DEMISTO | LogRhythm

Automated Security Operations and Incident Response

Benefits

- Harness rich, correlated data from LogRhythm in Demisto for automated, playbook-driven response
- Further enrich LogRhythm-prepared data with intelligence from other security technologies via Demisto's orchestration
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation
- Shorten decision-making cycle by automating key tasks with analyst review

Compatibility

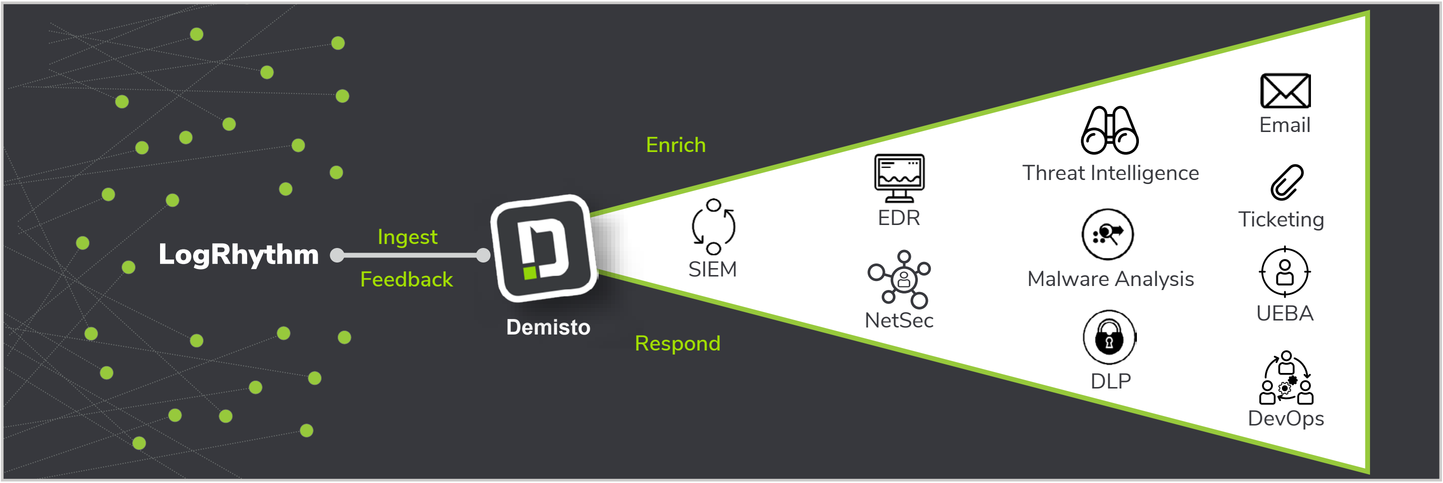
- Products: Demisto Enterprise, LogRhythm NextGen SIEM
- LogRhythm Versions: 7.3+

Sophisticated cybersecurity threats are continually emerging to target enterprises utilizing multiple attack vectors and entry points. Facing this challenge, security teams often expend time that could be better spent quelling the attack collecting data from disparate sources and performing repeatable tasks instead. SOCs need security tools that empower analysts with access to rich, correlated data, and automate repeatable tasks so that they have the time and energy they need for incident resolution.

Analysts can now leverage Demisto's security orchestration and automation capabilities with LogRhythm's deep data collection, preparation, and security analysis capabilities for efficient and accelerated threat detection and incident response.

Integration Features

- Ingest alarms from LogRhythm to create incidents in Demisto and trigger automated triage, enrichment, and response through playbooks.
- Access LogRhythm alarms and associated statuses and comments for deeper investigations in Demisto.
- Update LogRhythm alarm statuses and comments from within Demisto to provide continued access to LogRhythm monitoring and reporting.
- Leverage hundreds of Demisto product integrations to further enrich threat detection alarms from LogRhythm and coordinate response across security functions.
- Run 1000s of commands (including for LogRhythm) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1

AUTOMATED ALARM INGESTION, ENRICHMENT, AND RESPONSE

Challenge: If SOCs use multiple solutions for data/log enrichment and incident response, it can be tough to track the lifecycle of an incident due to screen switching, data fragmentation, and lack of single-window documentation. Analysts spend time completing low-level tasks that can be better spent resolving the incident.

Solution: If SOCs use LogRhythm NextGen SIEM for data enrichment and threat detection and Demisto Enterprise for security orchestration and automation respectively, they can automate incident creation in Demisto for each alarm type in LogRhythm. They can also trigger playbooks to execute upon incident creation. These playbooks orchestrate enrichment and response actions across the entire stack of products that a SOC uses in a single screen and seamless workflow.

For example, analysts can create tickets, quarantine endpoints, retrieve PCAPs, and send emails as automatable playbook tasks.

Benefit: LogRhythm's rich insights and data coupled with Demisto playbooks can speed up incident triage and resolution. Analysts can get a comprehensive view of the incident's lifecycle, access documentation from a single source, and forego the need to switch between screens while performing investigation actions.

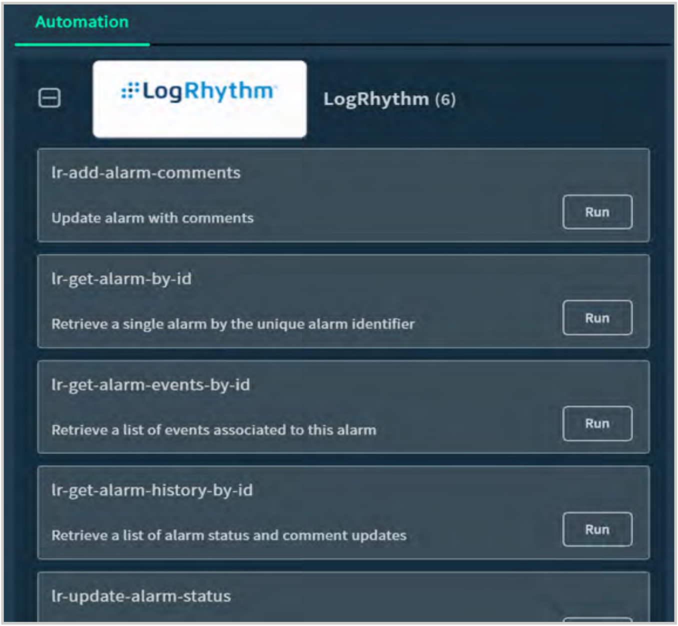
USE CASE #2

INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: While standardized, repeatable playbooks can automate commonly performed tasks to ease analyst load, an investigation requires additional tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing connections between incidents, and finalizing resolution. For organizations that depend on multiple security technologies, performing these tasks traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: After running enrichment playbooks, analysts can gain greater visibility and new actionable information about the attack by running LogRhythm commands in the Demisto War Room. For example, if playbook results present alarm details from LogRhythm, analysts can access a list of events related to that alarm and associated statuses/comments by running the respective LogRhythm command. Analysts can also run commands for other security tools in real time using the War Room, providing a single-console view for end-to-end investigation.

The War Room will document all analyst actions and over time will suggest the most effective analysts and command-sets.



lr-add-alarm-comments
Update alarm with comments

lr-get-alarm-by-id
Retrieve a single alarm by the unique alarm identifier

lr-get-alarm-events-by-id
Retrieve a list of events associated to this alarm

lr-get-alarm-history-by-id
Retrieve a list of alarm status and comment updates

lr-update-alarm-status

Benefit: The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their network from a common window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from the same window. They will also prevent the need for collating information from multiple sources for documentation.

About Demisto

Demisto is the only Security Orchestration, Automation and Response (SOAR) Platform that combines orchestration, incident management and interactive investigation into a seamless experience. Demisto's orchestration engine automates security product tasks and weaves in human analyst tasks and workflows. Demisto Enterprise, powered by its machine learning technology, acquires knowledge from the real-life analyst interactions and past investigations to help SOC teams with analyst assignment suggestions, playbook enhancements, and best next steps for investigations. The platform (and you) get smarter with every analyst action. For more information, visit www.demisto.com or email info@demisto.com.

About LogRhythm

LogRhythm is a leader in NextGen SIEM, empowers organizations on six continents to reduce risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm platform combines user and entity behavior analytics (UEBA), network traffic and behavior analytics (NTBA) and security orchestration, automation and response (SOAR) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations center (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant. Learn more at http://www.logrhythm.com.