Using Splunk UBA to Detect Insider Threats

Highlights

- **Behavior modeling and peer group analytics to identify insiders**
- **Numerous anomaly and threat models focused towards insider thread detection**
- **Fully automated and continuous threat monitoring —no rules, no signatures, no human analysis**

It is a commonly known fact that over two-thirds of attacks or data loss originate from insiders—either caused by inadvertent actions/takeovers or malicious intentions. Enterprises need to constantly watch their environments for suspicious activities by employees, contractors and partners. Suspicious activities must be stitched into patterns that reveal insider threats in an actionable manner and in a timely fashion to prevent data and financial loss.

The Challenge

Insiders have an advantage—they are within an organization and have access to the environment. No perimeter defense or rules-based system can be effective in detecting, let alone preventing, their malicious activity. As a result, insider threats are amongst the hardest to catch and most successful in exfiltrating valuable corporate and customer data.

Since insiders already possess the necessary privileges, rules-based systems and checks do not detect malicious or suspicious activity. All of these seemingly benign and legitimate actions, when used for mal-intent, manage to evade even the smartest security tools today, leaving IP theft, financial fraud and other corporate crimes undetected until it's too late.

The Solution

The common thread across various forms of insider threats is the deviation of a user's or an asset's behavior from its past or from its peer groups. This deviation can indicate fraudulent or malicious activity, which is the key to detecting these actors.

Behavior of entities, especially users, devices, system accounts, and privileged accounts, can be mined to reveal anomalies, even when they occur in low frequency and over extended periods of time.

Splunk User Behavior Analytics (Splunk UBA) not only captures the footprint of these threat actors as they traverse enterprise, cloud and mobile environments, but also runs them through its advanced machine learning algorithms to baseline, detect deviations and find anomalies continuously. These aberrations are then stitched into a meaningful sequence over time using pattern detection and advanced correlation to reveal the actual kill chain, which is not only comprehensible but also immediately actionable.

"Our single largest challenge, especially since we are a bank with billions in assets. Only a behavior-based approach that monitors my employees can solve our problems."

— CISO, major US bank

User and Entity Behavior

Understanding user and entity behavior—and its context—is the key to determining insider threats. In order to detect suspicious behavior, Splunk User Behavior Analytics creates a continuously self-learning baseline of each user, device, application, privileged account and shared service account, based on which it derives deviations from the normal.

Splunk User Behavior Analytics assigns a score to denote the intensity of the threat to each user/account so that the enterprise can not only review insider threats on a daily basis, but also watch their top malicious users and take preventive action.

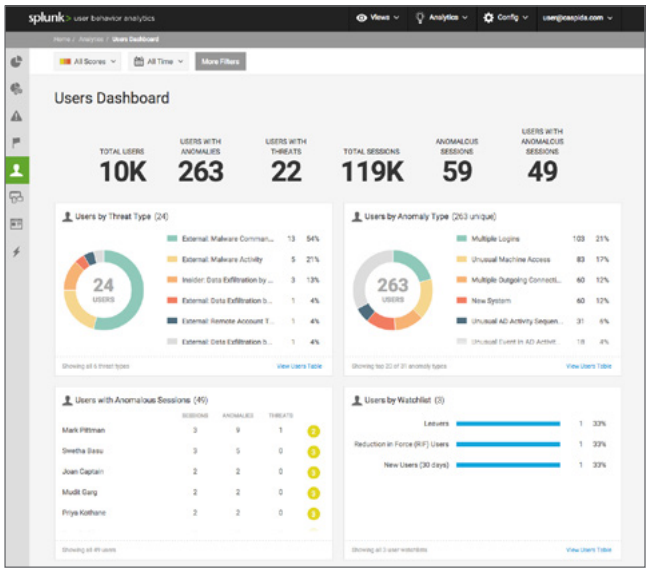
Sample Threats Detected

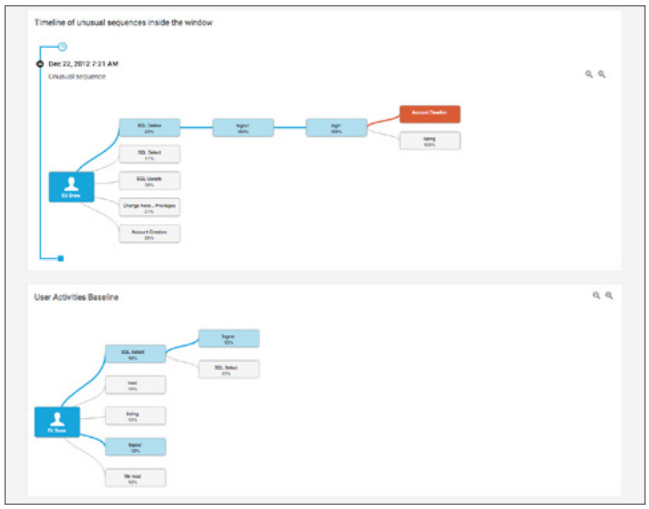
- **Privileged Account Abuse –** inappropriate usage of access permissions
- **Privilege Escalation –** transformation of identity and access credentials
- **Data Exfiltration –** the act of stealing private, confidential and sensitive data within an organization by malware or an attacker
- **Unusual activity –** accessing external domains, remotely accessing high privileged assets, and unusual login duration, time or location
- **Credential Compromise –** stealthy takeover of accounts for malicious purposes

Why Behavior Analytics from Splunk?

Machine learning, statistical profiling and other anomaly detection techniques need a foundation. A massively scalable and readily available data platform is required to support advanced analytics—one that provides users accessibility, quality and data coverage from a range of security and enterprise systems. 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. The threat detection capabilities in Behavior Analytics extend the search/pattern/expression (rule) based approaches currently in Splunk and Splunk ES for detecting threats.

Splunk can provide the data platform and security analytics capabilities needed to allow organizations to monitor, alert, analyze, investigate, respond, share, and detect known and unknown threats regardless of organizational size or skillset.





Splunk User Behavior Analytics - Users Dashboard

Learn more about Splunk User Behavior Analytics by contacting ubainfo@splunk.com.

22-13552-Splunk-UBA to Detect Insider Threats-111-TB