Federal Data Sheet

DetectX

Simplify Agency Threat Detection and Compliance

As insider threats, ransomware, and more sophisticated external threats rise, security teams remain diligent in their fight to stay ahead of attackers. It's imperative for agencies to identify the most critical threats to focus resources where they will have the most impact. Information about threat severity is needed at mission-speed – and the reaction time of your security team must be just as fast.

Agencies require tools that can identify and analyze threats in real time, providing intelligence to identify attackers, categorize and rank the severity of their actions, and give visibility into every asset on the network. LogRhythm DetectX provides analysts with the visibility and rapid threat detection needed to protect your critical assets.

Target and Prioritize Threat Detection

As part of the NextGen SIEM Platform, LogRhythm DetectX provides comprehensive log collection, management, and analysis to automatically detect and alert on suspicious or threatening activities on your networks. DetectX delivers prebuilt security analytics content and visualizations designed to accurately detect malicious activity while helping your agency adhere to compliance regulations. DetectX prioritizes remediation actions to target threats that pose the greatest security liability. During log analysis, DetectX qualifies threats faster by normalizing and analyzing streams of logs to identify patterns of compromise and attack progression.

Content such as LogRhythm's MITRE ATT&CK module provides threat models, dashboards, alarms, and reports based on the adversary tactics and techniques mapped within the framework. DetectX's threat detection content reduces time on false positives while integrating relevant, actionable threat intelligence for proactive mitigation.

Simplify Compliance Through Automated Policy Management

Compliance mandates continue to challenge agencies to interpret requirements and implement necessary security controls. LogRhythm DetectX simplifies adherence to regulatory requirements by providing tools that create awareness and strengthen your overall security posture.

Our prebuilt compliance and threat detection modules automatically detect violations as they occur, removing the burden of manual reviews. LogRhythm Labs develops and updates a comprehensive library of compliance modules for FISMA, NIST, PCI, HIPAA, and other applicable mandates. Compliance content, including rules, investigations, and reports are mapped to the individual controls for each regulation. Our Consolidated Compliance Framework further streamlines your compliance program by providing a core, shared module mapped to multiple regulations, encompassing the most common cybersecurity controls.

Benefits

- **Protect mission-critical data and systems** with more effective threat detection and qualification
- **Identify and stop the latest threats** through prebuilt, continuously updated threat detection modules
- **Meet compliance objectives** and minimize budget utilization with built-in compliance automation capabilities
- **Proactively defend your agency** by applying relevant, actionable threat intelligence

Features

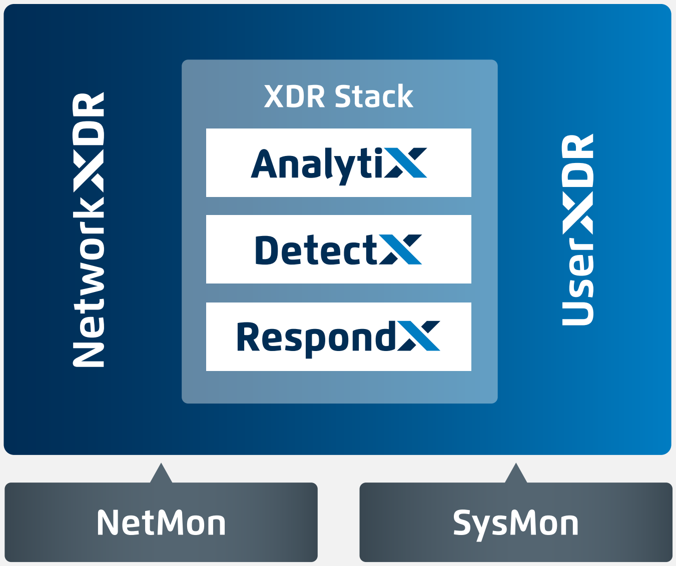
- **Out of the box support for 950+ log sources**, with the ability to ingest custom log sources, ensures that all network log data can be collected and analyzed for threat behaviors.
- **Prebuilt analytics modules** contain models and alarms that recognize known patterns and characteristics of bad behavior, whether from malicious outsiders or insider threats.
- **Threat prioritization** scores and prioritizes alarms based on risk.
- **Consolidated compliance support** helps teams demonstrate continuous compliance, detecting control-specific violations as they occur.
- **Easy-to-use rule builder** creates advanced analytics by chaining together commonly used rule blocks such as Observed, Not Observed, Unique Values, Behavioral Whitelisting, Statistical Analysis, and Trend.

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

Software offerings can be pre-deployed on a LogRhythm server or on a server or VM with appropriate specs.

The LogRhythm NextGen SIEM Platform has been awarded Common Criteria Certification at Evaluation Assurance Level (EAL) 2+. The solution has also been awarded a Certificate of Networthiness (CoN) from the United States Army. LogRhythm solutions are available for purchase via GSA, SEWP, ITES, and all major GWACs or agency BPAs.

Contact federal@logrhythm.com for a full list of LogRhythm's certifications and contract vehicles.

Interested in seeing DetectX and the XDR Stack in action?

Request a demo today!