LogRhythm NDR

The Network Doesn't Lie

Quickly detecting and responding to network-borne threats like lateral movement and internal access abuse can be challenging. Traditional signature-based tools like intrusion prevention systems (IPS) and next-generation firewalls (NGFW) are limited to detecting threats with only a single data point at a single point in time. This creates a high reliance on signature-based approaches that can be evaded, while also generating a high number of false positive alarms. And if your team is struggling with limited resources already, these blind spots and false positives can further tax and challenge your team's ability to rapidly detect and respond to threats.

Network Detection and Response (NDR) addresses the need for continuous network monitoring and response to advanced threats. Unlike IPS and NGFW, it analyzes multiple data points over time to recognize threat indicators. Response orchestration, including automation, addresses staff shortages and churn, as well as overall team efficacy. NDR solutions are focused on providing comprehensive network visibility, relevant insights, and rapid response options to help security analysts discover, investigate, and mitigate advanced threats across the network.

Strengthen your Security Posture and Threat Resiliency with LogRhythm NDR

LogRhythm NDR is a focused network security solution that detects advanced network-borne threats in real-time and features integrated security orchestration, automation, and response (SOAR) capabilities for investigation and response. It offers immediate value and ease of use without requiring sophisticated network forensics expertise.

Using purposed, versatile sensors that generate rich network details, LogRhythm NDR incorporates multiple machine analytics approaches to expose evolving threats more effectively, including:

- Known indicators of compromise (IOC) signature-based inspection
- Tactics, techniques, and procedures (TTP) scenario-based modeling
- Behavioral analysis

The result is full coverage against threats – from known to unknown – without requiring heavy tuning or lengthy supervised machine learning training periods.

LogRhythm NDR recognizes applications at Layer 7, providing immediate visibility to the applications in use in your network. To enable more accurate machine-based analytics, the solution generates rich metadata, nuanced by the application type. Analytics are performed both at the sensor and centrally, economically distributing resource use while providing optimal insights to threat activity. Analysts are empowered via customizable dashboards, risk-based alarms, and guided workflows to recognize and mitigate threats effectively.

Expansion Beyond NDR

The power and responsiveness of LogRhythm NDR is enabled through the same advanced security analytics, centralized search and visualizations, and SOAR functionality as the LogRhythm NextGen SIEM Platform. These shared capabilities make LogRhythm NDR expandable to grow with your organization, allowing you to utilize excess capacity to monitor additional network and log data sources and to add capacity to fulfill additional security use cases across other attack surfaces, such as endpoint and user (UEBA) activity.

Benefits

- Gain the speed and full network visibility needed to combat modern attacks across your on-premise, remote, and cloud environments
- Empower incident responders with real-time network insights and analytics
- Accelerate and automate your security workflow with embedded SOAR capabilities

Use Cases

LogRhythm NDR addresses a wide array of network-borne threats, including:

- Network reconnaissance
- Compromised hosts/devices
- Lateral movement
- Data theft/exfiltration
- Command and control detection
- Ransomware

Detection

- Purpose-built network sensors
- Recognition of thousands of applications at Layer 7 with advanced analytics performed at wire speed
- Corroborate high-risk network activities at both the network and application level to minimize false positives
- Incorporate additional sources of data (e.g., log and machine data, open source, and commercial threat intelligence feeds)
- Custom and prebuilt dashboards for threat hunting

Forensics

- Searchable rich Layer 2–7 network traffic metadata
- Visualizations from categorized application traffic
- Full and selective intelligent packet capture for times when complete detail is needed
- Replay captured data for additional analysis
- Generate irrefutable network-based evidence for threat analysis, policy enforcement, audit support, and legal action

Response

- Integrated SOAR capabilities minimize response time, increase efficiency, and ensure high-quality incident response
- Guided, customizable playbooks for tracking, documentation, and enforcement of defined workflows
- Case management for end-to-end collaboration and management of alerts, evidence, and escalations
- Automated, flexible, and scriptable responses increase investigative efficiency
- Metrics for measuring and improving SOC responsiveness

LogRhythm NDR in Action

Insider Threat

Problem: An employee at a financial firm is planning to leave the company and wants to take proprietary information to his new, competing company. He attempts to transfer large amounts of sensitive company information to an external cloud storage service.

Solution: LogRhythm NDR detects early activities indicative of insider threat, such as attempts to access certain internal file repositories and other abnormal file access attempts. The solution also alerts on network activity like large file transfers. Such alerts are corroborated and elevated based on the severity of the event. At this point, either manual or automated action can be taken with LogRhythm NDR. In the manual action, an analyst can automatically create an incident case in LogRhythm NDR and prepopulate it with data relevant for an investigation, including rich network session metadata. Or, LogRhythm NDR can take automated action and immediately quarantine the account, limiting damage.

Benefit: LogRhythm NDR can automatically detect and act on potentially damaging insider threats, protecting your organization's sensitive and valuable information.

SCADA Attacks

Problem: Supervisory control and data acquisition (SCADA) systems are critical for industrial organizations. However, attacks have and will continue to occur on SCADA systems and can cause extensive damage, including loss of human life. How can SCADA systems be protected?

Solution: LogRhythm NDR can be deployed in a variety of locations to inspect the traffic flow between devices. The solution can identify and decode a wide variety of SCADA protocols, including Modbus, and is flexible enough to allow analysts to choose which functions to alert on. LogRhythm NDR was deployed in customer's SCADA environment and configured to alert on specific Modbus functions that an analyst would rarely expect to see. LogRhythm NDR detected and alerted on an unexpected function. The analyst was able to immediately investigate, determine the action was not authorized, and remediate before damage was done.

Benefit: LogRhythm NDR provides real-time visibility into SCADA environments. It detects and responds to compromises, helping prevent major breaches of industrial control grids.

Flexible Deployment Options

LogRhythm NDR software-based sensors acquire data in a wide variety of ways, including from a network TAP, SPAN port, GRE connection, or a third-party packet broker, and can be deployed as a dedicated hardware appliance or virtual machine. The solution easily integrates with existing infrastructure.

- Highly scalable appliances: Keep up as the demands of your network grow. Individual appliances support up to 5 Gbps sustained, 10 Gbps peak traffic, or more when distributed.
- Software appliances for remote sites: A flexible solution for monitoring low-bandwidth remote sites.
- Virtual sensors: Improve your visibility into your cloud infrastructure.

LogRhythm NDR is delivered as a subscription, enabling a predictable operational expense without a large capital outlay.

To schedule a demo or for more information, visit us today at www.logrhythm.com/ndr