Data Sheet

Security Orchestration, Automation, and Response

LogRhythm
The Security Intelligence Company

Incident Response in Seconds, Not Days

When your organization detects a compromise, rapid incident response can mean the difference between quick containment and a damaging data breach. Relying solely on manual processes increases response times, leaving you more greatly exposed to risk. However, automating common investigation and response actions and protocolizing incident response workflows minimizes response times, better securing your organization.

With LogRhythm, you can search, make decisions, collaborate, and respond faster – before a threat harms your organization. Native security orchestration, automation, and response (SOAR) capabilities in the LogRhythm NextGen SIEM Platform reduce the number of security tools and steps your team needs to respond to events.

LogRhythm's SOAR capabilities include guided workflows for rapid and accurate incident response, increasing efficiency, facilitating higher quality incident response, and optimizing analyst workload. Furthermore, by adopting case playbooks, analysts can respond and remediate within a single platform, enabling greater efficiency and efficacy when every second counts. Supporting the entire threat investigation, these efficiencies empower your team to better respond to and remediate cyber threats.

Security Orchestration, Automation, and Response in Action

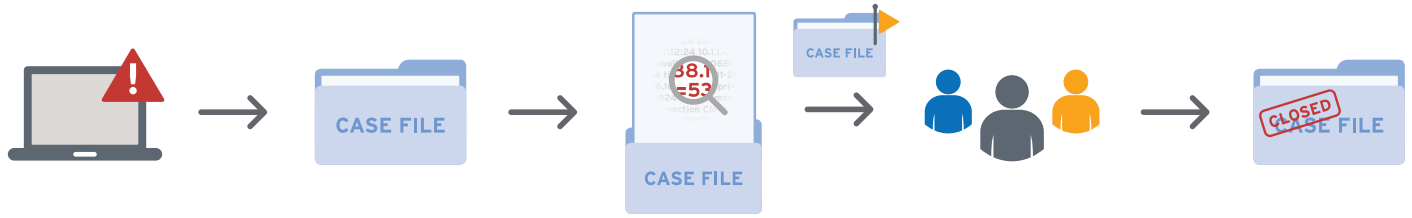
LogRhythm's SOAR aligns with escalation processes, ensuring efficient and expedited incident response workflows across the threat lifecycle. Integrated case management and task automation provide consistent investigative tools throughout the incident response process. Moreover, they simplify evidence identification and collection into a central repository.

Case and Incident Management

- Case playbooks for incident management
- Case tasks with automated due dates
- Tagging and workflow customization
- Group collaboration supporting tiered operations
- Evidence Locker for securing and sharing artifacts like logs, files, and annotations
- One-click threat intelligence and contextual lookups
- Real-time feed of investigation and response activities
- Customizable dashboards, including multi-case task views
- REST API for third-party integration
- Metrics and reports on mean time to detect (MTTD), mean time to respond (MTTR), time to qualify (TTQ), and time to investigate (TTI)
- Automated and approval-based execution options, including support for multi-party approval chains

SmartResponse™ Automation Framework

- Ability to implement playbooks by pre-staging SmartResponse actions for specific alarms
- Simple plug-in architecture
- Library of plug-ins created by LogRhythm and Community members
- Tools for developing custom plug-ins and integrated test facility to enable validation of automation actions
- Ability to target actions using event data
- FIPS-certified credential management for actions that require a login
- Secure remote execution via LogRhythm SysMon



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

Case Creation
A Case can be created with one click, streamlining threat qualification within the incident response process.

Investigation
Following an assigned playbook, a Case can be updated throughout the UI to include relevant alarm details, log data, and notes.

Collaboration
Case tasks enable multiple level SecOps teams to divide responsibilities to best leverage differing skill sets and expedite incident response.

Mitigation & Response
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 an investigation, an analyst typically performs multiple searches to understand the nature, intent, and scope of a suspicious activity and whether it represents true risk to the organization. If centrally

accessible, 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 with prescribed analyst workflows, team collaboration tools, and built-in escalation processes.

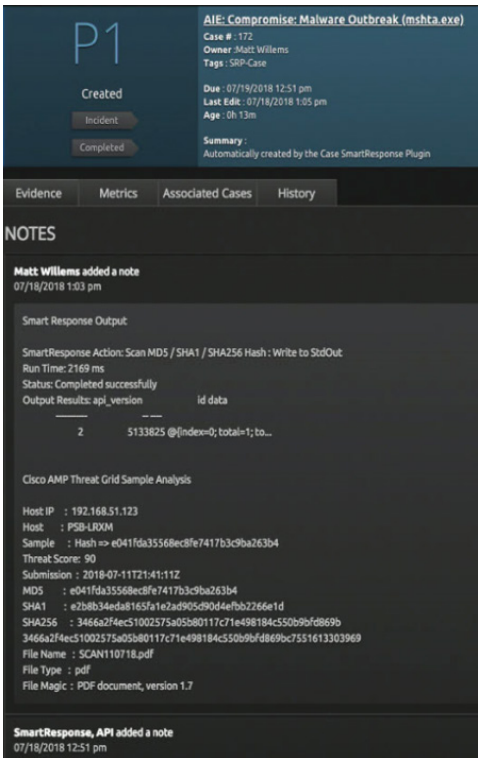
It's easy to create and track remediation and recovery progress within LogRhythm. For streamlined viewing, users can quickly filter and sort cases based on specific incidents, status, case owner, and age. An analyst or incident responder can easily add playbooks, escalate a case, set a priority, and assign an investigator. They can also utilize case tags and view a timestamped news feed of all completed actions.

During an investigation, playbooks provide procedural tasks with LogRhythm serving as the central evidence repository. You can store information from a dashboard, alarm, search result, and even externally generated evidence like a screen capture. Annotation is possible through case notes.

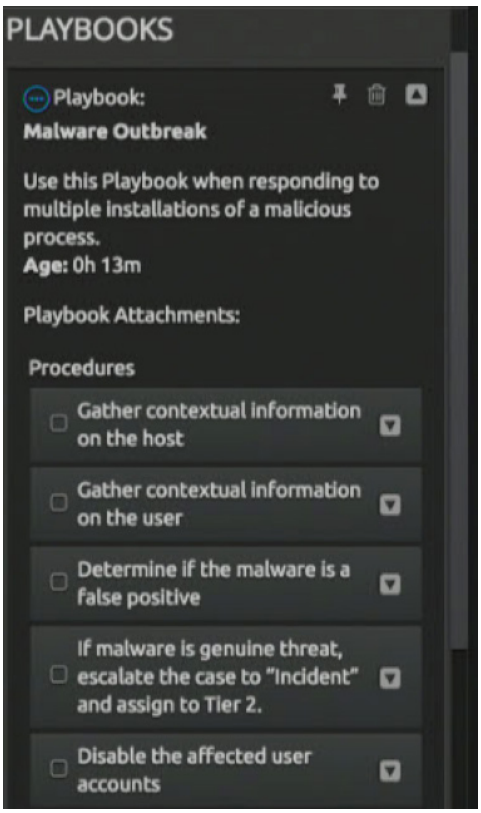
A case can be shared with collaborators with specific task assignments and due dates. Collaborators add forensic evidence and annotations to expedite threat detection and response in real time. Access can be restricted to ensure confidentiality. All case activity is tracked in the case history, providing the current status and a tamper-proof audit trail.

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

Results: Case management enables organizations to drastically improve the maturity and efficiency of their security operations and incident response efforts. Companies report it streamlines their investigations and helps them resolve incidents more quickly.



A case contains many types of evidence including logs, SmartResponse output, and analyst notes



Playbooks provide defined steps to follow in resolving a case, providing consistency and direction for SOC analysts

Empower Analysts with Case Playbooks

Problem: There is an industry-wide shortage of seasoned, experienced analysts as well as rapid employee turnover in Tier 1 positions. The difficulty of recruiting and retaining security analysts makes providing consistent and effective incident response problematic.

Solution: With LogRhythm, prebuilt, customizable playbooks enable your Tier 1 analysts to investigate incidents using consistent methodologies to yield measurable outcomes.

Customizable playbooks provide a repeatable workflow available to the entire team and allowing all security analysts to scale and accelerate their investigations and responses – no matter the level of security expertise each team member possesses. Your Tier 1 analysts use playbooks to handle more common investigative tasks while learning best practices; your senior analysts are freed to focus on areas of higher value and risk to your organization.

Results: With LogRhythm, you'll be able to utilize pre-built playbooks developed by LogRhythm Labs for common threat types, assuring your team is more consistent, productive, and accurate throughout their investigations.

Remediate at Scale with SmartResponse Automation

The SmartResponse automation framework provides continuity across your threat detection and response workflow, without APIs or custom integration work. Available in the Community, LogRhythm provides an extensive library of out-of-the-box SmartResponse actions and tools for customers to develop their own plugins.

The framework programmatically stages specific actions based on observed activity. Alarms pass data to the SmartResponse action, enabling dynamic, precise execution. SmartResponse uniquely enables automated incident response, as well as approval-based invocation so users can review the situation before executing countermeasures. Multiple SmartResponse actions can be executed from a single alarm or within a Case, enabling simultaneous or stepped actions.

Automation Use Cases

Incident response teams are empowered with pre-packaged, customizable automation, reducing time to respond from days to minutes. SmartResponse use case examples include:

Endpoint Quarantine: Disable the port/device where a suspicious device is located.

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 close the connection by updating your network infrastructure's access control list.

Kill Processes: If an analyst detects an unknown or blacklisted process on a critical device, SmartResponse can kill it.

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.
- **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.

- **Analyst-Triggered Execution:** Execute an action manually with just one click. SmartResponse enables instantaneous execution of responses from within the LogRhythm user interface.
- **Remote Execution:** Centrally manage the execution of actions across remote sites. SmartResponse enables analysts to invoke actions delivered to and executed locally via a LogRhythm agent, enabling global incident response.

Enable Auditing and Accountability

LogRhythm tracks and logs all steps taken to contain and mitigate compromises, eliminating the burden of manually capturing incident response activity. Captured audit trails and reportable case metrics enable you to refine your incident response processes, communicate with management, and address compliance controls.

Make the Most of Existing Investments

SOAR allows you to integrate current and future security technologies easily. It provides broad vendor support, so you can respond across your network, including your security devices, IT infrastructure, networking, system, and applications. This accelerates response and remediation across your threat lifecycle management processes.

Benefits of LogRhythm Security Orchestration, Automation, and Response

- Centralize and safeguard security investigations
- Standardize incident response processes
- Enable efficient team collaboration
- Automate workflows and response

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