CISCO Connect

L'IA Agentique pour les opérations de securité : moins de bruit, plus d'impact Agentic SOC by Splunk

Digital Resilience

Moez Kamel
Global Security Specialist – EMEA

Nicolas Mayer
Security Solution Architect – EMEA

21 Mai, 2026

Unrelenting Pressure on SOC Teams

Gaps in coverage

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

Fragmented, manual tooling

Siloed solutions, manual and reactive capabilities wear on team effectiveness

Overwhelming attack surge

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

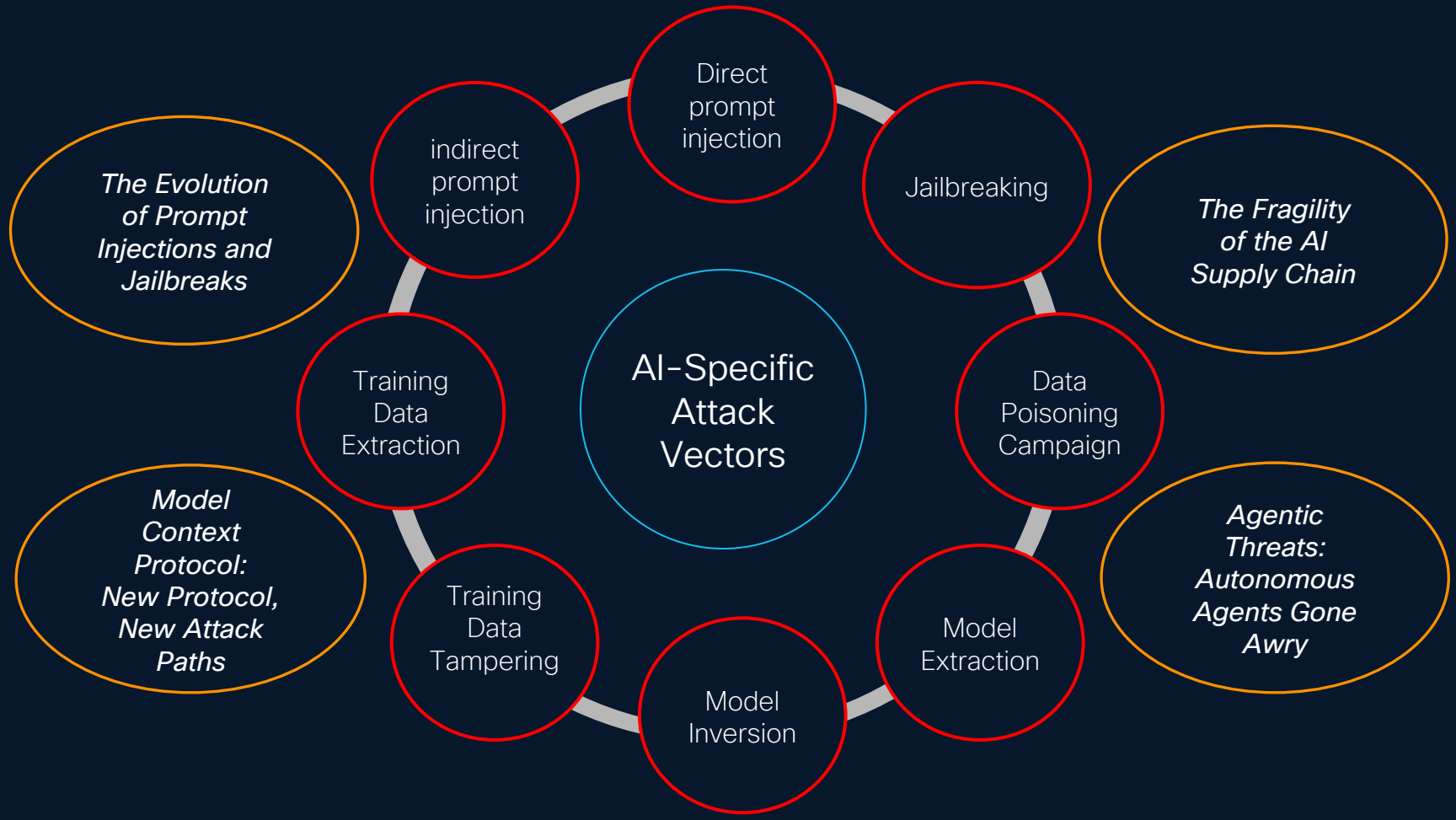
The result: a record 50%+ of security leaders[1] and practitioners likely plan to quit their role in the next 12 months[2].

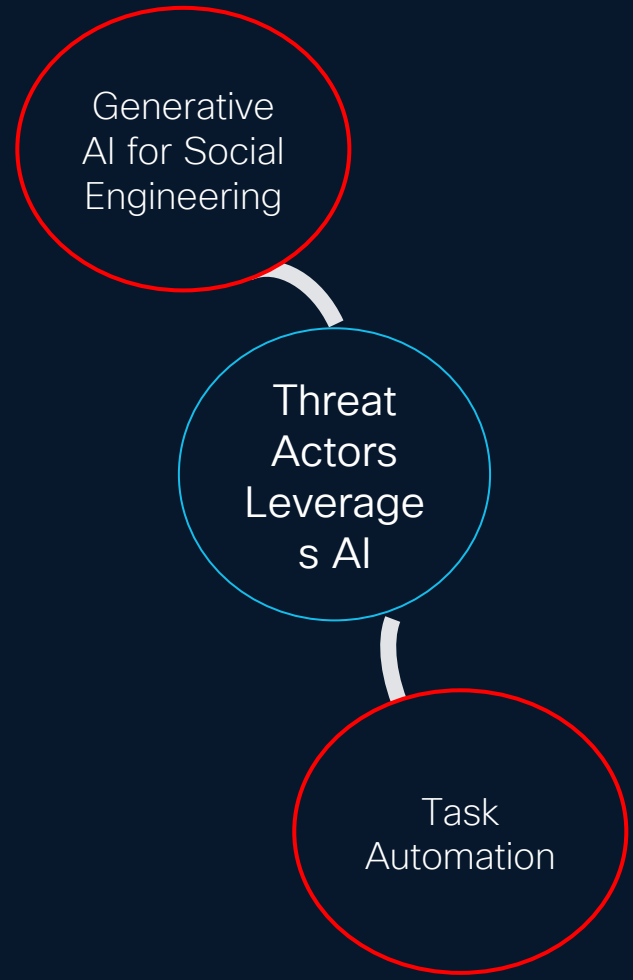
Security from the Agentic Frontier

The AI Transformation is here and we must transform for it

cisco

State of AI Security
AI Threats Landscape



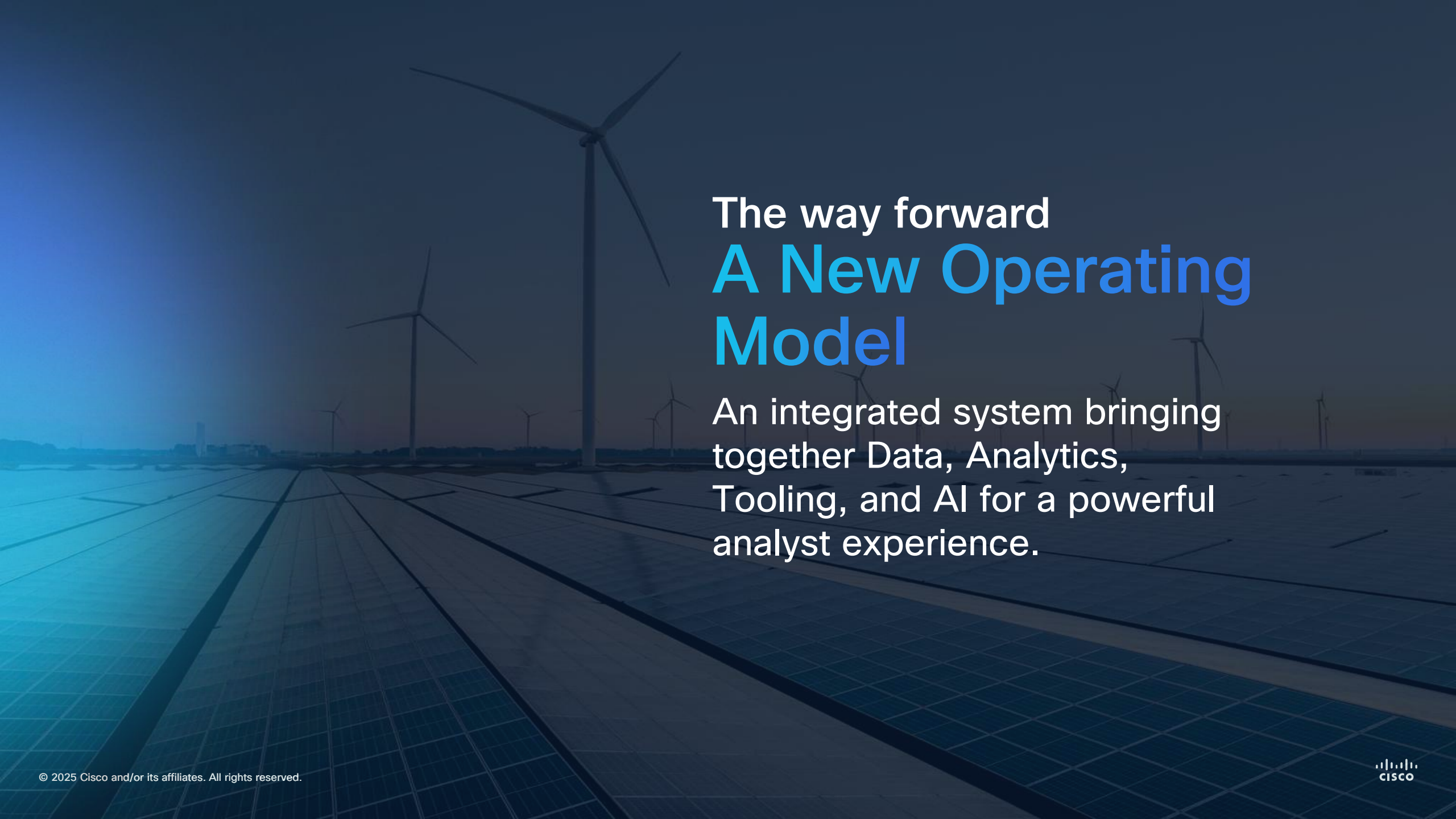


Your security team is stretched thin.

It's time for an agentic SOC platform that:

- **Automates the mundane**
- **Clarifies the complex**
- **Stops threats at machine speed**

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



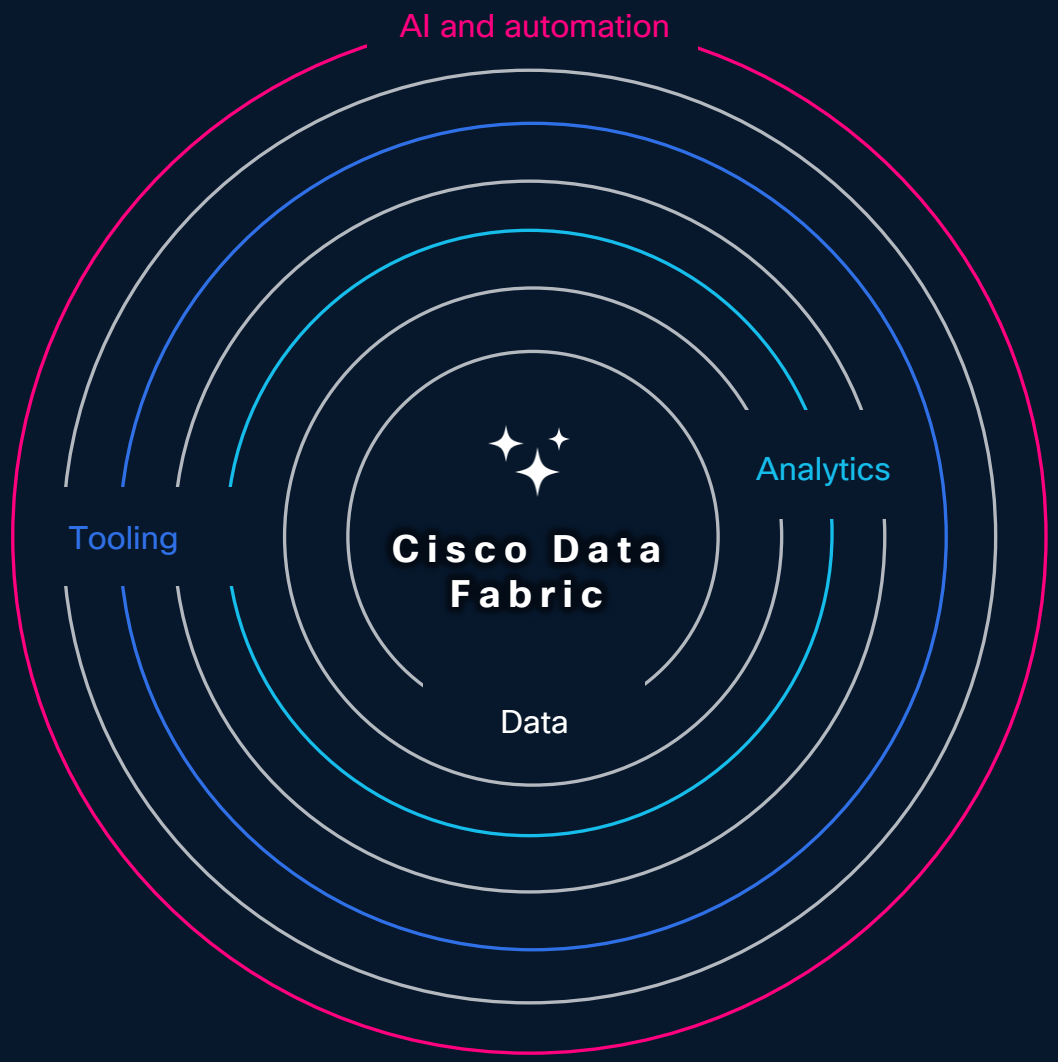
The way forward

A New Operating Model

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

Agentic SOC

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



A Foundation of High-Fidelity Data

Data fabric
Data management
Data pipelines

Analyzed at Machine Speed

TI enrichment & context
Correlated detections
Investigation & hunting

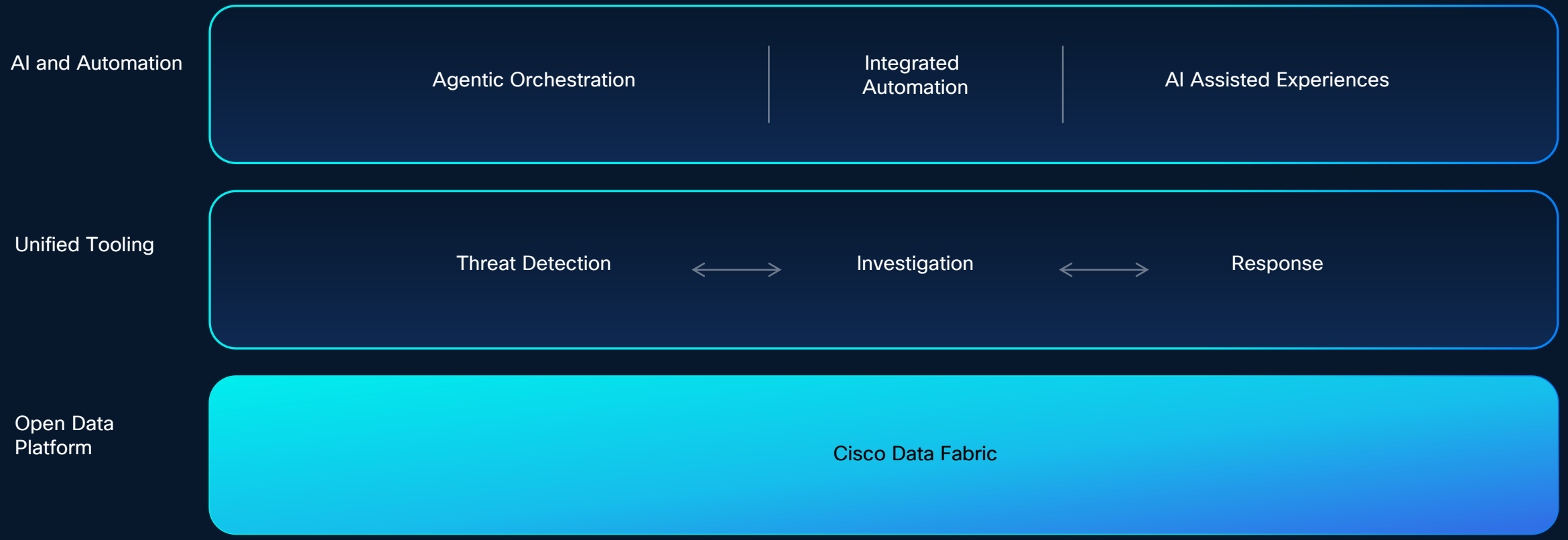
With Intuitive SOC Tooling

Single work surface for TDIR
Team coordination
Integrated workflows

And Human-led AI & Automation

Customizable agents
Reasons and acts decisively
Prevents emerging threats

The new operating model for security in the Agentic era



Human-in-the Loop

Simplify and distill the analyst experience.

AI to maximize the human.

Domain-specific

AI to accomplish a specific security goal.

No AI for the sake of AI.

Open and Extensible

AI that is understandable and specific for each environment.

No closed boxes.

cisco

Human-AI Operating Model

How AI Trust is Earned : Evidence Packets

Auditable	Traceable	Provable
		
Human Out Of The Loop (Auto)	Human On The Loop (Supervised)	Human In The Loop (Approved)
LOW RISK	MODERATE RISK	HIGH RISK

cisco

Enterprise Security

Now available in two editions

Dedicated and purpose-built Security AI Agents

Detection agent

Malware Reversing Agent

Triage Agent

Orchestration/ SOP Agent

Guided Response + Automation Agents

SPEED

Detection

Triage

Investigation

Response

cisco

Augmenting Splunk with AI

- Cisco Foundation Models
- AI Toolkit
  LLM Integrations
- Data Science and Deep Learning
  3rd Party Runtime Connectors

Splunk Native AI

Flexible and Customisable → Simplicity of Use

Custom AI/ML Platform

- AI Toolkit
  DSDL Toolkit
- Native search commands

Human Guided AI Assistants

- AI Assistant for SPL
- AI Canvas
- OOTB ML Analytics
- AI Assistant in ES
- UEBA
- Detection Studio

Autonomous AI Agents

- Triage Agent
- Malware Reverse Engineering Agent

AI for Security

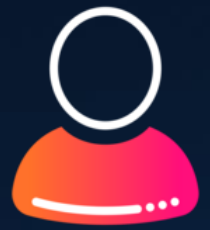
AI enhanced with Splunk

- MCP Servers

The SOC Operation

Initial Triage

Incident Response



Advanced Response

Engineering

Management

TDIR Platform

cisco

Agentic Automation

Triage Agent

ASK

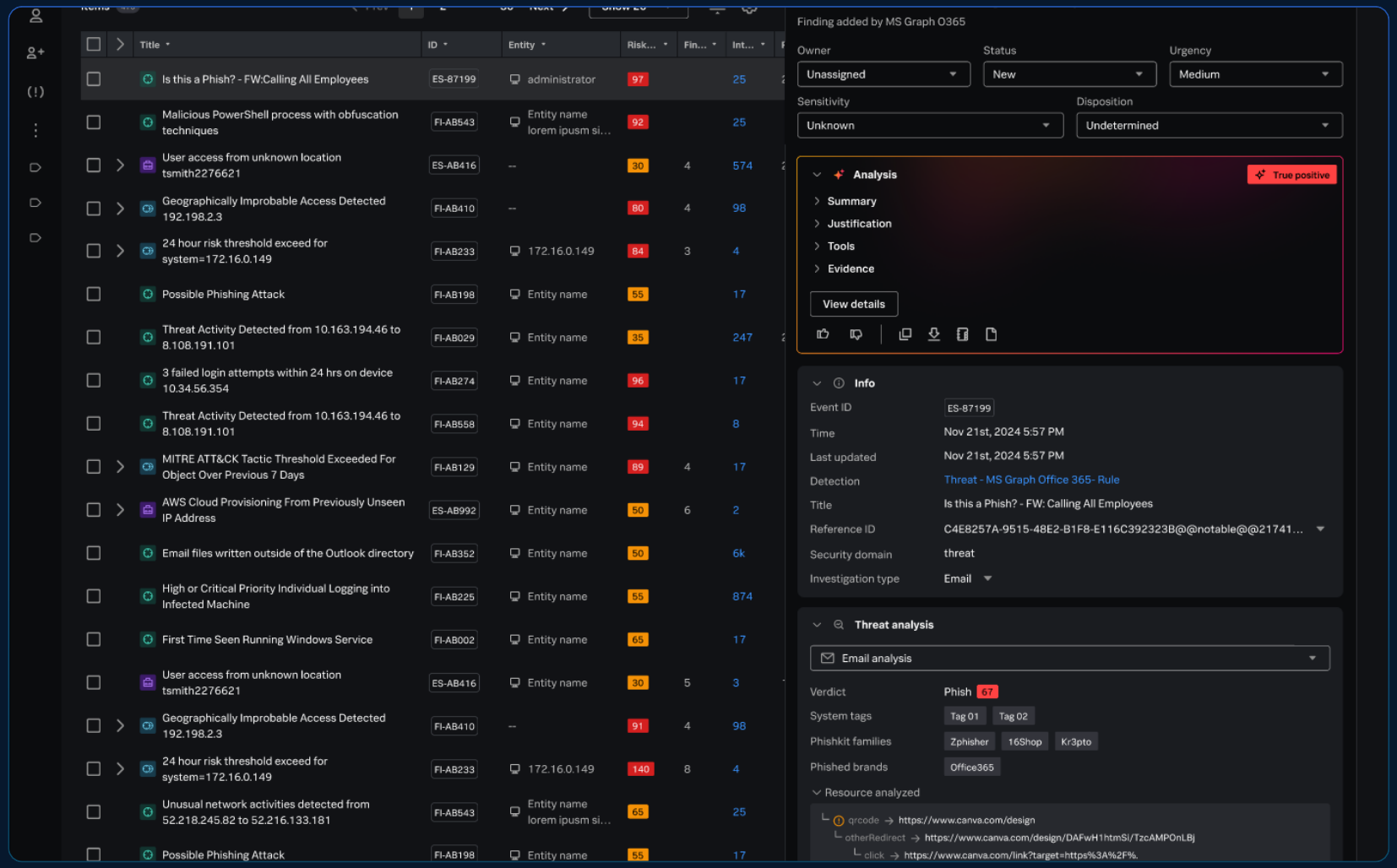
Streamline alert prioritization and disposition

SEE

Automate insights to reduce MTTR

ACT

Plan and Execute investigations



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

Agentic Automation

Investigation Canvas

ASK

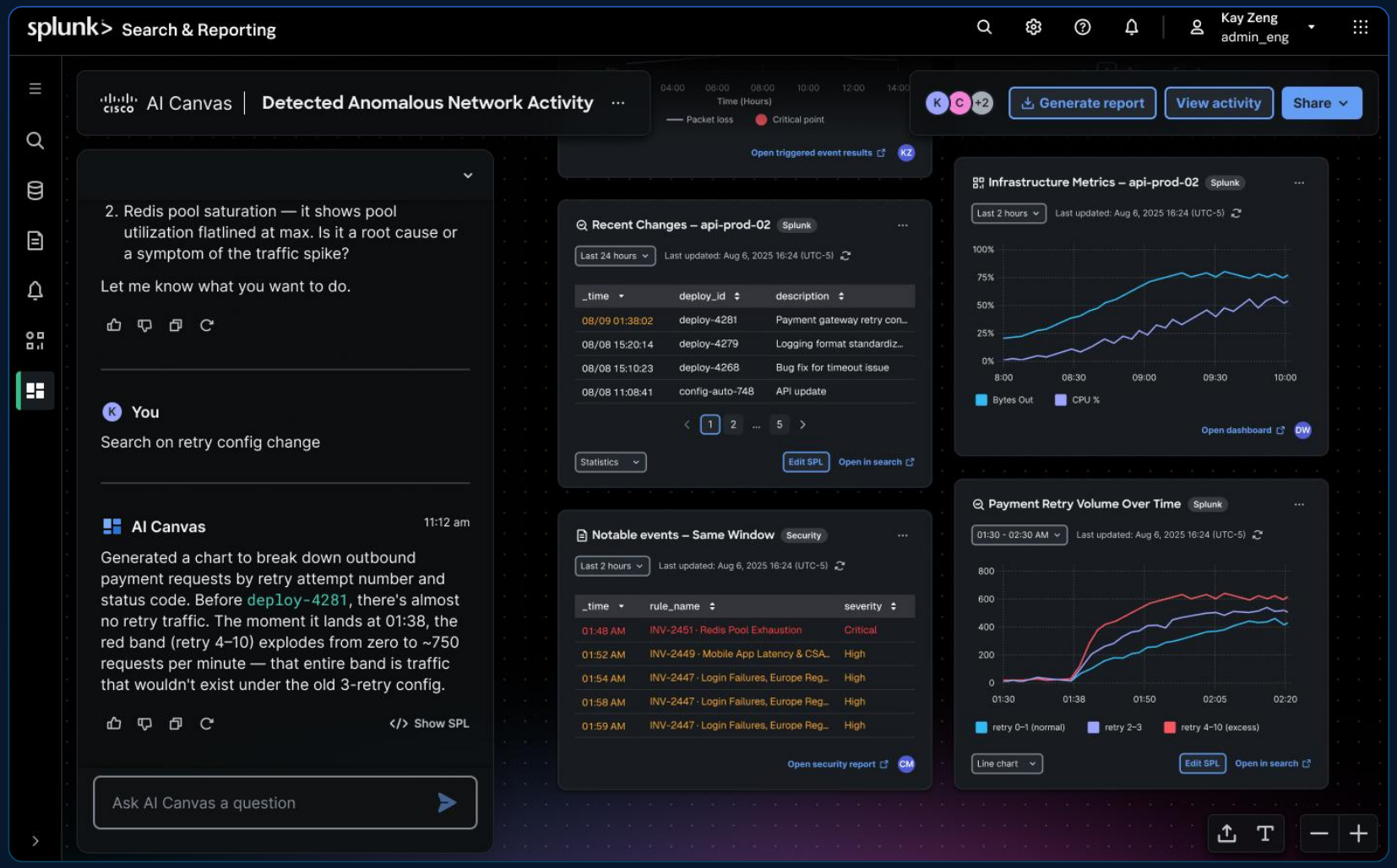
Type what you want to know

SEE

Investigation Canvas builds the visualization for you

ACT

Launch SOAR-powered actions right inside the workspace

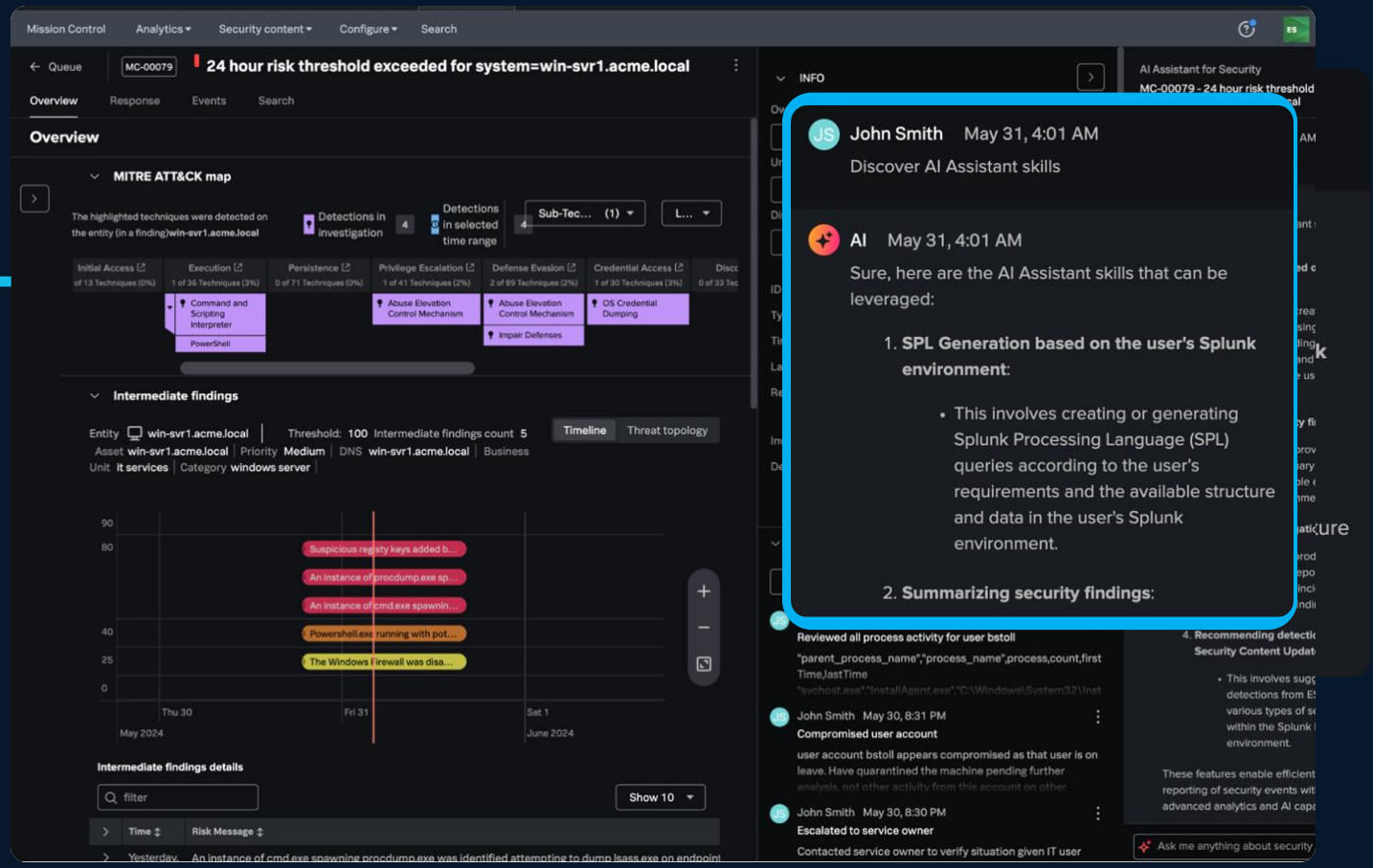


Enable analysts to move from question → insight → response in a single generative workspace.

AI Assistant in Security

Guided security workflows

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



AI Playbook Authoring

- Generative AI to build automation
  - Interactive AI Building

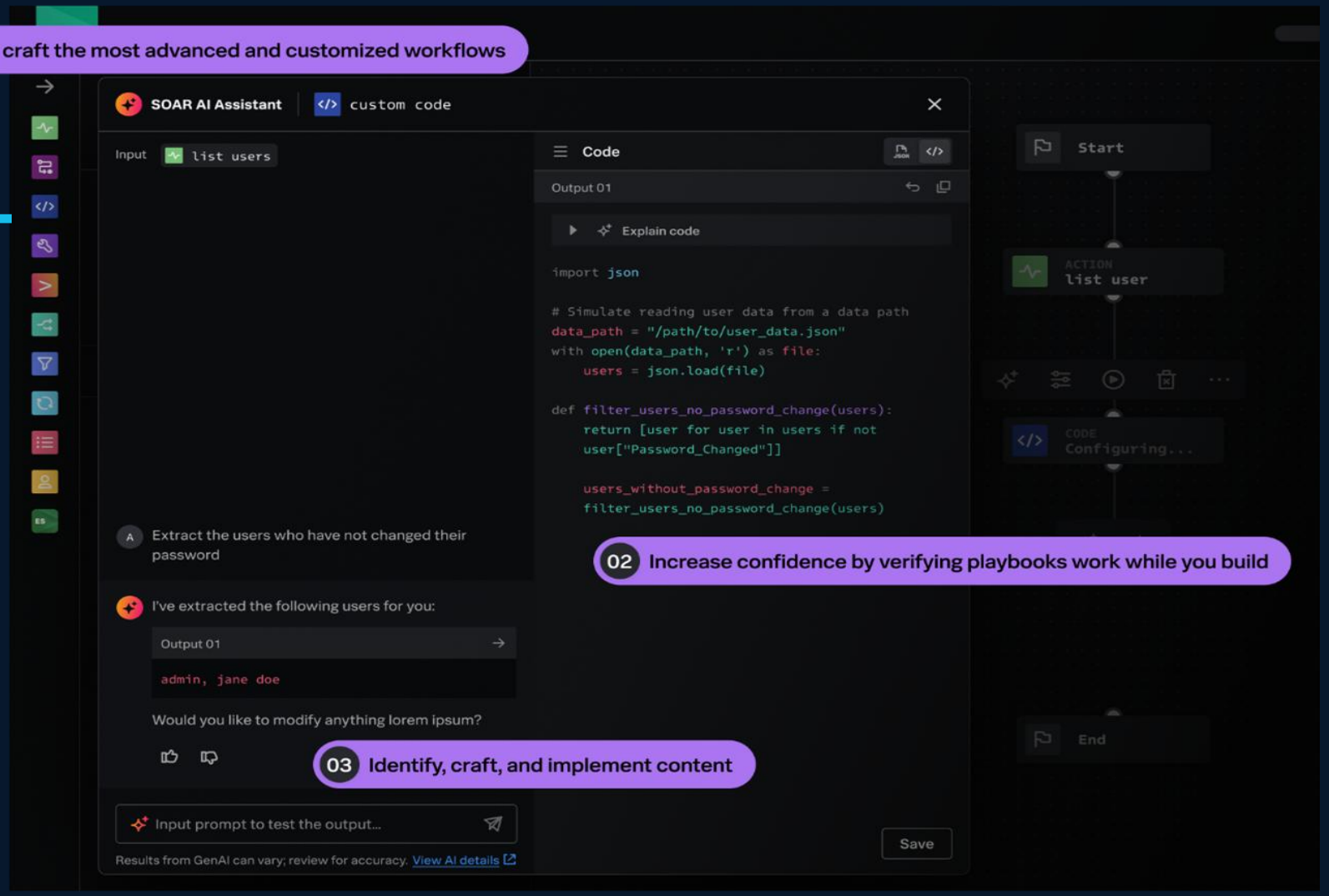
    Gen AI builds based on prompts that map to your exact use case

  - Refine with AI

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

  - Complete with Confidence

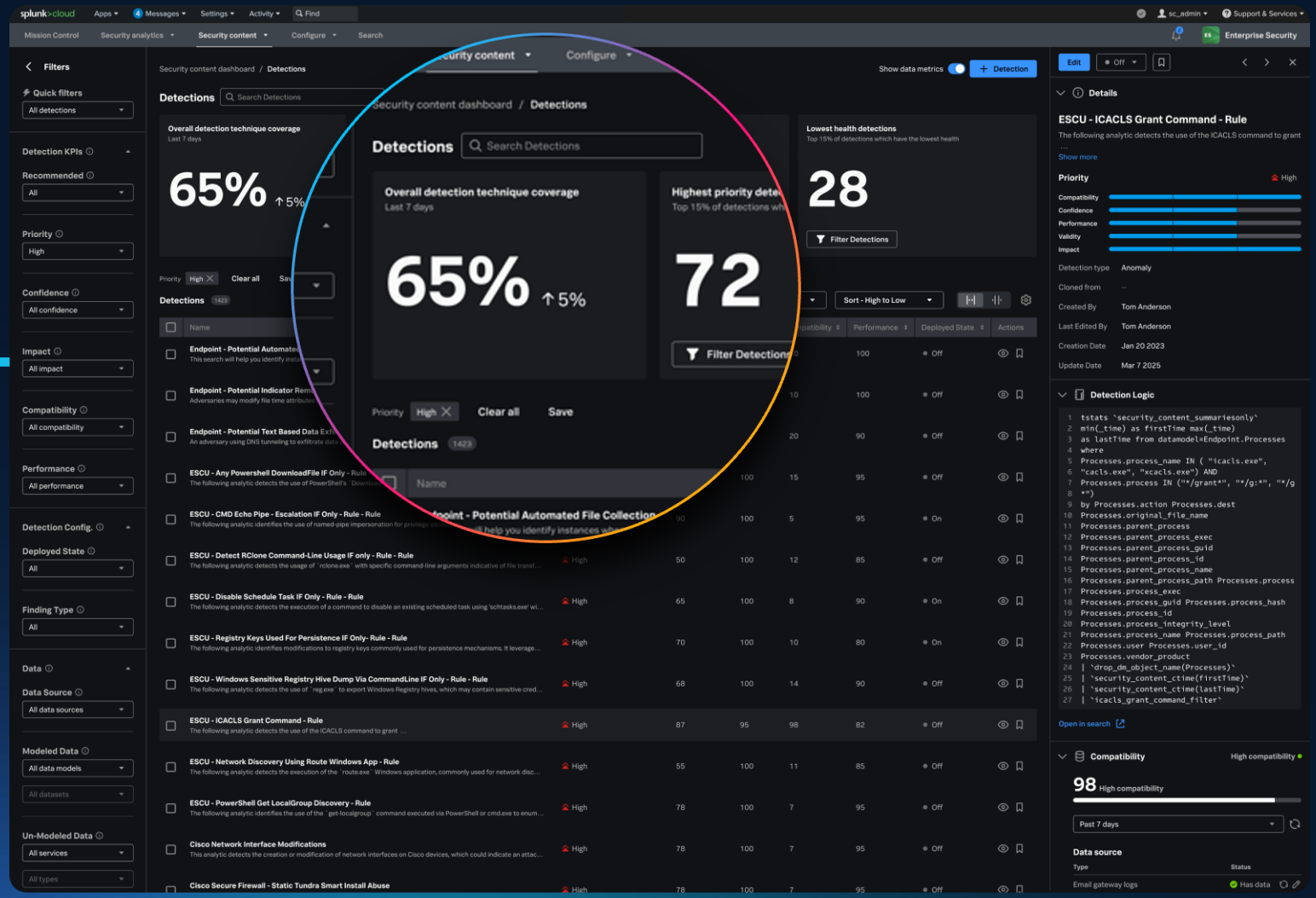
    unlike other solutions Splunk's AI approach to playbook authoring optimizes on accuracy



Detection Studio

Powered by SnapAttack

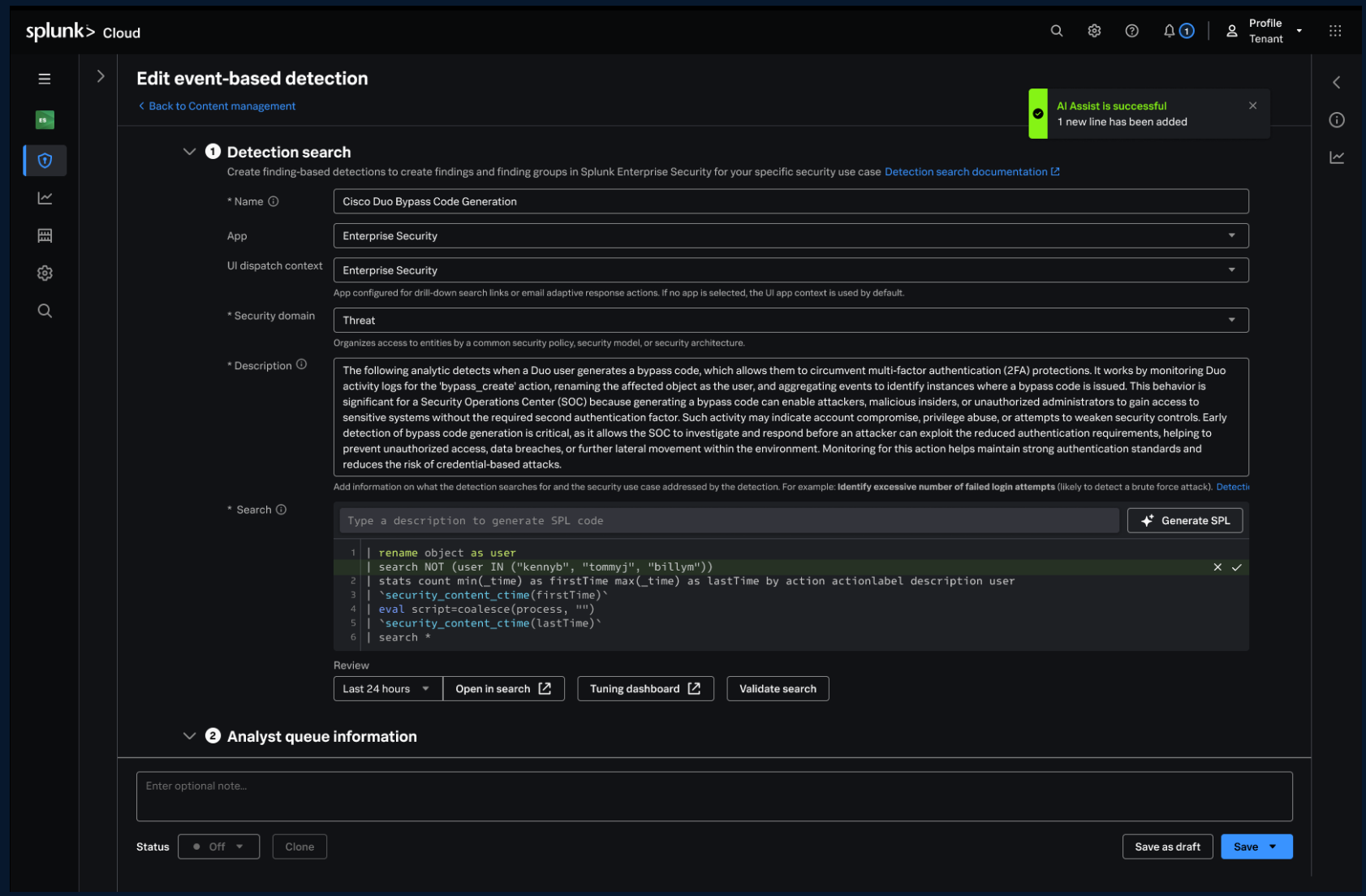
- AI Guided Detection Creation
- Detection Health, Coverage and Effectiveness Visibility
- Detection-as-code lifecycle management



Alpha coming soon

Detection Builder Agent

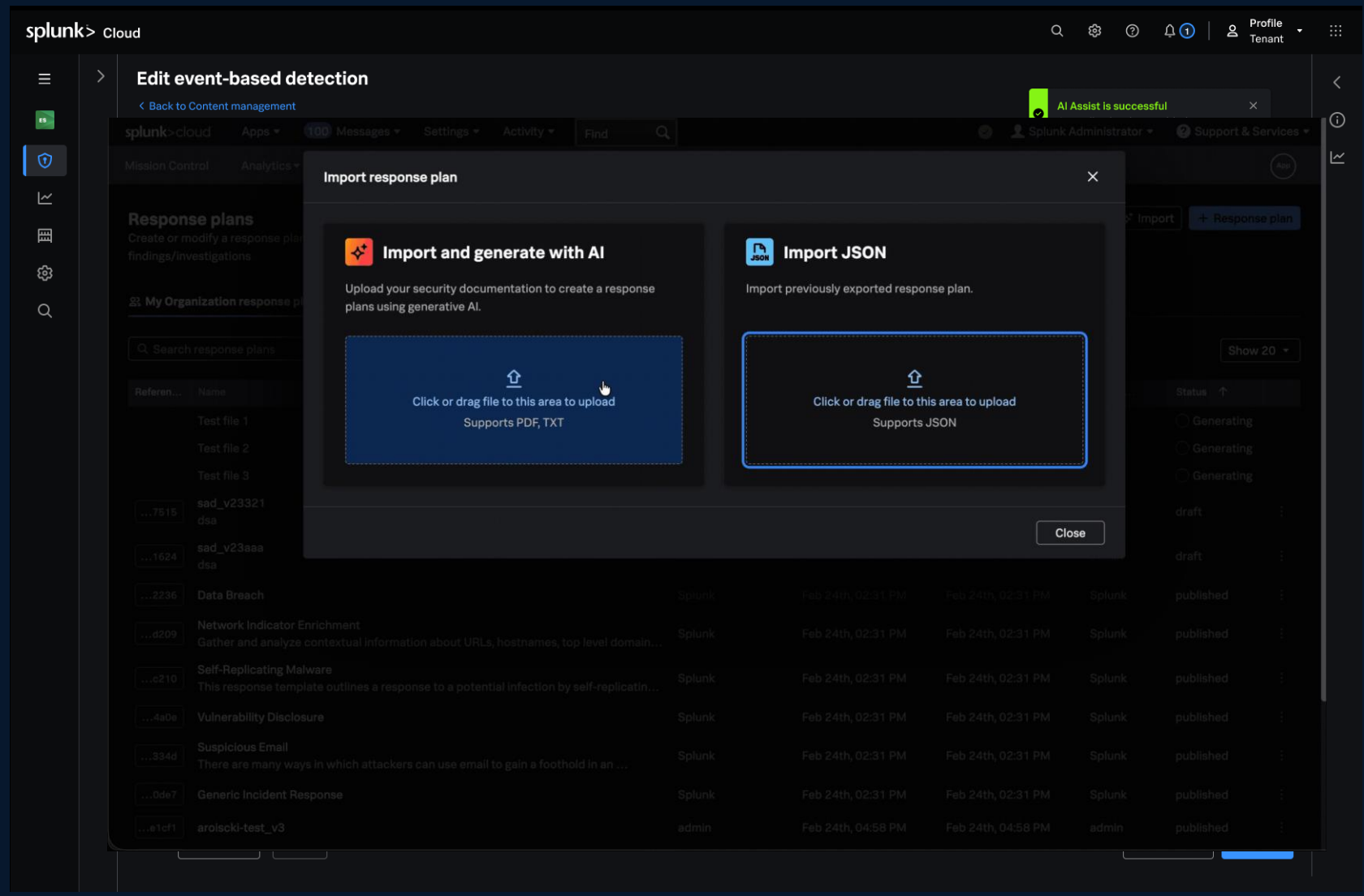
- Go from detection hypothesis to production in minutes with accuracy
- Quickly import, tune, and tag detections
- Personalize detections for your environment.



GA

SOP Agent

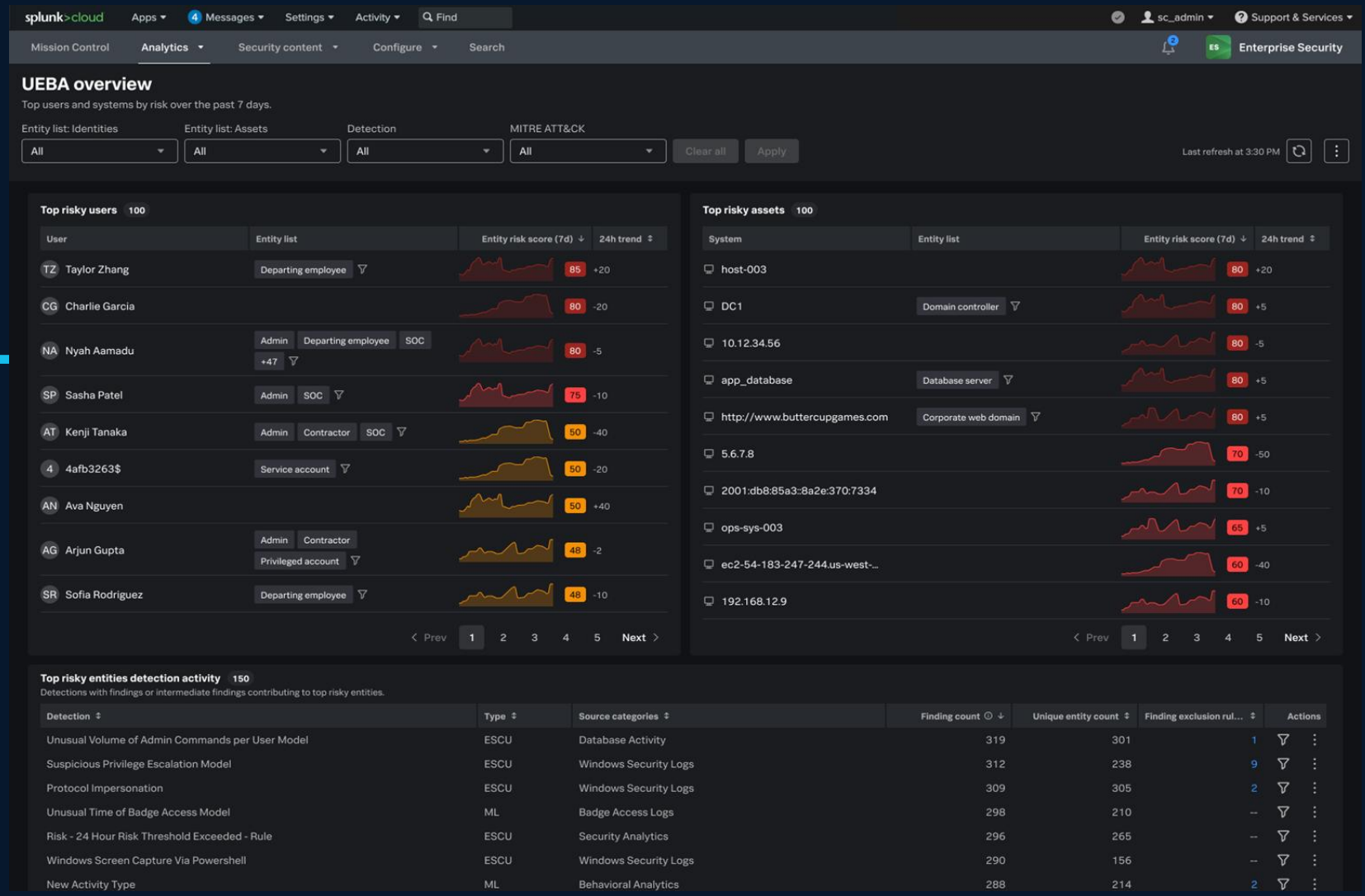
- Import security standard operating procedures into Splunk Enterprise Security response plans so AI agents can act on them.



UEBA

Enterprise Security's UEBA capability

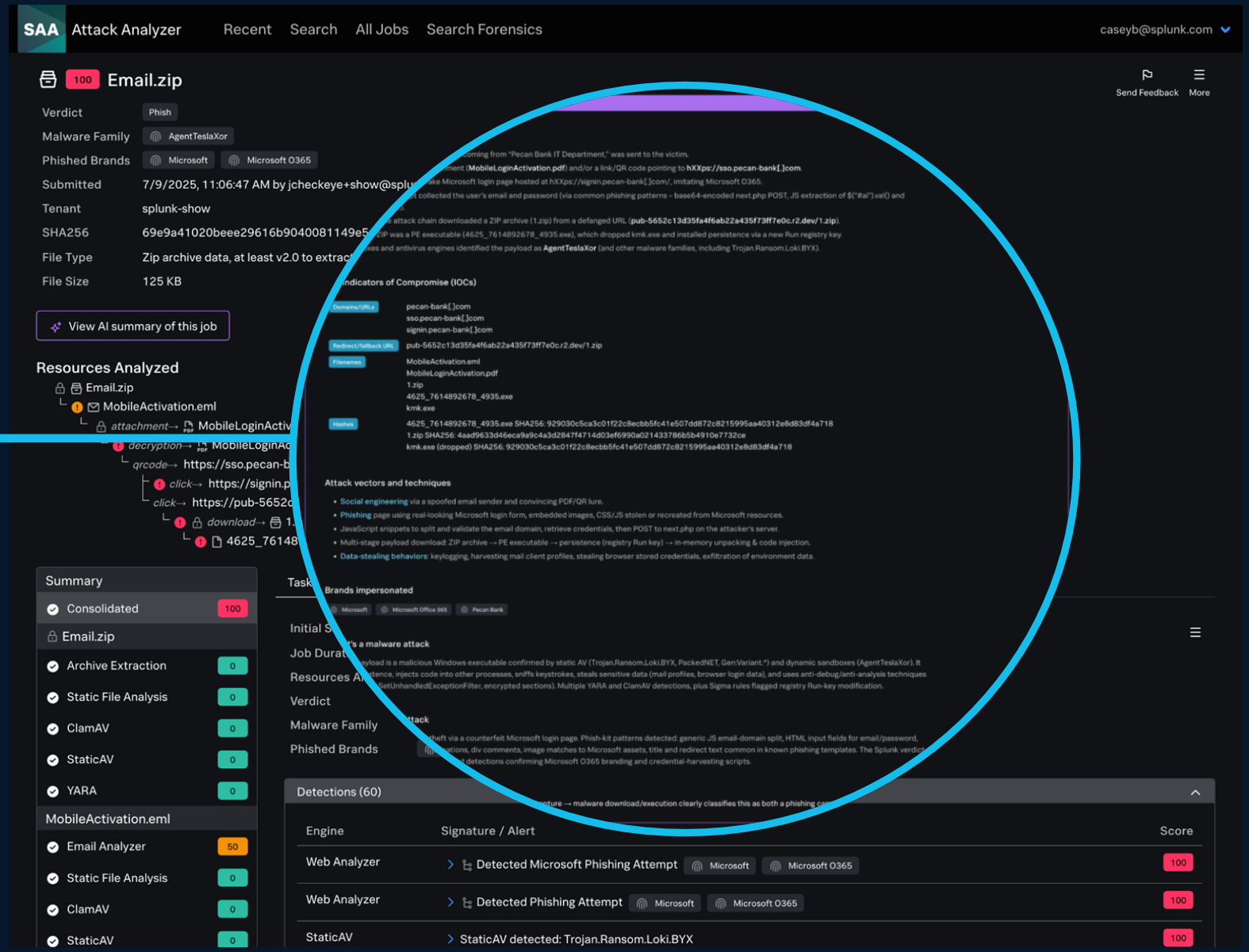
- CMP and Cloud enabled UEBA engines within ES
- Unsupervised AI and ML Behavioral baseline and detection
- Provide rich context for insider threats



GA Now

Malware Threat Reversing Agent

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



The SOC Platform

Operations

- Triage Agent
- AI Assistant
- AI Playbook Authoring
- Detection Studio

TDIR Platform

Detection

- UEBA
- AI Defense
- Malware Threat Reversing Agent
- AI Toolkit

Data

Cisco Data Fabric

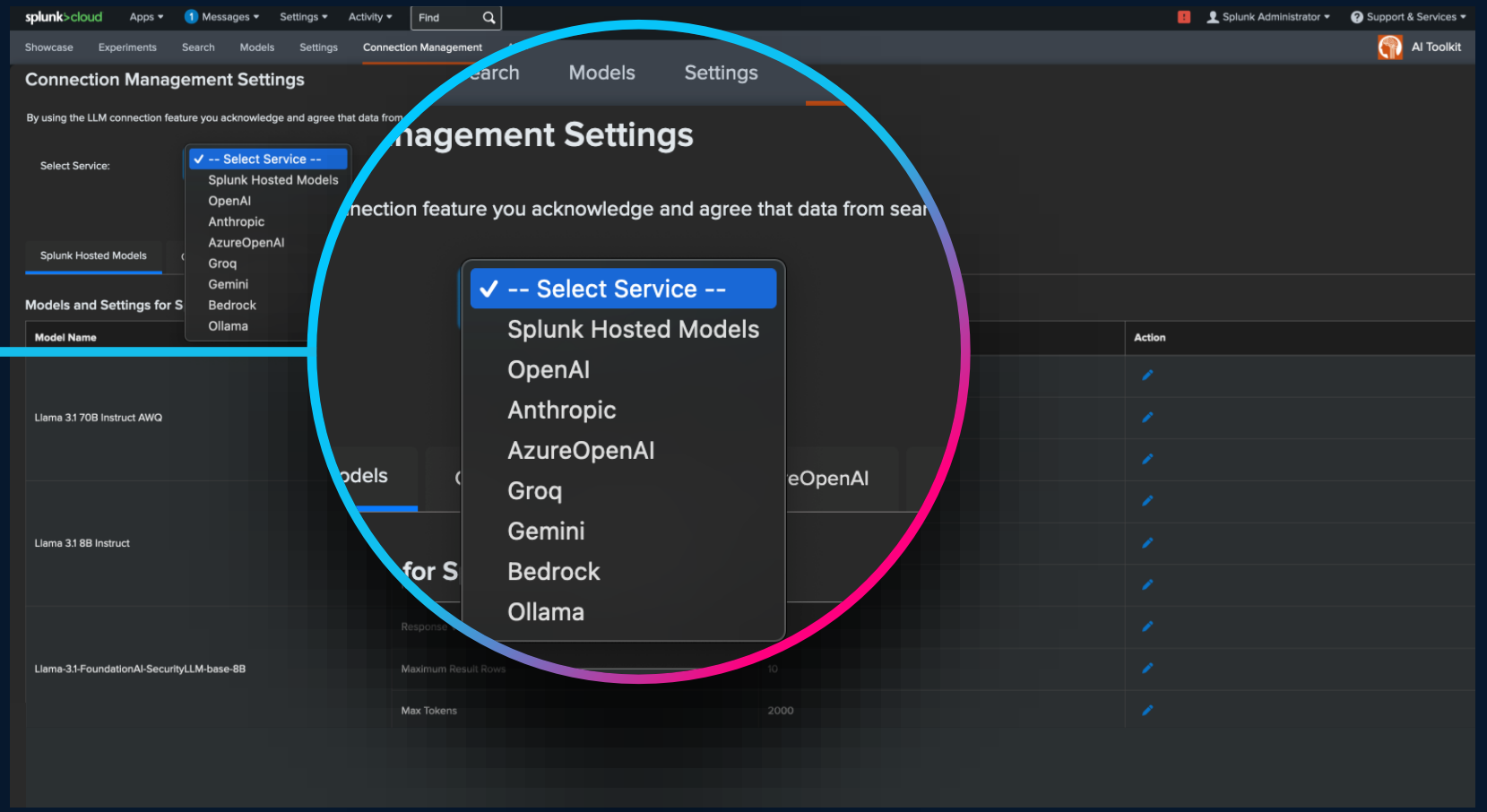
- AI-powered data management
- Federated Search and Analytics
- AI-Native Experiences and Platform for AI
- Machine Data Lake

cisco

Scaling AI Capabilities

Splunk AI Toolkit

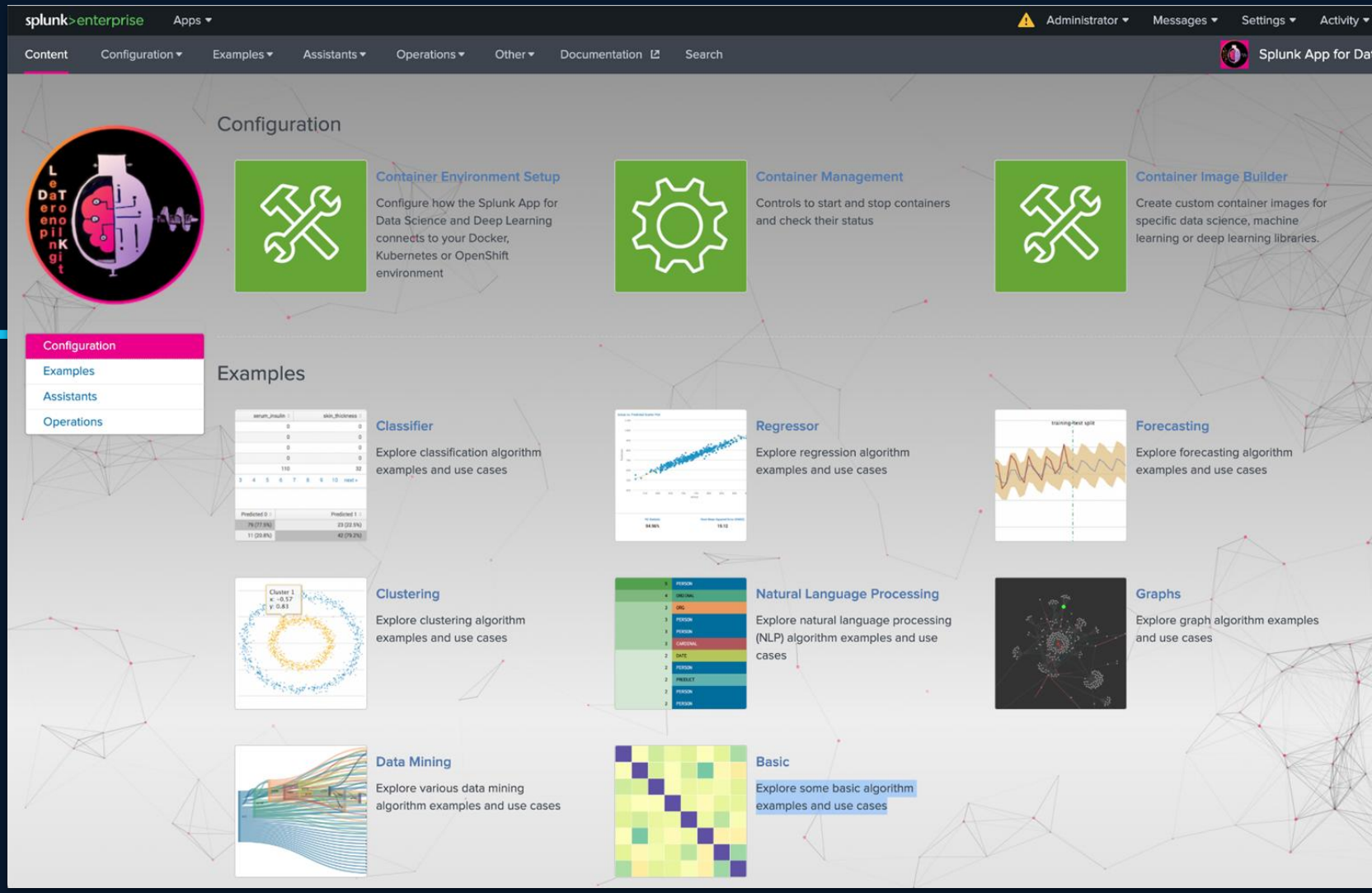
- Build and deploy AI models
- Query Splunk with 3rd party LLMs
- Access Splunk hosted models, coming soon



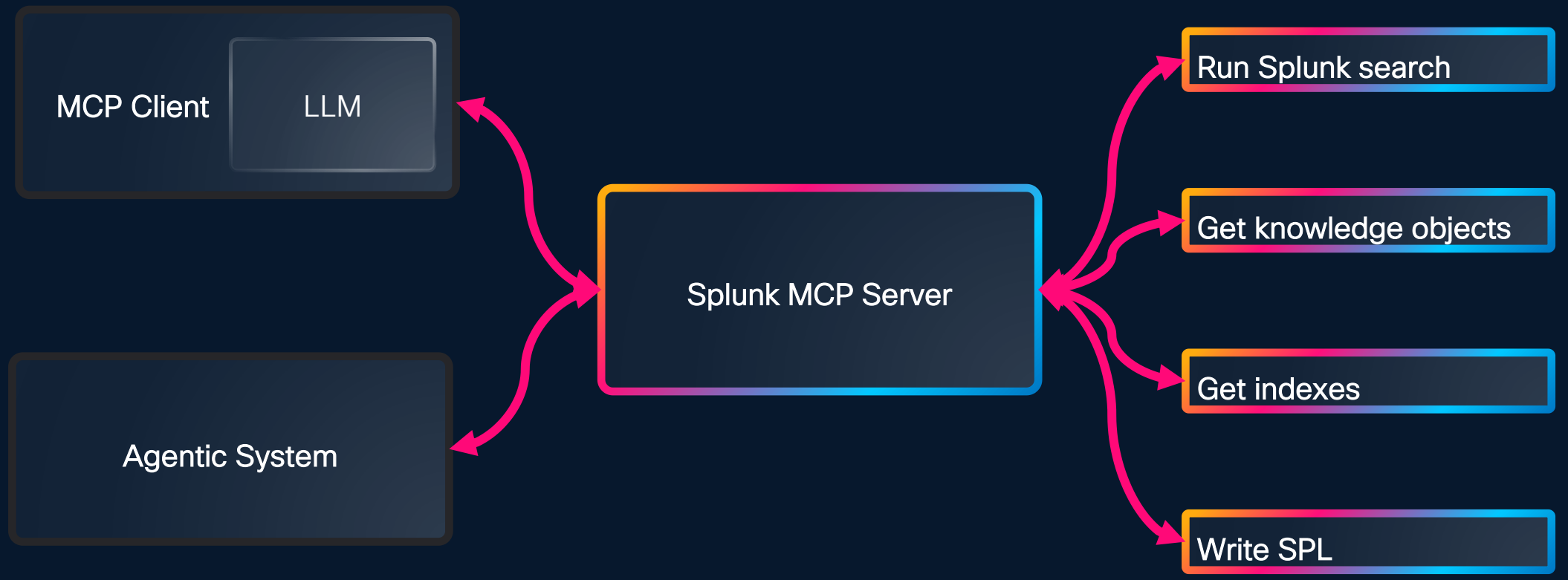
Splunk DSDL

Splunk App for Data Science and Deep Learning

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



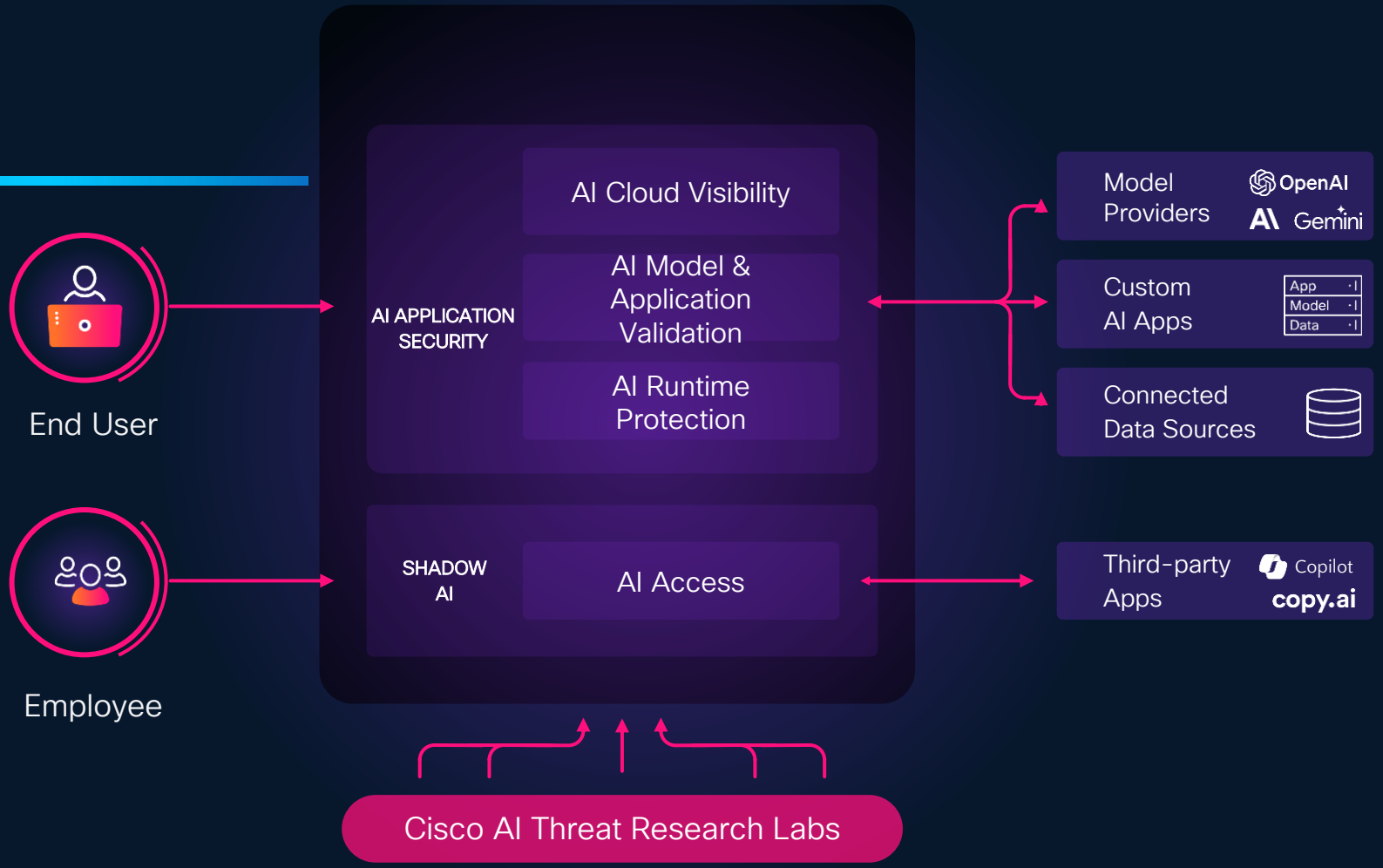
Splunk MCP Server



AI Defense with Cisco

Secure AI applications

Secure AI access



Splunk Enterprise Security + AI Defense

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

Cisco AI Defense

AI Context
Events, Messages, Actions, and Policy names

AI Visibility
Network Connections and Applications

AI Governance
Guardrail entities and Ruleset types

Splunk Enterprise Security

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

CISCO Connect

Thank you


CISCO