LogRhythm

SentinelOne V2
SmartResponse™ Automated Actions

Boost cyberattack protection with LogRhythm's centralized data collection & automation

Benefits

- Allows for automated hashes to lock down systems in the event of an attack
- Improves positive alarms in the environment
- Includes additional configuration actions such as editing fixed parameters and saving the new configuration file
- Features new actions around agent and hash analysis that ensure the integrity of critical files

Solution overview

Understanding what's occurring in your network and across your endpoints is critical to stay on top of threats. But without a centralized way to collect log data, that mission can be overwhelming. You need the right tools to detect suspicious activity and act quickly. The LogRhythm SmartResponse™ automated actions for SentinelOne V2 improve your response workflow, allowing automated hash values to lock systems down if an attack occurs and blacklist malicious SHA1 hash values.

As logs are ingested into the LogRhythm SIEM Platform, the SentinelOne V2 SmartResponse automated actions use the SentinelOne RESTful API to disconnect machines from the network if nefarious activity occurs on an endpoint, as well as troubleshoot and update endpoints and investigate details surrounding various threats. Such actions can be performed from the LogRhythm SIEM via custom AI Engine rule sets or manually from the Web Console. With the SentinelOne V2 SmartResponse, you have a broader scope and greater visibility into threats that could harm your network.

SentinelOne

About LogRhythm and SentinelOne

LogRhythm and SentinelOne work together to help organizations around the globe increase network visibility and protect against modern cyberattacks. LogRhythm offers extensive support for and integration across SentinelOne's product portfolio. The combined solution empowers security teams to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence.

Log collection

Securing any security operations center (SOC) begins with high-fidelity and trustworthy log data. While other vendors outsource their log collection methodology to the SOC analyst, LogRhythm provides log sources reviewed by dedicated security experts with dozens of years of security experience. LogRhythm Machine Data Intelligence (MDI) Fabric optimizes and stabilizes the ideal route of collection for over 1,000 log sources. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts that allow for precision rule creation and comprehensive remediation efforts in the event of an attack.

The LogRhythm and SentinelOne integration includes Common Event Format (CEF) Syslog to detect common attack patterns. LogRhythm's AI Engine rules are triggered for logs that get ingested and sent to SentinelOne, as well as for log data pulled from SentinelOne.

How data collection works

The LogRhythm SIEM Platform collects from every device, application, and sensor in an environment while our MDI Fabric classifies and contextually structures every log message. Logs are streamed to the LogRhythm platform where they are parsed and normalized to the LogRhythm schema, using features such as our patented TrueTime™ process, which records the actual time of occurrence, automatically correcting time zone, device clock offsets, and collection offsets. Normalized data is then sent to the LogRhythm SIEM for analysis, storage, and reporting via a consolidated dashboard of all security events.

How automated workflows work

To streamline security response workflows, organizations can use SmartResponse automated actions, which are part of LogRhythm's security orchestration, automation, and response (SOAR) solution. LogRhythm SmartResponse automated actions accelerate response to malware threats to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the SentinelOne V2 SmartResponse. While LogRhythm has a dedicated engineering team that builds actions, this is by nature an open framework that enables SentinelOne customers to modify actions or write their own custom integrations.

The SentinelOne V2 SmartResponse contain multiple responses that are configured to execute automatically in the event of an alarm, or manually through the analyst workflow. For example, if malicious activity occurs on any endpoint, an analyst can disconnect a machine from the network. The SentinelOne V2 SmartResponse automated actions centralize functionalities of manual and automated response between the LogRhythm SIEM and SentinelOne.

In addition, the SentinelOne V2 SmartResponse also provides additional details off alarms and detects if certain kind of hash values come through the LogRhythm SIEM. This alerts analysts if immediate action is needed. Other example actions and their use cases are provided in the table on the next page.

SmartResponse™ automated actions for SentinelOne V2

Action	Description	Use Case
Create SentinelOne V2 Configuration File	Execute this response and rerun it before using other available actions whenever you change the fixed-value parameter.	Functionality that must be run first before other SmartResponse functions can be executed.
Blacklist Hash	Adds the provided SHA1 hash value as a blacklist item.	Add malicious SHA1 hash values as blacklist.
Broadcast Message and Restart Machine	Broadcasts a message on the provided endpoint and restart the endpoint.	Troubleshoot or update an endpoint; will broadcast a message before restarting a machine.
Create Firewall Rule	Creates a new firewall rule.	Create a new firewall rule according to requirements.
Disconnect Endpoint from Network	Disconnects an endpoint from the network.	Disconnect a machine from the network if malicious activity occurs on any endpoint.
Get Endpoint Information	Displays information about a specific endpoint or displays a list of endpoints.	Fetch endpoint information for analysis.
Get Hash Reputation	Displays the reputation for the given hash value.	Fetch hash reputation.
Get Threats	Retrieves the threat information based on the configured filters.	Investigate the details of various threats.
Initiate Scan	Triggers a scan on the specified endpoint.	Initiate a scan to check the health of a specified endpoint.