CISCO Engage | Tech Day Milwaukee

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

January 20, 2026

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

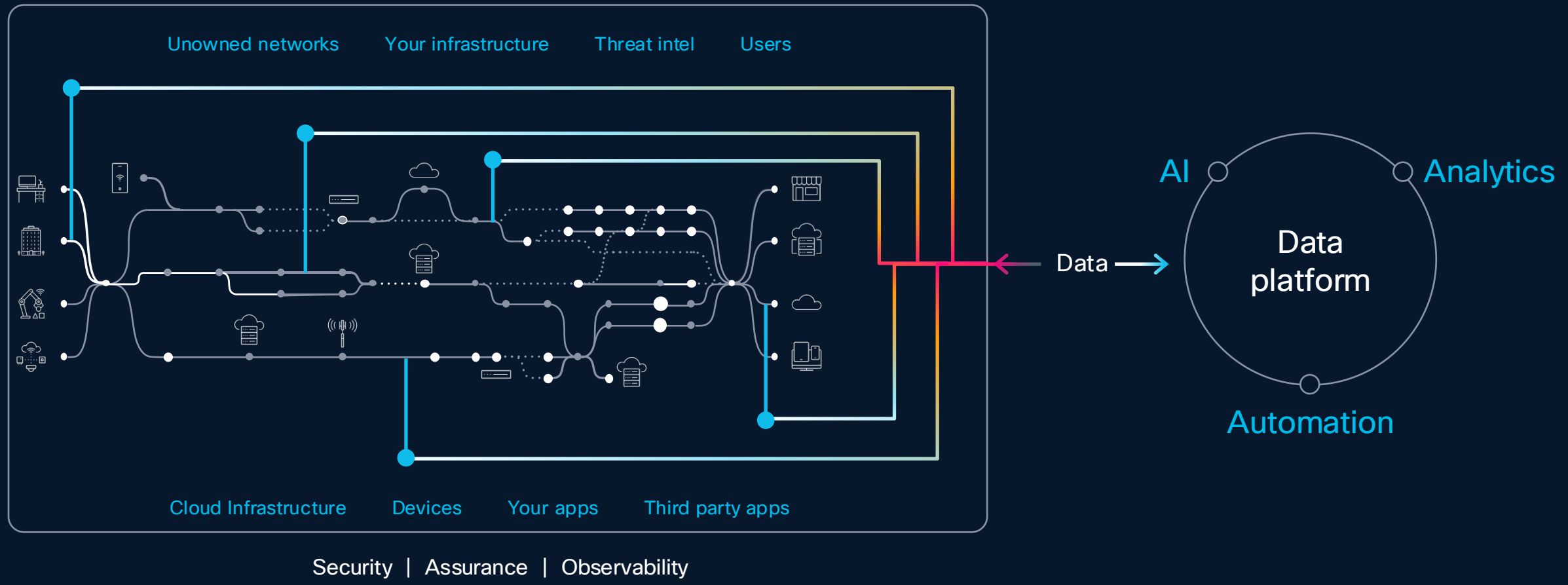
Record
Every conversation

Understand
what is **normal**

Be alerted to
change

Respond to
threats quickly

The 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

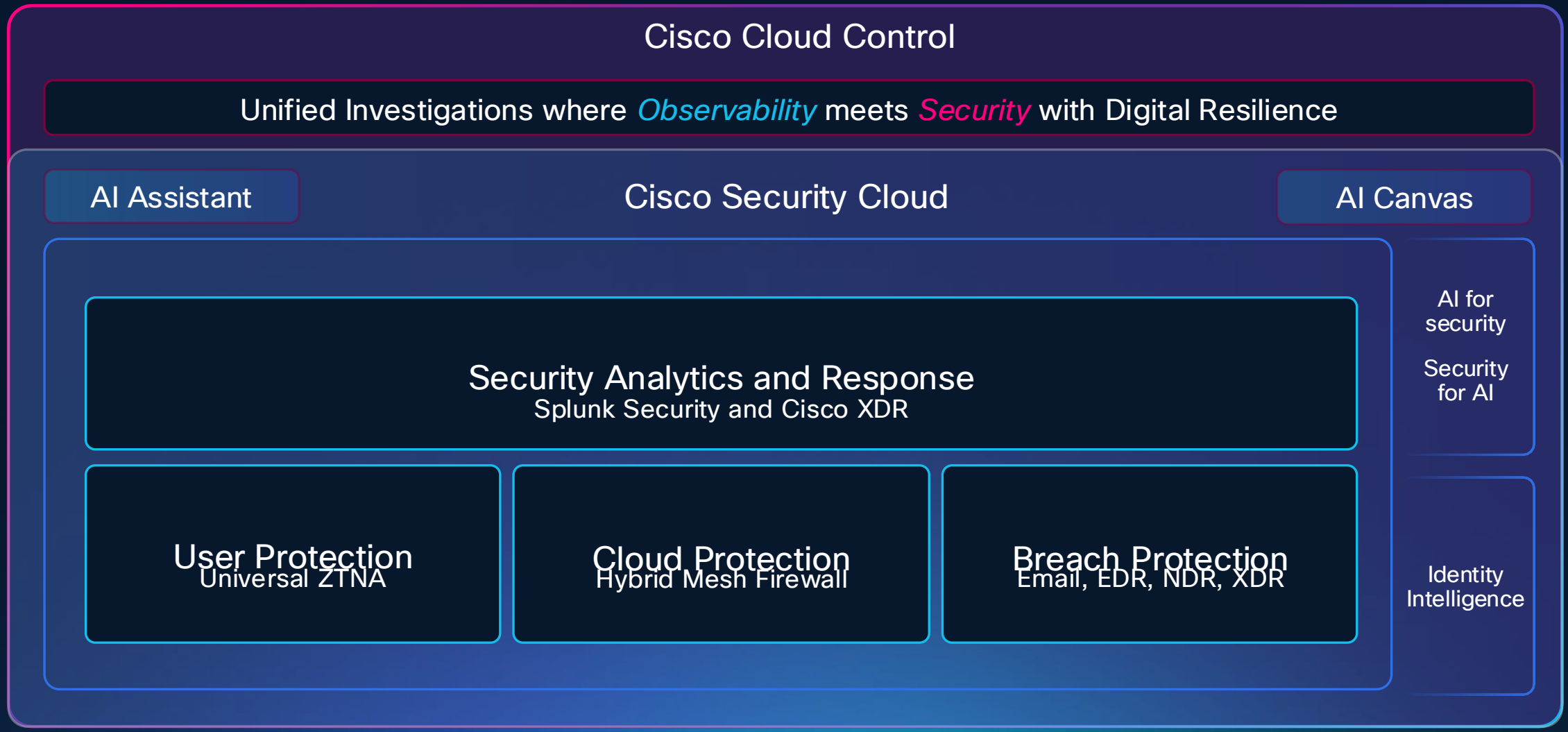
AI Powered Cisco Security Cloud: Cisco shines where Security meets the Network

Future-Proofed Workplaces	AI-Ready Data Centers	Digital Resilience
 **Accelerate Zero Trust Network Access** Identity | SSE	 **Secure Data Center Networking** Segmentation | Firewall	 **Power Security Operations** XDR | SIEM | SOAR
User Protection Suite	Cloud Protection Suite	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'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.

AI-Driven Risk Optimization

Proactive AI-led risk mitigation across the enterprise attack surface

Preventive and Dynamic Exposure Management

AI-driven exposure detection and remediation before attacks begin

Proactive and Predictive Security Operations

AI recommended detections and playbooks for likely attack paths

Autonomous Resolution at Machine Speed

AI-led security remediation with human-in-the-loop response

An Expanding Ecosystem of AI Agents

A shared community advancing autonomous, preventative, and adaptive SOC capabilities

Adaptive and Intelligent Data Fabric

An adaptive, unified data fabric transforming chaos into continuous operational resilience

Unify the SOC platform

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

cisco


XDR ≠ EDR++


Email
Network
Cloud
Firewall
Endpoint
Identity
SECURITY TOOLS

Cisco XDR

An equal seat at the table

Cisco XDR

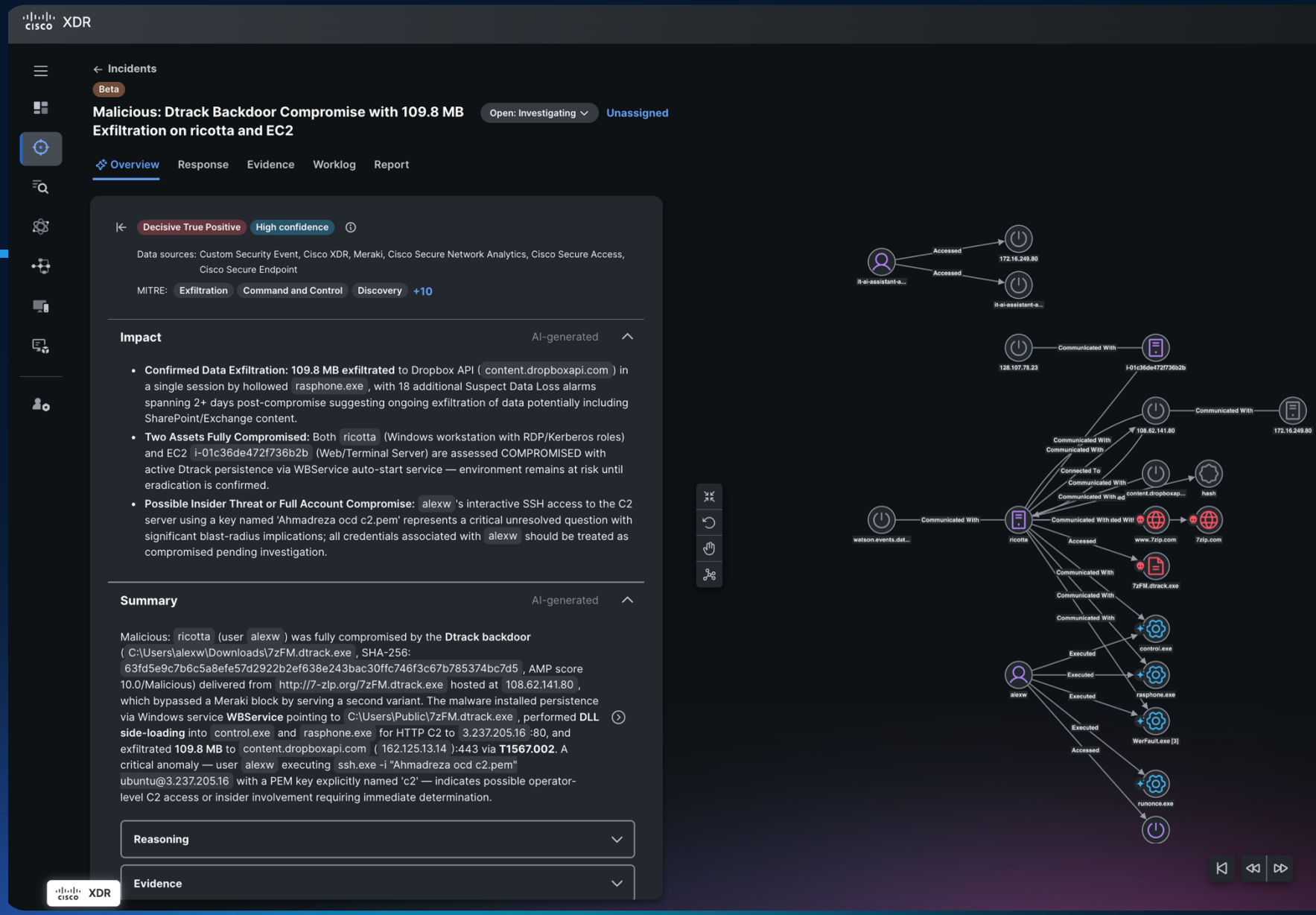
Improve Alert Fidelity

Instant Attack verification with a clear verdict

Command Every response and action

Single place to see all Security Alerts

Network at the core



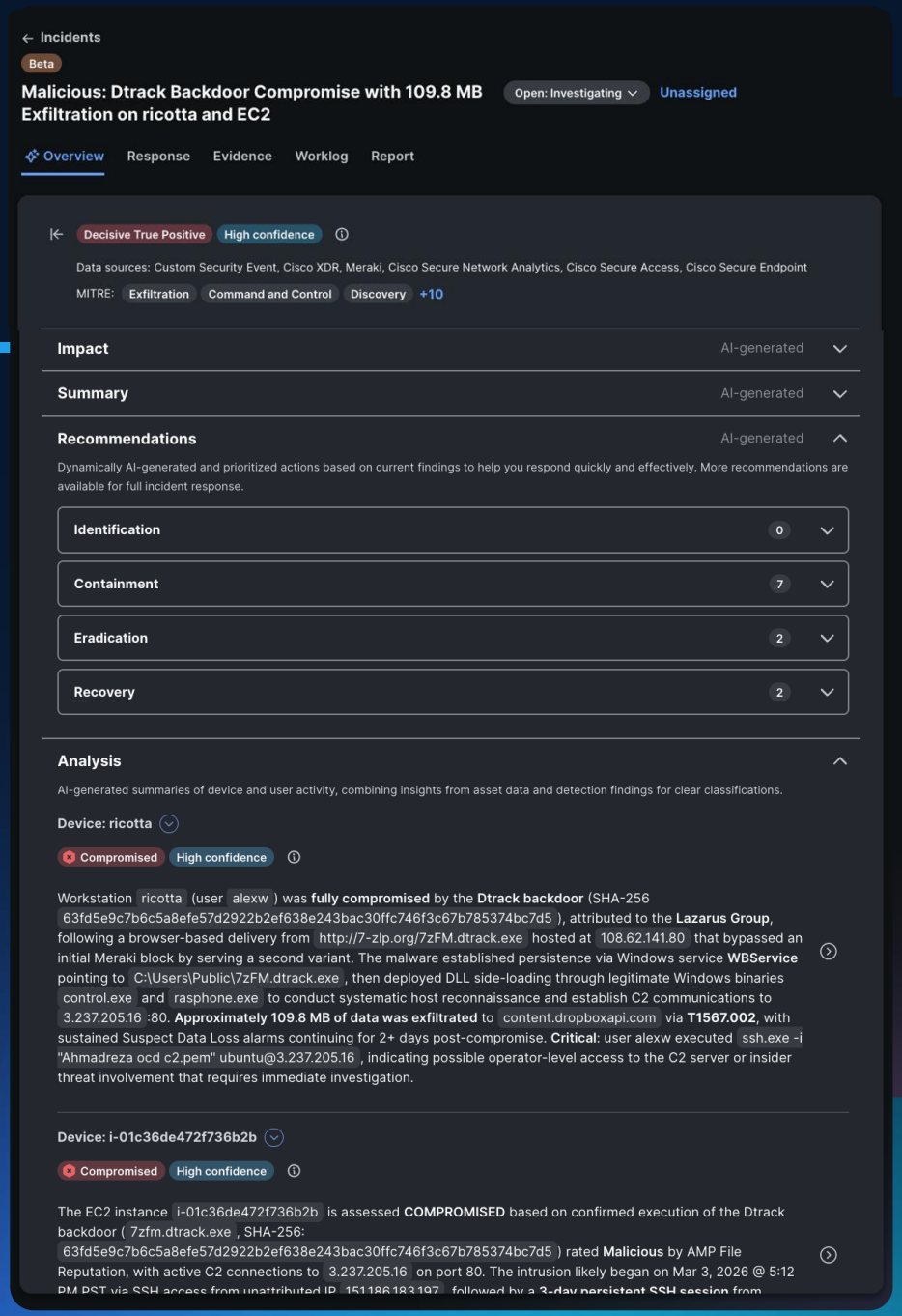
Instant Attack Verification

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

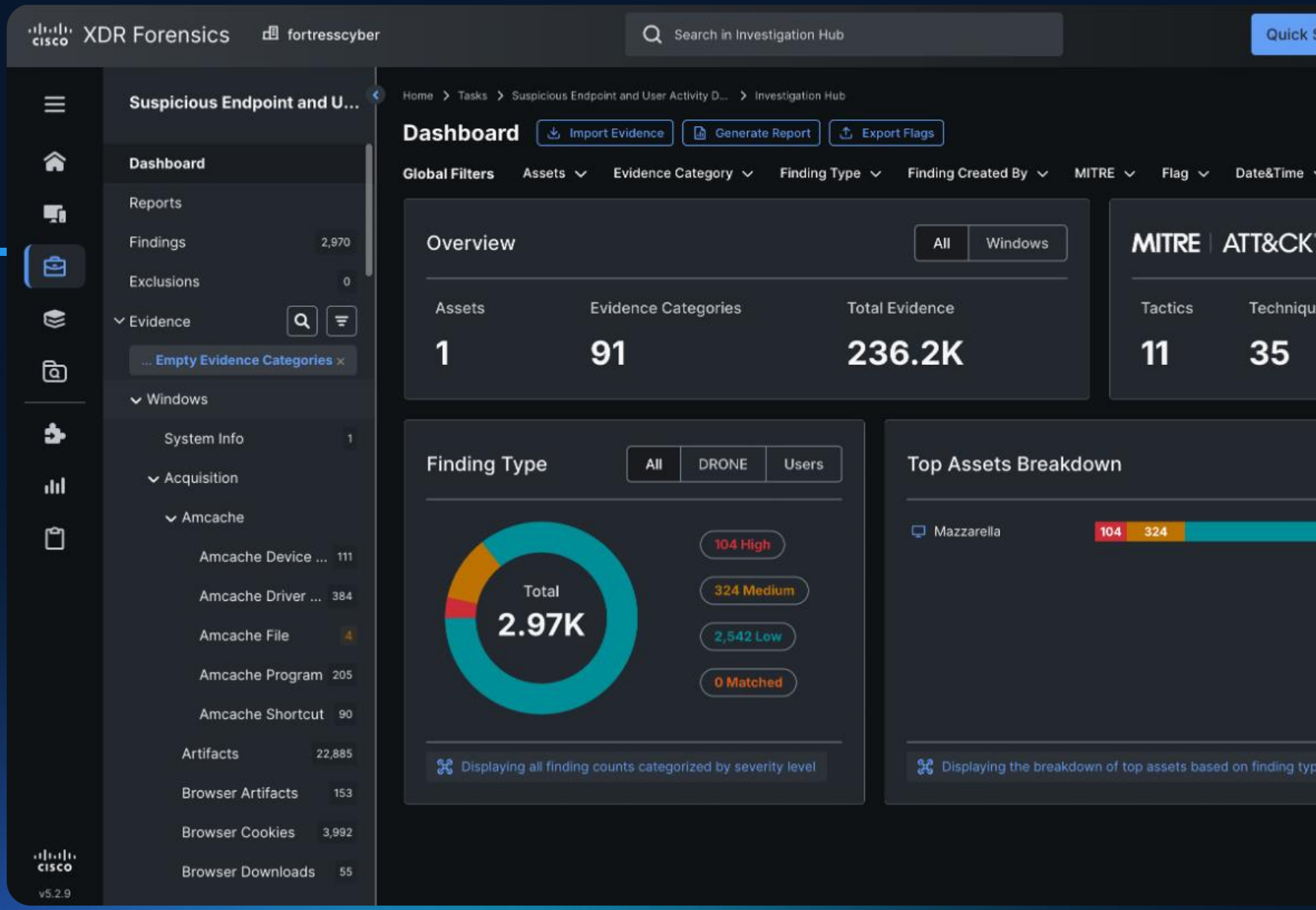


Cisco XDR Forensics

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

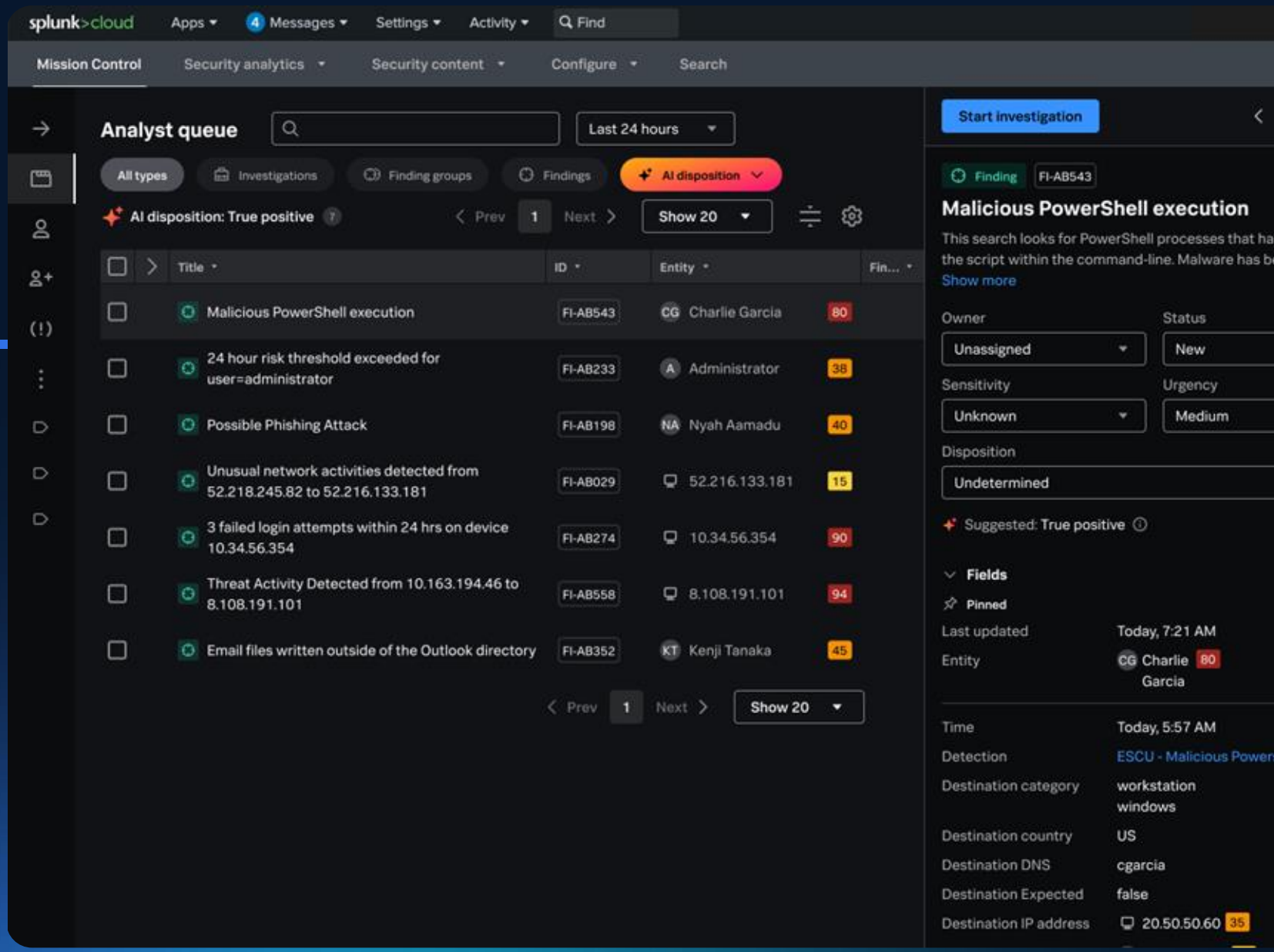


Enterprise Security Essentials

The leading AI-powered SecOps platform

Simplify your analyst experience with unified workflows

Includes Threat Intelligence and Exposure Management



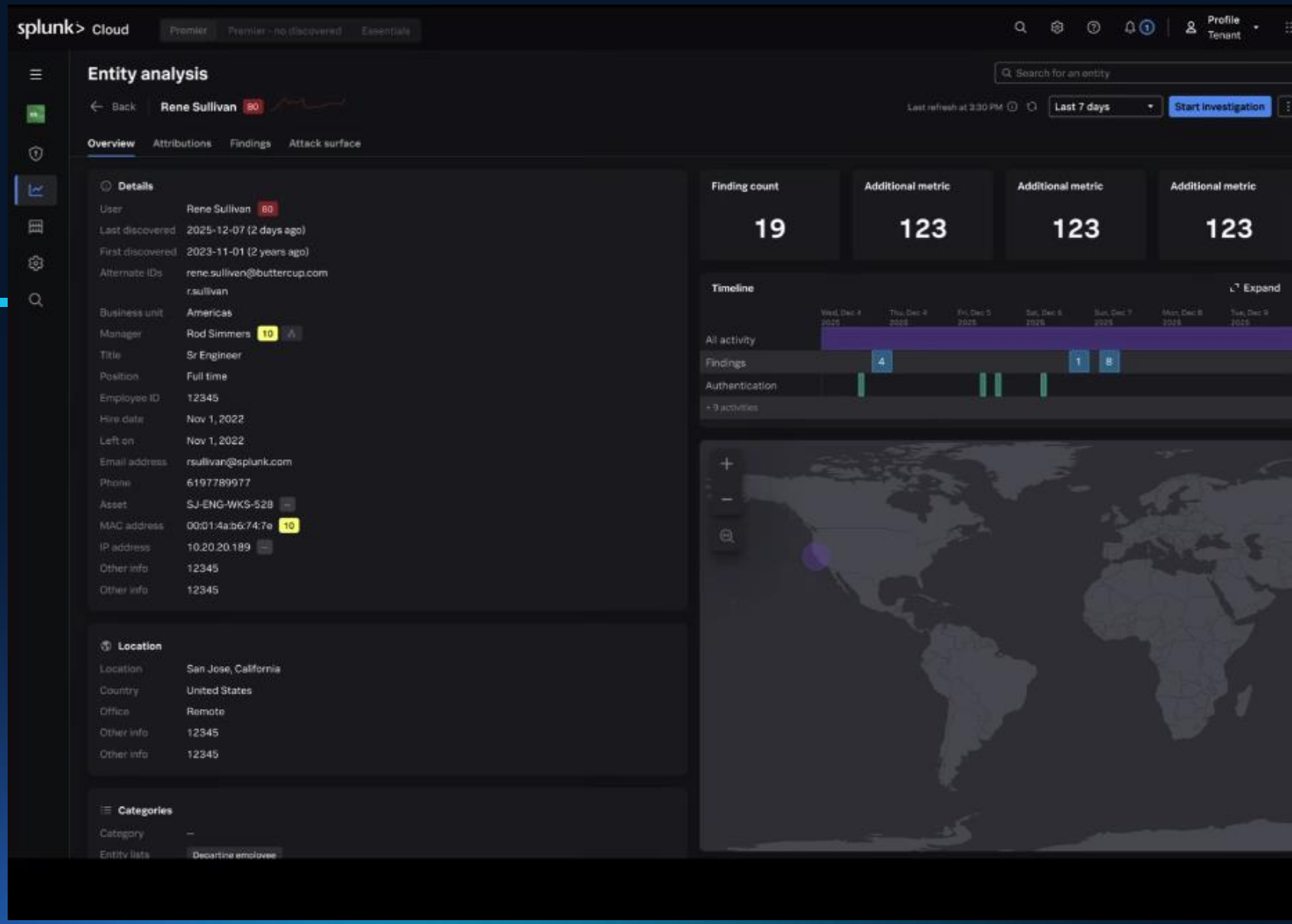
See it in action

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.

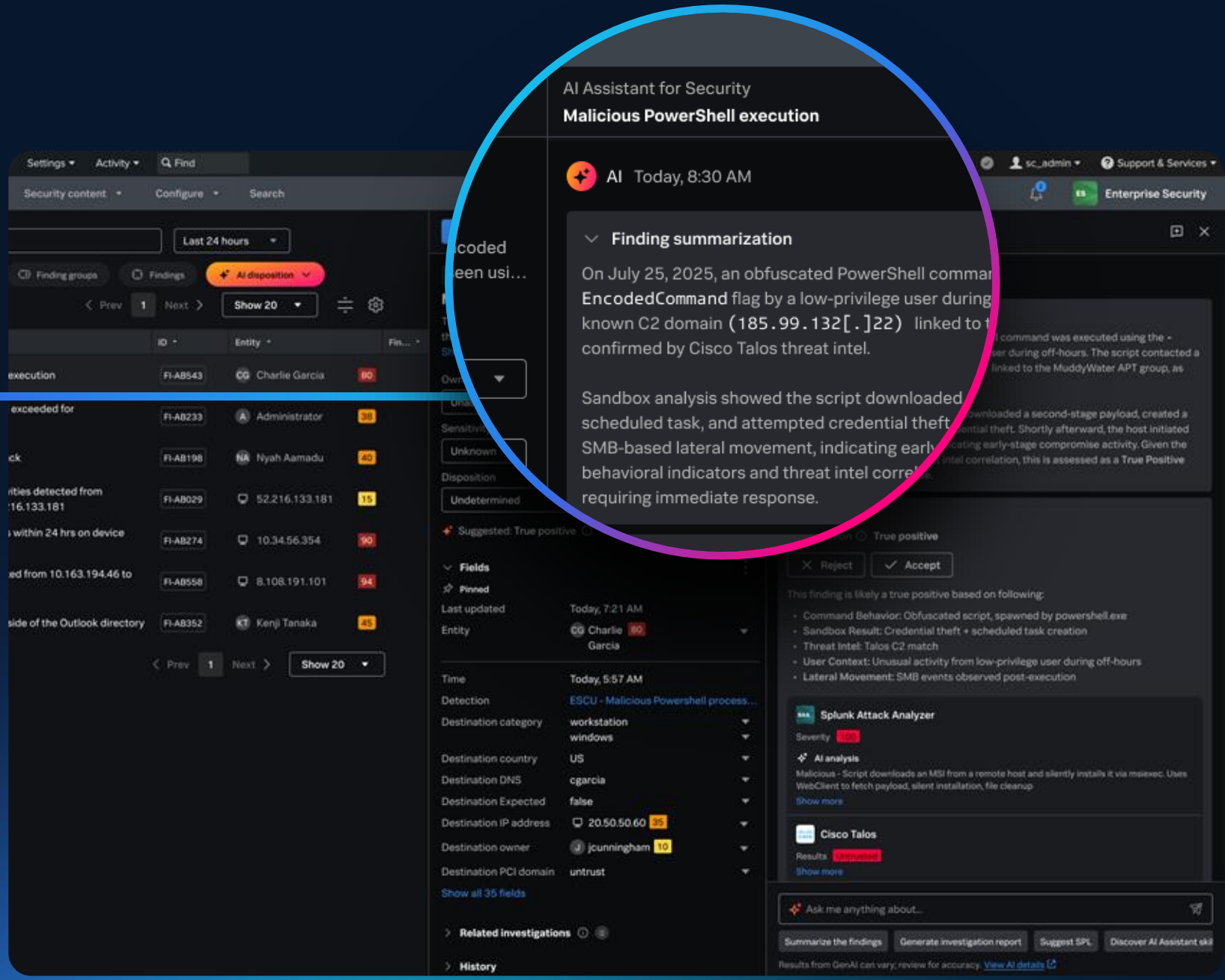


Enterprise Security Premier

The leading AI-powered SecOps platform

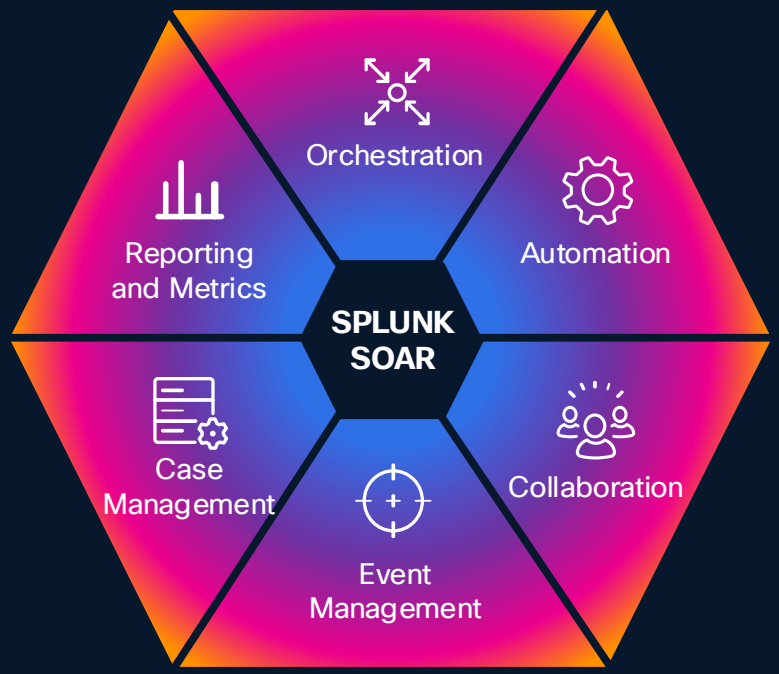
Simplify your analyst experience with unified workflows

Includes UEBA, SOAR and AI Assistant and more



See it in action

Spunk SOAR

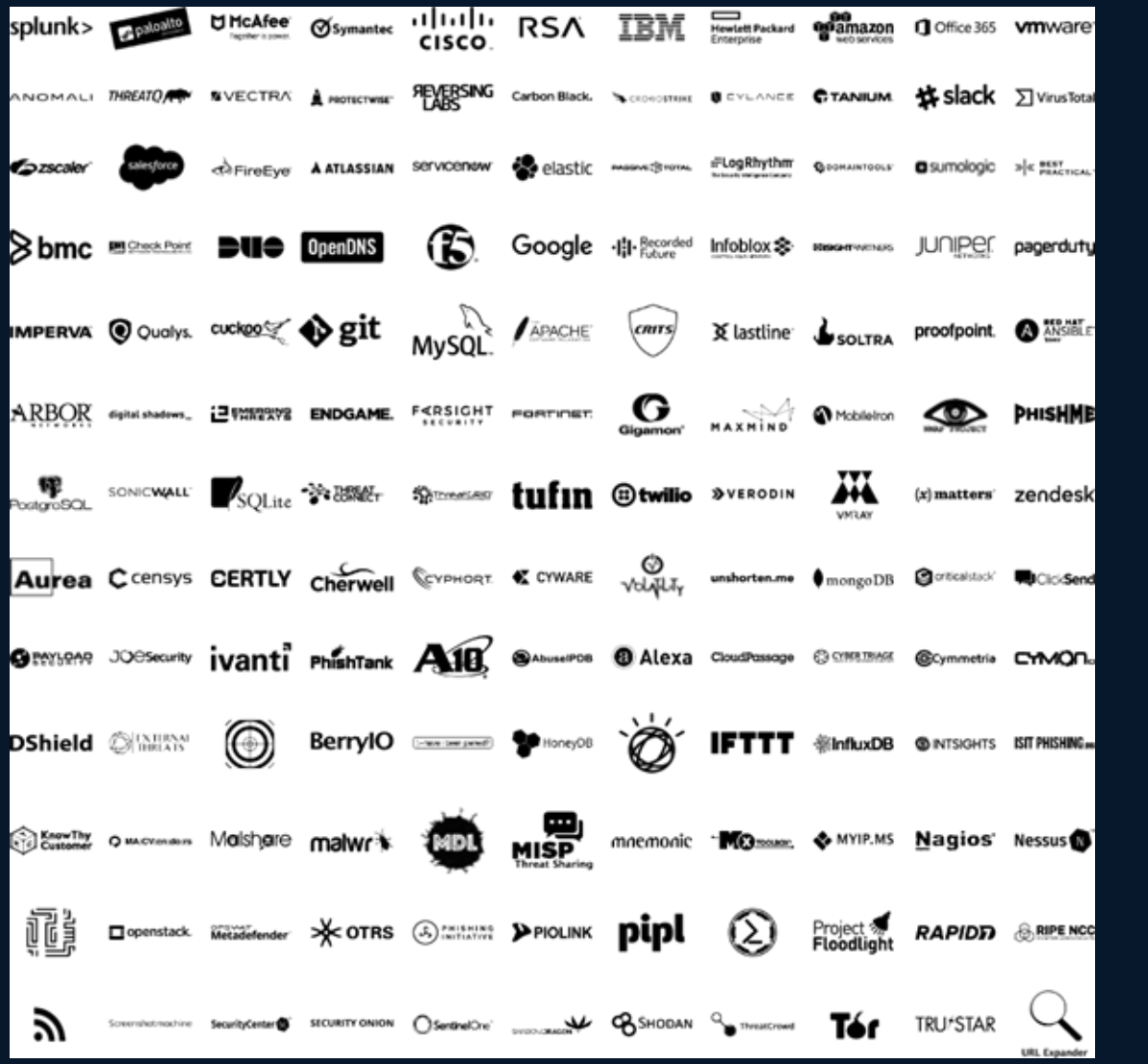


Orchestration

Coordinate complex workflows across your SOC

300+
APPS & GROWING

2800+
AUTOMATED ACTIONS

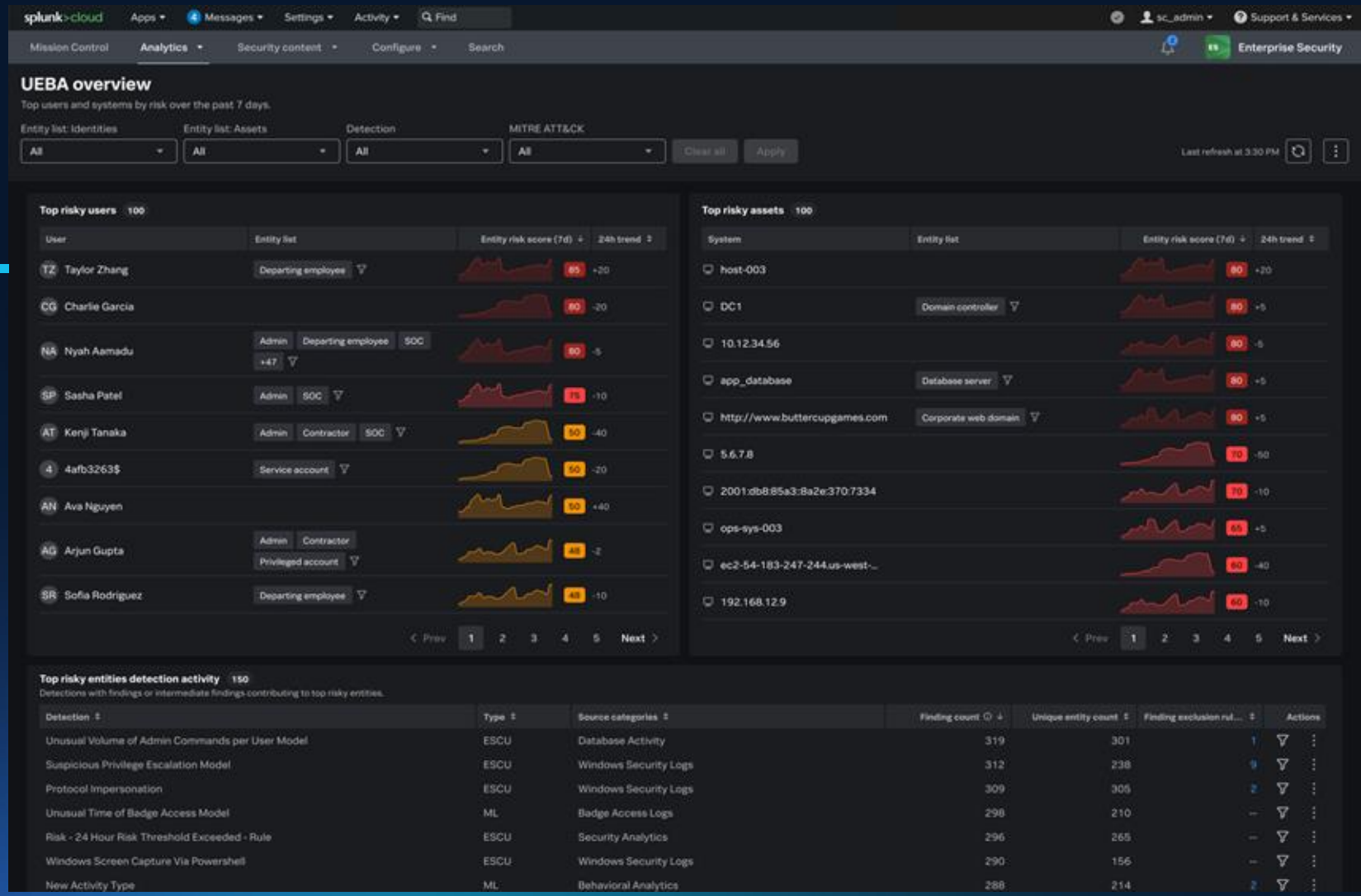


UEBA Insider Threat Detection

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.



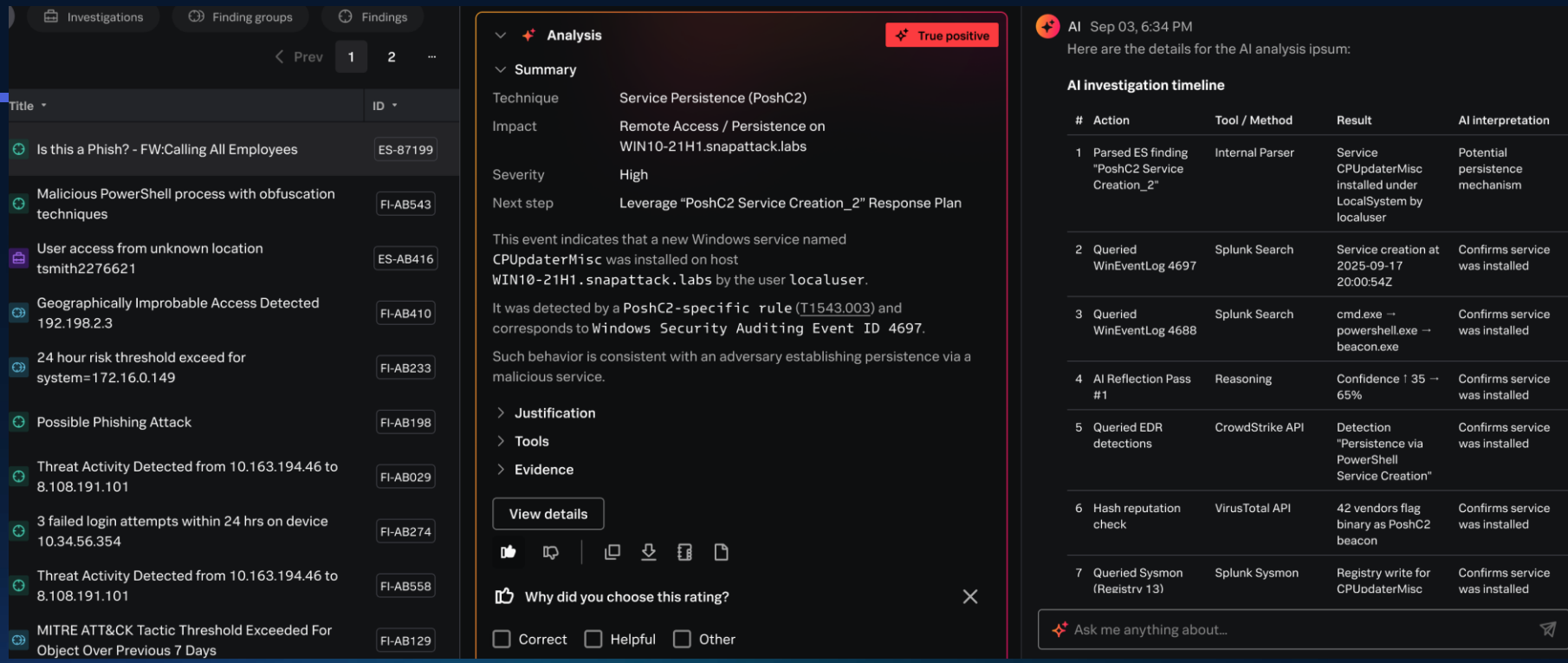
Triage Agent

Automatically determine alert disposition

Streamline alert prioritization

Plan and execute investigations

Automate insights to reduce MTTR



See it in action

AI Security Assistant

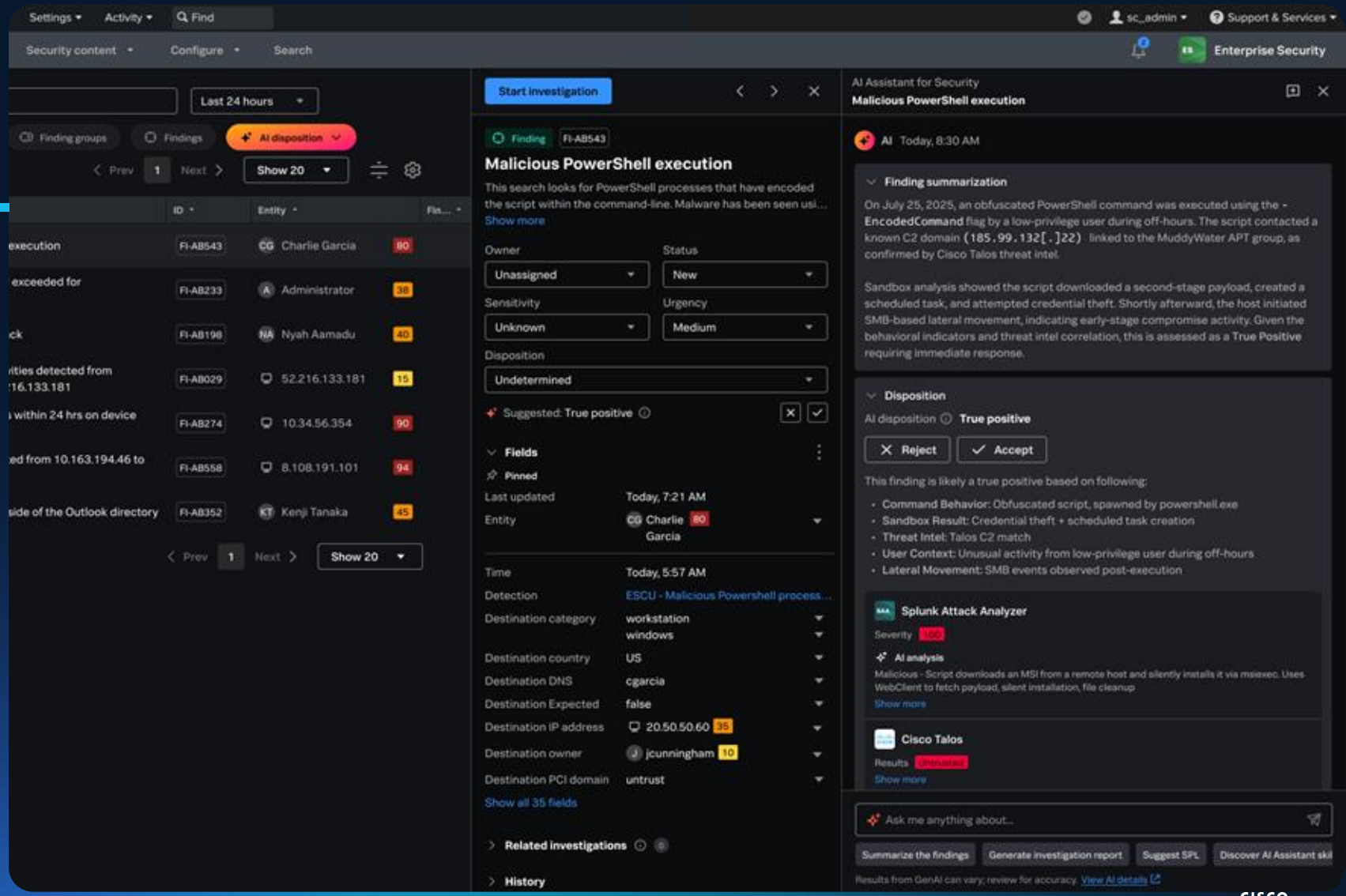
Embedded across all analyst workflows

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



See it in action

cisco

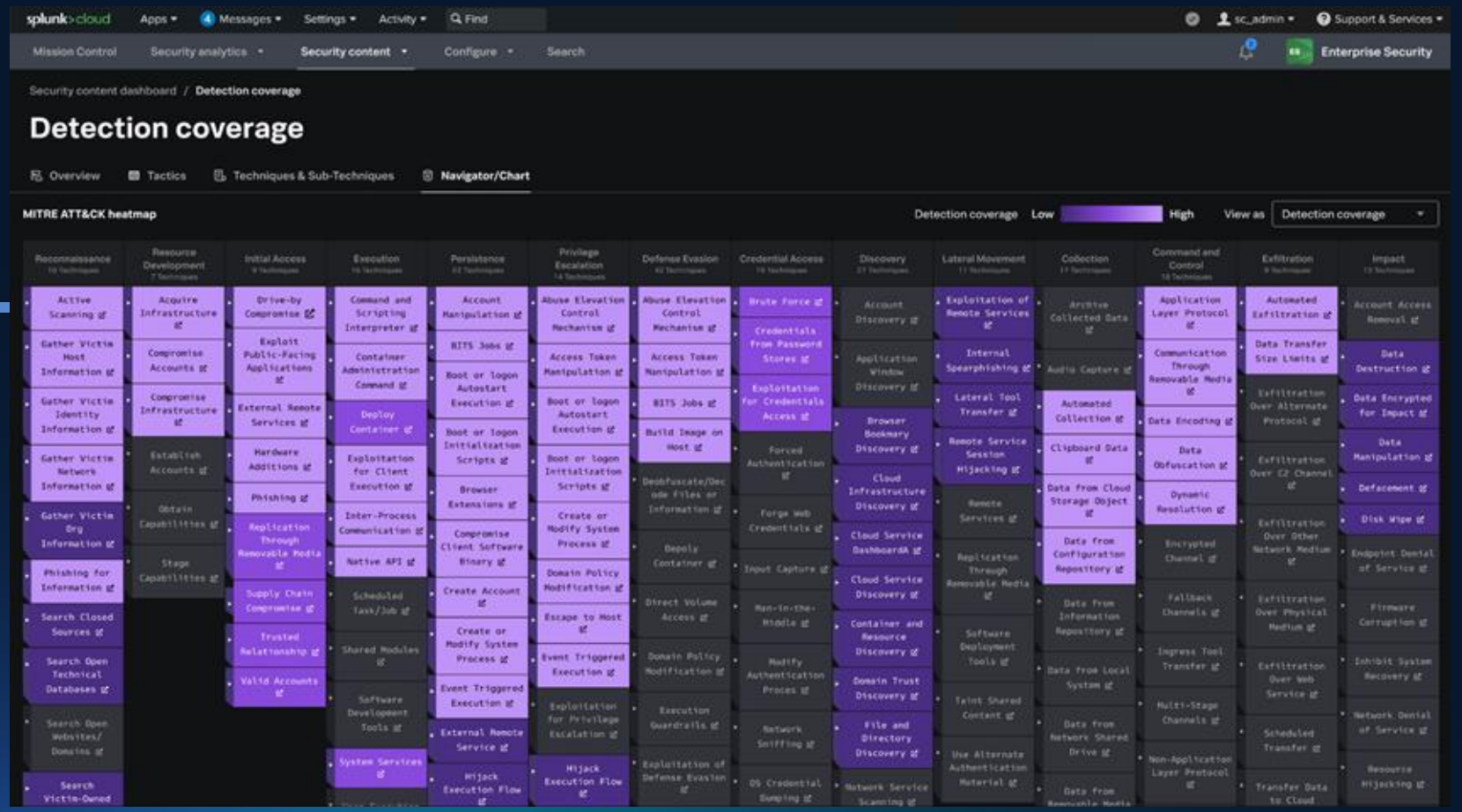
Detection Studio

Powered by SnapAttack

Streamline detection creation workflows

Evaluate detection health

Expand versioning and detection-as-code



See it in action

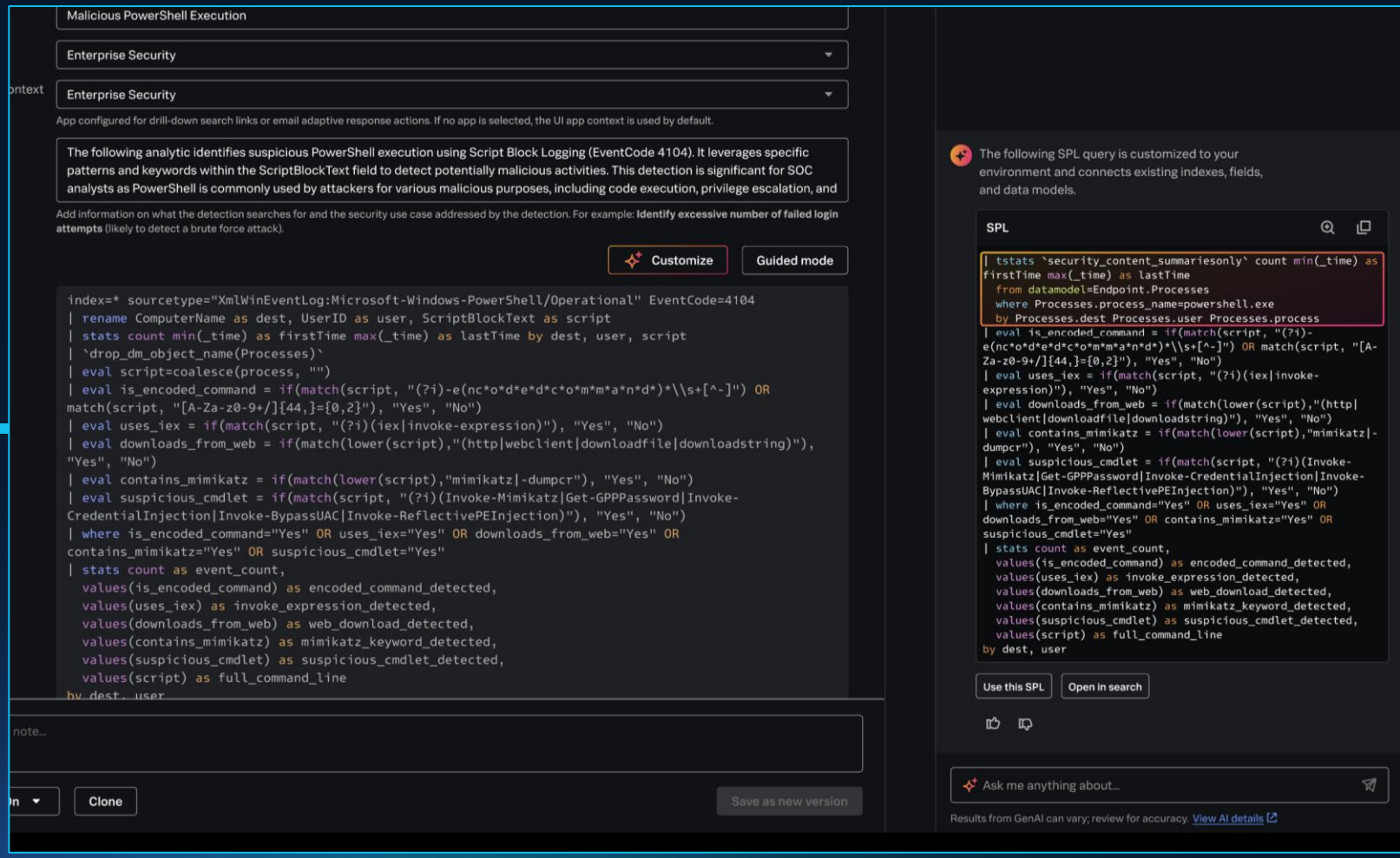
AI Assistant for Detection Authoring

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

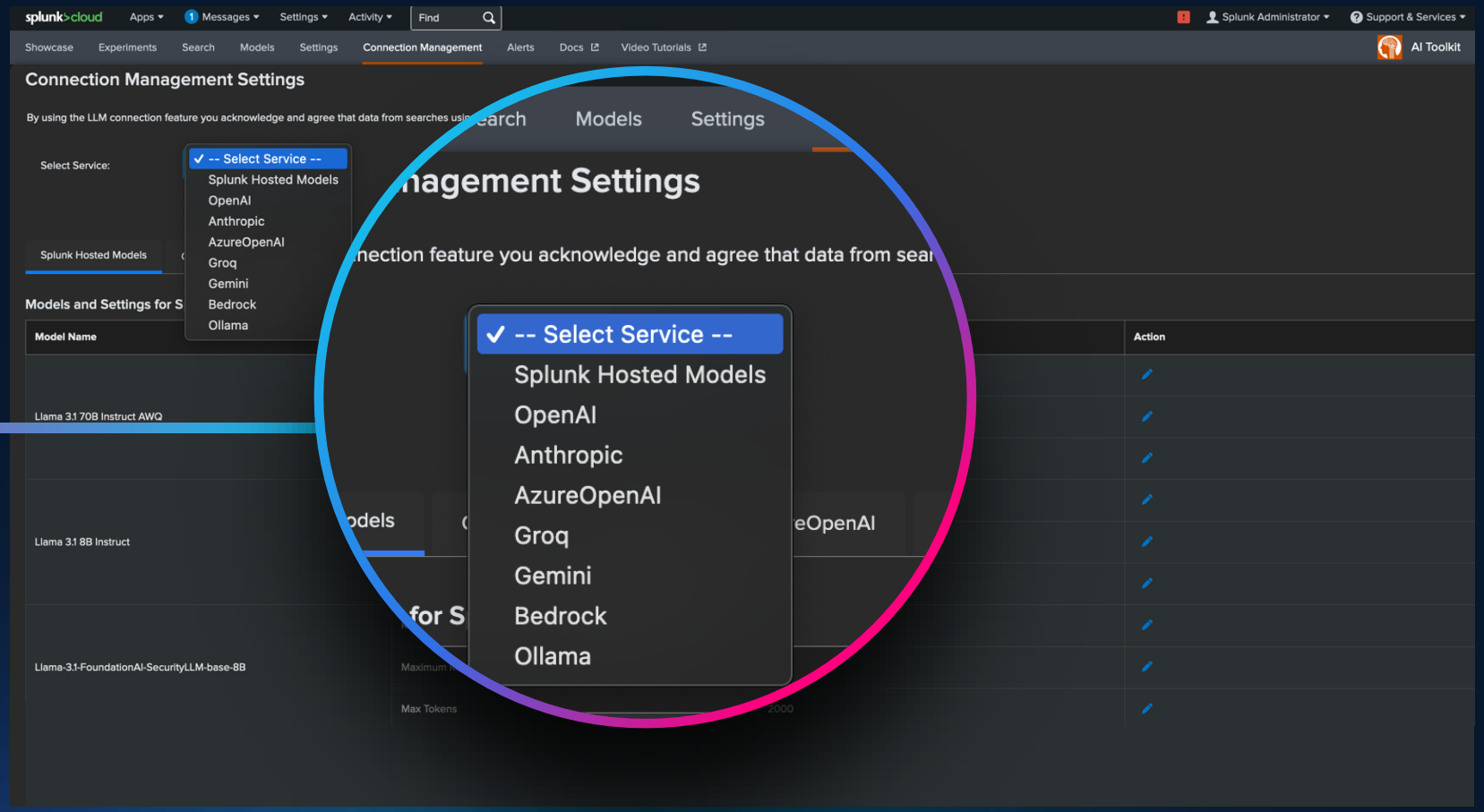


AI Toolkit with LLM Integrations

Build and deploy AI models

Query Splunk with 3rd party LLMs

Access Splunk hosted models, coming soon




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

Customer Journey

Foundational

- 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
- Simplified Investigation
- Integrated SOAR solution
- Essential Third-Party Integrations
- Integrated Endpoint Forensics
- Agentic AI Investigations
- AI Generated Reporting
- < 1 year of Data Storage

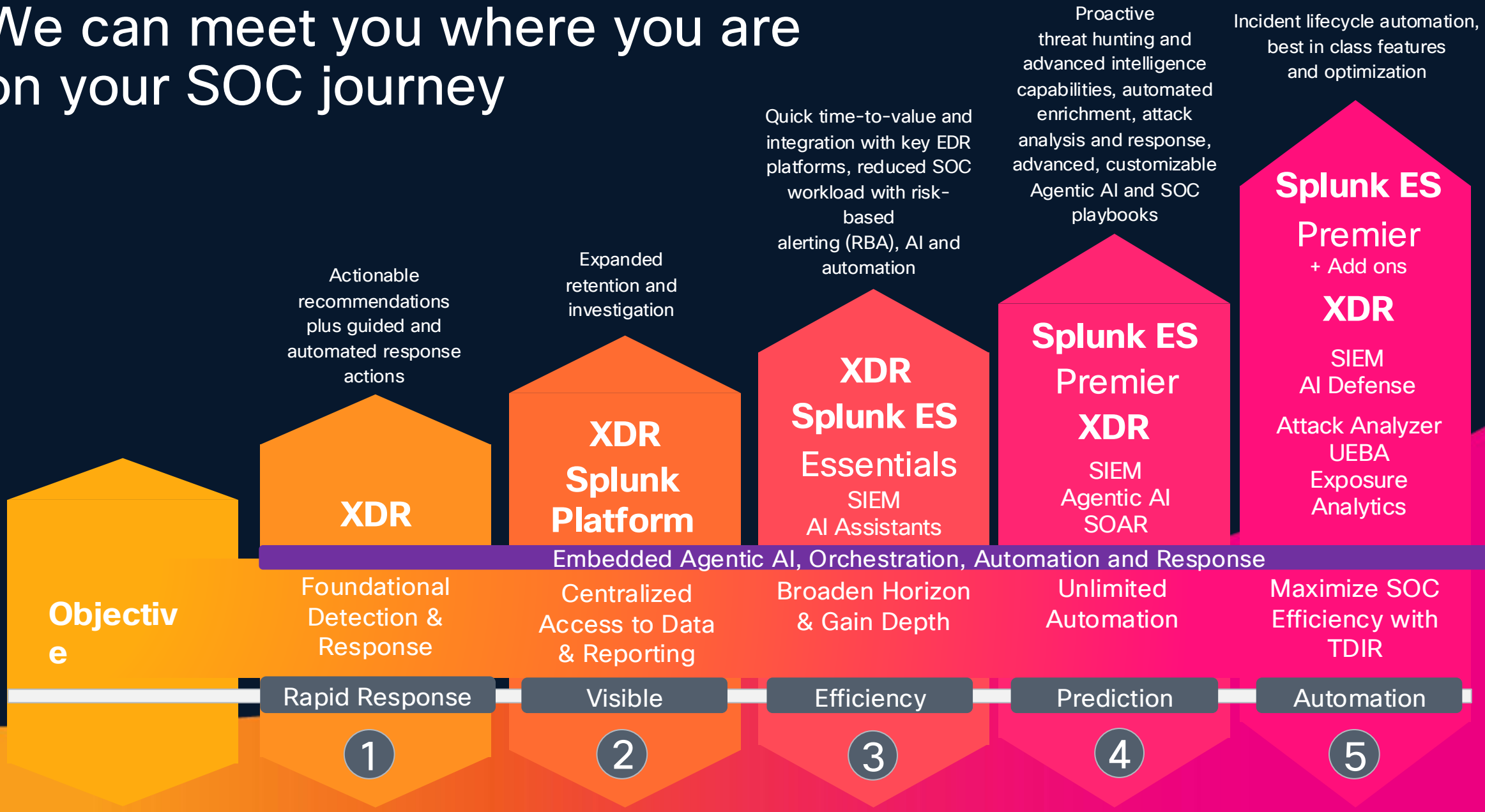
Transformative

- 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

Maximized

- 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
- Everything in ES & XDR
- Detection Validation
- Insider Threat / UBA
- Customizable Risk-based Alerts
- Asset Risk Intelligence
- Next Generation Sandbox
- Detection Validation
- Machine Learning Took Kit
- Data Science Took 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

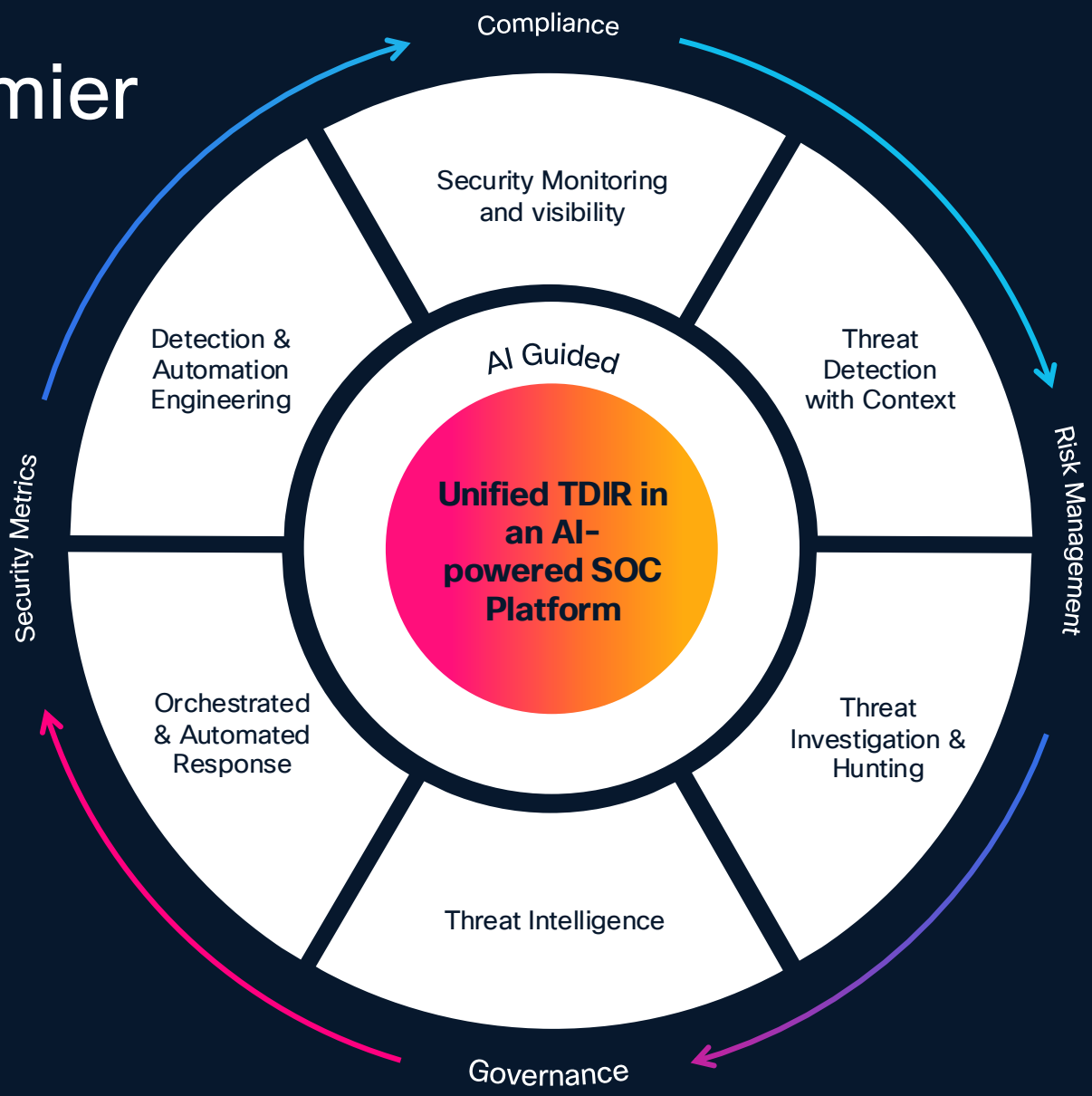
Premier

- 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**

SecOps Analyst | Incident Responder | DevSecOps Security Automation | CTI / Threat Hunter | SOC Director | CISO

Unified Security Platform

Cisco Security Cloud Platform
Multi-tenancy, Role Based Access Control, Entitlement & Provisioning

AI Assisted Investigation | Endpoint Forensics | Orchestrated Response

Cisco AI Canvas

Splunk Cloud Platform
Single Tenant, Role Based Access Control, Entitlement & Provisioning

AI Assisted Search | Detection Engineering | Threat Hunting | Compliance, Fraud, IT

3rd Party Policy Enforcement

Unified Reporting & Dashboards

TALOS — 500 threat researchers + Third party intelligence + AI powered algorithms

Cisco Breach Protection Suite – Cisco XDR

Asset Insights | Identity Intelligence | Threat Intelligence Automation

Cisco Security Cloud App

Splunk Enterprise Security + SOAR

Asset Intelligence | User Behavior Analytics | Attack Analyzer

Cisco XDR Analytics

Splunk Enterprise (Core Search)

Cisco Managed Telemetry (*DR)

Network | Endpoint | Email | Cloud | Apps | Identity

3rd Party Verified & Community telemetry

3rd Party telemetry

Cisco Data Fabric (S3, ASL, Splunk)

INTEGRATED SECURITY CAPABILITIES: Cisco XDR & Splunk

Cisco XDR

Splunk (Core & Enterprise Security)

1. Get Data in (GDI) to Splunk using Cisco Platform Security Cloud Control Technical Add-On

Cisco Platform Security Cloud Control Technical Add-On

4. Bi-directional event closure

5. Sharing risk context and native detections for full platform analysis

2. Enhanced analysis leveraging extended data in Splunk Core or Splunk Enterprise Security as a finding

6. Cisco XDR Dashboard in Splunk App Analytics

T1/T2

3. Automated Escalation when T1/T2 team members need help or deeper investigation

AUTOMATED CORRELATION AND INCIDENT DETERMINATION

DEEP INVESTIGATION AND TRIAGE

AUTOMATED AND INCIDENT RESOLUTION

LIFECYCLE MANAGEMENT

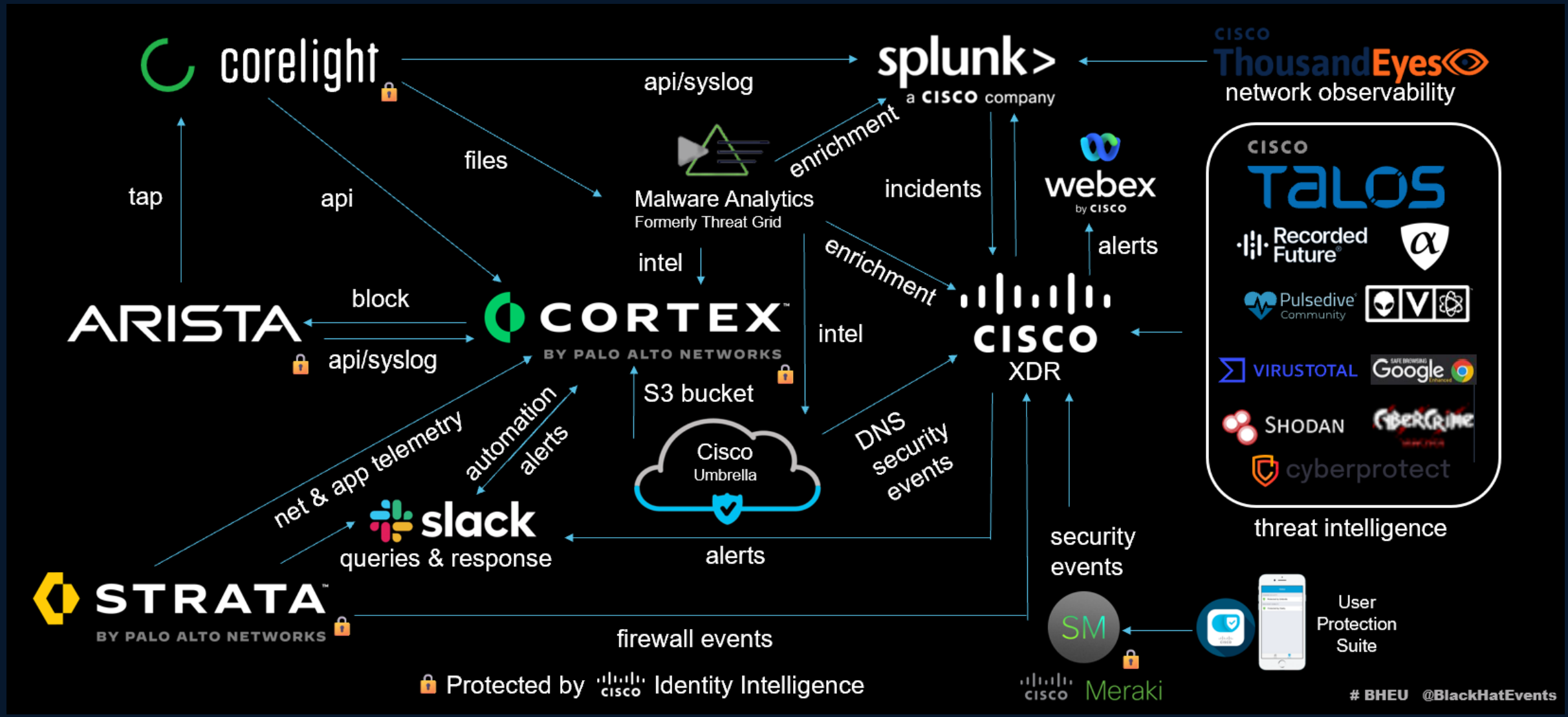
CISCO Engage | Tech Day Milwaukee

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

cisco

Thank you


CISCO