LOGRHYTHM LABS EMBEDDED EXPERTISE

Data Sheet

LogRhythm Labs is an organization within LogRhythm that performs dedicated research to continually enhance the Security Intelligence Platform with embedded machine data intelligence, real-time threat detection, and automated compliance assurance. Recognizing that attackers are deeply vested in finding new and inventive ways to evade traditional security defenses and penetrate corporate networks, LogRhythm recruits security experts with hands-on field experience to vigorously investigate and understand how malicious behavior patterns are exposed.

LogRhythm Labs is comprised of three teams: the Machine Data Intelligence team, the Threat Intelligence team, and the Compliance Intelligence team. Members of these teams have extensive experience as network architects, security analysts and compliance officers at multinational corporations and federal entities. For continued development and exposure to unique use cases, Labs analysts work closely with customers, field teams and technology partners to form a community of dedicated security experts.

Machine Data Intelligence

Labs' Machine Data Intelligence team ensures that LogRhythm can interpret data from virtually any data source across the enterprise. The team regularly builds and updates processing rules for hundreds of operating systems, applications, and network devices. These processing rules translate disparate and often incomprehensible messages into a uniform language by enriching all captured data with common classifications and event names, a Risk-Based Priority (RBP), geolocation tagging and additional contextual details such as directional information. For example, different systems may describe a seemingly common activity such as an authentication success in many alternative ways, including login successful, logon successful, authentication successful, etc. LogRhythm Labs' Machine Data Intelligence team recognizes the true activity described in the log message and accurately assigns a common classification and event name, in this case "authentication success". This extensive data preparation strengthens the accuracy of real-time machine analytics and improves search results.

Data Preparation Process

Data Classification	Every message is automatically categorized within three levels of event classification for better understanding of the data.
Common Event Name	All data is assigned a specific Common Event in a natural language for quicker comprehension and greater accuracy in search results and analytical rules, such as correlation or behavioral baselining.
Risk Based-Priority (RBP)	Every message is assigned a dynamic RBP value from 0 to 100 to calculate the level of severity of the event. Understanding the relative risk enables analysts to focus on the most critical events within their organization.
Geolocation	Automated geographic context around any event helps identify the country, region, and city of all activity. Geolocation data is updated as IP addresses change.
Context Infusion	Data is infused with relevant contextual information including target risk rating, vulnerability status and directionality.
User Context	Separates origin users from impacted users to determine if users are performing the action or being affected by the action.
Host Context	Separates origin hosts from impacted hosts to determine if hosts are the source of an attack or the target of an attack.

Another function of Labs' Machine Data Intelligence team is contextual data integration. Contextual data integration allows the Security Intelligence Platform to enrich data leveraging various external sources including open source threat feeds, custom subscription services, GeoIP location, and rules that update predefined lists, such as a list of known administrative accounts or suspicious users. This additional data increases visibility into security risks, exposes behavioral abnormalities, and automates manual processes. For example, LogRhythm Labs maintains and regularly updates a list with over 2100 applications categorized by type, making it easy for admins to search for specific types of applications running on the corporate network such as peer-to-peer apps. Leveraging this application list, admins can be automatically alerted to the use of unauthorized internet file sharing services.

Threat Intelligence

LogRhythm Labs examines live attacks and malware within an advanced threat research lab and continually researches the latest trends in security threats by studying industry reports and blogs. Understanding the blueprint of evolving attack vectors and vulnerabilities allows LogRhythm Labs' Threat Intelligence team to decipher commonalities in data movement and behavior that are indicative of nefarious activity. This insight is used to create an arsenal of advanced correlation rules within LogRhythm's AI Engine. AI Engine rules perform patented machine analytical techniques that continuously monitor the customer environment for malicious behavioral patterns and abnormal activity.

The Threat Intelligence team combines a subset of AI Engine rules, lists, reports, investigations, dashboard layouts, and Smart**Response**™ plugins into purpose-built Security Analytics Suites. Each Security Analytics Suite is designed to address a specific security need and customers can select the individual suites that align to their objectives to quickly take advantage and find value from LogRhythm Labs' research. For example, the Advanced Persistent Threats Security Analytics Suite uses a collection of AI Engine rules designed to detect behaviors representative of advanced attacks. Rules include behavioral modelling of activities on the endpoint (e.g. log types, authentication activity, process activity) as well as network activity (e.g. traffic rates, traffic destinations, application types) and others. The APT Security Analytics Suite not only recognizes when an individual behavioral anomaly occurs, but includes rules that recognize when multiple activities or anomalies occur from a common host or user to corroborate the identification of an advanced attack. By analyzing behaviors across multiple stages of an advanced attack and linking multiple behavioral anomalies together, the APT Security Analytics Suite provides more accurate event recognition and prioritization of complex attacks.

Security Analytics Suites

Privileged User Monitoring	Recognizes behavioral patterns indicative of privileged user account misuse or compromise
Web Application Defense	Analyzes web server logs and other related data sources to expose behavioral attack patterns targeting applications
Advanced Persistent Threats	Exposes key indicators of APT-like behavior including custom malware and botnet communication through advanced security analytics and continuous monitoring
Retail Cyber Crime	Monitors the entire payment card infrastructure including POS system and back-office servers for signs of abnormal or malicious activity
Network Behavior Anomaly Detection	Detects deviations in network activity from a pre-established baseline of normal activity and performs advanced correlation on data collected from network devices
SANS Critical Security Capabilities	Provides a broad range of advanced capabilities that map directly to various components of the SANS Critical Security Controls to help organizations maintain a secure network
Honeypot	Collects and monitors feeds from multiple open-source honeypots to detect attackers and gather threat intelligence on emerging threat vectors and patterns

Compliance Intelligence

The LogRhythm Labs' Compliance Intelligence team is comprised of subject matter experts in various industry regulations and compliance standards. Compliance experts are responsible for understanding current compliance requirements and researching new regulations. They leverage that expertise to develop and maintain compliance-specific Compliance Automation Suites to provide enterprises with out-of-the-box report packages, investigations, alarms and automated Smart**Response**™ plugins that are specifically mapped to individual controls as specified by the regulation. Additionally, LogRhythm Labs develops AI Engine rules that monitor individual compliance controls. These rules not only perform ongoing monitoring, but can alert on specific compliance violations in real time. This awareness saves time and effort for customers maintaining their compliance state. Labs' commitment to strengthening and automating LogRhythm's regulatory capabilities provides customers with continuous compliance assurance.

Compliance Automaton Suites

PCI DSS	**HIPAA**	**FISMA**	**NIST 800-53**	**DoDI 8500.2**
SOX / GLBA	**ISO 27001**	**NERC CIP**	**GPG-13**	**NEI 10**

Embedded Expertise

Customers take advantage of Labs' research through frequent Knowledge Base updates, which automatically embed analytics-driven defense capabilities into LogRhythm's Security Intelligence Platform. This allows customers to take advantage of new and updated device support, geolocation data, AI Engine rules, lists, investigations, dashboards, and Smart**Response**™ plug-ins associated with new and existing Security Analytics and Compliance Automation suites.

Labs' research is also published in LogRhythm's blog and shared directly with customers in the Support Portal and Discussion Forum, monthly customer Tips and Tricks webinars, and the Labs-produced Threat Detection Cookbook. The Threat Detection Cookbook contains "recipes," including ingredient lists (aka data sources), for building and enabling AI Engine rule blocks that address a myriad of specific security concerns.

Through continuous innovation, customer partnerships, and unwavering dedication to cyber security, Labs' embedded expertise empowers customers around the globe to strengthen their network security, defend against targeted attacks, and achieve steady-state compliance.