Preventing Account Compromise with User and Entity Behavior Analytics

Challenge

Innovative threat actors apply socially engineered attacks, such as spear phishing, to gain control of valuable resources through a privileged user's account. Successful account takeover of users with access to sensitive material means hackers can initiate nefarious activity without triggering common alarms associated with outside attacks. Sixty-eight percent of breaches take months or longer to discover[1] – this number is buoyed by difficult-to-detect privileged account takeovers.

Insider threats result in data exfiltration or damage to systems or information. With newly acquired account access, perhaps the threat actors can cause significant damage to your organization. They might create a new account to transfer company funds or information. Or they could use the stolen credentials to move laterally across your network to access account information – targeting new prospects for further compromise.

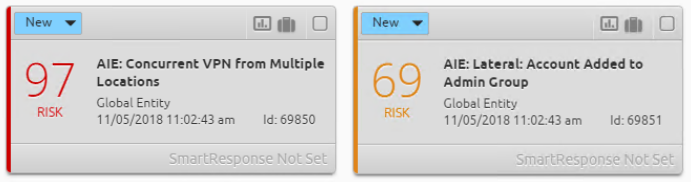
Going undetected for months provides ample time for a threat actor to access sensitive data and cause major damage. With no immediately discernible way to see if a threat actor hijacked a privileged user's account, the challenge ultimately lies in detecting when user "John Smith" is no longer John Smith.

Solution

LogRhythm's UEBA allows you to promptly detect, investigate, and remediate suspicious insider threat behavior through sophisticated security analytics.

Around 80 percent of common threats are traditional "known-knowns" – threats that analysts can readily see and remediate. The majority of incoming attacks can be readily and automatically handled by LogRhythm AI Engine's scenario-based analytics. You can utilize built-in analytics scenarios or create custom rules to establish tactics, techniques, and procedures (TTPs) and signature-based indicators of compromise (IOC) rules to quickly recognize and categorize different known scenarios within their threat landscape.

For the more difficult 20 percent of "unknown-unknown" threats that analysts cannot easily detect, LogRhythm's behavioral analytics surface more nuanced anomalous behavior. Within the platform, machine learning (ML) enables deep behavioral profiling by providing anomaly detection that recognizes subtle shifts in user activity. LogRhythm UEBA also performs peer group analysis, identifying anomalies in the behavior of individuals relative to their peers. The platform assigns threat score cards to anomalous behavior based on a user's prior actions and peer group analysis, allowing analysts to prioritize threats that may be most pressing as true insider threats.



Prioritized, risk-based alarms provide immediate identification of critical events that indicate activity related to a compromised account.

Benefits

Built-in Functionality: Scenario-based analytics are built into the LogRhythm NextGen SIEM Platform, significantly reducing your workload and providing immediate value to your LogRhythm investment. In utilizing ML to help your security operations center (SOC) defeat evolving threats, your analysts can focus on creative problem solving for more relevant, qualified threats – reducing your mean time to detect (MTTD).

SmartResponse: SmartResponse™ actions allow you to automatically remediate incoming known threats with playbook actions. Through a mix of prebuilt and custom SmartResponse actions, your SOC can utilize automation to isolate and shut down threats quickly – reducing your mean time to respond (MTTR).

Dashboard Metrics: Digestible, intuitive dashboards highlight threat response metrics and provide measurable analytics for both analyst and executive review. This gives you access to customized analytics to help you monitor potentially risky users.

1. Verizon Data Breach Investigations Report, 2018

Threat Lifecycle Management (TLM) Workflow with UEBA

LogRhythm's Threat Lifecycle Management (TLM) security workflow guides customers through our platform's various solutions. This end-to-end framework provides a comprehensive means for analysts and SOC managers to handle incidents quickly and effectively. Below are the steps of the TLM workflow that LogRhythm customers experience with UEBA.

Collect: Centrally collect data that reveals user activity, such as authentication logs and application log-ins, data transfer and access, and internal and external context. Uniformly prepare collected data to reveal key details and associate all activity to specific users with LogRhythm TrueIdentity™.

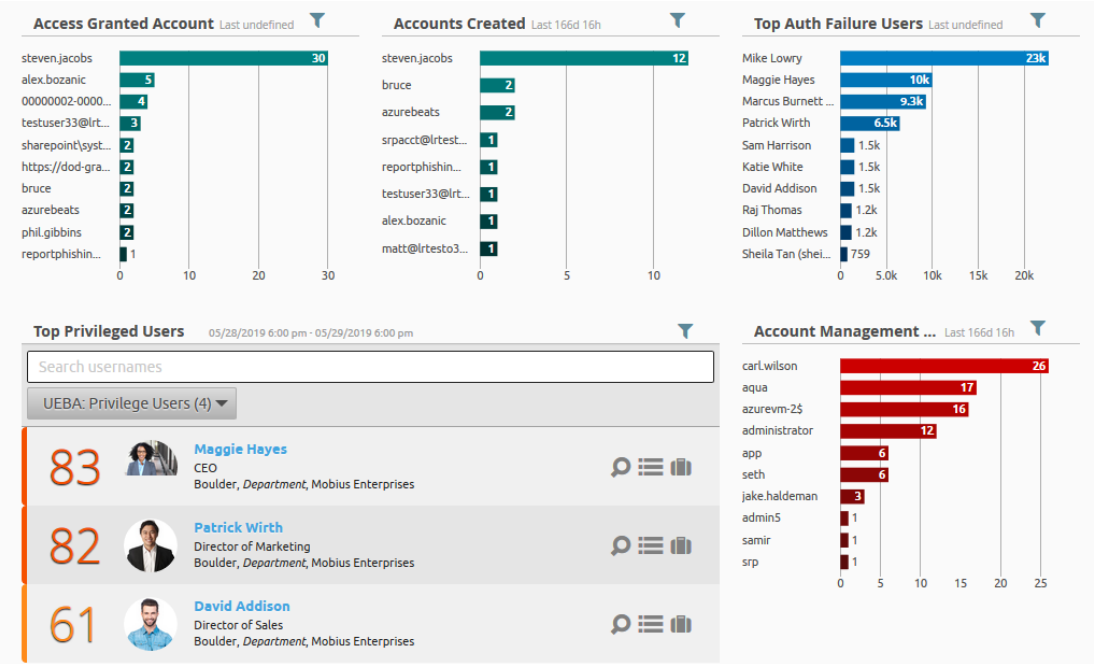
Discover: Through the combination of scenario- and ML-based analytics techniques, use LogRhythm UEBA to effectively deliver full-spectrum analytics and enable comprehensive monitoring for known and unknown threats and identifying risks through score cards.

Qualify: Focus on the most concerning user-borne threats by prioritizing the riskiest events and users so that you can uncover threats before they result in a damaging cyberattack. Leverage LogRhythm's built-in prioritization capabilities to enable multi-tier security operations teams.

Investigate: Explore LogRhythm's central repository of user activity data by searching, drilling down, and pivoting through data to investigate the threat. Enable team collaboration with workflows designed to enable rapid detection and response.

Neutralize: Stop the threat before it harms your organization by executing SmartResponse actions, such as suspending the privileged user account and invoking a memory dump for post hoc forensic analysis.

Recover: Strengthen your organization's resilience to user-borne threats by identifying and eliminating bottlenecks in technology, people, or processes that slowed detection and response. Address delays in capturing contextual user data and performing lookups through implemented SmartResponse integrations.



Customizable dashboards aggregate information across the user base to identify starting points for investigation and threat hunting.

Want to learn more about LogRhythm UEBA? Download the white paper.