PRODUCT OVERVIEW

Core Threat Analytics Suite

LogRhythm
The Security Intelligence Company

Today's cyber threats are rapidly growing in both complexity and sophistication, exposing organizations to an increasing level of risk to damaging attacks and data breaches. And while most are aware of the increased exposure to attacks, organizations are consistently hampered by a lack of personnel, limited security expertise, and an incomplete set of tools to effectively combat cyber-threats. Implementing an effective, next-generation security operation requires a holistic approach to security intelligence to expedite the detection, prioritization and neutralization of cyber-threats originating from inside and outside the network. This demands real-time visibility and understanding of threats targeting the complete attack surface that includes endpoints, network resources and user accounts.

Core Threat Analytics

☑ Rapid Deployment/Minimal Configuration

☑ Endpoint, Network, and User Visibility

☑ Automated Risk Assessment

☑ Security Best Practice Enablement

LogRhythm's Core Threat Analytics Suite helps organizations overcome operational and technical obstacles 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. It was developed by LogRhythm Labs to rapidly deliver critical behavioral analytics tied to user, endpoint, and network activity for immediate protection from common attack vectors. It is specifically designed to work with the most common types of log data readily available in most customer environments, such as Active Directory/LDAP, Anti-virus/Anti-malware, firewall, Host, IDS/IPS, and VPN, as well as network flow data.

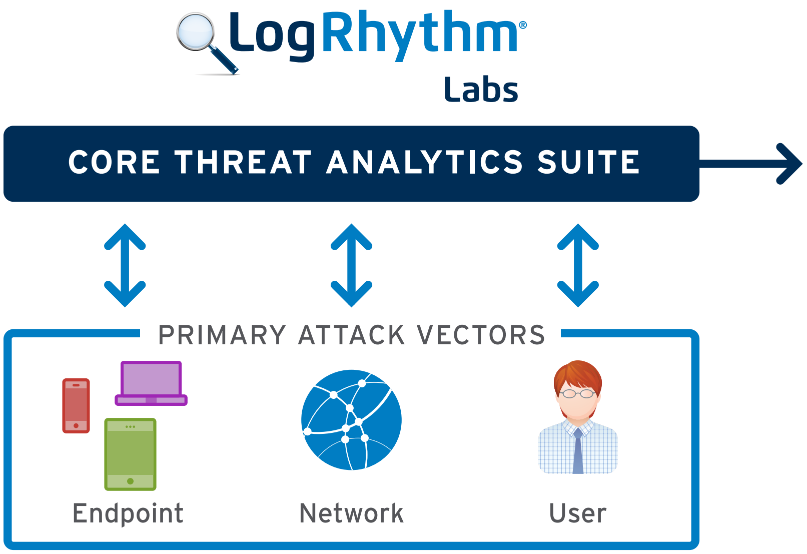
How It Works

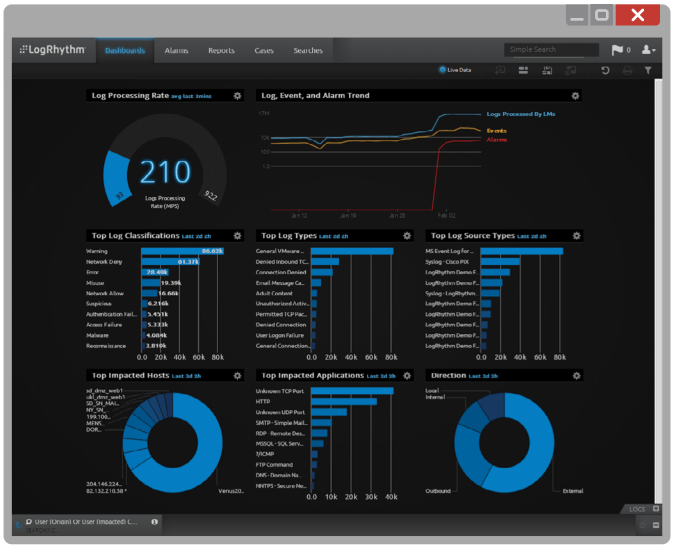
The Core Threat Analytics Suite is powered by LogRhythm's AI Engine and leverages a broad collection of automated machine analytics rules designed to operate with minimal configuration or tuning. They employ a variety of threat detection techniques including advanced correlation, pattern recognition, blacklisting and whitelisting, and statistical analysis. Customers can rapidly deploy and configure the module to look for a variety of anomalies tied to endpoint, network and user activity. The Suite comes with a straightforward deployment guide that includes recommended setup and tuning instructions for simple adherence to best practices and rapid ROI.

Endpoint
Suspicious Configuration Changes
Failed Malware Cleaning
Audit Log Tampering
Attack Related Damage
And more...

Network
Brute Force Attacks
Malware Outbreaks
Suspicious Network Activity
Early Attack Behavior
And more...

User
Account Compromise
Suspicious Account Activity
Lateral Movement
Privilege Abuse
And more...





The majority of successful attacks and data breaches involve the use of compromised or stolen user accounts, endpoints that have been exploited by means such as custom malware, and/or by penetrating network perimeter defenses through the use of zero day or targeted attacks. Core Threat Analytics takes a holistic approach to network defense, monitoring all three primary attack vectors in real-time using a variety of techniques. It empowers customers by detecting the initial security event, prioritizing which activities pose the greatest threat, and initiating automated actions to neutralize attacks before they cause significant damage.

Malware Outbreak: Host-based antivirus solutions are good at picking up individual instances of malware but may not surface a higher priority outbreaks that are affecting multiple endpoints or provide access to the origination point for remediation. Core Analytics rules will automatically detect an outbreak by correlating log data from existing antivirus solutions common in most customer environments. Customers can then immediately drill down on the event details to see all infected systems and identify the original point of entry. SmartResponse plug-ins can be enabled to immediately neutralize the threat by quarantining infected machines.

Data Exfiltration: Because they are disguised as legitimate activity, insider threats are frequently detected late in the attack cycle by traditional security solutions. This makes it imperative to immediately halt the attack and focus efforts on minimizing any damage that might be occurring when the attack is discovered. Using readily available log data from host systems as well as network monitoring and security devices, out-of-the-box Core Threat Analytics rules will correlate attack behavior with specific actions. This identifies when more damaging activity such as data exfiltration is taking place. Customers can intelligently prioritize their incident response to investigate the highest risk activities first, while SmartResponse can automatically neutralize the threat by disabling the user account or blocking the destination IP.

Compromised User Account: Compromised credentials remain the most common method by which attackers are successfully breaching networks. Detecting when credentials have been stolen and are being used in an attack, however, is difficult without the proper tools and expertise. Core Threat Analytics delivers preconfigured rules that correlate authentication activity collected from existing Active Directory/LDAP logs with attack data from IDS/IPS devices to identify when compromised credentials may be involved in an attack. SmartResponse can either disable a suspiciously behaving account immediately or add it to a watchlist to trigger higher priority alarms tied to any future suspicious activity.

Privilege Abuse: Whether being used by malicious insiders or external attackers, privileged accounts have the potential to cause extensive damage to an organization. An Admin account, for example, can be used for a broad range of malicious activities, from deleting or stealing critical data to reconfiguring security settings that leave the network open to additional attacks. Core Threat enforces security best practices by monitoring active directory or LDAP logs to alert when any account is added to an Admin group, and can automatically validate that activity against an authorized whitelist of authorized privileged users to detect potential abuse. SmartResponse can automatically disable any account that has been granted unauthorized privileges until it has been verified.

Compromised Server: IDS/IPS devices typically generate such a large volume of events that it's difficult to distinguish between false positives and attack activities requiring immediate attention. Core Threat Analytics analyzes IDS/IPS events, log data from firewalls, and flow data to correlate attack events with network activity to detect when a targeted host system may have received a malicious payload. Organizations with additional network sensors, such as next generation firewalls or LogRhythm's Network Monitor, can correlate against deeper, packet-level detail for increased accuracy and greater event detail. SmartResponse can automatically neutralize the threat by initiating a quarantine of the compromised server.