USE CASE

# Alerting on the Absence of an Event

How do you know the total impact of a change control such as a patch management reboot? Or if your revenue generating devices are up and running throughout a distributed environment? If a user's credentials are compromised, do you have the means to anticipate expected activity as well as noticeably abnormal behavior? Many times these questions are more effectively answered not by what activity is recorded, but by what activity is not recorded.

While most solutions are capable of detecting and alerting on specific events taking place, most fall short when it comes to alerting on expected behavior. You need to know not only when the wrong thing happens, but when the right thing doesn't. With the complexity of today's networks, this can be as difficult as listening for the sound of a single raindrop in the middle of a thunderstorm.

## LogRhythm can notify in the absence of an event, whether based on an expected event or as the result of a correlated behavior.

| Monitoring for Expected Behavior | Validating Cause and Effect | Decreasing Downtime |
|---|---|---|
| **CUSTOMER CHALLENGE** | | |
| Many stealth attacks involve the use of stolen credentials. As a result, malicious behavior will frequently be overlooked because it originates from a supposedly legitimate source, allowing attackers unrestricted access to a targeted network. | Patch management frequently requires a reboot after installing critical security patches and updates. When a patch is rolled out to thousands of servers, particularly when many are remote, knowing when and where an individual server fails to restart among thousands can be a daunting task. | An outage may be detected but it is frequently difficult to know that all aspects of a server restarted properly. The machine may reboot but critical processes may still not be running. |
| **LOGRHYTHM SOLUTION** | | |
| LogRhythm can alert administrators to the absence of expected behavior, such as when a user logs in to a secure server and fails to log out within an expected time period – indicating that either policy has been violated or credentials have been potentially compromised. | LogRhythm can alert administrators when a server stops but does not restart within a certain time period. It can also send a notification when a log source is silent for a defined period of time. | LogRhythm can alert administrators whenever a process fails to restart within a certain timeframe. Process restarts can be automated, pulling all relevant information directly from the alarm message to perform automated remediation. |
| **ADDITIONAL BENEFITS** | | |
| LogRhythm's SmartResponse can be configured to disable a user account in response to specific policy violation's such as a failure to log off within a required time frame. Administrators have immediate access to real-time and historic forensic data related to the violation to validate the response. | LogRhythm's SmartResponse can be configured to initiate an automatic restart of critical servers in direct response to an alarm message. Administrators have the option to require up to three stages of authorization process prior to performing any active response initiated by LogRhythm. | LogRhythm creates an independent log of all processes and adds valuable context, including process name, user or account that owns the process, and process start time and duration. LogRhythm also provides easy list creation, allowing administrators to white-list critical processes for logical prioritization and rapid response. |