

Simulating the Latest Threats and Techniques with the MITRE ATT&CK Matrix



Table of content

01	Why should I simulate an APT attack?	03
02	Where do I start?	04
03	Start Testing Test Your SOC Capabilities Test Your Security Controls Test Across the Kill Chain Test Across the MITRE ATT&CK Framework Test in Depth	05
04	Dynamic Simulation Simulate Attacks Dynamically Simulate Attacks by Specific APT Groups Simulate Attacks Using the Latest Threat Intelligence Create Your Own Templates Simulate Whenever	07
05	Always Have Critical Insight	07

01 Why Should I Simulate an APT attack?

The most important reason to simulate APTs is to answer one big question:
“How would an APT attack affect our organization?”

...and many other questions:

- Will your defenses work as expected?
- Are you protected across the kill chain?
- Can you defend against experienced, global threat actors?
- Do your controls recognize the latest TTPs?



02 Where Do I Start?

01 | First, decide what you want to test.

How do our **Blue Team** security analyses, policies, and workflows perform?

Can a **Red Team** attack breach specific security vectors, such as email, endpoints, or web applications?

Do specific security controls—such as a WAF, behavior analytics platform, or email security solution—work as we expect?

02 | Use a proven framework as a guide for performing APT simulations across the kill chain.



The MITRE ATT&CK framework is the world's most authoritative and comprehensive knowledge base of current attack techniques and supporting tactics.

Based on real-world data, MITRE ATT&CK is used as a foundation for developing specific threat models and methodologies.

When used with simulation, MITRE ATT&CK enables you to objectively evaluate and measure the performance, risk, and capabilities of your cybersecurity controls.

03 | Choose your tools.

Different types of tools can be used to simulate APT attacks. Here are common examples.

Manual Open Source Tools: such as Endgame Red Team Automation, Mitre Caldera, Red Canary Atomic Red Team, Uber Metta

Pros	Cons
<ul style="list-style-type: none"> • Lightweight, highly portable • Generates platform-specific attacks • Free 	<ul style="list-style-type: none"> • Requires advanced technical skills • Requires modifications and scripting to test multiple attack techniques at a time • Lacks remediation suggestions

Online Services: such as ANY.RUN, Hybrid Analysis, VirusTotal

Pros	Cons
<ul style="list-style-type: none"> • Convenient, easy to use • Safe for analyzing threats • ANY.RUN and Hybrid Analysis tagged to the MITRE ATT&CK framework • Can customize and filter latest threats submitted using geography and date 	<ul style="list-style-type: none"> • Not simulation tools • Can only be used to review and analyze threats • Require additional expertise to correctly interpret impact on your specific environment

Breach and Attack Simulation (BAS): such as Cymulate Continuous Security Validation

Pros	Cons
<ul style="list-style-type: none"> • Simple to use • Automated for consistency and repeatability • Safe for analyzing threats in production environment • Tagged to the MITRE ATT&CK framework • Covers entire kill chain and latest attacker TTPs • Delivers in-depth visibility and actionable guidance 	<ul style="list-style-type: none"> • Optimized for companies with mature security program

Test Across the MITRE ATT&CK Framework

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppScript	msi_uninstall and install	Access Token Manipulation	Account Manipulation	Account Manipulation	Account Discovery	AppScript	Audio Capture	Commonly Used Port	Automated Lateralization	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Auth History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Networked Media	Data Compressed	Data Destruction
Enterprise Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Patching	Brute Force	Storage Enumeration	Application Deployment Software	Clipboard Data	Connective Proxy	Data Encrypted	Data Compromised for Impact
Hardware Addition	Compiled HTML File	AppCert DLLs	AppCert DLLs	BTFS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Deployment
Application Through Remoteable Media	Component Object Model and Distributed COM	AppCert DLLs	Application Shopping	Browser User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	File Content Wipe
Spamming Attachment	Control Panel Items	Application Shopping	Registry User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearfishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	File Structure Wipe
Spamming Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Content in Files	File and Directory Discovery	Logon Scripts	Data from Network Storage Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spamming Web Service	Execution through API	BTFS Jobs	Data Hijacking	Code Signing	Content in Registry	Network Service Scanning	Pass the Hash	Data from Remoteable Media	Domain Flooding	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Brute Force	Content Creation with Prompt	Complete After Delivery	Operation for Credential Access	Network Share Discovery	Pass the Ticket	Safe Storage	Domain Enumeration Algorithms	Exfiltration Over Physical Medium	Host System Recovery
Vendor Backdoor	Exploitation for Client Execution	Browser Extensions	Emulate	Component Firmware	Formal Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Facebook Checkins	Transfer Data to Cloud Account	Network Denial of Service
WMI Accounts	Organizational User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Multi-Step Proxy	Resource Hijacking
	Installable	Component Firmware	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Hooking	Peripheral Device Discovery	Man in the Browser	Multi-Step Proxy	Multi-Stage Channels	Runtime Data Manipulation
	Local Job Scheduling	Credentials Account	Hooking	Control Panel Items	Input Prompt	Permission Groups Discovery	Removable Media	Screen Capture	Multi-Step Proxy	Multi-Stage Channels	Service Stop
	LSASS Driver	DLL Search Order Hijacking	Image File Execution	Process Injection	Registry	Registry	Shared Network	Video Capture	Multi-Step Proxy	Multi-Stage Channels	System Shutdown/Restart

MITRE ATT&CK provides current attack tactics and specific techniques organized across the kill chain in a range of vectors.

You can drill down to extensive underlying detail to help focus your simulations.

Test in Depth

Tailor your simulations to test specific functionality, and use pinpointed techniques to identify weaknesses.

For example, use simulation to evaluate:

- Your EDR's ability to detect fileless attacks
- EUBA success in identifying insiders' attempts at data exfiltration
- How well network segmentation prevents lateral movement

ATT&CK

You can choose 5 techniques

Template Name: **Test**

APT Template Focus: **Initial Access Focused**

Delivery Method (Pre-Exploitation): **Email Attachment**

Payload Structure: **xlm**

EXECUTION (5/5)

- XSL Script Processing
- Service Execution
- Regsvcs/Regasm
- Dynamic Data Exchange
- Data Compressed
- Windows Remote Management
- Scheduled Task
- Trusted Developer Utilities
- Signed Script Proxy Execution
- Rundll32
- Msihta
- Installutil
- Compiled HTML File
- CMSTP
- Command Line Interface
- Powershell
- Regsvr32

PERFORMANCE (9/10)

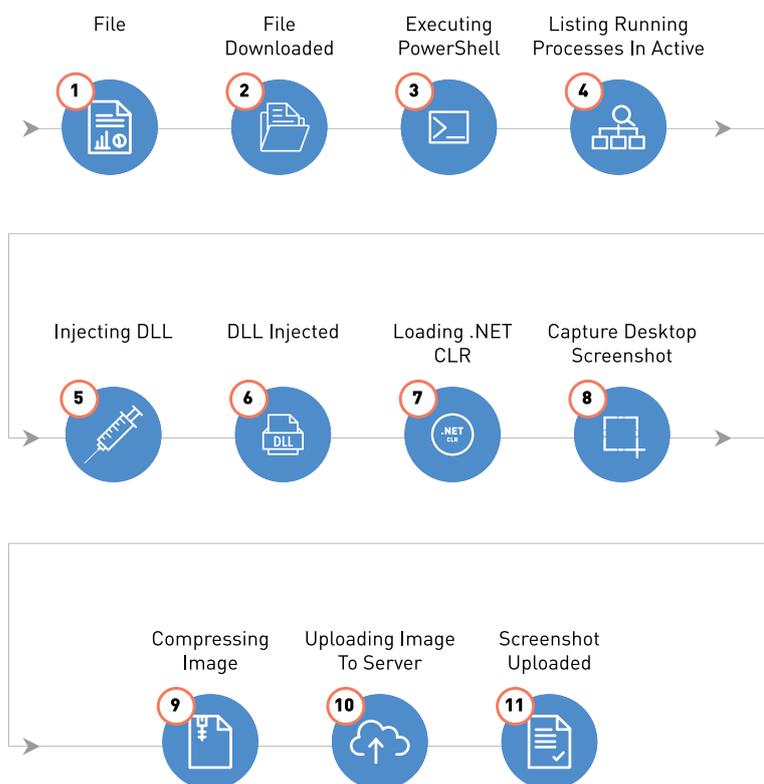
BACK NEXT

04 Dynamic Simulation

Simulate Attacks Dynamically

Using BAS, you can simulate APTs safely in your own environments with world-class attacker knowledge.

- Simulate across the full kill chain with techniques mapped to MITRE ATT&CK™ building blocks
- Run simulations with a logical flow of commands from one technique to the next—just as an attacker would do
- Watch the full attack story unfold—right in the dashboard



Simulate Attacks by Specific APT Groups

Simulate the actual operations of recognized APT groups, such as:

- Reaver
- Lazarus Group
- APT38
- Patchwork
- FIN8
- OceanLotus
- Cobalt Group
- OilRig
- and others...

Simulate Attacks Using the Latest Threat Intelligence

Using BAS, the latest threat intelligence is always available. Simulate the newest threats as they merge to ensure that your defenses are ready.

Create Your Own Templates

Create your own MITRE-based simulation templates.

Simulate Whenever

Schedule simulations, run them continuously, or when desired:

- Daily
- Weekly
- Monthly
- Right now

Always Have Critical Insight

Always know the state of your security controls with Cymulate BAS, whether it's right now or at any point in the future. By teaming with a proven framework—MITRE ATT&CK—and the latest threat intelligence, Cymulate BAS equips you to face the threat landscape with insight and readiness.

Ready to Cymulate? Get started with a [free trial](#)