CISCO Connect

Powering the SOC of the Future: Next-Gen Security Operations

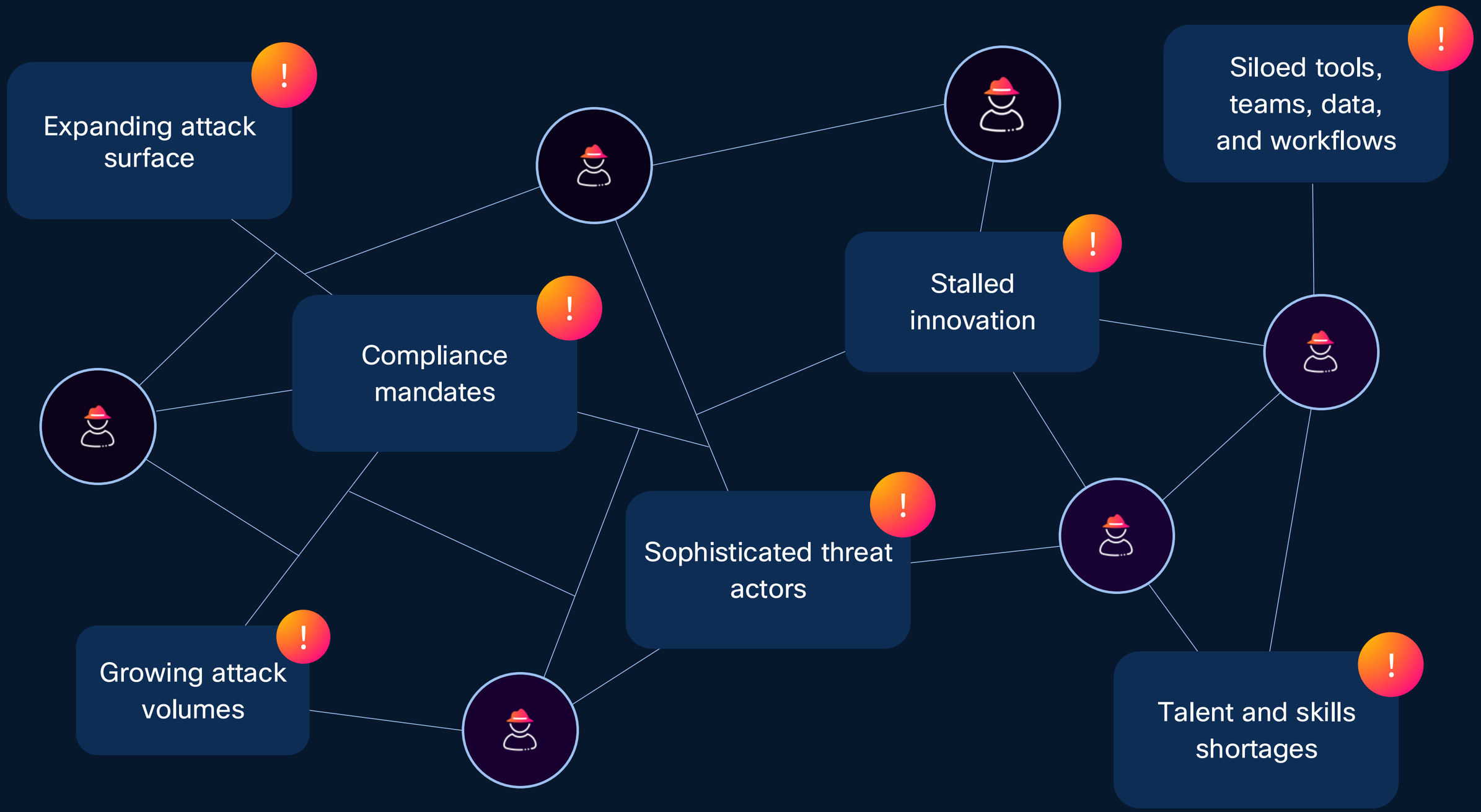
Derrick Lawson, CISSP GMON GCDA, Solutions Engineer

March 24, 2026

Forward-Looking Statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.


Expanding attack surface
Siloed tools, teams, data, and workflows
Compliance mandates
Stalled innovation
Sophisticated threat actors
Growing attack volumes
Talent and skills shortages

LLM01:2025 Prompt Injection

A Prompt Injection Vulnerability occurs when user prompts alter the...

Read More

LLM02:2025 Sensitive Information Disclosure

Sensitive information can affect both the LLM and its application...

Read More

LLM03:2025 Supply Chain

LLM supply chains are susceptible to various vulnerabilities, which can...

Read More

LLM04:2025 Data and Model Poisoning

Data poisoning occurs when pre-training, fine-tuning, or embedding data is...

Read More

LLM05:2025 Improper Output Handling

Improper Output Handling refers specifically to insufficient validation, sanitization, and...

Read More

LLM06:2025 Excessive Agency

An LLM-based system is often granted a degree of agency...

Read More

LLM07:2025 System Prompt Leakage

The system prompt leakage vulnerability in LLMs refers to the...

LLM08:2025 Vector and Embedding Weaknesses

Vectors and embeddings vulnerabilities present

LLM09:2025 Misinformation

Misinformation from LLMs poses a core vulnerability for applications relying...

Read More

LLM10:2025 Unbounded Consumption

Unbounded Consumption refers to the process where a Large Language...

Many SecOps Platforms Fail to Meet the Demands of the Agentic AI Era

Limited Data Storage Options

Closed ecosystem

Partial detection customization

Incomplete TDIR toolset

Opaque AI reasoning

Rigid data ingestion structures

Lack of mature pre-processing capabilities

Limited deployment options

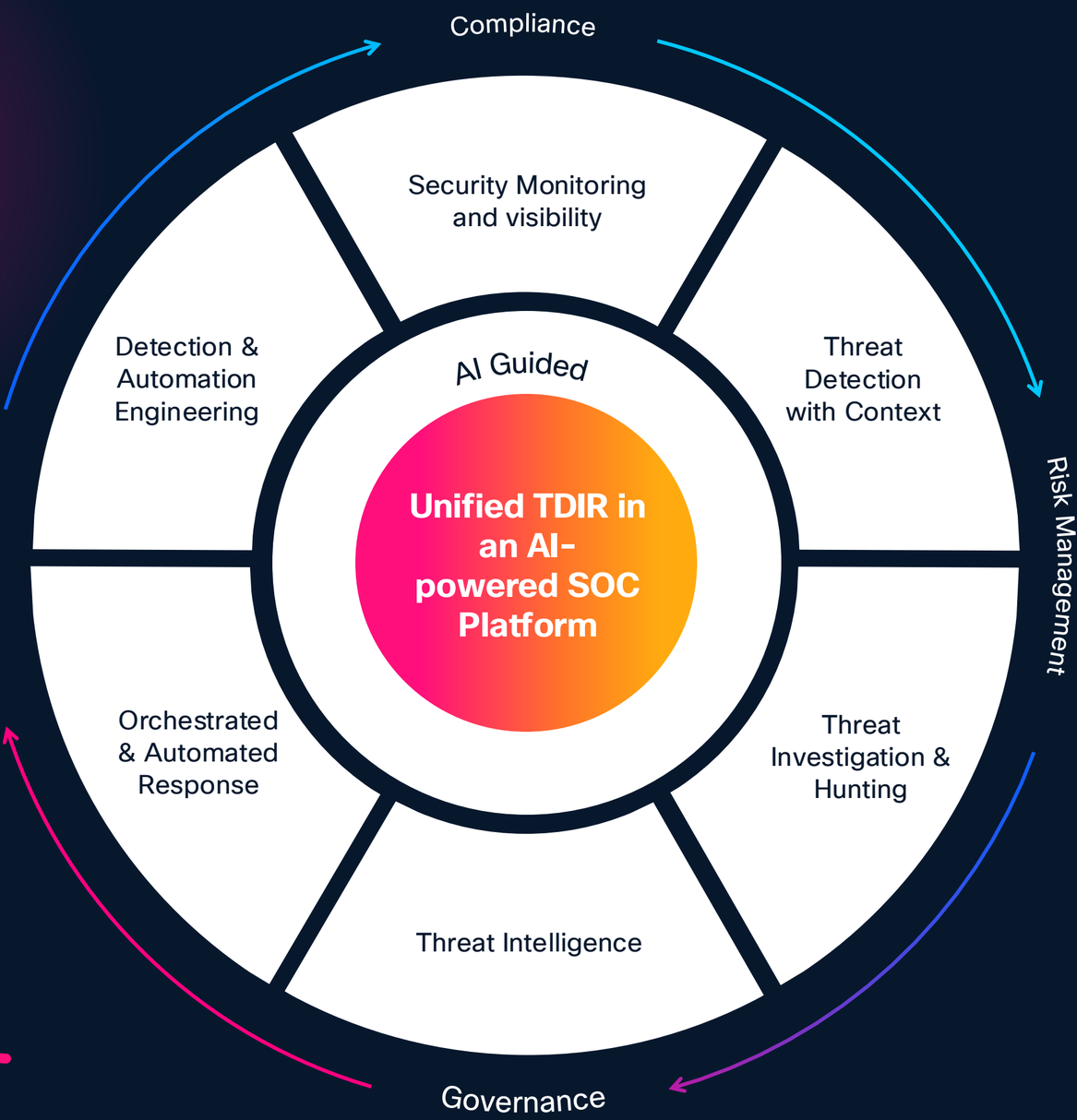
Inability to reduce alert volumes

All or nothing AI

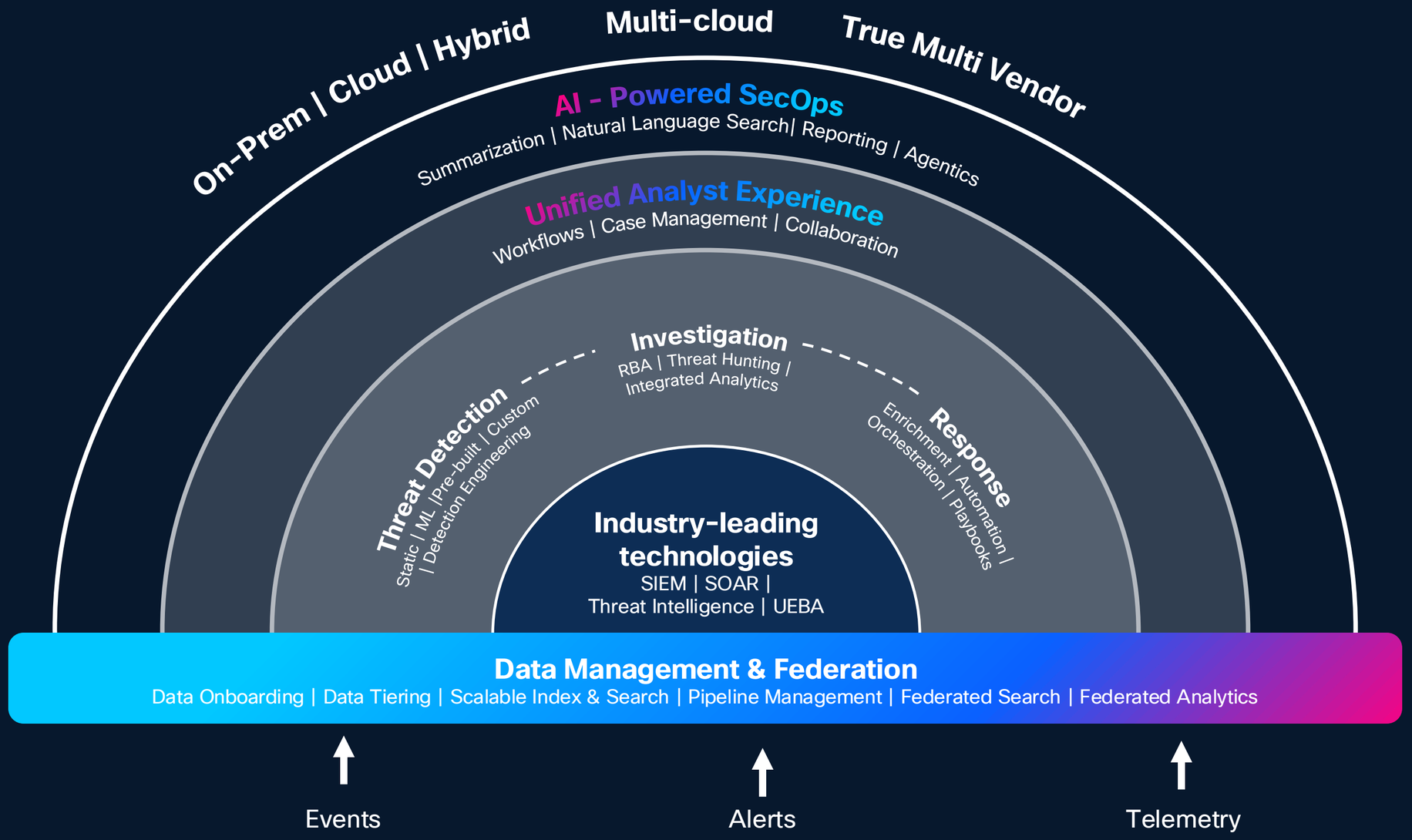
The SOC Reimagined

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

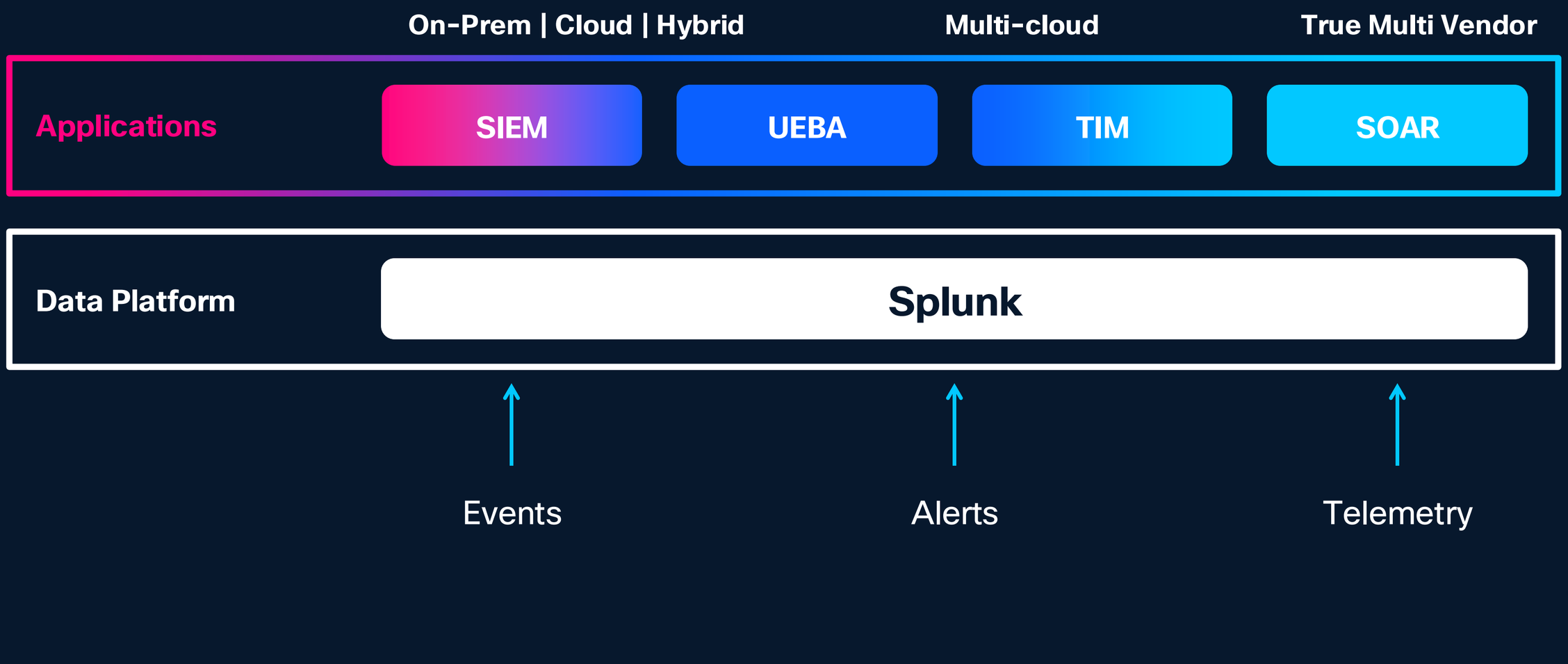
- Focus on the threats that matter most.
- Accelerate detection and response.
- Enable digital resilience for the business.



Splunk Enterprise Security



From Industry-Defining SIEM to the Most Complete SOC Platform



One SecOps Platform, Available in Two Editions

Use Case	Essentials Edition	Premier Edition
 Security Monitoring	Get a unified view across all environments for clearer threat visibility and faster, data-driven response	
 Threat Detection	Tackle unknown and known threats with a range of detections (correlations, rule-based, AI/ML, and custom)	**Elevate Threat Detection with AI** to easily understand and fine tune detection rules*
 Threat Investigation	Leverage the unified Mission Control interface to rapidly analyze, identify and investigate threats for an effective response	Accelerate investigation through **automated playbooks** and amplify human expertise with the **Triage Agent*** to automatically enriches alerts with more context.
 Threat Hunting	Use findings and searches to identify malicious activity and mitigate attacks before they escalate	Enhance threat hunting by leveraging **UEBA's ML-driven behavioral insights** and accelerate evidence gathering and response with **1-click automated runbooks**
 Automation	Use one time Adaptive Response actions for basic orchestration or integrate with a SOAR product for full spectrum automation	Accelerate response time, minimize human error, and ensure consistent enforcement of security policies. **Available OOTB for every person in the SOC**
 Insider Threat Detection	Requires manual implementation or integration with a separate product	Mitigate insider threat in real time using : **OOTB, proven, and scalable ML models, fully integrated in investigation workflows**

*In Alpha

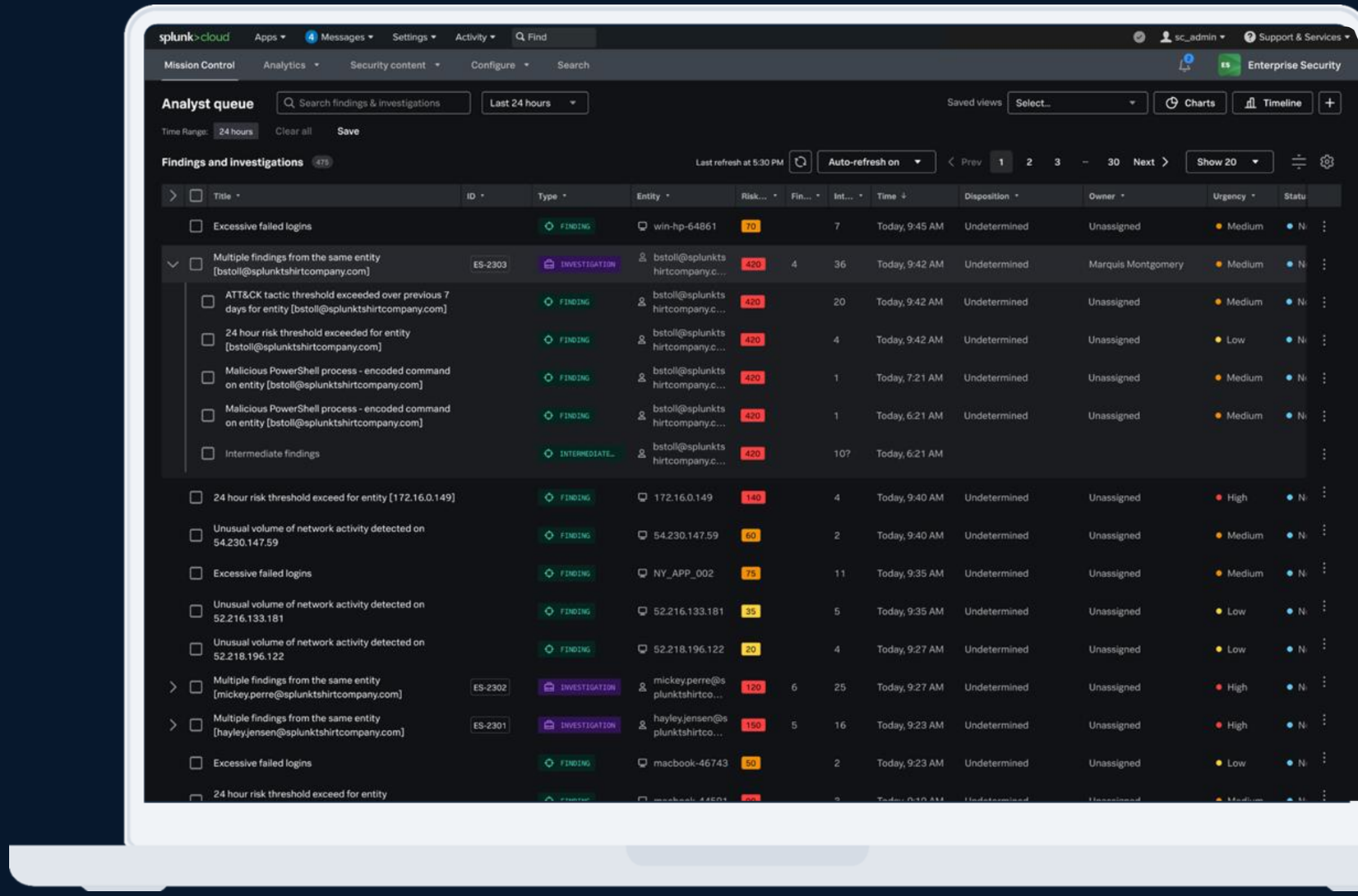
Unlock Full Fidelity Visibility

Make sense of all data and enable fast action

- Ingest, federate, and normalize **data from any source**, cloud, or OT for unified visibility.
- Optimize data routing, filtering, and storage to **control costs and maintain full access** for compliance and analysis.
- Enrich every alert **with integrated Cisco Talos and Splunk threat intelligence** for faster, more precise triage.
- Stay ahead with **world-class detections**—rule-based, AI-driven, and custom—continuously updated and mapped to MITRE ATT&CK.

New

- Deploy, test, and monitor detections faster with **Detection Studio***, enabling seamless coverage and quick gap closure.
- **Proactively address risk with RBA**, correlating weak signals, reducing false positives, and accelerating triage.

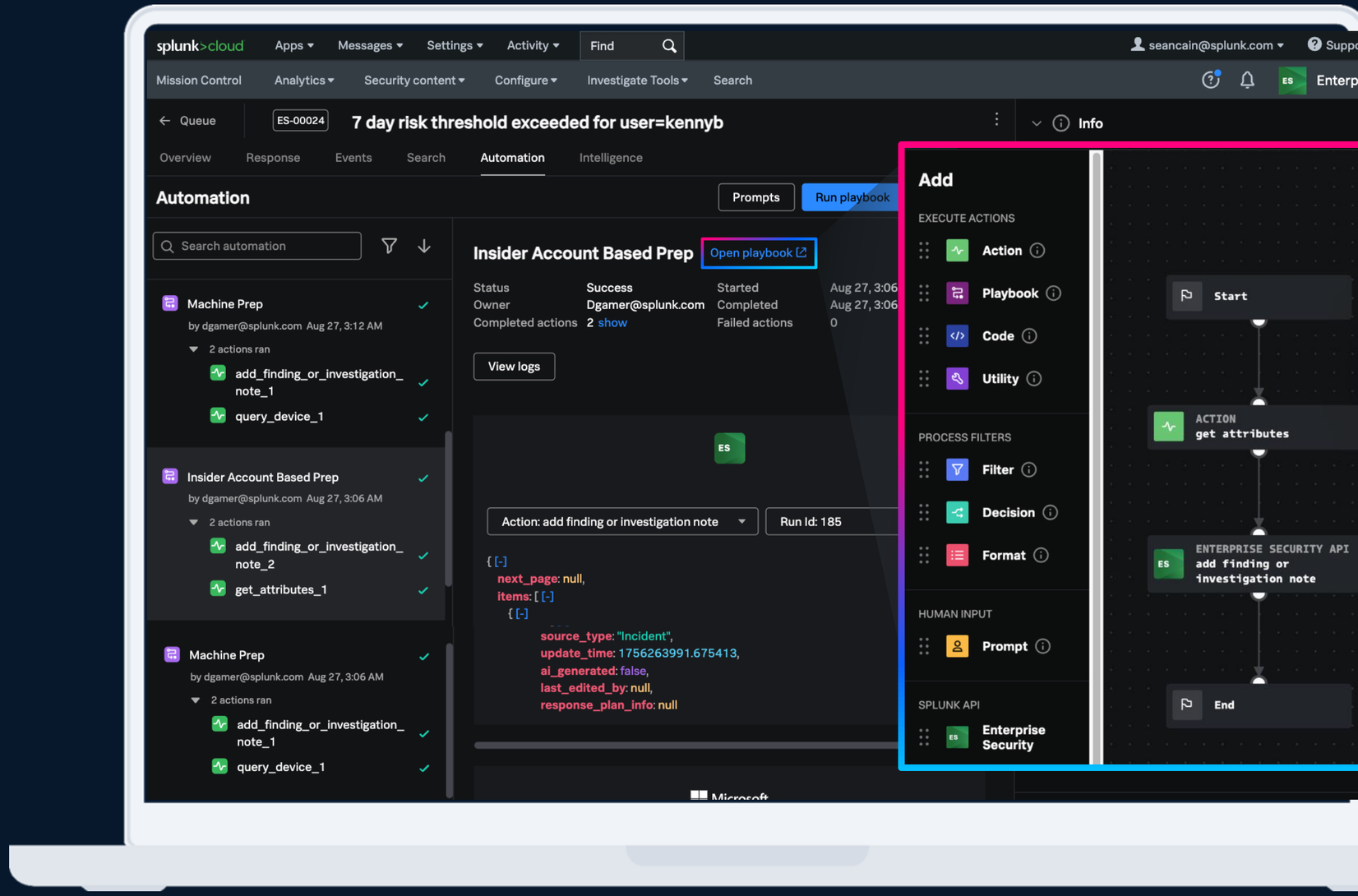


*In Alpha

Deliver the Best Analyst Experience

Unify threat detection, investigation and response (TDIR) workflows

- New **Get integrated, end-to-end TDIR workflows** with native SIEM, SOAR, UEBA, and threat intelligence for faster value and a unified analyst experience.
- New **Empower every analyst with embedded SOAR*** and case management to standardize playbooks, cut errors, and automate triage and response.
- New **Detect and mitigate insider threats with UEBA***, which baselines activity and elevates risky behaviors for rapid, confident action.



*In controlled availability

Accelerate the SOC

Use built-in AI and Agentics across every layer

Triage and Investigation

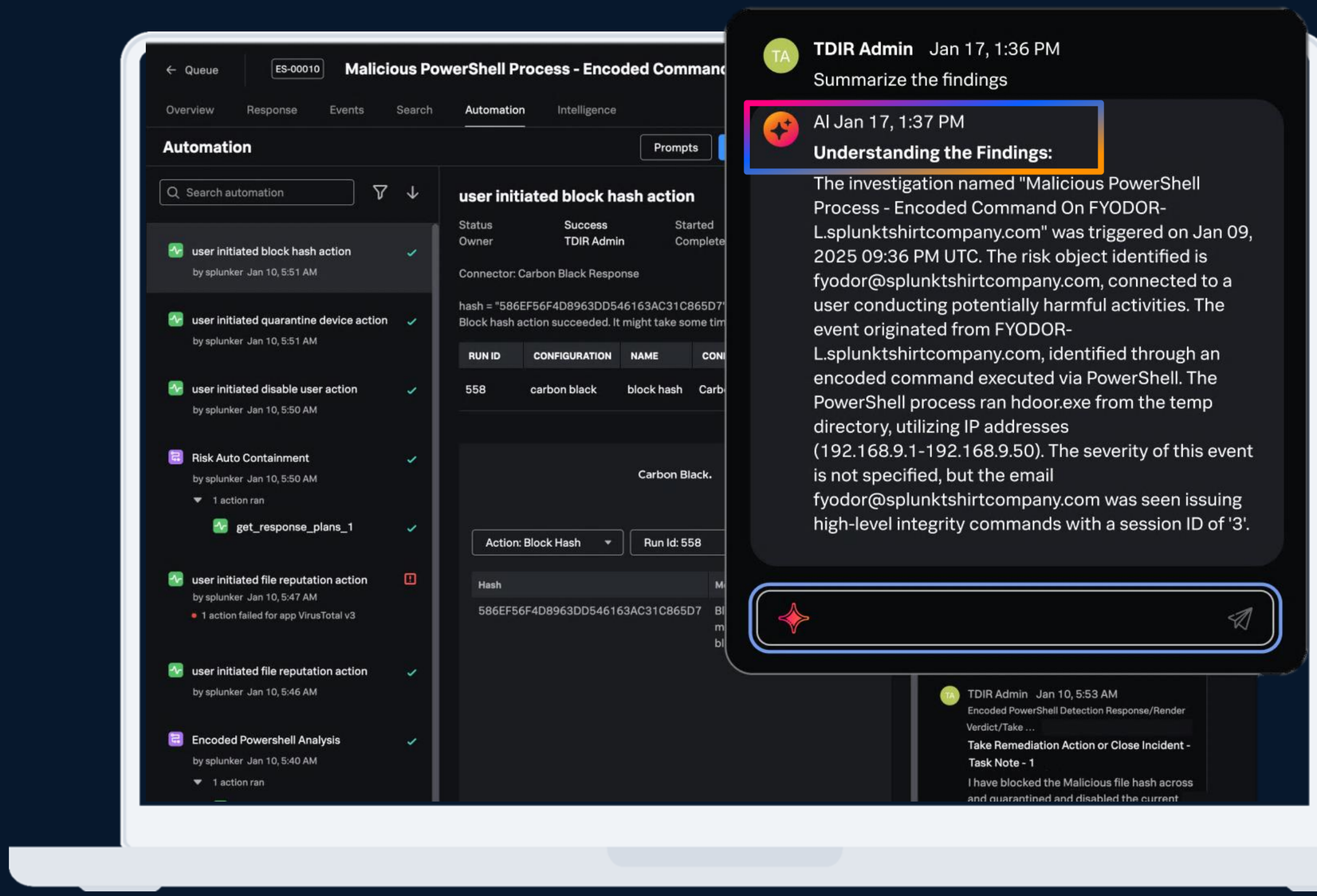
CA
- Use **AI Assistants*** to generate SPL queries, summarize findings, and provide investigation and remediation guidance from natural language.

Alpha
- Let **Triage Agents**** evaluate, prioritize, and explain alerts, reducing workload and highlighting critical issues.

Automation and Response

Alpha
- Accelerate automation with **AI Playbook Authoring**** that turns plain language into tested SOAR playbooks—no deep VPE expertise needed.

Alpha
- Rely on **Autonomous Response Agents**** to execute response actions in security tools based on set instructions.



* In Controlled Availability
**In Alpha

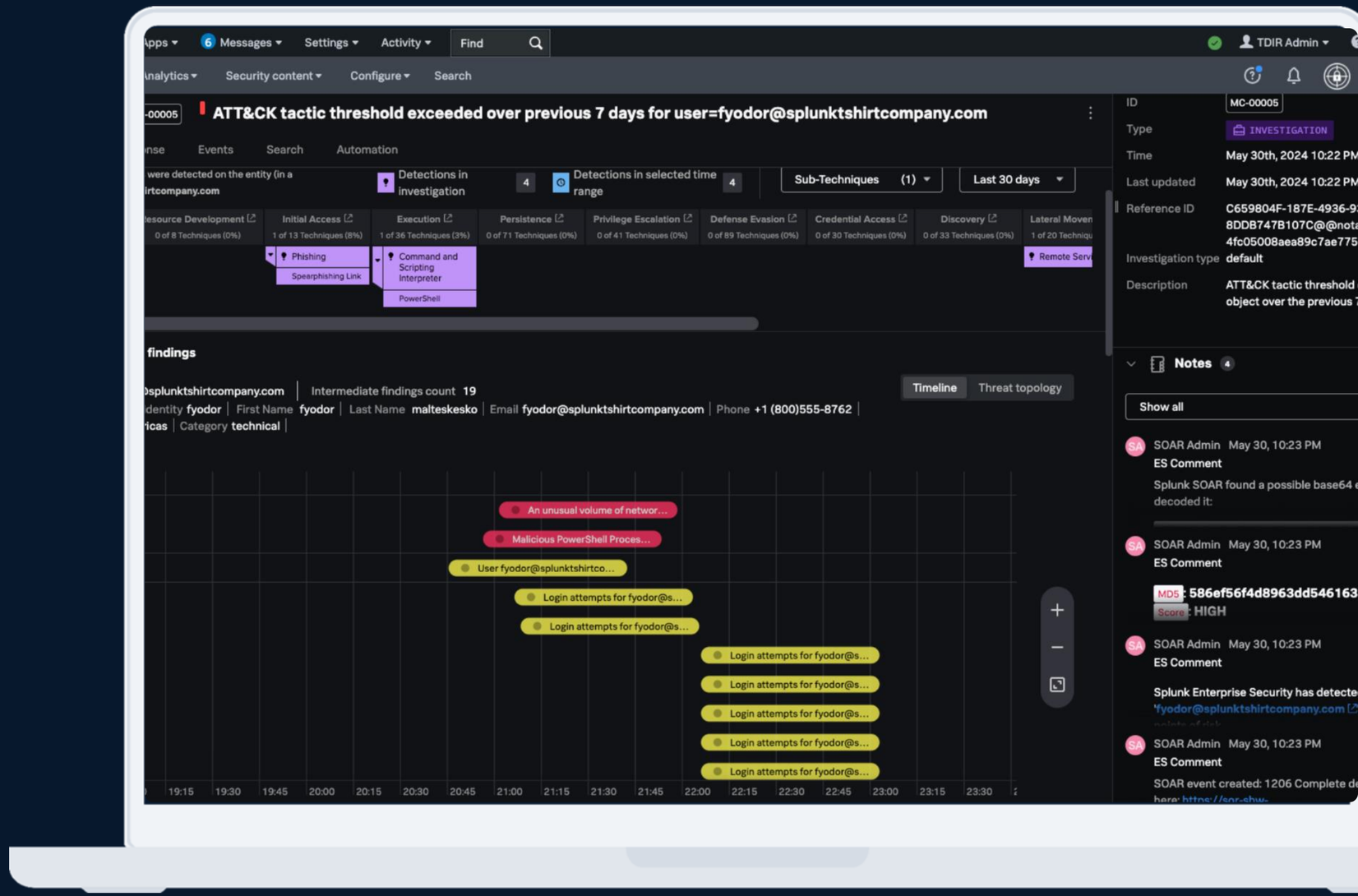
Demo

Highlights

Empower Accurate Detection with Context

Streamline investigations and increase productivity

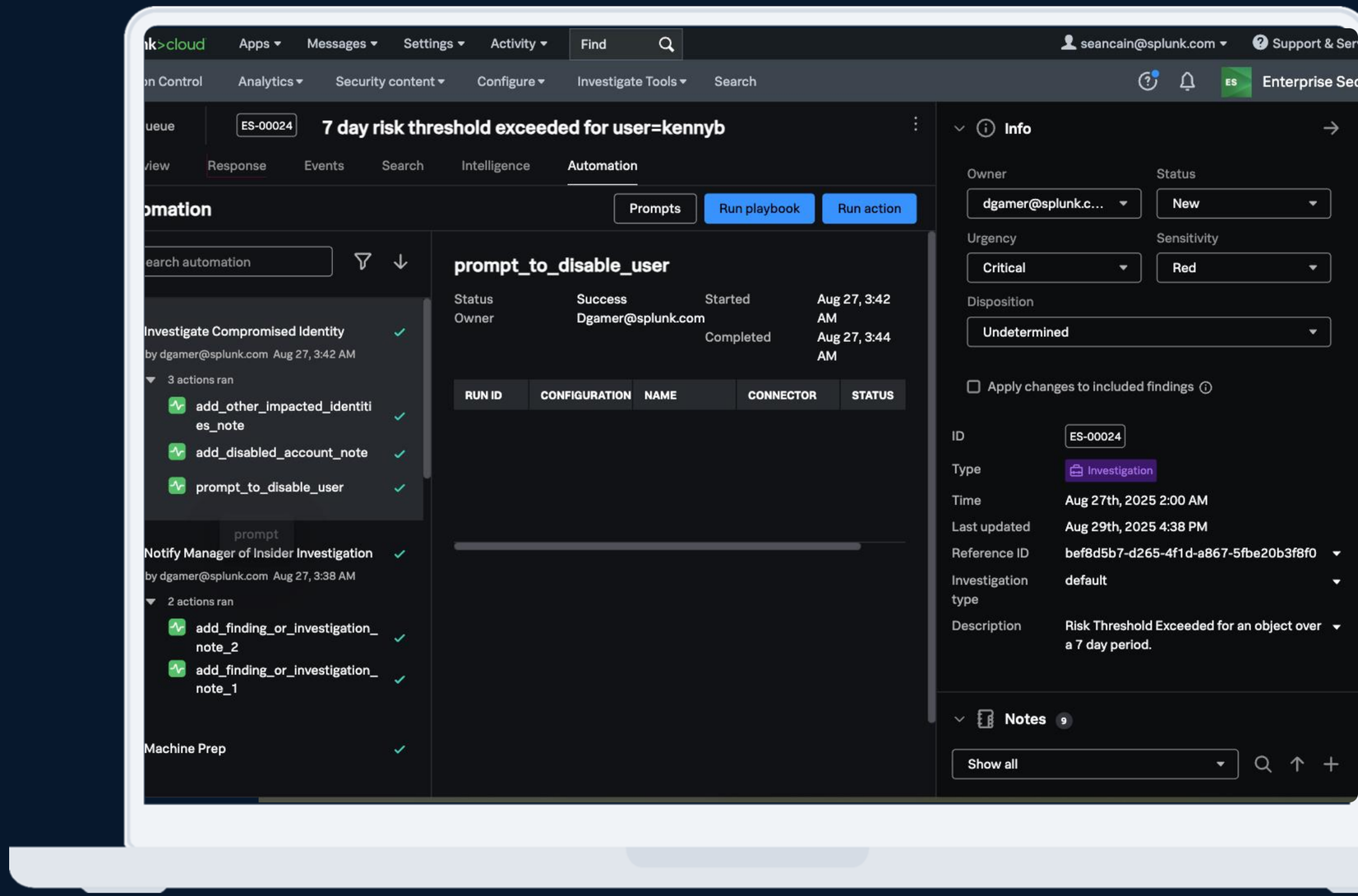
- Drastically reduce alert volumes by up to 90% with risk-based alerting.
- **New** Preview and directly test detections to prevent disruptions to analyst workflows
- **New** Audit capabilities for when detections are enabled or disabled with complete history of changes.
- **New** Enhancements to Finding-based Detections* for a more customizable experience to reduce alert fatigue and time spent on investigations.



*Feature now in Beta

Seamlessly Orchestrate Across the Security Fabric

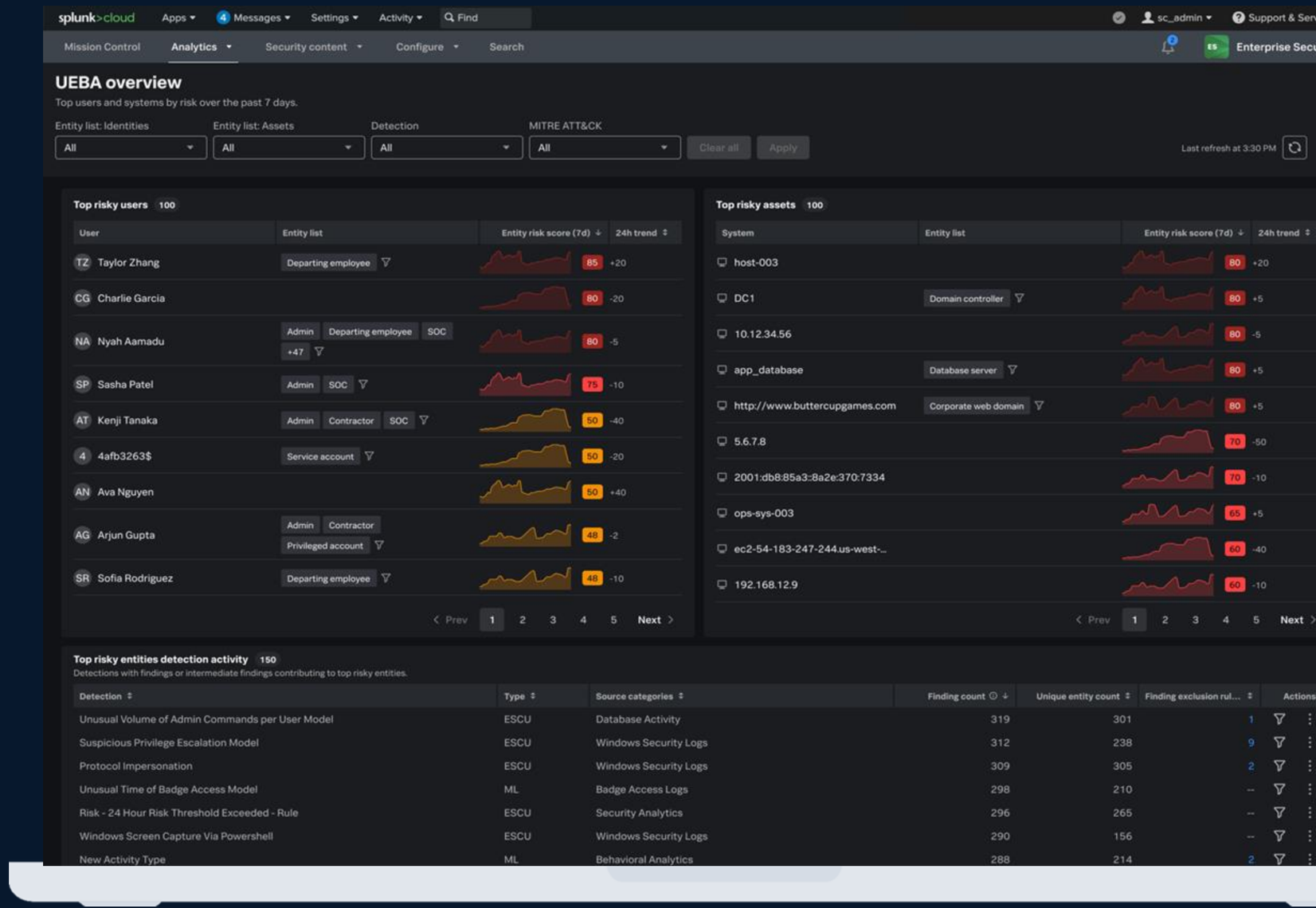
- **Automate with ease** and conquer complex workflows with a variety of prebuilt and customizable playbooks
- **Respond with threat context** based on key input parameters and automate a series of actions to respond to common threats
- **Foster collaborative investigations** with case management and workbook functions to help keep your team informed at all times



See it in action

Proactively Detect and Mitigate Insider Threats & Advanced Threats

- 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.

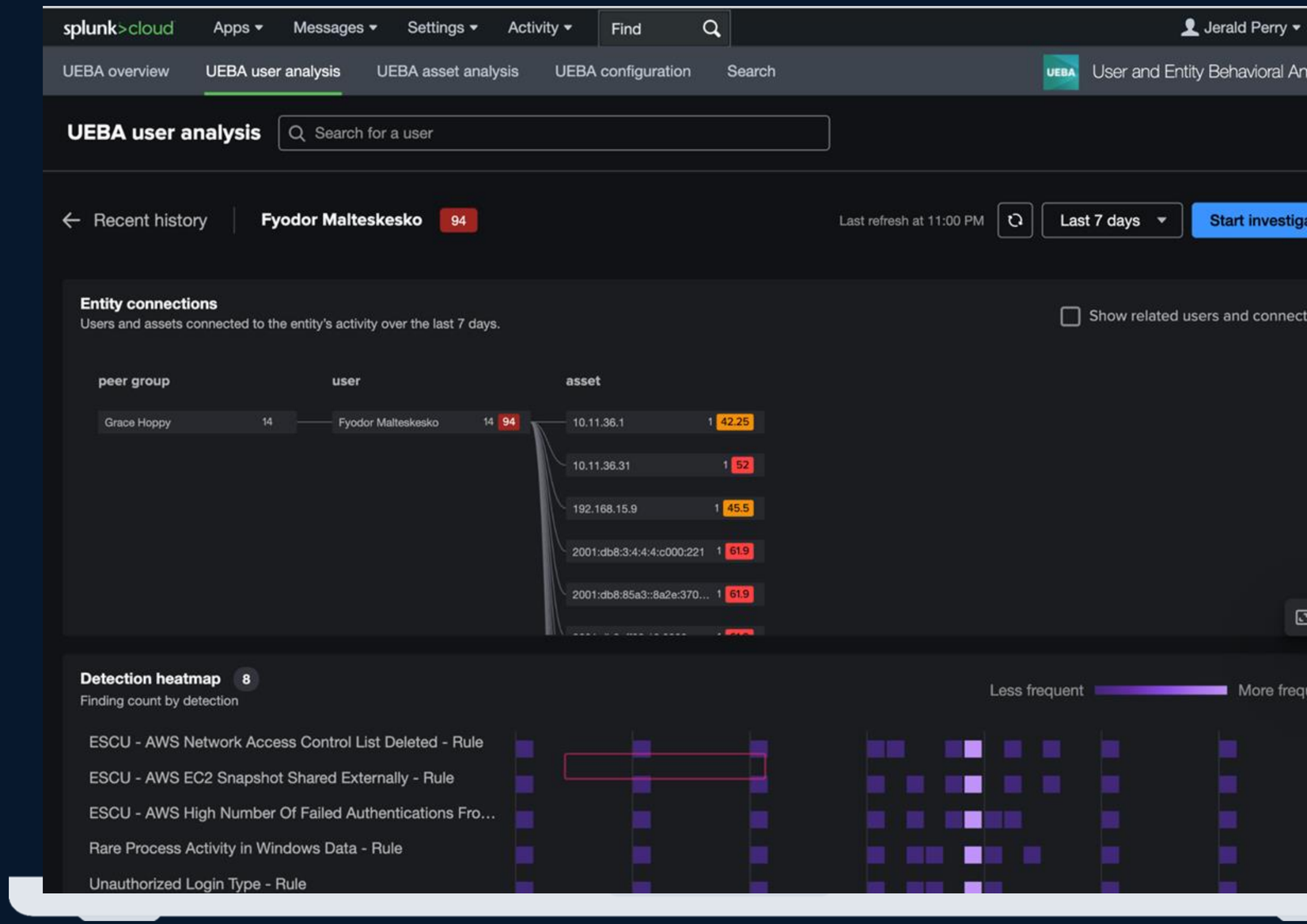


See it in action

Optimize SOC Efficiency with Automated Threat Detection and Prioritization

- A native capability within ES Premier that allows you to detect advanced insider threats, compromised accounts, and behavioral anomalies using machine learning
- Gain holistic risk insights across users, devices, and applications through detailed user and entity risk insights
- Streamline SOC workflows for efficient investigations and faster threat mitigation, reducing alert noise and allowing your analysts to focus their attention on high-priority threats

See it in action



Alpha coming soon

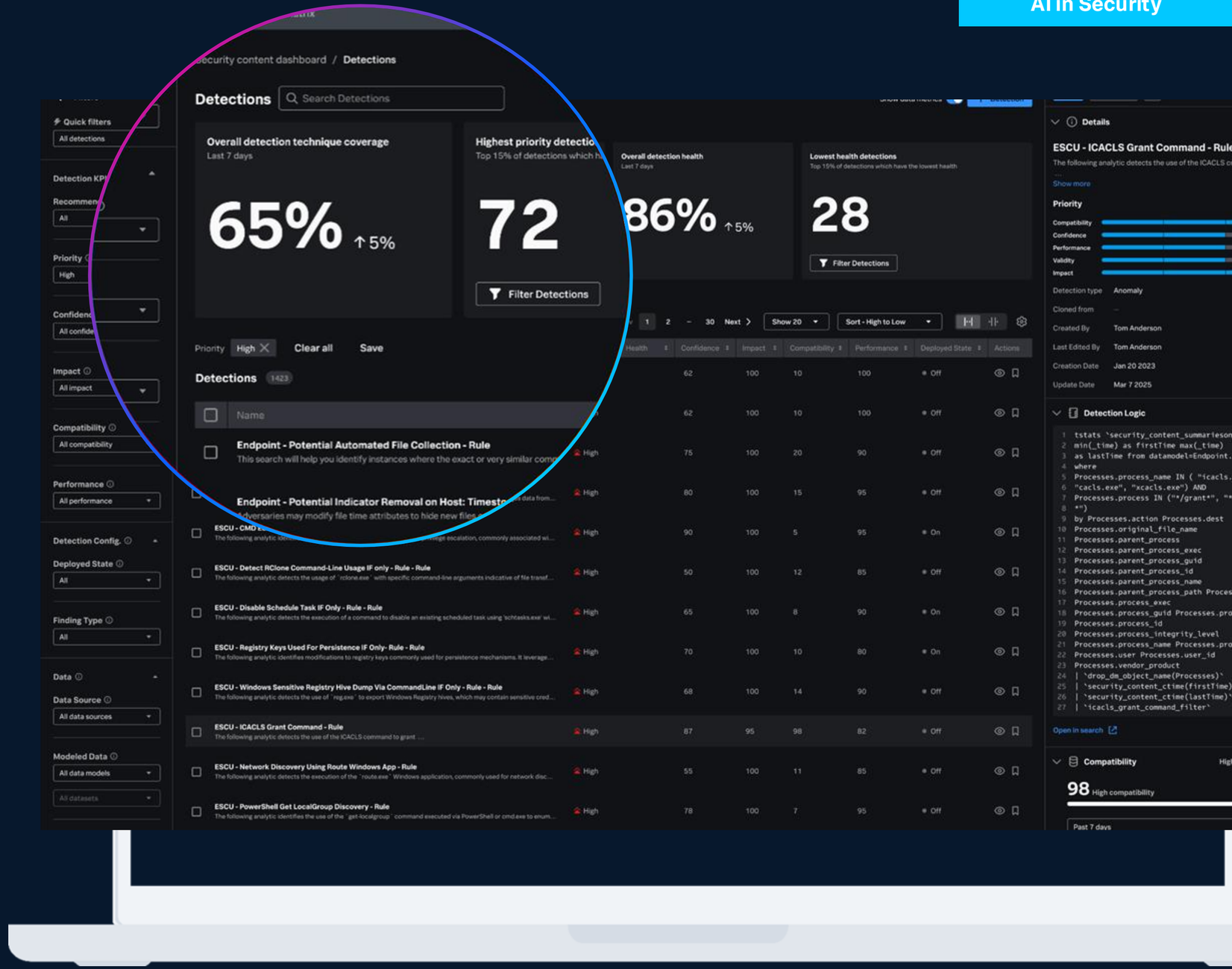
AI in Security

AI-Enhanced Detection Library

From hypothesis to production in minutes

- Iterate on detections
- Expand attack surface coverage
- Prioritize risks and actions

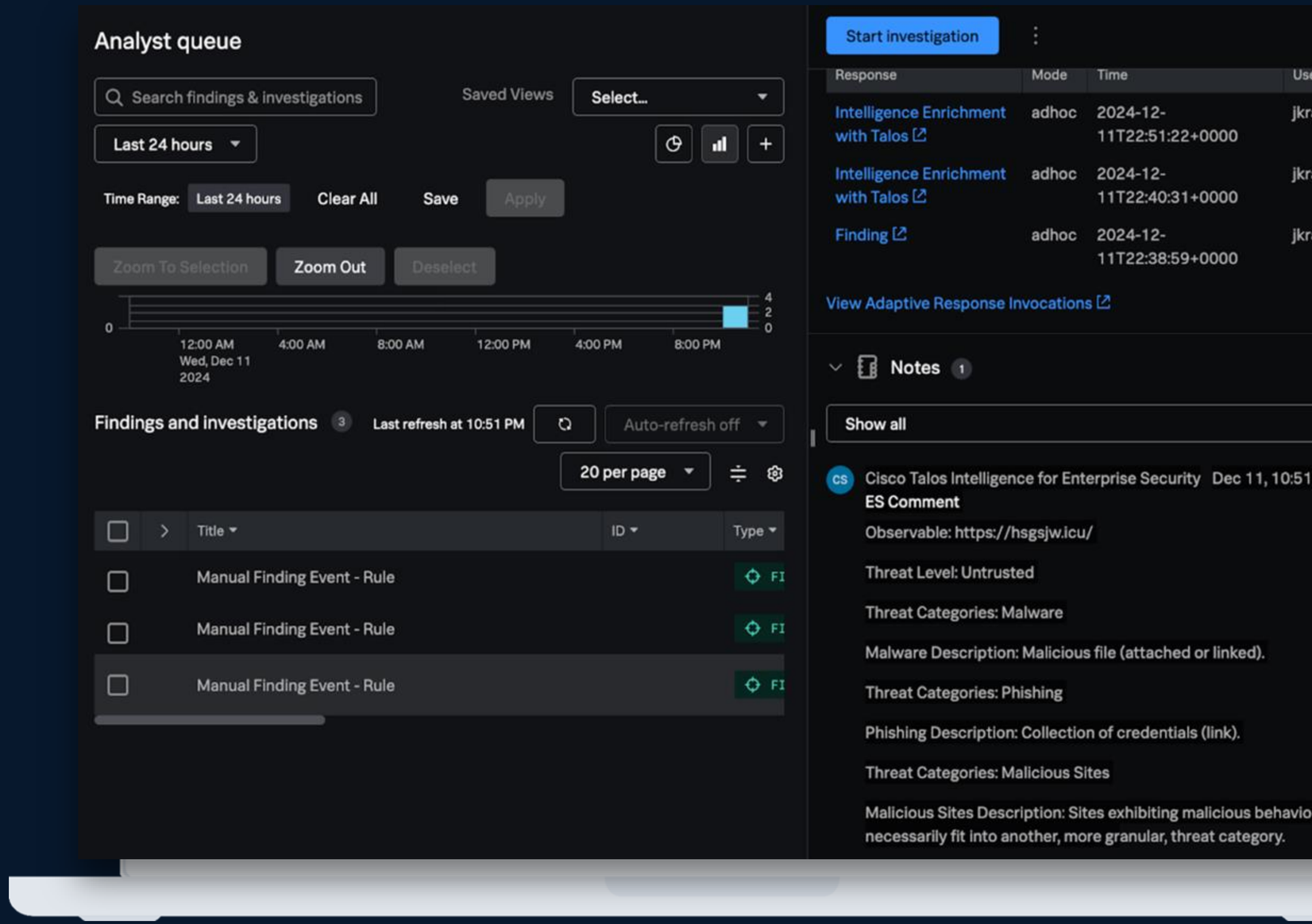
See it in action



Cisco Talos Intelligence for Enterprise Security

- App available for all Enterprise Security cloud customers
- Enrich findings with relevant intelligence from Cisco Talos
- Helps analysts quickly understand potential threats

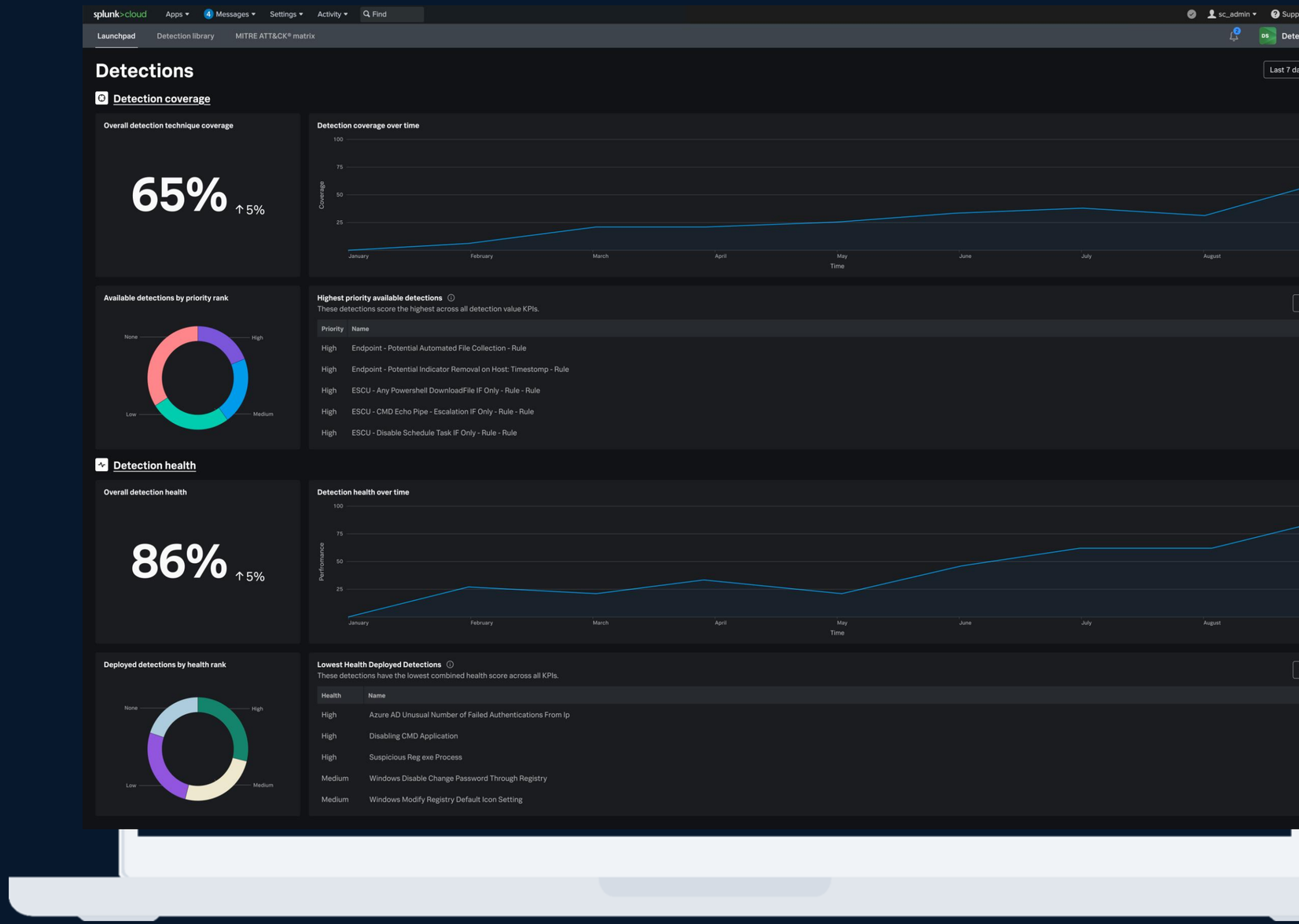
See it in action



Detection Studio*

The Complete Detection Lifecycle Experience

- Efficiently discover and deploy quality detections
- Seamlessly Contextualize Detection Coverage aligned to MITRE ATT&CK Framework



Manage SOC Data Your Way

Flexibility to manage, find and analyze actionable data in your SOC.

Filter and transform data at the Edge or in the Cloud prior to any indexing in Splunk.

Public Cloud | Private Cloud | On Premises

Data management

Filtering, Redacting & Routing

Bring search and analytics to external stores without ingestion.

Amazon S3 | Amazon Security Lake | Additional Data Lakes

Federation

Search & Analytics

Data normalization

CIM, OCSF

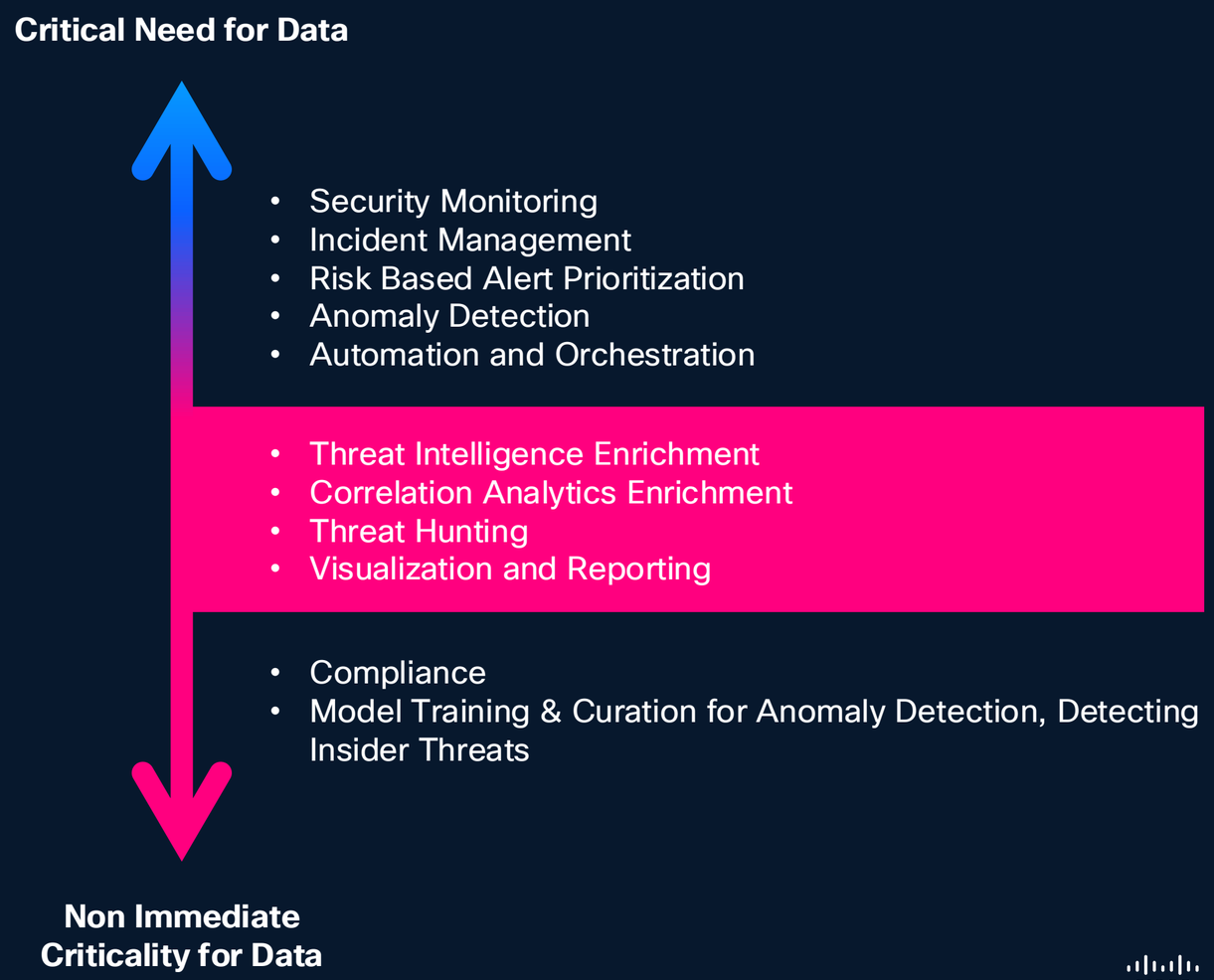
Splunk Enterprise Security

cisco

Optimize Data and Maximize Security Value

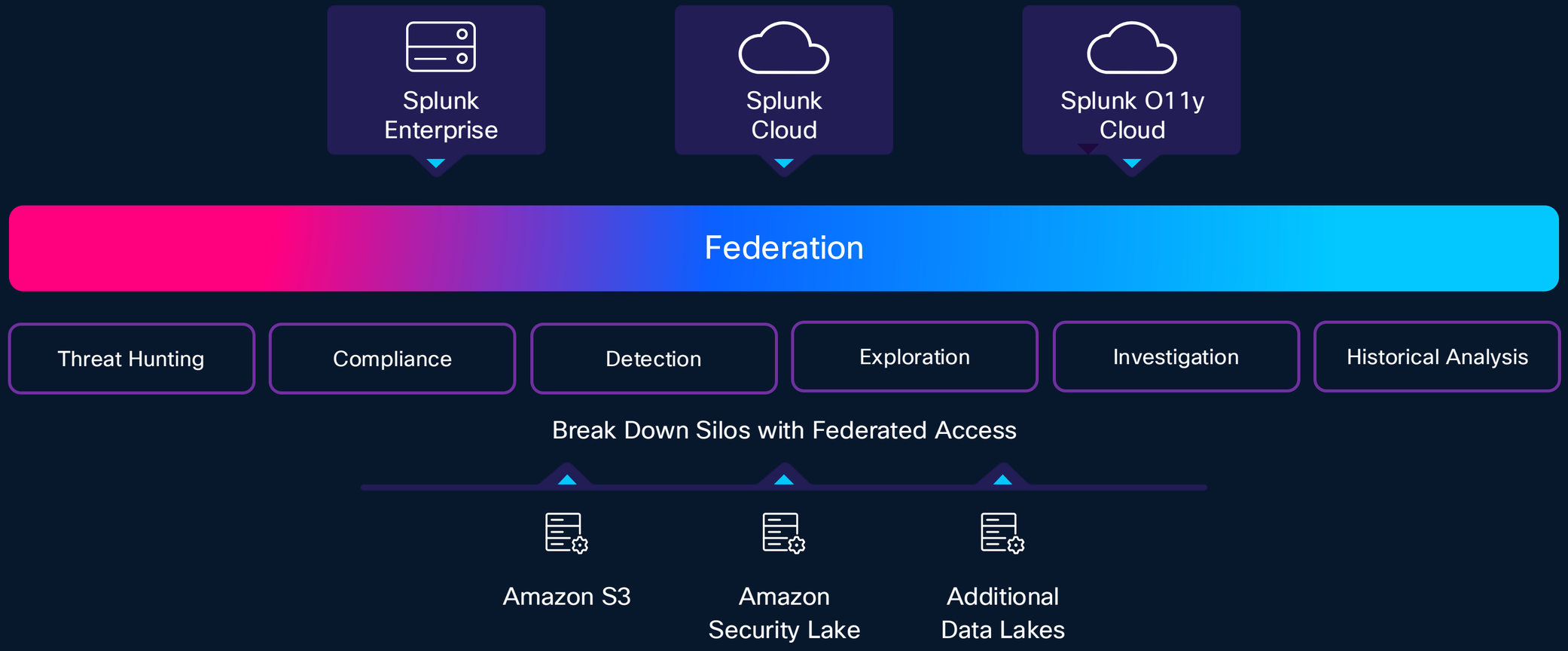
Empower SecOps with choice and efficiency across the entire data lifecycle

- Filter and route data efficiently **based on its value to your Enterprise**
  - Real time: prevention, detection and monitoring
  - Ad-Hoc: incident investigations, and threat hunting
  - Archive: longer term needs like forensics, audit, and compliance
- Consume both low yield and high value data **cost effectively.**
- Data is stored in ways that allow you to **minimize costs and maximize your value.**
- Normalize data to **speed investigations.**



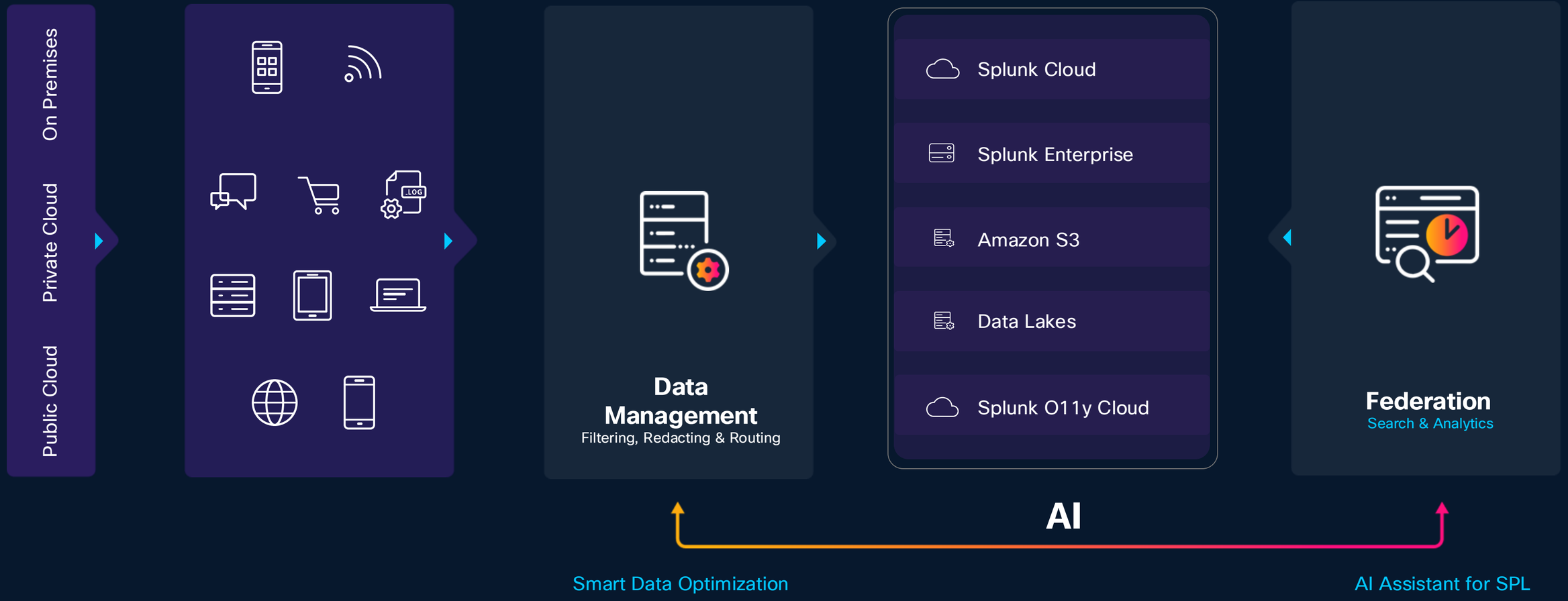
Federation

- Break down silos with federated access



Data Management and Federation Optimize Value

•Enable a broader range of use cases and better customer ROI



Summary

- The ES that you know and love has evolved into the leading AI-Powered SecOps Platform
- It's designed to end analyst fatigue and address challenges around:
  - Too much data that's burying important detections
  - Disconnect SOC toolset that drains time
  - The skills needed to keep pace with evolving threats
- It is available as ES Essentials and ES Premier

Let’s Build the SOC of the Future Together


CISCO