

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

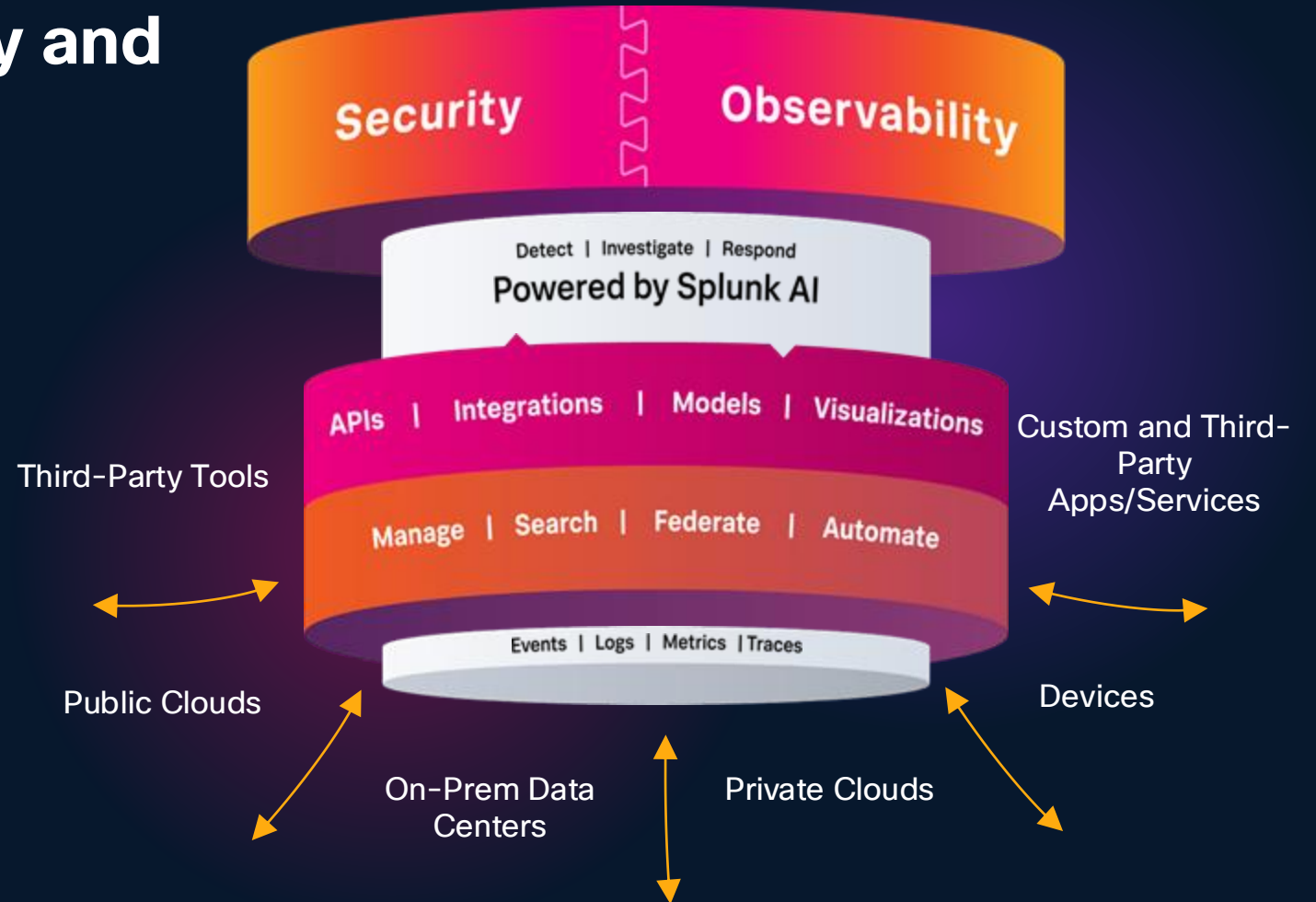
Niklas Blomquist – Strategic Security Advisor



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™

Collections

Apps

Find an app

Submit an app

Log In

Main Page / Apps

Discover Apps

BUILT BY

☐ Splunk

☐ Cisco

☐ Partners

☐ Community

PLATFORM

☒ SPLUNK

> PRODUCT

> VERSION

☐ SPLUNK SOAR


> PRODUCT

> VERSION

Showing 1-21 of 628 Results for security

Sort by New

Filtered by: Splunk



Realm Security Data Pipeline

By Devon Lattrell

The Realm.Security app integrates the full capabilities of the Realm.Security Data Pipeline Platform directly into you...


PLATFORM

Not Available

RATING

☆☆☆☆☆ (0)

DEVELOPER SUPPORTED APP



ITdesign App for One Identity SPP

By ITdesign Software Projects & Consulting GmbH

The ITdesign Safeguard for Privileged Passwords App & Add-On delivers deep visibility into One Identity Safeguard PA...


PLATFORM

Not Available

RATING

★★★★★ (2)

DEVELOPER SUPPORTED APP



Transmit Security Events Add-on for Splunk

By Hai Sadon

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

★★★★★ (2)


DEVELOPER SUPPORTED ADDON



Flashpoint Add-on for Splunk




TA-ollama



Infigo SIEM Content

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



Splunk InfoSec App



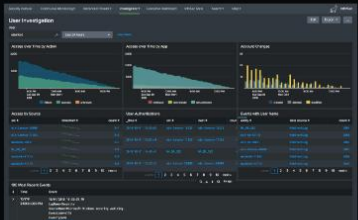
InfoSec App for Splunk

InfoSec app for Splunk is your starter security pack.

Built by [Splunk LLC](#)



Log in to Download



Latest Version 1.7.1

August 1, 2025

[Release notes](#)

Compatibility



Splunk Enterprise, Splunk Cloud
Platform Version: 10.1, 10.0, 9.4, 9.3
CIM Version: 5.X

Rating

5 ★★★★★ (14)

Log in to rate this app

Support

Splunk Supported App

[Learn more](#)

Summary

Details

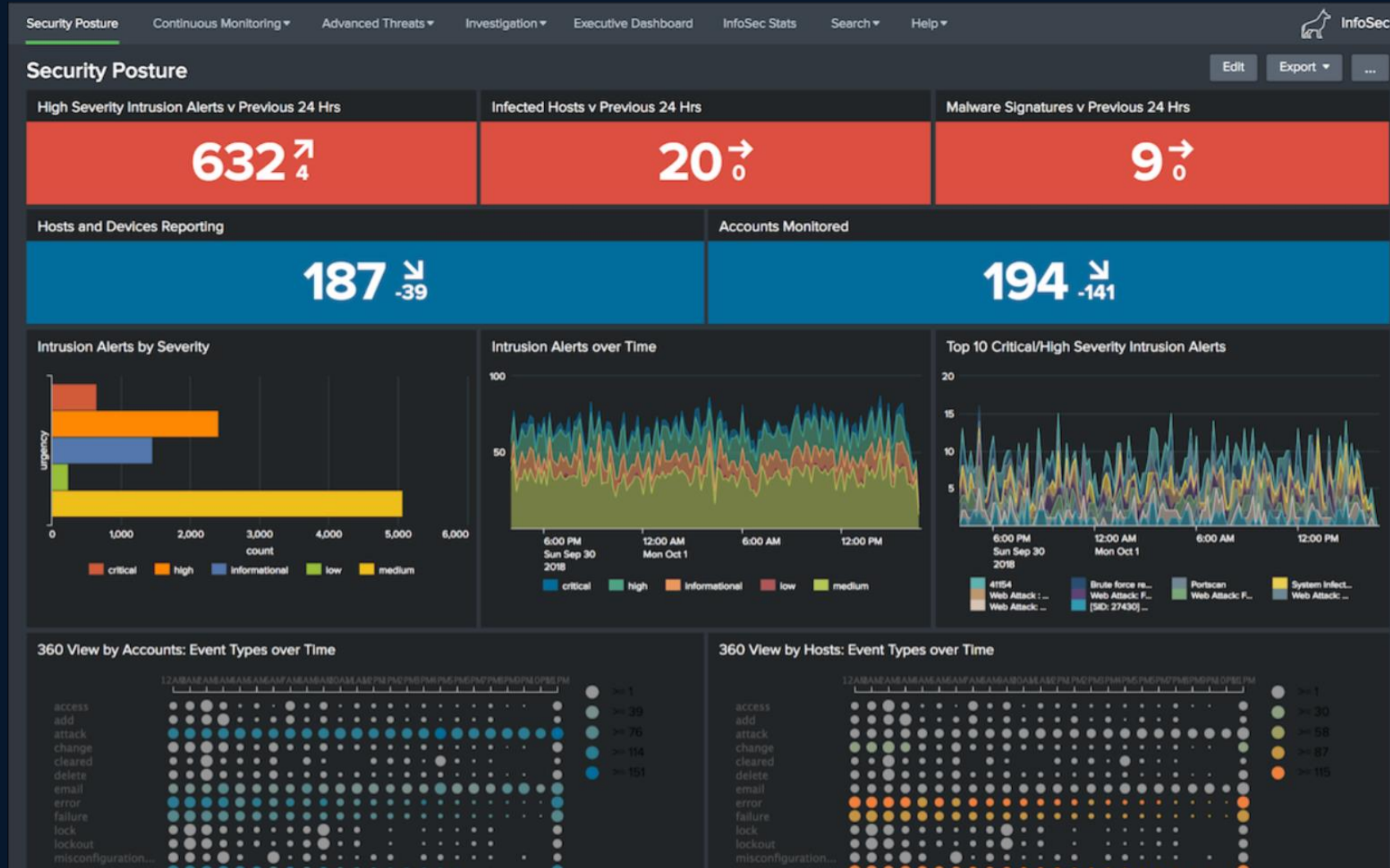
Installation

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 Q


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

Detect Outliers in Bitcoin Transactions

This example uses the Detect Categorical Outliers Assistant on three fields of data that include user and value.

Security

Detect Outliers in Disk Failures

This example uses the Detect Categorical Outliers Assistant on four fields of data that include model and serial number.

IT

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.

Security

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.

IT

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.

Business Analytics

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.

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.

IT

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.

Business Analytics

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

5 ★★★★★ (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.

Write SPL



find all lookup tables



To find all lookup tables in the Splunk environment, we can use the following SPL query:

```
| rest / servicesNS/-/-/data/lookup-table-files
```



in north america



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

Splunk Platform

**Traditional
environments**

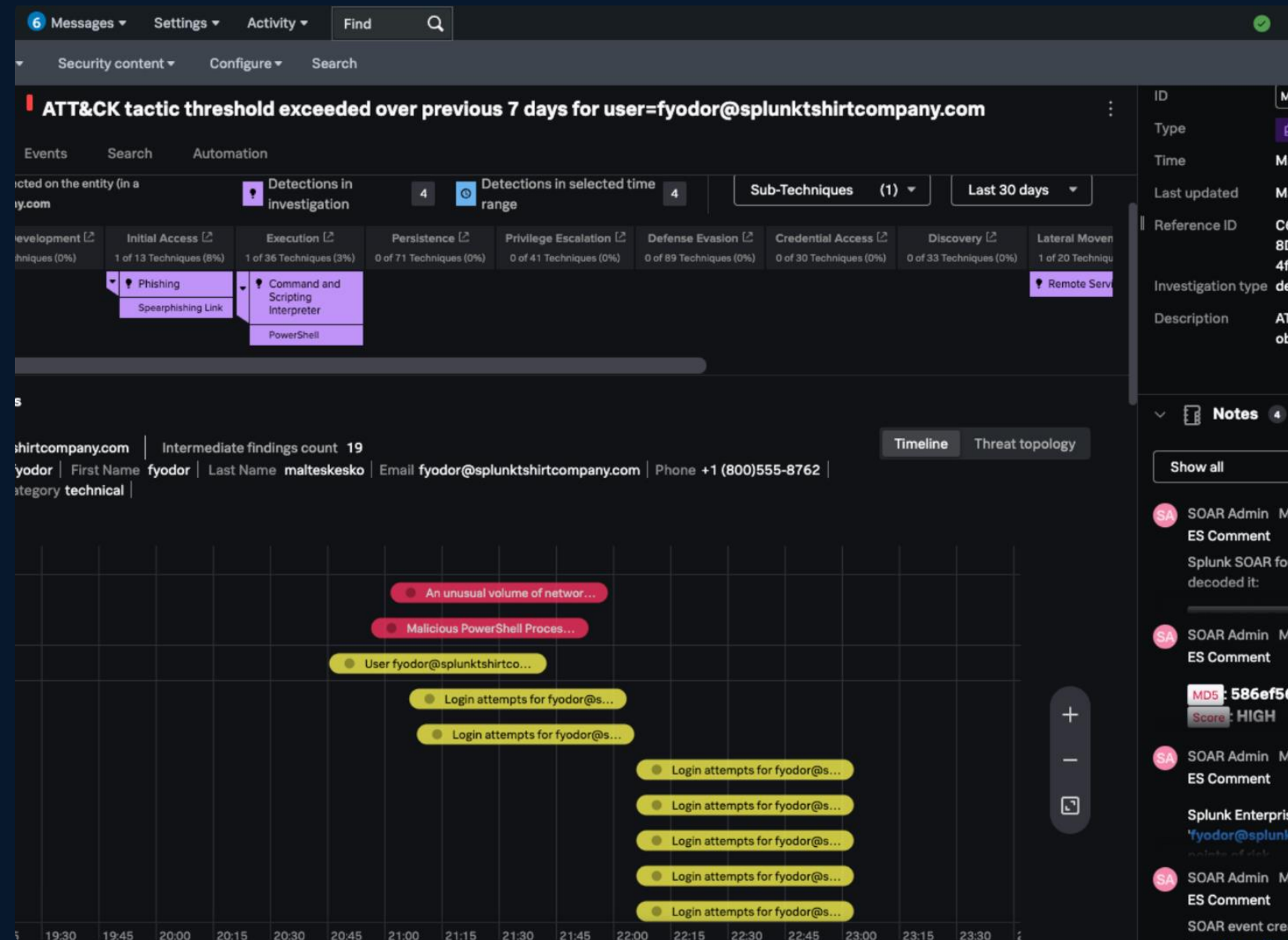
**Cloud native
environments**



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 Agentic across every layer.



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.

The screenshot displays the 'Analyst queue' interface in Splunk Enterprise Security. At the top, there's a search bar for 'Findings and investigations' and a 'Last 24 hours' filter. Below this, a table lists various security events. The table has columns for Title, ID, Type, Entity, Risk score, Findings count, Intensity, Time, Disposition, Owner, and Urgency. The findings are categorized into 'FINDING' (green icon) and 'INTERMEDIATE' (blue icon). Some findings are grouped under 'INVESTIGATION' (purple icon). The table shows a mix of alerts, including 'Excessive failed logins', 'Multiple findings from the same entity', and '24 hour risk threshold exceed for entity'. The risk scores are color-coded: red for high (e.g., 420, 140, 150), yellow for medium (e.g., 70, 60, 75), and green for low (e.g., 35, 20, 55). The urgency levels are also indicated by colored dots: red for high, yellow for medium, and green for low.

Title	ID	Type	Entity	Risk	Fin...	Int...	Time	Disposition	Owner	Urgency
Excessive failed logins		FINDING	win-hp-64861	70		7	Today, 9:45 AM	Undetermined	Unassigned	Medium
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
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
24 hour risk threshold exceeded for entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		4	Today, 9:42 AM	Undetermined	Unassigned	Low
Malicious PowerShell process - encoded command on entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		1	Today, 7:21 AM	Undetermined	Unassigned	Medium
Malicious PowerShell process - encoded command on entity [bstoll@splunkshirtcompany.com]		FINDING	bstoll@splunkshirtcompany.c...	420		1	Today, 6:21 AM	Undetermined	Unassigned	Medium
Intermediate findings		INTERMEDIATE...	bstoll@splunkshirtcompany.c...	420		10?	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
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
Excessive failed logins		FINDING	NY_APP_002	75		11	Today, 9:35 AM	Undetermined	Unassigned	Medium
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
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
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
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
Excessive failed logins		FINDING	macbook-46743	50		2	Today, 9:23 AM	Undetermined	Unassigned	Low
24 hour risk threshold exceed for entity [macbook-44591]		FINDING	macbook-44591	90		3	Today, 9:19 AM	Undetermined	Unassigned	Medium
Unusual volume of network activity detected on 34.215.24.225		FINDING	34.215.24.225	55		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.

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

The screenshot displays the Splunk Cloud Enterprise Security interface. The top navigation bar includes links for Apps, Messages, Settings, Activity, Find, and a search bar. The user is logged in as seancairn@splunk.com. The main content area shows a list of automation workflows under the 'Automation' tab. The 'Insider Account Based Prep' workflow is highlighted, showing its status, owner, and completion details. A 'Run playbook' button is visible. On the right, a 'Playbook Editor' is open, showing a flowchart with steps: 'Start', 'ACTION get attributes', 'ENTERPRISE SECURITY API add finding or investigation note', and 'End'. The 'Add' sidebar on the left lists various action types: Action, Playbook, Code, and Utility. The 'Process Filters' section includes Filter, Decision, and Format. The 'Human Input' section includes Prompt. The 'Splunk API' section includes Enterprise Security.

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 shows the Splunk SOAR Automation interface. At the top, there's a breadcrumb trail: Queue > ES-00010 > Malicious PowerShell Process - Encoded Command. Below this are tabs for Overview, Response, Events, Search, Automation (selected), and Intelligence. The Automation tab has a search bar and a filter icon. A list of automation actions is shown, each with a status icon (green checkmark or red X) and a description. The first action, 'user initiated block hash action', is highlighted. To the right, the details for this action are shown, including the status (Success), owner (TDIR Admin), and connector (Carbon Black Response). A table lists the run details for this action.

RUN ID	CONFIGURATION	NAME	CON
558	carbon black	block hash	Carb

TA TDIR Admin Jan 17, 1:36 PM
Summarize the findings

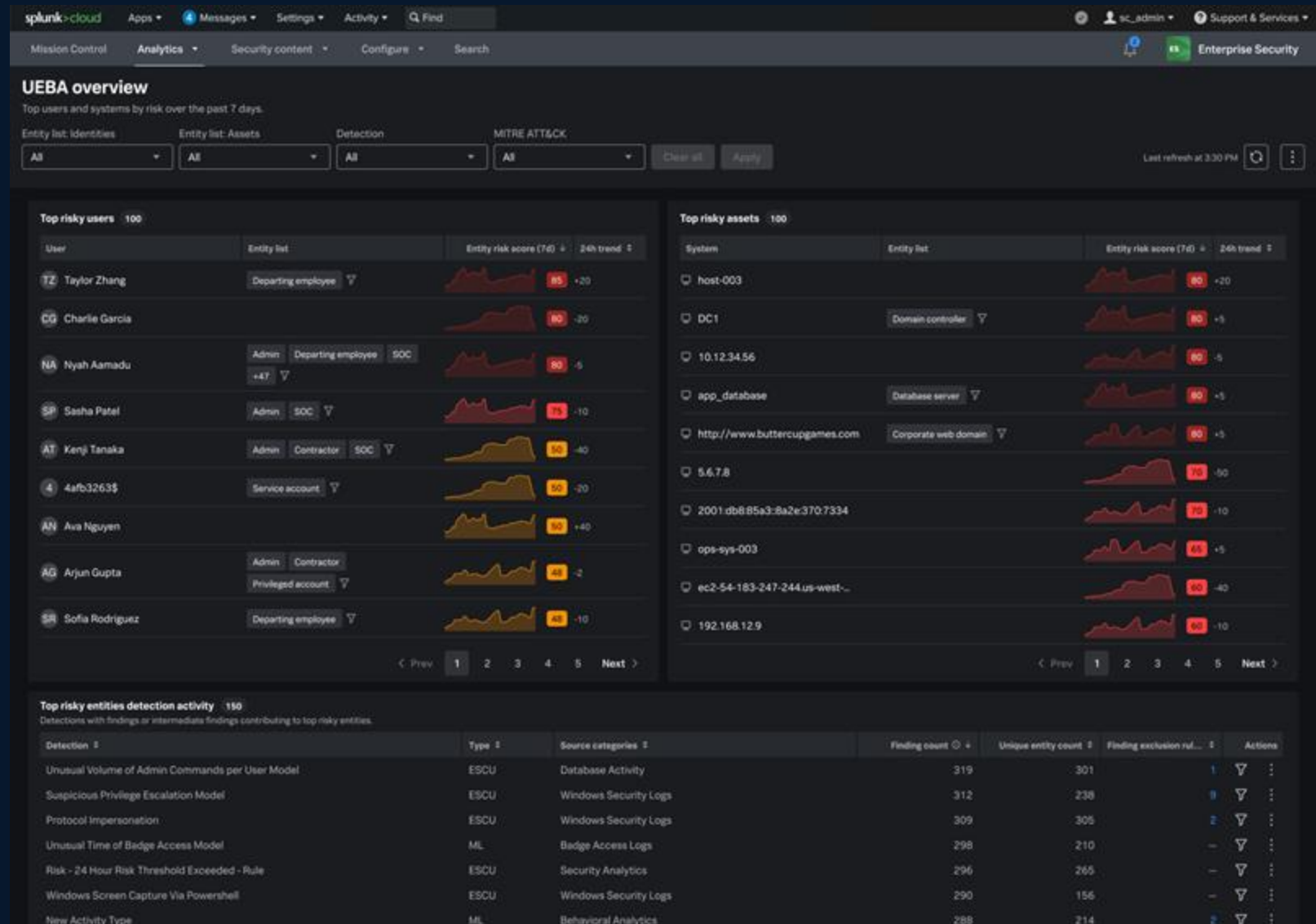
AI Jan 17, 1:37 PM
Understanding the Findings:

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

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?