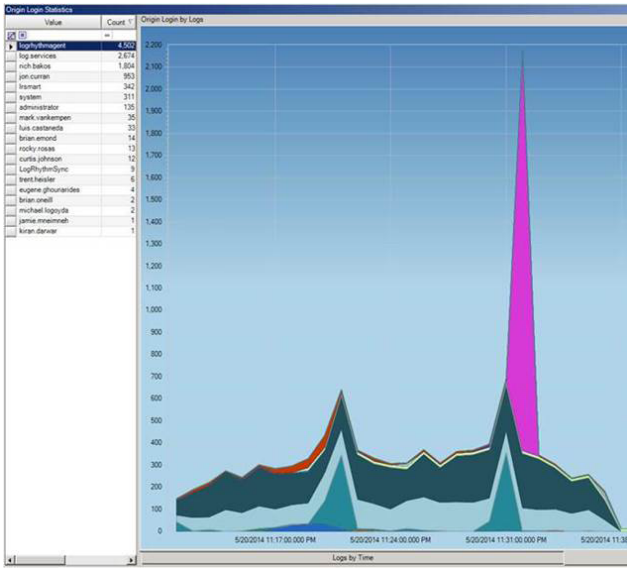
LOGRHYTHM LABS EMBEDDED EXPERTISE

Security Analytics Suite - Privileged User Monitoring

LogRhythm Labs

Privileged user accounts have direct access to sensitive data systems, making them a key component of network security. A compromised privileged user account can result in the loss of intellectual property, compromised data integrity and damaged reputation. In addition, due to their high clearance levels, accounts with escalated privileges also pose a significant insider threat. As a result, it is considered a best practice to closely monitor privileged account use.

LogRhythm's Privileged User Monitoring Security Analytics Suite includes a set of saved searches, reports, and analytical rules to allow enterprises to detect suspicious activity from privileged users. The suite leverages the advanced research from LogRhythm Labs' dedicated team of security experts to recognize behavioral patterns indicative of privileged user account misuse or compromise within LogRhythm's Security Intelligence Platform. Knowledge from the Labs team is continually embedded in the suite via bi-weekly updates based on continuous research.



Privileged User Monitoring - Investigation on Privileged User Activity

The Privileged User Monitoring Security Analytics Suite automates the task of continuously monitoring accounts with elevated privileges. By performing real-time correlation and behavioral analytics across privileged accounts use of various applications and devices, the suite is able to deliver meaningful alerts and automated remediation when suspicious privileged user activity is observed. Through LogRhythm's analytics, key scenarios can be captured illustrative of abuse, such as use of temporary accounts or mass account modifications. The suite supports the identification of privileged user account abuse and recognizes early indicators of either insider threat activity or compromised credentials.

Additionally, LogRhythm integrates with Active Directory to automatically and seamlessly set up Privileged User Monitoring with group-based rules for accounts with elevated privileges.

Privileged User Monitoring in Action

LogRhythm uniquely recognizes account-level detail such as origin user and impacted user to distinguish when a user performs actions on a different account. The Privileged User Monitoring Security Analytics Suite helps organizations detect the following scenarios:

New Account Added to a Privileged Group: Enterprises need to be able to detect and monitor new accounts being added to a privileged user group. The Privileged User Monitoring Suite triggers an alarm whenever the common event "Account Added to Group" is observed. Administrators can approve or deny a Smart**Response**™ plug-in that will automatically add the user to a self-maintaining list of privileged users. This automates the management and oversight of assigning user access to privileged groups to expose unauthorized or suspicious activity.

User Impersonating an Admin Account: Administrators need to be alerted when unauthorized accounts attempt to run programs as administrators. LogRhythm's Privileged User Monitoring Suite detects any user not on the privileged user list attempting to run a Windows program as an administrator. LogRhythm can also detect when a Unix or Linux user not in the sudoers group tries to sudo a process. When this activity is observed, LogRhythm triggers an alarm.

Unauthorized Mailbox Access: Organizations need to be able to detect inappropriate access to corporate email accounts. LogRhythm's Privileged User Monitoring Suite can detect whenever a user tries to repeatedly access another user's Exchange mailbox, either successfully or unsuccessfully. When this activity is observed, LogRhythm triggers an alarm enabling IT and security teams to take immediate action.

LogRhythm's Privileged User Monitoring Security Analytics Suite provides out-of-the-box Lists, AI Engine Rules, Reports, Investigations/Layouts and Smart**Response**™ plug-ins that enable organizations to detect suspicious privileged user behavior. The suite is constantly updated based on ongoing research from LogRhythm Labs. Below is a sample of the content provided in the suite.

Application Lists

Privileged Users	List of users with escalated privileges
Privileged Groups	List of groups where any member of the group inherits elevated privileges
Sensitive Users Email	List of sensitive Exchange user accounts

AI Engine Rules

Mass File Deletion by a Privileged User	Privileged user may be destroying large amounts of data
Password Changed on Multiple Accounts by a Privileged User	Privileged user changing two or more account passwords
Multiple Accounts Deleted by a Privileged User	Privileged user deleting more than one account
Multiple Accounts Disabled by A Privileged User	Privileged user disabling more than one account
Multiple Users Added to Privileged Group	More than three users being added to a Privileged User group
Multiple Users Removed from Privileged Group	Multiple users removed from a Privileged User group
Impersonation	User not in Privileged User list right-clicks on any process and chooses "Run as administrator"
Multiple Failed Attempts to Logon To Non-Primary Exchange Account	User repeatedly tries to access another user's Exchange account in the "Sensitive Users Emails" list and the user is not the primary Windows account on that mailbox
New Administrator Activity	New user is added to a privileged user group
User Not In Sudoers File	User not in Privileged User list tries to sudo anything on *NIX host and is not in the sudoers file on that host
Password Modified by Privileged User	Privileged User changes the password of a privileged user account (not their own)
Privileged User's Password Modified	Someone changes the password of a privileged user account (not their own)
Recently Disabled Privileged User Account Access Success/Failure	A recently disabled/deleted privileged user account attempts to authenticate/access resources on the network

Reports

Privileged User Activity Summary	Report showing privileged user activity based on users specified in the Privileged User list
Non-Primary Mailbox Account Activity	Report showing users accessing Exchange accounts specified in the list "Sensitive Exchange Accounts"

Investigations / Layouts

Privileged User Activity	Investigation filters down on the Privileged Users list generated by the Privileged User Monitoring Suite

Smart**Response**™

User Management	Automatically disable or enable an Active Directory account
Add Item to List	Automatically adds users to privileged user list

Deployment

The Privileged User Monitoring Security Analytics Suite can be deployed in environments with multiple operating systems including various Linux, Windows, and Solaris distributions. Implementation is streamlined by providing pre-populated lists with commonly escalated privileged groups that can be customized to match organizational structure. Reports, searches, and analytical rules share these common lists

©2014 LogRhythm Inc. | LogRhythm_Solution_Brief_ Privileged_User_Monitoring _05.14