

Splunk Enterprise Security

A data-centric, modern SIEM solution

splunk > turn data into doing®

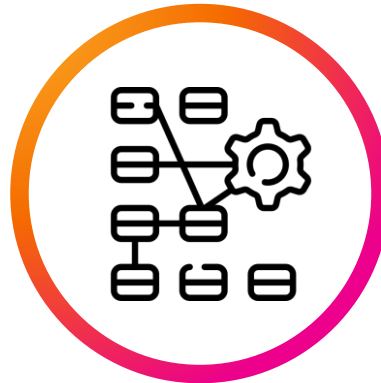




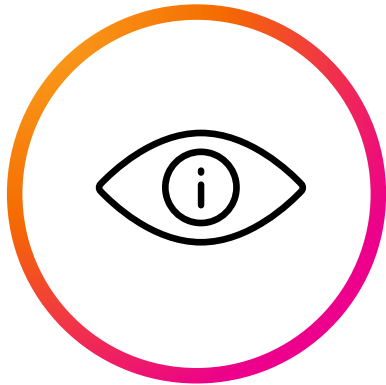
Digital transformation and innovation
often introduces



complexity

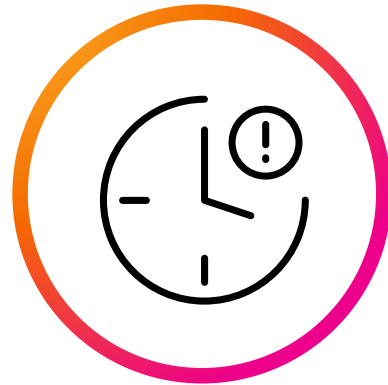


Common Security Challenges



Lack of Visibility

No insight into security posture and risk



Long Dwell Times

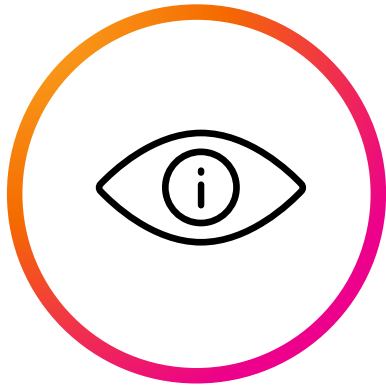
Over 200 days to detect a breach



Lack of Flexibility

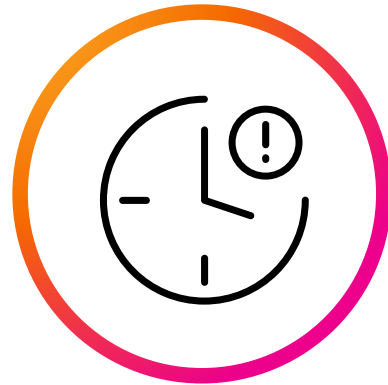
Inability to meet organizational needs

Other SIEM Solutions Fall Short



Lack of Visibility

Limited data ingest
No centralized visibility



Long Dwell Times

Alert fatigue with no prioritization
Slow, incomplete investigations



Lack of Flexibility

Closed ecosystem
Unable to support growth

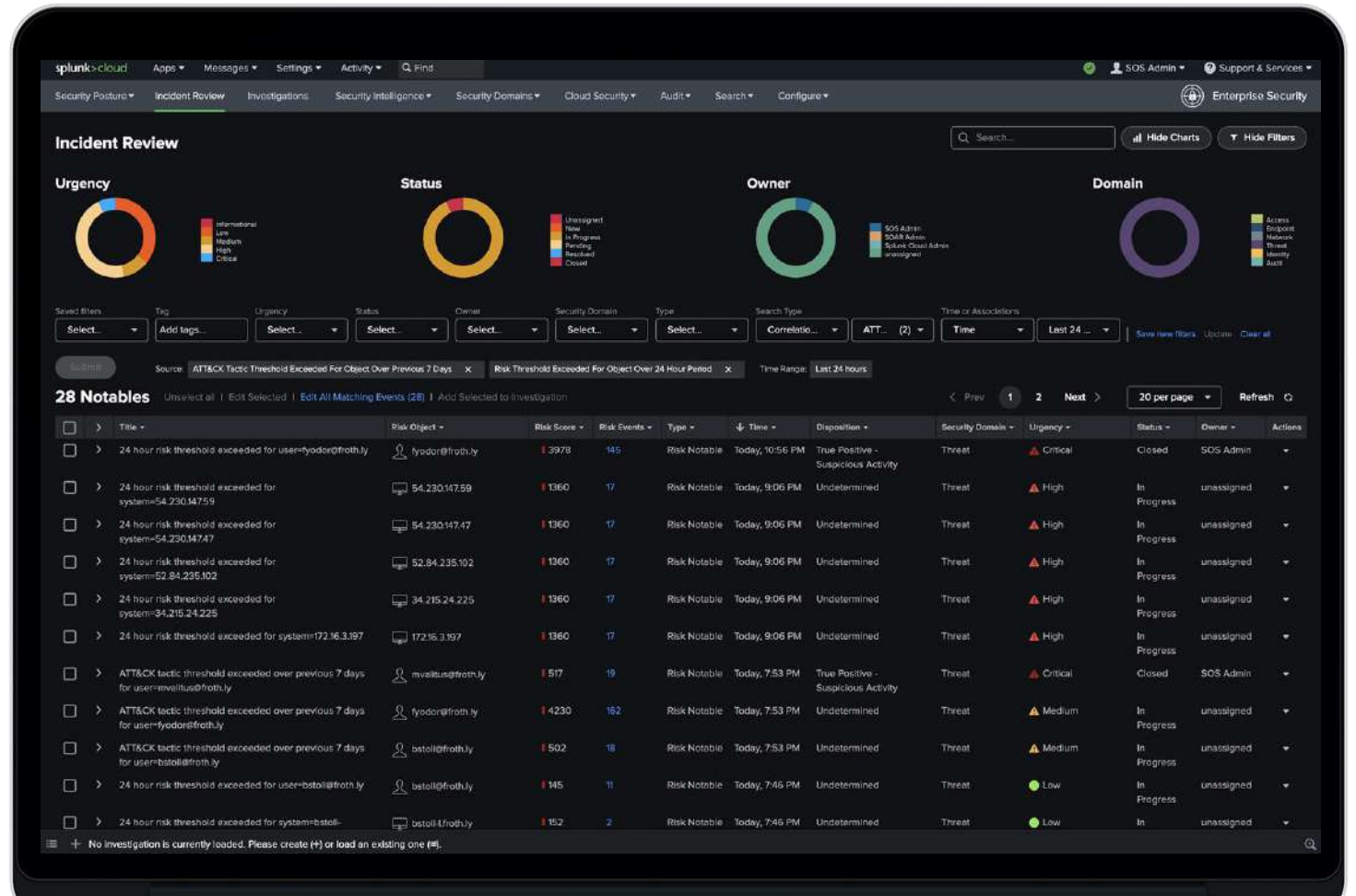


**A Data-Centric,
Modern SIEM** is the
Key to Achieving
**Optimized Security
Operations** and **Cyber
Resiliency**

Splunk Enterprise Security

A data-centric, modern SIEM

- Gain insight into your security posture and investigate with speed and flexibility
- Reduce false positives by up to 80%, detect more sophisticated threats, and align security operations to industry frameworks
- Use pre-built detection and investigation content to more easily secure your AWS, Azure, and Google Cloud Platform data
- Scale to search and monitor terabytes of data per day

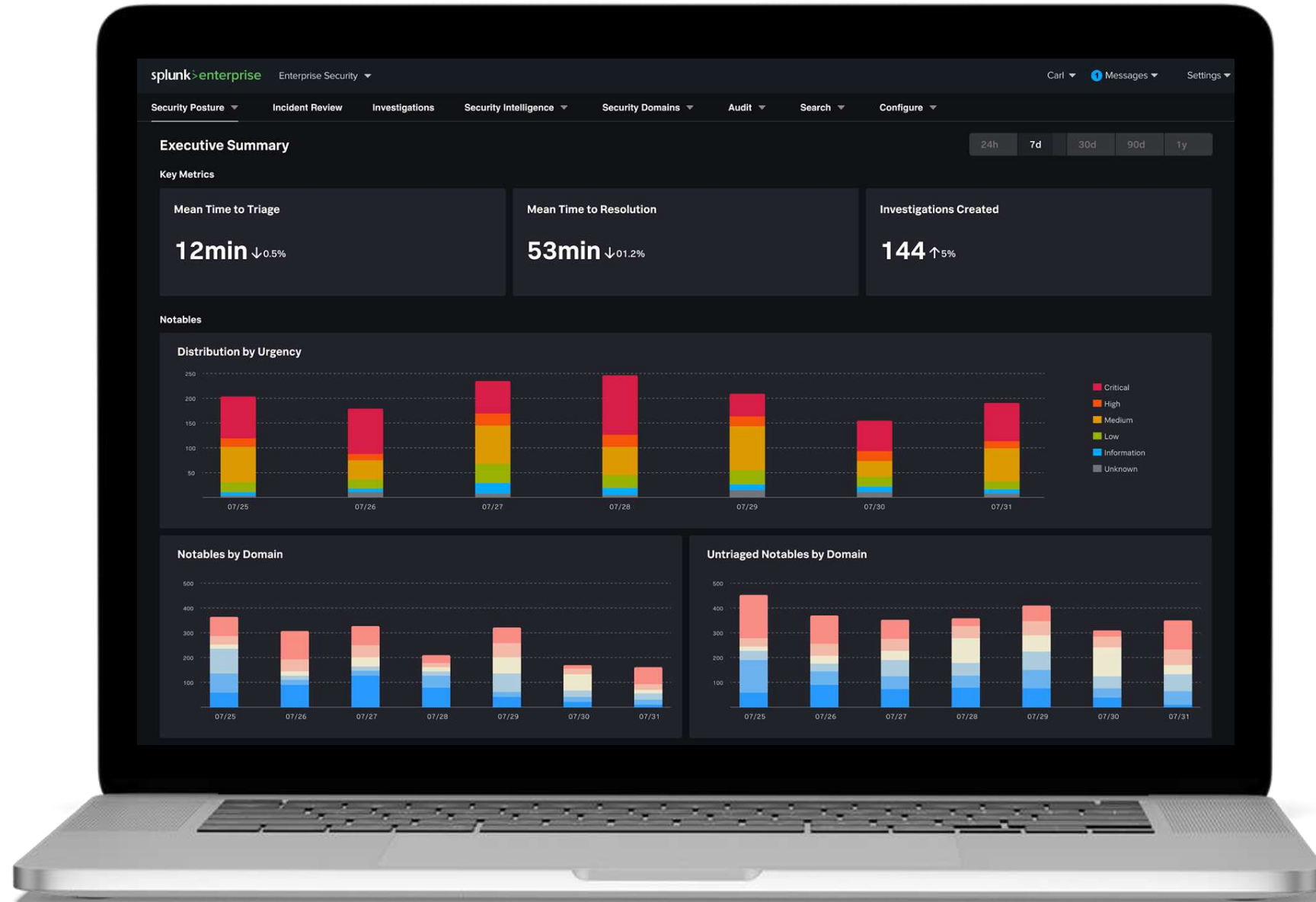




Data-Driven Insights

Full-breadth visibility

- Unlock the ability to ingest, normalize, and gain insights on any data from any source
- Schema-on-read and distributed indexing capabilities ensure fast, flexible investigations
- Perform continuous monitoring with pre-built and customizable dashboards, detections, content, reports, and frameworks
- Search and correlate across cloud, on-premises, or hybrid data sources and deployments

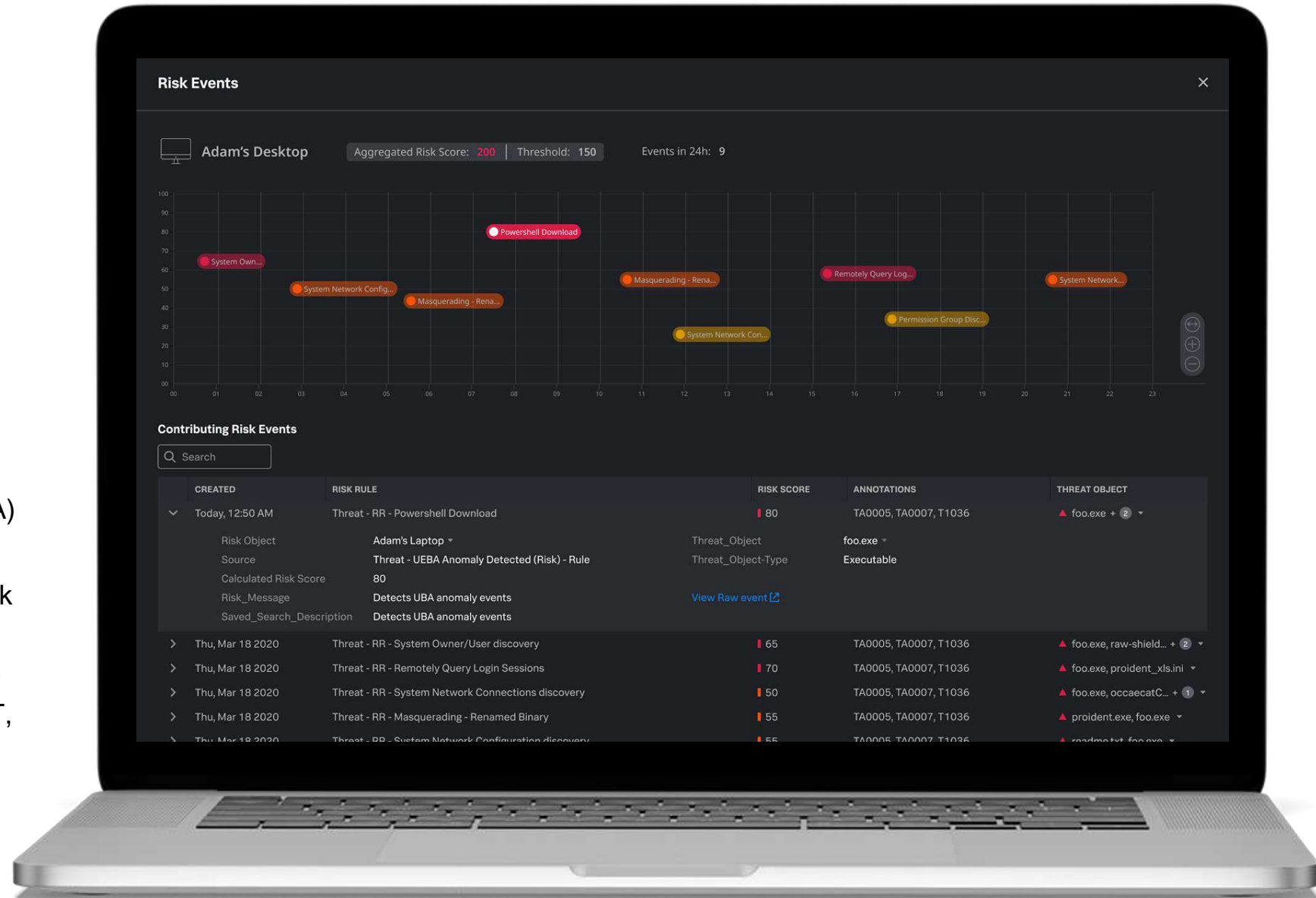




Advanced Analytics

Boost productivity

- 1170+ detections with 100+ cloud-based detections
- 30% increase in true-positive alert rates with Risk-Based Alerting (RBA)
- Enrich and prioritize alerts with integrated threat intelligence (Splunk Intelligence Management)
- Align security operations to industry frameworks (MITRE ATT&CK, NIST, CIS 20, and Kill Chain)
- Dive deep with intuitive search and investigation capabilities

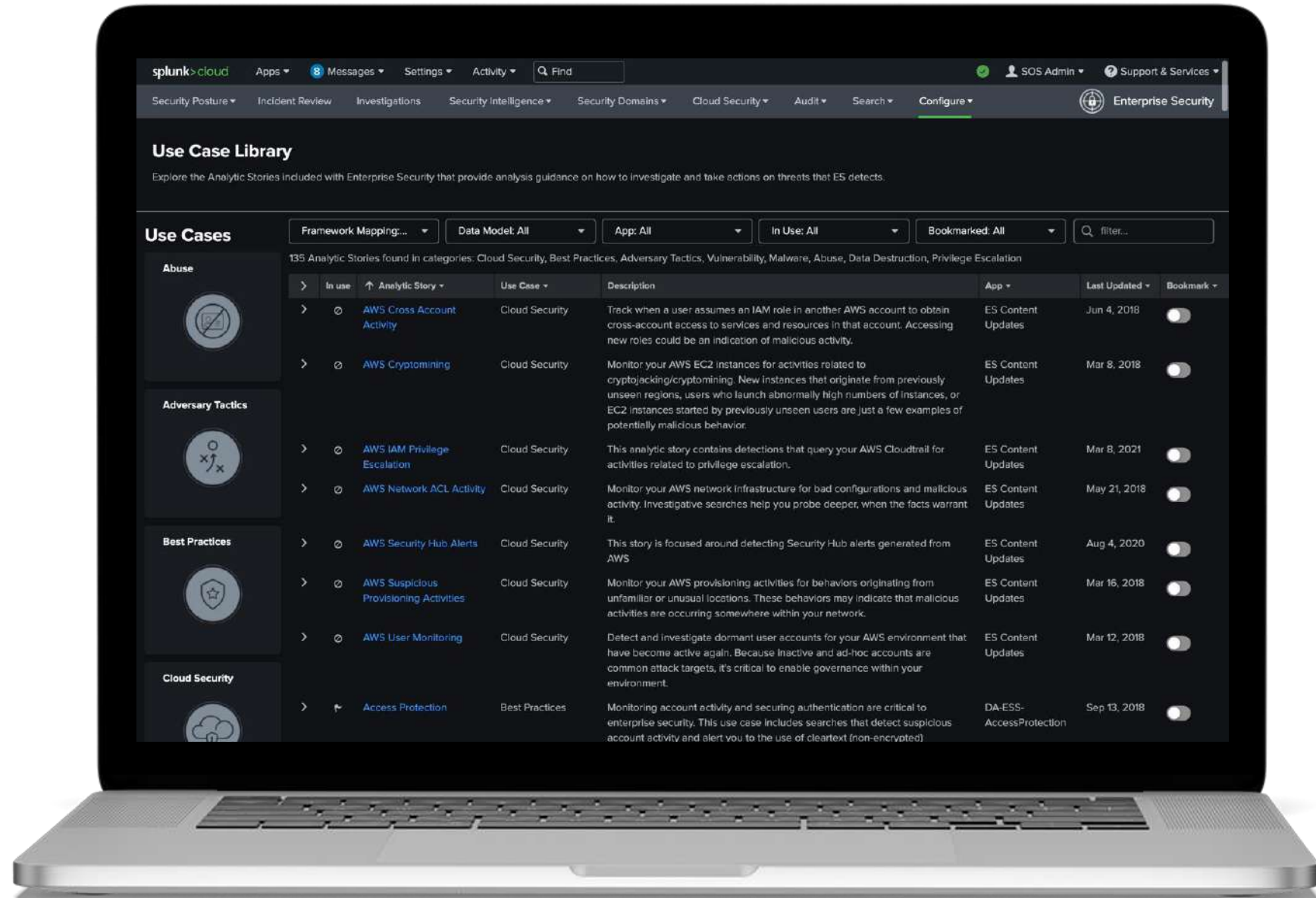




Scale and Flexibility

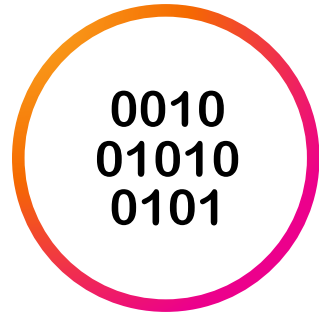
Open and extensible

- Scale to search and monitor terabytes of data per day
- Gather context across your multi-vendor security and IT stack with technology integrations from Splunkbase
- Stay on top of new and emerging threats with automated content delivery from the Splunk Threat Research Team
- Customize and tune pre-built detections, content, frameworks to address what's critical



The Splunk Difference

A data-centric approach to security



Any Data, Any Source

Make disparate data available, queryable, and actionable ¹



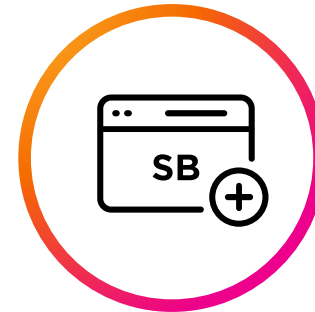
Fast, Flexible Investigations

Achieve 100% compliance and 5x faster security investigations ²



Proven Scalability

Ingest TBs of data per day and perform over 1M searches per week ³



Open Ecosystem

2,800+ integrations to support your best-in-class technology stack ⁴

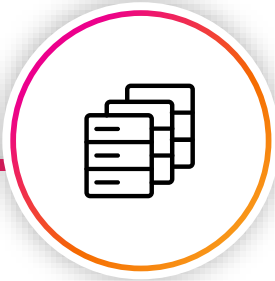


Support for All Deployments

Effectively monitor and secure complex multicloud or hybrid environments ⁵

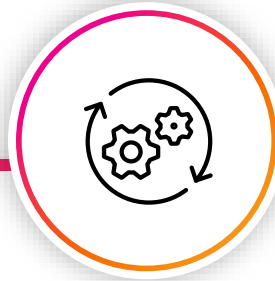
Source 1: Nasdaq customer story
Source 2: Check Point Software customer story
Source 3: Intel customer story
Source 4: Slack customer story & Splunkbase
Source 5: Travis Perkins PLC customer story

What's New in Splunk Enterprise Security 7.1?



Cloud Based Streaming Analytics

Enables scalable, real-time streaming analytics for a broad range of advanced security detections that address common use cases.



Threat Topology

Allows analysts to immediately discover the scope of a security incident and quickly pivot between affected assets and users in the investigation.



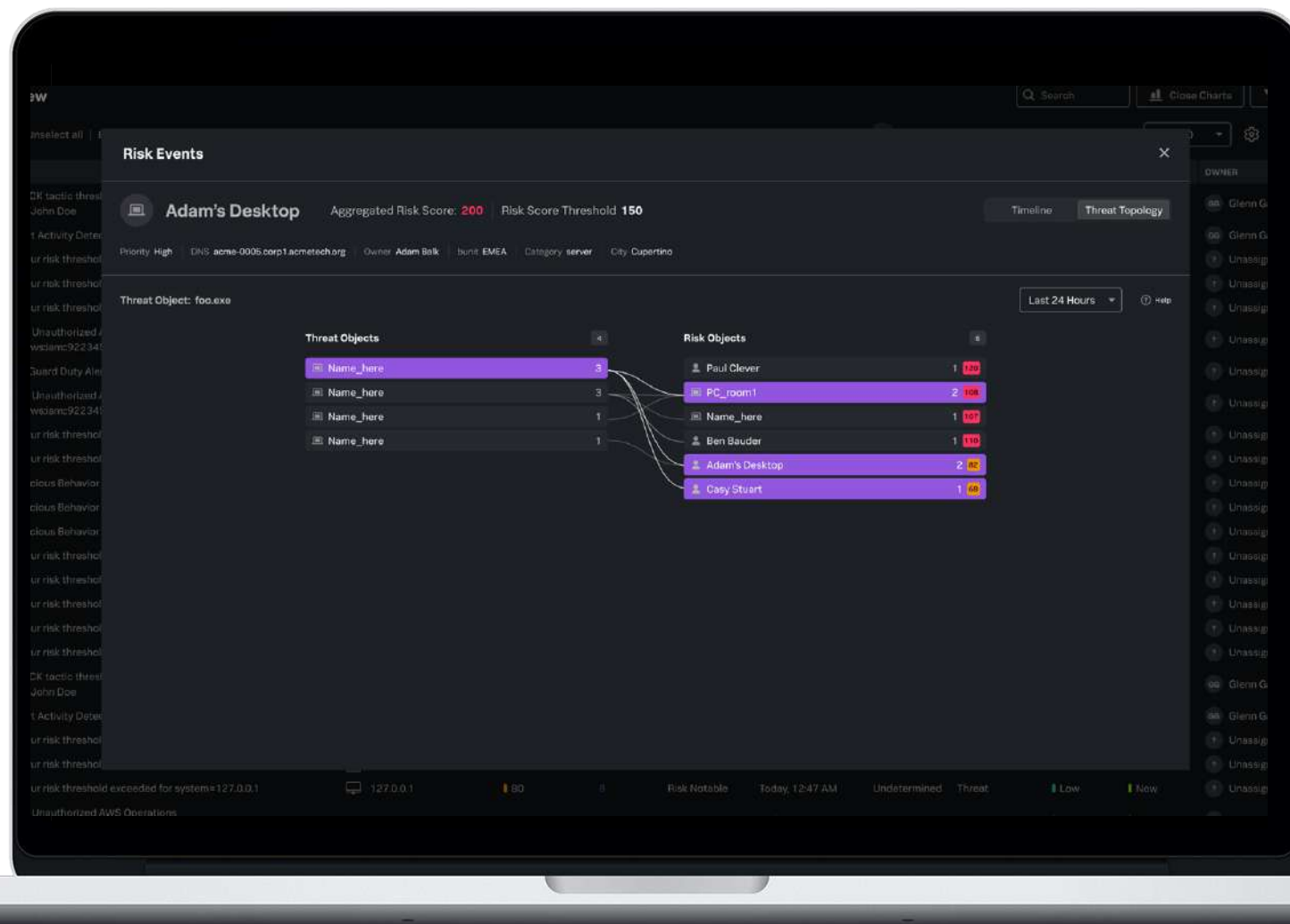
MITRE ATT&CK Framework Matrix

Provides the ability to visualize MITRE ATT&CK tactics and techniques in Risk Notable Events and operationalize the MITRE ATT&CK framework when responding to Notable Events

Quickly Discover the Scope of an Incident to Respond Accurately

Threat Topology Visualization

- Comprehensive view into security incidents
- Quickly determine the severity level of an incident
- Identify additional impacted subjects of an investigation without writing a single line of code or query language



Improve Security Workflow Efficiencies With Embedded Frameworks

MITRE ATT&CK Framework Matrix Visualization

- Visualize MITRE ATT&CK tactics and techniques in Risk Notable Events
- Operationalize the MITRE ATT&CK framework when responding to Notable Events

The screenshot displays the Splunk Enterprise Security interface, specifically the Incident Review section. The top navigation bar includes options like Security Posture, Incident Review, Investigations, Glass Tables, Security Intelligence, Security Domains, Audit, Search, Configure, and SA-Investigatogator. The main content area shows 347 Notables with a table listing incidents. One notable event is expanded to show a MITRE ATT&CK Matrix Visualization for the risk object 'Adam's Desktop'.

TITLE	RISK OBJECT	AGGREGATED RISK	RISK EVENTS	TYPE	CREATED	DISPOSITION	SECURITY DOM
ATT&CK tactic threshold exceeded over previous 7 days for user=John Doe	John Doe	160	9	Risk Notable	Today, 12:51 AM	Undetermined	Threat
Threat Activity Detected (25.204.169.136)	--	--	--	Notable	Today, 12:50 AM	Undetermined	Threat
24 hour risk threshold exceeded for system=Adam's Desktop	Adam's Desktop	410	9	Risk Notable	Today, 12:50 AM	Undetermined	Threat

MITRE ATT&CK Posture for this Notable
The highlighted techniques were detected on the risk object Adam's Desktop

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
<ul style="list-style-type: none"> Gather Victim Identity Information Credentials Employee Names Gather Victim Host Information Client Configurations 		<ul style="list-style-type: none"> Drive-by Compromise Credentials Phishing Spearphishing Attachment Spearphishing Link 		<ul style="list-style-type: none"> Account Manipulation Device Registration Browser Extensions Event Triggered Execution Change Default File Association PowerShell Profile 			<ul style="list-style-type: none"> Brute Force Password cracking Forge Web Credentials Web Cookies 			

Description:
Threat activity (25.204.169.136) was discovered in the "dest" field based on threat intelligence available in the ip_intel collection

Additional Fields

Category	Value	Action
Category	Threat Intelligence	-
Destination	25.204.169.136 45	-
Destination Expected	false	-
Destination PCI Domain	untrust	-
Destination Requires Antivirus	false	-

Related Investigations:
Currently not associated with any investigation.

Correlation Search:
[Threat - Threat List Activity - Rule](#)

History:
[View all review activity for this Notable Event](#)

History:
[View all threat activity involving dests="25.204.169.136"](#)

Integrated Threat Intelligence Enrichment

Splunk is making it even easier for analysts to understand threat context and take action with **Threat Intelligence Management***

SOC Analyst Challenges

Lack of time to to identify related intelligence

Alert Fatigue

Manual Repetitive Tasks

The Solution



Threat Intelligence Management

Gain more context around risk and threats targeting the organization

Reduce noise and surface the highest fidelity intelligence

Simplify security workflows

Uses Cases in Enterprise Security



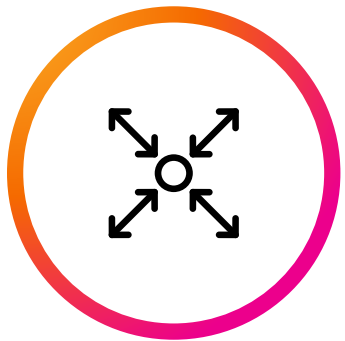
**Security
Monitoring &
Analysis**



**Advanced &
Insider Threat
Detection**



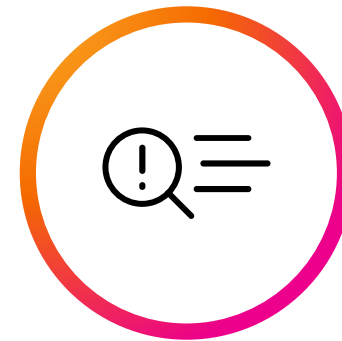
**Incident
Investigation
& Forensics**



**Incident
Response**

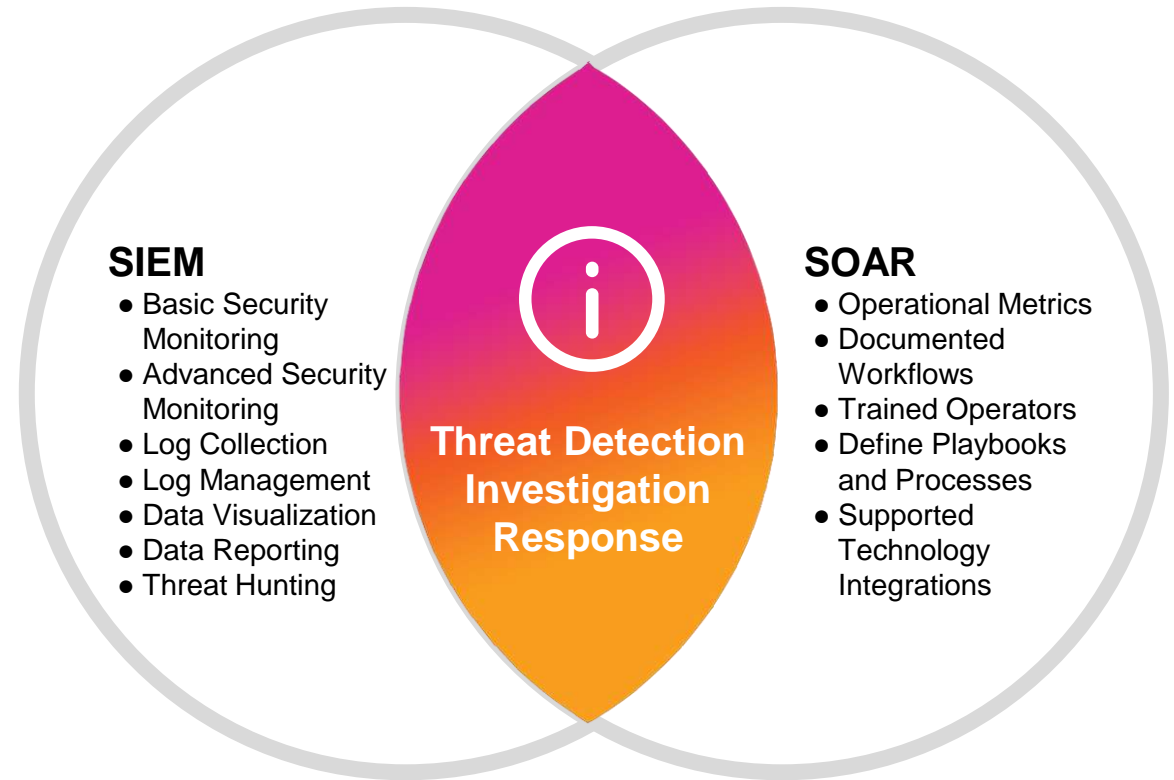


Compliance



**Threat
Hunting**

SIEM & SOAR Merging



[SOAR Will Not Make You Better at Running SIEM](#)

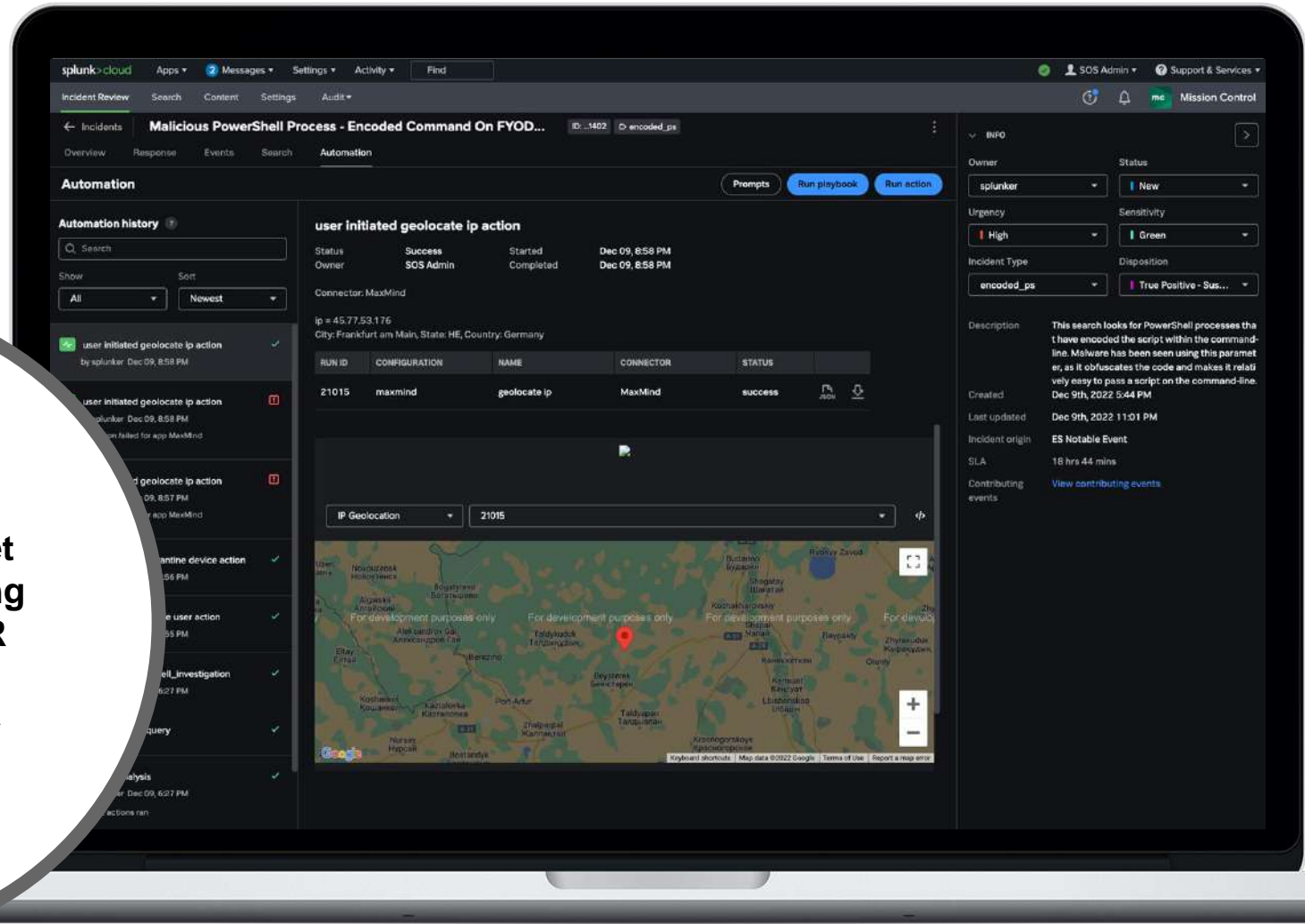
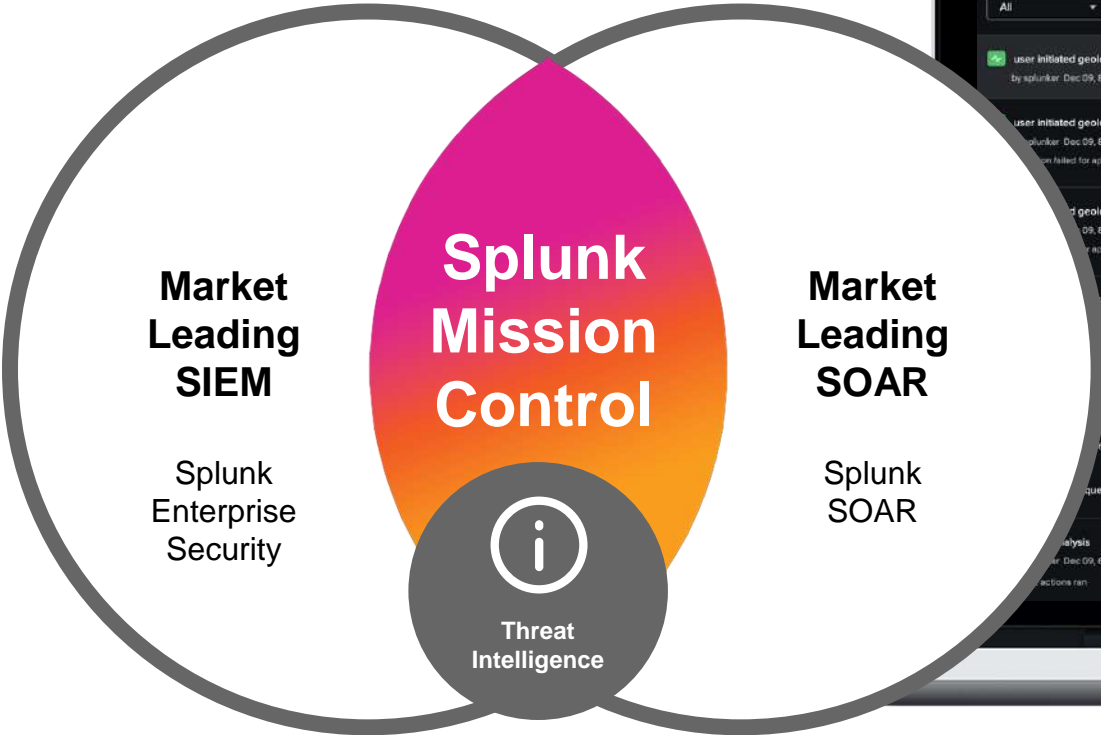
Published 4 May 2022 - ID G00759000

By Analyst(s): AI Price

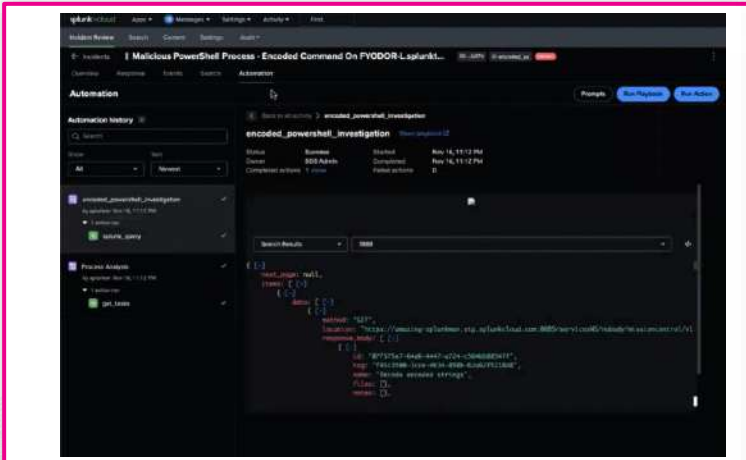


Prepare for Take-off

Unified Security Operations

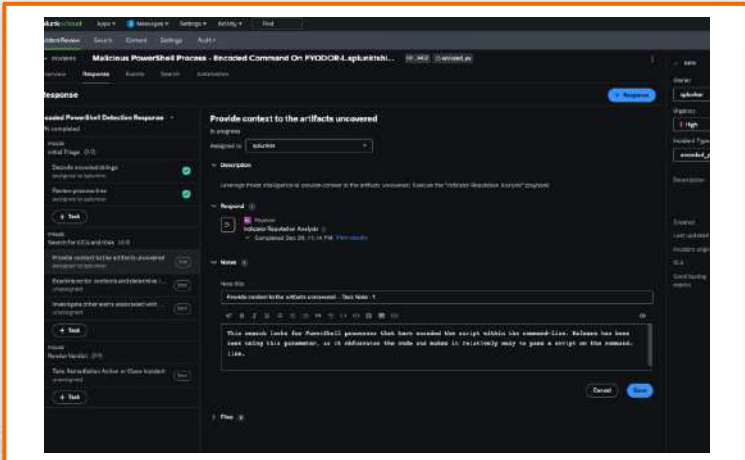


Why Mission Control for Unified Security Operations



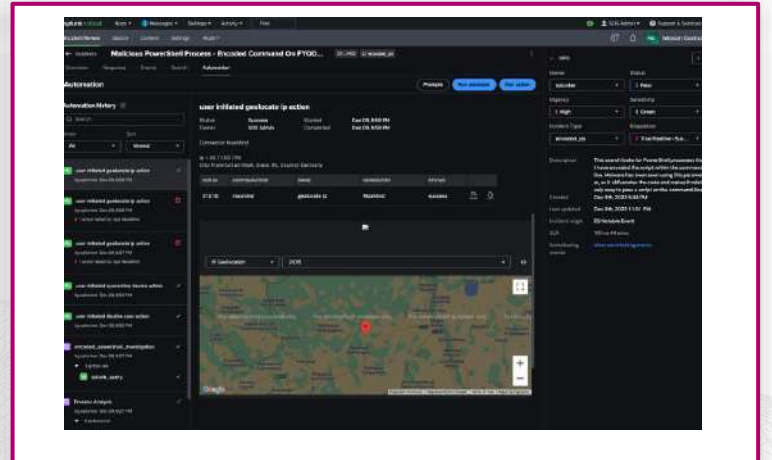
Unify Detection | Investigation | Response Capabilities And Data To Act Based On Prioritized Insights

UNIFY



Simplify your security workflows by codifying your processes into response templates

SIMPLIFY



Modernize and empower your security operations with the speed of security automation

MODERNIZE

Splunk Is a Global Leader in SIEM

Gartner

Nine-Time Leader

2022 Gartner Magic Quadrant for SIEM

#1 in Market Share

2021 Gartner Market Share Report for SIEM

FORRESTER

Leader

Forrester Wave™: Security Analytics Platforms, Q4 2022

IDC

Leader

IDC MarketScape: Worldwide SIEM 2022 Vendor Assessment

#1 in Market Share

IDC Worldwide SIEM Market Share Report

SC MEDIA

Best SIEM Solution

2022 Trust Awards

TrustRadius

**Best Feature Set
Best Relationship**

2022 Best of Awards

Trusted by over 90 of the Fortune 100

TESCO



Coca-Cola



BOSCH

United States
Census
Bureau

ANZ

splunk>