# SPLUNK® USER BEHAVIOR ANALYTICS

Detect cyberattacks and insider threats

- Improve detection of known, unknown and hidden cyberattacks and insider threats
- **Increase security analyst effectiveness** by prioritizing threats and avoiding false positives
- **Easy to use** for SOC analysts, incident responders and SIEM administrators

# **Analytics-Driven Security Portfolio**



Sophisticated cyberattacks can be hidden and difficult to find, yet addressing these threats is critical to protecting confidential data. That means today's security teams are tasked with finding and responding to the threats hidden in their environments regardless of organizational size or skillset.

Splunk User Behavior Analytics (Splunk UBA) helps organizations find known, unknown and hidden threats using multi-dimensional behavior baselines, dynamic peer group analysis, and unsupervised machine learning to detect compromised or misused accounts or devices leading to data exfiltration or IP theft. Splunk UBA addresses security analyst and hunter workflows, requires minimal administration and integrates with existing infrastructure to locate hidden threats.

What Is Behavior-Based Threat Detection? Behavior-based threat detection is based on machine learning methodologies that require no signatures or human analysis, enabling multi-entity behavior profiling and peer group analytics — for users, devices, service accounts and applications. The result is automated, accurate threat and anomaly detection.

The entire lifecycle of security operations — prevention, detection, response, mitigation, to the ongoing feedback loop — must be unified by continuous monitoring and advanced analytics to provide context-aware intelligence. Splunk Enterprise, Splunk Enterprise Security (Splunk ES) and Splunk UBA work together to:

- Extend the search/pattern/expression (rule) based approaches in Splunk Enterprise and Splunk ES with threat detection techniques to detect threats with sophisticated kill chain visualizations.
- Provide security teams with machine learning, statistical profiling and other anomaly detection techniques that leverage the readily available data at massive scale in Splunk Enterprise.
- Combine machine learning methods and advanced analytics capabilities to enable organizations to monitor, alert, analyze, investigate, respond, share and detect known and unknown threats regardless of organizational size or skill set.

splunk > User Behavior Analytics	⊙ Explore ~ 🖗 Analytice ~ 🛠 Manage ~ Q, System ~			(Scope ~	admin ~			
*************************************	22 35 122 2	USERS Anomatous All Uninoum	DEVICES 225 Aromatica 833 Altimenal 61 AtExternel	14 леон 14 леон 135 лало	5 1000 14		Thread Union Analytics	1 Review Review Dashboard
A Latest Threats			A Threats Tin	neline (Last 7 De)	n)			
Data Exfibration by Suspicious User or Device	May 29	0		Mulmare				
Data Exfitration by Suspicious User or Device	May 28	0	C.	Ingramised Account				
Malware	May 28	0	Data Baffe	tration after Account Takezver				
Malware	May 28	0		Culturation				
Data Exfitration by Suspicious User or Device	May 28	0	E Printage Dat	alacion Powenhall Attivity				
Malware	May 28	0	Duta Extinuti	ion by Compromised Account				
Showing top 20 of 23 threads		View Details	Data Bellina	tion byicious Data Transfer				



	blunk > User Behavior Analytics						
	rer / Alvalialy Scaring Rulas						
۳	Anomaly Rules					Recompute Anomaly I	Scores
e .			Edit Anomaly Scoring Rule				
۰	Anomaly Action Anomaly Scores		Factor	Conditions		Score Delta	Enabled
		_	Anomalous domain features Suspicious domain name	Domain Features Detection +	~ 0	1	•
	Multiple Dessions Denial	Anomaly Sco	Exploit chain features Suspicious donain access patient (suggests	Exploit Chain Features Detection	* ~ 0·	1	•
	Period with Unusual Windows Security Event Sequences	NAME	equit charj				
	Potential Webshell Activity	Analysis of Dor Analysis of Dor	Timing features Suspicious domain access timing	Timing Features Detection >	~ 0	1	0
	Scanning Activity	Unclassified Dr.	Referrer features Suspensus referrer	Referrer Features Detection +	v 0	1	
	Suspicious Account Lockout		UIII features	URI Features Detection > ~	0	1	0
	Suspicious Data Movement	Anomaly Bas	Suprova un				
	Suspicious Domain Communication	BARE BOOME	Surpicious user agent	User Agent Features Detection	~ 0	5	•
	Suspicious Comain Name		DNS features	DNS Features Detection + +	0	1	
	Suspicious HTTP Redirects		angeous ore news				
	Suspicious Network Connection					Cancel	06
	Suspicious Network Exploration						



#### **Streamlined Threat Workflow**

Reduce billions of raw events to thousands of anomalies, then to tens of threats for quick review and resolution. Leverage security-semantics-aware machine learning algorithms, statistics and custom machine learning driven anomaly correlations to identify hidden threats without human analysis.

### **Threat Review and Exploration**

Visualize threats over a kill chain to gain context. These threats are generated by the ability of machine learning to stitch together anomalies observed across multiple-entities — users, accounts, devices and applications — into various attack patterns without any human analysis.

### **User Feedback Learning**

With user feedback learning, SOC teams can customize UBA anomaly models based on their organization's processes, policies, assets, user roles and functions. Anomaly scoring rules allows security practitioners to provide granular and explicit feedback on individual anomaly models to improve severity and confidence in threat detection.

## **Kill Chain Detection and Attack Vector Discovery**

Detect lateral movement of malware or malicious insider proliferation or respond to real-time detection of anomalous activity (e.g. dynamically generated domain name or unusual AD activity). Detect behavior based irregularities (e.g., unusual machine access, unusual network activity) or pinpoint botnet or CnC activity (e.g., malware beaconing, etc.) and much more.

Interested in elevating your security maturity with Splunk UBA capabilities that are already part of your existing Splunk investment? Then **connect with us and talk with our security experts**.

splunk>

#### Learn more: www.splunk.com/asksales

www.splunk.com

© 2018 Splunk Inc. All rights reserved. Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL 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.