Splunk User Behavior Analytics

Detect advanced and insider threats using machine learning

Product Benefits

Detect advanced threats and anomalous behavior using machine learning

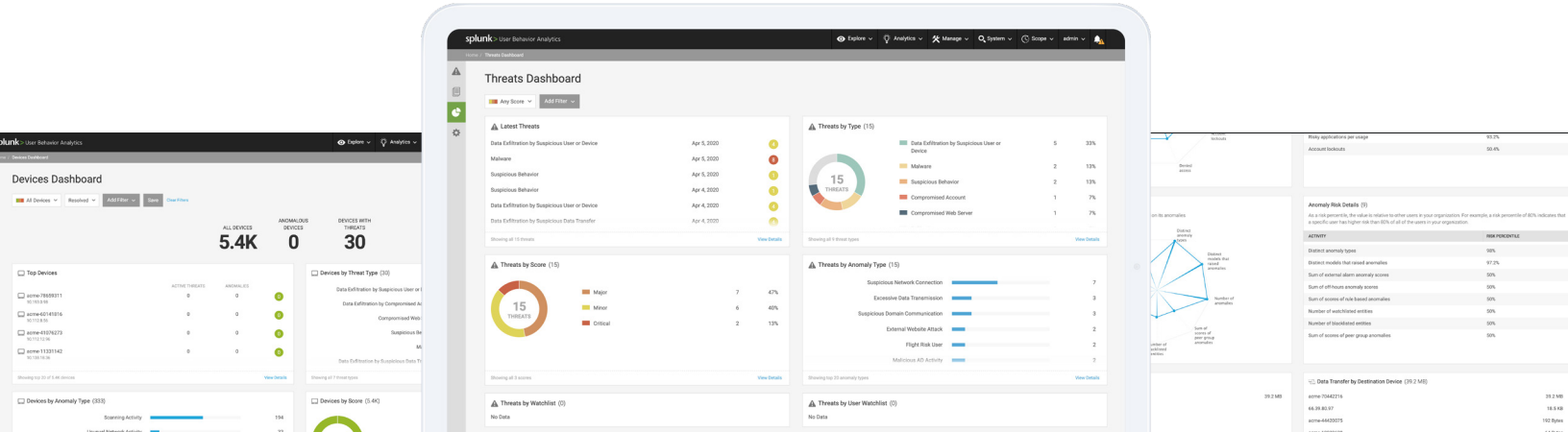
Enhance visibility and generate rich contextual insights to rapidly assess risk and take action

Simplify and streamline incident investigations and workflows to increase SOC efficiency

Sophisticated cyberattacks can be very difficult to uncover and detect. While manmade correlation rules can and do detect malicious behavior, they cannot be solely relied upon to identify 100% of threats in a given environment. Consider the limitations of human-fueled security tactics. Security teams are so overwhelmed by the sheer volume and sophistication of attacks that they have reached, if not exceeded, their capacity to effectively and rapidly observe, orient, decide, and take action. A more sound strategy is a combined human-and-machine approach to scale the SOC team with technology that can streamline and automate key elements of the detection, investigation, response and remediation cycle.

This is where machine learning changes the dynamic. Machine learning does not presuppose any conditions. It does not assume something is good — instead, it trains itself, learns what is normal, and what is abnormal behavior. Without any inherent bias, it learns from the environment and establishes a baseline, and anything that behaves atypically or contrary to that baselines is deemed anomalous.

Splunk User Behavior Analytics (UBA) helps organizations find known, unknown and hidden threats using multi-dimensional behavior baselines, dynamic peer group analysis, and unsupervised machine learning. This allows Splunk UBA to rapidly detect anomalous behavior — such as compromised or misused accounts or devices, IP theft or data exfiltration — and eliminate it. Using machine learning, Splunk UBA derives sequences and patterns across all anomalies, in addition to other indicators, to filter down and identify the top threats that are critical and actionable. Amidst all the noise, these threats represent the most likely risk to your business. Splunk User Behavior Analytics addresses security analyst and hunter workflows, requires minimal administration and integrates with existing infrastructure to locate hidden threats.



Detect advanced threats and anomalous behavior using machine learning

Splunk UBA uses unsupervised machine learning algorithms to establish baseline behaviors of users, devices, and applications, then searches for deviations to detect unknown threats, such as:

- Compromised user account – any deviation of user activity from normal thereby indicating that someone other than the legitimate owner is operating the account.
- Compromised machine – identification of network endpoints that have been compromised, infected by malware or are otherwise behaving suspiciously.
- Data exfiltration – detection of loss or theft of private and confidential data out of the enterprise across multiple threat vectors such as firewalls and proxies, cloud storage, attached storage, or email.
- Lateral movement – a trusted insider user scanning and expanding access across multiple resources.
- Account misuse – accidental misuse or deliberate abuse of superuser privileges

Enhance visibility and generate rich contextual insights to rapidly assess risk and take action

Splunk User Behavior Analytics visualizes threats across multiple phases of an attack to give security analysts a comprehensive understanding of attack root cause, scope, severity, and timelines. This context-rich view enables analysts to rapidly assess impact, and make informed decisions quickly and confidently. Graph and kill chain analysis provides deep investigative capabilities on any user, entity, anomaly or threat for faster insights.

Simplify and streamline incident investigations and workflows to increase SOC efficiency

Splunk User Behavior Analytics automatically reduces billions of raw events down to tens of threats for rapid review, without the need for time-consuming human-fueled detective work performed by an army of highly skilled security and data science professionals. Furthermore, by filtering alerts before they reach the SOC team, Splunk UBA frees up time for security analysts to focus on the most urgent and complex threats.

Pair SIEM with user and entity behavior analytics for comprehensive protection

By combining Splunk User Behavior Analytics' multi-entity, behavior-based anomaly and threat information with Splunk Enterprise Security's correlation rules and searches, security teams can establish a potent and wide-reaching defense against the most sophisticated threats. Splunk User Behavior Analytics automatically pushes threat information into Splunk Enterprise Security to create a centralized incident view and an end-to-end investigative workflow.

Read More >

Take a Tour >

Latest Release >

splunk>

Contact us: www.splunk.com/asksales

www.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.

24-491650-Splunk-Splunk User Behavior Analytics-PB-102