

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

Derrick Lawson, CISSP GMON GCDA, Solutions Engineer



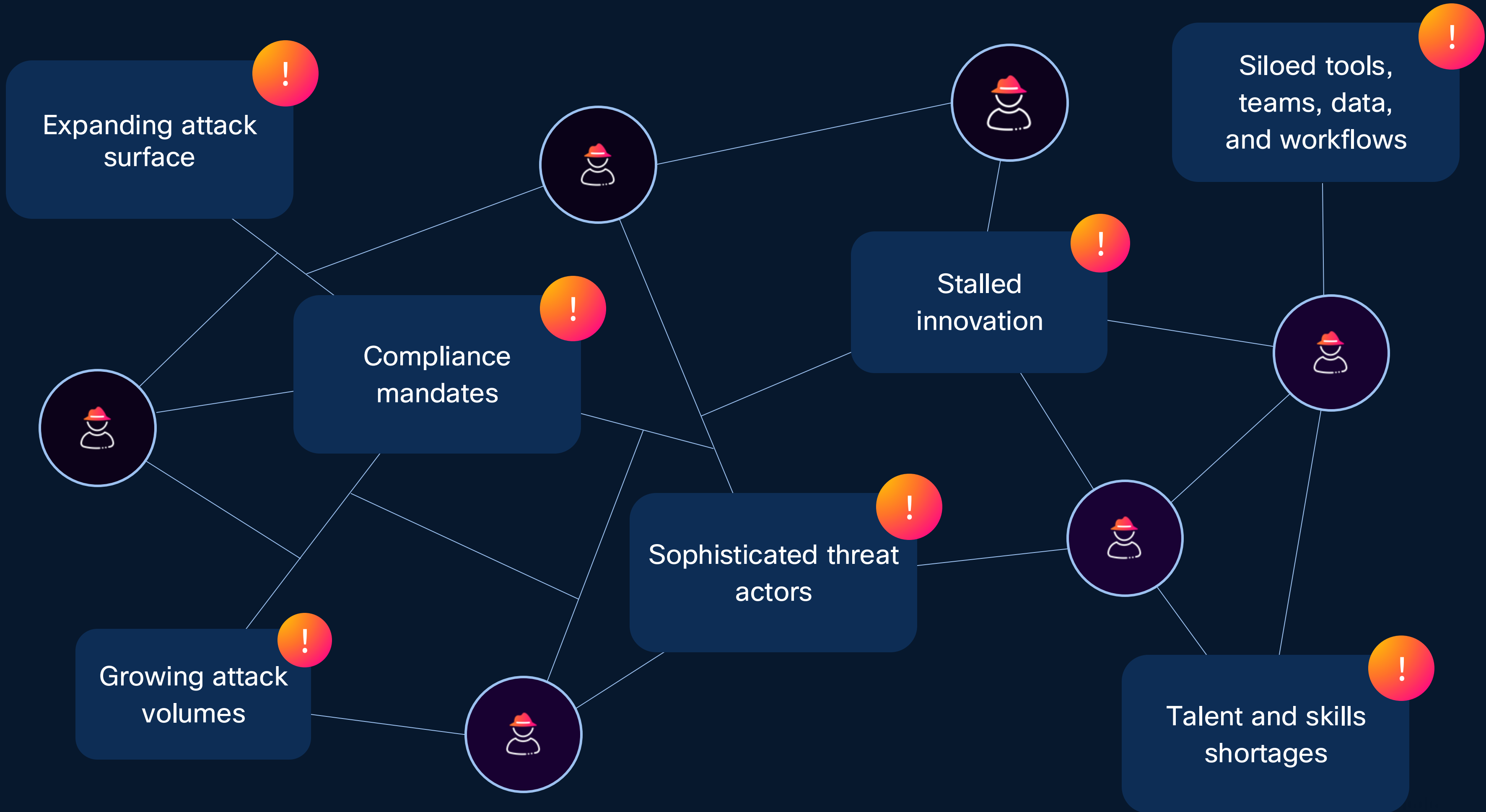
Forward- Looking Statements

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.

Splunk, Splunk>, Data-to-Everything, and Turn Data Into Doing are trademarks or registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.



LLM01: 2025

Prompt Injection →

LLM01:2025 Prompt Injection

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

[Read More](#)

LLM02: 2025

Sensitive Information Disclosure

LLM02:2025 Sensitive Information Disclosure

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

[Read More](#)

LLM03: 2025

Supply Chain

LLM03:2025 Supply Chain

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

[Read More](#)

LLM04: 2025

Data and Model Poisoning

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

LLM05:2025 Improper Output Handling

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

[Read More](#)

LLM06: 2025

Excessive Agency

LLM06:2025 Excessive Agency

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

[Read More](#)

LLM07: 2025

System Prompt Leakage

LLM07:2025 System Prompt Leakage

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

LLM08: 2025

Vector and Embedding Weaknesses

LLM08:2025 Vector and Embedding Weaknesses

Vectors and embeddings vulnerabilities present

LLM09: 2025

Misinformation

LLM09:2025 Misinformation

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

[Read More](#)

LLM10: 2025

Unbounded Consumption

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

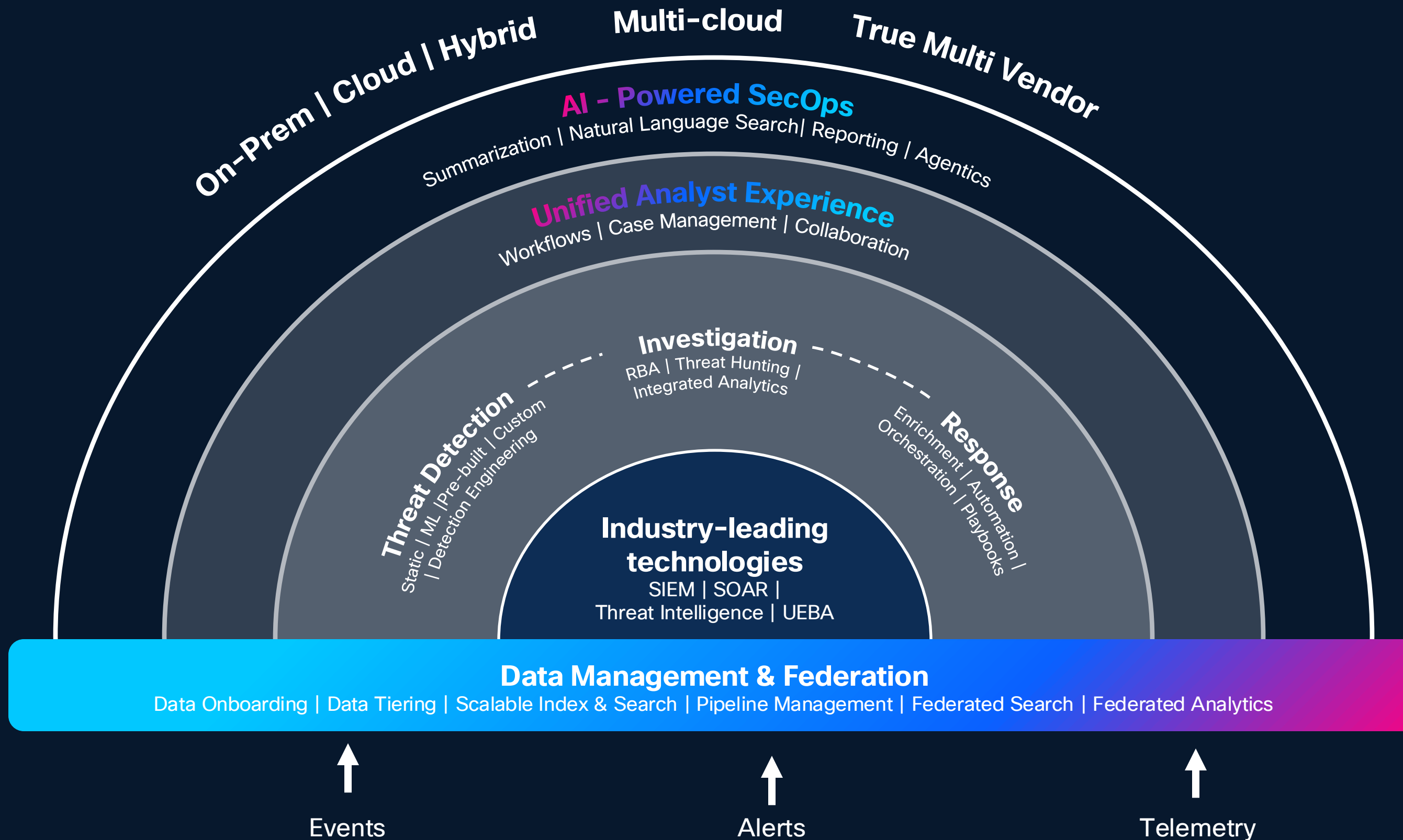
The SOC Reimagined

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

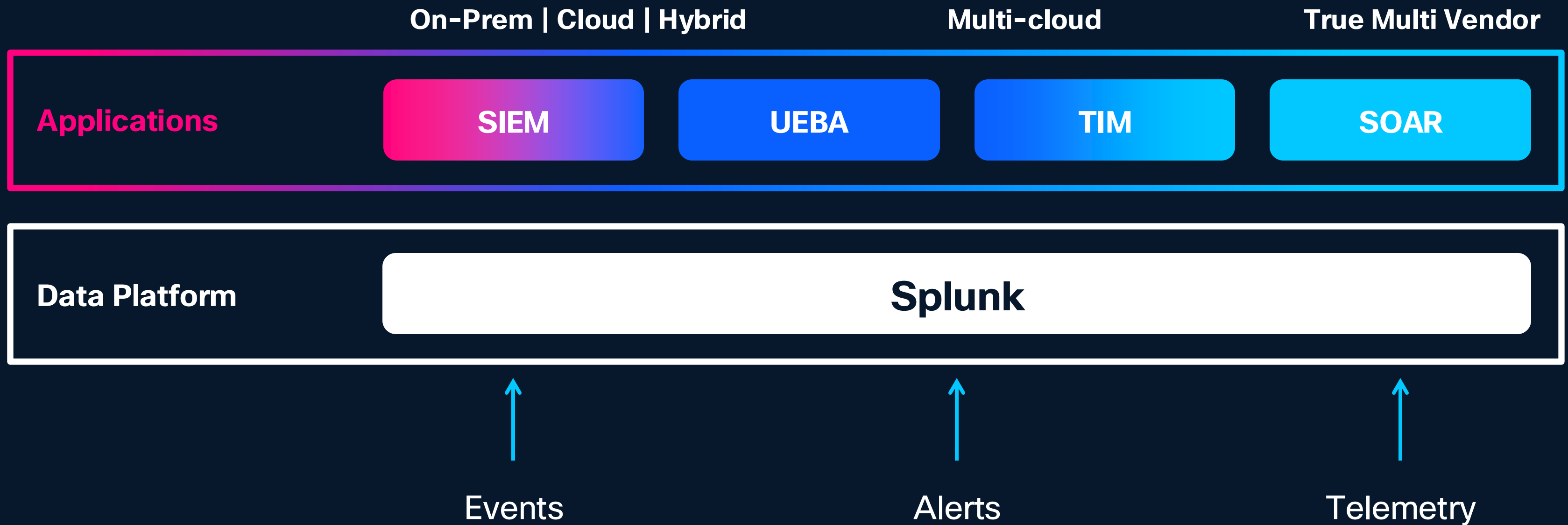
- Focus on the threats that matter most.
- Accelerate detection and response.
- Enable digital resilience for the business.









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.
- 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.

The screenshot displays the Splunk Enterprise Security Analyst Queue. The interface includes a search bar for findings and investigations, a time range filter set to 'Last 24 hours', and a 'Save' button. Below the search bar, there are navigation controls for 'Findings and Investigations' (475 total), including 'Last refresh at 5:30 PM', 'Auto-refresh on', and pagination options (1, 2, 3, 30, Next). The main table lists various findings and investigations with columns for Title, ID, Type, Entity, Risk, Findings, Investigations, Time, Disposition, Owner, Urgency, and Status. A 'New' badge is visible on the left side of the slide.

Title	ID	Type	Entity	Risk	Fin...	Int...	Time	Disposition	Owner	Urgency	Statu
Excessive failed logins		FINDING	win-hp-64861	70		7	Today, 9:45 AM	Undetermined	Unassigned	Medium	N
Multiple findings from the same entity [bstoll@splunkshirtcompany.com]	ES-2303	INVESTIGATION	bstoll@splunkshirtcompany.c...	420	4	36	Today, 9:42 AM	Undetermined	Marquis Montgomery	Medium	N
ATT&CK tactic threshold exceeded over previous 7 days for entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		20	Today, 9:42 AM	Undetermined	Unassigned	Medium	N
24 hour risk threshold exceeded for entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		4	Today, 9:42 AM	Undetermined	Unassigned	Low	N
Malicious PowerShell process - encoded command on entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		1	Today, 7:21 AM	Undetermined	Unassigned	Medium	N
Malicious PowerShell process - encoded command on entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		1	Today, 6:21 AM	Undetermined	Unassigned	Medium	N
Intermediate findings		INTERMEDIATE...	bstoll@splunkshirtcompany.c...	420		107	Today, 6:21 AM				
24 hour risk threshold exceed for entity [172.16.0.149]		FINDING	172.16.0.149	140		4	Today, 9:40 AM	Undetermined	Unassigned	High	N
Unusual volume of network activity detected on 54.230.147.59		FINDING	54.230.147.59	60		2	Today, 9:40 AM	Undetermined	Unassigned	Medium	N
Excessive failed logins		FINDING	NY_APP_002	75		11	Today, 9:35 AM	Undetermined	Unassigned	Medium	N
Unusual volume of network activity detected on 52.216.133.181		FINDING	52.216.133.181	35		5	Today, 9:35 AM	Undetermined	Unassigned	Low	N
Unusual volume of network activity detected on 52.218.196.122		FINDING	52.218.196.122	20		4	Today, 9:27 AM	Undetermined	Unassigned	Low	N
Multiple findings from the same entity [mickey.perre@splunkshirtcompany.com]	ES-2302	INVESTIGATION	mickey.perre@splunkshirtco...	120	6	25	Today, 9:27 AM	Undetermined	Unassigned	High	N
Multiple findings from the same entity [hayley.jensen@splunkshirtcompany.com]	ES-2301	INVESTIGATION	hayley.jensen@splunkshirtco...	150	5	16	Today, 9:23 AM	Undetermined	Unassigned	High	N
Excessive failed logins		FINDING	macbook-46743	50		2	Today, 9:23 AM	Undetermined	Unassigned	Low	N
24 hour risk threshold exceed for entity		FINDING	macbook-44504	200		2	Today, 9:10 AM	Undetermined	Unassigned	Medium	N

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.

The screenshot displays the Splunk Cloud Automation interface. At the top, a notification reads "7 day risk threshold exceeded for user=kennyb" with ID ES-00024. The main area is titled "Automation" and shows a list of playbooks. The "Insider Account Based Prep" playbook is selected, showing its status as "Success" and a list of actions: "add_finding_or_investigation_note_1" and "query_device_1". A "View logs" button is visible. Below the list, a detailed view of the "Insider Account Based Prep" playbook is shown, including a table with columns for Status, Success, Started, and Completed. The "Action: add finding or investigation note" is highlighted, and its output is displayed as a JSON object:

```
{ [-]
  next_page: null,
  items: [ [-]
    { [-]
      source_type: "Incident",
      update_time: 1756263991.675413,
      ai_generated: false,
      last_edited_by: null,
      response_plan_info: null
    }
  ]
}
```

On the right side, an "Add" panel is open, showing various action categories: EXECUTE ACTIONS (Action, Playbook, Code, Utility), PROCESS FILTERS (Filter, Decision, Format), HUMAN INPUT (Prompt), and SPLUNK API (Enterprise Security). A workflow diagram is visible on the far right, showing a sequence of steps: Start, ACTION get attributes, ENTERPRISE SECURITY API add finding or investigation note, and End.

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.

The screenshot displays a security dashboard interface. The main panel shows a list of automation actions under the heading "Automation". The actions include:

- user initiated block hash action (by splunker Jan 10, 5:51 AM) - Success
- user initiated quarantine device action (by splunker Jan 10, 5:51 AM) - Success
- user initiated disable user action (by splunker Jan 10, 5:50 AM) - Success
- Risk Auto Containment (by splunker Jan 10, 5:50 AM) - Success, with 1 action ran (get_response_plans_1)
- user initiated file reputation action (by splunker Jan 10, 5:47 AM) - Failure (1 action failed for app VirusTotal v3)
- user initiated file reputation action (by splunker Jan 10, 5:46 AM) - Success
- Encoded Powershell Analysis (by splunker Jan 10, 5:40 AM) - Success, with 1 action ran

On the right, a detailed view for "user initiated block hash action" is shown, including status (Success), owner (TDIR Admin), and connector (Carbon Black Response). A table lists the action details:

RUN ID	CONFIGURATION	NAME	CON
558	carbon black	block hash	Carb

Below the table, there are fields for "Action: Block Hash" and "Run Id: 558". A hash value is displayed: 586EF56F4D8963DD546163AC31C865D7.

Overlaid on the right is a chat window with the following content:

- TA TDIR Admin** Jan 17, 1:36 PM: Summarize the findings
- AI** Jan 17, 1:37 PM: **Understanding the Findings:**
The investigation named "Malicious PowerShell Process - Encoded Command On FYODOR-L.splunkshirtcompany.com" was triggered on Jan 09, 2025 09:36 PM UTC. The risk object identified is fyodor@splunkshirtcompany.com, connected to a user conducting potentially harmful activities. The event originated from FYODOR-L.splunkshirtcompany.com, identified through an encoded command executed via PowerShell. The PowerShell process ran hdoor.exe from the temp directory, utilizing IP addresses (192.168.9.1-192.168.9.50). The severity of this event is not specified, but the email fyodor@splunkshirtcompany.com was seen issuing high-level integrity commands with a session ID of '3'.
- TA TDIR Admin** Jan 10, 5:53 AM: Encoded PowerShell Detection Response/Render Verdict/Take ...
Take Remediation Action or Close Incident - Task Note - 1
I have blocked the Malicious file hash across and quarantined and disabled the current

Demo

Highlights

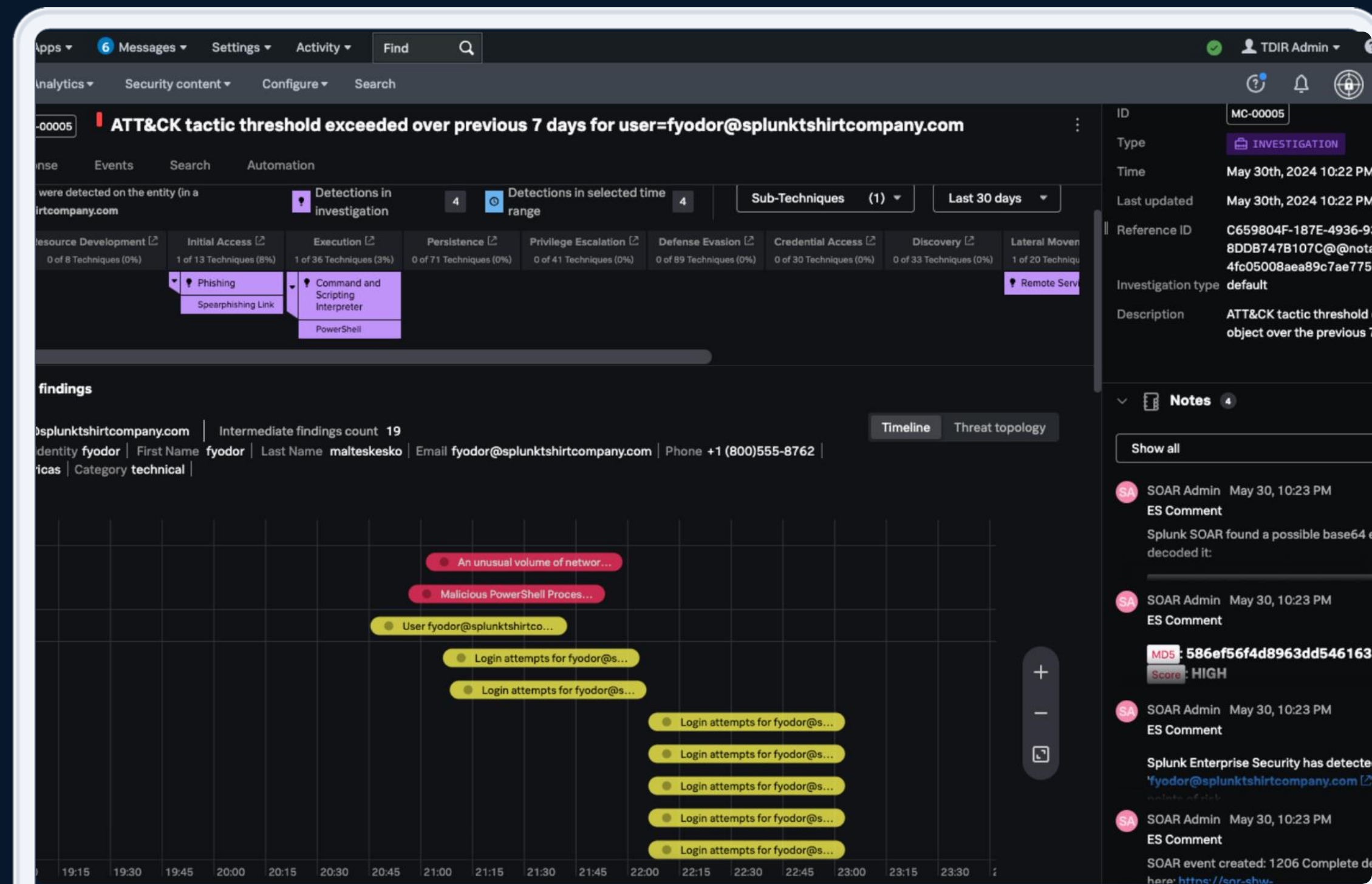
Empower Accurate Detection with Context

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

© 2025 Cisco and/or its affiliates. All rights reserved.



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](#)

The screenshot displays the Splunk SOAR interface for a workflow titled "7 day risk threshold exceeded for user=kennyb". The interface is divided into several sections:

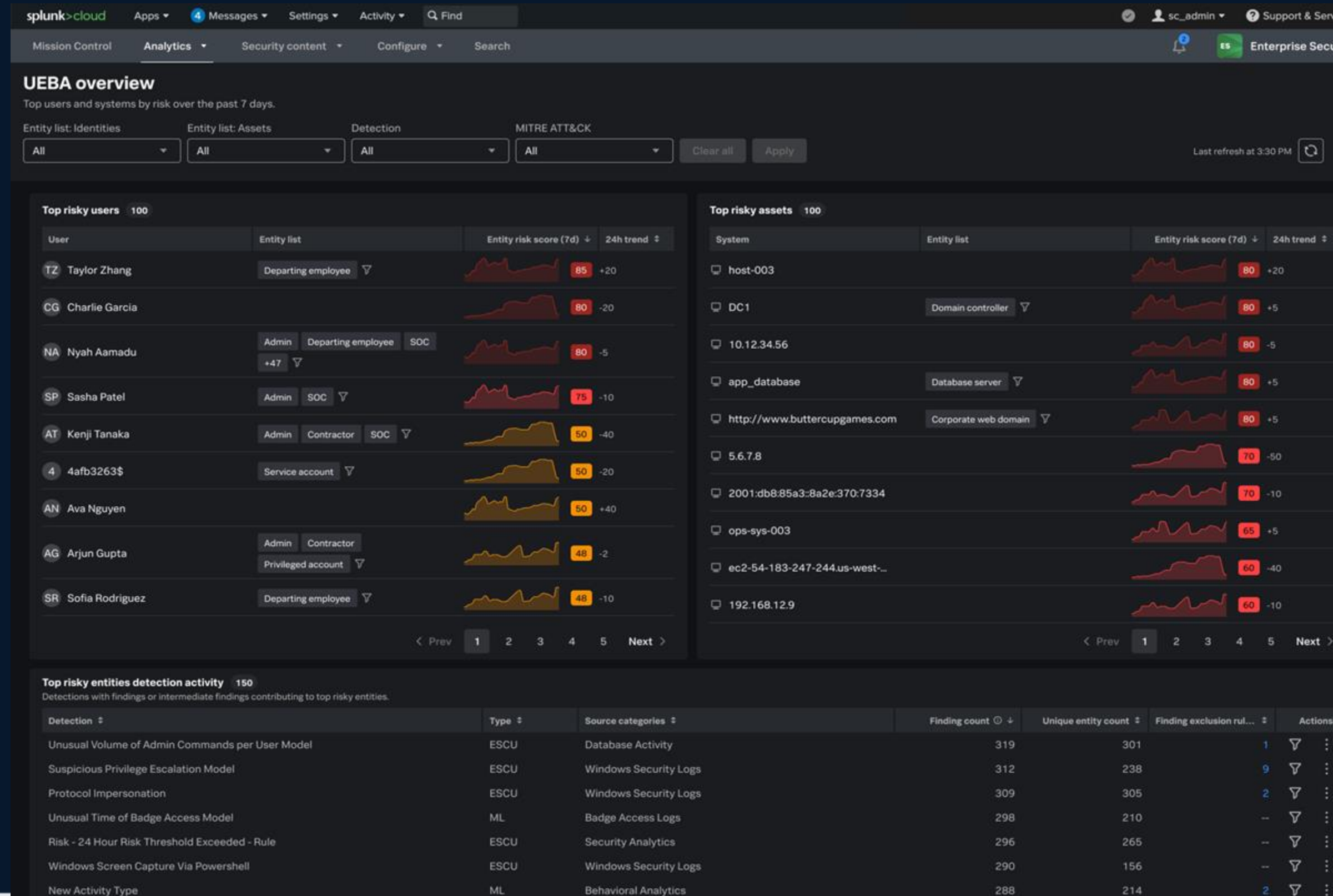
- Header:** Includes navigation menus (Apps, Messages, Settings, Activity, Find) and user information (seancain@splunk.com).
- Event Details:** Shows the event ID "ES-00024" and the title "7 day risk threshold exceeded for user=kennyb".
- Automation Panel:** Lists the workflow "Investigate Compromised Identity" with a status of "Success". It shows a list of actions:
 - add_other_impacted_identities_note (Success)
 - add_disabled_account_note (Success)
 - prompt_to_disable_user (Success)
- Task List:** Shows a "prompt" task with the title "Notify Manager of Insider Investigation" and a status of "Success". It lists two actions:
 - add_finding_or_investigation_note_2 (Success)
 - add_finding_or_investigation_note_1 (Success)
- Machine Prep:** Shows a "Machine Prep" task with a status of "Success".
- Task Execution Details:** A table shows the execution of the "prompt_to_disable_user" task:

RUN ID	CONFIGURATION	NAME	CONNECTOR	STATUS
		prompt_to_disable_user		Success
- Info Panel:** Provides metadata for the event:
 - Owner: dgamer@splunk.c...
 - Status: New
 - Urgency: Critical
 - Sensitivity: Red
 - Disposition: Undetermined
 - ID: ES-00024
 - Type: Investigation
 - Time: Aug 27th, 2025 2:00 AM
 - Last updated: Aug 29th, 2025 4:38 PM
 - Reference ID: bef8d5b7-d265-4f1d-a867-5f8e20b3f8f0
 - Investigation type: default
 - Description: Risk Threshold Exceeded for an object over a 7 day period.
- Notes:** A section for notes with a "Show all" button and search icons.

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](#)

The screenshot displays the Splunk UEBA user analysis interface. At the top, the navigation bar includes 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', 'Find', and a search icon. The user 'Jerald Perry' is logged in. The main navigation tabs are 'UEBA overview', 'UEBA user analysis' (selected), 'UEBA asset analysis', 'UEBA configuration', and 'Search'. Below the navigation, the 'UEBA user analysis' section features a search bar for a user. The current view is for 'Fyodor Malteskesko' with a risk score of 94. The interface shows 'Entity connections' for the user over the last 7 days, with a table listing connections to various assets. A 'Detection heatmap' is also visible, showing finding counts by detection rule.

peer group	user	asset	count	score
Grace Hoppy	Fyodor Malteskesko	10.11.36.1	14	42.25
		10.11.36.31	1	52
		192.168.15.9	1	45.5
		2001:db8:3:4:4:c000:221	1	61.9
		2001:db8:85a3::8a2e:370...	1	61.9

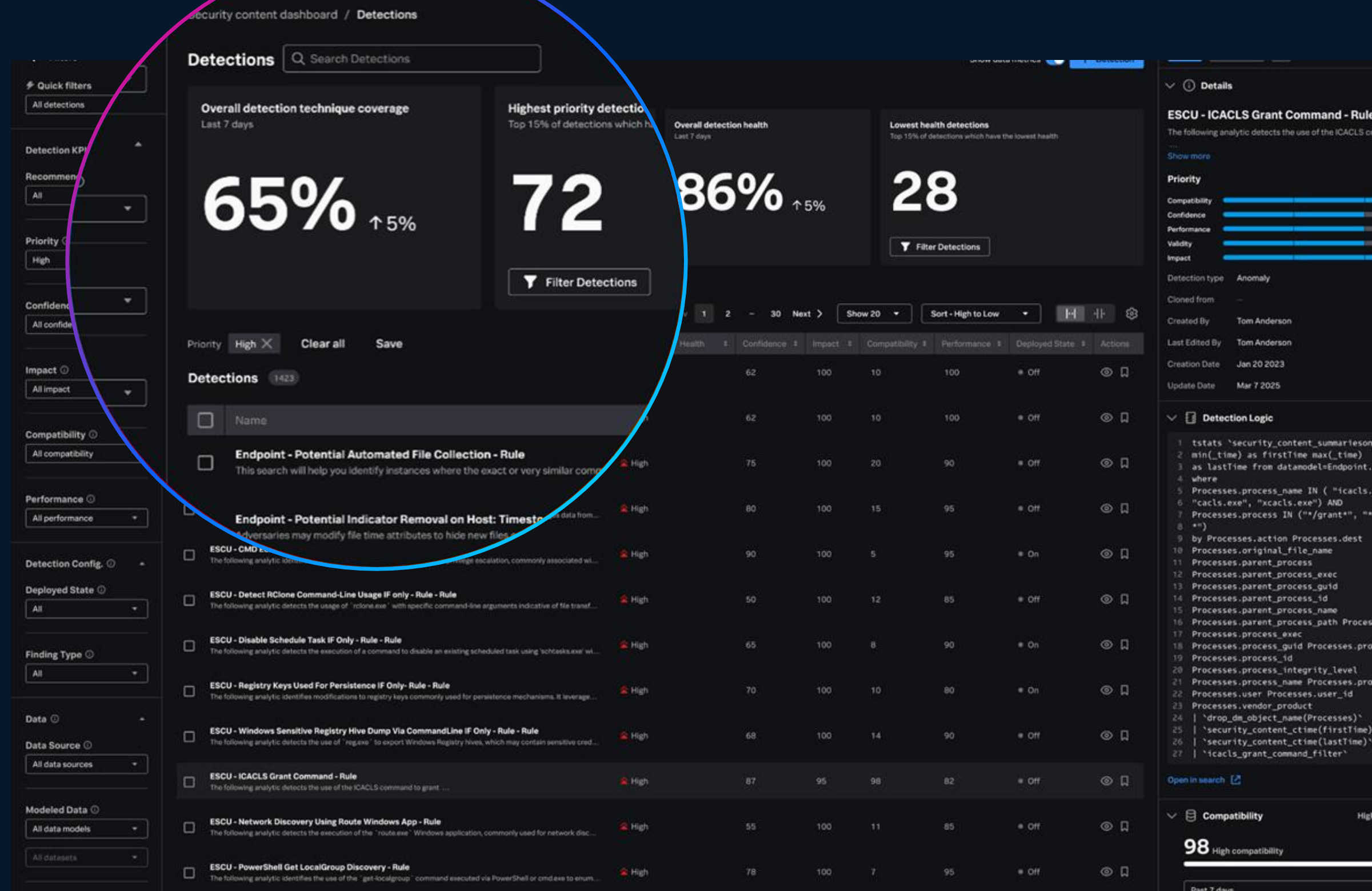
Detection Rule	Finding Count
ESCU - AWS Network Access Control List Deleted - Rule	8
ESCU - AWS EC2 Snapshot Shared Externally - Rule	1
ESCU - AWS High Number Of Failed Authentications Fro...	1
Rare Process Activity in Windows Data - Rule	1
Unauthorized Login Type - Rule	1

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

The screenshot displays the 'Analyst queue' interface. At the top, there is a search bar for 'Search findings & investigations' and a 'Saved Views' dropdown menu. Below this, a 'Time Range' filter is set to 'Last 24 hours', with options for 'Clear All', 'Save', and 'Apply'. A bar chart shows activity levels over a 24-hour period, with a peak around 8:00 PM. Below the chart, there are buttons for 'Zoom To Selection', 'Zoom Out', and 'Deselect'. The main section is titled 'Findings and investigations' with a notification badge '3' and a 'Last refresh at 10:51 PM' timestamp. It includes a refresh button, an 'Auto-refresh off' dropdown, and a '20 per page' dropdown. The table below lists three items, all of which are 'Manual Finding Event - Rule' with a type of 'FI'.

Response	Mode	Time	
Intelligence Enrichment with Talos	adhoc	2024-12-11T22:51:22+0000	jkr
Intelligence Enrichment with Talos	adhoc	2024-12-11T22:40:31+0000	jkr
Finding	adhoc	2024-12-11T22:38:59+0000	jkr

View Adaptive Response Invocations [View Adaptive Response Invocations](#)

Notes 1

Show all

cs Cisco Talos Intelligence for Enterprise Security Dec 11, 10:51 ES Comment

Observable: <https://hsgsjw.icu/>

Threat Level: Untrusted

Threat Categories: Malware

Malware Description: Malicious file (attached or linked).

Threat Categories: Phishing

Phishing Description: Collection of credentials (link).

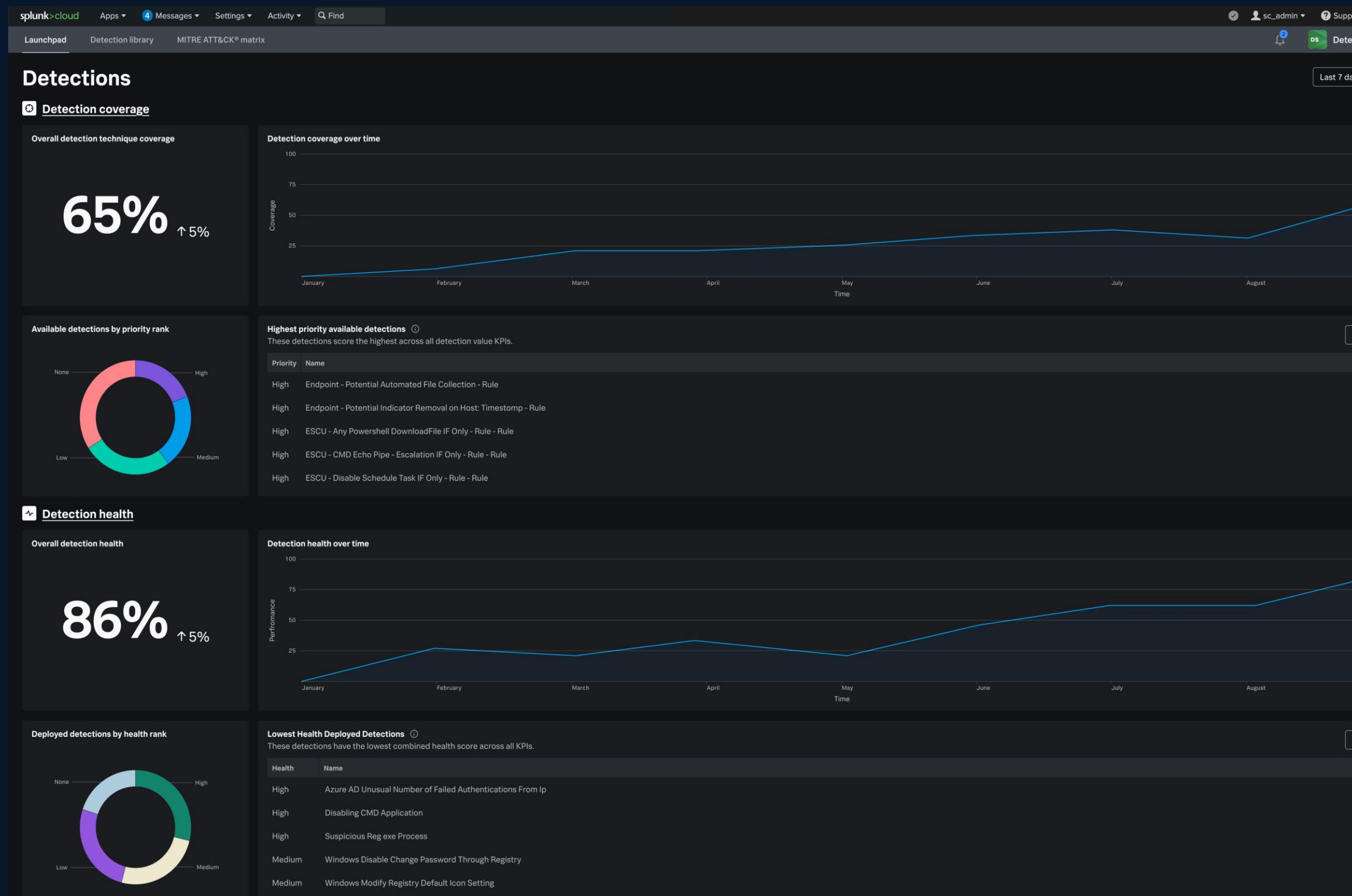
Threat Categories: Malicious Sites

Malicious Sites Description: Sites exhibiting malicious behavior. Malicious Sites do not necessarily fit into another, more granular, threat category.

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.


Bring search and analytics to external stores without ingestion.

Public Cloud Private Cloud On Premises



Data management
Filtering, Redacting & Routing

Amazon S3 Amazon Security Lake Additional Data Lakes



Federation
Search & Analytics

Data normalization
CIM, OCSF



Splunk Enterprise Security

Optimize Data and Maximize Security Value

Empower SecOps with choice and efficiency across the entire data lifecycle

Critical Need for Data

- 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.**

- Security Monitoring
- Incident Management
- Risk Based Alert Prioritization
- Anomaly Detection
- Automation and Orchestration

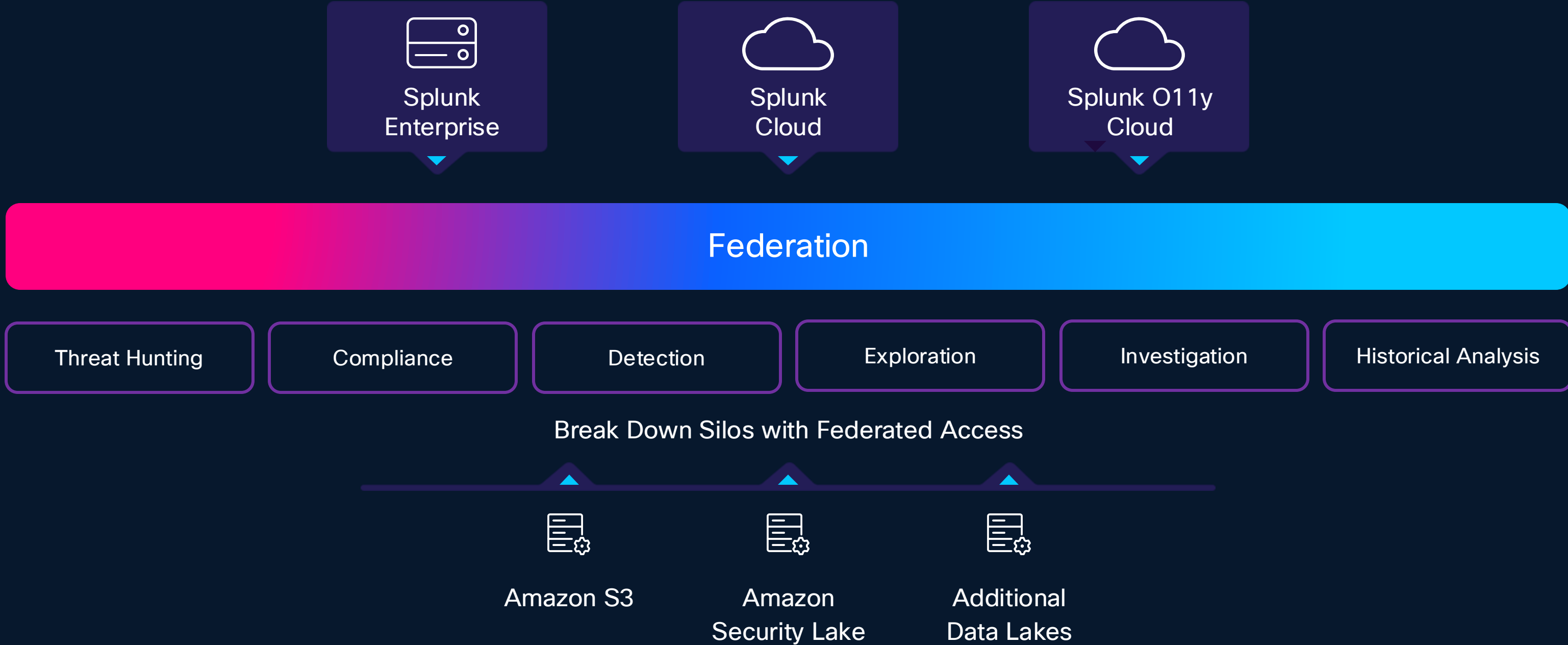
- Threat Intelligence Enrichment
- Correlation Analytics Enrichment
- Threat Hunting
- Visualization and Reporting

- Compliance
- Model Training & Curation for Anomaly Detection, Detecting Insider Threats

Non Immediate
Criticality for Data

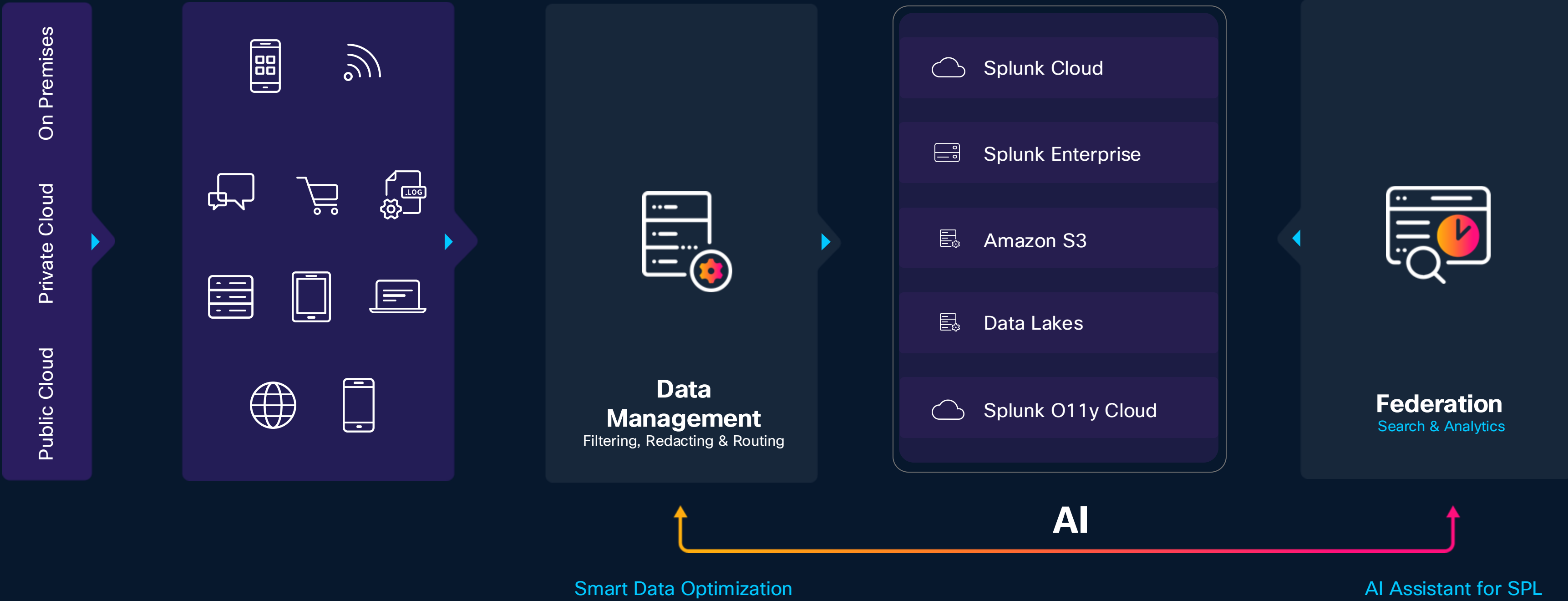
Federation

.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**

