Detect the Misuse of Admin Privileges with LogRhythm UEBA

Challenge

Administrators are important to your organization's security. Admins need privileged access to manage networks and systems to perform their jobs effectively. These trusted users act as security enforcers to keep your organization's sensitive information safe. However, these very same users are your biggest security risk. Even with the best intentions and appropriate policies, guidelines, access controls, admins can inherently open security holes or introduce vulnerabilities.

When an admin unintentionally shares access to sensitive files or inadvertently exposes your organization to risk by misusing privileges, we call this "admin misuse." For example, an admin may grant a service account broader system access to alleviate an application permission issue, introducing a vulnerability point for a hacker/malware. While unintentional, misuse of admin privileges opens the doors to malicious activity and a damaging breach against your organization.

Without advanced analytics, admin misuse is difficult to detect. The discovery of a breach takes months or even years to discover among insiders.[1] Whatever the source of the breach or anomalous activity, you need to detect and respond to admin account misuse and accidental missteps to avoid a devastating breach.

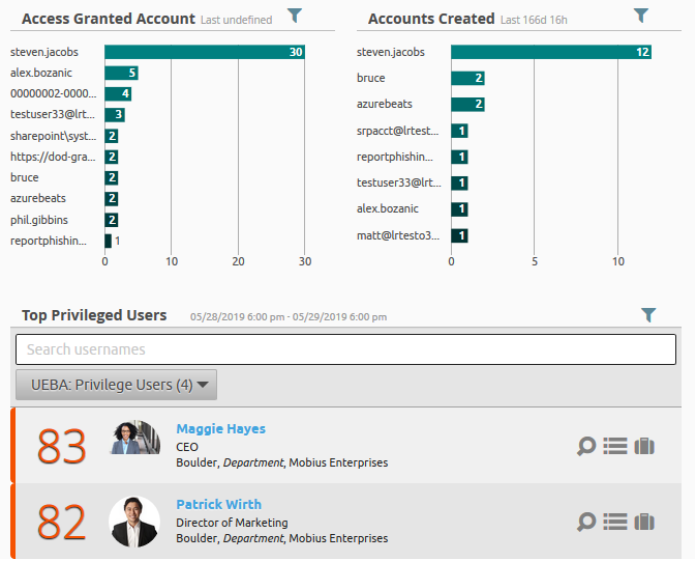
Solution

To detect a possible incident or anomalous behavior, you need to act quickly. User and entity behavior analytics (UEBA) helps you monitor for known and unknown threats and changes in user behavior, giving you greater insight to detect a possible threat or breach you might not otherwise uncover.

LogRhythm UEBA detects when access rights may break company data policies and when they are being misused. Its algorithms monitor the unauthorized creation, use, and deletion of admin accounts, as well as the elevation of permissions and suspicious use of admin accounts. LogRhythm's UEBA solution also monitors activity and triggers alarms when significant behavioral shifts occur.

LogRhythm provides a single view to enable threat detection, including dedicated dashboards for UEBA.

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 the norm or not mission critical to the user's work.



LogRhythm provides a single view to enable threat detection, including dedicated dashboards for UEBA.

UEBA Benefits

Maximize Threat Detection: To keep your organization protected, LogRhythm's UEBA solution features both scenario-based and machine learning (ML)-based analytic techniques. Scenario-based analytics help your organization surface and prioritize known attacks – in real time – by applying established tactics, techniques, and procedures (TTPs) and signature-based indicators of compromise (IOC) to recognize known scenarios along the Cyberattack Lifecycle.

Deep behavioral profiling enabled by supervised and unsupervised ML provides anomaly detection by recognizing subtle shifts in user activity.

Detect and Respond to Unauthorized Data Access/Exfiltration: When an unauthorized user is elevated to or accesses an admin account, LogRhythm UEBA can

1. Insider Threat: One pattern, four scenarios, thirteen countermeasures, Verizon Insights, Oct. 23, 2017

keep you informed. LogRhythm's full-spectrum analytics combined with native file integrity monitoring (FIM) helps you detect when a user inappropriately accesses protected data – in real time.

Embedded Security Orchestration and Automation Response (SOAR) capabilities, including LogRhythm's SmartResponse™ actions, allow you to automatically respond by isolating a host that is exhibiting anomalous behavior, or removing all permissions until an analyst can fully investigate. SmartResponse actions can be analyst-approved. These automated responses empower your team to shut down threats quickly – reducing your mean time to respond (MTTR).

Dashboard Metrics: LogRhythm UEBA offers digestible, intuitive dashboards that highlight threat response metrics and provided measurable analytics for analysts and executives. This enables you to access customized analytics that will help you monitor anomalous occurrences tied to your admin accounts.

Supporting Cohesive Workflows for Effective Threat Lifecycle Management

LogRhythm's NextGen SIEM Platform aligns your team's processes to enable effective Threat Lifecycle Management (TLM), helping your team sort through the noise to identify, investigate, and mitigate high-priority threats. This end-to-end framework helps analysts and SOC managers manage and mitigate incidents quickly and effectively. Below are the steps of the TLM workflow that LogRhythm customers experience with UEBA.

Collect: With LogRhythm NextGen SIEM, centrally collect data that reveals user activity, such as authentication logs and application log-ins, data transfer and access, active directory, host logs, and internal and external context. Uniformly prepare data to uncover key details and associate all activity to specific users with LogRhythm TrueIdentity™.

Discover: Through the combination of scenario- and ML-based analytics, use LogRhythm UEBA to effectively deliver full-spectrum analytics and enable comprehensive monitoring for threats known and unknown and rates 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: Drill down and sort through data to determine if, in fact, a misuse of an admin account occurred. Determine your response action based on the threat score. Maintain a list of users authorized to make changes administratively to quickly validate misuse.

Neutralize: Automate response actions to stop the admin account misuse. Use SmartResponse™ actions to disable the admin account and isolate the host from the network to stop the threat from further harming your organization.

Recover: Data filters back into the LogRhythm NextGen SIEM Platform by automatically creating a case file that contains all information and forensic evidence such as log data and email attachments related to the admin misuse. The LogRhythm NextGen SIEM Platform stores such incidents for further analysis, enabling you to strengthen your reporting efforts and help prevent similar attacks in the future.

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