splunk>

TECH BRIEF

SPLUNK FOR ADVANCED ANALYTICS AND THREAT DETECTION

Powered by Splunk Enterprise Security and Splunk User Behavior Analytics

The security threat landscape continues to evolve in both scale and sophistication. Detecting unknown, hidden and insider threats early to stay ahead of advanced adversaries is ever more challenging. Traditional security tools built on known and identified rulesets and signatures are adept in detecting known threats, but cannot scale to fully address the complexity of advanced security threats, such as insider threats, zero-day attacks, laterally moving malware and compromised accounts. Additionally, SOCs are constantly flooded with alerts, many of which are false positives. In an evolving threat landscape, security teams need to respond by adding new analytic capabilities, giving them more eyes to see potential threats.

Accelerate Investigation of Advanced Threats Through Automated Early Attack Detection

Splunk Enterprise Security (ES) delivers an analytics-driven, market-leading SIEM solution that enables organizations to discover, monitor, investigate, respond and report on threats, attacks and other abnormal activity found across the enterprise. It is built on a big data platform that provides superior scale and visibility into all security-relevant data, and is augmented with business context to provide for powerful, actionable insights. Splunk User Behavior Analytics (UBA) is a machine learning-powered solution that finds unknown threats and anomalous behavior across users, endpoint devices and applications.

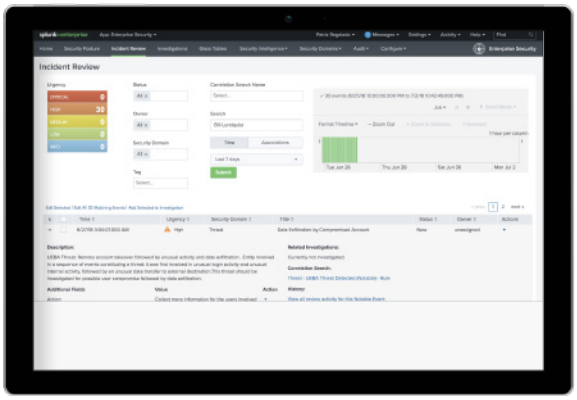
Together, Splunk ES and Splunk UBA rapidly address the most sophisticated threats. By sharing anomalies and threats and correlating them as part of the workflow, organizations can prioritize and accelerate investigations with risk scores added to a centralized incident view. Splunk UBA automatically pushes threat information into Splunk ES, which becomes a notable event. Threats detected by Splunk UBA are factored

REAP THE BENEFITS OF MACHINE LEARNING IN YOUR SOC

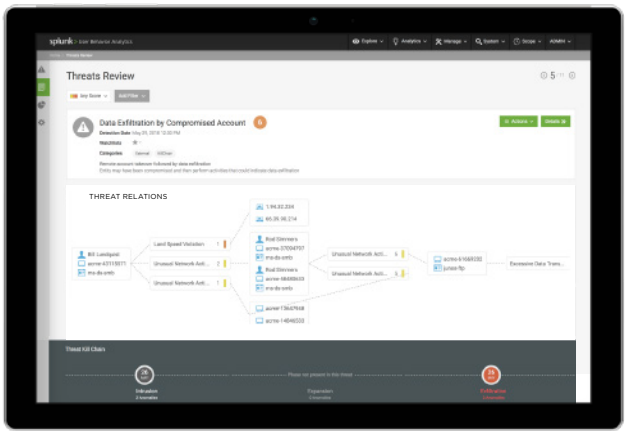
The benefits of machine learning in security speak for themselves. It can help you better analyze and respond to security incidents, better prepare for threats and minimize overall risk—all while reducing costs and stress on limited resources.

Machine learning is the perfect fit for security use cases like advanced threat detection and stopping insider threats, which require a more nuanced monitoring and response system. Advanced attacks involving lateral movement within a network, compromised privileged users and accidental access to sensitive information by unwitting users, can all be addressed by automated, machine learning-powered anomaly detection.

With machine learning, analysts and SOC teams can perform rapid investigations, find meaningful insights, determine the root cause of an incident, draw on historical trends and share findings without being bogged down by thousands of alerts and false alarms. Put simply, organizations can improve detection speed, analyze impact and respond quickly to any security incident.



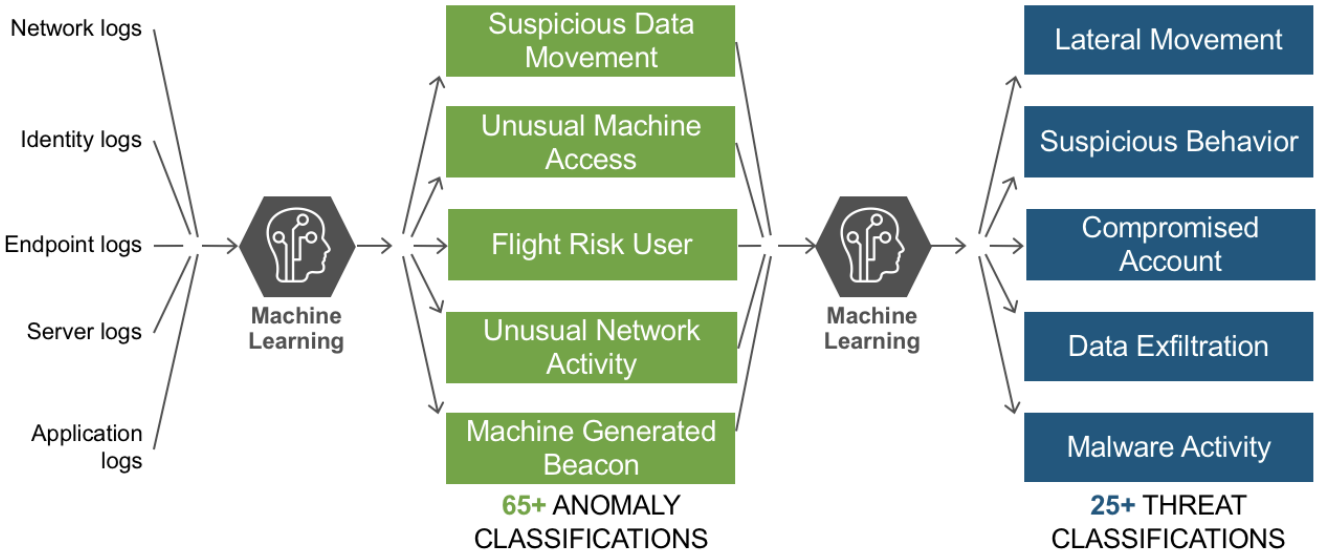
into the risk scoring algorithms within Splunk ES so you can continue to leverage the Splunk ES Risk Scoring framework and Incident Review workflow for threat management. Augmenting human-driven correlation rules and searches within Splunk ES paired with unsupervised machine learning-based threat correlations to detect unknown threats within Splunk UBA delivers faster threat detection.



Increase SOC Efficiency and Work Smarter by Leveraging the Power of Machine Learning to Augment SIEM

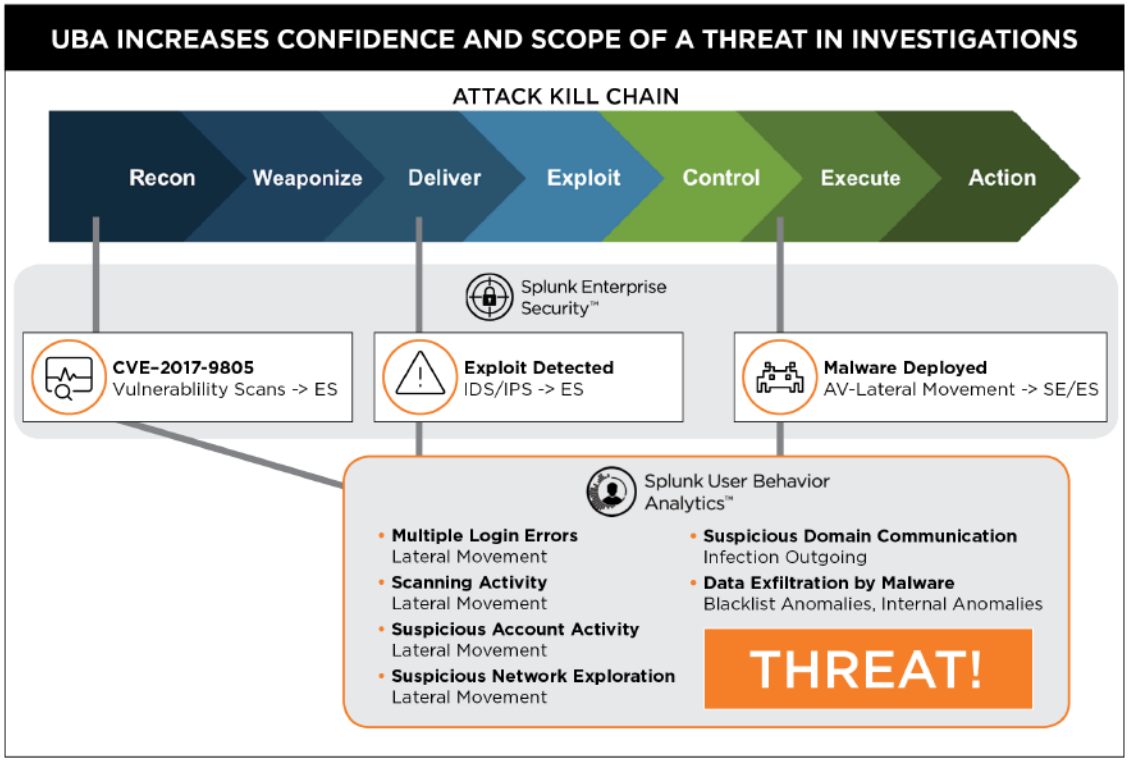
The powerful combination of human and machine-driven threat detection techniques in Splunk ES and Splunk UBA improves security analysts' productivity by scoring and highlighting the most important threats and anomalies to minimize alert fatigue. By expanding Splunk ES to ingest behavioral anomalies detected by Splunk UBA, Splunk makes it easy to automate a slew of SIEM tasks.

The powerful machine learning algorithms of Splunk UBA automatically stitch hundreds of anomalies into a single threat; filtering alerts before they come up to the SOC team, giving them time to focus on urgent and complex threats, while not requiring an army of highly skilled security and data science professionals. In a time when cybersecurity talent is stretched thin, this can be an added benefit to enterprises of any size applications.



Optimize Insider Threat Detection and Uncover Unknown Threats by Combining Threat Intel From SIEM and UBA

Tomorrow's attacks won't look like today's and that's why Splunk UBA automatically finds hidden or unknown threats using data science and unsupervised machine learning that enhance insider threat defense and advanced threat detection. By adding Splunk UBA multi-entity, behavior-based anomaly and threat information into Splunk ES, you can leverage the power of both products to gain deeper context about anomalies relative to users, devices and applications to better detect and respond to threats. The threat detection capabilities in Splunk UBA extend the search, pattern, and rule-based approaches in Splunk ES for detecting threats. Additionally, Splunk UBA's unique correlation and pattern detection using machine learning, graph analysis, along with behavior analytics augments Splunk ES to deliver automated detection of advanced threats spanning insider threats, account compromise, privileged account abuse, lateral movement, data exfiltration, and more.

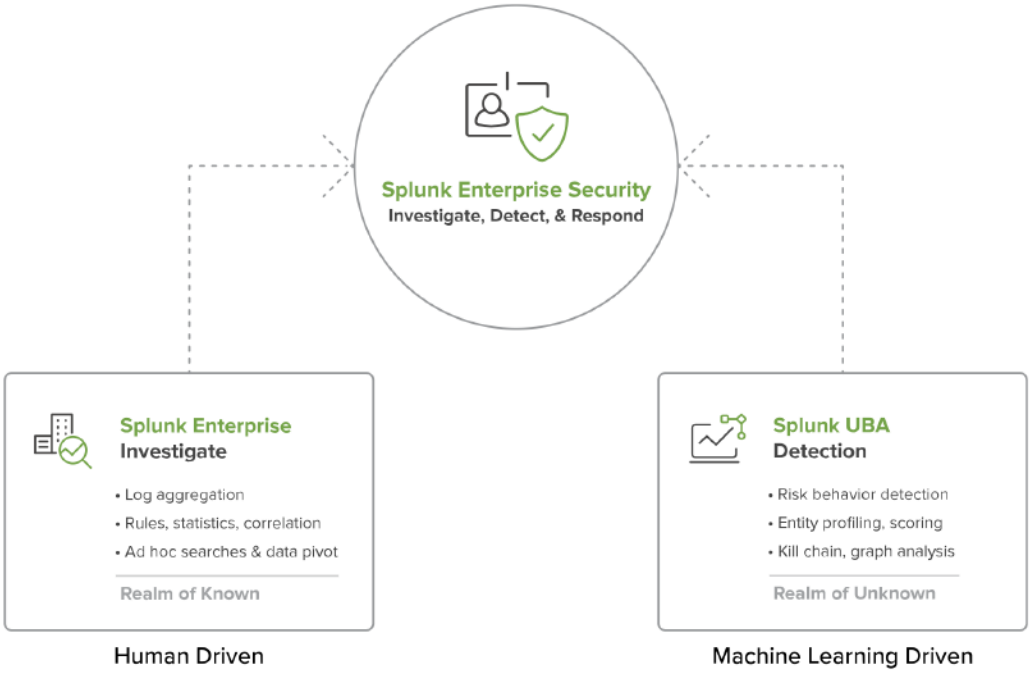


Furthermore, Splunk ES and Splunk UBA delivers dynamic and recurring security content updates that empowers security teams to proactively stay current with the latest threat detection techniques. Together, Splunk ES and Splunk UBA help uncover hidden potential incidents to stay ahead of–and more quickly respond to--advanced threats.

Proven, Analytics-Driven SIEM Supercharged With Machine Learning and Behavior Analytics

Splunk ES goes miles beyond traditional SIEM technology by arming you with detailed investigative and rapid-response capabilities as well as security frameworks such as Notable Event, Risk Scoring, and Threat Intelligence to help make informed decisions. These frameworks accelerate detection and response by contextualizing data, giving analysts the insight they need to move quickly through an investigation. By enhancing Splunk ES with Splunk UBA, customers can leverage the power of data science with event-based correlation and ad-hoc searching to gain insight across the entire enterprise.

When combined, Splunk ES and Splunk UBA provides a strong union of machine learning, anomalous user behavior detection, context-enhanced correlation and rapid investigation capabilities. The integrated solution provides a centralized view for incident investigation and management to help SOC teams quickly respond to prioritized, high-fidelity threats. The entire lifecycle of security operations–detection, investigation, prevention and, response, to the ongoing feedback loop, must be unified by continuous monitoring and advanced analytics to provide context-aware intelligence. The combined solution of Splunk ES and Splunk UBA delivers on this vision.



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

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com