LogRhythm®
The Security Intelligence Company

Unlock Peak Operational Efficiency for Your SOC

Learn How SmartResponse Automation Can Help Your Team Rapidly Qualify and Respond to Threats

Your team needs to detect threats fast.

Rapid qualification and response can mean the difference between quick containment and a breach of critical data.

To do this, your people and technology must use defined process to work together like a well-oiled machine.

But how do you achieve this level of peak operational efficiency?

Tune your security operation center with SmartResponse automation.

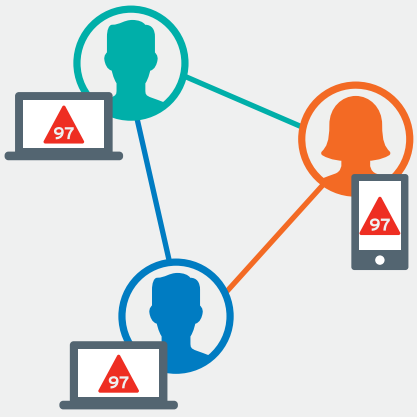
By automating common investigation and response actions with LogRhythm SmartResponse™, your team can drastically reduce its time to respond to threats.

What is SmartResponse?

SmartResponse actions – a feature of the LogRhythm NextGen SIEM Platform – take manual, repetitive work out of your team's workflow

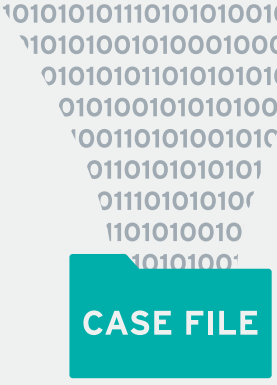
Notification & Collaboration

These SmartResponse actions alert your team so they can jump into action.



Gathering Contextual Info

These actions automatically assemble information and return it to your analysts for analysis, investigation, and case management.



Remediation

With LogRhythm SmartResponse, your team can perform all remediation actions, such as quarantining a host or disabling a user account, without having to leave the SIEM.

SmartResponse in Action

Incident Response in Seconds, Not Days

Reduce the time to preform common investigation and mitigation steps with SmartResponse automation.

See how it works.

LogRhythm AI Engine detects the presence of outbound internet relay chat (IRC) on your network – a chat protocol regularly used for command and control communication in malware.

01

Notification & Collaboration

Upon detection, a SmartResponse fires and notifies your team about the alarm via your security team's Slack channel.

After your analysts are alerted to the IRC, they need to rapidly gather information and start learning more about the external contact.

02

Gathering Contextual Info

The contextual SmartResponse action fires and gathers the information your analysts need to determine that the IP address used in the IRC is in a location from which your employees do not typically communicate.

Your analysts conclude the IRC is coming from a malicious IP address and quickly move to contain the breach through automation – while still ensuring they're responsible for calling the big shots.

03

Remediation

A remediation SmartResponse action fires, and upon your analysts' approval, blocks traffic from the host or optionally, the entire network range through integration with your perimeter firewall.

The Threat is Contained

Your team has used its time and resources to effectively stop this breach in its tracks.

Visit Shareables section of the LogRhythm Community to view all of the available SmartResponse plugins today and learn how to fully automate your SOC.

If you are not a LogRhythm customer, contact us for more information at info@LogRhythm.com.

LogRhythm®
The Security Intelligence Company