Data Sheet

SOAR | SmartResponse™ Automation

LogRhythm
The Security Intelligence Company

LogRhythm respondX is a security orchestration, automation, and response (SOAR) solution.

SmartResponse™ Automation is a LogRhythm RespondX feature that automates tasks for streamlined efficiency across the security response workflow.

Automation Helps Your SOC Accomplish More

Cybersecurity professionals are hard to find and even harder to keep, making it extremely difficult for organizations to build a mature security program. According to the 2018 $(ISC)^2$ Cybersecurity Workforce Study, there is a global shortage of close to three million cybersecurity professionals across the industry.

The $(ISC)^2$ study further indicates that SOC staff are more likely to be dissatisfied and switch jobs when they spend too much of their time repeating mundane tasks. Job responsibilities laden with tasks that fall into this category include security administration, incident response, and endpoint security management.

Operating in this inefficient response model leads to:

- **high staff turnover with rising salary costs**
- **longer periods of threat exposure from unaddressed security alarms**
- **lack of program maturity gained from strategic improvement focused work**

To overcome these challenges, SOC managers need to more effectively utilize their limited resources to gain consistent results. Automated response workflows help empower your SOC team to accomplish more and reduce the time it takes to protect against evolving security threats.

Activate the full potential of your SOC by using SmartResponse Automation for seamless execution of actions right at the source of your SIEM data and alarms, resulting in maximum productivity with minimum wasted effort or expense.

Benefits

- Simplify security response
- Improve response times
- Free analysts from mundane tasks
- Advance SOC program maturity
- Scale security operations
- Minimize impacts of tool sprawl

Collaborate Effectively

Security organizations recognize the value of using automation, however many are unable to dedicate the staff needed to properly develop and maintain effective integrations for their team.

Overwhelmed security analysts often resort to developing their own home-grown scripts to cut through alarm fatigue and manual processes. However, this can exacerbate issues, because when teams use an assortment of isolated techniques, scripts, and tools that are siloed and therefore not auditable or sharable, it is difficult to develop efficient, repeatable response workflows.

SmartResponse Automation provides a collaborative framework for sharing efficient task reduction to decrease energy expenditure and improve incident response times across the entire team.

With **SmartResponse Automation**, your analysts can trigger a vulnerability scan, quarantine an infected host, and disable a user account in seconds.

Activate Efficiency

Create Custom Plugins
Create and test your own custom plugins with the built-in automation toolkit using any common scripting language, including Python and PowerShell.

Tested & Certified Plugins
LogRhythm SmartResponse Automation Plugins (SRPs) enable trusted workflows by packaging a collection of fully tested and certified prebuilt actions for third-party integrations.

Measure Improvement

Incident response processes often involve many different people, teams, and technologies that result in scattered and incomplete visibility. To eliminate the burden of manually tracking every step taken to resolve each alarm, Case Metrics automatically captures all incident response activity.

Reportable audit trails and case metrics, organized by milestones, help you measure and refine your processes, communicate with management, and address compliance controls.

By measuring the effectiveness of your SOC, you will identify areas for improvement and gain insights to help you prioritize what tasks to automate next. Enabling you to simplify complex procedures into the click of a button and decrease the mundane tasks your team must perform daily. As a result, your team can shift their focus towards more satisfying and significant activities that advance the maturity of your security program.

Flexible Execution Options

Manual
Ad-hoc execution across cases and investigations

Approved
Authorized execution with up to three cascading approvers

Automatic
Triggered execution of one or more actions from an alarm

Remote
Extended host execution by LogRhythm SysMon Agents

Chained
Orchestrated execution of conditional sequenced actions

Streamline Workflows

To help you get started, LogRhythm offers an extensive library of prebuilt plugins for:

Collaboration

Send alarm notifications to messaging tools like Slack for updates across any device and accelerate incident investigation by grouping related alarms into a single case, then add a playbook and assign an analyst to:

- **Stay connected**
- **Expedite alarm triage**
- **Simplify communication**
- **Kick-off response workflows**

Contextualization

Retrieve host, user, and policy information for additional context enrichment with one-click before or during investigation to:

- **Expose threats**
- **Reduce false positives**
- **Qualify incidents faster**
- **Reduce platform switching**
- **Discover the scope of an incident**

Remediation

Respond to incidents by disabling access points and patching vulnerabilities and close the loop on investigations by updating information across systems and lists to:

- **Stop threats faster**
- **Reduce tedious steps**
- **Prevent "fat-finger" mistakes**
- **Ensure tasks like updates occur**
- **Secure execution with audit trails**
- **Restrict sensitive data access errors**
- **Enable easy execution of complex tasks**

Visit the SmartResponse Automation Plugin Library to look up integrations with your existing security solutions
https://logrhythm.com/products/smartresponse-automation-plugin-library/