

Splunk for SecOps: AI, Agentic AI, Optimized Workflows and Automation

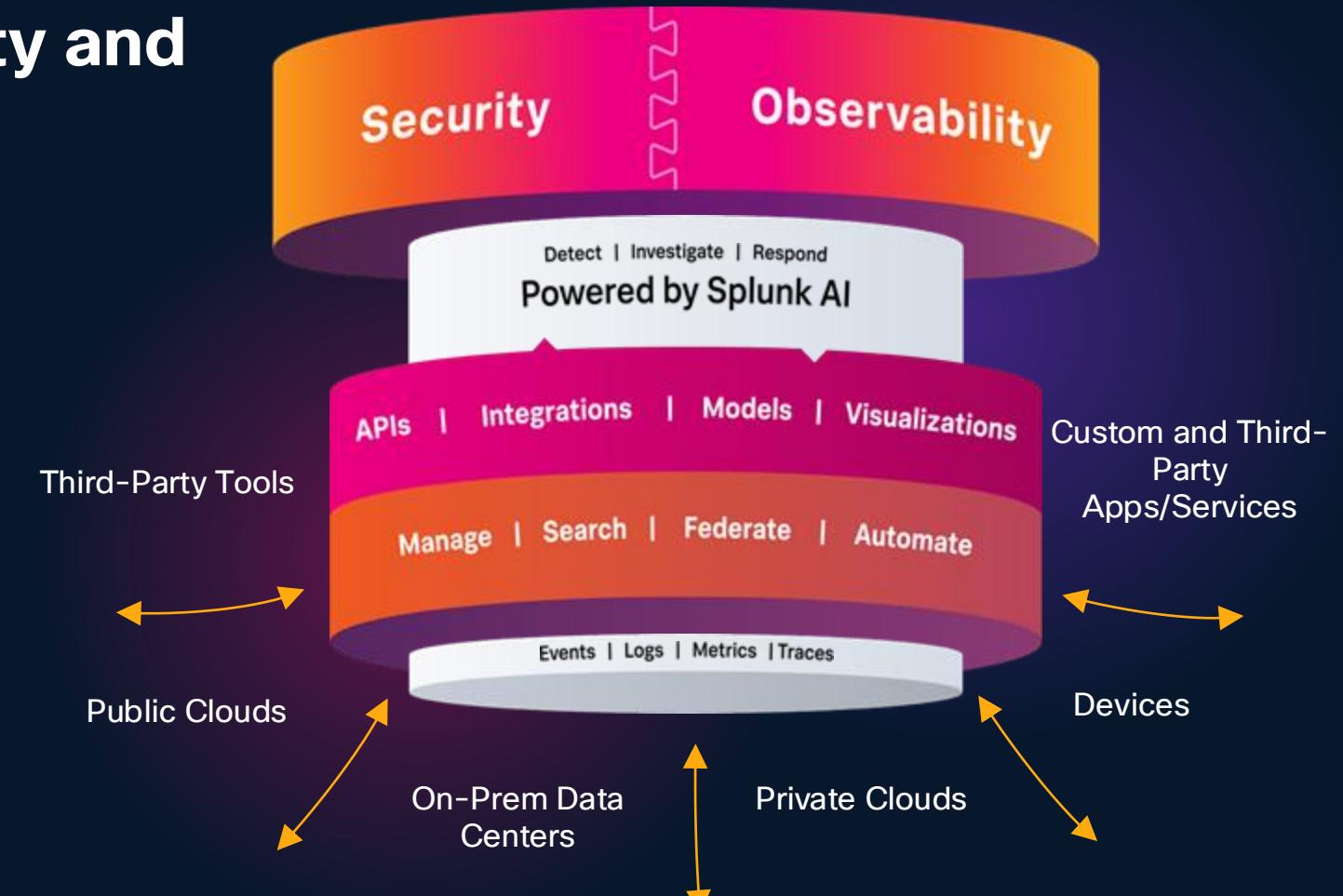
Niklas Blomquist – Strategic Security Advisor



Agenda

- 01 **Splunk platform**
- 02 **Common Security Use-cases**
- 03 **Splunk Apps**
- 04 **AI Do It Yourself**
- 05 **Splunk AI Assistant for SPL**
- 06 **Splunk Premium Products**
- 07 **Splunk AI Assistant for Security**
- 08 **Splunk User and Entity Behavioral Analytics**

Splunk: The Unified Security and Observability Platform



Most common Security Use Cases



Threat Detection



Investigation



Response



Compliance

Splunkbase

splunkbase Collections Apps Submit an app Log In

>Main Page / Apps

Discover Apps

BUILT BY

- Splunk
- Cisco
- Partners
- Community

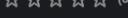
PLATFORM [Clear](#)

- SPLUNK**
 - > [PRODUCT](#)
 - > [VERSION](#)
- SPLUNK SOAR**
 - > [PRODUCT](#)
 - > [VERSION](#)

Showing 1-21 of 628 Results for **security** [X](#)

Filtered by: **Splunk** [X](#)

Sort by: [New](#) ▾

 Realm Security Data Pipeline By Devon Lattrell	 ITdesign App for One Identity SPP By ITdesign Software Projects & Consulting GmbH	 Transmit Security Events Add-on for Splunk By Hai Sadon
The Realm.Security app integrates the full capabilities of the Realm.Security Data Pipeline Platform directly into you... PLATFORM Not Available	The ITdesign Safeguard for Privileged Passwords App & Add-On delivers deep visibility into One Identity Safeguard PA... PLATFORM Not Available	The Transmit Security Events Add-on for Splunk is an essential add-on that seamlessly integrates the audit log... PLATFORM Splunk Enterprise, Splunk Cloud
RATING  (0)	RATING  (2)	RATING  (2)
 DEVELOPER SUPPORTED APP	 DEVELOPER SUPPORTED APP	 DEVELOPER SUPPORTED ADDON
 Flashpoint Add-on for Splunk	 TA-ollama	 Infigo SIEM Content

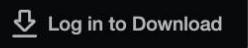
Splunk InfoSec App

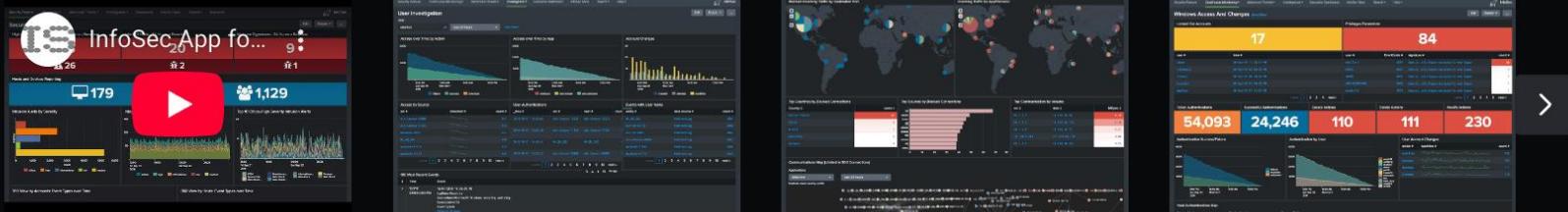
IS **InfoSec App for Splunk**

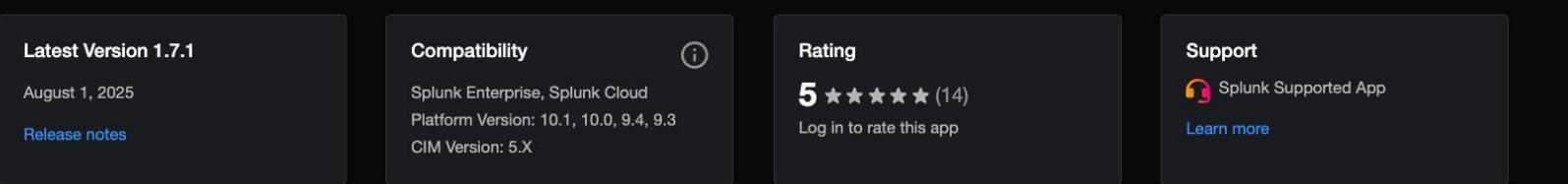
InfoSec app for Splunk is your starter security pack.

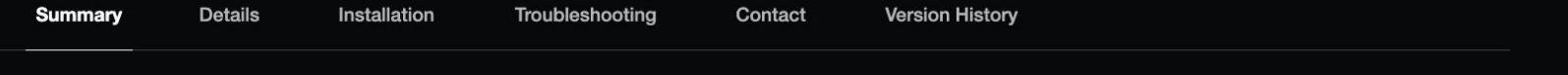
Built by [Splunk LLC](#)

 [Log in to Download](#)



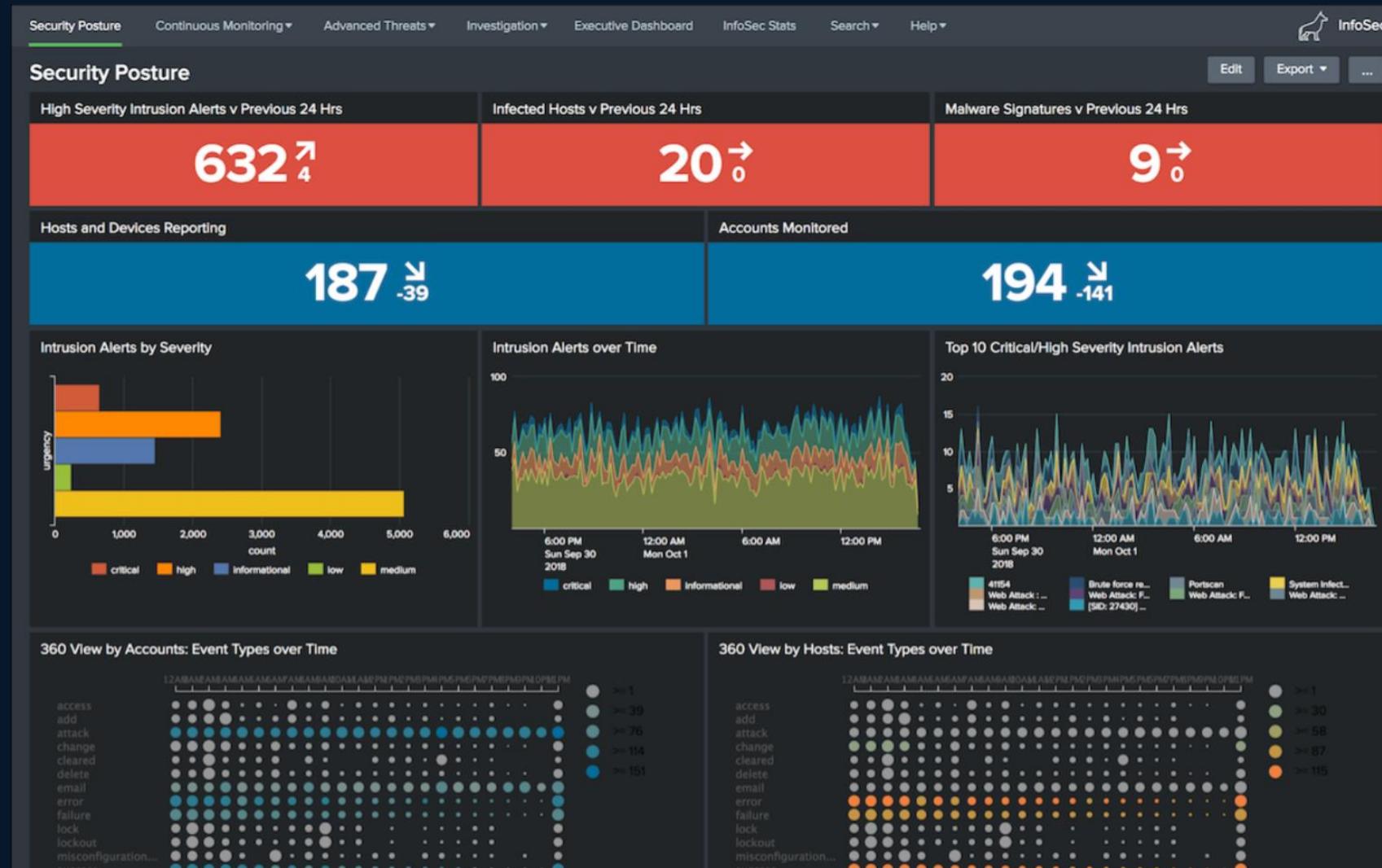






[Summary](#) [Details](#) [Installation](#) [Troubleshooting](#) [Contact](#) [Version History](#)

Splunk InfoSec App

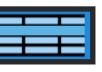


Splunk AI Toolkit

Showcase

Welcome to the AI Toolkit Showcase. Watch and learn from interactive end-to-end examples using real datasets. Click on an example to pre-populate the Assistant with the sample dataset and its settings. Inspect the Search Processing Language as well as the underlying code of these examples to see how it all works.

View examples by [ML Operation](#) [Industry](#) [Filter Examples](#) 

LLM Integrations 

View examples of how to enrich your data with output from externally hosted Large Language Models.

3 Examples Available

Predict Fields 

View examples that predict the value of a numeric or categorical field using the values from other fields in the event.

15 Examples Available

Detect Outliers 

View examples that detect numeric and categorical values that differ significantly from values in the rest of the data. Identified outliers are indicative of interesting, unusual, and possibly dangerous events.

14 Examples Available

Forecast Time Series 

View examples that predict the next value in a sequence of time series data by using past time series data.

9 Examples Available

Cluster Events 

View examples that partition events with multiple fields into groups of events based on the values of those fields.

8 Examples Available

Featured Examples 

<p>Detect Outliers in Bitcoin Transactions This example uses the Detect Categorical Outliers Assistant on three fields of data that include user and value.</p> <p><i>Security</i></p>	<p>Detect Outliers in Disk Failures This example uses the Detect Categorical Outliers Assistant on four fields of data that include model and serial number.</p> <p><i>IT</i></p>	<p>Detect Outliers in Number of Logins (vs. Predicted Value) This example uses the Detect Numeric Outliers Assistant and threshold method of Median Absolute Deviation to look for outliers in login information.</p> <p><i>Security</i></p>	<p>Detect Outliers in Server Response Time This example uses the Detect Numeric Outliers Assistant and threshold method of Median Absolute Deviation to look for outliers in server response time.</p> <p><i>IT</i></p>	<p>Find Anomalies in Supermarket Purchases This example uses the Smart Outlier Detection Assistant to find anomalies in supermarket purchase quantity metrics across different shops. The Smart Outlier Detection Assistant leverages the DensityFunction algorithm.</p> <p><i>Business Analytics</i></p>
---	--	---	--	--

[Smart Outlier Detection](#) [Detect Numeric Outliers](#) [Detect Categorical Outliers](#)

Smart Outlier Detection Examples

Detect numeric outliers using a step-by-step guided workflow to leverage a density algorithm and segment data in advance of your anomaly search.

<p>Find Anomalies in Hard Drive Metrics This example uses the Smart Outlier Detection Assistant to find anomalies in SMART (self-monitoring, analysis, and reporting technology) metrics across different hard drive models. The Smart Outlier Detection Assistant leverages the DensityFunction algorithm.</p> <p><i>IT</i></p>	<p>Find Anomalies in Supermarket Purchases This example uses the Smart Outlier Detection Assistant to find anomalies in supermarket purchase quantity metrics across different shops. The Smart Outlier Detection Assistant leverages the DensityFunction algorithm.</p> <p><i>Business Analytics</i></p>
---	--

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

 CISCO

Splunk AI Toolkit



Splunk MCP Server

MCP Server for Splunk Platform The Model Context Protocol (MCP) is an open standard and framework that enables seamless, secure, and standardized two-way communication between AI applications (like large language models) and external data sources or tools. It acts as a...

Built by [Splunk LLC](#)

 [Log in to Download](#)  

Latest Version 0.2.6

November 14, 2025

[Release notes](#)

Compatibility 

Splunk Enterprise, Splunk Cloud

Platform Version: 10.1, 10.0, 9.4, 9.3, 9.2, 9.1, 9.0, 8.2, 8.1, 8.0

Rating

 (6)

[Log in to rate this app](#)

Support

 Splunk Supported App

[Learn more](#)

Ranking

#7 In Artificial Intelligence

Splunk AI Assistant for SPL

Get your work done faster

Need to create a new dashboard to troubleshoot an issue? Spend more time thinking about the problem than the technology. Use natural language to prompt Splunk AI Assistant to generate SPL and get you started quickly.

Write SPL



This query does the following:

1. It filters the data source to only include logs from `aws:cloudwatchlogs:vpcflow`.
2. It uses the `iplocation` command to get the geographical location of the destination IP addresses.
3. It then uses the `geostats` command to calculate the count of IP addresses for each country and generates a map.

This query will give you a map visualization of the IP addresses in the `aws:cloudwatchlogs:vpcflow` logs, showing the distribution of IPs across different countries.

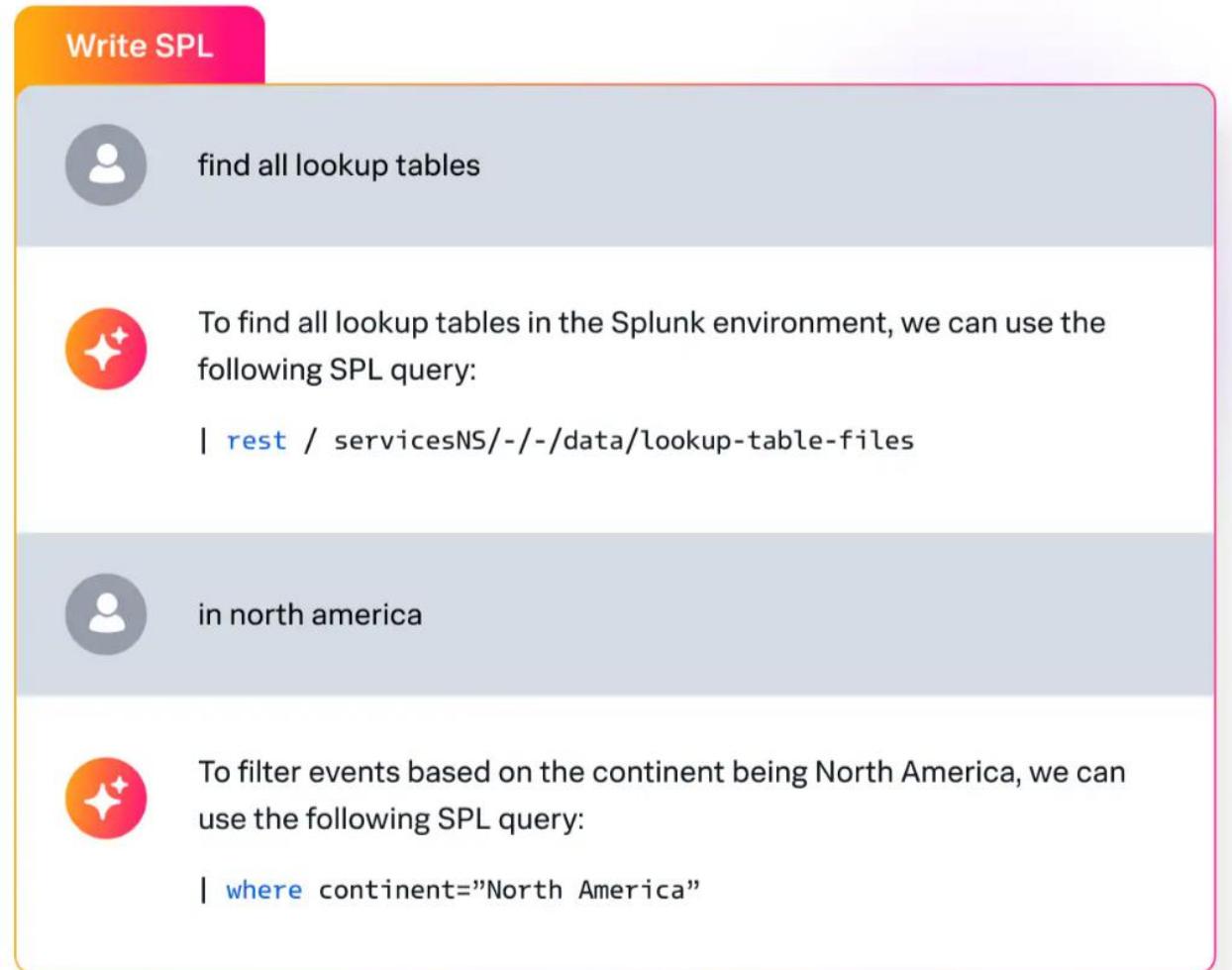
[Open in Search](#)

Splunk AI Assistant for SPL

Chat with your data

Analysis is an iterative process.

Chat with the Splunk AI Assistant to generate SPL and drill down into your Splunk data for a deeper level of insights.



The image shows a mobile-style interface for the Splunk AI Assistant. At the top, a pink bar says "Write SPL". Below it, a user icon and the text "find all lookup tables". To the right, an AI icon and the text: "To find all lookup tables in the Splunk environment, we can use the following SPL query:
| rest / servicesNS/-/-/data/lookup-table-files". Below this, another user icon and the text "in north america". To the right, another AI icon and the text: "To filter events based on the continent being North America, we can use the following SPL query:
| where continent="North America"

Splunk Security

Powering the SOC of the future with the leading TDIR solution

Unified threat detection, investigation & response

Splunk Asset & Risk Intelligence

Continuous asset discovery

Splunk Attack Analyzer

Automated threat analysis

Splunk SOAR

Security automation

Splunk Enterprise Security

SIEM

Traditional environments

Cloud native environments

Splunk Platform



Splunk Enterprise Security

The AI Powered SecOps Platform

- Unlock full-fidelity visibility** and control of your security data wherever it lives.
- Deliver the best analyst experience** and tooling with unified TDIR.
- Accelerate the SOC** with built-in AI and Agentics across every layer.

The screenshot displays the Splunk Enterprise Security interface. At the top, a navigation bar includes 'Messages', 'Settings', 'Activity', 'Find', and a search bar. Below the navigation is a sub-navigation bar with 'Security content', 'Configure', and 'Search'.

The main content area shows a critical alert: 'ATT&CK tactic threshold exceeded over previous 7 days for user=fyodor@splunktshirtcompany.com'. The alert is categorized under 'Events', 'Search', and 'Automation'.

Below the alert, a table provides a breakdown of detections:

Category	Technique	Count	Percentage
Initial Access	Phishing	1	8%
Execution	Command and Scripting Interpreter	1	3%
Persistence	PowerShell	1	0%
Privilege Escalation		0	0%
Defense Evasion		0	0%
Credential Access		0	0%
Discovery		0	0%
Lateral Movement	Remote Service	1	20%

On the right side of the interface, a sidebar lists various security-related fields: ID, Type, Time, Last updated, Reference ID, Investigation type, Description, and Notes. The 'Notes' section shows a list of comments from a SOAR Admin, including entries about network traffic, PowerShell processes, user logins, and MD5 hashes.

Splunk Enterprise Security

- 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.

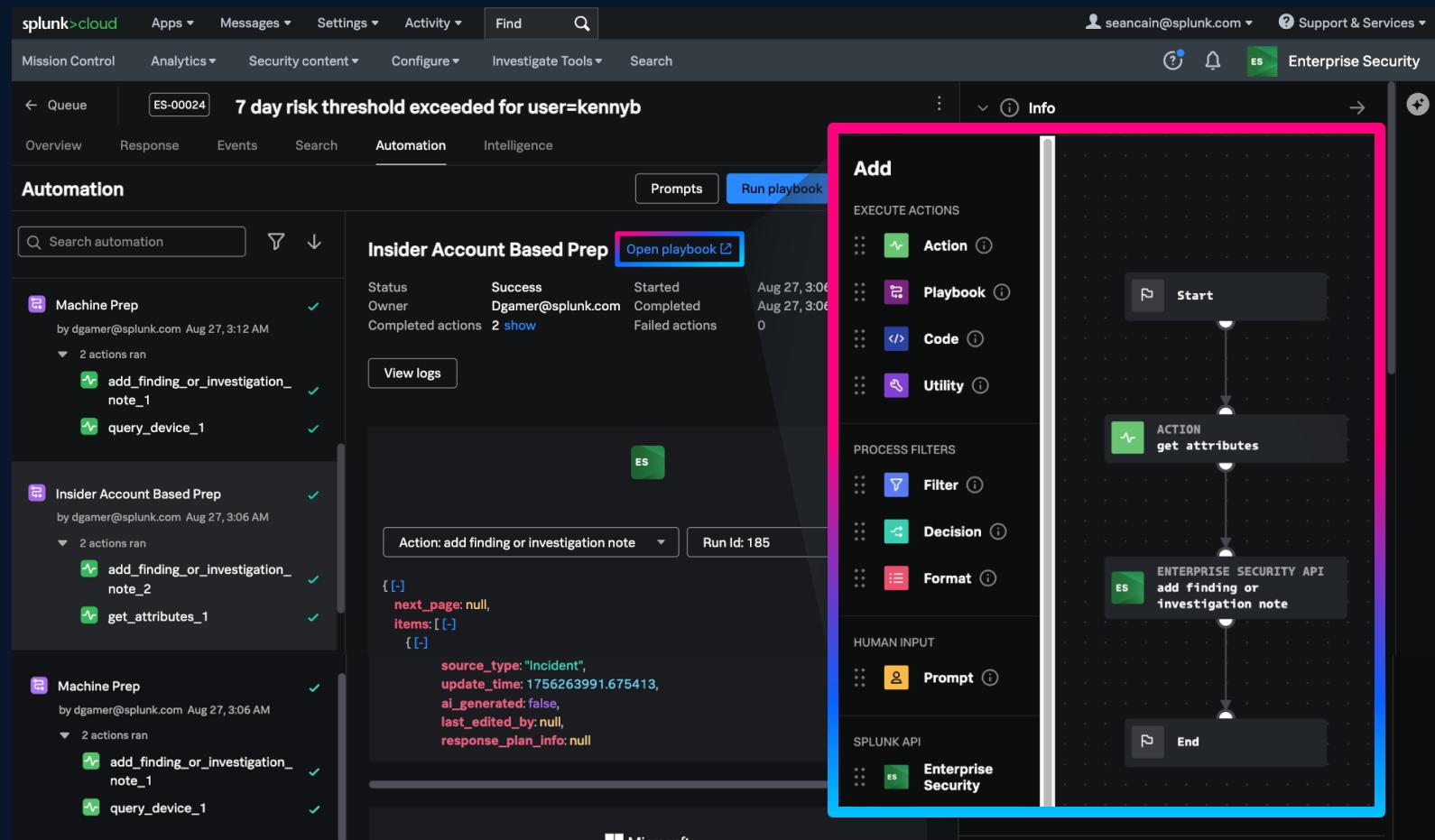
Analyst queue Last 24 hours Saved views Select... Charts Timeline

Time Range: 24 hours 1 2 3 ... 30 Next Show 20

>ID	Type	Entity	Risk...	Fin...	Int...	Time	Disposition	Owner	Urgency
ES-2303	INVESTIGATION	bstoll@splunktshirtcompany.com	420	4	36	Today, 9:42 AM	Undetermined	Marquis Montgomery	Medium
ES-2303	FINDING	bstoll@splunktshirtcompany.com	420	20	20	Today, 9:42 AM	Undetermined	Unassigned	Medium
ES-2303	FINDING	bstoll@splunktshirtcompany.com	420	4	4	Today, 9:42 AM	Undetermined	Unassigned	Low
ES-2303	FINDING	bstoll@splunktshirtcompany.com	420	1	1	Today, 7:21 AM	Undetermined	Unassigned	Medium
ES-2303	FINDING	bstoll@splunktshirtcompany.com	420	1	1	Today, 6:21 AM	Undetermined	Unassigned	Medium
ES-2303	INTERMEDIATE	bstoll@splunktshirtcompany.com	420	10?	10?	Today, 6:21 AM			
172.16.0.149	FINDING	172.16.0.149	140	4	4	Today, 9:40 AM	Undetermined	Unassigned	High
54.230.147.59	FINDING	54.230.147.59	60	2	2	Today, 9:40 AM	Undetermined	Unassigned	Medium
NY_APP_002	FINDING	NY_APP_002	75	11	11	Today, 9:35 AM	Undetermined	Unassigned	Medium
52.216.133.181	FINDING	52.216.133.181	35	5	5	Today, 9:35 AM	Undetermined	Unassigned	Low
52.218.196.122	FINDING	52.218.196.122	20	4	4	Today, 9:27 AM	Undetermined	Unassigned	Low
mickey.perre@splunktshirtcompany.com	INVESTIGATION	mickey.perre@splunktshirtcompany.com	120	6	25	Today, 9:27 AM	Undetermined	Unassigned	High
hayley.jensen@splunktshirtcompany.com	INVESTIGATION	hayley.jensen@splunktshirtcompany.com	150	5	16	Today, 9:23 AM	Undetermined	Unassigned	High
macbook-46743	FINDING	macbook-46743	50	2	2	Today, 9:23 AM	Undetermined	Unassigned	Low
macbook-44591	FINDING	macbook-44591	90	3	3	Today, 9:19 AM	Undetermined	Unassigned	Medium
34.215.24.225	FINDING	34.215.24.225	55	3	3	Today, 9:19 AM	Undetermined	Unassigned	Medium

Deliver the Best Analyst Experience

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



Accelerate the SOC

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.

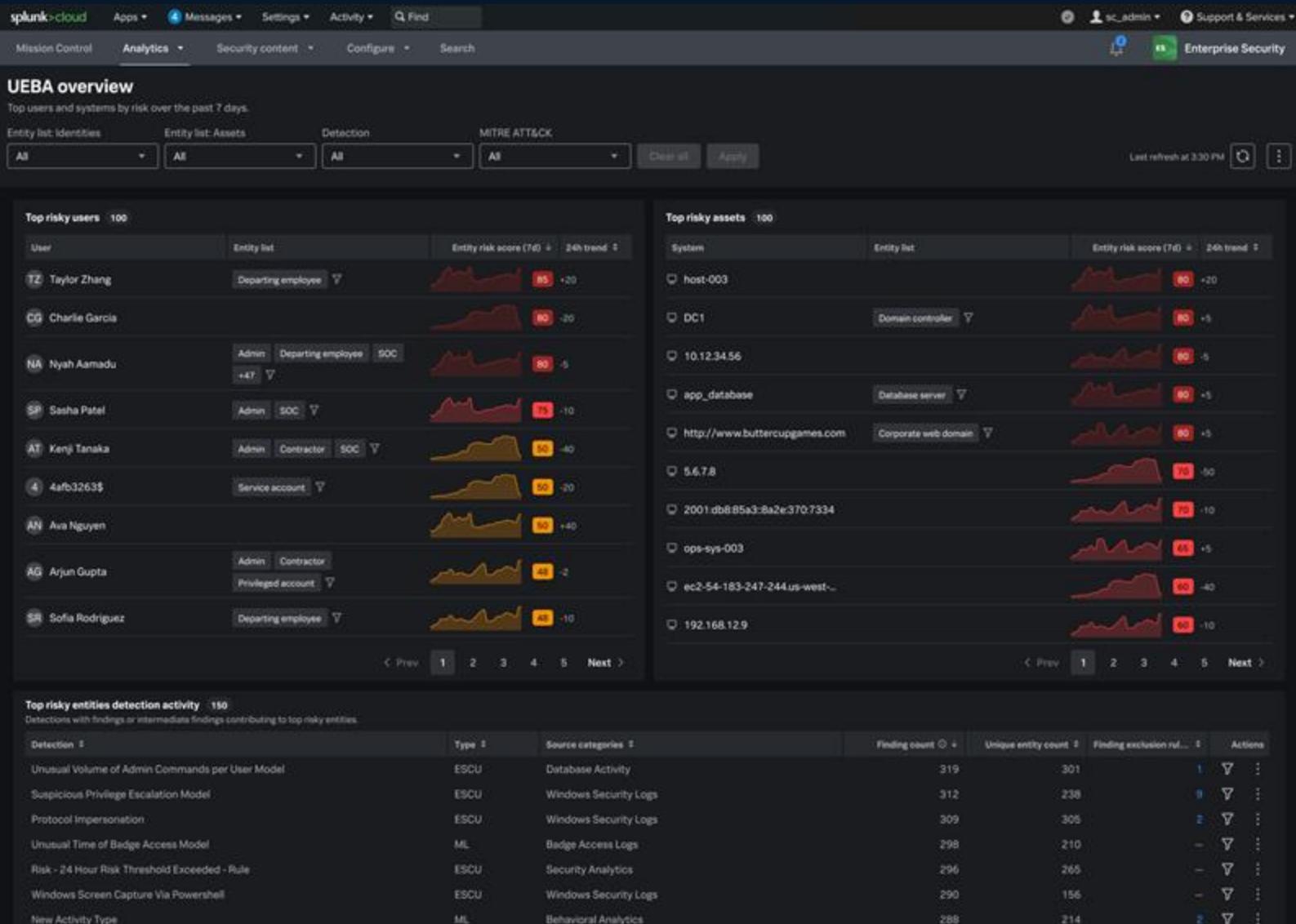
Automation and Response

- 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 SOC interface with three main panels. The left panel shows a list of automation actions: 'user initiated block hash action', 'user initiated quarantine device action', 'user initiated disable user action', 'Risk Auto Containment' (with a sub-action 'get_response_plans_1'), 'user initiated file reputation action' (with a note '1 action failed for app VirusTotal v3'), 'user initiated file reputation action', and 'Encoded Powershell Analysis'. The middle panel is titled 'Malicious PowerShell Process - Encoded Command' and shows a 'user initiated block hash action' with details: Status Success, Owner TDIR Admin, Started Complete, Connector: Carbon Black Response, Hash: 586EF56F4D8963DD546163AC31C865D7, and a note 'Block hash action succeeded. It might take some time'. The right panel is a summary of findings from TDIR Admin on Jan 17, 1:36 PM, with a highlighted section for 'Understanding the Findings' which details a malicious PowerShell process triggered on Jan 09, 2025, involving a Carbon Black connector and a specific hash value.

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.



Any questions?