aria CYBERSECURITY SOLUTIONS

TECH BRIEF

ARIA SDS Packet Intelligence App for Sumo Logic

Detects and stops the most harmful network-borne attacks early in the kill chain

Benefits

Superior Threat Detection: Detect hidden cyber-attacks within minutes as they become active within your network.

Stop Threats Earlier in Kill Chain: Stop the attacks immediately once detected – before harm is done.

Surgical Threat Containment: Stop attacks precisely and without taking devices or applications offline.

Detailed Network Visibility: Gain insights into your internal network traffic to accelerate incident detection and response. Set, monitor, and enforce network communication policies, etc.

The integration between Sumo Logic's Continuous Intelligence platform and the ARIA SDS Packet Intelligence (PI) application finds and stops the types of cyber-attacks that do the most harm.

The ARIA PI application integration with Sumo Logic automatically detects internal network threats including ransomware, malware, and advanced threats (APTs), and intrusions including attacks involving IoT devices. It gives SOC teams the ability to stop the threats as detected to minimize harm. Further, the solution can be used to visualize all internal network traffic communications, and both set and enforce connectivity policies.

The ARIA PI application feeds NetFlow metadata from every network packet to Sumo Logic's Continuous Intelligence platform, including those east-west paths that are typically overlooked. Once this data is available in the Continuous Intelligence platform, security professionals can use the ARIA queries to find network-borne threats and quickly create new queries to generate additional findings. The ARIA PI application plug-in for Sumo Logic allows these queries to be visualized into comprehensive and actionable dashboards.

The ARIA PI application provides metrics-based information into Sumo Logic efficiently in real time. This enables attacks to be identified automatically when leveraging the continuously running ARIA PI queries – all within minutes as soon as they become active. This innovative approach allows SoC teams for the first

time to conduct quick and efficient incident investigations related to ransomware, malware, and other intrusions including APTs and data exfiltration attempts. What's even better, these teams can use ARIA PI to take action and stop these threats transparently from within the network – before significant harm is done. They can do so using the user interface or automated workflows, so these actions can be taken quickly, consistently, and effectively by any team member.

Using the ARIA SDS PI application within a Sumo Logic environment empowers SoC teams to:

- Identify hard-to-detect attacks in real time early in the kill chain.
- Allow security analysts to accelerate investigative response to verify threats using ARIA's automated workflows.
- Give security analysts the ability to stop the attacks at the threat-conversation level. These teams can leave critical production or IoT devices online by blocking the threat conversations until the issue can be resolved.
- Visualize all internal network traffic, including those between devices, virtual machines, containers, and IoT devices so proper connectivity policies can be developed, monitored, and enforced using ARIA PI transparently from within the network.

Queries and Dashboards

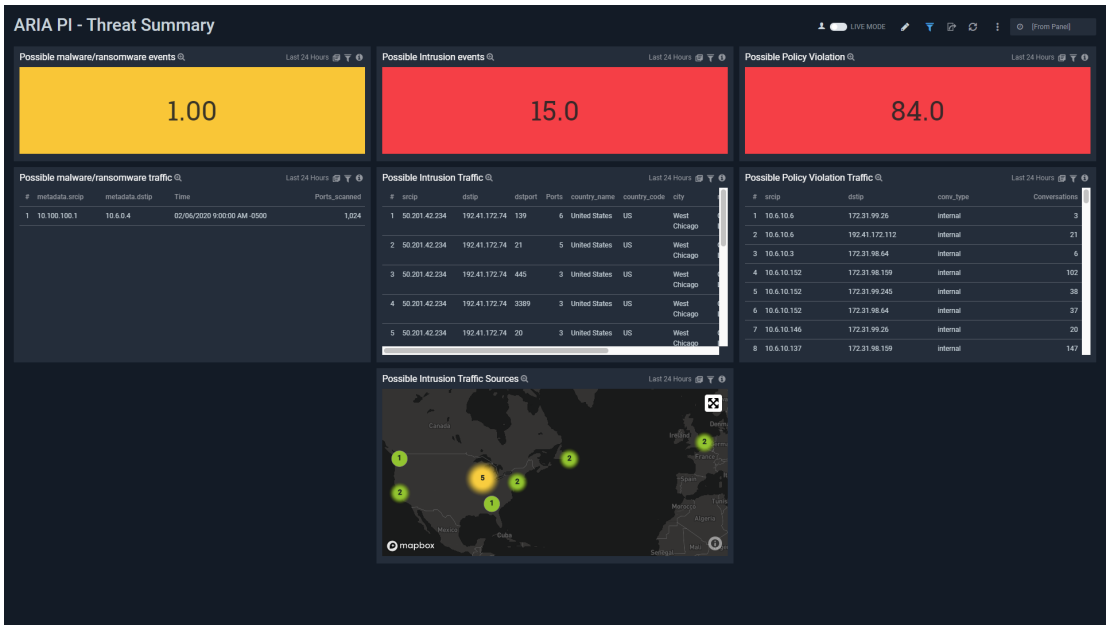
To get started, the ARIA Cybersecurity Solutions team has created a set of example queries and dashboards to detect cyber threats and attacks, as well as to visualize all internal network traffic communications.

Network Traffic Visibility Dashboard

The ARIA PI application creates unsampled NetFlow or IPFIX metadata for every network packet. Using this enriched data, this dashboard can help visualize, profile, and trend all internal network traffic. These visualizations can be used to drill down and highlight possible network segmentation gaps.

Threat Summary Dashboard

The ARIA PI solution provides an at-a-glance view that provides meaningful insights into network security. This gives users the ability to view threats and policy violations that are being detected by type, while also allowing them to investigate communication details in order to better monitor their security posture.



ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854

Connect with Us: ariacybersecurity.com • ARIAsales@ariacybersecurity.com • 800.325.3110

Follow Us: Linkedin • Facebook • Twitter • Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS