aria CYBERSECURITY SOLUTIONS

BUSINESS CASE

ARIA ADR Provides the Industry's Best Threat Detection and Response

SITUATION: To truly detect and stop all major threat types, companies must make significant investments in products, processes, and people. Most organizations start with firewalls and EDRs but soon realize this approach only covers 20% of their threat surface where attacks originate and proliferate.

CONCERNS: Tools such as SIEMs, UEBAs, network traffic analyzers, IDS/IPSs, threat intel feeds, and SOARs all deliver tremendous value in covering the remaining 80%, but each only provides a piece of the puzzle needed to find threats. Hence, even though this entire security stack of tools—which are thought of as the ultimate solution—still relies on separate processes to stop attacks. With this many tools the law of diminishing returns sets in because the daily (24x365) alert "noise" is too difficult to wade through. Then there is the required investment in highly trained security teams to operate and manage these disparate tools. Before they even get started, most organizations realize they can't support this endeavor and settle for purchasing only the individual components they can afford and manage. As a result, they end up with very limited coverage.

SOLUTION: ARIA ADR is a single, purpose-built platform that combines the analytics of five detection tools into one. It then uses AI and ML to feed these analytics through our patented dynamic threat behavior models, a significant advantage over approaches that use static rule sets. With ARIA ADR, you will automate the detection, verification, and remediation of cyber-attacks, while eliminating the labor-intensive intervention required by expensive security experts and SOAR tools. This unique approach makes the ARIA ADR solution extremely cost-effective to purchase and operate and the best way to quickly find and stop all major attack types.

END RESULT: Too many tools = too complex. Not enough tools = not enough coverage.
ARIA ADR provides organizations with the value of a complete security operations center (SOC), right out-of-the-box. All the tools and processes are consolidated into one automated platform, and it removes the need for expensive, highly trained analysts, providing ultimate ROI.

	THREAT TYPES									THREAT COVERAGE	
	Intrusions	Brute Force Attacks	Malware	Ransomware	DDoS Attacks	Compromised Credentials	Insider Threats	Data Exfiltration	Policy Violations	% Detects	% Remediates
SIEM	◔	◑	◔	◔	○	○	○	◔	◑	◔	○
UEBA	○	◔	○	○	○	◑	◕	◔	◔	◔	○
NTA	◑	◔	○	○	◔	◔	◔	◔	◑	◔	◔*
Threat Intel	○	○	◔	○	○	○	○	○	◔	◔	○
IPS	○	○	◑	◔	○	○	○	◔	◔	◔	◔**
SOAR	○	○	○	○	○	○	○	○	○	○	○***
ARIA ADR	●	●	●	●	●	●	●	●	●	●	●

*Does very little. Some can disrupt TCP/IP network detected attacks — but not UDP based, nor user based.
**Only stops known signature attacks and policy violations at the network traffic level.
***Helps IR staff stop certain attacks by following playbooks.