IXIA AND LOGRHYTHM NETWORK MONITOR COMBAT ADVANCED SECURITY THREATS

HIGHLIGHTS

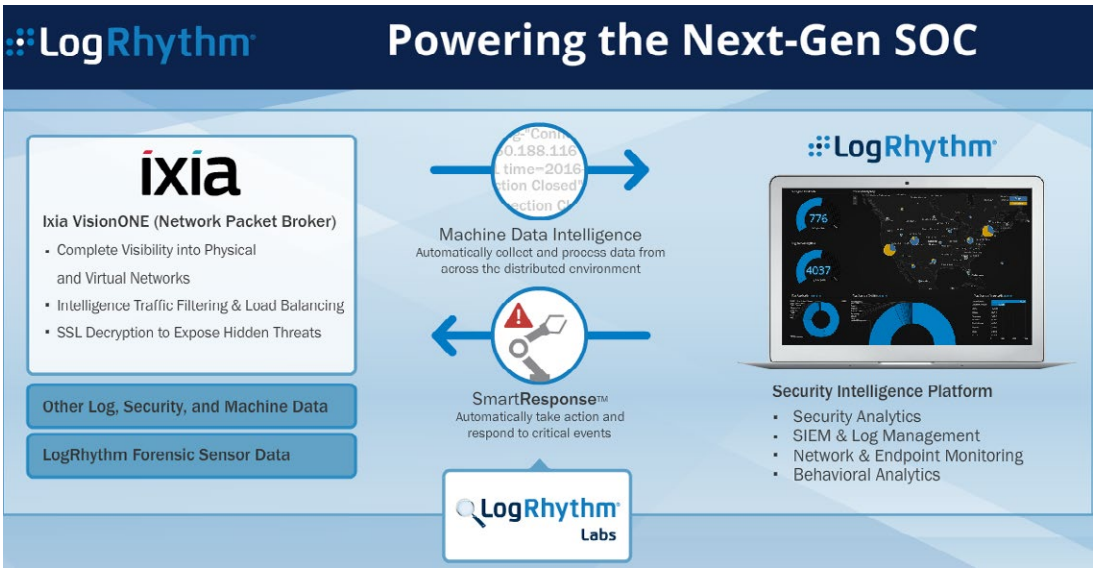
Ixia's Vision ONE provides complete access to network data feeds that LogRhythm Network Monitor then identifies, captures, and analyzes for real-time security threats. Leveraging Network Monitor's Deep Packet Analytics capability, the solution automates threat detection through continuous correlation of network data. Additionally, Vision ONE can provide a decrypted copy of SSL traffic to Network Monitor where advanced analytics expose threats hidden in network traffic such as advanced attacks, data exfiltration and network usage policy violations. The Vision ONE from Ixia complements Network Monitor by extending access to every network feed needed for analysis. The joint solution provides complete visibility into network traffic in a highly scalable system that is easy to deploy.

THE JOINT SOLUTION

- Full network visibility – Vision ONE extends access to data feeds from anywhere in the network for analysis by Network Monitor, including automatic identification of over 2,700 application and SmartFlow™, an extensive collection of Layer 7 metadata attributes of each network session.
- Automated threat detection – Network Monitor's Deep Packet Analytics continuously correlate against full packet payload and SmartFlow™ metadata using out-of-the-box rules and customizable scripts to detect threats previously only possible via manual packet analysis.
- Intelligent capture – Integrating Vision ONE with the SmartCapture™ capability of the LogRhythm Network Monitor solution allows for a rules-based selective packet capture of

full network sessions for packet level analysis when necessary, without the extensive storage requirements of traditional packet recorder solutions.

- Simplified deployment – The solution is flexible enough to work in any network environment and can share access with monitoring and security tools that are already deployed.
- Easily scalable – Additional 1G, 10G, 40G, or 100G Vision ONE ports can be added to meet bandwidth requirements, and traffic can be load-balanced across multiple Network Monitors.
- Maximum efficiency – Vision ONE filters and removes unneeded duplicate traffic so that the LogRhythm solution can operate at full efficiency.
- Real-time threat detection - Stateful, bi-directional SSL Decryption from Vision ONE enables Network Monitor to detect threats hidden in encrypted network traffic.



SOLUTION

Ixia's Vision ONE works in concert with Network Monitor to ensure that the LogRhythm solution has access to the data it needs to provide application-level network session analysis with deep packet inspection and full packet capture. Vision ONE passively directs out-of-band network traffic from multiple network access points– SPAN ports or TAPs – to Network Monitor for analysis. Traffic is aggregated from all needed access points in the network to provide comprehensive visibility and to address shortages in monitoring access points. Network Monitor performs deep packet inspection to classify applications, generating rich, searchable metadata and Layer 7 SmartFlow™. SmartCapture™ is used to intelligently record full packet captures for sessions relevant to high priority security threats, and Deep Packet Analytics, an exclusive Network Monitor capability, is used to correlate against this data to automate threat detection. This integrated solution provides complete visibility into forensic security data, without the extensive storage requirements or reliance on packet-level analysis of traditional packet recording products.

LOGRHYTHM NETWORK MONITOR SOLUTION

True enterprise security intelligence requires real-time awareness and understanding of all data traversing your network. Network Monitor helps organizations detect advanced threats in real-time via market-leading application recognition, customizable Deep Packet Analytics across network and application level data, and multidimensional behavioral analytics. Store session-based packet captures (either selectively or in full) and analyze them using out-of-the-box application identification and application-specific metadata recognition. Incident response team are enabled to work effectively and efficiently with unstructured search, session playback, and file reconstruction.

LogRhythm Network Monitor provides critical visibility for detecting and responding to today's advanced threats, enabling organizations to:

- Understand their network with Layer 2-7 visibility
- Detect unauthorized and unwanted applications
- Immediately recognize suspicious network activity including lateral movement
- Identify and prevent sensitive data loss
- Expedite network layer forensic analysis
- Monitor application bandwidth consumption

IXIA'S VISION ONE EFFICIENTLY DIRECTS TRAFFIC TO SECURITY, NETWORK, AND APPLICATION MONITORING TOOLS

Vision ONE provides Network Monitor access to all necessary network feed data. The NTO sits between the access points in the network that require monitoring and Network Monitor. Vision ONE aggregates traffic from multiple SPANs/TAPs in the network and directs it to any security or monitoring appliance including Network Monitor. This approach provides efficient access to asymmetric traffic across large heterogeneous networks. Vision ONE filters out duplicate and other traffic that does not need analysis, prior to consuming resources on monitoring appliances.

Vision ONE can share traffic from a network access point with multiple monitoring tools. This capability eliminates the common SPAN/TAP shortages that occur when another tool is attached to a needed access point. Additionally, by removing duplicate packets, Vision ONE can enhance the throughput and storage capacity of the monitoring appliance.

Vision ONE's intuitive control panel makes the NTO easy to set up and use. Simply drag-and-drop a virtual connection between SPANs/TAPs and tools to make a live connection.

ABOUT IXIA'S NETWORK VISIBILITY SOLUTIONS

Ixia's Vision ONE provides complete network visibility into physical and virtual networks, improves network security and optimizes monitoring tool performance. Vision ONE ensures that each monitoring tool gets exactly the right data needed for analysis. This improves the way you manage your data center and maximizes return on investment. Our customers include large enterprises, service providers, educational institutions and government agencies.

ABOUT LOGRHYTHM

LogRhythm empowers organizations to detect, respond to and neutralize cyber threats early in the threat lifecycle to prevent damaging data breaches and cyber incidents. LogRhythm solutions also deliver rapid compliance automation and assurance, and enhanced IT intelligence.

LogRhythm's award-winning Security Intelligence Platform integrates next-gen SIEM and log management with network forensics, endpoint monitoring and multidimensional security analytics. Its collaborative incident response orchestration and patented SmartResponse™ automation framework help security teams perform end-to-end threat lifecycle management. LogRhythm's unified solution powers the next-gen SOC, accelerating the detection and response to emergent threats across the holistic attack surface. For additional information:

Phone: (866) 384-0713
Email: info@logrhythm.com

ABOUT IXIA

Ixia delivers a powerful combination of innovative solutions and trusted insight to support network and security infrastructures from concept to operation. Whether you are preparing a product for launch, deploying a service or application, or managing performance in operation, we offer an extensive array of solutions for testing, visibility, and security—all in one place.

Our solutions are used worldwide to validate network functions, test the integrity of security infrastructures, and deliver an end-to-end view of the network. The result: stronger applications, better performance, increased security resilience, happier customers, and maximum ROI.

IXIA WORLDWIDE HEADQUARTERS
26601 AGOURA RD.
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 1.818.871.1805
www.ixiacom.com

IXIA EUROPEAN HEADQUARTERS
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC HEADQUARTERS
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127