

# Transforming Security Operations to Punch Above Your Weight Class

Briana Farro  
Director, Product Management



# Our World Is Continuously Changing And So Has *Everything* You Do





**Threat Actors Do Not Discriminate  
Based on an Organization's Size or  
Vertical**

# Your Teams Cannot Be Masters of All Tools and Possibilities



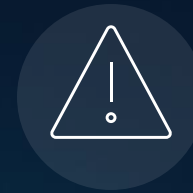
**Know**  
Every host



**Record**  
Every conversation



Understand  
what is **normal**

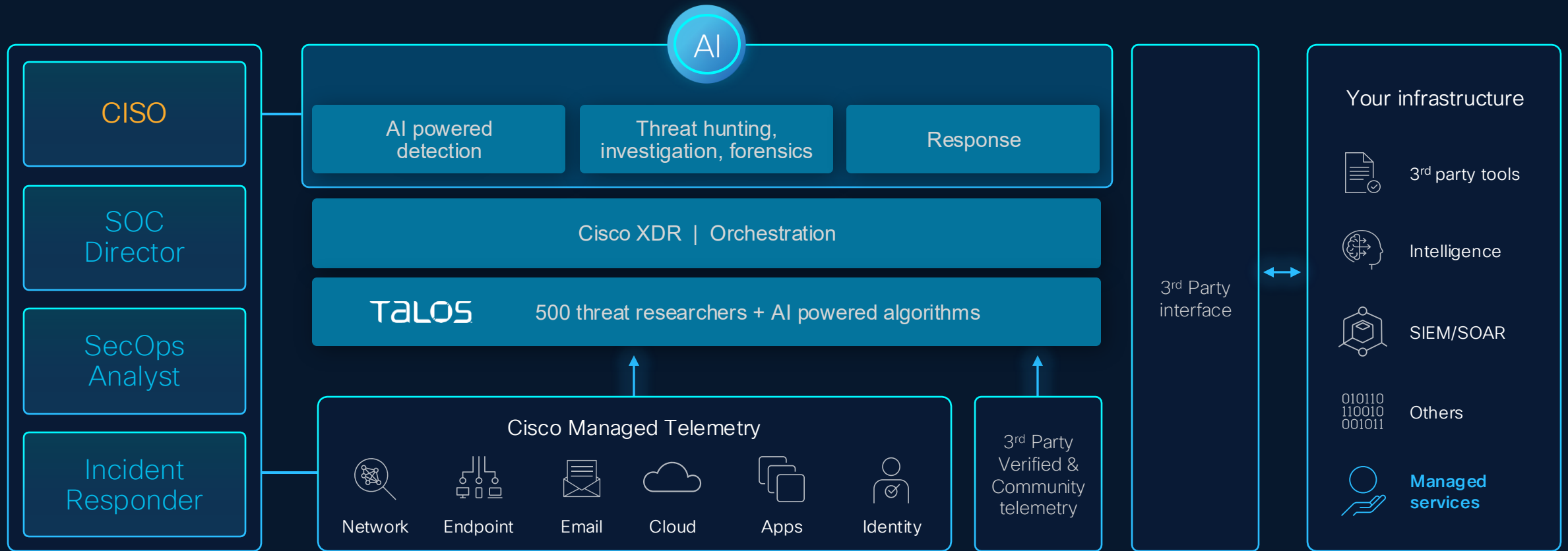


Be alerted to  
**change**



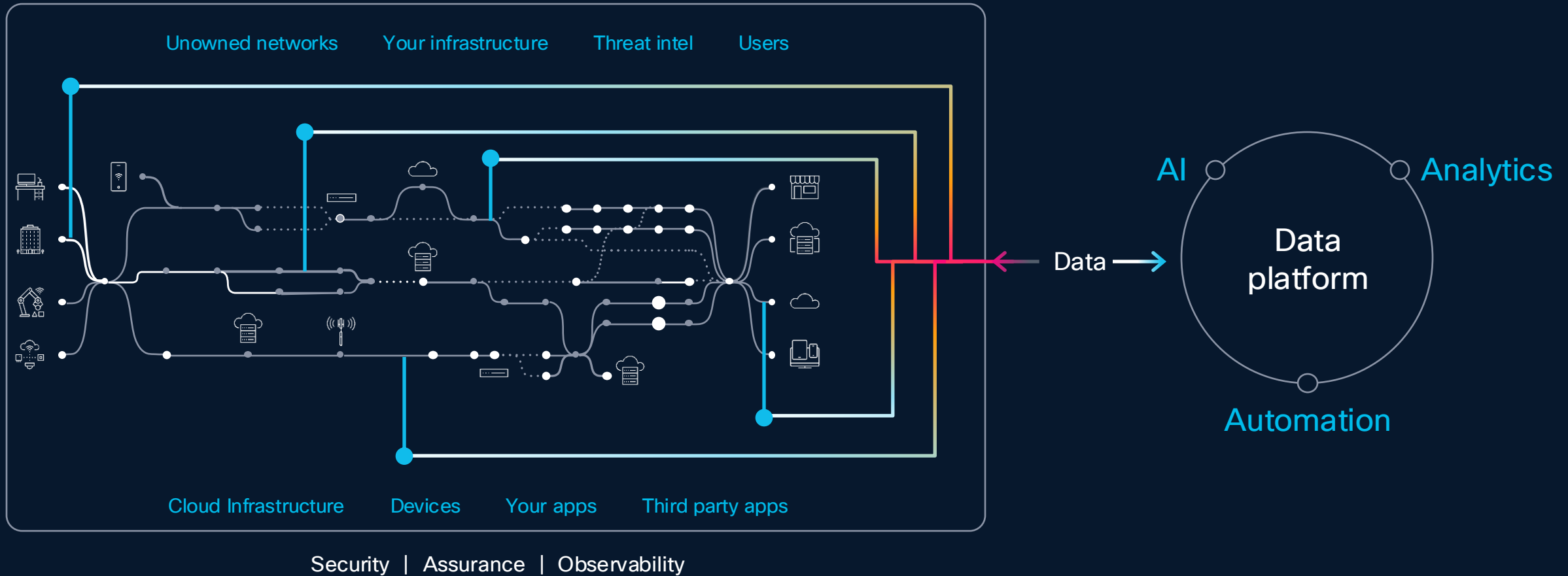
Respond to  
**threats** quickly

# The Realistic Architecture Needed



Real-time attack chain detection for the most common attacks with curated integration and response guidance

# The Power of Splunk and Cisco Means You Can Unify Data, Detection, Investigation, Response and Prevention



# Cisco Powers Your Technology Advancements

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

# 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



# 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.

# 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

We can meet you  
wherever you are  
on this journey

The background is a dark blue, isometric digital environment. It features several laptops and server racks scattered across the scene. A complex network of glowing white and light blue lines connects various points, suggesting data flow and connectivity. The overall aesthetic is clean, modern, and high-tech.

XDR  $\neq$  EDR++

Email

Network

Cloud

Firewall

Endpoint

Identity



SECURITY TOOLS

# Cisco XDR



An equal seat at the table

# Why We've Developed Cisco XDR



Threat Correlation vs.  
just Aggregation



Clear Prioritization risk  
& impact-base



Data repository  
supporting just-in-time  
and retroactive search



Guided Incident  
Response



Curated, commercially  
supported integrations  
with third-party solutions



Embedded  
Network & Cloud  
Detection



Asset context, device,  
user, data, workload with  
customizable asset value



Advanced  
Automation



Infused Threat  
intelligence

## Time to Value

- Reduces manual effort to detect and respond
- Detect the most complex threats
- Guidance on how analysts should respond
- Elevate productivity

# Customer Journey



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

# 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.



# 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

# Cisco XDR

Improve Alert Fidelity

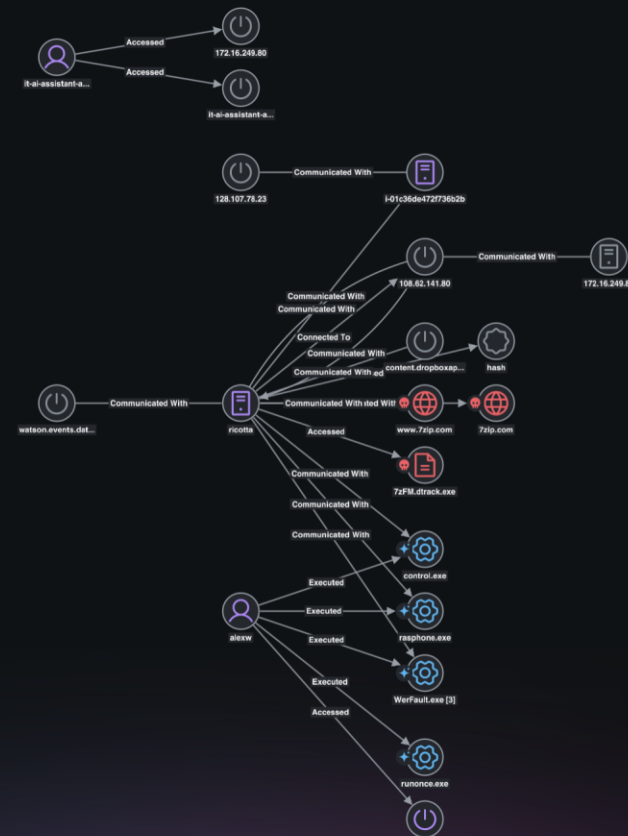
Instant Attack verification  
with a clear verdict

Command Every response  
and action

Single place to see all  
Security Alerts

Network at the core

The screenshot displays the Cisco XDR interface for an incident. At the top, it shows the incident title: "Malicious: Dtrack Backdoor Compromise with 109.8 MB Exfiltration on ricotta and EC2". The status is "Open: Investigating" and "Unassigned". Below the title, there are tabs for "Overview", "Response", "Evidence", "Worklog", and "Report". The "Overview" tab is active, showing a "Decisive True Positive" verdict with "High confidence". The data sources listed are Custom Security Event, Cisco XDR, Meraki, Cisco Secure Network Analytics, Cisco Secure Access, and Cisco Secure Endpoint. The MITRE tags include "Exfiltration", "Command and Control", and "Discovery" (+10). The "Impact" section, labeled as "AI-generated", contains three bullet points: 1. "Confirmed Data Exfiltration: 109.8 MB exfiltrated to Dropbox API ( content.dropboxapi.com ) in a single session by hollowed rasphone.exe , with 18 additional Suspect Data Loss alarms spanning 2+ days post-compromise suggesting ongoing exfiltration of data potentially including SharePoint/Exchange content." 2. "Two Assets Fully Compromised: Both ricotta (Windows workstation with RDP/Kerberos roles) and EC2 i-01c36de472f736b2b (Web/Terminal Server) are assessed COMPROMISED with active Dtrack persistence via WBSservice auto-start service — environment remains at risk until eradication is confirmed." 3. "Possible Insider Threat or Full Account Compromise: alexw 's interactive SSH access to the C2 server using a key named 'Ahmadreza ocd c2.pem' represents a critical unresolved question with significant blast-radius implications; all credentials associated with alexw should be treated as compromised pending investigation." The "Summary" section, also "AI-generated", provides a detailed narrative: "Malicious: ricotta (user alexw ) was fully compromised by the Dtrack backdoor ( C:\Users\alexw\Downloads\7zFM.dtrack.exe , SHA-256: 63fd5e9c7b6c5a8efe57d2922b2ef638e243bac30ffc746f3c67b785374bc7d5 , AMP score 10.0/Malicious) delivered from http://7-zip.org/7zFM.dtrack.exe hosted at 108.62.141.80 , which bypassed a Meraki block by serving a second variant. The malware installed persistence via Windows service WBSservice pointing to C:\Users\Public\7zFM.dtrack.exe , performed DLL side-loading into control.exe and rasphone.exe for HTTP C2 to 3.237.205.16 :80, and exfiltrated 109.8 MB to content.dropboxapi.com ( 162.125.13.14 ):443 via T1567.002. A critical anomaly — user alexw executing ssh.exe -i "Ahmadreza ocd c2.pem" ubuntu@3.237.205.16 with a PEM key explicitly named 'c2' — indicates possible operator-level C2 access or insider involvement requiring immediate determination." Below the summary 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

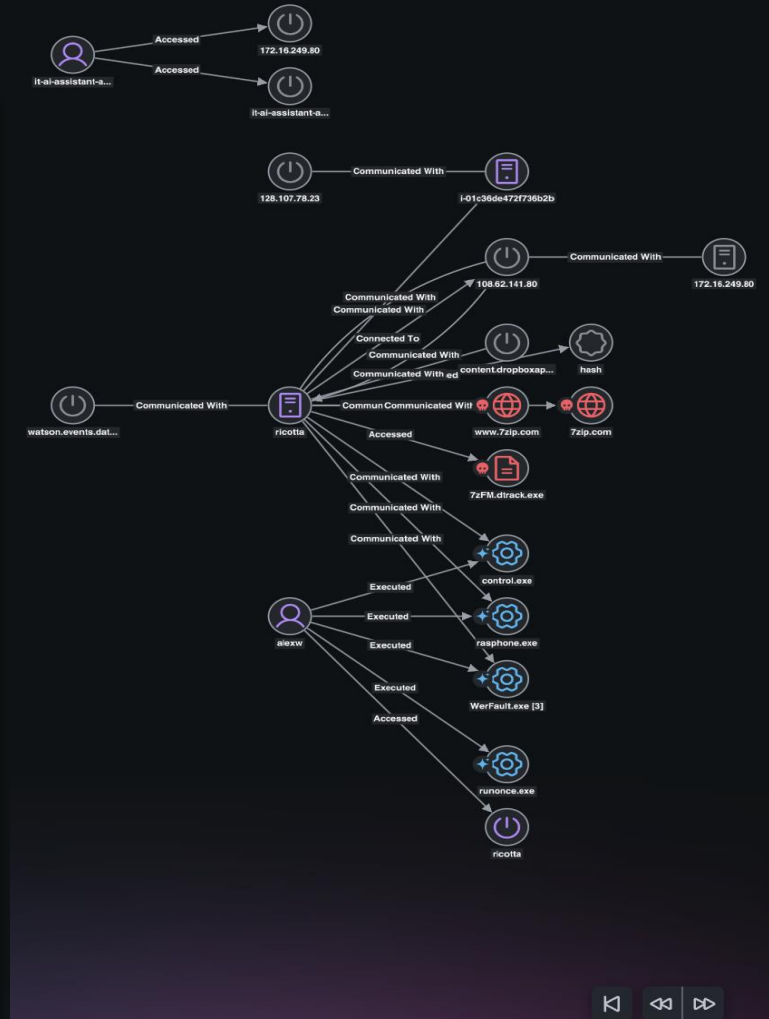
Compromised High confidence ⓘ

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-zlp.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 WBService 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 the following data:

Assets	Evidence Categories	Total Evidence
1	91	236.2K

Additional metrics shown include 11 Tactics and 35 Techniques under MITRE ATT&CK. The 'Finding Type' section features a donut chart with a total of 2.97K findings, categorized by severity: 104 High, 324 Medium, 2,542 Low, and 0 Matched. The 'Top Assets Breakdown' section shows a bar chart for the asset 'Mazzarella' with 104 High and 324 Medium findings.

The left sidebar contains a navigation menu with icons for Home, Reports, Findings (2,970), Exclusions (0), Evidence (with search and filter icons), Windows, System Info (1), Acquisition, Amcache (with sub-items: 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. 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 'Search'. The main area is titled 'Analyst queue' and features a search bar, a 'Last 24 hours' filter, and tabs for 'All types', 'Investigations', 'Finding groups', 'Findings', and 'AI disposition'. A list of findings is shown with columns for Title, ID, Entity, and a score. The top finding is 'Malicious PowerShell execution' (FI-AB543) with a score of 80, assigned to Charlie Garcia. Other findings include '24 hour risk threshold exceeded for user=administrator' (FI-AB233, score 38), 'Possible Phishing Attack' (FI-AB198, score 40), 'Unusual network activities detected from 52.218.245.82 to 52.216.133.181' (FI-AB029, score 15), '3 failed login attempts within 24 hrs on device 10.34.56.354' (FI-AB274, score 90), 'Threat Activity Detected from 10.163.194.46 to 8.108.191.101' (FI-AB558, score 94), and 'Email files written outside of the Outlook directory' (FI-AB352, score 45). On the right, a detailed view of the 'Malicious PowerShell execution' finding (FI-AB543) is shown, including a 'Start investigation' button, a description, and various metadata fields like Owner (Unassigned), Status (New), Sensitivity (Unknown), Urgency (Medium), and Disposition (Undetermined). A 'Suggested: True positive' label is also present.

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

# 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.

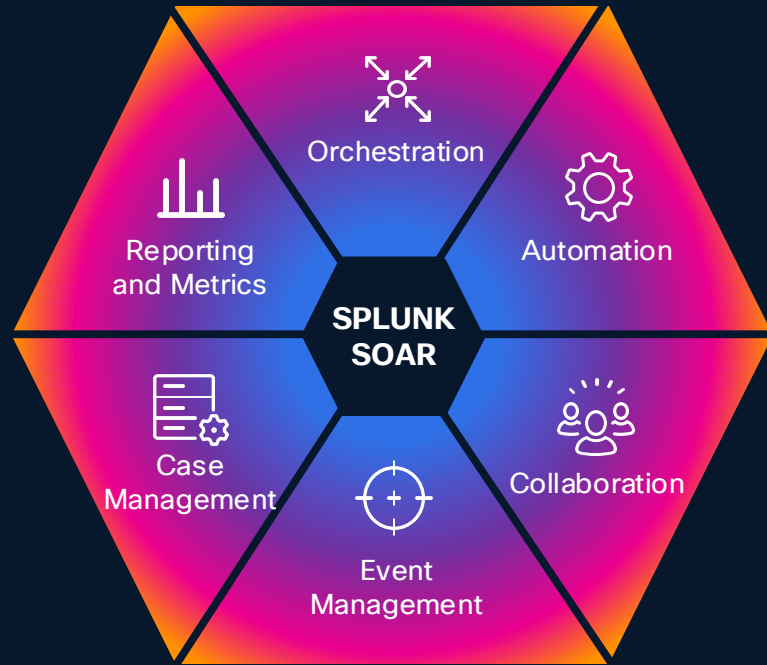
Exposure Analytics enriches security events with asset criticality, ownership, exposure and business context allowing detections and investigations to be prioritized based on actual risk to the organization rather than raw alert volume.

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 header includes 'splunk > Cloud' and navigation tabs for 'Premier', 'Premier - no (discovered)', and 'Essentials'. A search bar is present with the text 'Search for an entity'. The entity being analyzed is 'Rene Sullivan' (SO). The dashboard is divided into several sections:

- Overview:** Shows 'Back', 'Rene Sullivan (SO)', and a 'Last refresh at 2:30 PM' indicator. It includes a 'Last 7 days' filter and a 'Start investigation' button.
- 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 (Deactivate employee).
- Summary Metrics:** A row of four cards: 'Finding count' (19), and three 'Additional metric' cards (123, 123, 123).
- Timeline:** A horizontal bar chart showing activity from West, Dec 4 2024 to Tue, Dec 9 2024. It includes bars for 'All activity', 'Findings' (4), and 'Authentication' (1).
- Map:** A world map with a purple dot indicating the location of San Jose, California.

# Spunk SOAR



## Orchestration

Coordinate complex workflows across your SOC

**300+**

APPS & GROWING

**2800+**

AUTOMATED ACTIONS



# 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 "AI Assistant for Security Malicious PowerShell execution". The finding is dated "Today, 8:30 AM" and is categorized as a "True Positive". The "Finding summarization" section provides a detailed description: "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." Below this, it states: "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." The interface also includes sections for "Fields" (e.g., Time, Detection, Destination category), "Related investigations", and "History". At the bottom, there are buttons for "Summarize the findings", "Generate investigation report", "Suggest SPL", and "Discover AI Assistant skill".

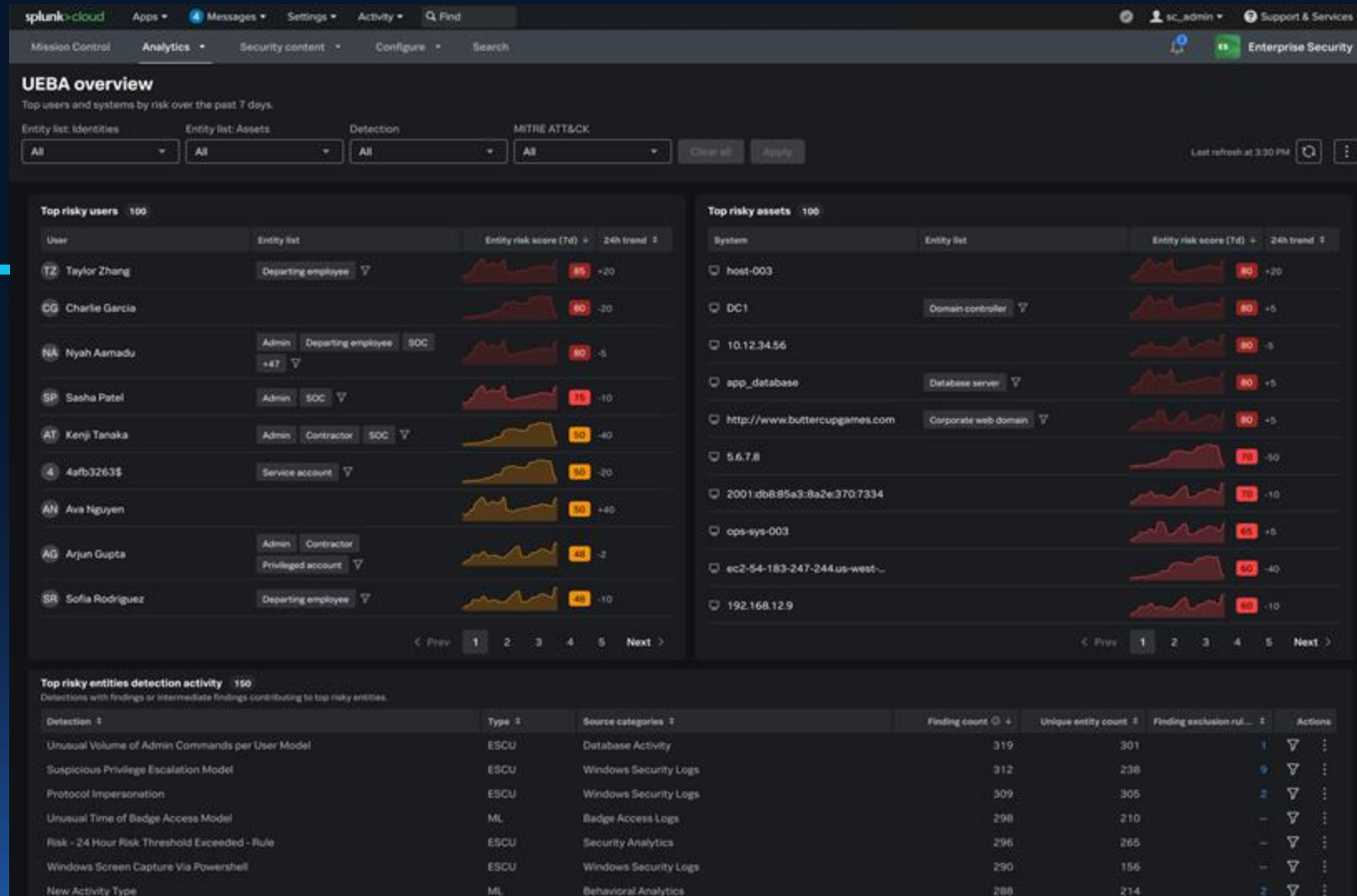
See it in action

# 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 MTRR

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 main panel shows a detailed analysis for the finding 'Service Persistence (PoshC2)'. It includes a summary, impact, severity, and next steps. The analysis text states: '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. A 'View details' button is present. At the bottom, there is a 'Why did you choose this rating?' section with radio buttons for 'Correct', 'Helpful', and 'Other'. A 'True positive' badge is visible in the top right corner of the analysis panel.

The screenshot shows the AI investigation timeline for the finding. It includes a header 'AI Sep 03, 6:34 PM' and a sub-header 'Here are the details for the AI analysis ipsum:'. The timeline is presented as a table:

#	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 of the timeline, there is a search bar with the text 'Ask me anything about...' and a magnifying glass 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 Enterprise Security console interface. The main panel shows a list of findings, with the selected finding being 'Malicious PowerShell execution' (FI-AB543) assigned to Charlie Garcia. The right-hand pane provides detailed information about this finding, including its status (New), sensitivity (Unknown), and urgency (Medium). The AI Assistant for Security is integrated into the interface, providing a 'Finding summarization' section that explains the finding based on command behavior, sandbox results, threat intel, and user context. It also includes a 'Disposition' section where the AI has suggested a 'True positive' and offers 'Reject' or 'Accept' options. Below the AI analysis, there are sections for 'Splunk Attack Analyzer' and 'Cisco Talos' results. At the bottom of the AI assistant pane, there are buttons for 'Summarize the findings', 'Generate investigation report', 'Suggest SPL', and 'Discover AI Assistant skill'. A search bar and navigation controls are visible at the top of the console.

See it in action

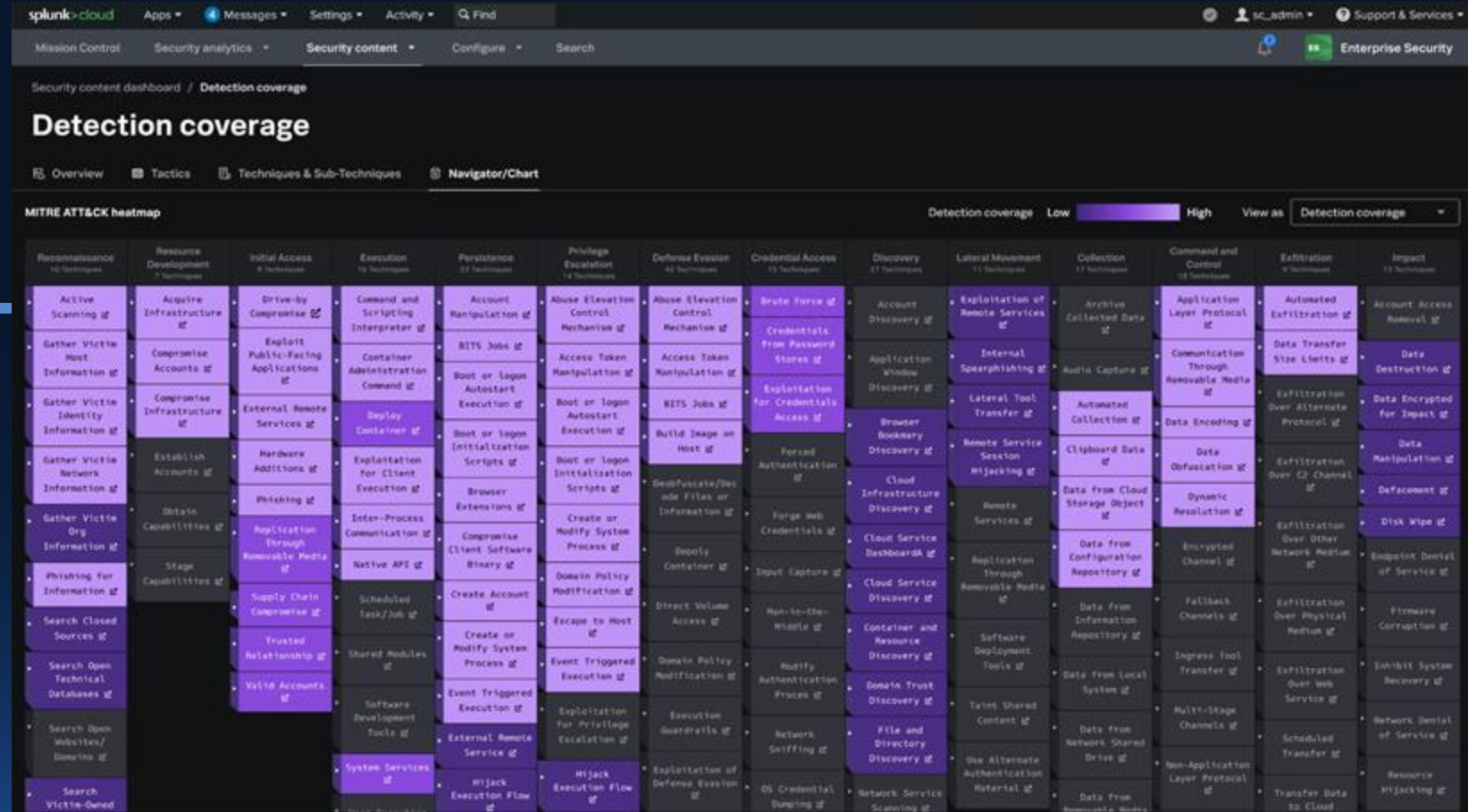
# Detection Studio

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+[^-]") OR
match(script, "[A-Za-z0-9+]{44,}={0,2}"), "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|-dumpcr"), "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
```

note...

Clone Save as new version

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+[^-]") OR match(script, "[A-
Za-z0-9+]{44,}={0,2}"), "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|-
dumpcr"), "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](#)

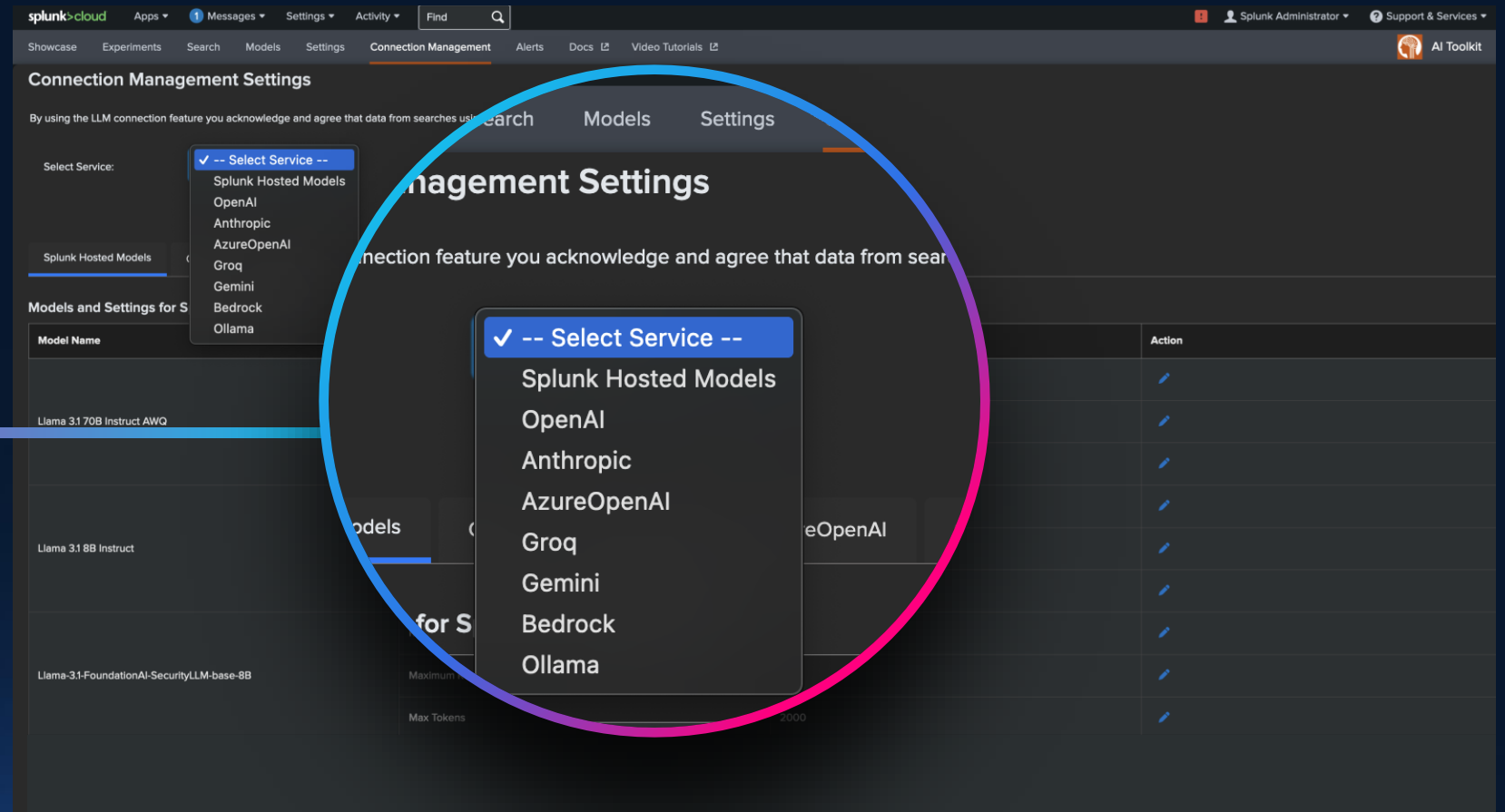
# AI Toolkit With LLM Integrations

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 a list of services to select from. The services listed are: Splunk Hosted Models, OpenAI, Anthropic, AzureOpenAI, Groq, Gemini, Bedrock, and Ollama. The 'Select Service' dropdown is highlighted with a blue circle. Below the dropdown, a table lists models and their settings. The table has columns for 'Model Name', 'Maximum', and 'Max Tokens'. The models listed are: 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 model.

Model Name	Maximum	Max Tokens	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

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

+



## Knowledge

Knowing what to look for

Threat Intel, Indicators,  
Detections, Context

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

+



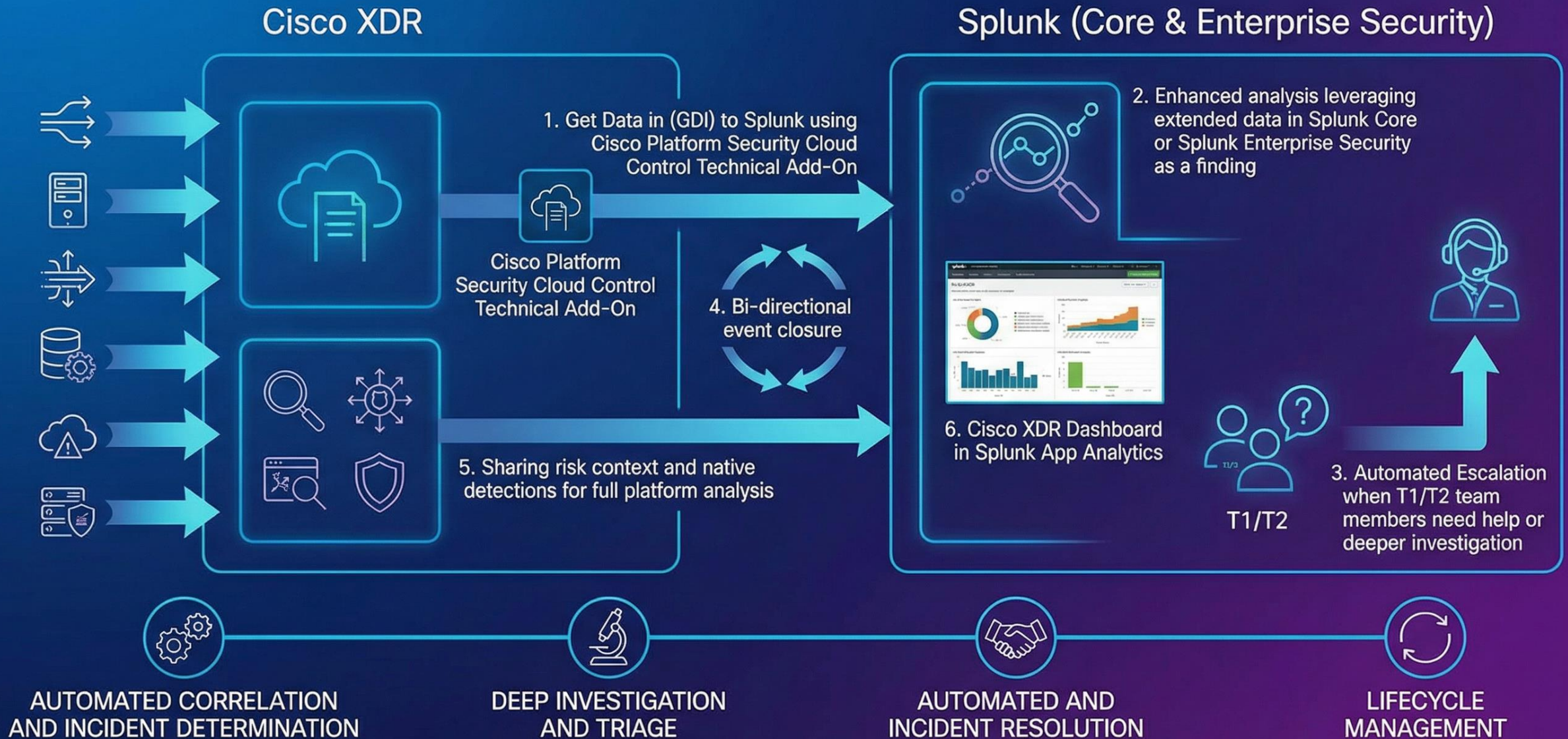
## Action

Ability to take Action

Policies, Blocking,  
Patching, Remediating

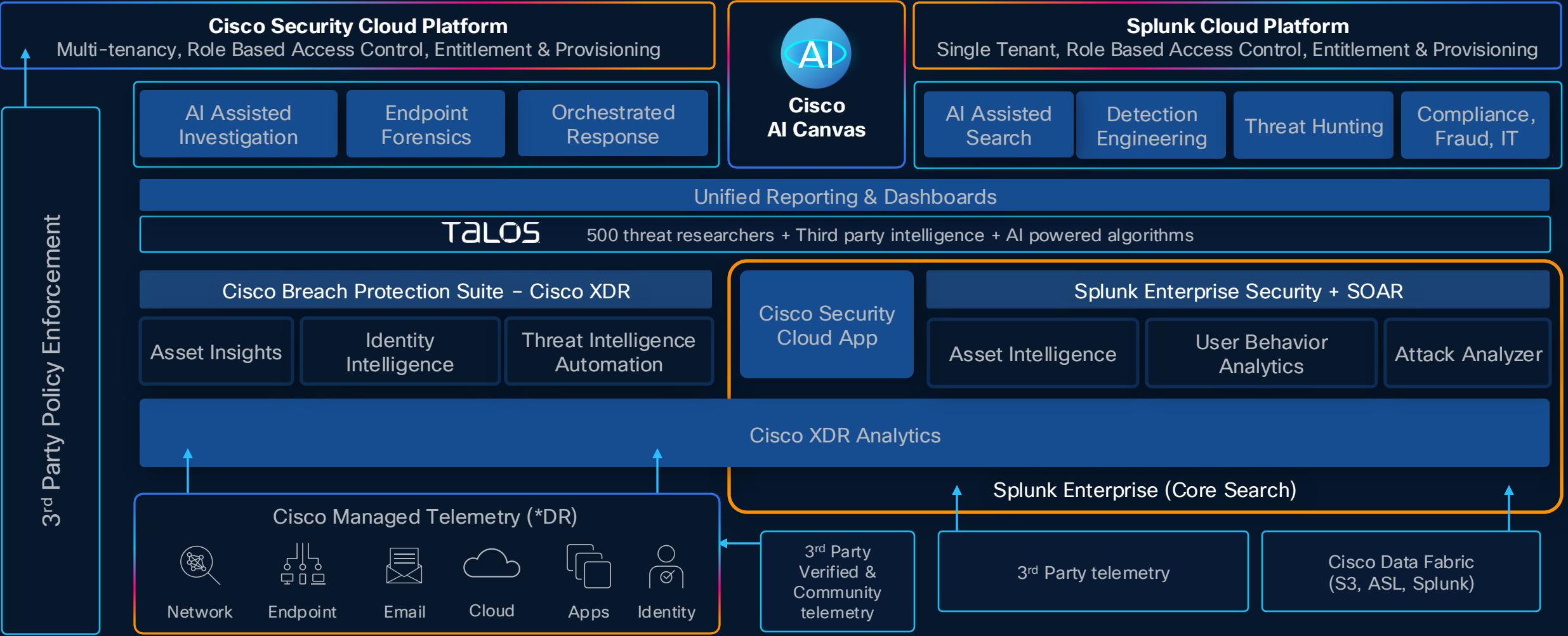
SOAR ecosystem:  
**+300 connectors** with  
**+2,800 automated actions**

# INTEGRATED SECURITY CAPABILITIES: Cisco XDR & Splunk





# Unified Security Platform



**Is This All Marketing?**



And I wanted to share a cool XDR example:

We had a Security Incident today with a user who fell for a fake CAPTCHA check and executed malware on their laptop.

Time for XDR to detect and analyze the data: 3 Minutes

Time for our SecOps engineers to contain the endpoint/user: 8 Minutes

**Security SLA total time with XDR: 11 Minutes**

We also have classic Managed SOC powered by only a SIEM running in the same environment. In comparison:

Time for SIEM to detect: 29 Minutes

Time for SOC engineer to analyze and notify customer: 50 Minutes

Time for SOC to contain incident: infinite Minutes

**Security SLA total time with managed SOC using SIEM alone: >79 Minutes**

*So, our organization has directly Identified, Analysed and Contained the incident before the SIEM had even registered the event!*

*Wouter Hindriks, European Customer and Managed Partner*

# Integrated Security for the World's Toughest Environments

Paris Olympics and Paralympics 2024:  
Strengthen Cyber Defenses for a Secure  
Olympic Games



NFL Draft & Superbowl (2022-2026):  
Protecting the fans, vendors, security,  
and experience



RSA Conference (2022-2026):  
Powering security at the world's  
toughest network

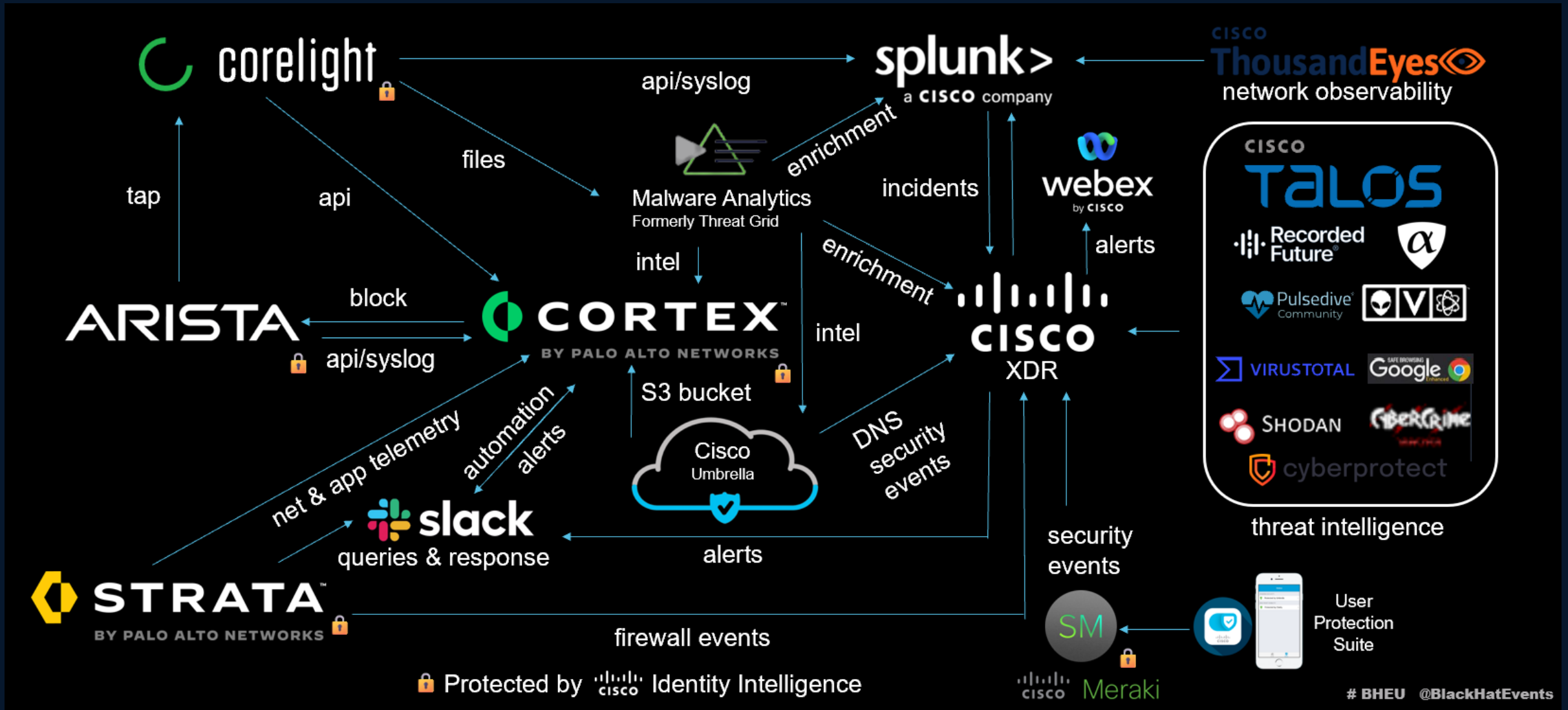


# What Is the Events SOC?

- Black Hat
- RSAC
- Cisco Live
- Global Sporting Events
- Mobile World Congress
- Prior and Upcoming Olympics



# Black Hat Europe 2025 SOC Integrations



# Is your attack surface adequately protected against emerging threats?

Learn more at [cisco.com/go/xdr](https://cisco.com/go/xdr)

Tackling Security  
with Limited  
Resources paper



See Cisco XDR  
in Action with  
Guided Demos



# We Can Meet You Where You Are on Your SOC Journey

**Objective**

Actionable recommendations plus guided and automated response actions

**XDR**

Foundational Detection & Response

Rapid Response

1

Expanded retention and investigation

**XDR  
Splunk  
Platform**

Centralized Access to Data & Reporting

Visible

2

Quick time-to-value and integration with key EDR platforms, reduced SOC workload with risk-based alerting (RBA), AI and automation

**XDR  
Splunk ES  
Essentials**

SIEM  
AI Assistants

Broaden Horizon & Gain Depth

Efficiency

3

Proactive threat hunting and advanced intelligence capabilities, automated enrichment, attack analysis and response, advanced, customizable Agentic AI and SOC playbooks

**Splunk ES  
Premier  
XDR**

SIEM  
Agentic AI  
SOAR

Unlimited Automation

Prediction

4

Incident lifecycle automation, best in class features and optimization

**Splunk ES  
Premier  
+ Add ons  
XDR**

SIEM  
AI Defense  
Attack Analyzer  
UEBA  
Exposure Analytics

Maximize SOC Efficiency with TDIR

Automation

5

Embedded Agentic AI, Orchestration, Automation and Response

# Industry Acclaimed & Analyst Approved



Notable leader in  
GigaOm Radar Report



CRN Hottest  
Cybersecurity Product



UX Design awards



Fastcompany  
design awards

**CISCO** Connect

**Thank you**

