Data Sheet

DetectX

Simplify Threat Detection and Compliance with DetectX Analytics

As ransomware and more sophisticated threats rise, security teams remain diligent in their fight to stay ahead of attackers. Yet organizations continue to chase benign threats due to limited resources and a lack of threat prioritization. Without proper tools to uncover malicious network activity or flag the latest compliance mandates, your organization may encounter false positives and alarm fatigue that result in threat exposure.

LogRhythm DetectX helps analysts gain visibility and detect threats quickly while limiting exposure to valuable assets. Analysts can target and prioritize threats using prebuilt security analytics and content customized to your environment and compliance needs.

Target and Prioritize Threat Detection

LogRhythm DetectX, part of the LogRhythm NextGen SIEM Platform, delivers prebuilt security analytics content and visualizations designed to accurately detect malicious activity while helping you meet compliance regulations. With DetectX, you can prioritize the activity that poses the greatest liability to your organization. Achieve rapid and accurate threat detection through diverse analytical techniques and use case-oriented alarms that produce a comprehensive view of malicious actions across your environment.

LogRhythm DetectX applies curated threat detection content that identifies patterns of compromise and threat progression to qualify threats faster. Content, such as the MITRE ATT&CK Module, provides threat models and alarms aligned to the adversary tactics and techniques mapped within the framework. DetectX also provides actionable threat intelligence to accelerate mitigation. LogRhythm's Threat Intelligence Service (TIS) operationalizes commercial and open-source threat intel to further corroborate malicious activity, leading to faster qualification and mitigation.

Simplify Compliance Through Automated Policy Management

Interpreting compliance requirements and implementing necessary measures to avoid legal consequences can be tricky. LogRhythm DetectX simplifies adherence to regulatory requirements and provides tools that create awareness and strengthens your 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 including PCI, GDPR, HIPAA, and NIST among others. Our Consolidated Compliance Framework includes rules, investigations, and reports mapped to the individual controls for each regulation to streamline your compliance program.

Benefits

- **Automatically prioritize security relevant activity** to address your most critical threats first
- **Achieve immediate value and long-term success** through prebuilt, continuously updated threat detection modules
- **Avoid costly violations and save time** with built-in compliance automation capabilities that align to specific controls
- **Proactively defend your enterprise** by applying actionable threat intelligence

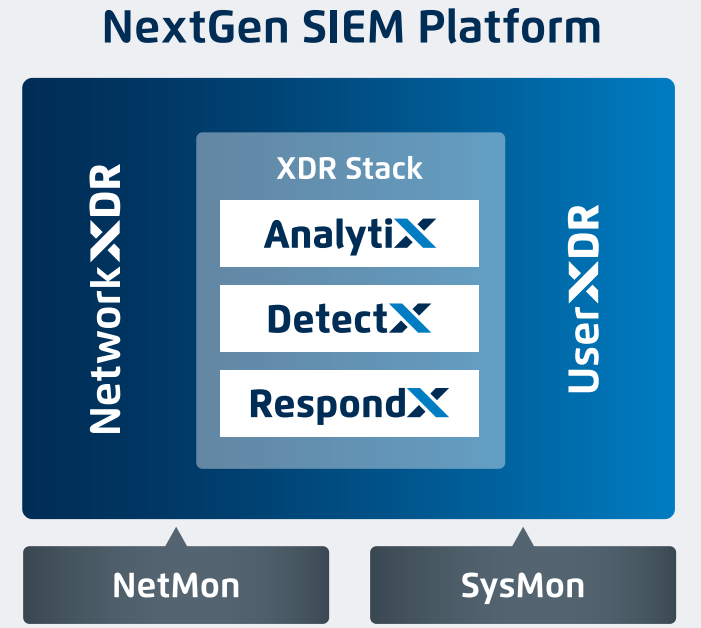
Features

- **Prebuilt analytics modules** contain models and alarms that recognize known patterns and characteristics of malicious actors
- **Threat Intelligence Service** uses STIX/TAXII to operationalize both commercial and open-source threat to feed information into the NextGen SIEM for threat qualification
- **Threat prioritization** scores and prioritizes alarms based on risk
- **Consolidated compliance support** helps teams demonstrate continuous compliance, detecting control-specific violations as they occur
- **In-memory analytics** outperform competitive solutions which require greater disk IOPS
- **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 Trends
- **Multi-stage analytics** reduce false positives for greater data accuracy and analyst efficiency

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 is 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.



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 DetectX and the XDR Stack in action?
Request a demo today!

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301

www.logrhythm.com