PRODUCT OVERVIEW

Network Threat Analytics Suite

LogRhythm
The Security Intelligence Company

Organisations in every industry are facing a growing number of increasingly sophisticated threats to their networks. Yet a chronic shortage of trained security professionals and a lack of true visibility into network activity has left organisations struggling to combat advanced cyber threats and breaches before they cause major damage. A holistic approach to security intelligence is an integral component of arming the next generation security operations centre, and a capable network analytics solution is a necessary component of a larger strategy to arm organisations with the contextual visibility to detect, prioritise and neutralise cyber threats.

Network Analytics

- ✓ Automated behavioral and statistical analytics
- ✓ Network forensics & deep packet inspection
- ✓ Data breach detection and prevention
- ✓ Security best practice enablement

LogRhythm's Network Threat Analytics Suite helps organisations understand the network activity occurring in their environment by delivering automated, out-of-the-box capabilities that reduce the time it takes to detect and respond to a broad range of cyber-threats. The Suite was developed by LogRhythm Labs to deliver deep analytics to network activity beyond what legacy NBAD and flow analysis tools can provide by leveraging machine data analytics to give network and security engineers the necessary context to prioritise threats and operate more efficiently. Network Threat Analytics leverages SmartFlow data from LogRhythm's Network Monitor, which delivers deep packet inspection with automated identification and meta-data extraction for over 2,500 applications. The Suite also analyses data from existing sources such as routers and switches, remote access gateways, firewalls, next-generation firewalls and VPN concentrators, as well as data from 3rd party network sensors.

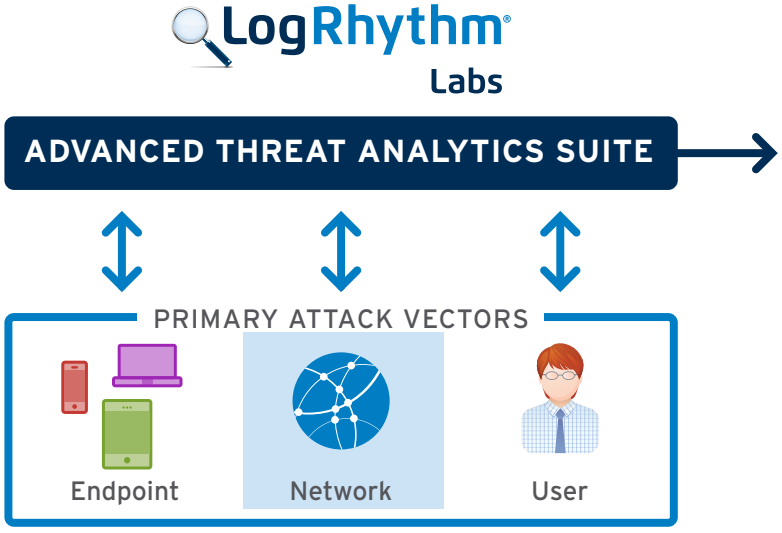
How it works

The Network Threat Analytics Suite is powered by a broad collection of advanced behavioural analytics rules for LogRhythm's AI Engine. AI Engine performs different analytics techniques, such as behavioural analysis, machine learning and analytics, and correlation across data sources, to provide unrivalled intelligence and key insights to security administrators, alerting them to compromised devices, propagating malware, attacker and hostile nation state breach attempts, data loss and more. Customers can deploy and configure the Network Threat Analytics module to detect a variety of anomalies related to the network activity and indicators of compromise. The Suite comes with a deployment guide containing recommended tuning and setup instructions for simple adherence to best practices and rapid ROI.

Malicious network activity
- Port scans and sweeps
- Internal reconnaissance
- Denial of service
- Botnet activity
- And more...

Web application attacks
- Sql injection attacks
- Cross-site scripting
- Excessive http errors
- Internal url directory traversal
- And more...

Data breach attempts
- Suspicious data transfers
- Malicious payload drops
- Abnormal traffic patterns
- Blacklisted communication
- And more...



With the amount of traffic moving in and out of today's networks, and the increasing sophistication of targeted attacks and zero-day threats, traditional signature-based tools and preventative network defence measures are no longer adequate. LogRhythm's Network Threat Analytics Suite takes a comprehensive approach to real-time monitoring and analysis of network behaviour using a variety of techniques. It empowers customers by detecting the initial security event, prioritising which activities pose the greatest threat, and initiating automated actions to neutralise attacks before they cause significant damage.

Pre-attack reconnaissance: In order to execute a successful intrusion or data breach attackers start by researching and identifying target assets in their victim's organisation. 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. LogRhythm's Network Threat Analytics rules are able to detect attacker reconnaissance activities and alert security administrators when that activity is followed by additional suspicious activity corroborating a true positive, such as increased network traffic or more complex attack behaviour. Customers can quickly take preventative measures by adding the IP addresses to a blacklist or firewall 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. The 2014 Verizon DBIR found that 60% of successful compromises involving web application exploits occur within minutes of the initial attack, with XSS and SQL injection being the most common methods employed. LogRhythm Network Threat Analytics can immediately alert security teams when a web-based threat is detected, including attempts to manipulate URL parameters and attempts to inject JavaScript into the applications pages. SmartResponse can then automatically neutralise the threat by initiating actions, including quarantining targeted servers and adding the attacking IP address to a firewall ACL.

Communication with suspicious IP addresses: Network communication to suspicious IP addresses and IP ranges is an excellent indicator of a malware outbreak or successful breach, yet many organisations have no way of automatically detecting when suspicious traffic is associated with known bad actors. LogRhythm's Network Threat Analytics Suite delivers several out-of-the-box rules that detect suspicious network activity and can automatically match that data against up-to-date threat intelligence data delivered by the LogRhythm Threat Intelligence Ecosystem. These rules automatically surface by prioritising which activity is the most threatening, including network communications to/from blacklisted or non-whitelisted geographic.

Botnet, command and control traffic: Immediate detection of botnets and other malware is a crucial component of network security, yet many organisations 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 servers, evading legacy security systems. LogRhythm's Network Threat Analytics Suite 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 Network Monitor 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, quickly detecting any breach activity is crucial to minimising its impact. LogRhythm's Network Threat Analytics Suite rules are able to zero in on exfiltration activities, such as data transfers of unusual size or to suspicious IP addresses. LogRhythm can also detect unusually long running sessions that may be hiding data exfiltration attempts by sending out data in small chunks. LogRhythm's Network Monitor can deliver additional forensic evidence to immediately identify which assets are being targeted through automated full packet capture in response to any detected exfiltration attempt.