aria CYBERSECURITY SOLUTIONS

OVERVIEW

ARIA SD-Security ADR Application

A single platform for enterprise-wide automated threat detection and remediation

Benefits

- **Find the threats that matter:** Those that other security tools typically miss.
- **Stop attacks early in the kill chain:** Real-time identification before harm is done.
- **Validate alerts:** Drastically reduce the volume of alerts and surface the real threats and attacks.
- **Resource light:** Easy to deploy; system does the work of an SoC analyst for you out of the box.
- **Reduce costs:** Functionality equal to security operations center without the expense.

ARIA'S Software Defined Security Advanced Threat Detection and Response (ADR) application provide superior threat detection and containment functionality in a purpose-built solution. Now, using a single platform, security resources can find, validate, and stop threats in minutes. Today, this level of functionality is only achieved through multiple tools requiring continuous tuning and run by a highly trained security operations center (SOC).

Achieving complete visibility into network conversations is critical to finding critical threats faster and earlier in the attack life cycle. The ARIA ADR application solves this by first ingesting the NetFlow metadata for every network packet as generated by the integrated ARIA Packet Intelligence (PI) application. Then, it ingests alerts and logs from the environment: like firewalls, endpoints and server infrastructure, cloud providers, as well as production applications. Using this wealth of information, it can quickly hone in on any suspicious activities and correlate them using artificial intelligence (AI) based threat models included in the application.

Included are models for every known threat, leveraging machine learning (ML), and dynamically created rule sets to find each threat by telltale behavior patterns. The ARIA ADR application self-correlates the individual behaviors to verify the threat, its target, and its progress through the kill chain before declaring an alert. By this process, it eliminates false positives and elevates high-priority attack alerts.

Examples of threat telltale behaviors include lateral spread, new or threatening log-in behaviors, new data connections to critical resources, and many more. There are hundreds of behaviors, most of which are innocuous until they are put into context as a series of activities that match threat behavior clusters in our threat models.

While AI and ML science may sound complicated, it's all contained within the ARIA ADR application. The result is threats can't hide. The application doesn't need signatures or continuous community updates on the latest type of threat. Analysts don't need to create any rules or perform searches – the system does all that. Meaning when an alert is generated, it is real, and it is actionable.

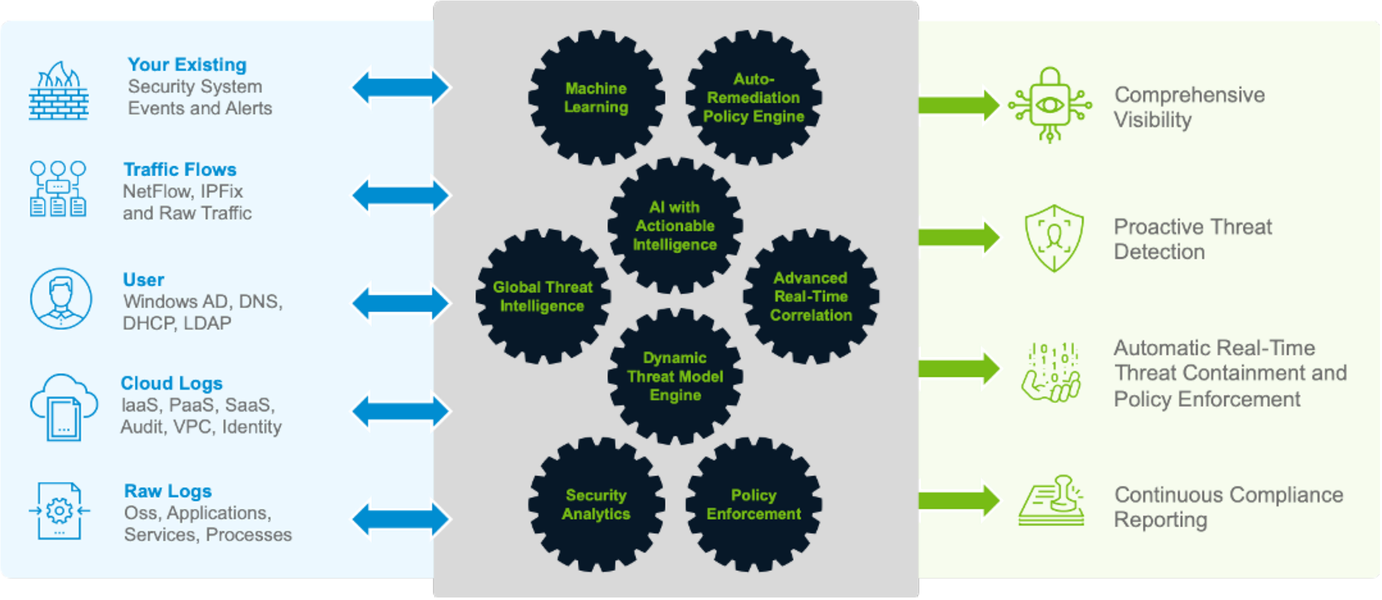
Types of Threats Found by ARIA ADR

Attacks	Intrusions	Breaches
Ransomware	Exploits	Data Exfiltrations
Malware		
Bots	APTs	
Brute-Force Attacks		Policy Violations
Compromised Credentials	DNS Stuffing	
Insider Attacks		
DDoS Attacks		

A key aspect of the ARIA ADR application is that once a threat is validated, it can communicate back by API to the ARIA PI application and instruct it to stop the conversations specific to that threat. It does this out of the box – no special configuration required. This is critical in containing threats like ransomware. It blocks all communication of infected devices or applications – isolating them off-line. However, since the application is intelligent, it can also tell the ARIA PI instances only to block the threat communication. This leaves critical devices and applications safely online, ensuring the continuation of normal business-critical operations until back-ups can be brought online.

There are other forms of containment ARIA ADR can execute upon. For instance, it can block specific external communications by writing polices to the firewall, and it can also deactivate a user or a device's compromised credentials. All of this is done by the system, either by the click of a button on the ADR UI – or automatically as the threats are alerted upon if so configured.

Our single pane of glass approach ensures ease of use. This process can be done through its UI or can be fully automated with no user involvement, leveraging the application's industry-leading SOC-AI™ capabilities. This is a major advantage over other security tools. SOC-AI™ is capable of automating – or removing the need for – most tasks a SOC performs. Most SIEMs and supporting detection tools that the ARIA ADR application replaces have a need for continual updating, which adds a heavy eight-hour-a-day workload by a highly trained SOC team. The SOC-AI functionality removes the need for tasking, including defining rules, filtering responses, creating and executing playbooks, verifying threats, and then taking action to contain the threats. Finally, it auto generates reports telling the status of your organization's security posture and provides reports required to prove industry compliance with PCI, HIPPA, and NIST. It truly can be viewed as having a SOC-in-a-box.


Your Existing
Security System Events and Alerts
Traffic Flows
NetFlow, IPFix and Raw Traffic
User
Windows AD, DNS, DHCP, LDAP
Cloud Logs
IaaS, PaaS, SaaS, Audit, VPC, Identity
Raw Logs
Oss, Applications, Services, Processes
Machine Learning
Auto-Remediation Policy Engine
AI with Actionable Intelligence
Global Threat Intelligence
Advanced Real-Time Correlation
Dynamic Threat Model Engine
Security Analytics
Policy Enforcement
Comprehensive Visibility
Proactive Threat Detection
Automatic Real-Time Threat Containment and Policy Enforcement
Continuous Compliance Reporting

The ARIA ADR results are incredibly accurate due to the ML and AI techniques used to eliminate false positives and validate all alerts. The SOC-AI capabilities are also valuable in establishing automated remediation actions and enforcing connectivity policies, therefore preventing violations. This gives organizations a solution that will evolve with attacks as they become more sophisticated, allowing them to maintain the upper hand in accelerated incident response.

With ARIA ADR organizations gain:

- Multiple technologies deployed in one application that provides the most thorough threat detection.
- Deep visibility into network traffic to detect threats missed by traditional means.
- Identification of attacks as they land and spread before harm is significant.
- Protection of their IoT environments.
- Precise containment based on threat conversation, leaving critical devices or applications online.

The result is a powerful cybersecurity solution for organizations that do not wish to invest in a SOC.

Contact Us to Schedule a Technical Demonstration or Arrange an Evaluation ✉ ARIAsales@ariacybersecurity.com

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