SOLUTION BRIEF

Security Automation and Orchestration

LogRhythm
The Security Intelligence Company

Incident response in seconds, not days

When an organisation detects a compromise, rapid incident response can mean the difference between quick containment or a damaging data breach. If you rely solely on manual processes, you will struggle with longer response times and face higher risk. But if you automate common investigation and response actions and if you use a centralised workflow for performing incident response, you will minimise response times and make your organisation more secure.

LogRhythm security automation and orchestration capabilities increase analyst efficiency to support the entire threat investigation, through full remediation and recovery. These efficiencies empower your team to more effectively respond to and remediate cyber threats.

Case and incident management

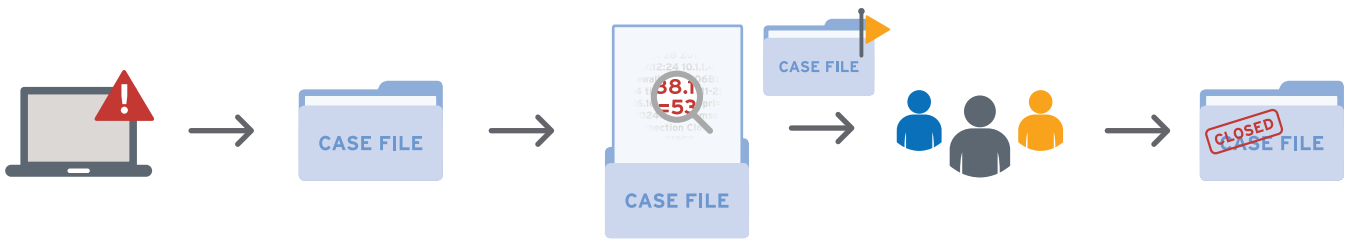
- Seamless workflow throughout the UI
- One-click case creation from alarm
- Tagging and workflow customisation
- Group collaboration supporting tiered operations
- Cyber Evidence Locker™ for securing and sharing artifacts like logs, files, and annotations
- One-click threat intelligence lookups
- Real-time feed of investigation and response activities
- Customisable dashboards
- Rest API for third-party integration
- Metrics and reports on mean time to detect (MTTD) and mean time to respond (MTTR)

SmartResponse™ Automation Framework

- Simple plug-in architecture
- Library of plug-ins created by LogRhythm Labs
- Tools for developing and importing custom and community plug-ins
- Ability to target actions using event data
- FIPS-certified credential management for actions that require a login
- Automated and approval-based execution options, including support for multi-party approval chains
- Secure remote execution via LogRhythm System Monitor
- Integrated test facility to enable validation of automation actions
- Ability to implement playbooks by pre-staging SmartResponse actions for specific alarms

Security Automation and Orchestration in action

Security Automation and Orchestration expedites workflows across the threat lifecycle



Threat detection

Case Management can be started from any concerning activity or high-impact event.

Case creation

A case can be instantly created with a single click, accelerating the ability to qualify threats within the incident response orchestration and automation process.

Investigation

Any Case can be viewed and accessed from any screen. Relevant alarm details, log data and notes are easily added through an intuitive one-click process.

Collaboration

Any authorised LogRhythm user can access a Case from anywhere, enabling real-time collaboration for expedited incident recognition and response.

Mitigation & response

Implement and automate countermeasures that mitigate risks presented by the threat and review incident details to eliminate future exposure.

Streamline threat detection and response with Case Management and Automation

Problem: During the investigation process, an analyst typically performs multiple searches. This is necessary to understand the nature, intent, and scope of a suspicious activity—and whether the incident represents true risk to the organisation. If not stored and managed centrally, the data accumulated throughout these searches may be difficult to interpret, lead to an incorrect conclusion, or result in an incident slipping through the cracks.

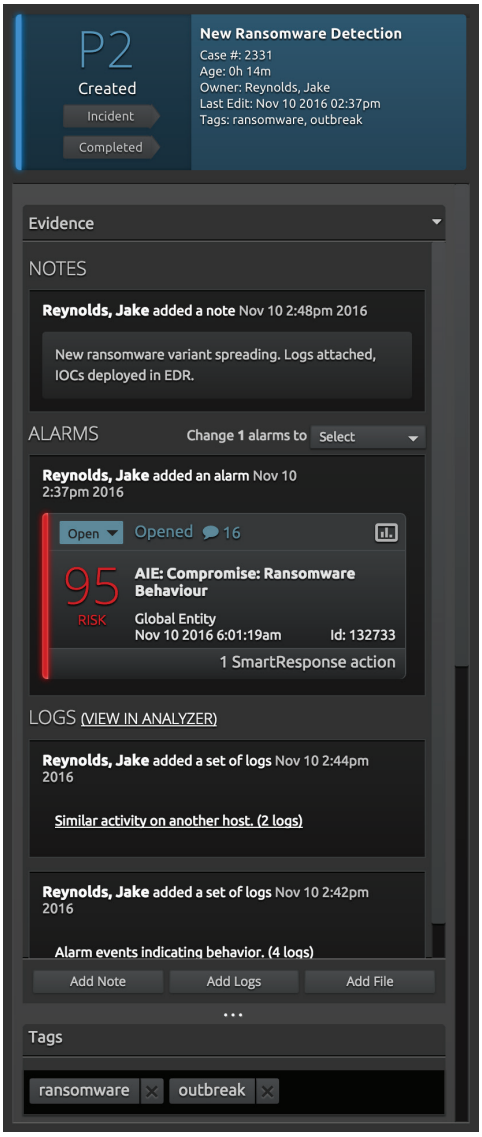
Solution: LogRhythm case management and SmartResponse automation streamline incident response and enable security orchestration, with prescribed analyst workflows, team collaboration tools, and built-in escalation processes.

It's easy to create and track remediation and recovery progress within LogRhythm. An analyst or incident responder can easily escalate a case, label a priority to the case, and assign an investigator to the case. An analyst can also utilise case tags and view a real-time news feed of all completed actions, with timestamps for each case.

During an investigation, LogRhythm serves as the central repository for all associated evidence. You can store information from a dashboard, alarm, search result, or even externally generated evidence like a screen capture. Annotation is possible through case notes.

Lastly, when a case is closed, case management surfaces any open issues for final resolution, such as open alarms and unapproved automation actions.

Results: Case management enables organisations to drastically improve the maturity and efficiency of their security operations and incident response efforts. For streamlined viewing, users can quickly filter and sort cases based on specific incidents, status, case owner, and age. Any case can be shared with collaborators for immediate access to centralised case details. Collaborators can add forensic evidence and annotations to expedite threat detection and response in real time. Access can be restricted to ensure confidentiality. All activity is tracked as part of the case history, providing real-time status and a tamper-proof audit trail. By using case management, threats don't slip through the cracks, investigations are streamlined, and incidents are resolved much more quickly.



Remediate at scale with SmartResponse automation

The SmartResponse automation framework provides seamless continuity across the end-to-end threat detection and response workflow, without APIs or custom integration work. LogRhythm Labs delivers an extensive library of out-of-the-box SmartResponse actions, and customers are enabled to also develop their own custom plug-ins.

The framework stages specific actions based on observed activity within the IT environment. These alarms can pass data to the SmartResponse action, enabling dynamic, precise execution. SmartResponse uniquely enables automated incident response, as well as semi-automated, approval-based operation so users can review the situation before countermeasures are executed. Multiple SmartResponse actions can be executed from a single alarm, or within a Case, enabling simultaneous or stepped investigation and mitigation actions.

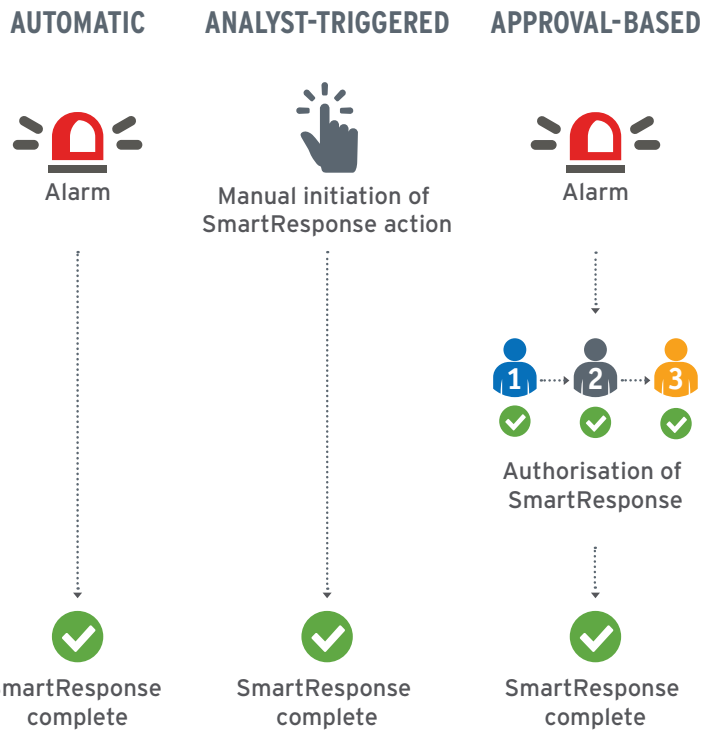
"Investigations and reporting works three times faster with LogRhythm. We are experiencing further reduced MTTD and MTTR by maximising efficiencies generated by orchestration and automation."

—IT Security Engineer, Large University

Flexible execution options

The LogRhythm SmartResponse automation framework supports several action execution options:

- **Automatic execution:** Configure SmartResponse actions to run in a fully automated manner. This capability speeds containment of high-risk threats and is particularly suitable for reoccurring actions.
- **Analyst-triggered execution:** Execute an action manually, with just one click. SmartResponse enables instantaneous execution of responses from within the LogRhythm user interface.
- **Approval-based execution**: Configure SmartResponse actions to run after one or more approvals are provided. Actions can be configured for a single approver or a hierarchical chain of approvers before the action is initiated.
- **Remote execution**: Centrally manage the execution of actions across remote sites. SmartResponse enables this capability with actions that can be delivered to and executed locally via a LogRhythm agent, enabling a truly global incident response capability.



Automation use cases

Incident response teams are empowered with pre-packaged and customisable automation, which can reduce time to respond from days to minutes. SmartResponse 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, SmartResponse can gather forensic data from the suspicious 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 an analyst detects an unknown or blacklisted process on a critical device, SmartResponse can kill it.

Enable auditing and accountability

LogRhythm tracks and logs all activity undertaken to contain and mitigate compromises, eliminating the burden to manually capture and consolidate incident response details. Captured audit trails and reportable case metrics enable you to refine your incident response processes, communicate with management, and address any compliance controls.

Make the most of existing investments

Security automation and orchestration allows you to integrate current and future security technologies easily. It provides broad vendor support, so you can respond across the network, regardless of the security devices, IT infrastructure, networking, system, and applications that are deployed. This accelerates response and remediation across the threat lifecycle management.

Benefits of LogRhythm Security Automation and Orchestration

- Centralise and safeguard security investigations
- Standardise incident response processes
- Enable efficient team collaboration
- Automate workflows and response
- Profoundly reduce mean time to respond to incidents

To schedule a demo, please contact your customer relationship manager.