splunk>

TECH BRIEF

USING SPLUNK USER BEHAVIOR ANALYTICS

Automating early breach detection and continuous threat monitoring

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 creating multi-dimensional behavior baselines around users, service accounts, devices and applications, and then executing unsupervised machine learning algorithms to generate anomalies and threats. Splunk UBA works in conjunction with Splunk Enterprise and Splunk Enterprise Security (Splunk ES) to automate the detection of:

- Malware and insider threats
- Account compromise and privileged account abuse
- Lateral movement
- Suspicious behavior
- Data exfiltration and IP theft

Specifically, Splunk UBA analyzes events collected in Splunk Enterprise and then performs behavior baselining, peer group analytics, clustering, graph walks and other techniques to find hidden threats by identifying and stitching anomalies together, for example:

- Remote account takeover
- Suspicious behavior
- Malware activity
- Data exfiltration by compromised account
- Data exfiltration by malware
- Lateral movement by insider
- Compromised account
- Infected device
- Fraudulent website activity

Data Sources

Splunk UBA provides machine learning driven correlation of anomalies across multiple data sources, which can include security products or services such as firewalls, web gateways, VPN technologies, endpoint solutions, DLP products, cloud applications, 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, proxy, DPL, etc.)

SIEM: Splunk ES or third party 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: FS-ISAC, Collective Intelligence Framework (CIF), etc.

Cloud Applications: AWS CloudTrail, Box, Office 365, etc.

Endpoint: application and security logs from laptops, desktops and servers or third party endpoint solutions

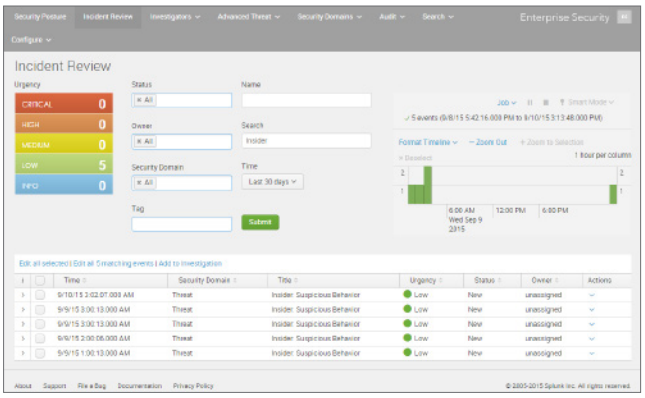
Custom Apps: live event streaming via JavaScript, Java, REST, Syslog

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. In addition, all Splunk UBA anomalies are also fed into Splunk ES for additional insight. This combined solution offers prevention, detection and response capabilities.



Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com