

Future for Security Operations

Walk through the Modern SOC


Rob Gresham, Principal Engineer, Splunk Security
Recovering DFIR/SOC Analyst

AJ Shipley, Vice President of Splunk Security Products, Cisco



Our world is continuously changing
and so has *everything* you do



A network diagram with red nodes and blue lines, overlaid on a glowing blue globe. The globe is composed of a grid of blue dots and lines, creating a sense of depth and connectivity. The network nodes are represented by red circles of varying sizes, connected by thin blue lines. The overall aesthetic is futuristic and digital.

**Threat actors do not discriminate
based on an organization's size or
vertical.**

Your teams cannot be masters of all tools and possibilities



Know
Every host



Record
Every conversation



Understand
what is **normal**

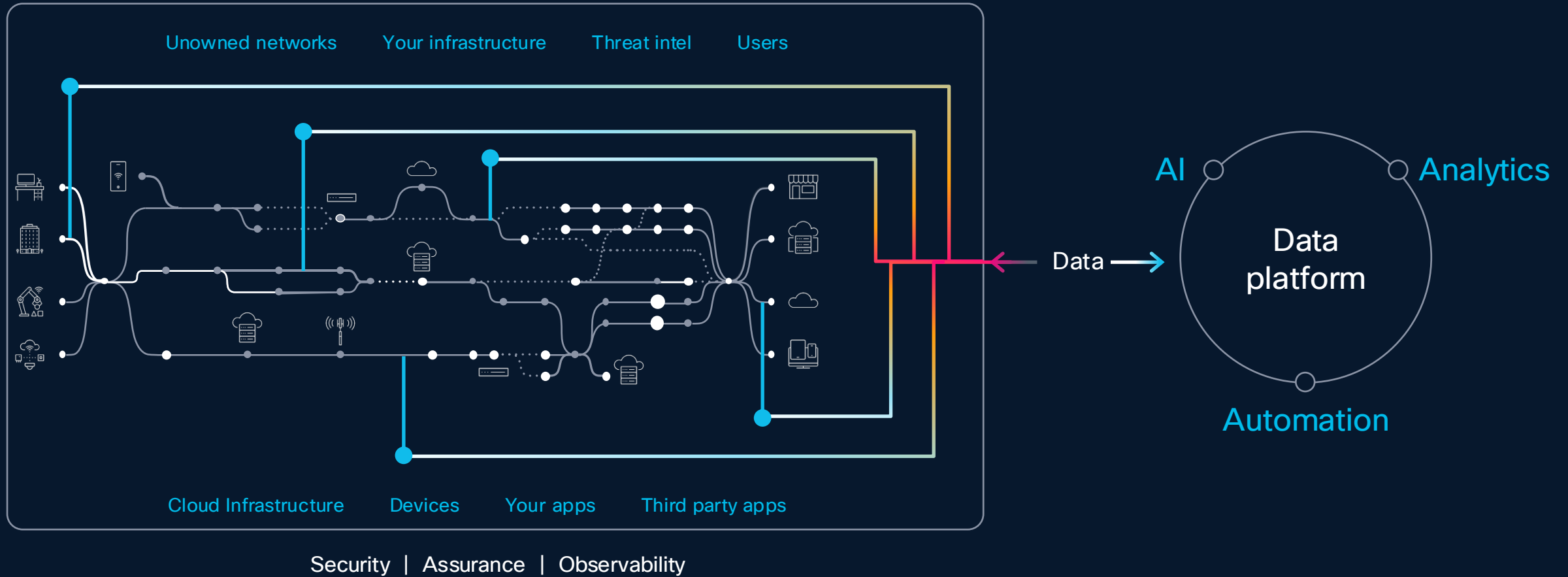


Be alerted to
change



Respond to
threats quickly

The power of Splunk and Cisco means you can unify data, detection, investigation, response and prevention



We are dedicated to
accelerating your
journey to realizing value



Cisco powers your technology advancements

Cisco Cloud Control

AI-ready data centers

Transform data centers to power AI workloads anywhere

Public and private clouds, on-premises, edge

Future-proofed workplaces

Modernize everywhere people work and serve customers

Campuses, branches, factories, homes, cars, hospitals, stadiums, hotels, and beyond

Digital resilience

Keep your organization secure, reliable, and performing with game-changing security, assurance, and observability across the entire digital footprint



Accelerated by Cisco AI



Cisco Security Cloud Platform

AI Powered Cisco Security Cloud: Cisco shines where Security meets the Network

Future-Proofed Workplaces



**Accelerate Zero Trust
Network Access**

Identity | SSE

User Protection Suite

AI-Ready Data Centers



**Secure Data Center
Networking**

Segmentation | Firewall

Cloud Protection Suite

Digital Resilience



**Power
Security Operations**

XDR | SIEM | SOAR

Splunk Security
Breach Protection Suite



The New Security Operating Model

Unify the data fabric, tooling, AI and automation in an analyst experience, to identify and stop threats before they impact the business.

What Cisco Brings to the Security Problem

Cisco Cloud Control

Unified Investigations where *Observability* meets *Security* with Digital Resilience

AI Assistant

Cisco Security Cloud

AI Canvas

Security Analytics and Response
Splunk Security and Cisco XDR

User Protection
Universal ZTNA

Cloud Protection
Hybrid Mesh Firewall

Breach Protection
Email, EDR, NDR, XDR

AI for security

Security for AI

Identity Intelligence

Cisco's Operating System for the Agentic SOC

Stop chasing incidents. Start shaping outcomes with a TDIR platform.



Surge Ahead of Attackers with AI and Automation

AI Assisted Experiences
(Human -Machine)

Built-in Integrations &
Automation
(MCPs, APIs)

Agentic Orchestration
(Machine-Human)



Simplify the Analyst Experience

Unified Work Surface

XDR+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



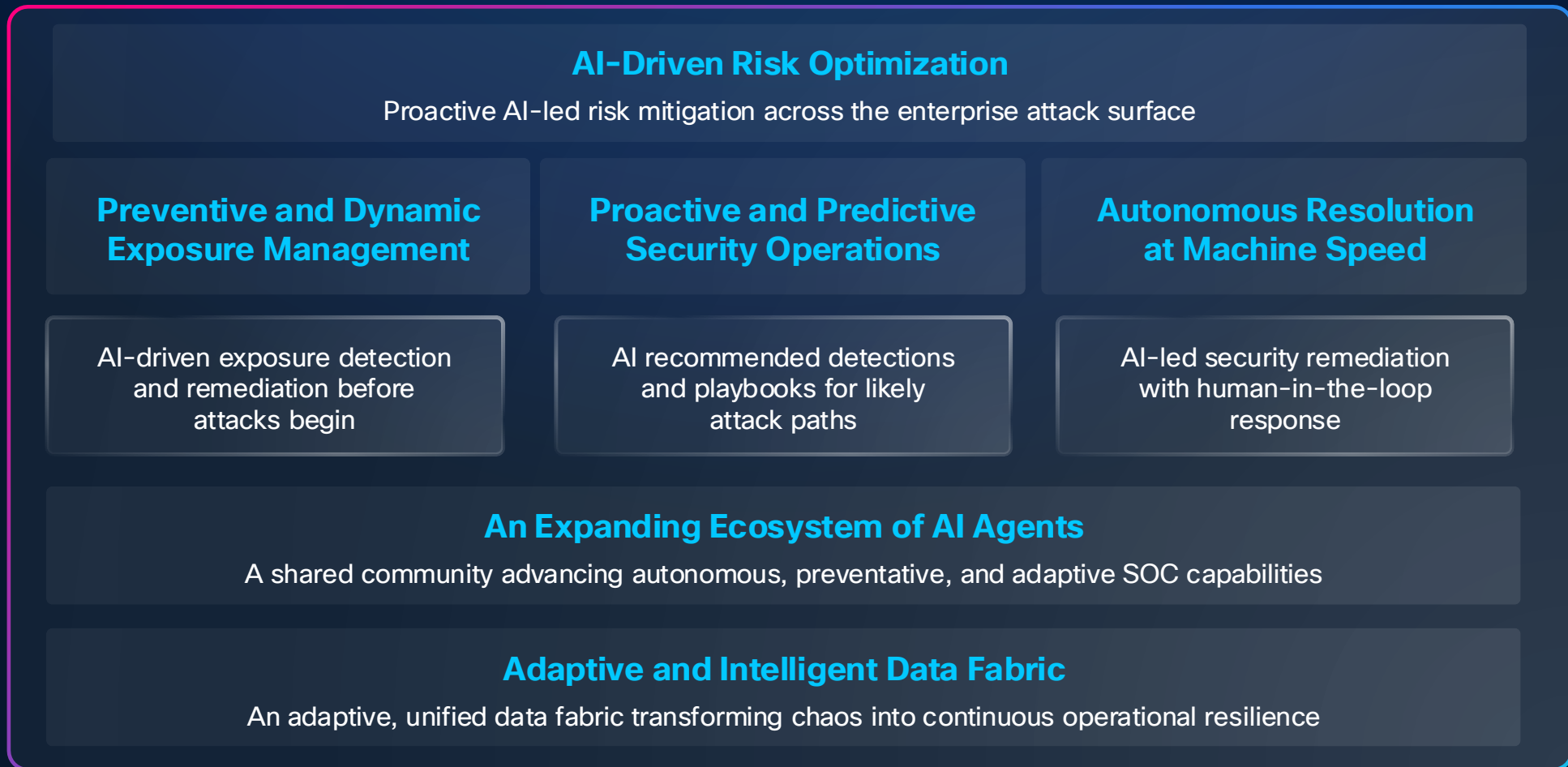
AI-Native Experiences
and Platform



Machine
Data Lake

Splunk Security's Product Forward-Vision

The future is rooted in the Agentic SOC -- where human expertise, AI, and data work together as a force multiplier, transforming heterogenous signals into decisive action against all emerging threats.



Unify the SOC platform

Unified Threat Detection, Investigation, & Response

Federated data
management

Advanced threat
detections

AI-accelerated
investigations

Automated
response

Unified security analyst experience

Better Together: SOC of the Future

Innovative XDR + Market Leading SIEM = **Unified TDIR**

Federated data
management

Advanced threat
detections

AI-accelerated
investigations

Automated
response

Unified Inventory

EMBEDDED AI

CONTENT AND THREAT RESEARCH



User/Cloud/
Breach/



Networking



Third-party
tools



Talos



Clouds



Devices



Data
centers



Applications

The background is a dark blue, isometric digital environment. It features several laptops and server racks scattered across a grid of glowing lines and nodes, suggesting a network or data center. The lighting is soft and focused on the central text.

XDR \neq EDR++

Email

Network

Cloud

Firewall

Endpoint

Identity



SECURITY TOOLS

Cisco XDR



An equal seat at the table

Cisco XDR

Improve Alert Fidelity

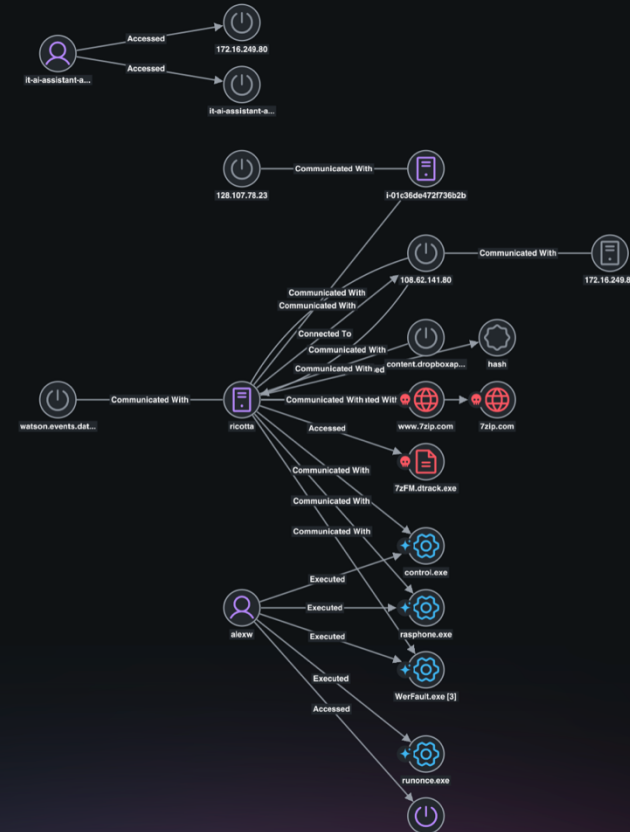
Instant Attack verification
with a clear verdict

Command Every response
and action

Single place to see all
Security Alerts

Network at the core

The screenshot shows the Cisco XDR interface. At the top, it says 'Incidents' with a 'Beta' tag. The main incident title is 'Malicious: Dtrack Backdoor Compromise with 109.8 MB Exfiltration on ricotta and EC2'. Below the title, there are tabs for 'Overview', 'Response', 'Evidence', 'Worklog', and 'Report'. The 'Overview' tab is active, showing a 'Decisive True Positive' and 'High confidence' status. It lists data sources and MITRE categories (Exfiltration, Command and Control, Discovery). The 'Impact' section, labeled 'AI-generated', contains three bullet points: 'Confirmed Data Exfiltration: 109.8 MB exfiltrated to Dropbox API...', 'Two Assets Fully Compromised: Both ricotta (Windows workstation with RDP/Kerberos roles) and EC2 i-01c36de472f736b2b (Web/Terminal Server) are assessed COMPROMISED...', and 'Possible Insider Threat or Full Account Compromise: alexw 's interactive SSH access to the C2 server...'. The 'Summary' section, also 'AI-generated', provides a detailed narrative of the attack, mentioning the user 'alexw', the malware 'Dtrack backdoor', and the exfiltration of 109.8 MB to Dropbox. At the bottom, there are expandable sections for 'Reasoning' and 'Evidence'.



Instant Attack Verification

Each alert is analyzed by AI agents to eliminate **false positives**

Turns complex attacks into **visual narratives** with explanation summary

Multiple AI agents launch investigation plan to **verify** real attack with a **clear verdict**

Clear Verdict to trigger a **decisive response** through automated playbooks

← Incidents

Beta

Malicious: Dtrack Backdoor Compromise with 109.8 MB Exfiltration on ricotta and EC2 Open: Investigating Unassigned

Overview Response Evidence Worklog Report

← Decisive True Positive High confidence ⓘ

Data sources: Custom Security Event, Cisco XDR, Meraki, Cisco Secure Network Analytics, Cisco Secure Access, Cisco Secure Endpoint

MITRE: Exfiltration Command and Control Discovery +10

Impact AI-generated ▾

Summary AI-generated ▾

Recommendations AI-generated ▲

Dynamically AI-generated and prioritized actions based on current findings to help you respond quickly and effectively. More recommendations are available for full incident response.

Identification 0 ▾

Containment 7 ▾

Eradication 2 ▾

Recovery 2 ▾

Analysis ▲

AI-generated summaries of device and user activity, combining insights from asset data and detection findings for clear classifications.

Device: ricotta ⌵

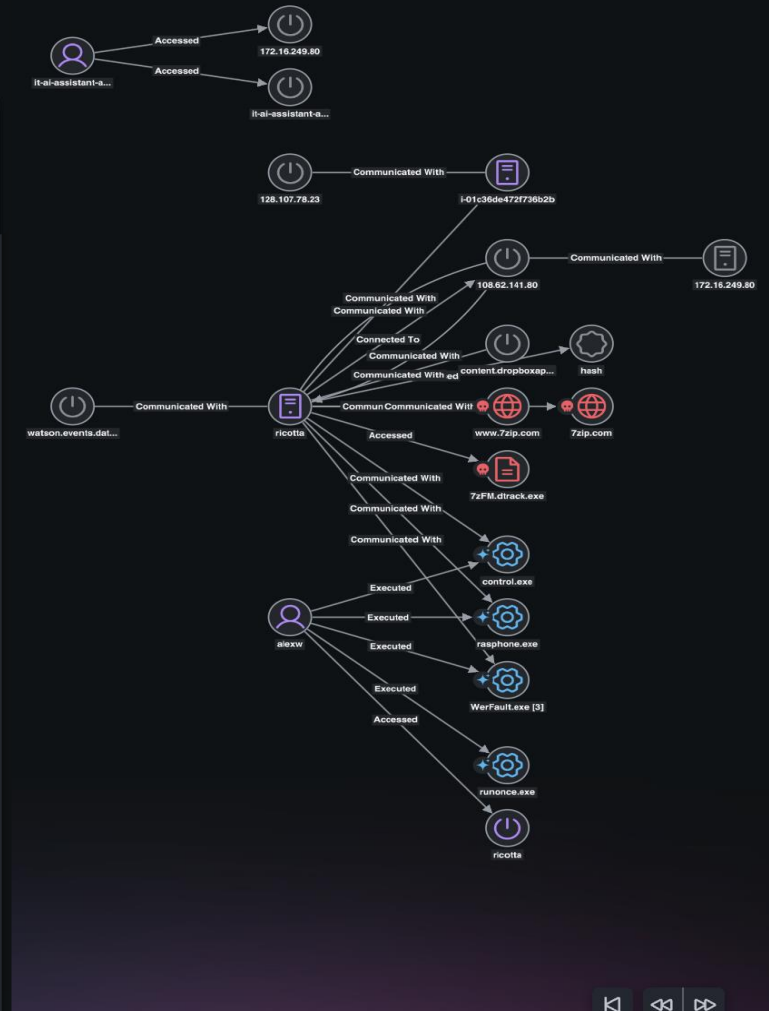
Compromised High confidence ⓘ

Workstation ricotta (user alexw) was fully compromised by the Dtrack backdoor (SHA-256 63fd5e9c7b6c5a8efe57d2922b2ef638e243bac30ffc746f3c67b785374bc7d5), attributed to the Lazarus Group, following a browser-based delivery from http://7-zip.org/7zFM.dtrack.exe hosted at 108.62.141.80 that bypassed an initial Meraki block by serving a second variant. The malware established persistence via Windows service WBSservice pointing to C:\Users\Public\7zFM.dtrack.exe, then deployed DLL side-loading through legitimate Windows binaries control.exe and rasphone.exe to conduct systematic host reconnaissance and establish C2 communications to 3.237.205.16:80. Approximately 109.8 MB of data was exfiltrated to content.dropboxapi.com via T1567.002, with sustained Suspect Data Loss alarms continuing for 2+ days post-compromise. Critical: user alexw executed ssh.exe -i "Ahmadreza ocd c2.pem" ubuntu@3.237.205.16, indicating possible operator-level access to the C2 server or insider threat involvement that requires immediate investigation.

Device: i-01c36de472f736b2b ⌵

Compromised High confidence ⓘ

The EC2 instance i-01c36de472f736b2b is assessed COMPROMISED based on confirmed execution of the Dtrack backdoor (7zfm.dtrack.exe, SHA-256: 63fd5e9c7b6c5a8efe57d2922b2ef638e243bac30ffc746f3c67b785374bc7d5) rated Malicious by AMP File Reputation, with active C2 connections to 3.237.205.16 on port 80. The intrusion likely began on Mar 3, 2026 @ 5:12 PM PST via SSH access from unattributed IP 151.186.183.197, followed by a 3-day persistent SSH session from



Cisco XDR Forensics

Trigger **forensics** before you know that you need it

100s of evidence components are captured even from **compromised** device

Evidence builds **confidence** to take **decisive** next steps

The screenshot displays the Cisco XDR Forensics interface. The top navigation bar includes the Cisco logo, 'XDR Forensics', the user 'fortresscyber', and a search bar. The main content area is titled 'Suspicious Endpoint and User Activity' and features a 'Dashboard' section with buttons for 'Import Evidence', 'Generate Report', and 'Export Flags'. Below this, there are 'Global Filters' for Assets, Evidence Category, Finding Type, Finding Created By, MITRE, Flag, and Date&Time. The dashboard is divided into several panels: 1. 'Overview' panel showing 1 Asset, 91 Evidence Categories, and 236.2K Total Evidence. 2. 'MITRE ATT&CK' panel showing 11 Tactics and 35 Techniques. 3. 'Finding Type' panel with a donut chart showing a total of 2.97K findings, categorized by severity: 104 High, 324 Medium, 2,542 Low, and 0 Matched. 4. 'Top Assets Breakdown' panel showing a breakdown for 'Mazzarella' with 104 High and 324 Medium findings. A sidebar on the left lists various evidence categories and their counts, including 'Findings' (2,970), 'Exclusions' (0), 'Evidence' (Empty Evidence Categories), 'Windows' (System Info: 1), 'Acquisition', 'Amcache' (Amcache Device: 111, Amcache Driver: 384, Amcache File: 4, Amcache Program: 205, Amcache Shortcut: 90), 'Artifacts' (22,885), 'Browser Artifacts' (153), 'Browser Cookies' (3,992), and 'Browser Downloads' (55). The bottom left corner shows the Cisco logo and version 'v5.2.9'.

Enterprise Security Essentials

The leading AI-powered SecOps platform
Simplify your analyst experience with unified workflows

Includes Threat Intelligence and Exposure Management

The screenshot displays the Splunk Cloud Analyst Queue interface. At the top, there are navigation tabs for 'Mission Control', 'Security analytics', 'Security content', 'Configure', and 'Search'. The main area is titled 'Analyst queue' and includes a search bar, a filter for 'Last 24 hours', and tabs for 'All types', 'Investigations', 'Finding groups', 'Findings', and 'AI disposition'. A table lists several findings with columns for Title, ID, Entity, and a score. The first finding is 'Malicious PowerShell execution' with ID FI-AB543, assigned to Charlie Garcia, and a score of 80. Other findings include '24 hour risk threshold exceeded for 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 10.163.194.46 to 8.108.191.101', and 'Email files written outside of the Outlook directory'. A right-hand panel provides details for the selected finding, including 'Start investigation', 'Finding FI-AB543', 'Malicious PowerShell execution', and various metadata fields like Owner (Unassigned), Status (New), Sensitivity (Unknown), Urgency (Medium), Disposition (Undetermined), and Fields (Pinned).

Title	ID	Entity	Score
Malicious PowerShell execution	FI-AB543	CG Charlie Garcia	80
24 hour risk threshold exceeded for user=administrator	FI-AB233	A Administrator	38
Possible Phishing Attack	FI-AB198	NA Nyah Aamadu	40
Unusual network activities detected from 52.218.245.82 to 52.216.133.181	FI-AB029	52.216.133.181	15
3 failed login attempts within 24 hrs on device 10.34.56.354	FI-AB274	10.34.56.354	90
Threat Activity Detected from 10.163.194.46 to 8.108.191.101	FI-AB558	8.108.191.101	94
Email files written outside of the Outlook directory	FI-AB352	KT Kenji Tanaka	45

See it in action

Exposure Analytics

Continuously discover asset inventories, identities and services across on-prem, cloud and hybrid environments, maintaining a real-time view of what exists and what its risk exposure is.

Exposure Analytics enriches security events with asset criticality, ownership, exposure and business context allowing detections and investigations to be prioritized based on actual risk to the organization rather than raw alert volume.

By correlating vulnerabilities, identities, and risk profiles, Exposure Analytics highlights attack paths and high-risk assets early, enabling faster remediation, better prioritization and reduced likelihood of material breaches.

The screenshot shows the Splunk Cloud interface for an Entity analysis. The main entity is Rene Sullivan, with a risk score of 80. The dashboard is divided into several sections:

- Overview:** Shows tabs for Overview, Attributions, Findings, and Attack surface.
- Details:** A list of attributes for Rene Sullivan, including User, Last discovered (2025-12-07), First discovered (2023-11-01), Alternate IDs, Business unit (Americas), Manager (Rod Simmers), Title (Sr Engineer), Position (Full time), Employee ID (12345), Hire date (Nov 1, 2022), Left on (Nov 1, 2022), Email address (rsullivan@splunk.com), Phone (6197789977), Asset (SJ-ENG-WKS-52B), MAC address (00:01:4a:b6:74:7e), IP address (10.20.20.189), and Other info (12345).
- Location:** Shows Location (San Jose, California), Country (United States), Office (Remote), and Other info (12345).
- Categories:** Shows Category (—) and Entity lists (Decartine employee).
- Summary Metrics:** A row of four boxes showing Finding count (19) and three Additional metrics (123).
- Timeline:** A horizontal bar chart showing activity from West, Dec 4 2025 to Thu, Dec 9 2025. It includes categories for All activity, Findings (4), and Authentication (1).
- Map:** A world map with a purple dot indicating the location of San Jose, California.

Enterprise Security Premier

The leading AI-powered SecOps platform

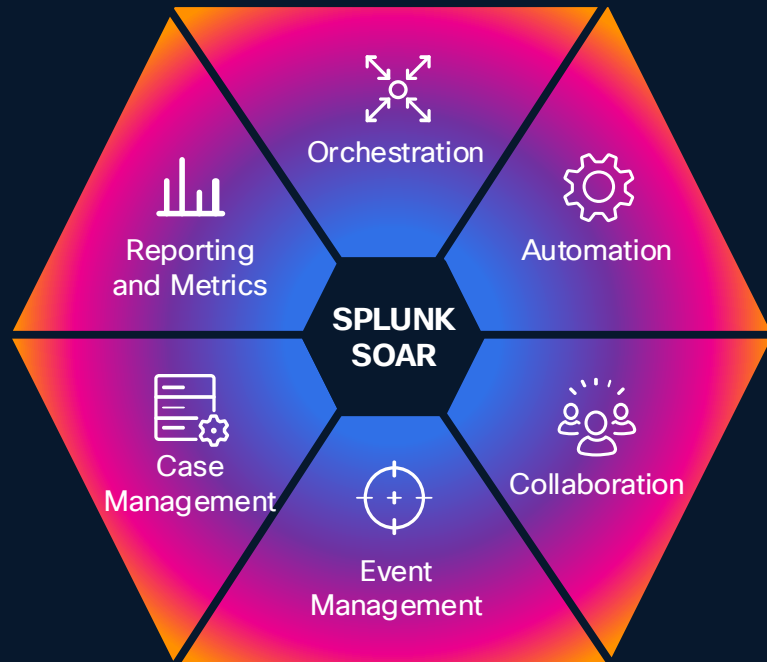
Simplify your analyst experience with unified workflows

Includes UEBA, SOAR and AI Assistant and more

The screenshot displays the Enterprise Security Premier interface. On the left, a table lists findings with columns for ID, Entity, and a score. The main panel shows a detailed view of a finding titled "Malicious PowerShell execution" with a score of 90. A circular callout highlights the "AI Assistant for Security" section, which includes a "Finding summarization" box. This box contains a summary of the finding: "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 a 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." Below the summary, there are sections for "Fields" (including Time, Detection, Destination category, etc.), "Related investigations", and "History". At the bottom right, there are buttons for "Summarize the findings", "Generate investigation report", "Suggest SPL", and "Discover AI Assistant skills".

See it in action

Spunk SOAR



Orchestration

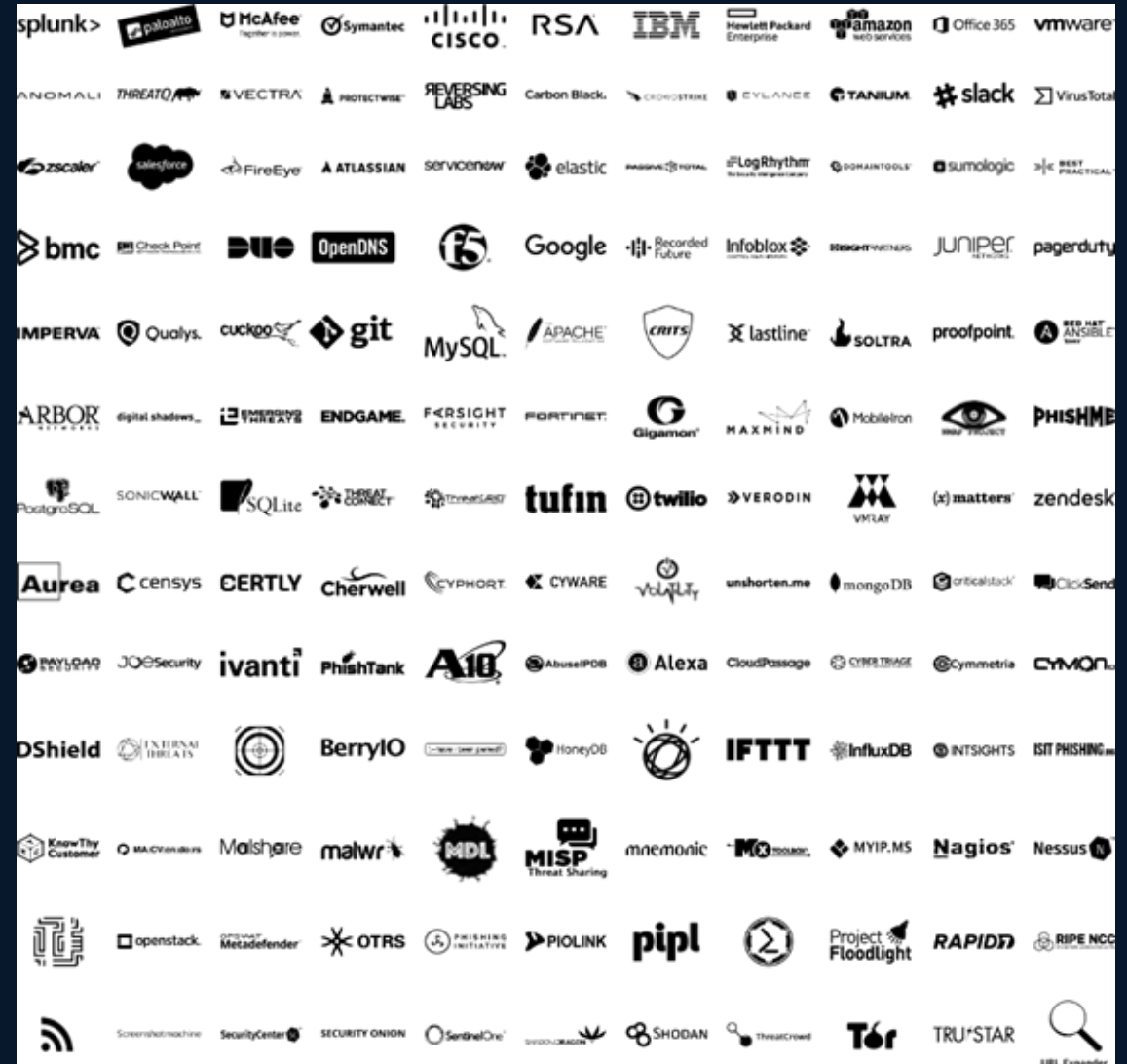
Coordinate complex workflows across your SOC

300+

APPS & GROWING

2800+

AUTOMATED ACTIONS

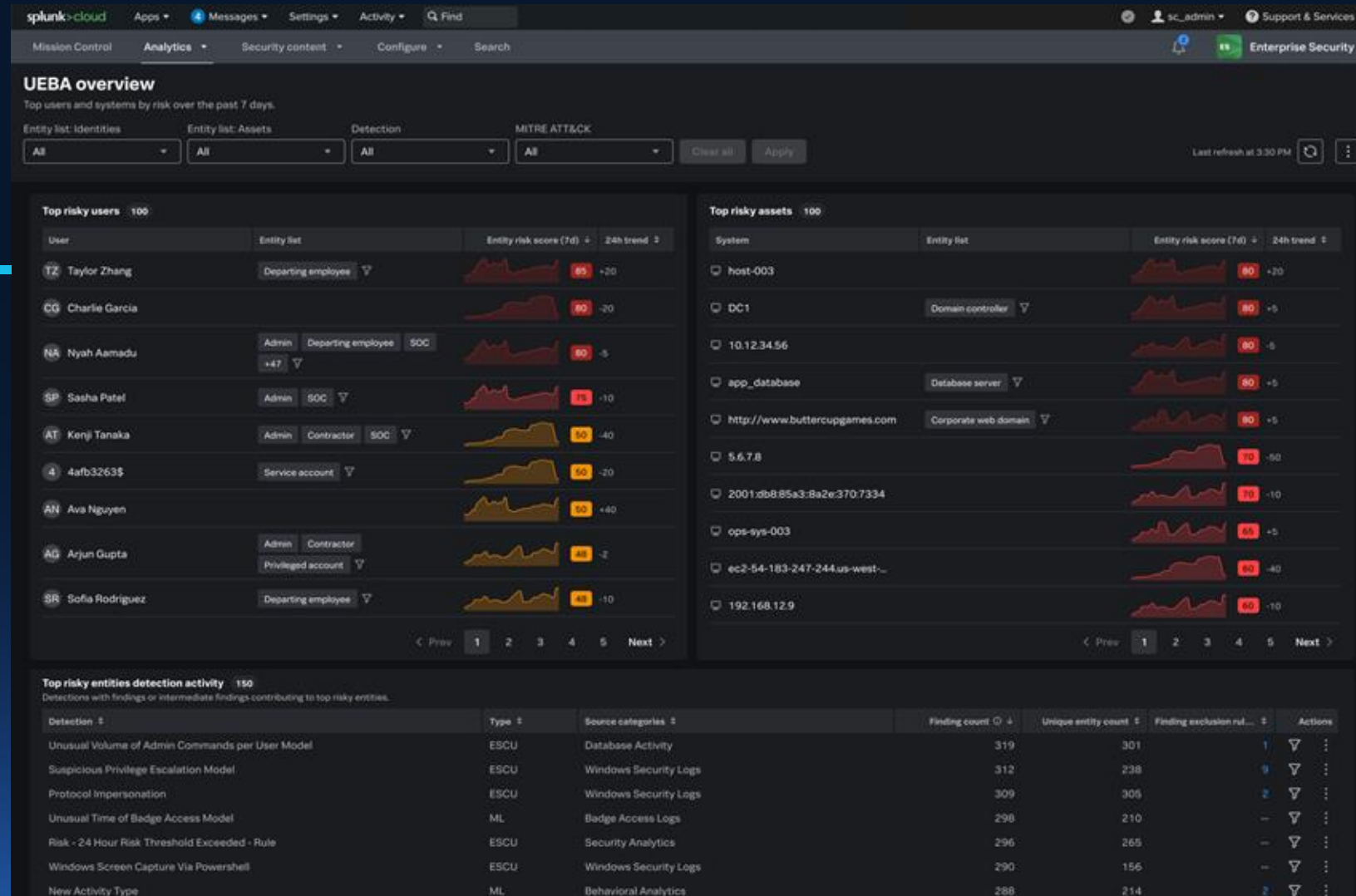


UEBA Insider Threat Detection

Establish user and entity behavior baselines to detect anomalies such as privilege abuse, lateral movement, and unauthorized access.

Identify insider risks—including compromised accounts and data exfiltration—without relying solely on correlation rules.

Unsupervised machine learning continuously adapts to evolving threats and insider attack tactics.



Triage Agent

Automatically determine alert disposition

Streamline alert prioritization

Plan and execute investigations

Automate insights to reduce MTR

The screenshot displays the Triage Agent interface. On the left, a list of findings is shown with columns for Title and ID. The findings include:

- Is this a Phish? - FW:Calling All Employees (ES-87199)
- Malicious PowerShell process with obfuscation techniques (FI-AB543)
- User access from unknown location tsmith2276621 (ES-AB416)
- Geographically Improbable Access Detected 192.198.2.3 (FI-AB410)
- 24 hour risk threshold exceed for system=172.16.0.149 (FI-AB233)
- Possible Phishing Attack (FI-AB198)
- Threat Activity Detected from 10.163.194.46 to 8.108.191.101 (FI-AB029)
- 3 failed login attempts within 24 hrs on device 10.34.56.354 (FI-AB274)
- Threat Activity Detected from 10.163.194.46 to 8.108.191.101 (FI-AB558)
- MITRE ATT&CK Tactic Threshold Exceeded For Object Over Previous 7 Days (FI-AB129)

The right pane shows a detailed analysis for a finding. It includes sections for Summary, Justification, Tools, and Evidence. The Summary section is highlighted as a 'True positive' and contains the following text:

Technique: Service Persistence (PoshC2)
Impact: Remote Access / Persistence on WIN10-21H1.snapattack.labs
Severity: High
Next step: Leverage "PoshC2 Service Creation_2" Response Plan

This event indicates that a new Windows service named CPUUpdaterMisc was installed on host WIN10-21H1.snapattack.labs by the user localuser. It was detected by a PoshC2-specific rule (T1543.003) and corresponds to Windows Security Auditing Event ID 4697. Such behavior is consistent with an adversary establishing persistence via a malicious service.

Below the summary, there are sections for Justification, Tools, and Evidence, along with a 'View details' button and a 'Why did you choose this rating?' section with radio buttons for Correct, Helpful, and Other.

The screenshot shows the AI investigation timeline section. It includes a header for the AI analysis and a table of investigation steps.

AI Sep 03, 6:34 PM
Here are the details for the AI analysis ipsum:

AI investigation timeline

#	Action	Tool / Method	Result	AI interpretation
1	Parsed ES finding "PoshC2 Service Creation_2"	Internal Parser	Service CPUUpdaterMisc installed under LocalSystem by localuser	Potential persistence mechanism
2	Queried WinEventLog 4697	Splunk Search	Service creation at 2025-09-17 20:00:54Z	Confirms service was installed
3	Queried WinEventLog 4688	Splunk Search	cmd.exe → powershell.exe → beacon.exe	Confirms service was installed
4	AI Reflection Pass #1	Reasoning	Confidence 1 35 → 65%	Confirms service was installed
5	Queried EDR detections	CrowdStrike API	Detection "Persistence via PowerShell Service Creation"	Confirms service was installed
6	Hash reputation check	VirusTotal API	42 vendors flag binary as PoshC2 beacon	Confirms service was installed
7	Queried Sysmon (Registrv 13)	Splunk Sysmon	Registry write for CPUUpdaterMisc	Confirms service was installed

At the bottom, there is a search bar with the text "Ask me anything about..." and a search icon.

[See it in action](#)

AI Security Assistant

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

The screenshot displays the Cisco Security Center interface. On the left, a table lists findings with columns for ID, Entity, and a score. The main panel shows details for finding FI-AB543, 'Malicious PowerShell execution', including owner, status, sensitivity, and disposition. A 'Start investigation' button is visible. On the right, the 'AI Assistant for Security' panel provides a 'Finding summarization' and a 'Disposition' section where the AI has suggested 'True positive'. Below this, it lists behavioral indicators like 'Command Behavior: Obfuscated script, spawned by powershell.exe' and 'Sandbox Result: Credential theft + scheduled task creation'. It also shows analysis from 'Splunk Attack Analyzer' and 'Cisco Talos'.

ID	Entity	Score
FI-AB543	Charlie Garcia	80
FI-AB233	Administrator	38
FI-AB198	Nyah Aamadu	40
FI-AB029	52.216.133.181	15
FI-AB274	10.34.56.354	90
FI-AB558	8.108.191.101	94
FI-AB352	Kenji Tanaka	45

See it in action

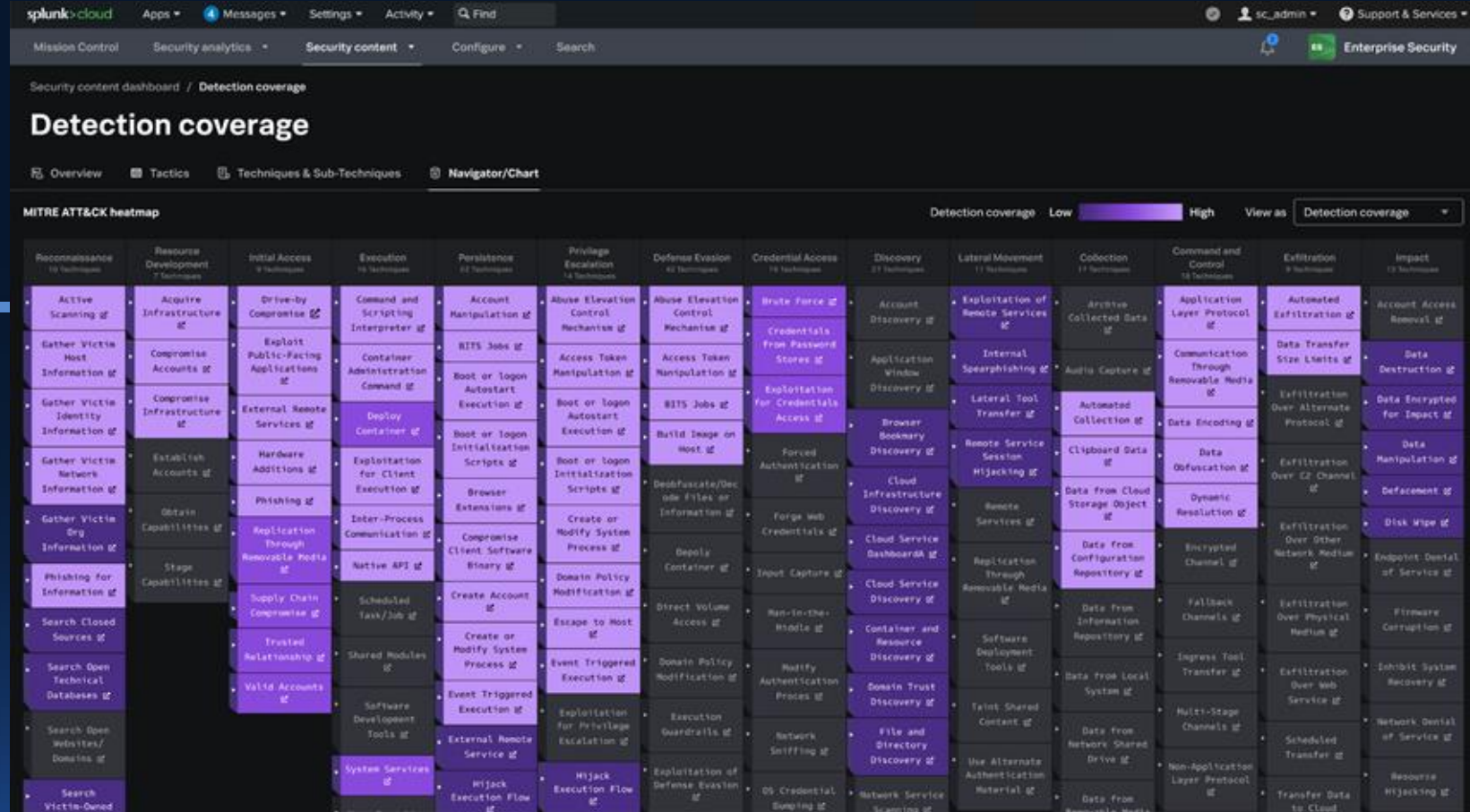
Detection Studio

Powered by SnapAttack

Streamline detection creation workflows

Evaluate detection health

Expand versioning and detection-as-code



[See it in action](#)

AI Assistant for Detection Authoring

Get detailed descriptions based on a short description

Generate SPL for the detection based on natural language description

Iterate on detection SPL to refine detection to be usable in your environment

Enable Detection Engineers to expand text in field values and iterate on SPL

Malicious PowerShell Execution

Enterprise Security

Enterprise Security

App configured for drill-down search links or email adaptive response actions. If no app is selected, the UI app context is used by default.

The following analytic identifies suspicious PowerShell execution using Script Block Logging (EventCode 4104). It leverages specific patterns and keywords within the ScriptBlockText field to detect potentially malicious activities. This detection is significant for SOC analysts as PowerShell is commonly used by attackers for various malicious purposes, including code execution, privilege escalation, and

Add information on what the detection searches for and the security use case addressed by the detection. For example: Identify excessive number of failed login attempts (likely to detect a brute force attack).

Customize Guided mode

```
index=* sourcetype="XmlWinEventLog:Microsoft-Windows-PowerShell/Operational" EventCode=4104
| rename ComputerName as dest, UserID as user, ScriptBlockText as script
| stats count min(_time) as firstTime max(_time) as lastTime by dest, user, script
| `drop_dm_object_name(Processes)`
| eval script=coalesce(process, "")
| eval is_encoded_command = if(match(script, "(?i)-e(nc*o*d*e*d*c*o*m*m*a*n*d*)*\\s+[^-]"), "Yes", "No")
| eval uses_iex = if(match(script, "(?i)(iex|invoke-expression)", "Yes", "No")
| eval downloads_from_web = if(match(lower(script), "(http|webclient|downloadfile|downloadstring)", "Yes", "No")
| eval contains_mimikatz = if(match(lower(script), "mimikatz|-dumprcr"), "Yes", "No")
| eval suspicious_cmdlet = if(match(script, "(?i)(Invoke-Mimikatz|Get-GPPPassword|Invoke-CredentialInjection|Invoke-BypassUAC|Invoke-ReflectivePEInjection)", "Yes", "No")
| where is_encoded_command="Yes" OR uses_iex="Yes" OR downloads_from_web="Yes" OR contains_mimikatz="Yes" OR suspicious_cmdlet="Yes"
| stats count as event_count,
  values(is_encoded_command) as encoded_command_detected,
  values(uses_iex) as invoke_expression_detected,
  values(downloads_from_web) as web_download_detected,
  values(contains_mimikatz) as mimikatz_keyword_detected,
  values(suspicious_cmdlet) as suspicious_cmdlet_detected,
  values(script) as full_command_line
by dest, user
```

The following SPL query is customized to your environment and connects existing indexes, fields, and data models.

```
SPL
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime
  from datamodel=Endpoint.Processes
  where Processes.process_name=powershell.exe
  by Processes.dest Processes.user Processes.process
| eval is_encoded_command = if(match(script, "(?i)-e(nc*o*d*e*d*c*o*m*m*a*n*d*)*\\s+[^-]"), "Yes", "No")
| eval uses_iex = if(match(script, "(?i)(iex|invoke-expression)", "Yes", "No")
| eval downloads_from_web = if(match(lower(script), "(http|webclient|downloadfile|downloadstring)", "Yes", "No")
| eval contains_mimikatz = if(match(lower(script), "mimikatz|-dumprcr"), "Yes", "No")
| eval suspicious_cmdlet = if(match(script, "(?i)(Invoke-Mimikatz|Get-GPPPassword|Invoke-CredentialInjection|Invoke-BypassUAC|Invoke-ReflectivePEInjection)", "Yes", "No")
| where is_encoded_command="Yes" OR uses_iex="Yes" OR downloads_from_web="Yes" OR contains_mimikatz="Yes" OR suspicious_cmdlet="Yes"
| stats count as event_count,
  values(is_encoded_command) as encoded_command_detected,
  values(uses_iex) as invoke_expression_detected,
  values(downloads_from_web) as web_download_detected,
  values(contains_mimikatz) as mimikatz_keyword_detected,
  values(suspicious_cmdlet) as suspicious_cmdlet_detected,
  values(script) as full_command_line
by dest, user
```

Use this SPL Open in search

Ask me anything about...

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

AI Toolkit with LLM Integrations

Build and deploy AI models


Query Splunk with 3rd party

LLMs

Access Splunk hosted
models, coming soon

The screenshot displays the 'Connection Management Settings' page in Splunk Cloud. A dropdown menu is open, showing the following options: 'Select Service --', 'Splunk Hosted Models', 'OpenAI', 'Anthropic', 'AzureOpenAI', 'Groq', 'Gemini', 'Bedrock', and 'Ollama'. The 'Select Service --' option is currently selected. The background shows a table with columns for 'Model Name' and 'Action'. The table contains several rows, including 'Llama 3.1 70B Instruct AWQ', 'Llama 3.1 8B Instruct', and 'Llama-3.1-FoundationAI-SecurityLLM-base-8B'. The 'Action' column contains edit icons for each row.

Model Name	Action
Llama 3.1 70B Instruct AWQ	
Llama 3.1 8B Instruct	
Llama-3.1-FoundationAI-SecurityLLM-base-8B	



In the era of AI,
security is more central than ever

Effective Security Operations Require



Visibility

Of the Attack Surface

Telemetry
& Logs

+



Knowledge

Knowing what to look for

Threat Intel, Indicators,
Detections, Context

+



Action

Ability to take Action

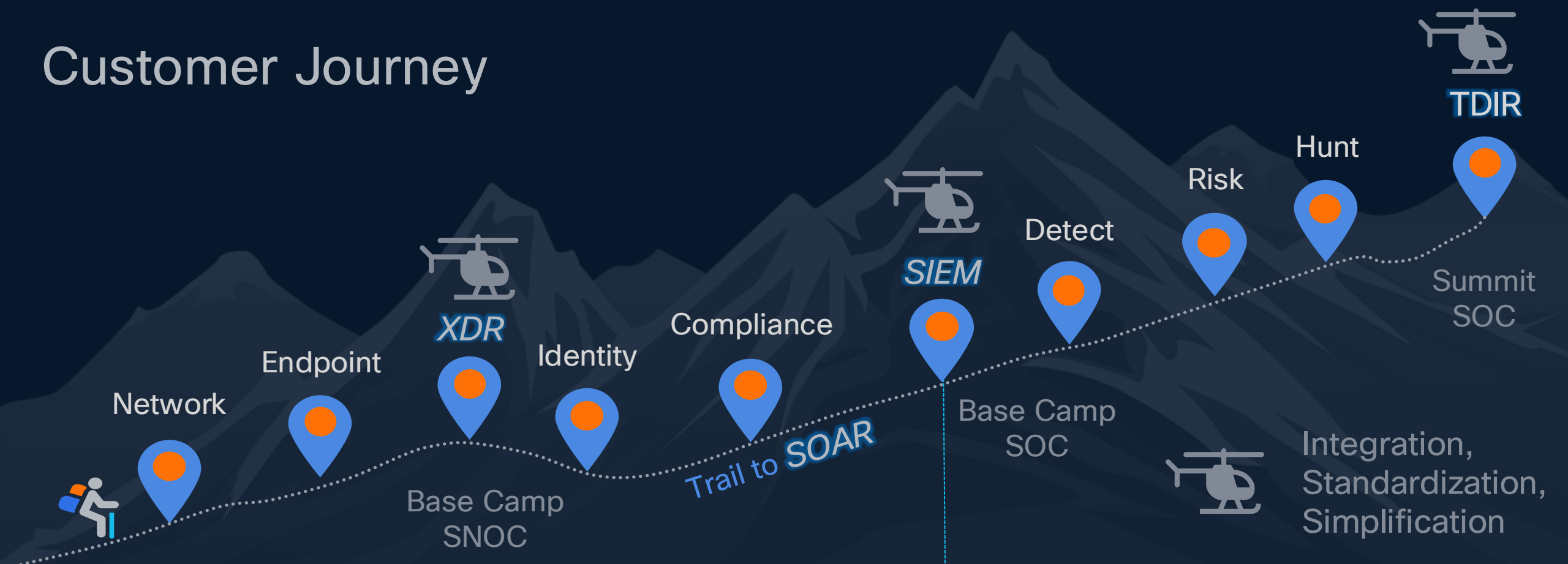
Policies, Blocking,
Patching, Remediating

Cisco Security Cloud
Technical Add-on:
+25K downloads

Cisco Talos: **2,000 new
samples** analyzed
every minute

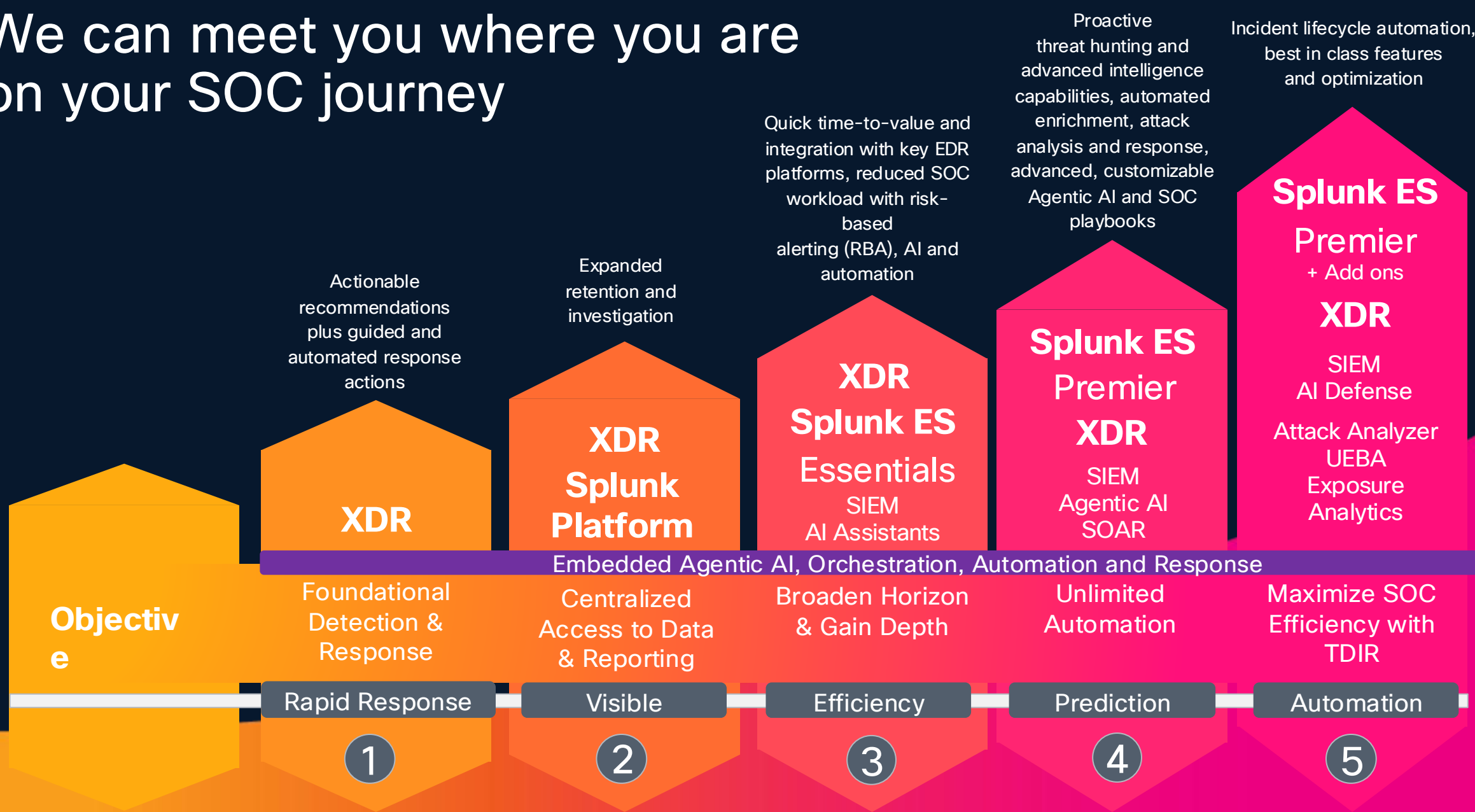
SOAR ecosystem:
+300 connectors with
+2,800 automated actions

Customer Journey



Foundational	Transformative	Maximized
<ul style="list-style-type: none"> Foundational TDIR Native Investigative Sources Endpoint + Network + Identity Threat Intelligence Mgmt Case Management Managed Analytics / Priority Asset Inventory Threat Visualization Managed Out of the Box Automation & Integrations 	<ul style="list-style-type: none"> Simplified Investigation Integrated SOAR solution Essential Third-Party Integrations Integrated Endpoint Forensics Agentic AI Investigations AI Generated Reporting < 1 year of Data Storage 	<ul style="list-style-type: none"> Unlimited Integrations Dashboards & Reporting Investigative Search (SPL) & Federated Search Basic Detections Cloud Deployments Government (GCC / State / Local) Essential Compliance InfoSec Monitoring > 1 year of Data Storage On-Premise Support
<ul style="list-style-type: none"> Ad-hoc Investigations Deep Threat Hunting Bespoke & Unlimited Automation Detection Engineering Integrated Foundational TDIR Endpoint & Log Forensics AI Assisted Searches Out of the Box Automation FEDRAMP Low & High 	<ul style="list-style-type: none"> Everything in ES & XDR Detection Validation Insider Threat / UBA Customizable Risk-based Alerts Asset Risk Intelligence Next Generation Sandbox Detection Validation Machine Learning Tool Kit Data Science Tool Kit 	

We can meet you where you are on your SOC journey



Cisco + Splunk Security

Now available

GA Now

Cisco XDR

Endpoint

Cloud

Network

Correlated

Identity

Response

GA Now

Essentials

Exposure Analytics

SIEM

TIM

EXA

GA Now

Premier

Exposure Analytics

SIEM

TIM

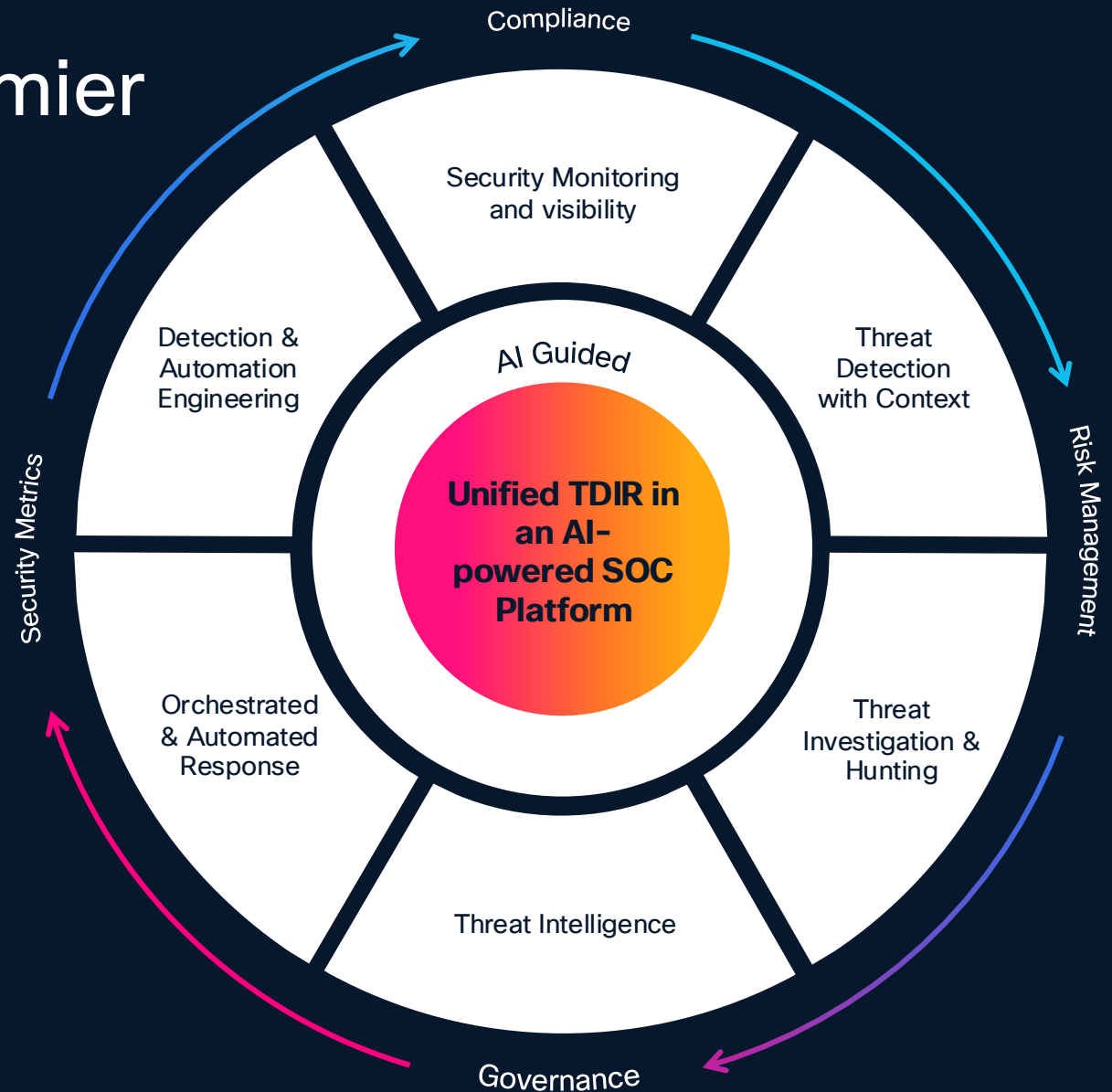
UEBA

SOAR

Reimagine the SOC with Cisco XDR + Splunk ES Premier

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.



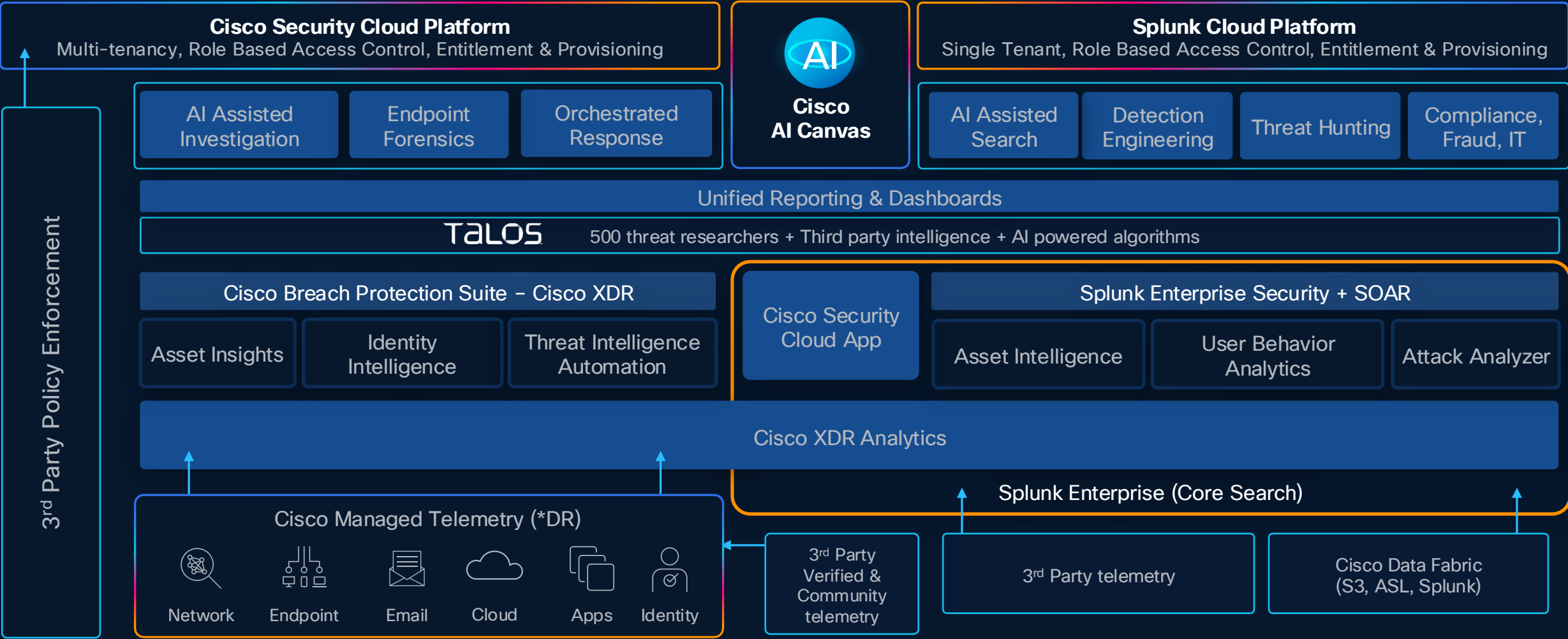
We can meet you wherever
you are
on this journey

Delivering critical capabilities for a foundational TDIR solution

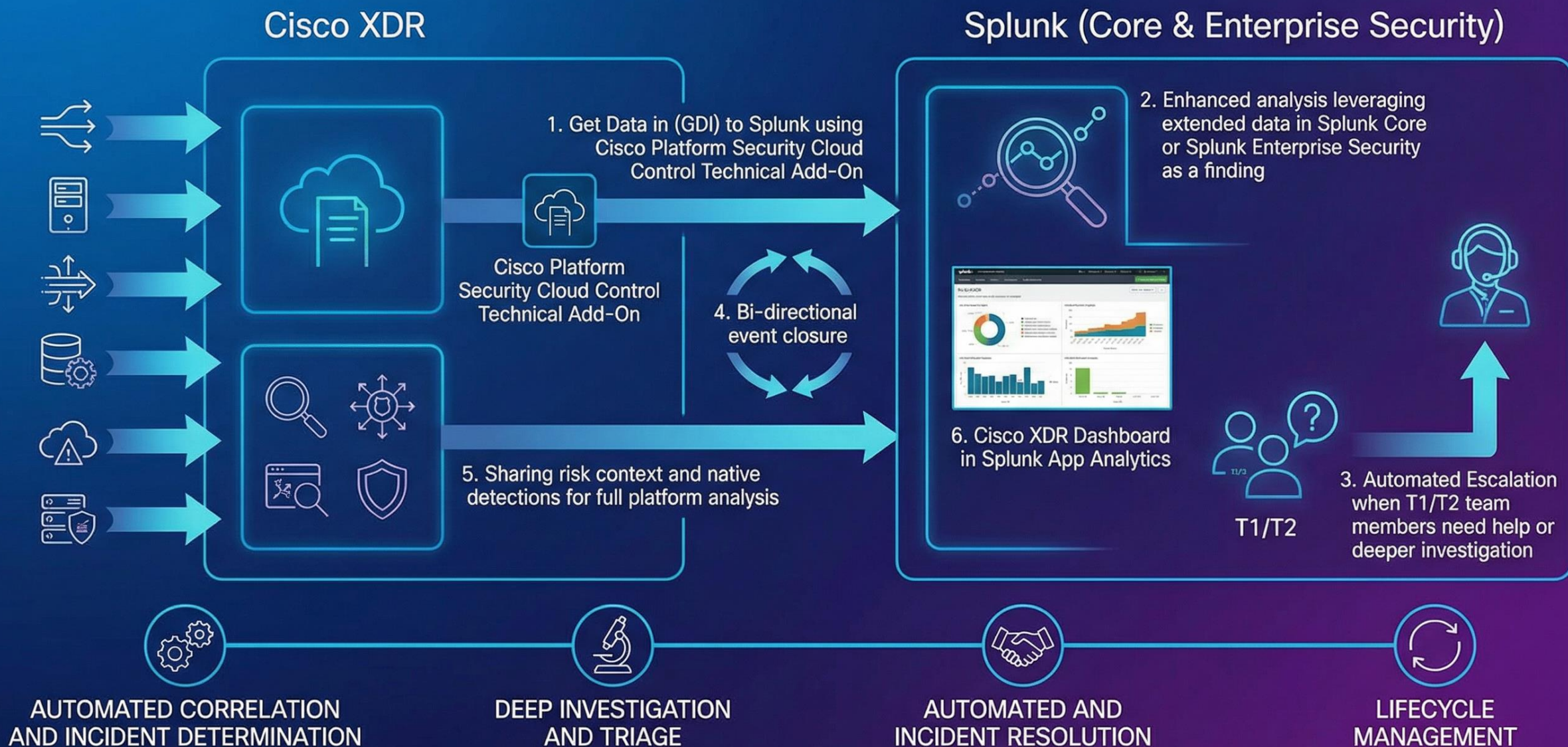
	Cisco XDR	Splunk Security	Splunk Security + XDR
Threat Detection:	Built-in detections focused on email, network & endpoint	Supports custom detections across any data source	Best-in-class detections across all threat vectors
Investigation:	Built-in workflows for common investigations	Flexible investigations including ad-hoc threat hunting	Full coverage for investigating known and unknown threats
Response:	Built-in responses for quick actions	Rich automations with custom playbooks	Automate any action, at scale.
	Easy-to-Use	Flexible	Complete Solution



Unified Security Platform



INTEGRATED SECURITY CAPABILITIES: Cisco XDR & Splunk



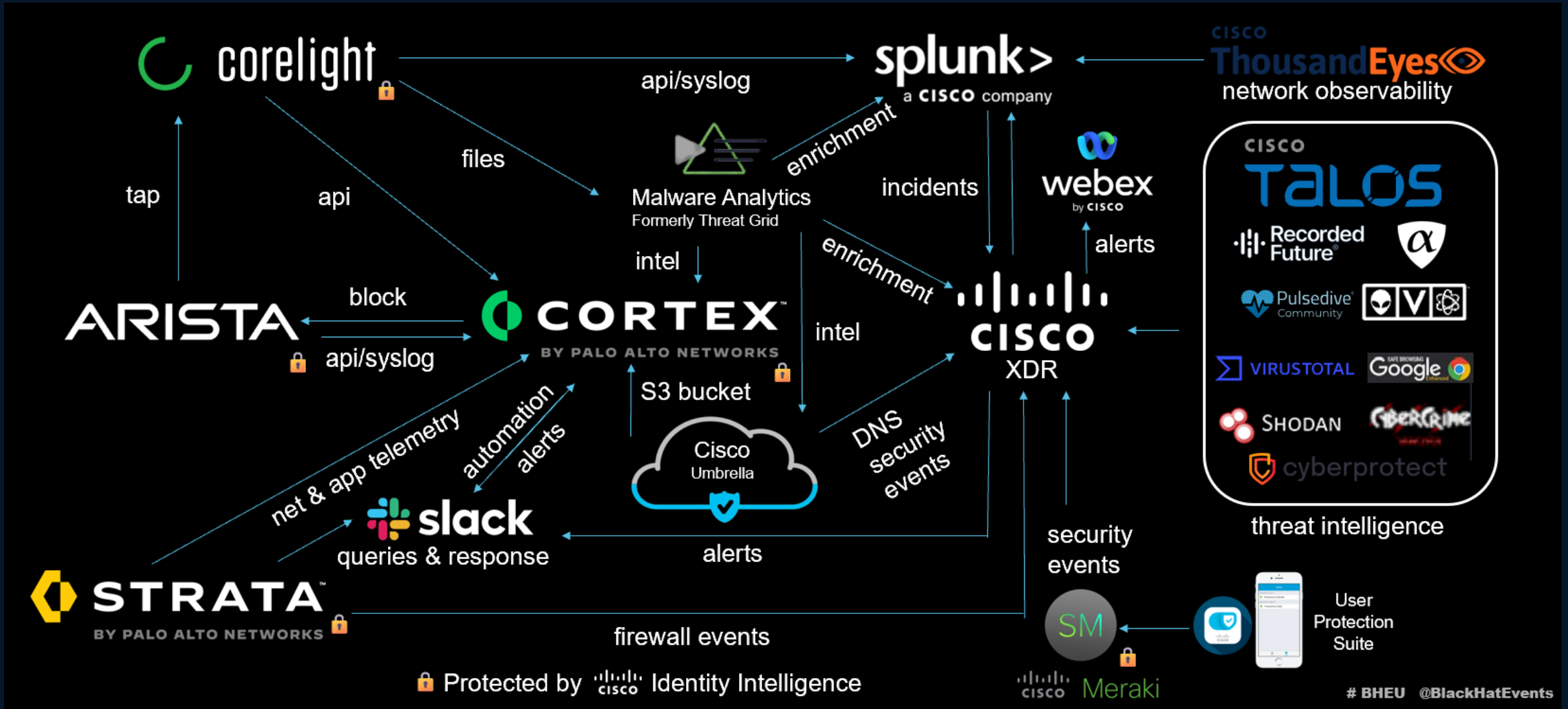
Cisco Security Events SOC

What is the Events SOC?

- Black Hat
- RSA
- Cisco Live
- Global Sporting Events
- Mobile World Congress
- Upcoming Olympics



Black Hat Europe 2025 SOC Integrations



Is your attack surface adequately protected against emerging threats?

Learn more at cisco.com/go/xdr

Tackling Security
with Limited
Resources paper



See Cisco XDR
in Action with
Guided Demos



Thank you



