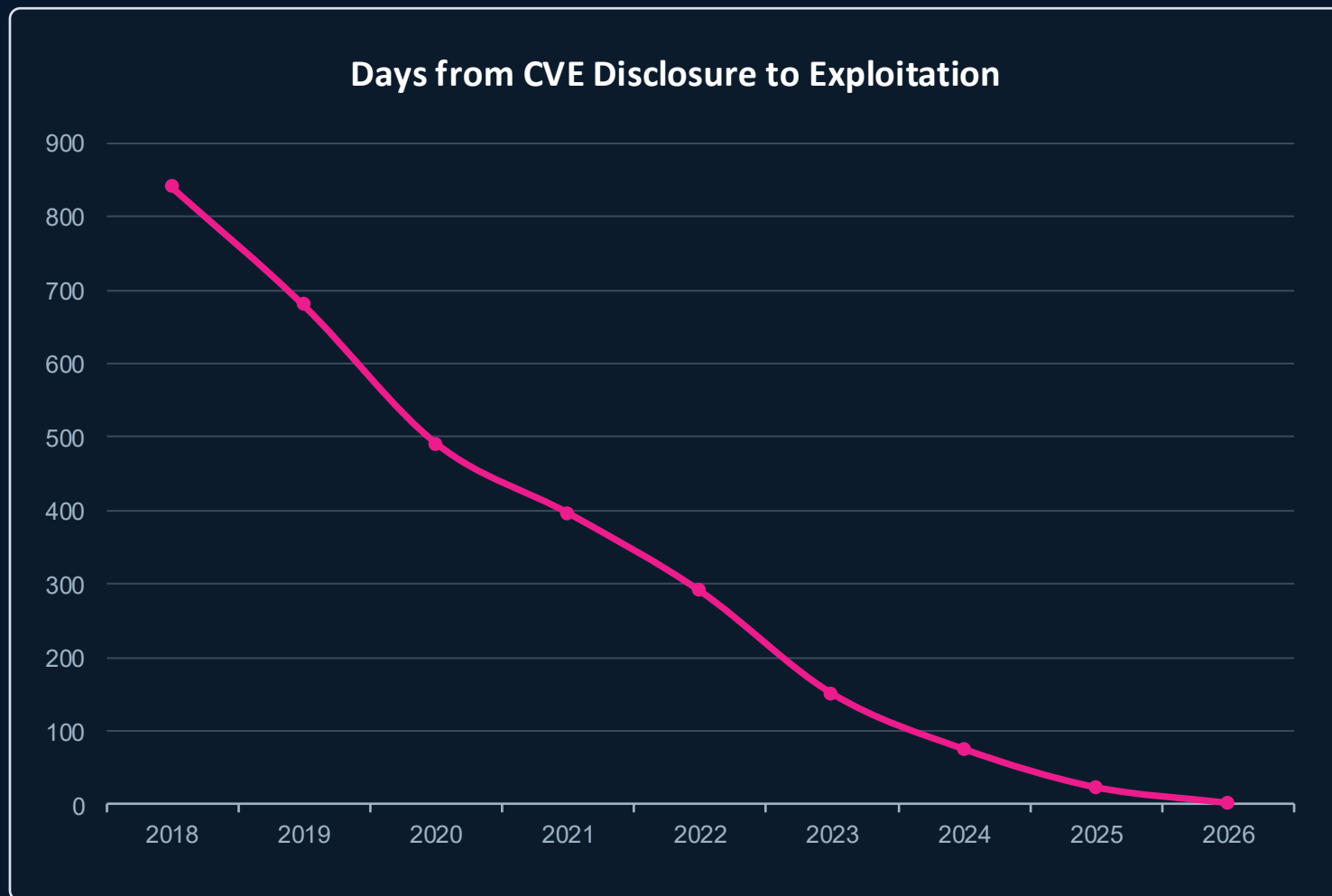
2025

48,000+ CVEs

2026

100k+ CVEs

The Collapsing Time-to-Exploit



Time-to-Exploit Milestones

2018

2.3 years

2021

13 months

2023

5 months

2025

23 days

2026

< 20 hours

Source: Zero Day Clock (zerodayclock.com) — 3,529 CVE-exploit pairs from CISA KEV, VulnCheck KEV & XDB

What if you could stay ahead?

Detect and react → Predict and prevent

Intelligence without context is just computation.

ALL SIGNALS. ONE FABRIC.

MACHINE TELEMETRY

- Logs
- Events
- Traces
- Metrics
- Flows
- Alerts
- Topology
- Configuration
- Identity

BUSINESS & POLICY CONTEXT

- Business Knowledge
- Policies & Rules
- Business Context
- Runbooks & SOPs
- Service Ownership



WHAT MATTERS

The model doesn't understand your business

Right data • Right context • Right moment

“Your context does.”

Data tells you what happened.

Context tells you what it means.

The SOC Reimagined

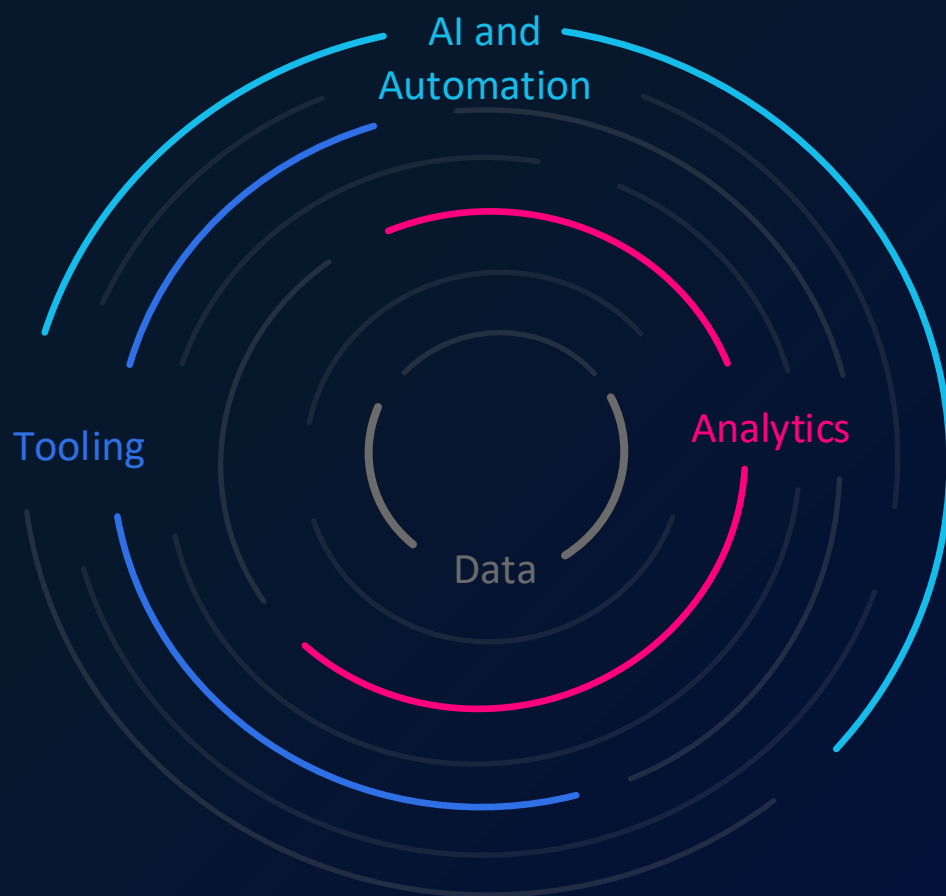
A human + AI partnership to harness massive volumes of data and:

- Focus on the threats that matter most.
- Accelerate detection and response.
- Enable digital resilience for the business.



A New Way: The Agentic SOC

An integrated system bringing together data, tooling, and AI to amplify the defender's impact



Human-led AI & Automation

- Community-driven agents
- Reasons and acts decisively
- Prevents emerging threats

With Intuitive SOC Tooling

- Single work surface for TDIR
- Team coordination
- Integrated workflows

Analyzed at Machine Speed

- TI enrichment & context
- Correlated detections
- Investigation & hunting

A Foundation of High-Fidelity Data

- Deep fabric
- Data management
- Data pipelines

Agentic SOC Maturity Model

Fragmented

Tool sprawl. Manual workflows throughout TDIR. Primarily reactive — the SOC responds to alerts, not threats.

- Stale asset inventory
- Alert volume > analyst capacity
- No unified case management
- Tool maintenance consumes analyst time

Unified

Consolidated TDIR. AI assistance embedded in the analyst workflow. Humans approve every containment action.

- Mission Control as single surface
- RBA replacing 1:1 alert rules
- AI Assistant for SPL and summarization
- Exposure Analytics active

Augmented

First agents in production for bounded tasks. Governance policy and SOPs in place. Agents demonstrate capability before authority is extended.

- Malware Reversing Agent in triage
- SOP Agent codifying runbooks
- Agent actions logged and attributable
- Triage Agent in pilot

Agentic

Multi-agent collaboration within human-defined boundaries. Analysts focused on threat hunting, detection engineering, and agent oversight.

- Detection Builder and Guided Response agents active
- SOAR handles containment within pre-authorized scope
- Continuous VulnOps workflow
- Human authority over consequential decisions preserved

Why Splunk

Streamline detection and response to focus on
what matters

Scale operations
by turning high-volume
data into high-fidelity
visibility



Stop threats at
machine speed with
AI and automation

The Operating System for the Agentic SOC

Stop chasing incidents. Start shaping outcomes.



Stop Threats at Machine Speed

AI Assisted Experiences
(Human –Machine)

Built-in Integrations &
Automation
(MCPs, APIs)

Agentic Orchestration
(Machine-Human)



Streamline Detection and Response

Unified Work Surface

SOAR+UEBA

TI Enrichment

AI-Driven Detection and
Response

Integrated Case Management

Scale Security Operations with the Cisco Data Fabric

Cost Controls

Out-of-the-Box
Content

Detection Studio and Playbook
Authoring



AI-powered
Data Management



Federated Search
and Analytics



AI-Native Experiences
and Platform



Machine
Data Lake

Enterprise Security

GA Now

Essentials

SIEM

Threat
Intelligence

Detection
Studio

Exposure
Analytics



AI Assistant | Detection Builder Agent |
SOP Agent

GA Now

Premier

Essentials

SOAR

UEBA

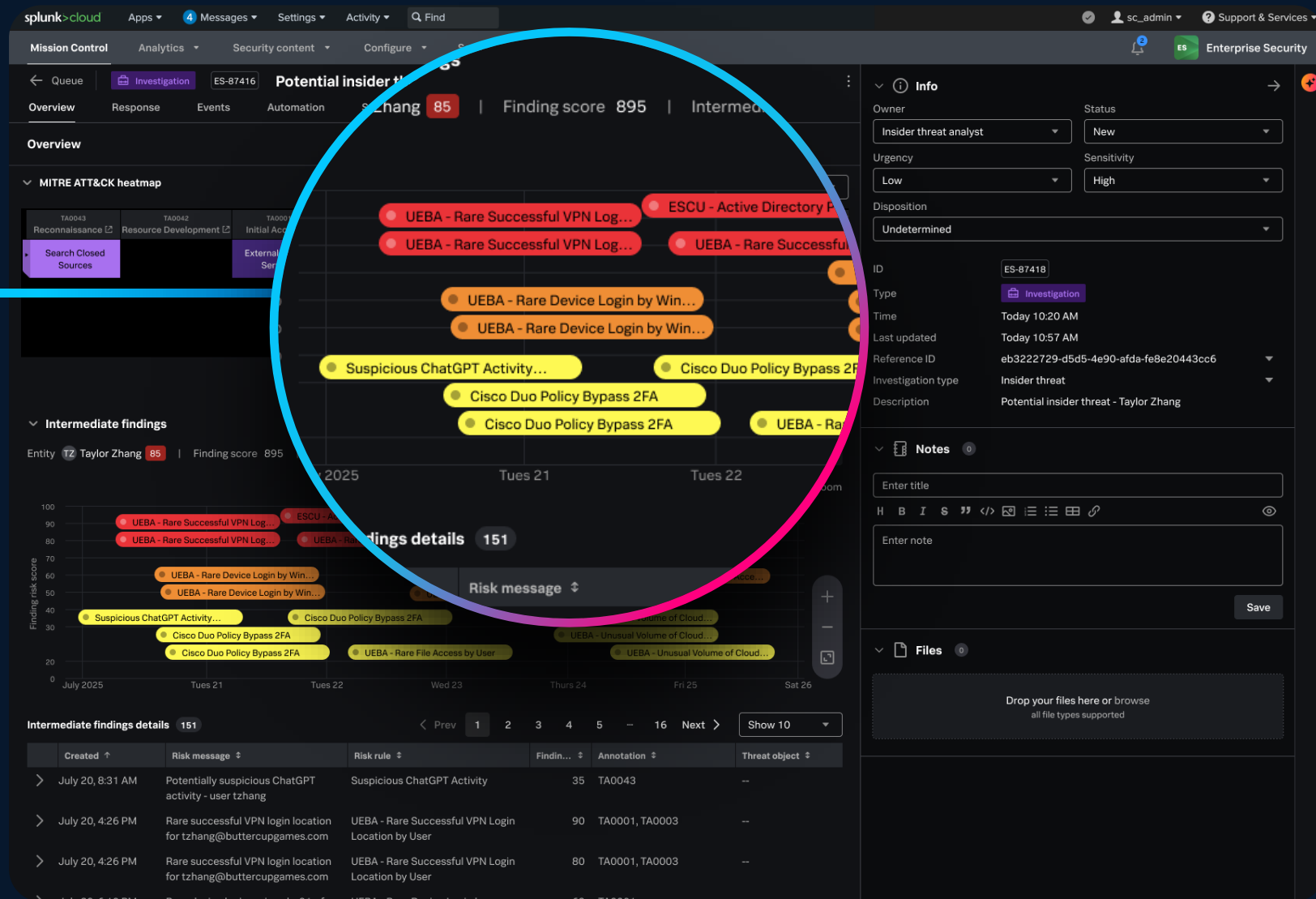
Automated
Threat
Analysis



Essentials plus Triage Agent | Malware Threat Reversing Agent
| Automation Builder Agent | Guided Response Agent*

Enterprise Security Premier Edition

- Includes UEBA, SOAR and AI Assistant
- Simplify your analyst experience
- Gain full visibility and control



Threat Intelligence Management

Accelerate investigations with integrated intelligence enrichment

- Investigate security events with relevant and normalized intelligence
- Gain more context around risk and threats targeting the organization
- Reduce noise and surface the highest fidelity intelligence for action through normalized scores from different sources

See it in action

The screenshot displays the Splunk Threat Intelligence interface for a 'Possible Phishing Attack' (ID: 2233). The interface is divided into several sections:

- Incident review:** Shows the incident title, ID, and a 'Phishing' tag.
- Intelligence:** The main section for threat object enrichment.
- Threat object:** A table listing various threat objects with their types and names.

TYPE	NAME
IP Address	10.11.36.20
IP Address	80.94.92.239
MD5	9e779da82d86bc...
SHA1	66ddb290df3d51...
SHA256	016c91035fec25...
IP Address	64.62.197.0
IP Address	64.62.197.0/24
IP Address	64.62.197.182
MD5	1f9bfb6b43rdfjsw...
URL	badurl.com
Threat actor	DEEP PANDA
IP Address	APT 17
URL	yingjikuaijie3.net
URL	system.net
- Observable overview:** Provides a summary of the threat object's observables.
 - Observable Type: IP Address
 - Last Reported On: 07/02/2022, 2:42 PM
 - Total IOCs: 80
 - Enclaves: All Sources Workflow, BBVA, Splunk ES
 - Tags: Suspicious, Investigation
- Most recent reporting from each source:** A table showing the most recent reports from various sources.

Timestamp	Source	Passthru score	Normalized score
02/05/2022, 2:42 PM	VirusTotal	99	High
02/05/2022, 2:42 PM	Recorded Future	52/70	High
02/05/2022, 2:42 PM	VIV	Medium	Medium
02/05/2022, 2:42 PM	digital shadows_	37	Medium

SOAR: Unify security operations and workflows

- **Native SIEM-to-SOAR workflows.** Trigger, run, and monitor playbooks directly from detections to automate triage, investigation, and response all in one place.
- **Seamless orchestration across your security stack.** Get more out of your security stack with the ability to integrate across 300+ third-party tools with support for 2,800+ automated actions
- **Reduce manual toil and MTTR.** Auto-handle low-severity incidents and repetitive tasks in seconds so analysts focus on high-impact investigations.

See it in action

The screenshot displays the Splunk SOAR web interface. At the top, a navigation bar includes 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', and a search bar. Below this, a header section shows 'Mission Control', 'Analytics', 'Security content', 'Configure', 'Investigate Tools', and a search bar. The main content area is titled 'Automation' and features a list of playbooks on the left and a detailed view of the 'Insider Account Based Prep' playbook on the right. The playbook view shows its status as 'Success', owner as 'Dgamer@splunk.com', and a table of actions. A 'View logs' button is present. A red box highlights the 'Open playbook' link. A red box also highlights the 'Add' sidebar, which contains sections for 'EXECUTE ACTIONS' (Action, Playbook, Code, Utility), 'PROCESS FILTERS' (Filter, Decision, Format), 'HUMAN INPUT' (Prompt), and 'SPLUNK API' (Enterprise Security). The main workflow diagram on the right shows a sequence: Start -> ACTION get attributes -> ENTERPRISE SECURITY API add finding or investigation note -> End.

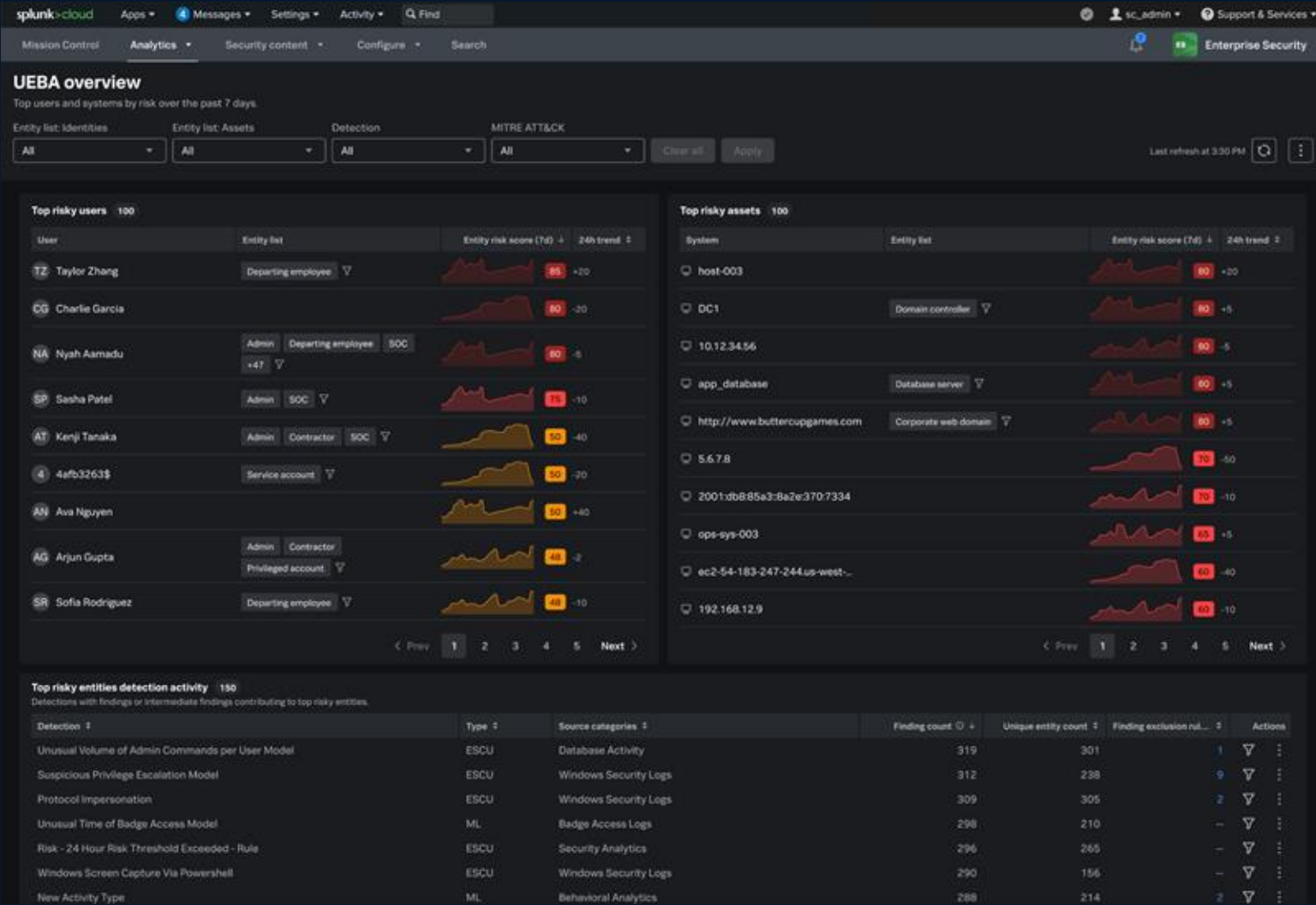
User & Entity Behavior Analytics

Part of ES Premier

Insider and advanced threat detection using advanced ML

Premium user centric workflows leveraging data already sent to Splunk

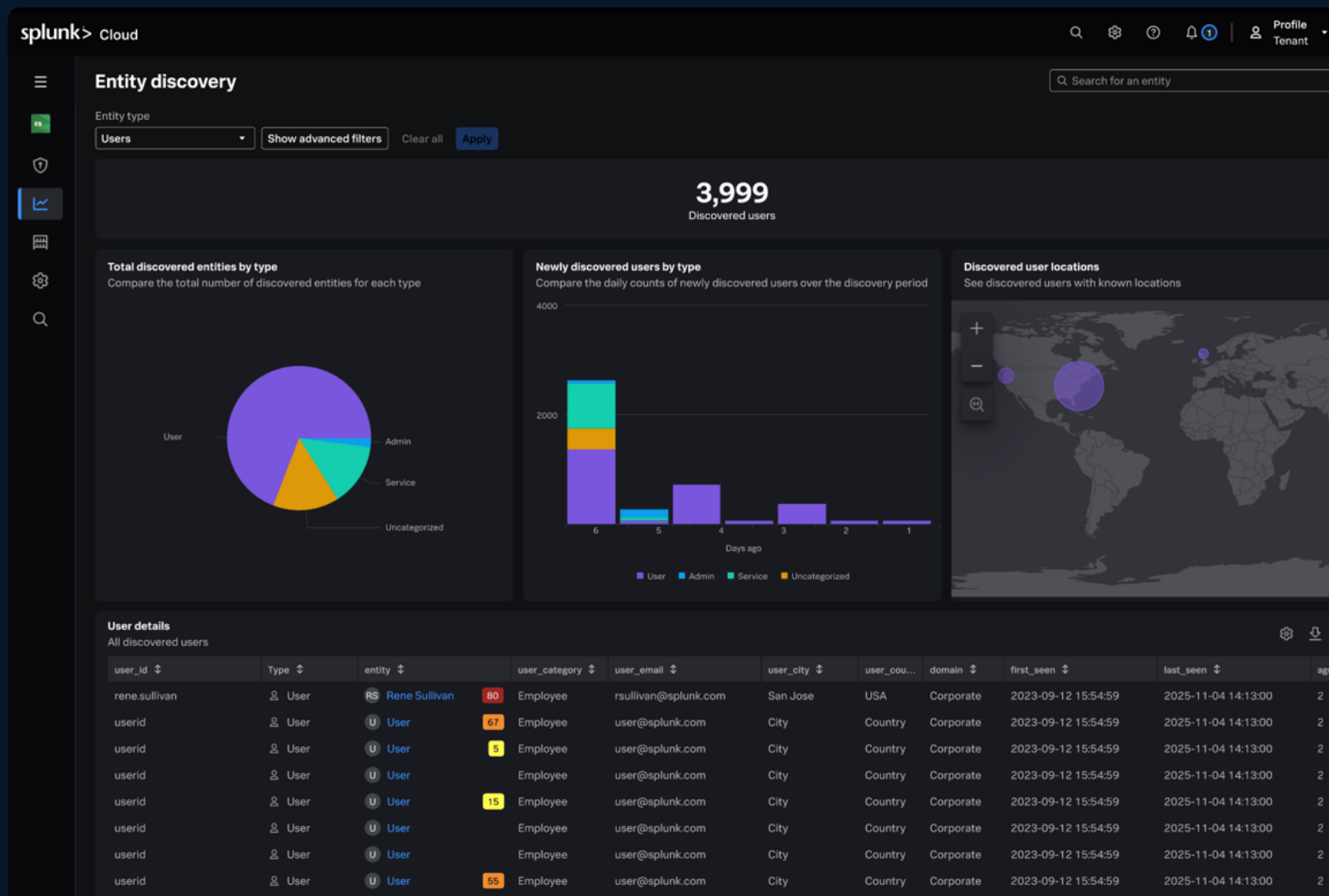
Tightly integrated with ES



Exposure Analytics

Introducing Exposure Analytics into Unified TDIR Platform

Exposure Analytics shifts security posture from reactive to preventive by unifying fragmented data and closing attack surface visibility gaps to provide a holistic view of assets, identities, and relationships.



Driving proactive security outcomes with Exposure Analytics



Continual Entity Visibility

Accelerate security investigations and ensure operational hygiene

For: SecOps Engr, Security Eng, IT Ops



Exposure Visibility And Posture

Identify gaps in security controls and strengthen security posture

For: Security Eng, IT Ops, GRC Supporting teams



Contextual Prioritization

Leverage contextual risk to prioritize investigations, hardening and remediation

For: IT Ops, SecOps, VM, Security Eng

Powering the **Agentic SOC**

Simplify the Analyst
Experience

Accelerate the SOC
with agentic AI

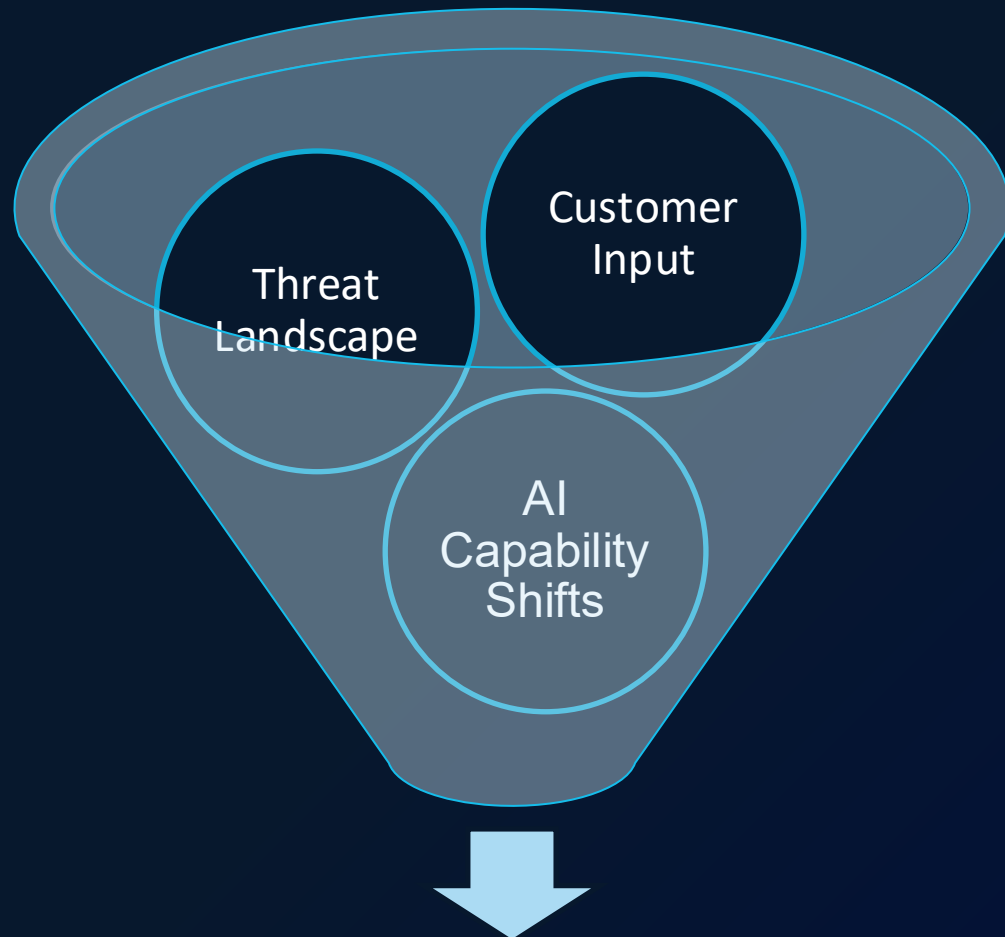
Expand detection
and visibility

Volume --> Value

Friction --> Flow

Silos --> Synergy

Patterns informing Splunk's AI strategy



Patterns informing Splunk's
AI strategy

- **AI assistant adoption has universal momentum**

- Investigation Assistance
- Automation Authoring
- Detection Engineering

- **Task agents in production use; fully agentic -> early**

- Specific task (e.g. Reverse Malware) – in production use
- Alert (e.g. Triage Alerts) – gaining traction
- Agentic across alerts (e.g. Optimize Detections) – early

- **Building trust in AI Agents - transparent and extensible**

- Fully auditable reasoning, execution with validation checks
- Customizable to perform inline with organizational SOPs
- Captures local knowledgebases / memory as needed

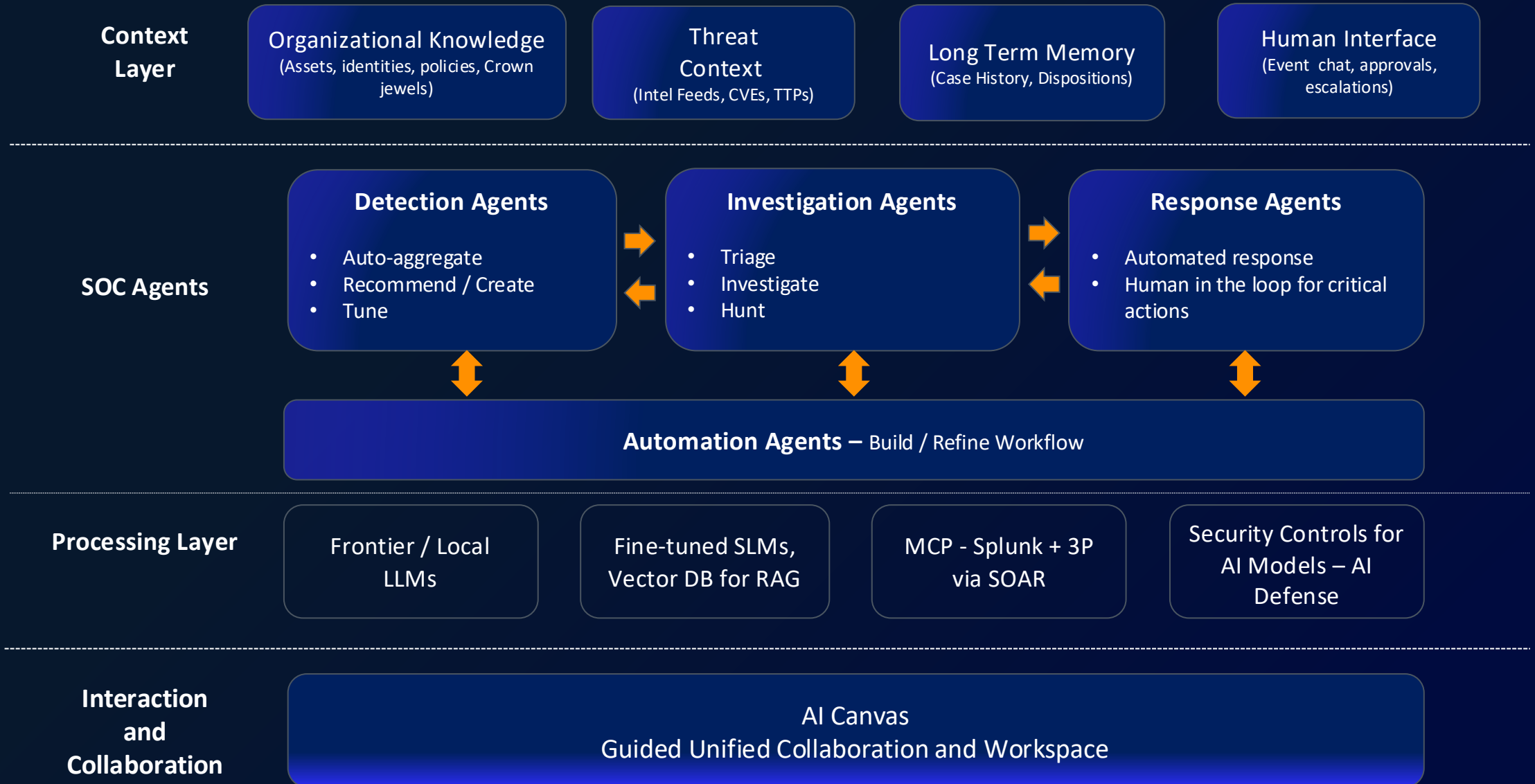
- **Higher UX expectations – AI embedded in Workflows**

- Approve AI recommendations vs start from scratch
- UIs need to be dynamic and support agent, human interaction

- **Democratization of security engineering**

- I can write a document describing it -> build it
- Use-cases leverage tools exposed by the SIEM

Agentic SOC Architecture



AI Assistant in Enterprise Security

- Embedded across all analyst workflows
- Guide investigations with AI-powered query generation and summarization
- Accelerate workflows with embedded, context-aware AI insights
- Empower decisions with AI-driven next step and remediation guidance

Currently available for Cloud users

Settings ▾ Activity ▾ Find

Security content ▾ Configure ▾ Search

Findings groups ▾ Findings ▾ AI disposition ▾

< Prev 1 Next > Show 20 ▾

ID	Entity
FI-AB543	Charlie
FI-AB198	Nyah
FI-AB029	52.216
FI-AB274	10.34.56.3
FI-AB558	8.108.191.101
FI-AB352	Kenji Tanaka

AI Assistant for Security

Malicious PowerShell execution

AI Today, 8:30 AM

Finding summarization

On July 25, 2025, an obfuscated PowerShell command was executed using the - EncodedCommand flag by a low-privilege user during off-hours. The script contacted a known C2 domain (185.99.132[.]22) linked to the MuddyWater APT group, as confirmed by Cisco Talos threat intel.

Sandbox analysis showed the script downloaded a second-stage payload, created a scheduled task, and attempted credential theft. Shortly afterward, the host initiated SMB-based lateral movement, indicating early-stage compromise activity. Given the behavioral indicators and threat intel correlation, this is assessed as a True Positive requiring immediate response.

Position: True positive

Reject Accept

This finding is likely a true positive based on following:

- Command Behavior: Obfuscated script, spawned by powershell.exe
- Sandbox Result: Credential theft + scheduled task creation
- Threat Intel: Talos C2 match
- User Context: Unusual activity from low-privilege user during off-hours
- Lateral Movement: SMB events observed post-execution

Splunk Attack Analyzer

Severity: Critical

AI analysis

Malicious - Script downloads an MSI from a remote host and silently installs it via msexec. Uses WebClient to fetch payload, silent installation, file cleanup

Cisco Talos

Results: Compromised

Ask me anything about...

Summarize the findings Generate investigation report Suggest SPL Discover AI Assistant skill

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

> Related investigations > History

Response automation and summarization

- Coordinate IR teams.
Automatically.

- Automatically create a war room
- Automatically summarize war room updates on the investigation
- Collaborate across your team to resolve threats faster

The screenshot displays the Splunk Cloud Enterprise Security interface for an investigation titled "24 hour risk threshold exceeded for user=cgarcia". The interface is divided into several sections:

- Navigation Bar:** Includes tabs for Queue, Investigation (selected), Events, Search, Automation, and Intelligence. A "Create Webex war room" button is visible.
- Overview Tab:**
 - MITRE ATT&CK map:** Shows intermediate findings.
 - Additional fields:**

Entity bunit	america
Entity priority	high
Entity type	user
MITRE	T1098, T1113
Original Splunk source	Network - unusual volume of network..., Network - vulnerability scanner detec...
Security domain	threat
 - Cisco Talos threat intelligence:**

Last updated	Aug 31, 2025 9:15 AM
Threat level	Untrusted
Threat categories	Spyware and Adware
 - Event:**

Event ID	6d7ba246-4cad-49a9-82ce-ebc6970262ce@inotable@6d7ba2464cad49a982ceebc6970262ce
Event type	modnotable_results, notable, risk_notables
- Related Investigations:** Includes History, Drill-down search, Drill-down dashboard, and Original event.
- Adaptive responses:** A table showing responses:

Response	Mode	Time	User	Status
Risk analysis	Saved	2024-01-05T16:31:39+0000	admin	Succ...
Notables	Saved	2024-01-05T16:31:39+0000	admin	Succ...
- Right Sidebar:**
 - Info:** Owner (Unassigned), Status (New), Urgency (Medium), Sensitivity (Unknown), Disposition (Undetermined), ID (ES-AB543), Type (Investigation), Time (Today 10:20 AM), Investigation type (Default), Description (Risk Threshold Exceeded for an object over a 24 hour period), Detection (Risk - 24 hour Risk Threshold Exceeded Rule).
 - Notes:** Search notes, AI-generated summary, and action items.

Triage Agent

- Streamline alert prioritization
- Plan and execute investigations
- Automate insights to reduce MTTR

The screenshot displays the Splunk Triage Agent interface. The top navigation bar includes 'splunk>cloud', 'Apps', '4 Messages', 'Settings', 'Activity', and a search bar. Below this, there are tabs for 'Mission Control', 'Security analytics', 'Security content', 'Configure', and 'Settings'. The main content area is titled 'Analyst queue' and features a search bar and filters for 'All types', 'Investigations', and 'Findings'. A dropdown menu is open, showing 'AI suggested disposition' with options: 'True positive' (checked), 'Benign positive', 'False positive', 'Other', and 'Undetermined'. The queue lists several alerts, including 'Malicious PowerShell execution', '24 hour risk threshold exceeded user=administrator', 'Possible Phishing Attack', 'Unusual network activities detected from 52.218.245.82 to 52.216.133.181', '3 failed login attempts within 24 hrs on device 10.34.56.354', 'Threat Activity Detected from 56.143.202.14 to 8.108.191.107', and 'Email files written outside of the Outlook directory'. The interface also shows a sidebar with 'Default views' and a list of items like 'Owned by me', 'Unassigned', 'Risk score', 'Saved views', 'My critical items', 'Unassigned SLA expiring', and 'Insider threat'.

Malware threat reversing agent

- Actionable insights in seconds. Not hours.
- Explains malicious scripts step-by-step
- Extracts IOCs, flags evasion, and maps to MITRE TTPs
- Reduces bottlenecks due to a lack of coding language expertise

AI analysis

Summary

MITRE TTPs

IOCs and Recommendations

100 Malicious

Script downloads an MSI from a remote host and silently installs it via msisexec. Uses WebClient to fetch payload, silent installation, file cleanup

Technical Analysis

- Step 1: Configure PowerShell to use TLS12 for secure connections
- Step 2: Define the URL for the MSI payload
- Step 3: Construct the temporary file path in the %TEMP% directory
- Step 4: Instantiate a WebClient object and set a custom User-Agent header
- Step 5: Download the MSI from the remote server to the temporary path
- Step 6: Verify the downloaded file exists at the temporary location
- Step 7: Invoke msisexec.exe to install the MSI silently with no restart
- Step 8: Remove the MSI installer file after successful installation
- Step 9: Handle any errors during download or installation and perform cleanup
- Obfuscation techniques identified: None

Relevant code

```
[Net .ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]:: Tls12
```

Description

TLS configuration for Power Shell remoting (Step 1 from analysis)

Purpose

Enforces usage of TLS1.2 for secure network communications. Prevents fallback to weaker SSL/TLS protocols.

Example matching Regex

Disposition

True positive

ID

ES-00004

Type

Investigation

Time

Today 10:20 AM

Last updated

Today 10:20 AM

Reference ID

84b056d2-9263-49b8-ad5b-c322f81da461

Investigation type

Default

Description

This detection identifies the execution of potent..

Show more

Notes

Enter note

Save

Files

Drop your files here or browse all file types supported

Automation Builder Agent

Accelerate time to
automation

- Translate natural language intent into functional, tested SOAR playbooks
- Enable more teams to contribute

The screenshot displays the Splunk SOAR Automation Builder Agent interface. The main window shows a playbook titled "Microsoft_Teams_War_Room" with a "1 Missing Configuration" warning. The playbook steps include:

- UTILITY: custom list enumerate
- ACTION: add channel number
- CODE: notify create time
- UTILITY: set meeting start time
- UTILITY: set meeting end time
- PROMPT: confirm create teams meeting
- ACTION: create teams meeting

The left sidebar shows the "Add" menu with options: EXECUTE ACTIONS (Action, Playbook, Code, Utility), PROCESS FILTERS (Filter, Decision, Format), and HUMAN INPUT (Prompt). The right sidebar features the "SOAR AI Assistant" panel with the following content:

received

5. Time manipulation utilities
The datetime utilities warn because:

- Input timestamps depend on a prior action
- Formatting must match Teams API expectations

✓ Your formats are valid ⚠ Warning exists in case upstream data is missing or malformed

Bottom line
You're seeing warnings because this playbook:

- Is **intentionally opinionated**
- Uses **hard-coded configuration**
- Assumes **happy-path execution**

✓ **Nothing is broken** ✓ **Safe to run** ⚠ Warnings are about **robustness, reuse, and edge cases**

If you want, I can:

- Walk through **each warning block-by-block**
- Help you **eliminate all warnings**
- Suggest a **"production-hardened"** version of this playbook

Just tell me how strict you want it to be.

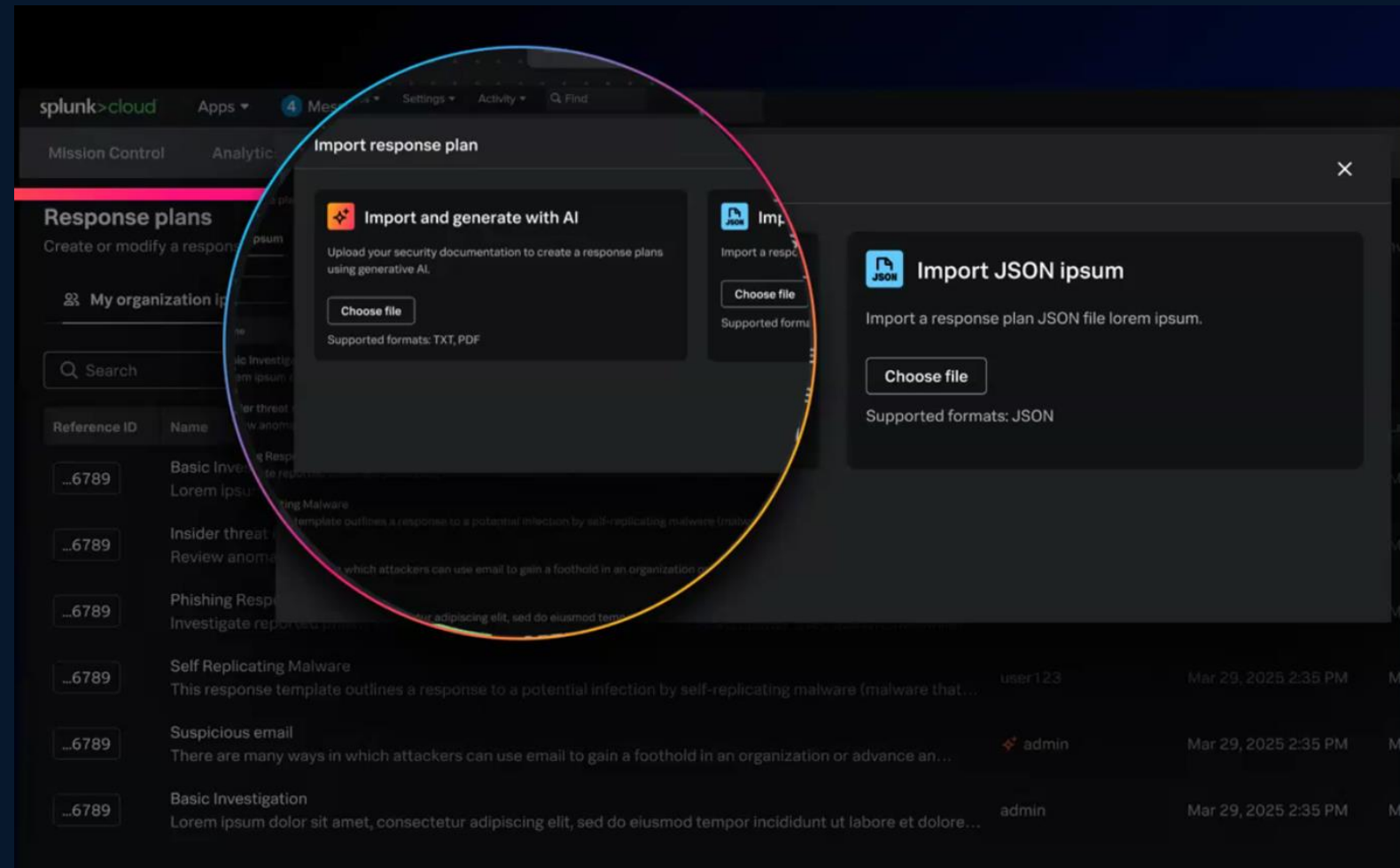
Ask me anything about...

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

SOP Agent

Accelerate time to automation

Import SOPs into Splunk ES response plans to align AI-driven responses with your organization's operational standards.

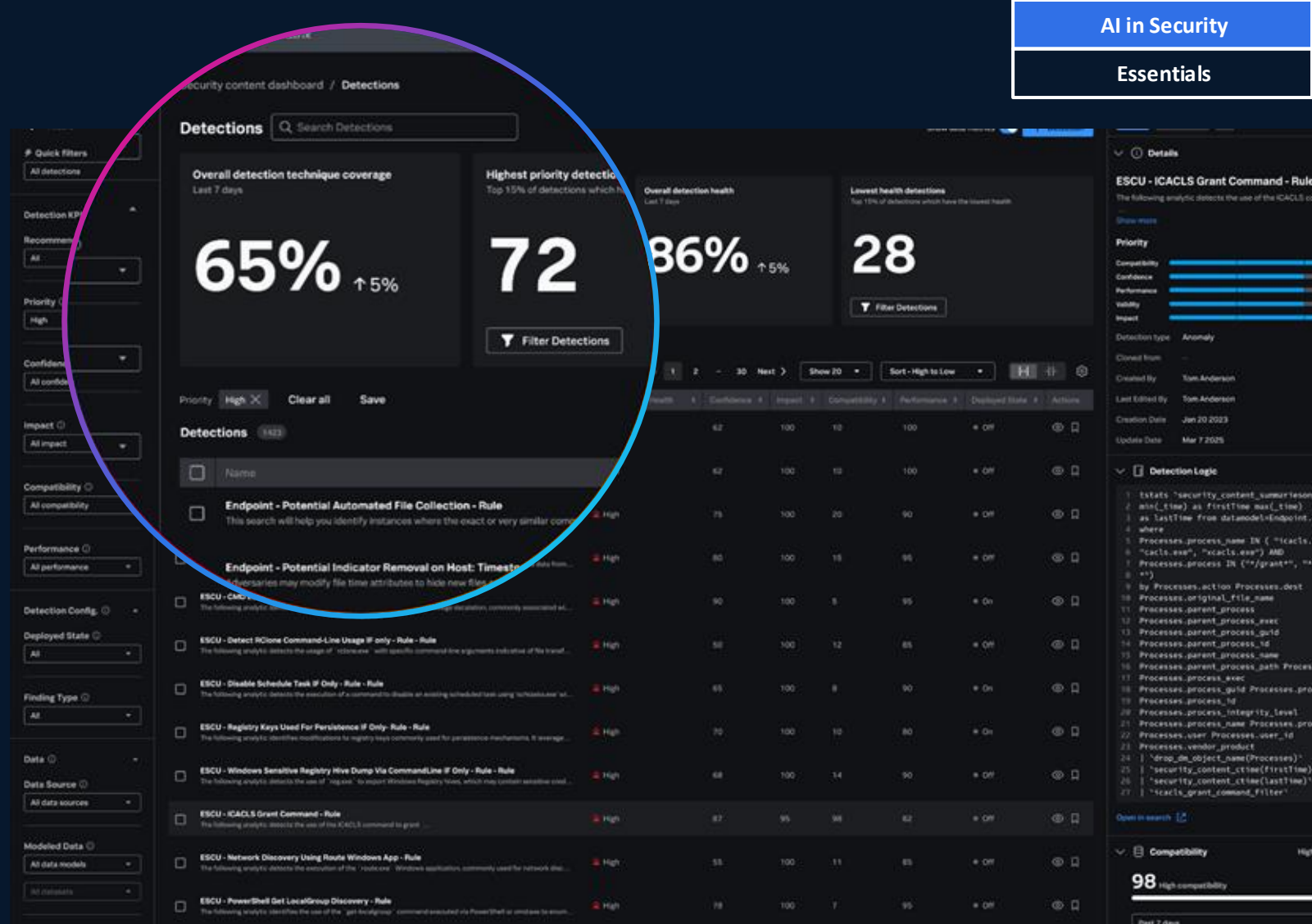


Detection Builder Agent

From hypothesis to production
in minutes

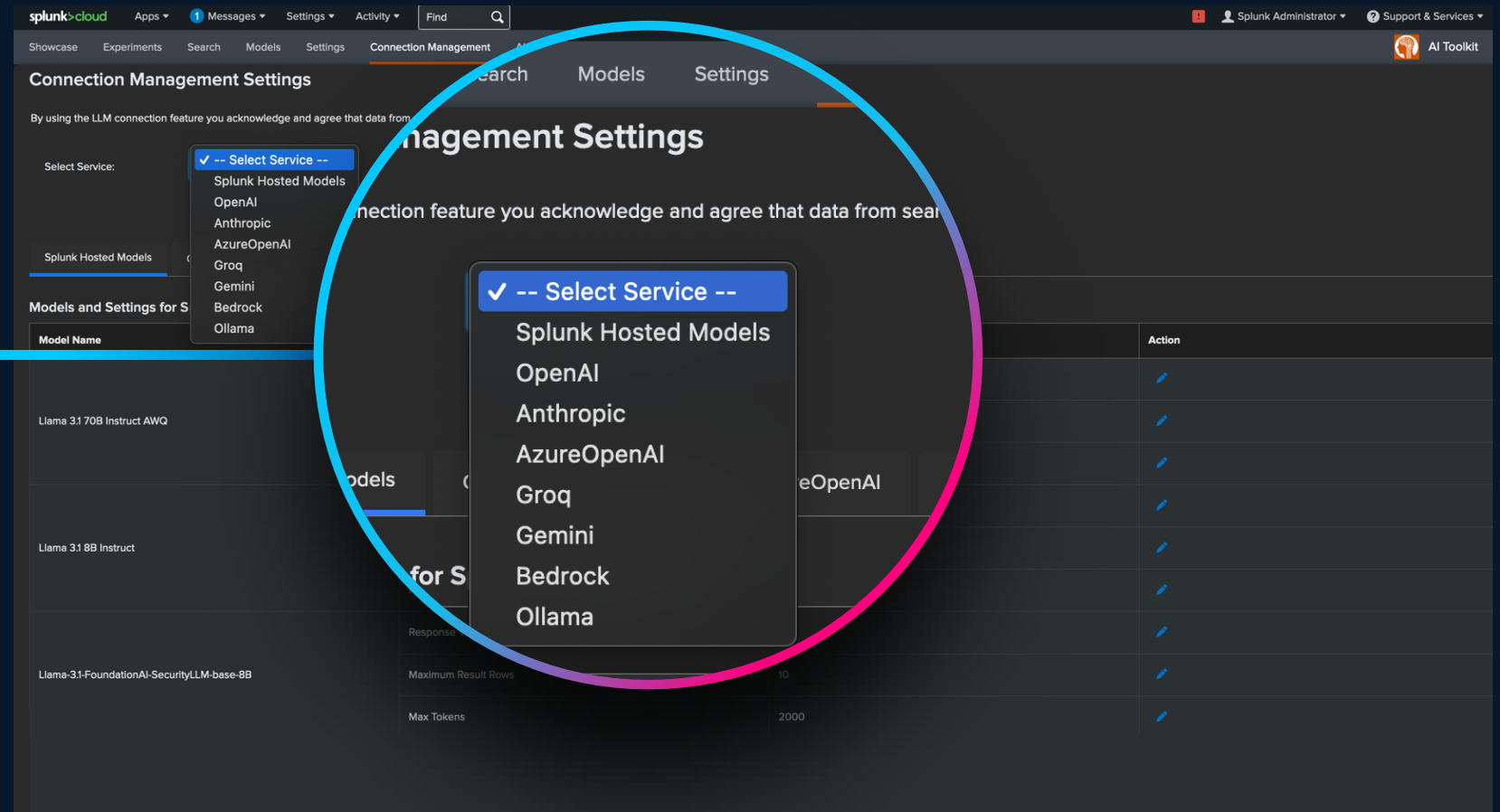
Streamline detection engineering:
import, tune, and personalize content to
move from hypothesis to production in
minutes.

See it in action



AI Toolkit with LLM Integrations

- Access secure AI/ML models
- Avoid AI infra maintenance
- Start faster with more flexibility



Guided Response Agent

Enrich findings with tool calls

Provide real-time context and in-workflow actions based on standard operating procedures (SOPs) to ensure rapid, compliant resolution.

* Cloud only

The screenshot displays the Guided Response Agent interface. At the top, a message from 'Tim Tailor' dated 'Sep 03, 6:34 PM' says 'Run a url reputation action'. Below this, an AI assistant icon responds: 'Sure I can help with that. I can use VirusTotal to run a 'url repation action'.' The assistant then provides context: 'Multiple URLs were found in this investigation. Based on phishing indicators, I recommend running a URL reputation check on the final redirect / landing page URL' and lists a specific URL: 'https://marketing.pipelinepub.com/acton/ct/11876/s-073e-2508:0/Bct/q-0697/1-03fc:73b/ct35_0/1/lu?sid=TV2%3AiGG9pwUZu'. Below the text is a configuration panel for the 'url reputation' action. It shows the connector 'VirusTotal' and the action 'url reputation'. The connector configuration is 'VirusTotal_v2' and the URL is 'https://marketing.pipeli...'. There are 'Run' and 'X' buttons at the bottom of the panel. At the very bottom of the interface is a search bar with the placeholder 'Ask me anything about...' and a 'View AI details' link.

Tim Tailor Sep 03, 6:34 PM
Run a url reputation action

Sure I can help with that. I can use VirusTotal to run a 'url repation action'.

Multiple URLs were found in this investigation. Based on phishing indicators, I recommend running a URL reputation check on the final redirect / landing page URL
'https://marketing.pipelinepub.com/acton/ct/11876/s-073e-2508:0/Bct/q-0697/1-03fc:73b/ct35_0/1/lu?sid=TV2%3AiGG9pwUZu', since that is the one most likely to host the malicious payload or credential harvesting site.

url reputation
VirusTotal • VirusTotal_v2
url: https://marketing.pipelinepub.com/acton/ct/11876/s-073e-2508:0/Bct/q

Action details

Connector	Connector configuration
VirusTotal	VirusTotal_v2
Action	url
url reputation	https://marketing.pipeli...

Run X

Ask me anything about...

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

Delivering productivity increases when investigating security incidents

Scenario: Security analyst is investigating a high priority RBA finding

With AI Assistant (in minutes*)

1. **Summarize findings within an Investigation**
 - a. Leverage Gen AI to generate a summary of findings and relevant MITRE ATT&CK techniques and tactics
2. **Generate SPL queries to investigate data**
 - a. Leverage Gen AI to suggest investigative SPL queries based on natural language prompts
3. **Conversational security inquiries**
 - a. Have security topic related conversations
4. **Generate post-investigation report**
 - a. Leverage Gen AI to create an Investigation Report capturing timeline of events, analyst investigation notes, and MITRE ATT&CK info

Without AI Assistant (~hours*)

1. **Review findings**
 - a. Manually review all correlated alerts and metadata to better understand the incident
 - b. Manually research tactics and techniques to better understand the incident
2. **Formulate investigation strategy**
 - a. Leverage tribal knowledge and experience to determine investigation next steps
3. **Broaden the investigation**
 - a. Using tribal knowledge and experience expand the investigation beyond initial findings by manually authoring investigative SPL queries
4. **Post-incident summary report**
 - a. Manually summarize and document initial findings, remediation actions, and other relevant information to close the incident



Turnkey AI that speeds up the path to innovation



AI-ready data

Connect and govern telemetry for accurate and auditable AI.



Augmented skills

AI assistants help non-experts answer the why.



Agentic acceleration

Supervised agents in a collaborative workspace cut time to resolution.



Differentiation with AI

Train custom models and create unique business outcomes.

What if you could stay ahead?

Detect and react → Predict and prevent

A person stands on a rocky ridge, looking out at jagged, snow-dusted mountains under a sky transitioning from purple to pink. Abstract streaks of yellow, orange, and pink light cut across the upper right corner. The words "Thank You" are centered in a large, sans-serif font, with "Thank" in light blue and "You" in a gradient of pink, purple, and blue.

Thank You