Splunk Enterprise Security

Detect what matters, investigate holistically and respond rapidly

Product Benefits



Realize comprehensive visibility to make sense of data noise and enable fast action.



Empower accurate detection with context to streamline investigations and increase productivity.



Fuel operational efficiency by unifying threat detection, investigation and response workflows.

Your security team faces significant challenges in today's threat landscape. They grapple with analyzing data noise, trying to gain visibility across hybrid, cloud and on-prem environments, while being inundated with vast amounts of data from various security and IT sources. It's a struggle to address every minor security issue and prioritize major vulnerabilities before they escalate. Solving for this requires the ability to turn volumes of raw data into actionable insights.

Threat detection is made even harder by a pervasive lack of context related to security events. Amidst security noise and an overwhelming number of alerts that require action, analysts struggle to discern high-priority threats from low-priority threats without sufficient context. To make matters worse, defending the organization from a wide range of risks now includes detecting sophisticated, AI-driven threat campaigns. Plus, security teams are burdened with managing an average of 25+ different security tools, across detection, investigation and response.

As the market-leading security information and event management (SIEM) and security analytics solution, Splunk® Enterprise Security is the trusted choice for security operations centers (SOCs) around the globe. Splunk has paved the way in advancing SIEM and security analytics by being at the forefront of innovation in security to help thousands of customers outpace adversaries. Its powerful capabilities enable you to realize comprehensive visibility, empower accurate detection with context and fuel operational efficiency. Built on the Splunk platform powered by AI capabilities, Splunk Enterprise Security delivers analytics at scale for continuous security monitoring with cost-effective data optimization. With Splunk, you can detect what matters, investigate holistically and respond rapidly.

							Time	o Range:	24 hours Clear all Save									
							Fin	dings a	and investigations (413)		Last ref		Auto-refr	sshon 💌 <	- 30 Next >	Show 20 🔹	÷ *	
							>											
Security content + Canfigure + S									Excessive failed logins		Q win-hp-64861	70		Today, 9.45 AM	Unassigned	• Medium		s * 📽 Mossages * Settings * Activity * Find Q
						View investiga	ation		Creative ratios signal		- ann poilost				unaagnuu	- mostan		
Last 24 hours - *					select.	• O FDEDIS	>		Multiple findings from the same entity [bstoli@splunktshirtcompany.com]		bstol@splunkts hirtcompany.c	420 4						🐹 📕 ATT&CK tactic threshold exceeded over previous 7 days for user=fyodor@splunktshirtcompany.c
I Save Apply						ATT&CK tao user=fyodo			24 hour risk threshold exceed for entity [172.16.0.149]			140) Evento Search Automation 14 detected on the entry lin a Detections in a Contections in exercised time , Sub-Techniques (1) *
Constant.	_								Unusual volume of network activity detected on 54230.147.59			60						w detection is needed time a sub-Technique (1) * requests an una Sub-Technique (1) * una Sub-Technique (1) * Una Sub-Technique (1) * Sub-Technique (1) * Sub-Techniq
PH 1000 PM 1000 AM 210 Mon, All 15	1 AM 4 80 AM	6.00 AM 8.00 AM	MA COLOR	13.00 PM 2	2.00 PM 6.00 PM	unassigned Urgancy			Excessive failed logins			26						ul E Teolologues (20) Teol 13 Sudorgues (20) E (el 13 Stadorgues (20) E el 13 Sudorgues (20
Ed. Assessment Barbar						Medium			Unusual volume of network activity detected on 52.216.133.181			35						Provide Part Part Part Part Part Part Part Part
Lestreheinzt DLoit PM D	Type *		2 3 ···		80 perpage × ≑ Drei¢	Cindetermined			Unusual volume of network activity detected on 52.218.196.122			20						dings
ed over previous 7 da (sacoser) company.com									Multiple findings from the same entity (mickey.perre@splunktshirtcompany.com)		요 mickeyperre@s plunktshirtoo	120 6						burktahintsompenyusen Intermediate Redrugs count. 19 Timelitee vity fysder Pent Name. fysder Last Name. metteskeeko Email fysder@epturktahintsompenyusen Phone +1 (200)(555-8762
									Multiple findings from the same entity (hayley,jensen@splunktshirtcompany.com)		& hayleyjenson@e plunktshirtoo	150 5						s Category technical
									Excessive failed logins			50						
led over previous 7 da sempany.com		 tyodor@splunk. tshirtoompany.co 	1052						24 hour risk threshold exceed for entity [macbook-44591]			30						A seasant valare di senori)
led over previous 7 da propeny.com	\$ F080396	g, betallijksplankt shirtcompany.com	246		Fedey, 4.32 PM				Unusual volume of network activity detected on 34215.24.225			55						Liter /yodor@splantahitos Log nation pit for /yodor@s
leci over previous 7 da shirtcompany.com		 mveltus-lapkn ktahirtoompany.oo 	461			Un Original spicific o			24 hour risk threshold exceed for entity [win- hp-85670]			66						Login stimpts for fysicings () Login stimpts for fysicings
			4000						Unusual volume of network activity detected on 172.16.0.127			60						Copyristministration for Proceedings Copyristministration for Proceedings
Why Detected on 54.2			4002						Excessive failed logins		C win-lenovo- 15752	70						Cogn attangst for typologies Cogn attangst for typologies Cogn attangst for typologies.
											- win-lenovo-	-						0. Lotte attempts for Environment.

Gain comprehensive visibility

Unmatched, comprehensive visibility by seamlessly ingesting, normalizing and analyzing data from any source at scale enabled by Splunk's data-powered platform with assistive AI capabilities.

Make sense of alerts

Be enabled for fast action when an alert is triggered with the custom alert actions feature. Custom alerts can be set to varying levels of granularity based on conditions such as data thresholds, trend-based conditions and behavioral pattern recognition like brute force attacks and fraud scenarios.

Prioritize focus with context

Drastically <u>reduce alert volumes by up to 90%</u> with risk-based alerting (RBA). RBA uses the Splunk Enterprise Security correlation search framework to collect risk events into a single risk index. Collected events create a single risk notable when they meet a specific criterion, so you can stay focused on imminent threats that traditional SIEM solutions might miss.

Utilize curated detections

Tap into 1,700+ out-of-the-box detections based on Splunk Threat Research deep dives into detection engineering to find and remediate threats faster. These detections also align to industry frameworks like MITRE ATT&CK, NIST CSF 2.0 and Cyber Kill Chain®.

Build high-confidence aggregated alerts

Enhanced detection capabilities help analysts understand and implement a risk-based alerting detection strategy with turnkey flexibility to build high-confidence aggregated alerts for investigation.

Complete threat detection, investigation and response

Native integration with <u>Splunk® SOAR*</u> automation playbooks and actions with the case management and investigation features of Splunk Enterprise Security and <u>Mission Control</u> delivers a single unified work surface. Optimize mean time to detect (MTTD) and mean time to respond (MTTR) for an incident.

Execute response workflows

Response Plans directly in Splunk Enterprise Security allow users to collaborate and execute incident response workflows for common security use cases easily.

Simplified terminology

The taxonomy in Splunk Enterprise Security aligns to the Open Cybersecurity Schema Framework (OCSF), making it easy for your security team to understand exactly what they are working on across detection, findings, and investigations workflows.

Build what you need

Access Splunk's network of 2,200+ partners and Splunkbase's 2,800+ partner and community-built apps that seamlessly integrate with your existing tools. Collect, search, monitor and analyze data using a centralized, vendor neutral solution to help you meet increasingly complex compliance requirements.



	-	
—		
		 7

ľ	=

Read more >

<u>Take a tour</u> >

<u>Latest releases ></u>

*Splunk SOAR subscription required

splunk>

Contact us: splunk.com/asksales

splunk.com

Splunk, Splunk> and Turn Data Into Doing are trademarks and 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. © 2024 Splunk Inc. All rights reserved.