TECHNICAL REVIEW

ARIA ADR

Technical Approach to Automated Threat Detection, Investigation and Response

This paper reviews several use cases to illustrate how ARIA ADR works and the technical approach taken to overcome the challenges related to the accurate detection and containment of a broad set of attacks that do the most harm today — before they can do significant damage.

Aria Logo

aria CYBERSECURITY SOLUTIONS

The Threat Landscape is Evolving and is Making Traditional Cybersecurity Approaches Ineffective

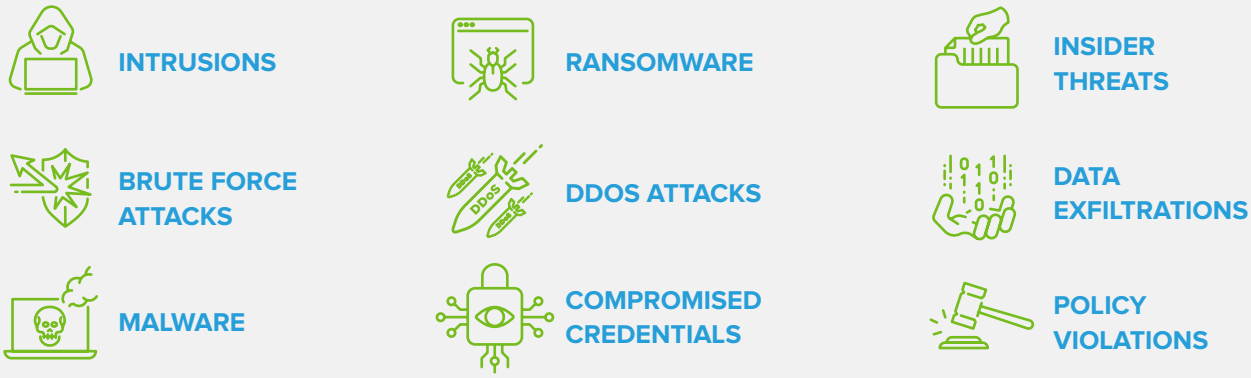
Modern threats and more importantly, modern attacks have changed. Older approaches that used playbooks to orchestrate a series of traditional search and detection processes – looking at partial data sets – aren't sufficient any more. They can't identify threats their data ingests don't see, and worse, tend to be slow and reliant on skilled, dedicated, threat-hunting staff that must be operate 24x7.

Organizations that primarily spend their time and dollars chasing vulnerabilities to attempt to stay a step ahead of hackers inevitably discover that this is inadequate as a form of protection. Why? Because most of the attacks that do the most harm today don't rely on code vulnerabilities or, if they do, they are usually found months too late – by the industry at large – that damage being done in thousands of organizations worldwide.

The SolarWinds Sunburst hack is an excellent example of this, but so too are any form of modern zero-day malware, ransomware, or intrusion techniques that trick end users into enabling the attack or take advantage of required openings in perimeter defenses.

Nine different threat attack types have emerged as the most harmful, and must either be quickly detected or stopped or defended against upfront.

Threats Detected by ARIA ADR



CRITICAL CONCERNS TO BE ADDRESSED

1 | Threats and attacks are being missed.

The SolarWinds Sunburst hack is an example of an advanced persistent threat (APT) attack that the cybersecurity industry still consistently misses – in this case, for almost a year, and now, more than 11,000 Orion software users are struggling with the question of whether they have Russian intruders lurking inside their networks.

Many of these companies have a stack of threat detection tools designed to prevent this from happening, but in reality these tools are ineffective because they can't detect intruders once they are inside the network. The same is true for ransomware, zero-day malware, and other intrusions/exfiltrations.

2 | The length of time it takes to detect attacks.

The problem with ransomware and/or targeted attacks is that once they land, real harm occurs in minutes, and it only gets worse the longer they are active in the network. Security tools and processes that rely on manual inspection and investigation can take days, weeks, or even longer to detect, verify, and isolate attacks.

3 | Stopping attacks requires additional people, processes, and time.

Detection and verification are only one half of the effort. Once an attack is found, it must be contained. Unfortunately, legacy processes often rely on other internal teams or third-party MSPs to take action, inevitably leading to significant further delays.

4 | Gaining visibility across the entire enterprise.

An effective threat detection solution must work across the entire organization – all physical sites, remote users, data centers, and cloud environments. If security teams need an extensive stack of tools to do this it adds extra effort and complexity, which equals lost time and risk to properly detect, verify, and stop attacks.

Solution

ARIA Cybersecurity Solutions designed the ARIA ADR solution to find, verify, and stop all types of attacks – automatically and in real time. ARIA ADR successfully addresses the previously discussed concerns and other more pragmatic issues, including making effective threat detection more affordable than today's traditional approaches.

HOW DOES IT DO THIS?

The ARIA ADR solution detects threats and attacks by their unique, tell-tale behaviors exhibited throughout their kill chain (lifecycle). This approach works because the attackers can't hide. The solution detects never-seen-before threats like zero-day attacks and file-less ransomware since it does not rely on signatures or SIEM-based static rule detection methods.

To achieve a much more effective approach, ARIA Cybersecurity built over seventy patented threat behavioral models to detect all types of modern threats and attacks. While the threat models include known threat behaviors, ARIA ADR also learns and finds anomalous threat/attack behavior using machine learning (ML) to distinguish abnormal from normal device, application, and user behaviors.

IT STARTS WITH THE DATA

ARIA ADR leverages only the right types of data sources to best identify a wide breadth of threats. At its heart, the solution is a big data platform that collects and digests threat and attack data from a variety of sources across the entire enterprise, such as on-premises, data centers, remote sites, the WAN, and public Cloud instances, including:

- **The output of existing security devices like firewalls, EDRs, and similar security tools**
- **Parsed logs from the IT infrastructure, including DNS, DHCP, and directories**
- **Parsed application logs, as well as from operating systems on servers and endpoints**
- **Network traffic by deriving NetFlow metadata from every packet**
- **APIs, such as from Microsoft 365 including SharePoint, Teams, and Active Directory**

A HIGHLY-EFFECTIVE AUTOMATED AI-SOC

These sources provide the raw inputs into the threat models to monitor for a wide range of attacks across the entire organization. Monitoring the internal network, including within the Cloud, can help detect many attacks that go missed today, such as ransomware, malware, and even intrusions. It does so by detecting behaviors across the network, such as when the initial Orion Sunburst hack tried to communicate externally, and at the same time spread within the network. As the attack takes root – at the point where bad external actors have control of certain assets – ARIA ADR detects these lateral spread attempts to gain access to critical applications and data.

ARIA ADR detects the following behaviors with artificial intelligence to correlate them all – without the need of an analyst:

- **Network scans**
- **New communication attempts to new device types or addresses never attempted before**
- **New login attempts**
- **Brute force login attempts**
- **New files access, to data movement**
- **Exfiltrations through email or DNS tunnels.**

A key concern is that so much threat data can create many threat indicators – much of it usually meaningless, unless it's a small part of a larger set of related threat behaviors. ARIA ADR relies on artificial intelligence (AI) to correlate the relevant threat indicators together. In other words ARIA ADR verifies the type of threat, its targets, and its criticality to the organization. ARIA ADR only surfaces confirmed alerts (not individual threat indicators).

For external threats, AI also checks the threat communication against our industry best Threat Intelligence to identify communication with known bad websites. It also checks and notes the countries being communicated with and detects communications to new countries, comparing all traffic with a list of restricted countries. This allows the AI function to verify further and add context to the alert. Also, AI helps scope the threat and makes recommendations on how to stop the attack.

ARIA ADR can do more than just make recommendations as its AI capabilities provide a means to stop the threat or attack. For any given alert, the appropriate action can be taken automatically. Appropriate action selected depends on the type of attack, the criticality of the targeted assets, and the available options.

Threat Containment Use Cases

Below are **three common cybersecurity scenarios** that organizations struggle with today and how ARIA ADR can stop and prevent future incidents from occurring.

1 | Threats and attacks are being missed.

This is accomplished by ARIA ADR writing a policy to the firewall management system instructing it to block connectivity to the bad sites, such as when CnC communication is attempted. Additional policies can be written to the firewall to block communication with any public IP address identified with an intrusion, exfiltration, or other threat/attack.

This type of remediation can be used on intrusions that were allowed by the Sunburst hack – once the APT intruder is detected by his/her actions, communication to the associated external control and/or exfiltration sites can be blocked.

2 | Threats and attacks are being missed.

If deployed inline, ARIA ADR can stop threats from spreading laterally inside the network, a telltale sign of ransomware or malware attacks. This can occur once intruders land on a compromised device and try to go deeper into the network to access critical devices and/or try to remove data from these systems. ARIA ADR can also protect critical assets from undesired communication of any kind before it's associated with a specific threat by setting a network communication policy. It is a great way to protect critical data or critical functions from unintended network connectivity.

3 | Detecting lost user credentials, insider threats, and related threat activity.

If given administrative control, ARIA ADR can deactivate those users' credentials on the directory. AI allows that user's compromised credentials to be deactivated from within the associated alert, while signaling that the user requires new credentials.

In some cases, all three options are available for a given attack – depending on its progression through the kill chain – and all are offered up in the highest order of relevance to most effectively stop the attack.

There are two options for executing a stop order in ARIA ADR:

1. **The first is from within the ARIA ADR alert screen and addresses a specific alert. It allows the recommended action to be taken with the push of a button. Policy actions can also be undone from the UI when the alert condition is cleared.**

2. **The second is fully automated, where ARIA ADR is configured to automatically stop all or only specific alerts under specific conditions. This includes certain types of attacks, at certain levels of criticality, and/or for only certain times of day (such as nights, weekends, etc.).**

Summary

ARIA ADR can overcome the critical challenges caused by today's threat detection and response processes and tools:

- **It finds and stops the attacks that do the most harm** – in real time, often before significant damage is done.
- **It does all the work of highly skilled analysts, around the clock, and at the speed of electrons** – so companies don't have to pay for these types of staff and still get much better outcomes.
- **It can be deployed in any type of environment** – on-premises, Cloud, and can be used by a remote workforce.
- **It provides the functionality of a security stack of seven different expensive tools in a single screen** – including SIEMs, NBAD/NTAs, UEBAs, IDS/IPS, threat intelligence, threat data lakes, and SOAR.
- **It allows part-time IT/security staff to effectively use the tool** – only spending a few minutes a day by getting notified when action needs to be taken.
- **It can be procured as part of a very cost-effective managed detection and response service.**

Bottom Line: Using ARIA ADR can save significant operational and capital cost savings, all while providing improved outcomes compared to leading threat detection tools by finding and stopping the threats that matter.

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

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