

RespondX

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

Security remains a growing concern for leadership as threats evolve and infrastructure expands. Complicating matters, organizations face the challenging task of finding skilled analysts to fill vital security roles. Without an efficient security response model, your organization can face false positives and alarm fatigue that result in periods of threat exposure. In addition, your team may experience fragmented workflows, be overloaded with mundane tasks, and face challenges managing complexity at scale.

LogRhythm delivers the tools your SOC team needs to simplify complex processes, speed workflows, and make your organization more efficient.

Amplify Your Team

[LogRhythm RespondX](#), part of the [LogRhythm NextGen SIEM Platform](#), helps your SOC team simplify complex processes. RespondX streamlines security workflows by coordinating and automating multiple steps in the response workflow. RespondX helps SOC teams quickly collaborate, qualify, and manage incidents, providing drill-down, search pivoting, context enrichment, and other investigative capabilities.

Security teams at any operational maturity level can use RespondX. There's no additional integration work or advanced training required. With RespondX, your team can respond efficiently, address complex use cases, and increase security maturity—without adding more personnel or another solution.

Automate Your Processes

As your team becomes more efficient, it can take on more complex use cases at scale. RespondX simplifies use cases and reduces workload with [orchestration and automation](#). With RespondX, your team can decrease workflow steps by dissecting complex use cases into manageable pieces that can be automated with [LogRhythm SmartResponse™ automation](#). By using standardized processes with Case Playbooks, your team can execute tasks quickly and efficiently.

Benefits

- **Reduce time** to qualify and investigate threats with SmartResponse automation
- **Streamline workflows** with standardized response processes
- **Increase analysts' productivity** by optimizing workflows
- **Accelerate response** by simplifying complex processes at scale

Features

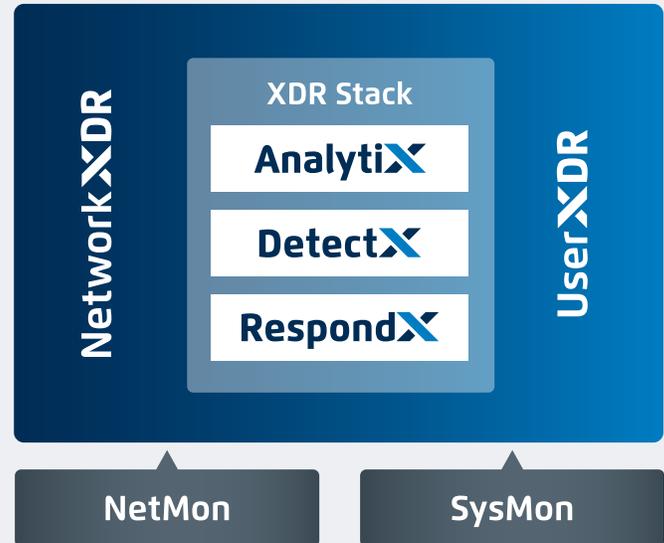
- **SmartResponse automation** reduces manual security tasks and platform switching
- **Case Management** centralizes collaborative incident management and evidence collection
- **Case Metrics** captures key incident response milestones and complete audit trails for reporting
- **Case Playbooks** standardizes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

Advance Your Security Operations Maturity with the XDR Stack

The NextGen SIEM Platform is a comprehensive set of capabilities that include the XDR Stack and other supporting elements:

- [AnalytiX](#) is a log management solution that centralizes your log data, enriches it with contextual details and applies a consistent schema across all data types.
- [DetectX](#) allows you to focus your efforts with targeted and prioritized threat detection.
- [RespondX](#) is a seamlessly integrated [security orchestration, automation, and response \(SOAR\)](#) that enables your team to effectively collaborate, qualify, and manage incidents with improved quality and speed.
- [NetworkXDR](#) helps you detect and respond to network-borne threats like lateral movement and internal access abuse.
- [UserXDR](#) helps you identify user-based threats such as compromised accounts and malicious insiders that can be difficult to detect.
- [NetMon](#) provides real-time visibility and security analytics to monitor your agency's entire network.
- [SysMon](#) helps you gain access to rich endpoint data to detect and respond to threats faster.

NextGen SIEM Platform



Deployment Options

The LogRhythm NextGen SIEM Platform can be deployed via multiple configurations including on-premise, SaaS, and hybrid.



Appliances

- Pre-staged
- Horizontal and vertical scalability
- Building-block architecture



Software

- Reference designs for dedicated hardware or virtual
- Mix and match with appliances
- Aligns to appliance building blocks



Cloud

- Support for private and public
- Reference designs and pre-created images
- Full SaaS



Interested in seeing RespondX and the XDR Stack in action?
[Request a demo today!](#)