ManageEngine
AD360

# MITRE ATT&CK tactics and techniques for a SECURE Active Directory

www.manageengine.com/active-directory-360/

# Introduction

Active Directory (AD) forms the crux of any business' security orchestration, especially for identity and access management (IAM). This, coupled with the expansive attack surface that AD offers, makes it the primary target for attackers seeking access to a network or sensitive data.

In the present climate where cyberattacks are at an all-time high, all organizations must allocate resources to identify threats or monitor their networks continuously. Unless efforts are taken to identify security vulnerabilities, fortify network security, and draft threat-informed defense strategies, organizations will be caught unprepared in the face of a cyberattack.

*An unprepared organization will be a victim of cyberattack. It is not a question of **if,** but **when** and **how bad.***

As threat actors come up with new strategies, the studies on cyberattack tactics and attack pathways have been growing simultaneously. The silver lining is that businesses, irrespective of their size and capability, now have access to numerous open-source resources like the MITRE ATT&CK framework that can aid them in making the necessary security decisions.

# Objective

This e-book attempts to provide awareness about the cybersecurity challenges that concern AD. IT admins often struggle with choosing the best course of action in the face of an unexpected cyberattack. Being aware of the common attack pathways and techniques used by threat actors can help them be better prepared for an eventual cyberattack by recognizing the signs of an attack and the subsequent tactics that will be deployed in the attack chain, securing any vulnerability that can be leveraged by the attackers, and so on. This can also be handy in formulating mitigation measures to prevent future cybersecurity attacks.

# The MITRE ATT&CK framework

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) is an open framework developed by MITRE, a not-for-profit organization. It is the go-to resource for IT security teams as an aid to detect threats, plan penetration testing scenarios, identify cyberdefense gaps, and improve their security intelligence and awareness.

This framework takes the form of a matrix built to mimic the real-world cybersecurity environment, and helps organizations navigate the cyberthreat landscape. It has been drafted to answer questions about the nature of an attack, identify the next possible moves of the attacker, determine the targeted security gaps, and more.

# What is the ATT&CK matrix?

The MITRE ATT&CK matrix encompasses all information about its various observations about attacker behavior and methods of attacks into the following components:

✓ Tactics: These are the immediate goals of attackers, such as reconnaissance to identify weak spots in the perimeter, initial access tactics to break into the network, and exfiltration to steal the data. Attackers commonly use multiple tactics to achieve their goals.

✓ Techniques: These are the methods used by attackers to achieve their tactical goals. The matrix is built in such a way that each tactic has multiple techniques listed for it.
Additionally, MITRE offers mitigation measures for the various cyberattack tactics and techniques in the matrix.

Additionally, MITRE offers mitigation measures for the various cyberattack tactics and techniques in the matrix.

The matrix has been drafted in a way that caters to diverse technologies and platforms, including:

✓ **Enterprise IT systems:** Windows, macOS, Linux, PRE, Azure AD, Microsoft 365, Google Workspace, SaaS, IaaS, networks, and containers.

✓ **Mobile devices:** Android and iOS.

# Why should you leverage the MITRE ATT&CK framework?

This section sheds light on the various challenges in IAM and why businesses should consider transitioning from traditional approaches to IAM security.

Here are a few cybersecurity challenges that can be solved by leveraging the MITRE ATT&CK framework.

1

### Identifying security gaps before the attackers do

The biggest challenge that IT admins face in AD security is identifying the existing security gaps that can be exploited by attackers. This is usually done through red team vs. blue team exercises as a way of proactively testing and enhancing the organization's security.

2

### The constantly changing cybersecurity threat landscape

Unless one works in the cybersecurity sector, it is a daunting task to keep track of all the threats and security vulnerabilities that are discovered every day. This leads to business owners struggling to keep up with cybersecurity trends and their impact on businesses.

3

### A lack of post-compromise protocols

The key to establishing countermeasures to threats is to have a good understanding of those threats. Having a comprehensive idea of the attack chain and identifying the next possible move is important for security teams to implement measures to contain the threat and ensure minimal to no damage or loss of data.

4

### The absence of a tried-and-tested mitigation plan

One of the most effective ways of fighting a cybersecurity attack is having mitigation measures in place. The lack of an incident response plan can make it difficult for organizations to function if a security breach occurs, and can bring business functions to a standstill.

# MITRE ATT&CK tactics you should know about to secure AD

A cybersecurity attack typically follows these steps: reconnaissance to identify security vulnerabilities, deploying an attack tactic to enter the target network and navigate to gain access to the data, and then exfiltration of sensitive data or gaining control of the network.

This section presents a comprehensive outlook of the important tactics and techniques essential for AD security.

## Reconnaissance

This is the first tactic deployed in most attack chains. Attackers use this tactic to gather intel that can help them find a breach in their target's network. A common example of this tactic being used in attacks on AD is LDAP reconnaissance, where the attackers try to map the target network, identify user accounts that can be exploited, and more.

Common techniques used in this tactic:

| ID | Technique | Description |
|---|---|---|
| T1590 | Gather Victim Network Information | Gathering information about the target's network, like domain name and IP ranges. |
| T1589 | Gather Victim Identity Information | Gathering identity information on the target, like employee names and email addresses, that can be used to identify their credentials. |
| T1591 | Gather Victim Org Information | Gathering information about the target organization, including the departments, roles assigned, and employee responsibilities, to identify the access levels. |

### Recommended mitigation measures:

- ✓ Organizations should limit the number of privileged accounts in their AD environment since threat actors gaining access to such accounts can put the entire network at risk.

- ✓ Administrators should clean up their AD environment by removing all stale accounts periodically. Stale accounts are significant threats because ex-employees or hackers can use the existing accounts to traverse through your AD domain.

## Initial access

With this tactic, the attacker tries to make use of the information obtained during reconnaissance to gain entry into the network. Attackers use various techniques to attempt to access accounts, like domain accounts or user accounts, in AD. Once they gain a foothold in the network, they often proceed to use the account credentials to gain control over other accounts, escalate the privileges of an account, and more.

Common techniques used in this tactic:

| ID | Technique | Description |
|---|---|---|
| T1190 | Exploit Public-Facing Application | Attempting to exploit vulnerabilities or bugs in an internet-facing machine or program via software or commands. |
| T1566 | Phishing | Using phishing to target the victim. |
| T1078 | Valid Accounts | Attempting to use the credentials of existing or compromised accounts to gain entry into the network. |

### Recommended mitigation measures:

- ✓ Patch and update all externally exposed applications.
- ✓ Enable MFA for all users to ensure no accounts will be compromised even if threat actors get access to users' passwords.
- ✓ Enable a stringent AD password policy and SSO for all enterprise applications to eliminate password fatigue.
- ✓ Monitor access and permissions regularly, and revoke excess access permissions in alignment with the principle of least privilege.

## Privilege escalation

The next tactic in the attack chain is usually privilege escalation. As the name suggests, attackers try to escalate their existing privileges, try to obtain higher privileges and access permissions by impersonating a user, and so on. This tactic is often aimed at achieving the penultimate goal of gaining access to an admin account, which will be used to achieve the attackers' malicious intents.

Common techniques used in this tactic:

| ID | Technique | Description |
|---|---|---|
| T1548 | Abuse Elevation Control Mechanism | Taking advantage of the built-in access control processes or mechanisms to elevate existing privileges. |
| T1037 | Boot or Logon Initialization Scripts | Using scripts that are automatically executed at startup to execute malicious administrative functions. |
| T1484 | Domain Policy Modification | Modifying the domain settings of the target AD environment to escalate privileges of user or computer accounts, GPOs or federation trusts, etc. |
| T1053 | Scheduled Task/Job | Utilizing scheduled programs or scripts to execute malicious code |
| T1078 | Valid Accounts | Attempting to use the credentials of existing or compromised accounts to gain entry into the network. |

### Recommended mitigation measures:

- ✓ Restrict access to write or modify the logon scripts or registry hives.
- ✓ Remove non-admin users from local administrator groups and other privileged groups.
- ✓ Establish an approval-based workflow for the execution of critical tasks like provisioning of privileged user accounts, providing access to critical applications, password resets, and enabling disabled privileged accounts.
- ✓ Audit all changes made to privileged accounts and security group memberships regularly.

## Lateral movement

Lateral movement is a tactic used by attackers to leverage their stolen credentials or access to navigate inside a network. This is often used in combination with other tactics like privilege escalation and is aimed at exploiting other privileged accounts, installing remote access tools in AD, and more. This can happen at the application level by using techniques to leverage the stolen user credentials, or the attackers may move from one machine to the next to access the domain controller.

Common techniques used in this tactic:

| ID | Technique | Description |
|---|---|---|
| T1210 | Exploitation of Remote Services | Using remote services to gain unauthorized access to a target's network. |
| T1563 | Remote Service Session Hijacking | Accessing a preexisting remote session to navigate the target's network. |
| T1550 | Use Alternate Authentication Material | Using alternate authentication materials, such as Kerberos tickets or application access tokens, to bypass the access controls in place. |

### Recommended mitigation measures:

- ✓ Enforce just-in-time access controls for critical services or applications. Provide access only to those who need it and only until the task is complete.
- ✓ Revoke remote access permissions to user accounts unless it's absolutely necessary.
- ✓ Enforce the principle of least privilege and Zero Trust.
- ✓ Monitor requests for new ticket-granting tickets or service tickets to a domain controller using alternate authentication methods like password hashes or Kerberos tickets, which can be used to bypass access controls for lateral movement in a network.

## Exfiltration

Exfiltration is the attack tactic used to siphon data out of the target network. This tactic involves techniques to compress, encrypt, or disguise the stolen data to avoid detection. In AD, this could be attackers using an exploited user account to copy data to a personal device, limiting the size of the data being transferred to avoid detection, and so on. Common techniques used in this tactic:

| ID | Technique | Description |
|---|---|---|
| T1052 | Exfiltration Over Physical Medium | Utilizing external devices like removable drives, MP3 players, or mobile phones to steal target data. |
| T1029 | Scheduled Transfer | Utilizing scheduling practices to exfiltrate data to avoid any spike in the traffic during non-busy hours. |
| T1537 | Transfer Data to Cloud Account | Backing up or transferring data to cloud environments or accounts to avoid detection by conventional transfer methods. |
| T1020 | Automated Exfiltration | Using automated processing mechanisms like automated report generation to exfiltrate data. |

### Recommended mitigation measures:

- ✓ Automate the process of monitoring abnormal access to files, network traffic, and commands executed for anomalies.
- ✓ Enforce data loss prevention practices, and limit the use of removable storage devices.
- ✓ Enforce limited or time-bound access as and when required instead of providing blanket access to all users.

# Improve AD security by choosing the right IAM tool to implement the MITRE ATT&CK framework

Unless the MITRE ATT&CK framework is used in tandem with robust IAM tools, it remains just another knowledge resource. Here are a few important capabilities you need to look for when choosing the right IAM tool for your enterprise:

### A good fit for your IT environment:

All businesses are unique, and so are their IT environments. Explore the target vulnerabilities, security risks associated with the nature of the enterprise, and the existing cybersecurity capabilities to choose an IAM tool that is a seamless fit for your security needs.

### Robustness:

The MITRE ATT&CK framework has been continuously updated ever since its introduction in 2013. Integrating the MITRE ATT&CK framework into your organization's security requires an IAM tool robust enough to stay on pace with the evolution of the cybersecurity landscape.

### Scalability:

As an organization grows, its security perimeter and attack surface also keep expanding. Unless the IAM solution is scalable and can be integrated with other IT solutions used in your organization, it will remain in a silo or become yet another security vulnerability.

### Resource efficiency:

The best way to go about incorporating the MITRE ATT&CK framework and its mitigation measures into your security framework is to operationalize and automate the identification and monitoring of threats. While this feels complex, there are many tools available on the market that can be implemented by anyone, even those without any scripting expertise.

# AD360: The right IAM tool to secure your AD environment

With AD360 by your side, you can protect against the many techniques used by threat actors and fortify your AD defense.

### 1. Automated AD cleanup:

Automate the process of clearing up all inactive user accounts to eliminate the possibility of those accounts being taken over by threat actors.

### 2. Comprehensive MFA:

Secure Windows, Linux, and macOS desktop logins; remote desktop connections; VPNs; and OWA with MFA. Choose from 20 different authentication methods as your secondary factor.

### 3. Enterprise SSO:

AD360 supports SSO configuration for over 120 applications out of the box. You can also configure SSO for your custom SAML-enabled enterprise applications to reduce password fatigue for users.

### 4. Approval-based workflows:

Build custom workflows that require approval from reviewers and approvers before the changes take effect. Eliminate the possibility of threat actors providing elevated privileges to their own accounts.

### 5. Comprehensive auditing:

Audit all changes made to your AD environment, including users, groups, and GPOs. Get reports delivered right to your inbox to identify any unintended changes before they become an issue.

### 6. User behavior analytics (UBA):

Create a baseline behavior for all users, and be notified whenever abnormalities are detected in users' behavior.

# About ManageEngine AD360

AD360 is a unified identity and access management solution that helps manage identities, secure access, and ensure compliance. It comes with powerful capabilities like automated identity life cycle management, secure SSO, adaptive MFA, approval-based workflows, UBA-driven identity threat protection, and historical audit reports for AD, Exchange Server, and Microsoft 365. AD360's intuitive interface and powerful capabilities make it the ideal solution for all your IAM needs, including fostering a Zero Trust environment.

$ Get Quote

Download