

ARIA ADR: Automating the MITRE ATT&CK Framework to Stop Cyberattacks

Created in 2013, the MITRE ATT&CK Framework has evolved to be used by organizations to understand hackers' attack behaviors and techniques. The framework is invaluable as it provides a standard that industry professionals can reference when discussing and investigating cyber threats and attacks. The goal over the last 12 months has changed as the ATT&CK framework is very good at helping finding nation state backed attackers whose techniques evade most modern tools and processes in use today.

Known techniques, steps and methods hackers use during attacks are indexed and detailed, providing a guidepost to understand approaches used against a particular platform. Much like how the threat landscape and cyber-attacks evolve, so does the framework as attack details are continually added — making the framework an invaluable resource for identifying attacker models, methodologies, and mitigation.

The challenge is that to be effectively used – it assumes that highly trained dedicated security analysts with a great set of tools have real-time 24x365 access to all threat surfaces within an organization. Yet, even if this were funded, fully understanding all the common adversary techniques is nearly impossible for any organization. It is simply too much to monitor every single attack type — never mind catalog and tracking the work within the framework by hand for use.

This short brief demonstrates how the ARIA Advanced Detection and Response solution does the work to protect organizations from attacks at every stage of the MITRE ATT&CK framework.

Mitre Att&ck Enterprise















RECON

WEAPONIZE

DELIVER

EXPLOIT

C&C

EXECUTE

MAINTAIN

RESOURCE DEVELOPMENT

ADR can detect and identify all networked devices. Detects compromised accounts and infrastructure.

INITIAL ACCESS

The adversary is trying to get into your network

ADR monitors all paths of access into the organization's environment: Through the Firewall, Over the Network, From the End point.

EXECUTION

The adversary is trying to run malicious code

ADR can detect execution of processes on monitored end points.

PERSISTENCE

The adversary is trying to maintain their foothold

ADR watches for threat behaviors over days and weeks, detecting and correlating threat behaviors exhibited by APTs/intrusions and other attacks.

PRIVILEGE ESCALATION

The adversary is trying to gain higher-level permissions

ADR monitors the Directories for privilege use and escalation, critical to detecting both compromised credentials and malicious insider types of misuse.

CREDENTIAL ACCESS

The adversary is trying to steal account names and passwords

ADR monitors credential use and access at the directories and at the applications. It can detect odd credential use behaviors leveraging ML, including what when, from where, how often and simultaneous use to name but a few vectors.

DISCOVERY

The adversary is trying to figure out your environment

ADR discovers all internal network connected assets, and allows for the classification of such assets so tthey can be properly monitored and upfront protected with strong network connectivity polices.

LATERAL MOVEMENT

The adversary is trying to move through your environment

ADR's superior approach to network monitoring detects all forms of lateral movement. Applying ML detects behaviors that are odd for devices or types of devices. Attack behaviors associated with intrusions and threat spreads are already known to the system and can be picked up as they go active.

EXFILTRATION

The adversary is trying to steal data

ADR can detect exfiltrations of data from Servers, VMs, containers and end points. In conjunction it can detect egress attempts across a large number of potential exit points including: the internal network, the Cloud USB interfaces, and even through the firewall such as via monitoring traffic over ports that must be left open

COMMAND AND CONTROL

The adversary is trying to communicate with compromised systems to control them

ADR was built to detect attempts to connect to external CnC. It detects CnC outreach behavior such as from TCP floods and beaconing. It adds to this the industry's most comprehensive Threat Intelligence feed that is updated daily with millions of known bad and cleaned up CnC sites. It can detect attempts - and stop them before connectivity to them is attained.

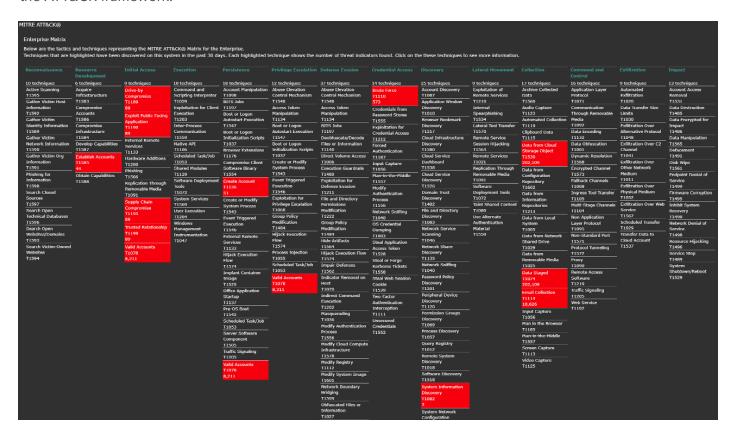
IMPACT

The adversary is trying to manipulate, interrupt, or destroy your systems and data

ADR detects accounts accessed and removed. It detects data manipulation destruction and removal. Detects internal network as well device based DoS attacks. Detects resource compromise/hijacking.

Let's look at an example of ARIA ADR at work. This system was deployed in an energy and utility provider. Cybersecurity had been outsourced to their MSP, but that approach had failed a required penetration test and security audit. ADR was put in to help the utility's IT staff to get a better hold on what was happening to ensure compliance with industry requirements. ADR ingested output from the utility's infrastructure including their firewalls, directories, as well as events from critical applications and from cloud services. Also included were events from Windows and Linux servers as well as from employee devices. Lastly network flow analytics were also ingested from the internal network and the firewalls. The goal is a wide and all-encompassing MAP of coverage as per the frameworks prescribed best practices.

What happened next was telling. After a month in place a simple concise alert appeared in the system UI indicating a verified intrusion into the utility had begun, detailing the devices involved. How was this found? The detail is shown by looking at ADR's rendering of the alerts threat behaviors found that corresponded to the ATT&CK framework.



As shown in the figure above, ADR at this stage of the attack (when captured off the UI) had seen over time 14 different behaviors as identified by the ATT&CK Framework. What this means is that as an attack progresses through its kill chain, it begins to exhibit more instances of a given behavior as well as additional behaviors. ADR maps these behaviors into 72 known attack types. Meaning it uses AI to associate the combination of behaviors into an alert and continues to confirm this alert with additional threat behavioral data added over time.

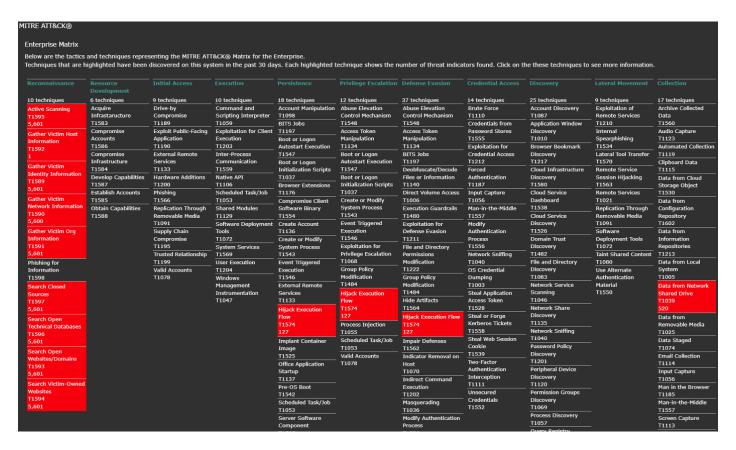
The key point is that this effort was all done by ADR. There was no human involvement in identifying the behaviors, correlating them into an attack, and then providing a validated and a persistent alert that was shown at the UI level which continued to have additional threat behavior added to it.

ADR allowed the IT team, via the same UI alert screen, to stop the attack activity with a single click. This action told the inline deployed ADR device to stop (block) all associated attack communication.

It will also stop the attackers from communicating in or sending data out through the firewall, and it can disable compromised or escalated credentials if used, to stop access to critical applications and services. After the attack the utility chose to enable the full automation option to automatically stop such attacks involving critical systems as detected and verified by ADR.

ADR also uses attack behavior-based threat models to pick up polymorphic malware and ransomware. Such attacks can't be picked up by AV or IDS signatures as the signatures change with each device compromise. In addition, counting on detecting communication back to known bad sites won't work as many of these attacks are programed to change site access continuously making it a battle to keep up. Behavioral approaches work best. And yet most behavioral based EDRs look for a set pattern of behaviors, and don't have the ability to employ the more flexible ATT&CK framework approach. Even the best like CrowdStrike can miss such attacks until they have seen the pattern in the wild and added it to an update. ADR does not count on seeing a fixed pattern of behaviors with its Al driven approach – allowing it to use the ATT&CK framework to sense any combinations of behavior patterns.

Below is such an example. In this case the ADR detected early-stage zero-day ransomware before it got further than the initial systems compromise. Note this zero-day version never used a C&C in the early stage that most systems rely on to identify the threats.



The customer was able to quarantine the device using ADR to prevent further spread, until the device could be cleaned and restored. The result was that the attack was stopped in the early phase where, through its programing, was attempting to laterally spread internally off the initially compromised device. ADR in this case contained what could have been a widespread disaster to a single device.



ARIA ADR was designed to automatically find and stop network-borne threats as soon as they become active, and most importantly, before significant harm occurs. The simple to deploy solution provides built-in Al-driven SOC functions that provide all the benefits of a traditional security operations center (SOC) but operates without humans, doing so 1000 times faster at a fraction of the comparable cost. Unlike other solutions, ARIA ADR provides full MITRE ATTACK Framework threat-surface coverage — on premises, data centers, remote devices, and the Cloud. Operated anywhere by IT resources with no cybersecurity training.

ARIA ADR was purpose-built to overcome the critical challenges caused by today's threat detection and response processes and tools. ARIA ADR:

- Finds, stops the attacks that do the most harm in near real time before significant damage is done.
- 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.
- Can be deployed across any environment on-premises, Cloud, and operated by a remote workforce.
- · Can run fully automated.
- Allows part-time IT/security staff to use the tool effectively only spending a few minutes a day by getting notified when action needs to be taken.
- Provides all the forensic detail required when an attack does happen
- Ensures compliance.
- · Lowers cyber insurance qualification and premiums by meeting new strict criteria



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







