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:

- **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

---

**Advanced Security Analytics**

- **Splunk® User Behavior Analytics**
- **Splunk® Enterprise Security**
- Security Analytics & Event Repository
- Data Science & Decision Engine
- Security Intelligence & Operations

---

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 skillset**
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 ML 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.

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.

Platform Architecture & Deployment Options
Splunk UBA includes the Hadoop ecosystem for scalable, cost-efficient and open data persistence. It’s designed for real-time and large-scale event analysis and includes time-series and graph databases for processing and analysis. RESTful APIs automate the tasks from data ingestion to analysis. Splunk UBA is proven to scale to over hundreds of terabytes of data and billions of events, and is deployable on-premises as software, on a virtual machine, or as a customer-managed public cloud instance (AWS).

Download Splunk Free or explore the online sandbox. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs. Learn more about Splunk User Behavioral Analytics by contacting ubainfo@splunk.com.

Learn more: www.splunk.com/asksales

© 2017 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.