PRODUCT OVERVIEW

LogRhythm and FireEye: Integrated Security Intelligence

LogRhythm
The Security Intelligence Company

LogRhythm and FireEye have developed an integrated solution for comprehensive enterprise intelligence and threat management. LogRhythm's advanced correlation and pattern recognition automatically incorporates threat intelligence from the FireEye Malware Protection System to deliver real-time threat protection based on up-to-date attack vectors and comprehensive security analytics.

LogRhythm for Integrated Security Intelligence

- ☑ Real-time event contextualization across multiple dimensions
- ☑ Improved risk-based prioritization
- ☑ Forensic visibility into malware attack vectors and patterns
- ☑ Tight integration for consolidated threat management

The integration allows organizations to:

- Model malware indicators from FireEye data using LogRhythm's behavioral analytics to extend the value of FireEye to other network segments
- Perform statistical analysis of FireEye and malware data and generate relevant reports
- Identify compromised users, hosts and devices using threat intelligence lists dynamically generated by correlating FireEye intelligence with machine data from across the IT environment
- Provide drill-down and deep forensic visibility into malware attack vectors and patterns
- Automate the remediation of zero-day malware attacks by quarantining infected applications, hosts, and users, and blocking malicious IP addresses from the network

By leveraging the FireEye platform with LogRhythm's Security Intelligence Platform customers benefit from increased network-to-endpoint visibility. The combined solution delivers the ability to rapidly detect and validate cyber threats and reduce incident response times.

LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's award-winning Security Intelligence Platform unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence. LogRhythm delivers:

- Next Generation SIEM and Log Management
- Independent Host Forensics and File Integrity Monitoring
- Network Forensics with Application ID and Full Packet Capture
- State-of-the art Machine Analytics
  - Advanced Correlation and Pattern Recognition
  - Multi-dimensional User / Host / Network Behavior Anomaly Detection
- Rapid, Intelligent Search
- Large data set analysis via visual analytics, pivot, and drill down
- Workflow enabled automatic response via LogRhythm's Smart**Response**™
- Integrated Case Management

FireEye

FireEye® has pioneered the next generation of threat protection to help organizations protect themselves from being compromised. Cyber attacks have become much more sophisticated and are now easily bypassing traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways, compromising the majority of enterprise networks. The FireEye platform supplements these traditional defenses with a new model of security to protect against today's new breed of cyber attacks. The unique FireEye platform provides the only next-generation threat protection fabric to dynamically identify and block cyber attacks in real time. The core of the FireEye platform is a signature-less, virtualized detection engine and a cloud-based threat intelligence network, which help organizations protect their assets across all major threat vectors, including Web, email, file, and mobile-based cyber attacks. The FireEye platform is deployed in over 40

LogRhythm and FireEye are tightly integrated, combining the value of next-generation threat protection with the threat management capabilities of LogRhythm. The combined offering empowers customers to identify behavioral anomalies, detect advanced threats, and prioritize responses based on accurate enterprise security intelligence.

Preventing Spear Phishing Attacks

Challenge Increasingly sophisticated malware combined with social engineering tactics are making it easier for spear phishing attacks to bypass anti-spam and reputation-based technologies, tricking end-users into executing zero-day exploits. This gives criminals quick control of a privileged system and user accounts which they can then leverage to infiltrate the rest of the IT environment.

Solution The FireEye Email MPS analyzes every attachment using a signature-less, Multi-Vector Virtual Execution (MVX) engine to detect zero-day attacks. LogRhythm then combines this data with advanced correlation and pattern recognition across all machine data to alert users to potential zero-day attacks targeting high-priority and/or vulnerable assets.

Additional Benefit Smart**Response**™ Plug-ins are designed to actively defend against attacks by initiating actions that offset the threat, such as automatically adding malicious IP addresses to a firewall ACL to prevent end-users from unknowingly downloading malware, or disabling compromised accounts to prevent malware from propagating.

Detecting Suspicious Network Traffic

Challenge Traditional security tools are designed to defend against known threats and vulnerabilities but provide little insight into what is actively happening within an organization's network. This results in many zero-day attacks going undetected by the organization.

Solution LogRhythm can automatically incorporate data from the FireEye platform into internal lists that can be leveraged by alarms, investigations and reports to identify higher priority events based on up-to-date zero-day threat analysis data. LogRhythm's AI Engine can also correlate zero-day threat data against suspicious behavior patterns for greater accuracy and quicker response times.

Additional Benefit LogRhythm's Smart**Response**™ can automatically shut down any non-whitelisted process that is started on a host. Additional visualization tools can be used to map all locations within the environment where the same process is running for rapid forensic and root cause analysis.