aria CYBERSECURITY SOLUTIONS

DATASHEET

ARIA Automated Investigative Response Application

Intelligent Cyber-Threat Identification for Rapid Response

Features and Benefits

Gain complete insight: Gain superior visibility into breaches involving your critical assets. Know which records were exposed and which weren't.

Focus efforts, act faster: Reduce intrusion detection and response to just a few hours.

More effective: Get automated threat-conversation extractions and notifications that allow for a focused and complete analysis of any breach.

Significant ROI: Shorten investigation time to a few hours compared to a few weeks using today's traditional IR techniques.

Better analysis: Enhance forensic analysis with the ability to pivot around events and use the information to look at what other critical assets an intruder or malicious insider may have attempted to access.

Reacting quickly and effectively to a cyber breach is difficult, time-consuming, and expensive. New and pending data privacy regulations, such as HIPPA and PCI DSS, as well as the EU's GDPR, are significantly tightening the notification period on breaches, including inadvertent access to the systems, to as little as a few days.

To fully meet compliance time constraints, organizations need an investigative response solution that not only validates that a breach occurred, but also enables them to determine the entire scope of the breach, including identification of the accessed data. To be truly effective, such a solution should be automated in order to minimize time delays and provide a focus for breach investigation.

In addition, security resources receive a staggering number of alert events from their firewalls, SIEMs, or other security technologies.

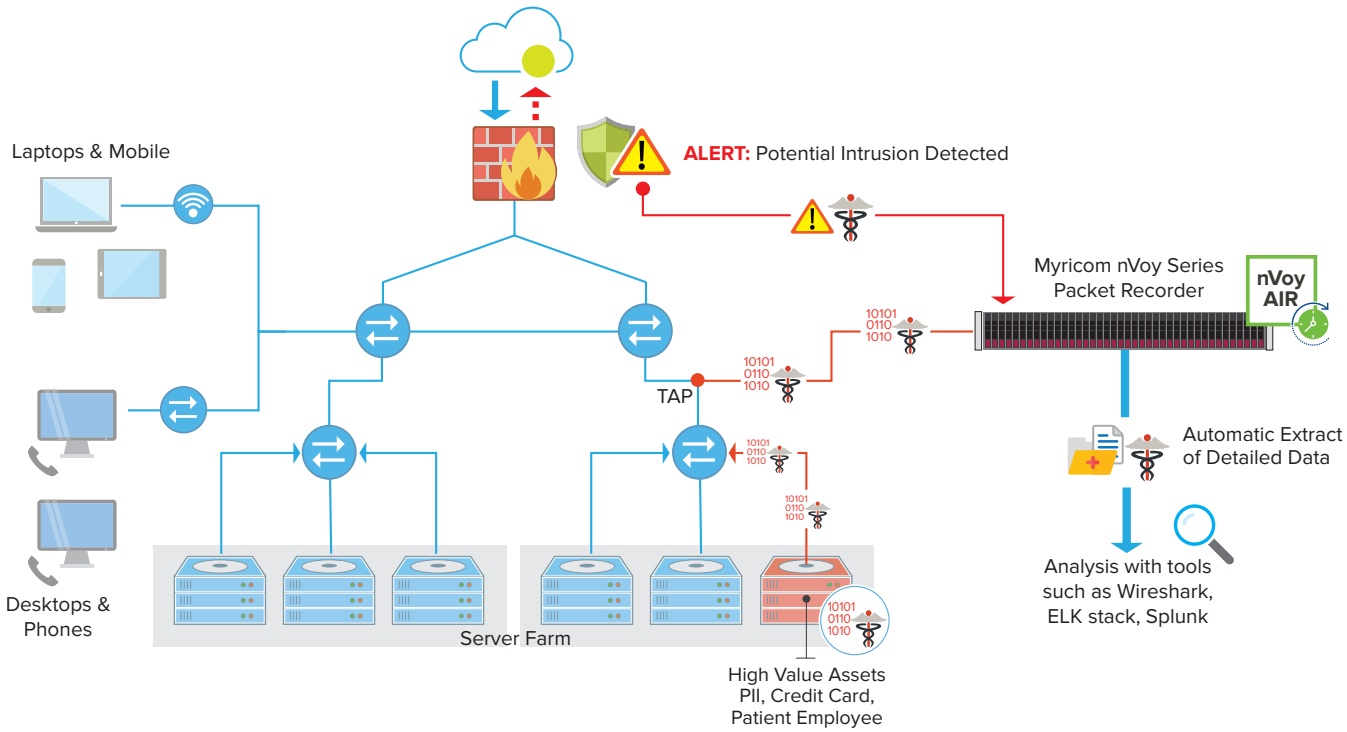
Even organizations with large, highly trained security teams are struggling to keep up with the volume. Manually combing through the events to determine which are worth further investigation takes time and adds the risk of error and missing a critical alert.

An Automated Investigative Response Solution

To address this challenge, the ARIA Automated Investigative Response (AIR) application automates two critical elements of the incident investigation process. When the ARIA AIR application is paired with our nVoy Packet Recorder, or other packet recorder, it assesses all alerts issued by a firewall or IDS/IPS to determine if any are against a user-specified list of critical assets (devices, applications, or a combination of the two). If so, the ARIA application uses the alert event data, including the source and/or target address, along with the recorded timestamps to drive the nVoy Packet Recorder to produce an extraction file of all the conversations between those devices.

By automating these two pieces – the alert identification and extraction of conversations – it eliminates manual intervention and thus, drastically reduces the risk of missing an alert, puts resources to better use, and most importantly, saves crucial time during the investigation.

An additional benefit is that this process can run 24 x 365 and generates the data required to remain in compliance with minimal human effort. There is no system to watch – the ARIA AIR application can notify your analyst team or your managed service provider when an extract is created so that work can begin immediately.



A Comprehensive and Cost-effective Investigative Response Solution

ARIA Cybersecurity Solutions, including the ARIA SDS applications and nVoy security appliances, are designed to dramatically change the approach to visualizing and verifying intrusions of critical data because it drops into any existing security infrastructure. Leveraging the combined strengths of today's leading security tools, such as firewalls, SIEMs or IDS/IPS, and the ARIA Cybersecurity Solutions, any organization can deploy an effective, time saving, and cost-efficient threat defense solution to protect their critical assets.

The nVoy Packet Recorder captures data provided by the tap, filters the traffic down to just the conversations occurring between critical device/applications and records, timestamps, and indexes all of these conversations at full line rate. This allow for quick search and creation of a file containing the extraction of particular data conversation of interest. Such extractions are saved on the recorder for detailed forensic analysis, as well as evidence for compliance purposes.

Because the recording is continuous, an analyst can "go back in time" to create extractions prior to the triggered intrusion notification that contain all prior conversations by the "intruder" and all the critical assets. Recordings can also be saved for extended periods on any optional network attached storage (NAS) device and pulled back to the recorder for extractions.

The nVoy Packet Recorder provides and preserves the critical evidence needed to verify a breach and view the entire scope of records exposed and accessed. Security analysts perform forensics against the actual data set – not just the log metadata, which does not provide enough definitive detail as to what happened. The other problem is that logs can be turned off and erased by skilled attackers once they breach a system. That can't happen with a passive data recording system that captures everything.

Contact Us Today: sales@ariacybersecurity.com or 800.325.3110

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 / Linkedin / Facebook / Twitter / Blog

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES Myricom NETWORK ADAPTERS