

# 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 they can be properly monitored and upfront protected with strong network connectivity policies.

### 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.

MITRE ATT&CK®

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for the Enterprise. Techniques that are highlighted have been discovered on this system in the past 30 days. Each highlighted technique shows the number of threat indicators found. Click on the these techniques to see more information.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	27 techniques	14 techniques	25 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Fuzzing	Account Access Removal
Gather Victim Host Information	T1583	T1199	T1059	Built-in Jobs	T1548	T1548	T1119	T1087	T1524	T1560	T1071	T1020	T1531
T1592	Compromise Accounts	89	Exploitation for Client Execution	T1137	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	T1586	Exploit Public Facing Application	T1203	Automated Execution	T1124	T1124	T1555	Browser Bookmark	T1524	T1123	T1524	T1020	Data Encrypted for Impact
T1589	Infrastructure	T1190	Inter-Process Communication	T1547	Root or Logon	Root or Logon	RTLS Jobs	Discovery	Lateral Tool Transfer	T1119	T1092	T1496	
Gather Victim Network Information	T1584	External Remote Services	T1559	Initialization Scripts	T1547	T1547	Desktop/Cache/Decode	T1212	Cloud Infrastructure Session Hijacking	T1115	T1122	T1048	Data Manipulation
T1590	Develop Capabilities	Native API	T1027	Files or Information	T1027	T1027	Forced Authentication	T1563	Remote Service	T1115	T1122	T1565	Data Manipulation
Gather Victim Org Information	T1587	T1123	Browser Extensions	T1176	Direct Volume Access	T1187	Cloud Service	Remote Services	T1021	T1568	T1568	T1561	Disk Wipe
T1591	Establish Accounts	Hardware Additions	T1023	Compromise Client System Process	T1054	T1054	Input Capture	Configuration Through Removable Media	T1091	T1602	T1527	T1011	Service
Phishing for Information	T1585	Phishing	T1129	Software Deployment Tools	T1136	T1136	Modify Authentication	T1526	Software	T1080	T1108	T1490	Network Denial of Service
T1598	Obtain Capabilities	T1588	Replication Through Removable Media	T1091	System Services	T1569	Event Triggered Execution	T1222	OS Credential	T1083	T1093	T1029	Service
Search Closed Sources	T1597	Supply Chain Compromise	T1195	89	Trusted Relationship	T1199	89	Valid Accounts	T1078	8,211			
Search Open Technical Databases	T1596	Trusted Relationship	T1199	89	Valid Accounts	T1078	8,211						
Search Open Websites/Domains	T1593	Valid Accounts	T1078	8,211									
Search Victim-Owned Websites	T1594												

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 AI 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.

MITRE ATT&CK®

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for the Enterprise. Techniques that are highlighted have been discovered on this system in the past 30 days. Each highlighted technique shows the number of threat indicators found. Click on these techniques to see more information.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	6 techniques	9 techniques	10 techniques	18 techniques	12 techniques	37 techniques	14 techniques	25 techniques	9 techniques	17 techniques
Active Scanning T1595 5,601	Acquire Infrastructure T1583	Drive-by Compromise T1189	Command and Scripting Interpreter T1059	Account Manipulation T1098	Abuse Elevation Control Mechanism T1548	Abuse Elevation Control Mechanism T1548	Brute Force T1110	Account Discovery T1087	Exploitation of Remote Services T1210	Archive Collected Data T1560
Gather Victim Host Information T1592 1	Compromise Accounts T1586	Exploit Public-Facing Application T1190	Exploitation for Client Execution T1203	BITS Jobs T1197	Access Token Manipulation T1134	Access Token Manipulation T1134	Credentials from Password Stores T1555	Application Window Discovery T1010	Internal Spearphishing T1534	Audio Capture T1123
Gather Victim Identity Information T1589 5,601	Compromise Infrastructure T1584	External Remote Services T1133	Inter-Process Communication T1559	Boot or Logon T1547	Autostart Execution T1197	BITS Jobs T1197	Exploitation for Credential Access T1212	Browser Bookmark Discovery T1217	Automated Collection T1570	Clipboard Data T1119
Develop Capabilities T1587 5,601	Hardware Additions T1200	Native API T1106	Initialization Scripts T1037	Boot or Logon T1037	Deobfuscate/Decode Files or Information T1140	Deobfuscate/Decode Files or Information T1140	Forced Authentication T1187	Cloud Infrastructure Discovery T1580	Remote Service Session Hijacking T1563	Data from Cloud Storage Object T1530
Gather Victim Network Information T1590 5,600	Establish Accounts T1585	Phishing T1566	Scheduled Task/Job T1053	Browser Extensions T1176	Direct Volume Access T1006	Direct Volume Access T1006	Input Capture T1056	Cloud Service Dashboard T1538	Remote Services T1021	Data from Configuration Repository T1602
Gather Victim Org Information T1591 5,601	Obtain Capabilities T1588	Replication Through Removable Media T1091	Shared Modules T1129	Compromise Client Software Binary T1554	Create or Modify System Process T1543	Exploitation for Defense Evasion T1211	Man-in-the-Middle T1557	Cloud Service Modify T1526	Replication Through Removable Media T1091	Data from Information Repositories T1213
Phishing for Information T1598	Supply Chain Compromise T1195	Software Deployment Tools T1072	Tools T1569	Event Triggered Execution T1068	Execution T1546	File and Directory Permissions Modification T1040	Authentication Process T1556	Domain Trust Discovery T1482	Software Deployment Tools T1072	Data from Local System T1005
Search Closed Sources T1597 5,601	Trusted Relationship T1199	User Execution T1204	System Services T1546	Event Triggered Execution T1068	Exploitation for Privilege Escalation T1068	Group Policy Modification T1484	Network Sniffing T1040	File and Directory Discovery T1083	Taint Shared Content T1088	Data from Local System T1005
Search Open Technical Databases T1596 5,601	Valid Accounts T1078	Windows Management Instrumentation T1047	External Remote Services T1133	Group Policy Modification T1484	Group Policy Modification T1484	Hide Artifacts T1564	OS Credential Dumping T1003	Network Service Scanning T1046	Material T1550	Data from Network Shared Drive T1039 520
Search Open Websites/Domains T1593 5,601	Hijack Execution Flow T1574 127	Hijack Execution Flow T1574 127	Hijack Execution Flow T1574 127	Hijack Execution Flow T1574 127	Hijack Execution Flow T1574 127	Process Injection T1055	Steal Application Access Token T1528	Network Share Discovery T1135	Software Deployment Tools T1072	Data from Removable Media T1025
Search Victim-Owned Websites T1594 5,601	Implant Container Image T1525	Scheduled Task/Job T1053	Scheduled Task/Job T1053	Scheduled Task/Job T1053	Scheduled Task/Job T1053	Impair Defenses T1562	Steal Web Session T1539	Network Sniffing T1040	Software Deployment Tools T1072	Data Staged T1074
	Office Application Startup T1137	Office Application Startup T1137	Office Application Startup T1137	Office Application Startup T1137	Office Application Startup T1137	Indicator Removal on Host T1070	Cookie T1539	Password Policy T1201	Software Deployment Tools T1072	Email Collection T1114
	Pre-OS Boot T1542	Pre-OS Boot T1542	Pre-OS Boot T1542	Pre-OS Boot T1542	Pre-OS Boot T1542	Indirect Command Execution T1202	Two-Factor Authentication T1111	Peripheral Device Discovery T1120	Software Deployment Tools T1072	Input Capture T1056
	Scheduled Task/Job T1053	Scheduled Task/Job T1053	Scheduled Task/Job T1053	Scheduled Task/Job T1053	Scheduled Task/Job T1053	Masquerading T1036	Unsecured Credentials T1552	Permission Groups T1069	Software Deployment Tools T1072	Man in the Browser T1185
	Server Software Component T1057	Server Software Component T1057	Server Software Component T1057	Server Software Component T1057	Server Software Component T1057	Modify Authentication Process T1057	Process Discovery T1057	Process Discovery T1057	Software Deployment Tools T1072	Man-in-the-Middle T1557
								Guest Registry T1113		Screen Capture T1113

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 programming, 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 AI-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



**Contact Us at [ARIAsales@ariacybersecurity.com](mailto: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 01854**

**Connect with Us:** [ariacybersecurity.com](http://ariacybersecurity.com) • [ARIAsales@ariacybersecurity.com](mailto:ARIAsales@ariacybersecurity.com) • 800.325.3110

**Follow Us:** [LinkedIn](#) • [Facebook](#) • [Twitter](#) • [Blog](#)

**aria** CYBERSECURITY  
SOLUTIONS

**ariasDS**

**nVoy** SECURITY  
APPLIANCES

**Myricom** NETWORK  
ADAPTERS