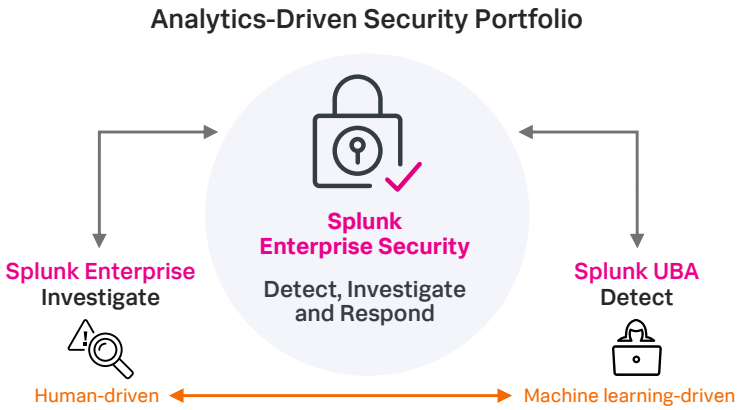
Splunk® User Behavior Analytics

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



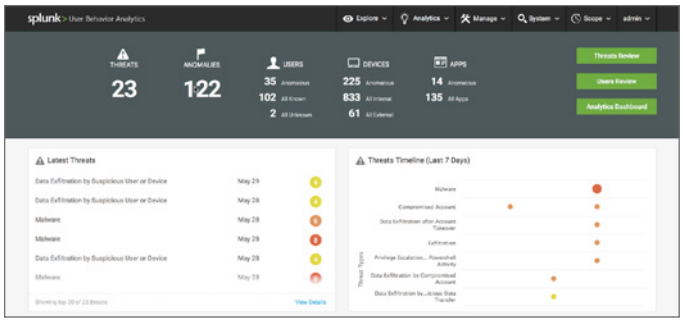
Sophisticated cyberattacks can be hidden and difficult to find, yet addressing these threats is critical to protecting confidential data. That means today's security teams are tasked with finding and responding to the threats hidden in their environments regardless of organizational size or skillset.

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.

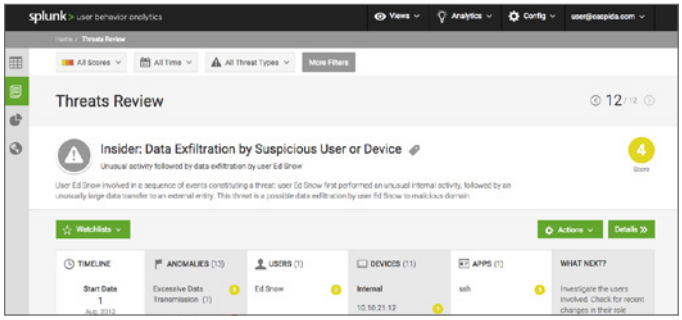
The entire lifecycle of security operations — prevention, detection, response, mitigation, to the ongoing feedback loop — must be unified by continuous monitoring and advanced analytics to provide context-aware intelligence. Splunk Enterprise, Splunk Enterprise Security (Splunk ES) and Splunk UBA work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



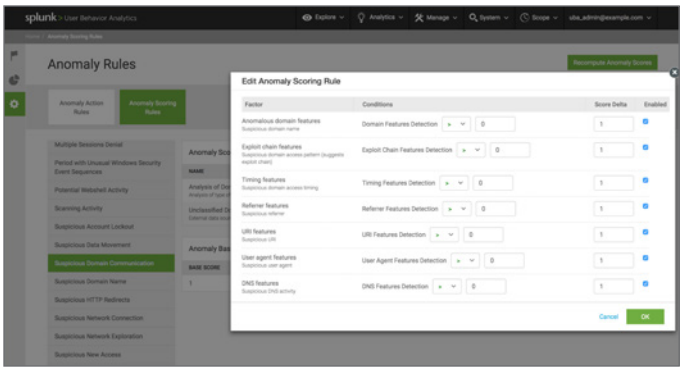
Streamlined Threat Workflow

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.



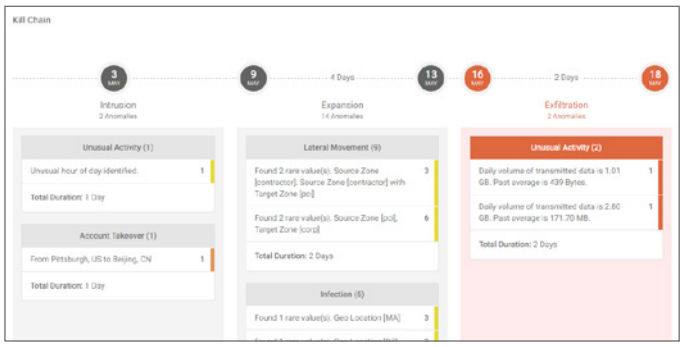
Threat Review and Exploration

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

2020-Splunk-SEC-UBA-109-PB