PRODUCT OVERVIEW

LogRhythm and Sourcefire: Enterprise Security Intelligence

LogRhythm

Sourcefire and LogRhythm have developed an integrated offering for comprehensive enterprise security intelligence and incident response management. LogRhythm incorporates Sourcefire's network security and advanced malware protection via the secure eStreamer API and correlates it against other security device and machine data throughout the IT environment. This delivers multi-dimensional behavioral analytics, extended visibility and continuous monitoring for real-time threat detection & response.

LogRhythm for Enterprise Security Intelligence

- ☑ Multi-Dimensional Behavioral Analytics
- ☑ Real-time event contextualization
- ☑ Adaptive defense for protecting vulnerable assets
- ☑ Tight integration for consolidated threat management

The integration provides:

- Deeper visibility and contextual awareness into network events with advanced correlation across the entire IT environment to deliver enterprise-wide threat detection
- Access to the most up-to-date threat intelligence to help organizations detect advanced malware attacks and realize the extent of the outbreak for fast remediation
- Automated and immediate action against threats such as advanced persistent threats (APT) and zero-day attacks
- Unparalleled, embedded security expertise through the collective experience of LogRhythm LabsTM and Sourcefire's Vulnerability Research Team (VRT)
- Continuous compliance assurance to ensure that appropriate personnel are alerted when a network event occurs that maps to a specific compliance requirement that mandates alerting

LogRhythm leverages Sourcefire's eStreamer API for secure and complete access to all types of structured Sourcefire event data, including flow data and impact flags. Sourcefire's impact flags score the relevance of an attack based on the vulnerability of the device. LogRhythm incorporates this information into an automated Risk Based Prioritization (RBP) rating to ensure that the most important events are identified and acted upon.

LogRhythm

LogRhythm uniquely combines enterprise-class SIEM, Log Management, File Integrity Monitoring and Machine Analytics, with Host and Network Forensics, in a fully integrated Security Analytics platform. The LogRhythm solution gives customers profound visibility into threats and risks in areas that were previously exposed. Designed to help prevent breaches before they happen, LogRhythm Security Analytics accurately detects an extensive range of early indicators of compromise, enabling rapid response and mitigation. The deep visibility and understanding delivered by LogRhythm Security Analytics empowers enterprises to secure their networks and comply with regulatory requirements. 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

Sourcefire

Sourcefire, Inc. (Nasdaq:FIRE), a world leader in intelligent cybersecurity solutions, is transforming the way global mid- to large-size organizations and government agencies manage and minimize network security risks. With solutions from the network to the endpoint, Sourcefire provides customers with Agile SecurityTM that is as dynamic as the real world it protects and the attackers against which it defends. Trusted for more than 10 years, Sourcefire has been consistently recognized for its innovation and industry leadership with dozens of patents, world-class research, and award-winning technology. Today, the name Sourcefire has grown synonymous with innovation, security intelligence and agile end-to-end security infrastructure.

Sourcefire and LogRhythm have developed an integrated offering for comprehensive enterprise security intelligence and incident response management. LogRhythm incorporates Sourcefire's network security and advanced malware protection via the secure eStreamer API and correlates it against other security device and machine data throughout the IT environment. This delivers multi-dimensional behavioral analytics, extended visibility and continuous monitoring for real-time threat detection & response.

Challenge With new, increasingly sophisticated viruses being created daily, it is difficult for organizations to detect zero day exploits using traditional security tools because they lack the signature needed spot the malware. And once an organization does become aware of an advanced malware problem, it is almost impossible to pinpoint the source and contain the infection.

Solution Sourcefire's FireAMP leverages a cloud-based antimalware model which pushes real-time security updates to identify malicious files on the wire. LogRhythm performs advanced correlation and behavioral analytics on FireAMP events to help identify which devices, hosts, applications and users have been targeted and/or successfully impacted and sends all relevant context in a high-priority alarm for immediate action.

Additional Benefit Smart**Response**™ Plug-in can initiate immediate protective action by isolating the source of malicious files, such as by adding the source IP to a firewall ACL to prevent critical applications and servers from exposure. This process can be completely automated or it require as many as three levels of authorization.

Challenge In large organizations, high-volume, global communication is common but makes it difficult for IT administrators to identify and prevent unauthorized or suspicious data transfers to or from rogue IP addresses. Manually monitoring network traffic and updating blacklists to prevent the infiltration of bad code is inefficient and time consuming.

Solution Sourcefire's Next-Generation IPS solution can identify malicious activity coming from a foreign IP address and securely send the log data and associated flow data to LogRhythm via eStreamer. LogRhythm can correlate this log and flow data against other security vectors such as hosts and application to provide complete visibility into the scope of an attack. High-priority alerts are then sent to administrators, ensuring continuous compliance.

Additional Benefit LogRhythm's Smart**Response**™ can automatically add Destination IPs to lists of targeted devices, which can then be leveraged by alarms, investigations and reports to identify the most likely targets for attack and allow organizations to respond more quickly to higher priority events.