ATTACKIQ

CONTINUOUS SECURITY VALIDATION

# How To Get Started Testing with

# The MITRE ATT&CK™ Framework

# Contents

## Notice

AttackIQ® publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.

# MITRE | ATT&CK™


## What is MITRE ATT&CK?

The AttackIQ® platform has automated use of the MITRE ATT&CK framework, the most authoritative, comprehensive, and complete set of up-to-date attack techniques and supporting tactics in the world. MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world data. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

MITRE's stature in the cyber community and the independence of their intellectual property in the ATT&CK matrix make it the ideal platform from which security operations management, executive staff, and the Board of Directors can objectively evaluate and measure cybersecurity controls' performance, risk, and capability.


## Why is the MITRE ATT&CK Framework Important to You?

MITRE ATT&CK is, in both depth and breadth, the largest attack knowledge base, providing suggested mitigation techniques, detection procedures, and other important technical information. MITRE has expanded the kill chain to include the widest variety of tactics, which are then supported by detailed techniques. This organized approach enables you to methodically select the attack you need to validate your security controls and to understand the gaps in order to rationally expand your security controls set.

MITRE ATT&CK is the largest, most in-depth, organized, and strongly supported knowledge base of adversarial behavior. You can precisely validate your security controls and gain visibility into gaps in your defenses. Security management can rapidly and easily identify critical problems for remediation. This objective assessment provides a data-driven approach to prioritizing and scaling your cybersecurity program and budget.

## How Can You Get Started Testing Your Security Capabilities Against MITRE ATT&CK?

Regardless of the sophistication of your security program, one principle still holds true: keep it simple. When applying the vast knowledge base of MITRE ATT&CK, start with the most critical areas of concern to you — go deep, not wide. Test your detection, prevention and response capabilities end-to-end and then determine the next tactics of the framework to focus your efforts.

_Initial Access

_Execution

_Persistence

_Privilege Escalation

_Defense Evasion

_Credential Access

_Discovery

_Lateral Movement

_Collection

_Exfiltration

_C&C

## Communicating Through a Common Lexicon to the Business

MITRE ATT&CK has brought a well-matured taxonomy of the tactics and techniques that may be leveraged by any prospective attacker. This provides, for the first time, a common lexicon that enables stakeholders, cyber defenders, and vendors to clearly communicate on the exact nature of a threat and the objective assessment of the cyberdefense plan that can defeat it. This common lexicon brings a universal language that can be used to describe the procedures of an attacker or attack tools, and then exactly the techniques which they deploy. The precise lexicon of MITRE ATT&CK enables more precise assessment of threats and a faster, better-targeted response.

## Testing Your Known Security Controls Against Adversarial Behavior

With this approach, you can use the MITRE ATT&CK tactics and techniques to help you both measure the efficacy and configurations of your security controls and validate their performance against your assumptions. Security control categories might include data loss prevention (DLP), endpoint detection and response (EDR), web filtering, firewalls, and more.

This is highly useful as you can immediately validate that your security controls are configured correctly, performing as expected, and delivering the return on investment that you expect. The goal is to keep it simple. The average enterprise may have as many as 75 security products, so it helps to start by prioritizing this list and selecting the first five that are highly critical to your business operations.

For example, firewalls are fundamental to your security stack. AttackIQ will enable you to test this important control, including network segmentation, application control policy enforcement, and malware protection. Another important category might you select is EDR, where you similarly could test suspicious and/or anomalous endpoint activities.

In any case, list the top three to five capabilities you assume are present and the key reasons you purchased the product in the first place. Then it becomes relatively easy to map those capabilities to the MITRE ATT&CK tactics and techniques that you can then use to test the configuration and effectiveness of your security controls.

By using AttackIQ to complete end-to-end testing of critical areas for which you assume you have defensive coverage, you will be equipped with objective data in the form

of a report to present to your team to prioritize remediation of gaps. This report can also be shared with management and other business units within your organization to communicate the state of your security posture.

AttackIQ's platform can make this easy for you in regards to selecting key controls to test and ready-to-use reporting for yourpresentation about the effectiveness of current security controls. Your team, your CISO, and your CIO will find this objective measurement invaluable.

"AttackIQ gives your threat intelligence program the objective data you need to respond authoritatively to requests for assessment of risk. Most importantly, you can assess the risk of a past event, such as an insider attack, of being repeated."

Stephan Chenette
CTO and Co-Founder
AttackIQ, Inc.

## Use MITRE ATT&CK and Your Threat Intelligence Program to Uncover Your Exposure

Threat intelligence programs develop from the experience your organization has gained from internal events as well as the data you may acquire externally. Threat intelligence data is dynamic - it is constantly changing based upon your experience. The MITRE ATT&CK knowledge base enables you to turn your tactical experience into a strategic threat intelligence capability.

If your security program is mature and you have implemented a threat intelligence program with a dedicated team within your organization, you can leverage that intelligence within the AttackIQ platform. This can include knowledge of past breaches that your organization has withstood and likely attacks that you expect might occur given external intelligence information.

### Threat Intelligence Programs Can Yield Powerful Results

If the timing is not right for you to deploy a full-scale threat intelligence program, you can still support your basic program with AttackIQ. AttackIQ can help your team integrate data learned from recent events at your organization, such as an insider attack. All of the tactics and techniques of that insider attack can then be modeled within your threat intelligence program by using AttackIQ. This will enable your team to understand the gaps in your defense architecture and how to remediate them; as well as determine if you will be able to prevent the next similar internal attack.

Let's look a bit deeper at the example of an insider data breach. Let us suppose that your threat intelligence program has documented internal breaches where attackers have gained Credential Access by using Credential Dumping. Credential Dumping is the process whereby account authentication data is obtained for software and operating systems.


Within MITRE ATT&CK you will find "Credential Dumping" techniques under the larger pool of "Credential Access" tactics. "Credential Dumping" is very common ; it is used in 80 percent of all post-breach activities on a compromised Windows device.

Once you click on "Credential Dumping" in the MITRE ATT&CK matrix, you'll see the definition:

> **Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.**

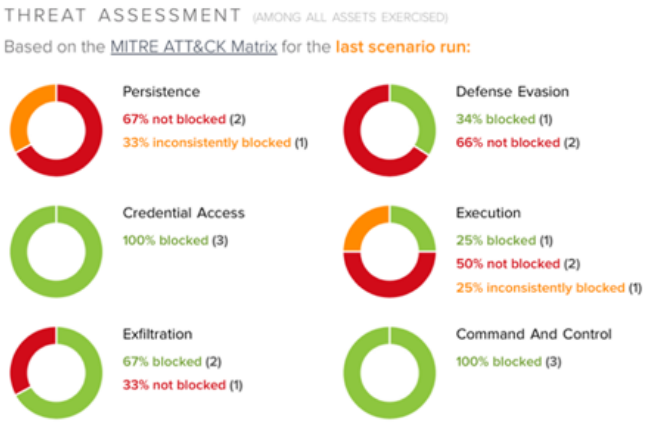
You will also see a listing of several tools and methods that are listed as known to be used by attackers in the wild to accomplish this technique. These include:

### Windows

- SAM (Security Accounts Manager)
- Cached Credentials
- Local Security Authority (LSA) Secrets
- NTDS from Domain Controller
- Group Policy Preference (GPP) Files
- Service Principal Names (SPNs)
- Plaintext Credentials
- DCSync

### Linux

- Proc filesystem




## Scale Threat Intelligence to Meet Any Adversary

The next level in using the MITRE ATT&CK framework is to test the adversarial behaviors learned from your threat intelligence program that you are unsure you can defend against. This may include the tactics and techniques of an advanced persistent threat (APT) group that is known to target your industry. This is a sophisticated and capable threat, usually well-funded and intent on using a portfolio of well-honed techniques to compromise and break your defenses.

In order to gain the ammunition you need to prepare, your threat intelligence program will bring in outside sources of information that may include indicators of compromise (IOCs) that include IP addresses, hashes, and adversarial behavior and patterns. Now you can benefit from the collective wisdom delivered by the threat intelligence program. AttackIQ enables you to automate the running of this adversarial behavior, measure and assess the impact to your defenses, and take steps to minimize or eliminate any gaps going forward.

In sum total, this enables you to observe, orient, decide, and act (OODA Loop) against adversarial behavior in an iterative fashion which will constantly improve your defense performance and significantly increase probability of successful outcomes for your team. All of this is uniquely enabled by AttackIQ and the MITRE ATT&CK knowledge base.

# Measure, Validate, Decide

You will see how your cybersecurity defense stack performs against different attacker behaviors — perhaps from known internal breaches to attacks modeled after the most recent and sophisticated APT attackers. You will learn if your existing cybersecurity stack will detect and prevent it, and if your security operations team will be able to respond to such an attack technique effectively. You will be enabled to objectively test your tactics, techniques, procedures, and personnel.

Gap analysis remains critical. If there are gaps, you can take a data-driven approach to prioritize resources to remediate the gaps in your program, as well as make informed decisions around future security control investments. Then you can dedicate resources to purchase new or optimize existing security techniques and controls in your network. Security teams often find misconfigurations that are easily corrected.

You can also bring deficiencies back to the vendor community to see if there may be features they can add - using objective data from the MITRE ATT&CK tests makes it easy to present this to the vendor.

## Mitre Att&ck Matrix for Enterprise

### ATT&CK Matrix for Enterprise

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control |
|---|---|---|---|---|---|---|---|---|---|---|
| Drive-by Compromise | AppleScript | .bash_profile and .bashrc | Access Token Manipulation | Access Token Manipulation | Account Manipulation | Account Discovery | AppleScript | Audio Capture | Automated Exfiltration | Commonly Used Port |
| Exploit Public-Facing Application | CMSTP | Accessibility Features | Accessibility Features | BITS Jobs | Bash History | Application Window Discovery | Application Deployment Software | Automated Collection | Data Compressed | Communication Through Removable Media |
| Hardware Additions | Command-Line Interface | Account Manipulation | AppCert DLLs | Binary Padding | Brute Force | Browser Bookmark Discovery | Distributed Component Object Model | Clipboard Data | Data Encrypted | Connection Proxy |
| Replication Through Removable Media | Compiled HTML File | AppCert DLLs | AppInit DLLs | Bypass User Account Control | Credential Dumping | File and Directory Discovery | Exploitation of Remote Services | Data Staged | Data Transfer Size Limits | Custom Command and Control Protocol |
| Spearphishing Attachment | Control Panel Items | AppInit DLLs | Application Shimming | CMSTP | Credentials in Files | Network Service Scanning | Logon Scripts | Data from Information Repositories | Exfiltration Over Alternative Protocol | Custom Cryptographic Protocol |
| Spearphishing Link | Dynamic Data Exchange | Application Shimming | Bypass User Account Control | Clear Command History | Credentials in Registry | Network Share Discovery | Pass the Hash | Data from Local System | Exfiltration Over Command and Control Channel | Data Encoding |
| Spearphishing via Service | Execution through API | Authentication Package | DLL Search Order Hijacking | Code Signing | Exploitation for Credential Access | Network Sniffing | Pass the Ticket | Data from Network Shared Drive | Exfiltration Over Other Network Medium | Data Obfuscation |
| Supply Chain Compromise | Execution through Module Load | BITS Jobs | Dylib Hijacking | Compiled HTML File | Forced Authentication | Password Policy Discovery | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Physical Medium | Domain Fronting |
| Trusted Relationship | Exploitation for Client Execution | Bootkit | Exploitation for Privilege Escalation | Component Firmware | Hooking | Peripheral Device Discovery | Remote File Copy | Email Collection | Scheduled Transfer | Fallback Channels |
| Valid Accounts | Graphical User Interface | Browser Extensions | Extra Window Memory Injection | Component Object Model Hijacking | Input Capture | Permission Groups Discovery | Remote Services | Input Capture | | Multi-Stage Channels |
| | InstallUtil | Change Default File Association | File System Permissions Weakness | Control Panel Items | Input Prompt | Process Discovery | Replication Through Removable Media | Man in the Browser | | Multi-hop Proxy |
| | LSASS Driver | Component Firmware | Hooking | DCShadow | Kerberoasting | Query Registry | SSH Hijacking | Screen Capture | | Multiband Communication |
| | Launchctl | Component Object Model Hijacking | Image File Execution Options Injection | DLL Search Order Hijacking | Keychain | Remote System Discovery | Shared Webroot | Video Capture | | Multilayer Encryption |
| | Local Job Scheduling | Create Account | Launch Daemon | DLL Side-Loading | LLMNR/NBT-NS Poisoning | Security Software Discovery | Taint Shared Content | | | Port Knocking |
| | Mshta | DLL Search Order Hijacking | New Service | Deobfuscate/Decode Files or Information | Network Sniffing | System Information Discovery | Third-party Software | | | Remote Access Tools |
| | PowerShell | Dylib Hijacking | Path Interception | Disabling Security Tools | Password Filter DLL | System Network Configuration Discovery | Windows Admin Shares | | | Remote File Copy |
| | Regsvcs/Regasm | External Remote Services | Plist Modification | Exploitation for Defense Evasion | Private Keys | System Network Connections Discovery | Windows Remote Management | | | Standard Application Layer Protocol |
| | Regsvr32 | File System Permissions Weakness | Port Monitors | Extra Window Memory Injection | Securityd Memory | System Owner/User Discovery | | | | Standard Cryptographic Protocol |
| | Rundll32 | Hidden Files and Directories | Process Injection | File Deletion | Two-Factor Authentication Interception | System Service Discovery | | | | Standard Non-Application Layer Protocol |
| | Scheduled Task | Hooking | SID-History Injection | File Permissions Modification | | System Time Discovery | | | | Uncommonly Used Port |
| | Scripting | Hypervisor | Scheduled Task | File System Logical Offsets | | | | | | Web Service |
| | Service Execution | Image File Execution Options Injection | Service Registry Permissions Weakness | Gatekeeper Bypass | | | | | | |
| | Signed Binary Proxy Execution | Kernel Modules and Extensions | Setuid and Setgid | HISTCONTROL | | | | | | |
| | Signed Script Proxy Execution | LC_LOAD_DYLIB Addition | Startup Items | Hidden Files and Directories | | | | | | |
| | Source | LSASS Driver | Sudo Caching | Hidden Users | | | | | | |
| | Space after Filename | Launch Agent | Sudo | Hidden Window | | | | | | |
| | Third-party Software | Launch Daemon | Valid Accounts | Image File Execution Options Injection | | | | | | |
| | Trap | Launchctl | Web Shell | Indicator Blocking | | | | | | |
| | Trusted Developer Utilities | Local Job Scheduling | | Indicator Removal from Tools | | | | | | |
| | User Execution | Login Item | | Indicator Removal on Host | | | | | | |
| | Windows Management Instrumentation | Logon Scripts | | Indirect Command Execution | | | | | | |
| | Windows Remote Management | Modify Existing Service | | Install Root Certificate | | | | | | |
| | XSL Script Processing | Netsh Helper DLL | | InstallUtil | | | | | | |
| | | New Service | | LC_MAIN Hijacking | | | | | | |
| | | Office Application Startup | | Launchctl | | | | | | |
| | | Path Interception | | Masquerading | | | | | | |
| | | Plist Modification | | Modify Registry | | | | | | |
| | | Port Knocking | | Mshta | | | | | | |
| | | Port Monitors | | NTFS File Attributes | | | | | | |
| | | Rc.common | | Network Share Connection Removal | | | | | | |
| | | Re-opened Applications | | Obfuscated Files or Information | | | | | | |
| | | Redundant Access | | Plist Modification | | | | | | |
| | | Registry Run Keys / Startup Folder | | Port Knocking | | | | | | |
| | | SIP and Trust Provider Hijacking | | Process Doppelgänging | | | | | | |
| | | Scheduled Task | | Process Hollowing | | | | | | |
| | | Screensaver | | Process Injection | | | | | | |
| | | Security Support Provider | | Redundant Access | | | | | | |
| | | Service Registry Permissions Weakness | | Regsvcs/Regasm | | | | | | |
| | | Setuid and Setgid | | Regsvr32 | | | | | | |
| | | Shortcut Modification | | Rootkit | | | | | | |
| | | Startup Items | | Rundll32 | | | | | | |
| | | System Firmware | | SIP and Trust Provider Hijacking | | | | | | |
| | | Time Providers | | Scripting | | | | | | |
| | | Trap | | Signed Binary Proxy Execution | | | | | | |
| | | Valid Accounts | | Signed Script Proxy Execution | | | | | | |
| | | Web Shell | | Software Packing | | | | | | |
| | | Windows Management Instrumentation Event Subscription | | Space after Filename | | | | | | |
| | | Winlogon Helper DLL | | Template Injection | | | | | | |
| | | | | Timestomp | | | | | | |
| | | | | Trusted Developer Utilities | | | | | | |
| | | | | Valid Accounts | | | | | | |
| | | | | Web Service | | | | | | |
| | | | | XSL Script Processing | | | | | | |

Gartner

"Security and risk management leaders who are charged with showing that their security programs are effective and good uses of corporate funds should consider using security validation services such as those offered by AttackIQ."

Gartner Cool Vendors
Monitoring and Management of Threats to Applications and Data
Gartner Group
2017

## Summary

MITRE ATT&CK was created to help bring structure and organization to the understanding of adversarial behavior. It is a knowledge base of actual cyber attack tactics, techniques, and procedures.

Your security program should be proactively running scenarios to test the effectiveness of your capabilities on an automated and continuous cycle. You can start testing your basic AV to prevent commodity malware and test your Network Firewall to see how your perimeter is being protected. You can also implement and test network segmentation to see if that is performing correctly. Keep it simple!

If your security program is more mature and utilizes hundreds of security technologies and processes, dozens of security teams, and a threat intelligence program, you can test against your known security stack and against potential adversarial behavior. This will give you a more comprehensive view of the effectiveness of your current capabilities and help you prioritize remediation efforts and investments in new controls.

Select the most critical security products you currently have in place to test. Then move on to the next step: testing the most likely attacker behavior in your network. As you go beyond these steps, continue to layer in more products and more testing techniques. Each step will enable you to present an incredibly useful data-driven objective output to your organization.

ATTACKIQ

### About AttackIQ

AttackIQ, a leader in the emerging market of continuous security validation, built the industry's first platform that enables red and blue teams to test and measure the effectiveness of their security controls and staff. An open platform, AttackIQ™ supports the MITRE ATT&CK Matrix, a curated knowledge base and model for cyber adversary behavior used for planning security improvements and verifying defenses work as expected. AttackIQ's platform is trusted by leading companies around the world. For more information visit www.attackiq.com. Follow AttackIQ on Twitter, Facebook, LinkedIn, and YouTube.