Automated Early Breach Detection
Cyberattacks are sophisticated and it’s difficult to find hidden threats early—yet early detection is critical to preventing the loss of confidential and sensitive enterprise and customer data.

While sophisticated threats like APTs and insider attacks hide within the enterprise, indications of breaches can be gleaned by analyzing data. Locating a breach requires advanced detection methods such as finding dynamic and polymorphic threat patterns and identifying behavior of threat actors over weeks, months and even years.

Splunk Enterprise deployments contain a wealth of security data that has information about threats. Because Splunk Enterprise aggregates and analyzes machine data for Operational Intelligence, it contains data that’s sprinkled with the signals that indicate hidden threats, including key context that points to a breach.

Splunk User Behavior Analytics (Splunk UBA) extends the Splunk platform by analyzing its repository and locating and contextualizing these signals. By performing correlation analysis based on machine learning, graph analysis and behavior analytics methodologies, Splunk UBA works in conjunction with Splunk Enterprise and Splunk Enterprise Security (Splunk ES) to automate the detection of:

- APTs, malware and insider threats
- Account compromise and abuse
- Botnet and malware beaconing
- Lateral movement
- Data exfiltration

Specifically, Splunk UBA analyzes events collected in Splunk ES and then performs behavior modeling, peer group analytics, graph mining and other techniques to find hidden threats by identifying anomalies and stitching them together to form actionable threat patterns, for example:

- Suspicious login activity
- Privileged account abuse
- Virtual machine/container breach
- Data exfiltration
- Unusual SaaS and remote user behavior
- Rogue mobile device transmitting malware
- Data theft from privileged app infiltration
- AWS/cloud asset compromise
- Malware Command and Control (CnCs) or bad IP addresses
- Systems infected with malware

Data Sources
Splunk UBA provides correlation and pattern detection for attacks and threats across multiple data sources. Data sources can include security products or services, such as threat feeds, applications and hosts/servers/other endpoints, networking devices and essentially any infrastructure within the environment that generates machine data.
Examples of Data Sources

Identity and Privileged User Activity: entity ID and authentication events (Active Directory, single sign-on, VPN, etc.), and privileged account management applications

Activity: HTTP transactions, intra-network activities (firewall, web gateway, VMs, proxy, DPL, etc.)

SIEM: existing SIEM and log management products (HP/ArcSight, LogRhythm, IBM/QRadar, etc.)

Hadoop Ecosystem: existing Hadoop data repositories (Cloudera, Hortonworks, etc.)

Malware Detection: existing sandbox or dynamic analysis products (FireEye, Palo Alto Wildfire, etc.)

External Threat Feeds: external threat feeds (FS-ISAC, Google CIF, etc.)

Cloud, Mobile: mobile device events, remote application logs, AWS CloudTrail, Box, etc.

Endpoint: application and security logs from laptops, desktops and servers

Custom Apps: live event streaming via JavaScript, Java, REST, Syslog

Automated Continuous Threat Monitoring

Splunk UBA visualizes threats along the kill chain and provides supporting evidence so that the security analyst can take immediate action based on a prioritized list of significant threats to investigate. This approach avoids overloading the analyst with alerts and false positives.

Analytics-based workflow enables a hunter to investigate anomalies and look for policy violations or potential intent to exfiltrate data.

Splunk UBA adds automation to either a standalone enterprise deployment or an enterprise security deployment. In an enterprise security deployment, it automatically pushes threat information into Splunk ES, which then becomes a notable event. Threats discovered by Splunk UBA will be taken into account as part of the risk scoring algorithms within Splunk ES. This enables Splunk Enterprise Security users to continue leveraging the Splunk ES Risk Scoring Framework and Splunk ES Incident Review workflow for threat management. The combined solution offers customers complete threat detection and prevention capabilities that address even the most sophisticated threats including APTs, malware and insiders.

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.