Splunk Enterprise Security

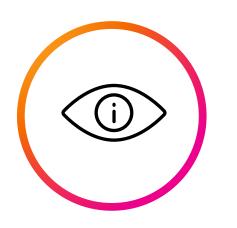
A data-centric, modern SIEM solution





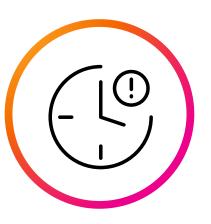


Common Security Challenges



Lack of Visibility

No insight into security posture and risk



Long Dwell Times

Over 200 days to detect a breach

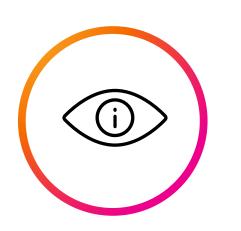


Lack of Flexibility

Inability to meet organizational needs

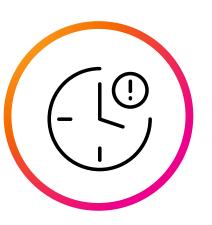


Other SIEM Solutions Fall Short



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

		Q Find								👤 SOS Admin 🕶		
Security Postu	ara V Incident Roview Investigations Security I	ntelligence • Security Don	nains • Cloud	Security *	Audit • Se	arch • Config	uro v			¢	Enterpris	e Security
Incident	Review							Q Search		II Hide Cha	rts 🔍 🔻 Hk	de Filters
Urgency		Status				Owner			Do	main		
	attriational		Livesup1	ent.						-		Access
	Low Health		Talw In Progra Pariding Residued				SOS Admin SDAR Admin Splank Caud uransigned	Admin				Encpoint Network Threat Identity
		\sim	Crossed				/			\sim		Aut
Saved filters	Teg Grgency Sate	. Owner	Security D	omain	Туре	Search Type		Time or Associations				
Select	Add tags. Select. * Select.	ect Select	✓ Select	L	Select	* Correlati	s ▼] ATT (2) ▼	Time -	Last 24 🔻		G Ubilant Cha	
(1.00mit i)	Source AFT&CK Tactic Threshold Exceeded For Object 0	ver Previous 7 Days X Risk	Threshold Exceeded I	For Object Over :	24 Hour Period	X Time Range:	Last 24 hours					
28 Nota	bles Unselected 1 Edit Selected 1 Edit All Matching	Events (28) 1 Add Selected to							2 Next >	20 per pag	e 🛩 Ref	resh O
		Risk Object -	Risk Score -	Risk Events -	Type -	↓ Time -	Disposition •	Security Domain +	Urgency +	Status -	Owner -	Actions
	24 hour risk threshold exceeded for user=fyodor@froth.ly	<u><u>R</u> lyodor@froth.ly</u>	3978		Risk Notable	Today, 10:56 PM	True Positive - Suspicious Activity	Tryeat	Critical	Closed	505 Admin	
	24 hour risk threshold exceeded for system=54.230.14759	54.230.147.59	1360		Risk Notable	Today, 9:06 PM		Threat	🛕 High	in Progress	unassigned	
\square	24 hour risk threshold exceeded for	54.230.147.47	11360		NUMBER OF STREET	Today, 9:06 PM	Visit Contractor				unassigned	
-	system-54.230.147.47				MISK NOTBOIE	ioday, 9:06 PM	Ondetermined	Threat	High	In Progress	unassigned.	
	system=54.230.147.47 24 hour risk threshold exceeded for system=52.84.235.102		1360			Today, 9:06 PM		Threat Threat	▲ High		unassigned	
	system-54.230.147.47 24 hour risk threshold exceeded for				Risk Notable		Undetermined			Progress In		
	system=54.230.14747 24 hour risk threshold exceeded for system=52.84.235.102 24 hour risk threshold exceeded for	52.84.235.102	1360		Risk Noteble Risk Notable	Today, 9:06 PM	Undetermined Undetermined	Threat	A High	Progress In Progress In	unassigned	
	system=54.230.14747 24 hour risk threshold exceeded for system=52.84.235.102 24 hour risk threshold exceeded for system=34.215.24.225	💭 52.84.235.102	1360 1360		Risk Notable Risk Notable Risk Notable	Today, 9:06 PM Today, 9:06 PM	Undetermined Undetermined Undetermined	Threat Threat	A High	Progress In Progress In Progress In	unassigned unassigned	
	system=54.230.147.47 24 hour risk threshold exceeded for system=52.84.235.02 24 hour risk threshold exceeded for system=34.215.24.225 24 hour risk threshold exceeded for system=172.16.3.197 ATT&CK texts: threshold exceeded over previous 7 days	- 52.84.235.102 - 34.215.24.225 - 17236.3397	1 1360 1 1360 1 1360		Risk Notable Risk Notable Risk Notable Risk Notable	Today, 9:06 PM Today, 9:06 PM Today, 9:06 PM	Undetermined Undetermined Undetermined True Positive - Suspicious Activity	Threat Threat Threat	▲ High ▲ High ▲ High	Progress In Progress In Progress In Progress	unessigned unassigned unassigned	
	system=54.230.147.47 24 hour risk threshold exceeded for system=52.84.235.102 24 hour risk threshold exceeded for system=34.215.24.225 24 hour risk threshold exceeded for system=172.16.3.197 ATT&CK tactic threshold exceeded over previous 7 days for user=mvailtus@froth.ty ATT&CK tactic threshold exceeded over previous 7 days	- 52.84.235.102 34.215.24.225 172.16.3.937 & musikusegironn.ly	1360 1360 1360 1360 517		Risk Notable Risk Notable Risk Notable Risk Notable Risk Notable	Today, 9:06 PM Today, 9:06 PM Today, 9:06 PM Today, 7:53 PM	Undetermined Undetermined Undetermined True Positive - Suspicious Activity Undetermined	Threat Threat Threat Threat	High High High High Critical	Progress In Progress In Progress Clased In	unassigned unassigned unassigned SOS Admin	
	system=54.230.147.47 24 hour risk threshold exceeded for system=52.84.235.052 24 hour risk threshold exceeded for system=34.215.24.225 24 hour risk threshold exceeded for system=172.16.3.397 ATT&CK textic threshold exceeded over previous 7 days for user=mevidus@hoth.ly ATT&CK textic threshold exceeded over previous 7 days for user=forder#etMay ATT&CK textic threshold exceeded over previous 7 days		1360 1360 1360 517 4230		Risk Notable Risk Notable Risk Notable Risk Notable Risk Notable	Today, 9:06 PM Today, 9:06 PM Today, 9:06 PM Today, 7:53 PM Today, 7:53 PM	Undetermined Undetermined Undetermined True Positive - Suspicious Activity Undetermined Undetermined	Threat Threat Threat Threat Threat	High High High Gritical Kedium	Progress In Progress In Progress Closed In Progress In Progress In	unassigned unassigned unassigned SOS Admin unassigned	
	system=54.230.147.47 24 hour risk threshold exceeded for system=52.48.4365.102 24 hour risk threshold exceeded for system=34.215.24.225 24 hour risk threshold exceeded for system=172.16.3397 ATT&CK tactic threshold exceeded over previous 7 days for user=inveitus8/hoth.ly ATT&CK teatic threshold exceeded over previous 7 days for user=fivide/soft-fiber- tor user=fivide/soft-fiber- ATT&CK teatic threshold exceeded over previous 7 days for user=fivide/soft-fiber- ATT&CK teatic threshold exceeded over previous 7 days for user=fivide/soft-fiber- ATT&CK teatic threshold exceeded over previous 7 days for user=fiber-fiber-fiber- for user=fiber-fiber-fiber- for user=fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber- fiber-fiber-fiber-fiber-fiber-fiber-fiber-fiber- fiber-fib	- 52.84.235.102 - 54.215.24.225 - 172.16.3.937 - musiture@froth.ly - fyodor@froth.ly - fyodor@froth.ly - stoll@froth.ly	1360 1360 1360 517 4230 502		Risk Notable Risk Notable Risk Notable Risk Notable Risk Notable Risk Notable	Today, 9:06 PM Today, 9:06 PM Today, 9:06 PM Today, 7:53 PM Today, 7:53 PM	Undetermined Undetermined Undetermined True Pasitive - Suspicious Activity Undetermined Undetermined Undetermined	Threat Threat Threat Threat Threat	A High High High Critical Critical Medium	Progress In Progress In Progress Clased In Progress In Progress	unassigned unassigned SOS Admin unassigned unassigned	
	system=54.230.147.47 24 hour risk threshold exceeded for system=52.84.235.04 24 hour risk teneshold exceeded for system=34.215.24.225 24 hour risk threshold exceeded over previous 7 days for user=meditus@hoth.ly ATT&CK tactic threshold exceeded over previous 7 days for user=hydoin8feeth.ly ATT&CK tactic threshold exceeded over previous 7 days for user=hydoin8feeth.ly	52.84.235.102 34.215.24.225 172.15.3.997 2. hyodorafroth ly 3. obtolit/froth.ly 2. bstolit/froth.ly 3. bstolit/froth.ly 2. bstolit/froth.ly 3. bstolit/froth.ly	1360 1360 1360 517 4230 502 145		Risk Notable Risk Notable Risk Notable Risk Notable Risk Notable Risk Notable	Today, 9:06 PM Today, 9:06 PM Today, 9:06 PM Today, 7:53 PM Today, 7:53 PM Today, 7:53 PM	Undetermined Undetermined Undetermined True Pasitive - Suspicious Activity Undetermined Undetermined Undetermined	Threat Threat Threat Threat Threat Threat	High High High High Gritical Hiddum Hiddum Low	Progress In Progress In Progress Closed In Progress In Progress In Progress In Progress	unassigned unassigned unassigned unassigned unassigned	

Data-Driven Insights

Full-breadth visibility

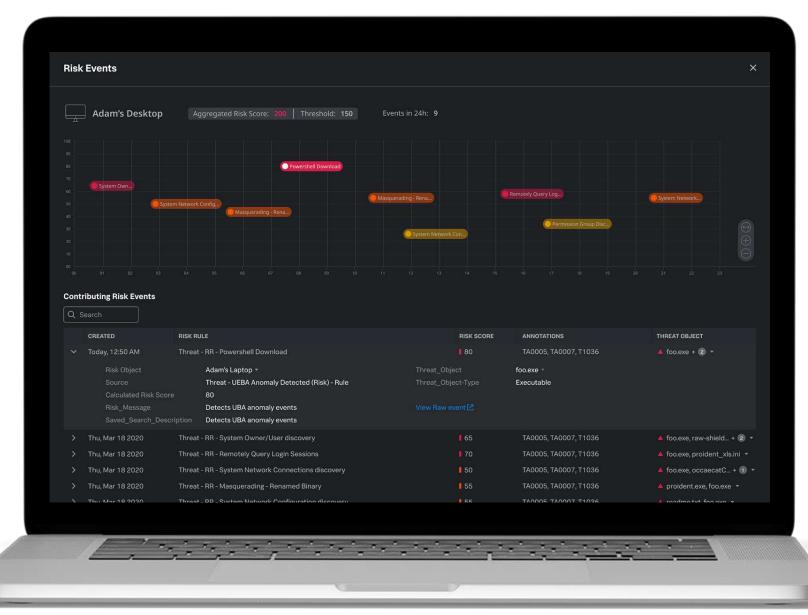
- Unlock the ability to ingest, normalize, and gain insights on any data from any source
- Schema-on-read and distributed indexing capabilities ensure fast, flexible investigations
- Perform continuous monitoring with pre-built and customizable dashboards, detections, content, reports, and frameworks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



Advanced Analytics

Boost productivity

- 1170+ detections with 100+ cloudbased 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 multivendor 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

splunk>cloud	Apps 🕶	8 Messages •	Settings •	Activity 🕶	Q Find					0	1 SOS Admin •	Support & Services •
Security Posture •	Incident R	eview Investiga	ations Se	curity Inteilige	nce • Security	Domains *	Cloud Security *	Audit 🕶	Search *	Configure •	Ċ	Enterprise Security

Use Case Library

Explore the Analytic Stories included with Enterprise Security that provide analysis guidance on how to investigate and take actions on threats that ES detects.

Use Cases		ork Mapping V	0.10.0.0	App: All		Q, filter	
Abuse				ices, Adversary Tactics, Vulnerability, Malware, Abuse, Data Destruction, Privilege			
	> In us	ae ↑ Analytic Story -	Use Case -	Description	Арр -	Last Updated +	Bookr
	> o	AWS Cross Account Activity	Cloud Security	Track when a user assumes an IAM role in another AWS account to obtain cross-account access to services and resources in that account. Accessing new roles could be an indication of malicious activity.	ES Content Updates	Jun 4, 2018	
Adversary Tactics	> 0	AWS Cryptomining	Cloud Security	Monitor your AWS EC2 instances for activities related to cryptojacking/cryptomining. New instances thet originate from previously unseen regions, users who launch abnormally high numbers of instances, or EC2 instances started by previously unseen users are just a few examples of potentially malicious behavior.	ES Content Updates	Mar 8, 2018	•
×Ĵ×	> o	AWS IAM Privilege Escalation	Cloud Security	This analytic story contains detections that query your AWS Cloudtrail for activities related to privilege escalation.	ES Content Updates	Mar 8, 2021	0
	> o	AWS Network ACL Act	livity Cloud Security	Monitor your AWS network infrastructure for bad configurations and malicious activity. Investigative searches help you probe deeper, when the facts warrant it.		May 21, 2018	•
Best Practices	> o	AWS Security Hub Aler	rts Cloud Security	This story is focused around detecting Security Hub alerts generated from AWS	ES Content Updates	Aug 4, 2020	•
	> o	AW5 Suspicious Provisioning Activities	Cloud Security	Monitor your AWS provisioning activities for behaviors originating from unfamiliar or unusual locations. These behaviors may indicate that malicious activities are occurring somewhere within your network.	ES Content Updates	Mar 16, 2018	•
Cloud Security	> o		Cloud Security	Detect and investigate dormant user accounts for your AWS environment that have become active again. Because inactive and ad-hoc accounts are common attack targets, it's critical to enable governance within your environment.	ES Content Updates	Mar 12, 2018	0
	۰ <	Access Protection	Best Practices	Monitoring account activity and securing authentication are critical to enterprise security. This use case includes searches that detect suspicious account activity and alert you to the use of cleantext (non-encrypted)	DA-ESS- AccessProtection	Sep 13, 2018	•

The Splunk Difference

A data-centric approach to security





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

splunk > turn data into doing

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

ළිරිටු

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

Cloud & On-Prem

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 of query language

	m's Desktop Aggregated Risk Score: 18 acme-0005.corpt.acmetecharg Owner Adam Bek	* 3 1	Pertino Risk Objects # Paul Clever PC_poom1 # Name_hare	1 500 2 100 1 507	Timeline Threat	аросцу () О нир () О ни	
Risk Events CR tactic thread CR tactic t	m's Desktop Aggregated Risk Score: 16 acme-0005.corpt.acmetecharg Owner Adam Bak oc.exe Threat Objects III Name_here III Name_here III Name_here	bunt EMEA Chitopory server City Co	Pertino Risk Objects # Paul Clever PC_poom1 # Name_hare	1 500 2 100 1 507		X Topology 0 +40 0 +00 0 0 0 0 0 0 0 0 0 0 0 0	
John Doe I Activity Deter t Activity Deter ur Halt threshol ur Halt threshol ur Halt threshol Unauthorized J wedam: 92234: Saard Duty Ale Unauthorized J wedam: 92234:	NS acme-0005.corp1.acmetech.org Owner Adam Belk DG.exe Threat Objects III Name_here III Name_here III Name_here	bunt EMEA Chitopory server City Co	Pertino Risk Objects # Paul Clever PC_poom1 # Name_hare	1 500 2 100 1 507		Topology an 0 ∞ 0 0 0 +we 0 0 +we 0	
t Activity Detrait ur risk, threashol ur risk, threashol ur risk, threashol ur risk, threashol biograms22234; Suard Duty Ale; Uneuthortzeid J weden::92234; Suard Duty Ale; Uneuthortzeid J weden::92234;	NS acme-0005.corp1.acmetech.org Owner Adam Belk DG.exe Threat Objects III Name_here III Name_here III Name_here	bunt EMEA Chitopory server City Co	Pertino Risk Objects # Paul Clever PC_poom1 # Name_hare	1 500 2 100 1 507		00 00 0 ₩00 0 ₩000 0 ₩00 0 0 0 0 0 0 0 0 0 0 0 0	
ur risk threshol ur risk threshol Un authorized J versience 922 344 Samed Duty Ale Un authorized J versience 922 344 Un authorized J versience 922 344	oo.exe Threat Objects Marrie_here M Narrie_here M Narrie_here	* 3 1	Risk Objects # Paul Clever PC_room1 @ Name_here	1 (20) 2 (10) 1 (10)	Last 24 Hours 👻	© ₩₩	
ur risk, threashol Uhaudhortzed / wstain:522340 Suard Duty Ale Uhauthortzeid / wstain:522340 ur risk threshol	Threat Objects III Name_here III Name_here III Name_here	3 1	1 Paul Clever	1 (20) 2 (10) 1 (10)	Last 24 Hours *		
	I Name_here I Name_here I Name_here	3 1	1 Paul Clever	1 (20) 2 (10) 1 (10)			
	iiii Name_here	E,	PC_room1 Name_here	2 <mark>108.</mark> 1 107			
	III Name_here	1	Rame_here	1 107			
			A				
	III Name_here						
ur rink threehol			Ben Bauder	1 🚥			
			1 Adam's Desktop	2 😰			
			L Casy Stuart	1 🙉			
		-					

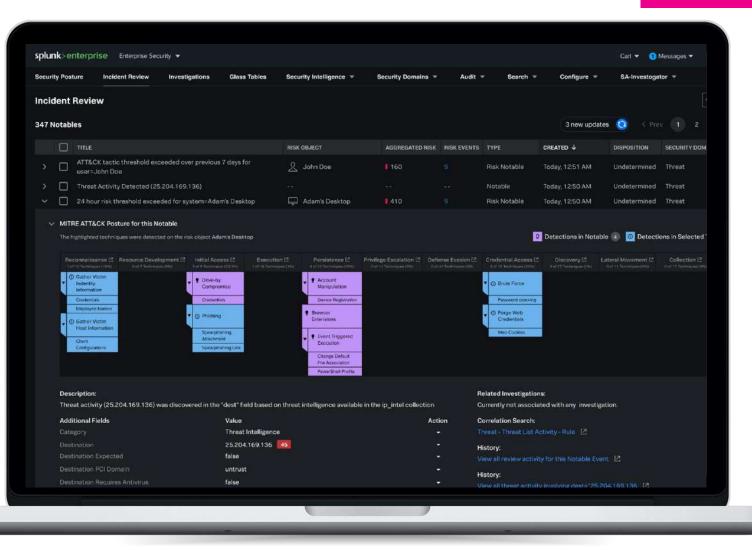


Cloud & On-Prem

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





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



SIEM & SOAR Merging



SIEM

- Basic Security Monitoring
- Advanced Security
 Monitoring
- Log Collection
- Log Management
- Data Visualization
- Data Reporting
- Threat Hunting

SOAR

Threat Detection

Investigation

Response

- Operational Metrics
- Documented Workflows
- Trained Operators
- Define Playbooks
 and Processes
- Supported Technology Integrations

SOAR Will Not Make You Better at Running SIEM Published 4 May 2022 - ID G00759000

By Analyst(s): Al Price



Prepare for Take-off

Market

Leading

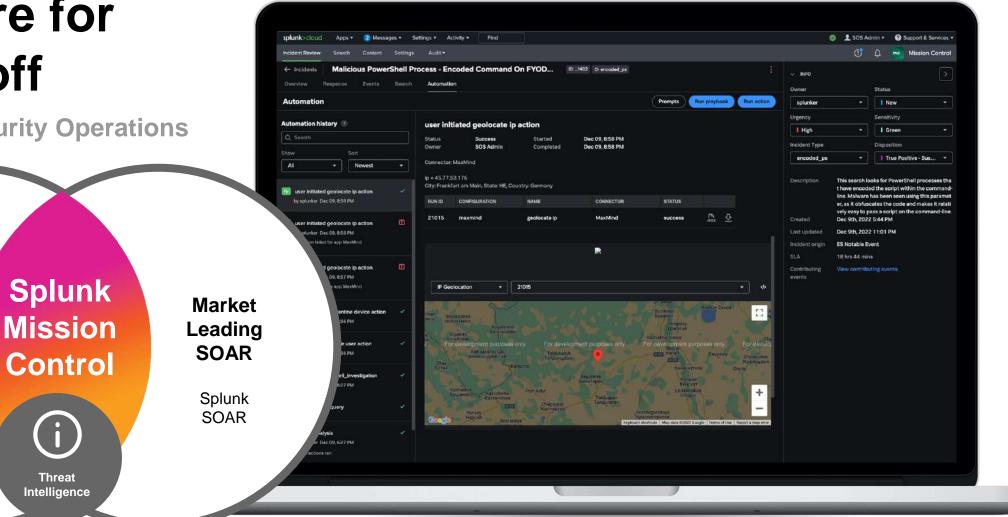
SIEM

Splunk

Enterprise

Security

Unified Security Operations



Why Mission Control for Unified Security Operations

I Malicious PowerShell Pro	cess - Encoded Command On FYODOR-Laplankt	
Comment of Mancheds Powersones Pro		
Automation	Ep (Proset) (mark	aylour Rus Actor
Automation history	(E. Sourcestantes 2 model presided investigation	
	encoded_powershell_investigation	
Non Internet	Stream Reserved Stream March 14, 1112 MM Complement Antipues Stream March 1112 FM Complement Antipues Transm March 1112 FM	
Annual Association Description Annual Association Annual Association		
ann. swy	Bentheute + 1888	
PLANE ADAPTING OF THE STATE OF	(13) mercanine with, mercanine (1) (1) (1) (1) (1) (1) (1) (1)	and an other

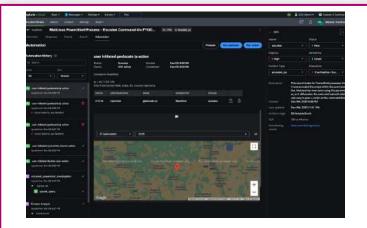
Unify Detection | Investigation | Response Capabilities And Data To Act Based On Prioritized Insights

UNIFY

Malicinus PowerShell Proc	ea - Encoded Command On FYODOR-Laplunktabl W HV Deviced as	10.000
ative Maganda Karro Scotto		ineres.
espanse	(There is a second s	- Speland
anded Programs Defection Responses	Provide context to the artifacts uncovered backgroup	Ine
manik Wited Triage, (27)	Prograd to Tablebia +	-
Decide encodentings -	- Devertudon	Beating
Review processo bare	venenge from miligering ander openen in the officer seconder. General the follows installed August graphese	
(+144)	Compared Society of Autors of Compared Society of Compared So	
mean terrational total state	Compared to D1 11 14 PM Texasian	Lastan
Producement to the at the increase of the incr	and the second in the second sec	
toonante activisadorenia L. 😑		
investigate other event and table unit.	Possible index to the order to make a second and the second and th	
(+1a)	et a 1 % 2 % 2 % 2 % 4 % 6 % 8 % 6 % 6 % 6 % 6 % 6 % 6 % 6 % 6	
Name Restor Weller, (P.R.	iver only this parameter, as it definition the mide and adder it fulltively may to pass a swript on the summaid. Line.	
This formula is follow a the should $\mathbb{T}_{\mathrm{constrained}}$		
(+144)		

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

Forrester®





Nine-Time Leader

2022 Gartner Magic Quadrant for SIEM

#1 in Market Share

2021 Gartner Market Share Report for SIEM

Leader

Forrester Wave[™]: Security Analytics Platforms, Q4 2022

Leader

IDC MarketScape: Worldwide SIEM 2022 Vendor Assessment

#1 in Market Share

IDC Worldwide SIEM Market Share Report

Best SIEM Solution

2022 Trust Awards

R TrustRadius

splunk>

Best Feature Set Best Relationship

2022 Best of Awards

Trusted by over 90 of the Fortune 100

