PRODUCT OVERVIEW

SmartResponse™ Automation Framework

LogRhythm®

Incident response in seconds, not days

When an organisation detects a compromise in their network, speedy incident response can mean the difference between quick containment and a damaging data breach. Organisations that rely solely on manual processes struggle to reduce response times and face higher risk. Companies working to accelerate response times should automate common investigation and response actions.

Unfortunately, automation has been out of reach for most organisations. Developing a home-grown solution is usually cost-prohibitive, and existing commercial options are either inflexible or require extensive and costly customisations.

An effective automation tool must offer:

- Efficient workflows and flexible approval processes
- Straightforward integration into the IT environment
- Support for multiple operating systems
- Ability to traverse disparate networks
- Integrated testing
- Minimal cost and complexity

Automated remediation that works

Smart**Response**™ uniquely enables automated incident response. It also allows semi-automated, approval-based operation so users can review the situation before countermeasures are executed.

LogRhythm reduces the time needed to perform common investigation and mitigation steps, preventing high-risk compromises from snowballing. Examples include triggering a vulnerability scan on a suspect endpoint, and more drastic measures such as quarantining a compromised endpoint or disabling a suspect user account.

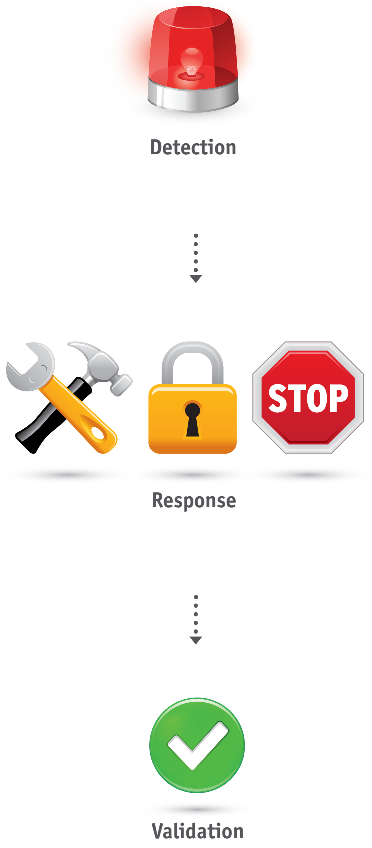
Pre-built & custom plug-ins

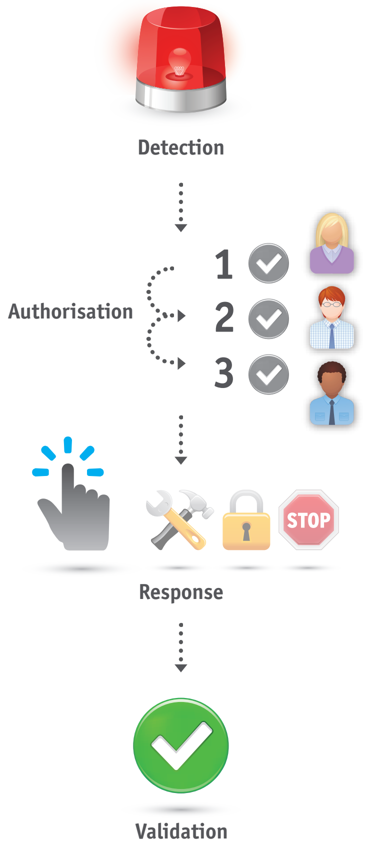
LogRhythm Labs provides customers an extensive library of pre-built Smart**Response**™ actions. LogRhythm also helps users create custom plug-ins using their preferred programming/scripting technology, such as Bash, Java, .NET, Perl, PowerShell or Python. Users can test custom plug-ins with an integrated tool that documents output and identifies errors. These pre-built and custom Smart**Response**™ actions put customers in control.

Alarm integration

The Smart**Response**™ Automation Framework is tightly integrated into the LogRhythm platform, providing seamless continuity across the end-to-end threat detection and response workflow.

Users set up Smart**Response**™ actions to be triggered by specific alarms. These alarms can pass data to the Smart**Response**™ action, enabling dynamic, precise execution. Multiple Smart**Response**™ actions can be executed from a single alarm, enabling simultaneous investigation and mitigation actions.





Sophisticated approval processes

Users might want to wait for Smart**Response**™ execution until an incident responder or a formal approval chain can verify the actions. With Smart**Response**™, users can implement sophisticated approval scenarios as a pre-condition for execution. LogRhythm also supports more sophisticated approval chains, including multi-party approvals from different groups when cross-organisational approvals are required.

Flexible execution options

The LogRhythm Smart**Response**™ Automation Framework supports several action execution options:

- **Full chain execution:** Configure Smart**Response**™ actions to run in a fully automated manner without approvals. This capability speeds compromise containment, neutralising high-risk threats within seconds.

- **One-click execution:** Execute an action manually. LogRhythm Smart**Response**™ Automation Framework allows single-click, instantaneous execution of responses from within the LogRhythm user interface.

- **System monitor remote execution:** Initiate actions in remote sites over disparate networks that may not be accessed directly through IP routing. Smart**Response**™ enables this capability with responses that can be delivered to and executed locally on System Monitor agents. Smart**Response**™ remote execution thus enables a truly global, distributed incident response capability.

Full audit and accountability

Incident response processes often involve many different people, teams and technologies. With Smart**Response**™, LogRhythm tracks and logs all activity undertaken to contain and mitigate the compromise. This eliminates the burden to manually capture and consolidate incident response information, including approvals and notifications. Capturing audit trails helps an organisation refine its incident response processes, communicate with management, and address any compliance controls.

Make the most of existing investments

LogRhythm Smart**Response**™ Automation Framework allows users to integrate with current and future security technologies easily. It provides broad vendor support, so users can respond across the network, regardless of the security devices, IT infrastructure, networking, system and applications that are deployed.

Use cases

Incident response teams are empowered with pre-packaged and customisable plug-ins, which can reduce time to respond from days to minutes. Smart**Response**™ use case examples include:

- **Endpoint quarantine:** Identify the network port where a suspicious device is located and disable the port/device.
- **Suspend users:** If an account compromise is suspected, halt a user's account access—no matter what device they use.
- **Collect machine data:** In the case of malware, Smart**Response**™ can gather forensic data from the suspect endpoint.
- **Suspend network access:** If data exfiltration is occurring, the incident response team can kill the connection by updating the access control list used by corporate firewalls.
- **Kill processes:** If a team detects unknown or blacklisted processes on critical devices, Smart**Response**™ can kill the specific running program.