Solution Brief

Leading SIEM 2.0 Solution and Network Security Intelligence & Analytics

Summary:

Solera DeepSee™ delivers comprehensive Security Intelligence & Analytics and provides full context to any security event identified by LogRhythm's SIEM 2.0 platform.

For: Detection, replay and reconstruction of any network event to support:

- Incident Response
- Situational Awareness
- Network Security Assurance

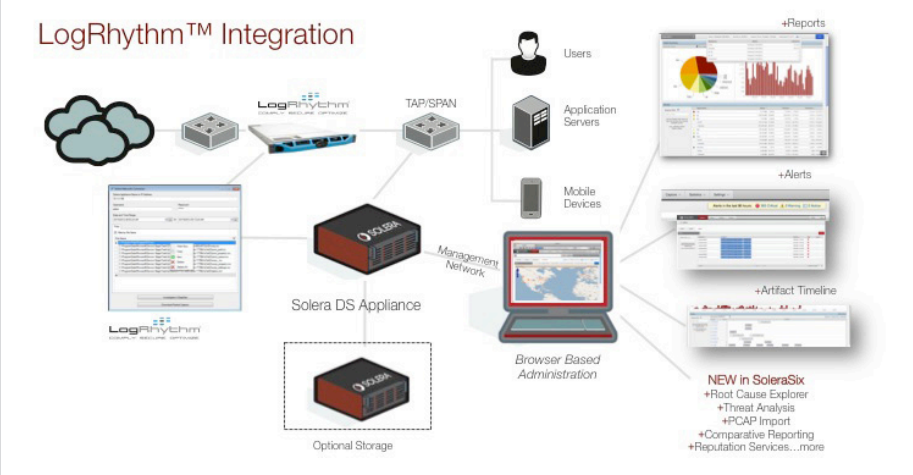
Today's IT infrastructures face persistent threats that are highly dynamic and constantly morphing. Traditional network security products cannot prevent every attack or security breach—there are simply too many vulnerabilities and clever perpetrators to expect that an organization can forever avoid a security breach. Astute organizations now understand the need to shift resources from a simple "prevention" mode to a complete detection, defense and response system for cyber-security. After all, the worst attacks are the ones you never know about. Now, the best-in-class security correlation and advanced pattern recognition of LogRhythm's next-generation SIEM 2.0 platform combines with Solera's Security Intelligence & Analytics solution to deliver advanced context-aware security. This provides network administrators and security professionals with deep visibility into IT security threats and advanced targeted attacks to answer the most difficult post-breach questions—enabling them to prevent their recurrence and mitigate further risk.

Unique LogRhythm Capabilities	Unique Solera Networks Capabilities
LogRhythm is an enterprise solution that is easy to install, manage and use. Flexible deployment options meet the implementation and scalability requirements of any organization.	Revolutionary new Solera DeepSee Software solution un-boxes the power of security intelligence and analytics. Deployed either on your hardware, as a Virtual Appliance, or on pre-configured appliances, DeepSee enables end-to-end visibility of any threat or advanced targeted attack.
LogRhythm's Advanced Intelligence (AI) Engine delivers next-generation advanced correlation and pattern recognition via an easy-to-use GUI. Extensive out-of-the-box rules can be quickly modified and custom rules can be easily created, arming customers with greater situational awareness to defend against rapidly evolving cyber-threats.	DeepSee reconstructs recorded network traffic into the original documents, images, messages, and files that traversed the network, making full event reconstruction possible with impressive speed. Reconstruct email attachments, windows file transfers, PDF, Word, PowerPoint, Excel, and more, for complete evidence of any network event.
LogRhythm delivers comprehensive visibility and situational awareness into network attacks, breaches, and insider threats. A powerful, fully interactive and intuitive console provides critical information in real-time.	Root Cause Explorer is the incident responder "Easy Button." Using extracted network objects, the tool reconstructs a timeline of suspect web sessions, emails, and chat conversation to help the analyst quickly identify the source of an infection or compromise and reduce time-to-resolution.
LogRhythm's SmartResponse™ delivers automated protection to defend against a broad range of cyber-threats and enforce compliance policies. Up to three levels of user authorization can be instituted to meet internal response policies and eliminate the fear of false positives.	Solera DB indexes every packet in a high-performance database to allow quick retrieval, while the efficient deep packet inspection engine classifies over 850 applications and thousands of points of application meta data.

LogRhythm/Solera Networks Solution Components

LogRhythm is an enterprise-class security platform that seamlessly combines log and event management, file integrity monitoring and host activity monitoring—delivering advanced cyber threat defense, detection and response within a fully integrated SIEM 2.0 solution. For full context and artifact reconstruction to any data that LogRhythm has collected and correlated, direct integration into Solera Networks allows customers to know—at the packet level—exactly what happened before, during and after an event to mitigate further risk.

Sample Implementation



Solera DeepSee Security Intelligence and Analytics solutions make all network traffic and data flows instantly visible and replayable, enabling administrators and security professionals to detect the full source and scope of any network security event, while protecting the network against further attack.

Solera Networks seamlessly integrates with LogRhythm, instantly providing full packet-level detail to any LogRhythm-generated alert and specific details of what happened before, during and after an alert was triggered, including actual artifacts (documents, files, executables, etc.) recreated from raw network packets.

Solera DeepSee Software and Appliances include the powerful suite of DeepSee applications to deliver unmatched visibility into your network:

- Ultra-fast full packet-capture, classification and replay of all network traffic (layer 2-7)
- Geolocation to see the exact origin of traffic and identify hot spots
- Root Cause Explorer™ to chain events together and paint a clear path to the source of a breach or attack

Applying Security Intelligence and Analytics

Incident Response — Effective incident response starts with solid integration with the most popular security tools on the market, such as LogRhythm's award-winning SIEM 2.0 solutions. With the correct data, responding to an incident is instant, active and efficient. Through the REST-based Web services API, Solera Networks integrates with LogRhythm to make all collected data available through standard PCAP format for sharing or analysis on a packet level.

Situational Awareness — Today sophisticated, persistent and targeted attacks are specifically designed to circumvent traditional defenses that organizations have implemented. While LogRhythm's SIEM 2.0 solution provides early detection and alerting of security events in even the most complex enterprise IT environments, Solera DeepSee Software acts like a security camera that can recreate and replay network traffic surrounding any event reported by the LogRhythm platform, jointly providing complete situational awareness to defend networks against past, present and future threats.

Network Security Assurance — Network security assurance verifies today that your network was not impacted by threats that were unknown yesterday. Because breaches can be transient and/or persistent – and signatures are typically written for initial exploits – until now there has been no way for historical incidents to be detected. With LogRhythm and Solera Networks, organizations can replay traffic to their LogRhythm platform after any tools in their sensor fabric have been updated with the latest definitions. When a major new exploit is discovered, the network security assurance offered by LogRhythm and Solera Networks can provide the peace of mind that the organization is secure.

Learn More

For more information on the LogRhythm/Solera Networks solution, contact:

Solera Networks
10713 South Jordan Gateway, Suite 100
South Jordan, UT 84095
877-5SOLERA (877-576-5372)
www.soleranetworks.com
Email: info@soleranetworks.com

LogRhythm, Inc.
4780 Pearl East Circle
Boulder, CO 80301
(303) 413-8745
www.logrhythm.com
Email: info@logrhythm.com

LogRhythm™

SOLERA NETWORKS™