DATA SHEET

Network Threat Detection Module

LogRhythm
The Security Intelligence Company

Your organization is likely facing increasingly sophisticated network-borne threats. A capable network analytics solution is a necessary component of a larger, holistic strategy to arm organizations with the contextual visibility to detect, prioritize, and neutralize cyberthreats.

The LogRhythm Network Threat Detection Module delivers comprehensive analytics beyond what legacy Network Behavior Anomaly Detection (NBAD) and flow analysis tools can provide. This module empowers your organization to understand the network activity occurring in your environment by delivering automated, preconfigured rules, dashboards, investigations, and reports that reduce the time it takes to detect and respond to a broad range of cyberthreats. With this module, your network and security engineers will have the necessary information to prioritize threats and operate more efficiently from machine analytics.

How it Works

The Network Threat Detection Module consists of a collection of advanced analytics rules for LogRhythm AI Engine. AI Engine performs different analytic techniques, such as behavioral analysis, machine learning and analytics, and correlation across data sources, to provide unrivaled intelligence and insights. Your security team will benefit from alerting on compromised devices, propagating malware, breach attempts, data loss, and more. Your team can also customize the module's rules to detect specific threats on your network, while preconfigured reports and dashboards provide a high-level overview of current threats and anomalies.

This module calls on SmartFlow™ data from LogRhythm NetMon, which delivers deep packet inspection with automatic identification and metadata extraction for over 3,200 applications. This module also analyzes data from other sources such as routers and switches, remote access gateways, firewalls, next-generation firewalls and VPN concentrators, as well as third-party network sensors.

Benefits of the Network Threat Detection Module

- ✓ Expose advanced malware
- ✓ Detect denial of service attacks
- ✓ Surface zero-day attacks
- ✓ See internal port probes
- ✓ Expose covert network channels and data exfiltration

Stay a step ahead of attackers by detecting:

Malicious network activity

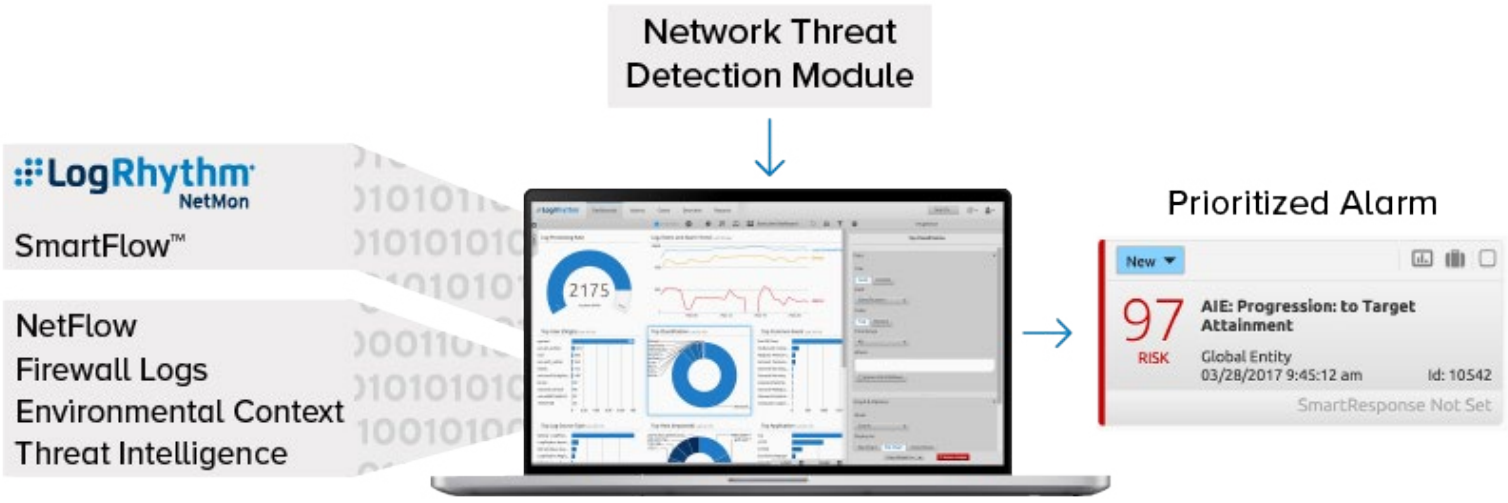
- Port scans and sweeps
- Internal reconnaissance
- Denial of service
- Botnet activity

Web application attacks

- SQL injection
- Cross-site scripting
- Excessive HTTP errors
- Internal URL directory traversal

Data breach attempts

- Suspicious data transfers
- Malicious payload drops
- Abnormal traffic patterns
- Blacklisted communication



Detecting Attacks Across the Cyber Attack Lifecycle

Pre-Attack Reconnaissance

To execute a successful intrusion or data breach, attackers start by researching and identifying target assets in their victim's organization. Activities like ping sweeps, port scans, and sweeps typically create a noisy footprint, so attackers will take steps such as conducting "slow and low" reconnaissance to evade detection.

The LogRhythm Network Threat Detection Module's rules detect reconnaissance activities and alert when those activities are followed by additional suspicious activity corroborating a true positive. Users can quickly take preventative measures, such as adding the IP address to a blacklist or firewall access control list (ACL) or initiating a vulnerability scan to determine if targeted assets are vulnerable to the specific attack.

Web Application Attacks

Internet facing servers and web applications provide a vulnerable, publicly available entry point that can be quickly exploited by attackers.

LogRhythm's Network Threat Detection Module can immediately alert when a web-based threat is detected, including attempts to manipulate URL parameters and attempts to inject JavaScript into the application's pages. SmartResponse™, LogRhythm's integrated automation tool, can then automatically neutralize the threat by initiating automated actions, including quarantining targeted servers and adding the attacking IP address to a firewall ACL.

Botnet, Command and Control Traffic

Immediate detection of botnets and other malware is a crucial component of network security, yet many organizations lack the tools necessary to identify malicious traffic associated with an outbreak. Infected bots will frequently use standard traffic ports normally used for HTTP/HTTPs, Telnet, FTP, SSH, and other legitimate traffic to bypass firewall ACLs and hide their activity when communicating with command and control (C2) servers, evading legacy security systems.

LogRhythm's Network Threat Detection Module delivers out-of-the-box rules to detect many forms of malicious network activity tied to botnets, such as abnormal outbound traffic on IRC ports or to suspicious top-level domains (TLDs). For additional context, LogRhythm's NetMon performs deep packet inspection to quickly detect suspicious traffic tied to botnet activity.

Disguised Data Transfers and Exfiltration

When an attacker has gained a foothold in the IT environment and is attempting to extract sensitive information such as PII, credit/debit card data, or health records, rapidly detecting any breach activity is crucial to minimizing its impact.

The Network Threat Detection Module's rules can zero in on exfiltration activities, such as data transfers of unusual size or to suspicious IP addresses. The module can also detect unusually long-running sessions that may be hiding data exfiltration attempts by sending out data in small chunks. LogRhythm's NetMon can deliver additional forensic evidence to immediately identify which assets are being targeted through automated full packet capture in response to any detected exfiltration attempts.

LogRhythm Labs

The LogRhythm Labs team delivers unparalleled security research, analytics, incident response and threat intelligence services to protect organizations from damaging cyberthreats. The team created and maintains LogRhythm's Holistic Threat Detection Suite, including the Network Threat Detection Module, User Threat Detection Module, and the Core Threat Detection Module, as well as a range of industry-specific and compliance mandate-specific module offerings. These offerings are updated regularly and are offered for free to LogRhythm customers.

Additional Reading

- Network Threat Detection Deployment and User Guides
- LogRhythm NetMon data sheet
- Also see the LogRhythm blog for further reading on addressing network-borne threats