



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




## Table of Contents

<b>02</b>   Why Should I Simulate an APT attack? .....	<b>3</b>
<b>03</b>   Where Do I Start? .....	<b>4</b>
<b>04</b>   Start Testing .....	<b>5</b>
<b>05</b>   Dynamic Simulation .....	<b>7</b>


# 01 | Why Should I Simulate an APT attack?

The most important reason to simulate an APT attack is to answer the question




**How would an APT attack affect our organization?**


And many other questions




Are we protected across the kill chain?



Can we defend against experienced, global threat actors?




Will our defenses work as expected?



Do our controls detect the latest TTPs?

## How it works

Cymulate facilitates managing your security posture 24X7X365 within minutes and based on facts, in just three simple steps:



**1 Simulate**  
Simulate attacks across any vector.

Email Gateway

**51** /100 ▼-3

[Full Report](#) [History](#)

**2 Evaluate**  
Know where your company is exposed.

**62%** Report Summary

[Generated Report](#) [History](#) [Policy](#)

**3 Remediate**  
Fix your security gaps.

## 02 | Where Do I Start?

### First, decide what you want to test.

How do our **Blue Team** security analysis, 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 expected?

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

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

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

### Use a framework for performing APT simulations across the kill chain.

## MITRE | ATT&CK

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.

### Breach and Attack Simulation (BAS):

such as Cymulate Continuous Security Validation

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

# 03 | Start Testing

## Test Your SOC Capabilities

Operationalize the ATT&CK framework and launch attacks across the full cyber kill chain to learn if your SOC team can detect an APT and respond quickly. You can test SOC response without your SOC team being aware of the simulation or with full awareness.

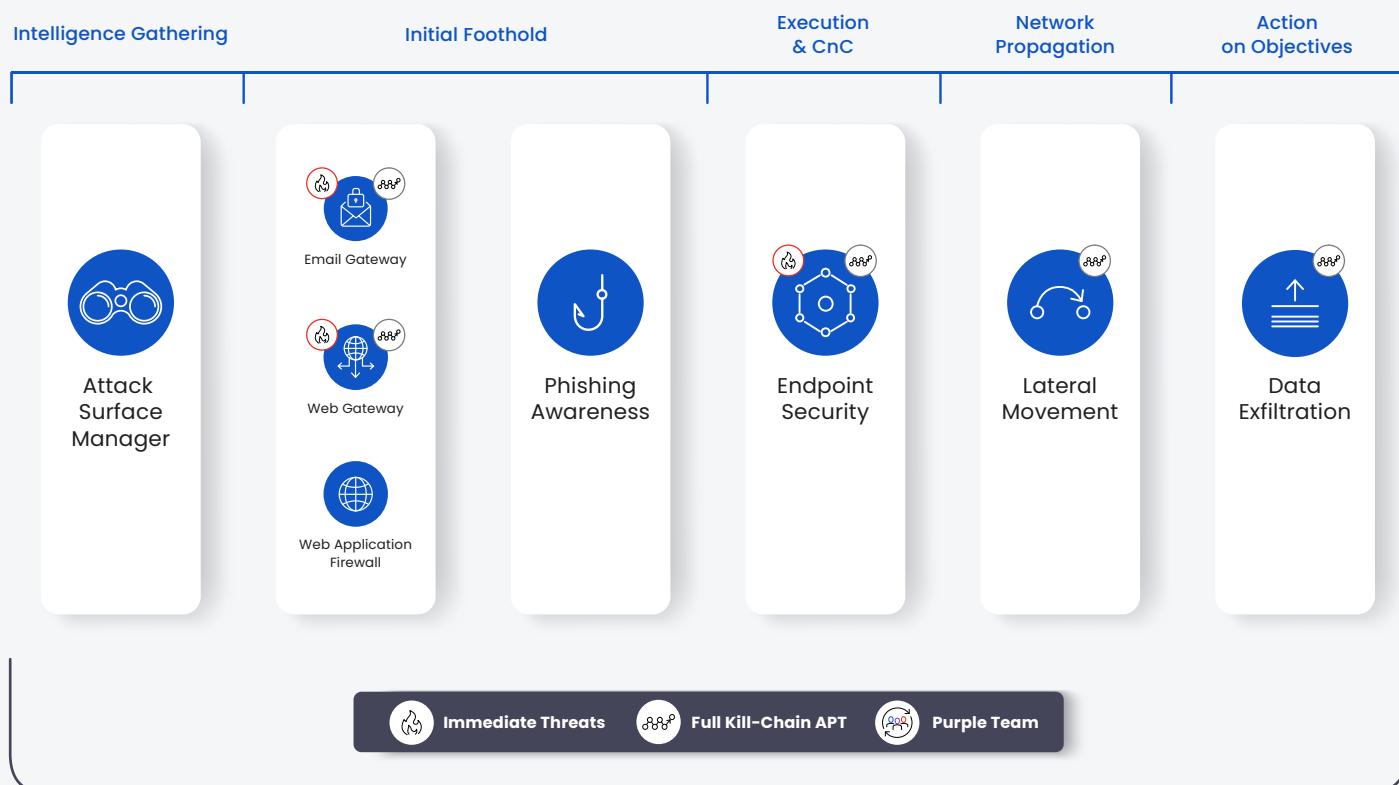
Can your blue team successfully detect techniques such as attempts to encrypt files, exfiltrate data, or move laterally?  
How do they respond to the attempt?

## Test Your Security Controls

Use simulation to:

- Model sophisticated multi-step, multi-vector attacks
- Evaluate monitoring and incident response capabilities
- Detect unknown issues at unknown locations

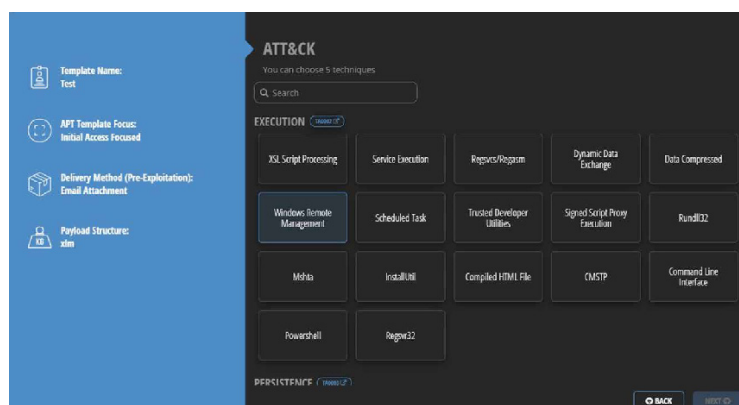
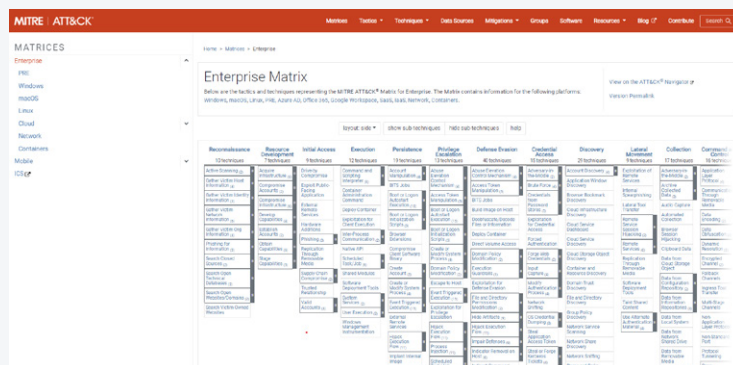
## Test Across the Full Kill Chain



## Test Across the MITRE ATT&CK Framework

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:

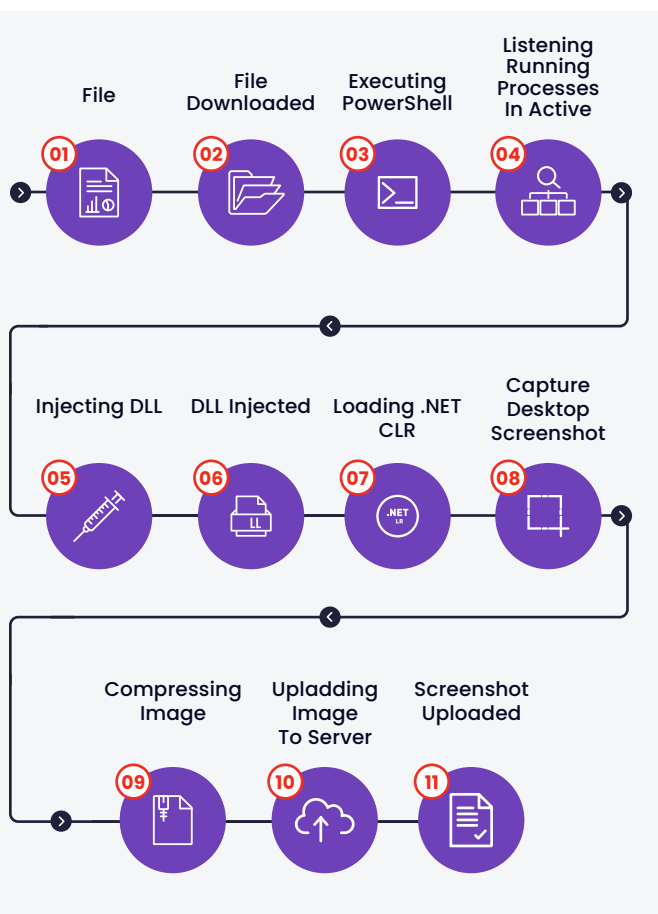
- Your EDR's ability to detect fileless attacks
- EUBA success in identifying insiders' attempts at data exfiltration
- How well network segmentation prevents lateral movement

# 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 emerge 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 XSPM, 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.

## About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company—and every company—will be.

Contact us for a live demo, or get started with a free trial

[Start Your Free Trial](#)