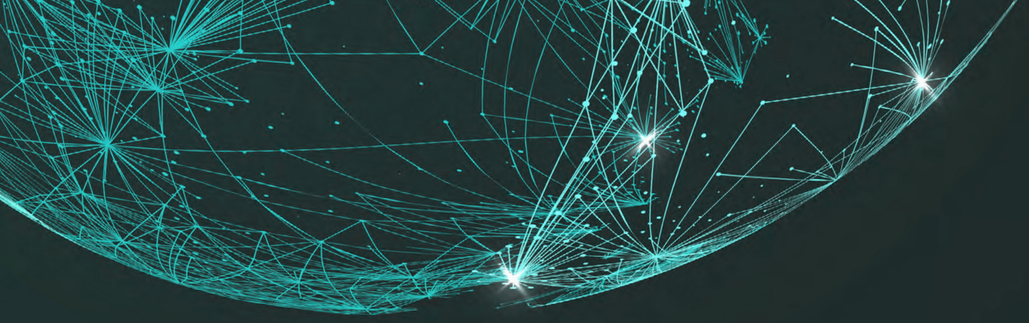


LogRhythm
The Security Intelligence Company

RespondX

LogRhythm's Security Orchestration, Automation, and Response (SOAR) Solution

There are approximately three million unfilled analyst jobs in the information security market today, and it is increasingly difficult to find skilled people to fill these roles.[1] Meanwhile, security is a growing concern for leadership across industries as threats rapidly evolve, infrastructure expands, and the penalties for breaches continue to increase.

Operating in an inefficient response model leads to:

- False positives and alarm fatigue that result in periods of threat exposure
- Inefficient fragmented workflows overloaded with mundane tasks
- Inability to manage complexity at scale

To overcome these challenges, SOC teams need orchestration and automation for effective collaboration and response efficiency.

Amplify Your Team

LogRhythm RespondX delivers the tools your SOC team needs to capture and simplify complex processes. Available with the XDR Stack, RespondX provides streamlined workflows and the knowledge transfer security teams need to effectively combat evolving threats. Because it is easy to use, RespondX is a good fit for security teams at any operational maturity level with no additional integration work or management overhead.

Encompassing the entire incident response workflow, RespondX enables your SOC team to effectively collaborate, qualify, and manage incidents with improved quality and speed. RespondX provides immediate drill-down, search pivoting, context enrichment, and other investigative capabilities only enabled by a fully embedded solution with full access to all the data and threat intelligence behind your security alarms. Amplify your team and enable them to respond efficiently, scale to address complex use cases, and advance to a new level of security maturity – without adding headcount or another point solution.

[1] (ISC)^2 CYBERSECURITY WORKFORCE STUDY, 2018

Benefits

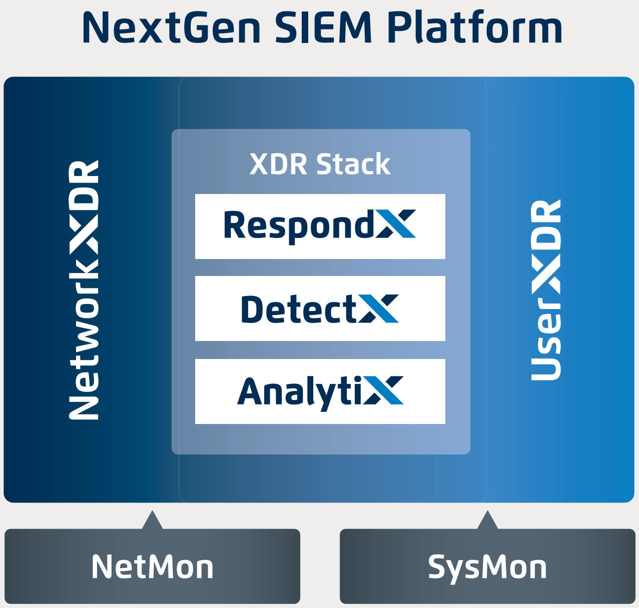
- **Triage acceleration** reduces the time and effort to qualify and investigate threats.
- **Workflow efficiency** simplifies complex processes at scale.
- **Response effectiveness** optimizes security workflows to empower analysts and increase productivity.

Features

- **SmartResponse™ Automation** reduces manual security tasks and platform switching.
- **Case Management** centralizes collaborative incident management and evidence collection.
- **Case Metrics** captures key incident response milestones and complete audit trails for reporting.
- **Case Playbooks** standardizes response processes and knowledge sharing across the security team.
- **Contextualization** enriches any type of investigation with instant context lookups.

Minimize Your Processes

When your team iterates towards peak efficiency, it also develops the ability to address more complex use cases at scale. With RespondX, your team can break down complex use cases into manageable pieces, using automation to decrease the number of steps to the ideal minimum for manual determination. This approach uses orchestration and automation to simplify use cases and decrease the overall expenditure of responding effectively. Standardizing processes within Case Playbooks further enables analysts at every level to execute quickly and consistently. The result is a security program that can continuously adapt to accommodate more data and alarms, support any type of SOC workflow, and defend against evolving attack techniques.


NextGen SIEM Platform

Advance Your Security Operations Maturity with the XDR Stack

RespondX increases the productivity of your team and advances the operational maturity of your security program. Address your SOAR use cases with RespondX to orchestrate security activities across the enterprise without the additional management overhead or integrating yet another costly product.

With LogRhythm's modular NextGen SIEM Platform design, your organization can add capabilities and increase its security sophistication as the need arises.

LogRhythm's XDR Stack centralizes all the necessary components to establish a security foundation capable of identifying malicious patterns, uncovering unknown threats, and ensuring rapid threat response and compliance adherence.

See **RespondX** and the **XDR Stack** in action by requesting a demo today!