

SmartRemediation™ | Intelligent, Rapid Response

LogRhythm delivers immediate protection from security threats, compliance policy violations and operational issues with **SmartRemediation**. Intelligent, process-driven capabilities give organizations the power to automatically take action in response to any alarm. **SmartRemediation** delivers immediate action on real-world issues, such as when suspicious behavior patterns are detected, specific internal or compliance-driven policies are violated, or critical performance thresholds are crossed. LogRhythm ensures that responses are based on accurate information by performing real-time analysis on all log data, helping to minimize false positives as well as the delays associated with manual intervention.

Automated Remediation That Works for You

Many organizations find that implementing automated remediation creates more risk than it is designed to prevent. One of the problems is that it is typically an all-or-nothing process, meaning any enabled action will be taken without providing an option for external validation. Because of the number of variables tied to an individual event and the risks associated with incorrectly interrupting critical operations, most organizations are justifiably reluctant to employ automated remediation beyond that tied to the most mundane use cases.

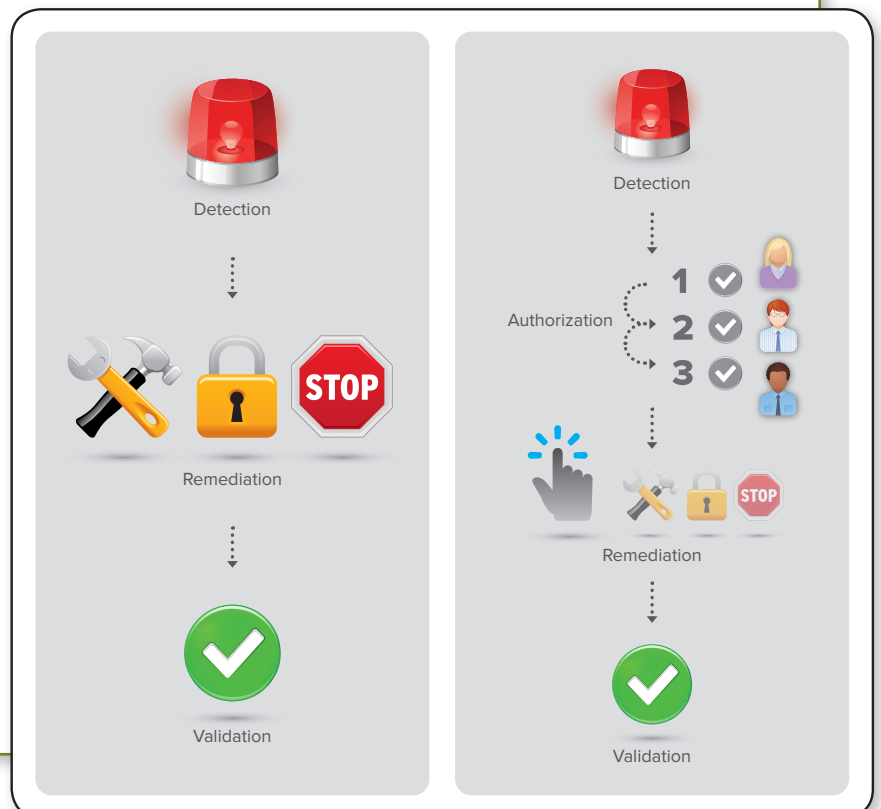
LogRhythm's **SmartRemediation** was specifically designed so that any remediation can be easily configured to meet important organizational policies and to provide assurances that each response is the correct action to take. It comes with an optional, built-in approval process that can require up to 3 levels of authorization prior to taking action. That gives organizations the option of reviewing the facts first – before the wrong person's access is removed or a critical application is mistakenly shut down. And if that particular remediation is determined to be the correct course of action, the response is already queued up for immediate execution at the click of a button.

How It Works

A simple, plug-in based GUI allows administrators to import any script-based response, which can then be activated by any advanced correlation or event-based alarm.

LogRhythm's **SmartRemediation** includes:

- The ability to run any script in response to specific alarms
- Optional requirements for up to three levels of authorization
- Targeted responses to exact alarm parameters, such as:
 - Suspicious IP addresses to block
 - Specific rogue users to quarantine
 - Individual processes to start or stop
 - Over 50 unique fields for maximum precision
- Incident Response Management with:
 - Current remediation status
 - Alarm recipient tracking
 - Authorization path auditing
- One-click testing for script validation



SmartRemediation in Action

LogRhythm Labs provides out-of-the-box access to practical scripts designed to address common organizational issues related to security, compliance and operations. SmartRemediation can execute any script that a user can create, with optional safeguards to require up to three levels of authorization before performing any action. Examples include:

Advanced Threat Detection & Response (External)



Problem Malware frequently attempts to access an environment by logging in to multiple servers, moving from one target to the next until access is granted.

Detection LogRhythm can alarm on suspicious behavior, such as access attempts to multiple hosts within the network from a single IP Address or nonwhite-listed location.

Response SmartRemediation can pull the attacking IP Address directly from an alarm and add it directly to a firewall ACL, instantly terminating potentially dangerous access to your network.

Advanced Threat Detection & Response (Internal)



Problem Systems administrators have the ability to access and modify systems and create accounts with escalated privileges, allowing them to engage in a broad range of malicious activity while avoiding detection.

Detection LogRhythm can notify when any new account with escalated privileges is created, or if suspicious modifications have been made to accounts accessing critical systems.

Response SmartRemediation can automatically remove newly added or recently modified privileged accounts until the activity has been verified as legitimate.

Compliance Automation & Assurance



Problem Many compliance regulations require strict access controls to confidential data, such as protected health information (PHI) or customer credit card accounts.

Detection LogRhythm can determine which users are authorized to access critical assets or specific files, detecting in real-time when an access policy is violated and generating an alarm.

Response SmartRemediation can immediately remove any user guilty of an access violation from the network until the incident can be investigated, actively enforcing policy and protecting critical assets.

Operational Intelligence & Optimization



Problem Detecting when all aspects of a server have restarted properly after routine maintenance is challenging – particularly in large enterprises with a large number of distributed hosts

Detection LogRhythm can independently detect when a critical process stops and/or fails to restart following a specific event, such as a reboot.

Response SmartRemediation can restart individual processes, pulling all relevant information, such as the process name and impacted host, directly from the alarm.

LogRhythm Headquarters

3195 Sterling Circle
Boulder, CO 80301
303-413-8745

LogRhythm EMEA

Siena Court, The Broadway
Maidenhead Berkshire SL6 1NJ
United Kingdom
+44 (0) 1628 509 070

LogRhythm Asia Pacific Ltd.

8/F Exchange Square II
8 Connaught Place, Central
Hong Kong
+852 2297 2812