Protect Your Privileged Accounts with LogRhythm UEBA

Challenge
When privileged users abuse their network access, they have the potential to cause damaging, headline-making breaches, and acts of sabotage. For example, an IT user could abuse his or her permissions by accessing a file in finance to view co-worker financial information. This IT user abused his privileges and gained access to sensitive data for his own personal use, despite such a file being unnecessary to his work. Such a data breach typically results in millions in fines and losses due to privacy violations and negative press.

Privileged account abuse is difficult to detect or anticipate, as this type of crime relies heavily on human behavior. Privileged account abusers can have a number of motivating factors such as monetary rewards, a workplace dispute, or sheer curiosity. For instance, disgruntled employees have been known to delete or corrupt crucial data as a means of retribution. Whatever the motive, these insiders often access this sensitive data as a means to a malicious end and have the potential to cause immeasurable harm to your business.

Solution
With LogRhythm UEBA, you can monitor for data exfiltration, policy violations, and other dangerous activity. To avoid a data breach, your organization must detect and respond quickly to anomalous activity. User and entity behavior analytics (UEBA) helps you monitor for known threats and behavioral changes in user data, providing critical visibility to uncover user-based threats that might otherwise go undetected.

It can be challenging to keep track of privileged users and ensure all access is appropriate. LogRhythm automatically monitors and baselines user behavior to recognize significant deviations and provide the immediate identification of malicious activity.

LogRhythm UEBA tracks your privileged user activity by monitoring for unauthorized new account creation, temporary accounts, privilege escalations and group membership changes, abnormal access, and other risky activity. You’ll be able to identify when a privileged user accesses systems or files that are out of their norm or not mission critical to their work.

Benefits
Recognize a Potential Threat with Machine Learning:
Machine learning (ML) enables your SIEM to recognize patterns and spot anomalies without tuning requirements or being explicitly programmed to do so. With LogRhythm utilizes ML to recognize suspicious user activity or concerning shifts in behavior. Machine learning-enhanced UEBA can leverage risk information to identify new activity that conflicts with expected patterns, such as a low-risk user suddenly connecting to a high-risk system and transferring large amounts of data from it to a laptop. ML supervises your network so that your security analysts can focus on creative problem solving for qualified threats — reducing your mean time to detect.

Comprehensive User Profiling with LogRhythm TrueIdentity™:
LogRhythm TrueIdentity™ maps disparate user accounts and related identifiers to build a comprehensive baseline of a user’s actual identity. By baselining a user’s profile and comparing that activity to the individual’s peers, you can rapidly surface anomalous behavior for qualification and investigation.

Rapidly Neutralize a Threat with Security Orchestration Automation and Response (SOAR):
LogRhythm’s embedded SOAR capabilities feature pre-built playbooks and SmartResponse™ actions. Pre-built playbooks contain executable best practices and guided case workflows to enhance collaboration across your
entire security team. SmartResponse actions allow you to automatically notify your team about a potential threat and collect additional contextual information, such as threat intelligence about a host. SmartResponse actions can also be used to perform mitigation and countermeasures such as automatically removing the permission groups of a host that is exhibiting anomalous behavior. Through SOAR, your security operations center (SOC) can utilize automation to isolate and shut down threats quickly – reducing your mean time to respond.

Maximize SOC Efficiency and Identify Areas of Improvement with 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 future potentially risky users. Metrics track your team's time to detect and time to respond to a threat. You can determine if your team is consistently improving in remediation times and overall performance, verifying that your SOC is operating at peak efficiency.

Neutralize User-Based Threats with Effective Threat Lifecycle Management

Threat Lifecycle Management (TLM) is a framework for more effective threat recognition and mitigation. LogRhythm's NextGen SIEM Platform helps align your SOC's workflows to enable more effective TLM through risk-based alarms, guided drill-downs, and pivot searches. LogRhythm facilitates threat detection with scenario and behavioral analytics. It expedites responses to security events via automated investigatory steps and countermeasures called SmartResponse actions. The below outlines the processes that enable effective TLM 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 analytic techniques, UEBA effectively delivers full-spectrum analytics, enabling comprehensive monitoring for threats known and unknown and labeling 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 malicious insiders and prevent them from continued abuse of their access. Utilize LogRhythm's built-in prioritization capabilities to enable multi-tier security operations teams to function together seamlessly.

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

Neutralize: Stop an insider before harm can be done to your organization by executing SmartResponse actions, such as suspending the privileged user account or removing the user from his permissions group. SmartResponse actions can be configured to automatically execute or for approval-based execution. You can rapidly neutralize a threat automatically or with a simple click to approve an action.

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

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