Threat Intelligence Management

Accelerate investigations with integrated intelligence enrichment



Gain more context around threats with a full breadth of embedded intelligence.



Reduce noise and surface the highest fidelity intelligence for action.



Simplify security workflows by accessing intelligence within Splunk Enterprise Security.

Security analysts are constantly overwhelmed by alerts and repetitive, manual tasks — negatively impacting their ability to triage and investigate critical security events. Analysts don't have the time to sift through multiple data feeds spanning countless sources, making it difficult to identify and synthesize intelligence related to an incident. The security operations center (SOC) requires seamless access to relevant threat intelligence along with a normalized scoring of data sources to have an objective view into critical events, as well as a comprehensive view into the potential risk to the enterprise.

Embedding threat intelligence into the operational framework of the SOC's detection, investigation and response workflows reduces mean time to detect (MTTD) and mean time to respond (MTTR), allowing analysts to manage events from a single console.

Threat Intelligence Management — a feature of <u>Splunk® Enterprise Security</u> — helps analysts to fully investigate security events by providing relevant and normalized intelligence to better understand threat context and accelerate time to triage. Analysts can manage security events and leverage threat intelligence feeds directly within Splunk Enterprise Security without pivoting to other tools, ultimately reducing time to investigate. This ensures informed, timely and actionable intelligence across the SOC's ecosystem of teams, tools and partners.

	splunk>enterprise	splunk>enterprise Apps •			r 👻 🧐 Messages 👻 Settin	gs ▼ Activity ▼ H	le							
	Incident review													
	← Incidents													
	Overview Resp													
a * 😰 Mosagea * Settinga * Activity * Find	Intelligence							yn + Satrap + Achrly + Gried 🕘 🛔 505 Anie + Iwwshystora Security Innibyena - Security Domeins - Cloud Security - Audit - Search - Configuen -						
												_		
clous PowerShell Process - Encoded Command On FYOD 0.3432 O annual jn	Threat object 25		 Observable overv 	view										
e Denta Seach Adomation	Q Search	1 of 2 pages < >	Observable Type IP	Address				Status		Owner		Dom	hain	
				/02/2022, 2:42 PM					Cranspred New Pridbay Pridbay Tenstvel Cranad	\cap	SCA James SCAJ Anno Schart Couch Annah Unterland		\frown	
user initiated geolocate ip action Sinhun Success Stanted Dec 09,858 PM			Total IOCs 80						Perding Respired Creat				$\mathbf{\nabla}$	
Son Owner 803 Admin Completed Dec 93, 888 PM Freed. Connector: MaxMind				Sources Workflow										
lig in 45-27.08.176 City: Frankfurt an Main, State Hil, Country: Germany	IP Address		BB	IVA lunk ES				Select. • Select.	• Select. •			• Last 34 •		
	# мр5	9e779da82d86bc		uspicious Investigation				Over Presiden 2 Days 32 Bill		weitHow Reliad x Tree Targe Last 24 hours		1 2 Not >	20 per page	
nie jo unicion III 21815 maximinal geolocante (p. MaxiMinal euccess) Intern														
Addred D	# SHA1	66ddb290df3d51			Show more		reded for user-fyedenii/holh/y	A possestant		Risk Notable Today, 10:56 PM True Positive - Sappidous Ad				
ne je action III	# SHA256													
	· IP Address		 Most recent reporting from each source 											
In device action of the second s	IP Address		Q Search			< Prev 1 of 2 p	veded for			Risk Notable Today, 9:06 PM Undetermined				
Law action - Residence on the providence only For development purposes only For development purposes only	we is the second s									Risk Natable Today, 905 PM Undetermined				
In Antonio	IP Address		Timestamp \downarrow							Rick Notable Today, 753 PM True Fostive			Progress Closed S	
Investigation	😁 # мD5	1f9bfb6b43rdfjsw		Virus Total		I High								
And		baduri.com	02/05/2022, 2:42 PM	-I Becorded	52/70	High				Risk Notable Today, 753 PM. Undetermined		A Medium		
Condition - Marine - And And -	available data		02/05/2022, 2.42 PM		1 32/10	night				Risk Natable Today, 745 PM Undetermined		. Lew		
	😔 Threat actor				I Medium	Medium	1	T another A		Kon National Loosy, 746 PM Undetermined				

Informed, timely and actionable intelligence across the SOC's ecosystem of teams, tools and partners

Threat Intelligence Management reduces the number of alerts to investigate by filtering out intelligence that isn't relevant to the organization, allowing analysts to monitor for intelligence related to specific use cases. By synthesizing intelligence into a single, normalized view, Splunk is making it even easier for analysts to understand threat context and take action.

Monitor against curated IOC lists to reduce alert volume and speed up detections

The Intelligence Workflows allow analysts to create indicator of compromise (IOC) lists in order to receive relevant alerts that align to specific detection use cases. This reduces alert fatigue by detecting IOCs relevant to an analyst's environment and accessing pertinent intelligence.

Access integrated intelligence within events to reduce time to investigate

Threat Intelligence Management integrates directly with the Splunk Enterprise Security Risk-based alerting (RBA) framework so analysts can detect sophisticated threats and reduce alert fatigue. RBA attributes risk to users and systems and generates an alert in the form of Splunk Enterprise Security Risk Notable Event, when risk and behavioral thresholds are exceeded.

Having Threat Intelligence Management integrated into Risk Notable Events provides analysts with an integrated intelligence solution to support the investigation of critical events. Threat Intelligence Management empowers analysts to conduct a full investigation of a Risk Notable Event by centralizing, normalizing and prioritizing intelligence into the investigation management user interface.



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.