MITRE | ATT&CK

Cymulate

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

Cymulate

Table of content

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?

Cymulate

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.

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.

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
• Lightweight, highly portable • Generates platform-specific attacks • Free	• 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
• 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	• Not simulation tools • Can only be used to re view 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
• 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	• Optimized for companies with mature security program

03 Start Testing

Cymulate

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?

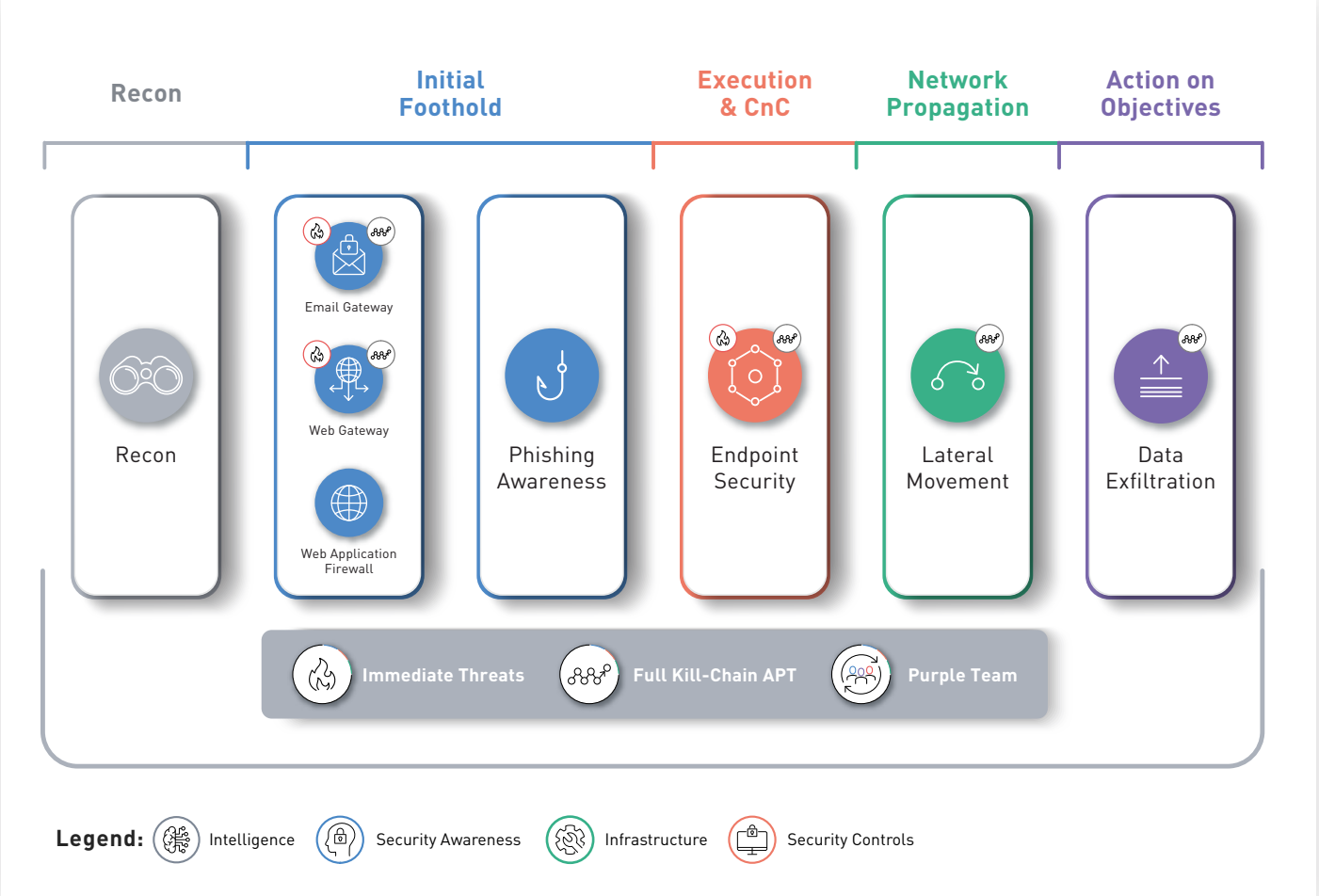
How do they respond to the attempt?

Test Your Security Controls

Use simulation to:

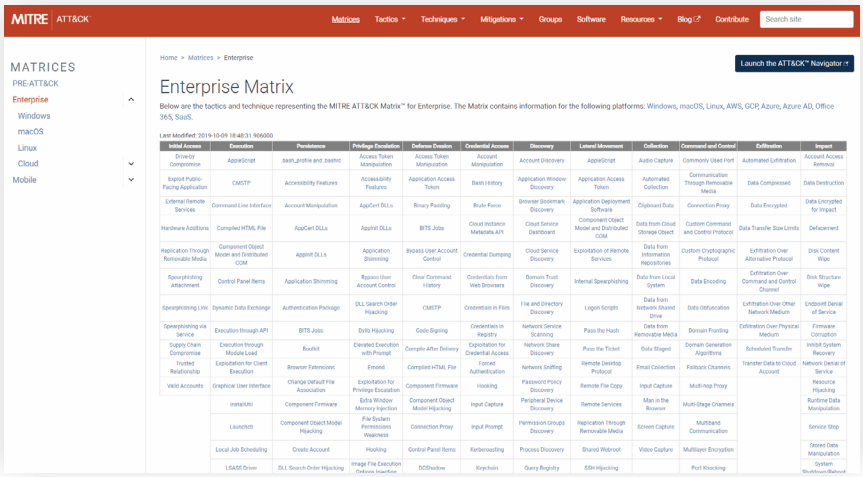
- Model sophisticated multi-step, multi-vector attacks
- Evaluate monitoring and incident response capabilities
- Detect unknown issues at unknown locations

Test Across the Kill Chain



03 Start Testing

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.

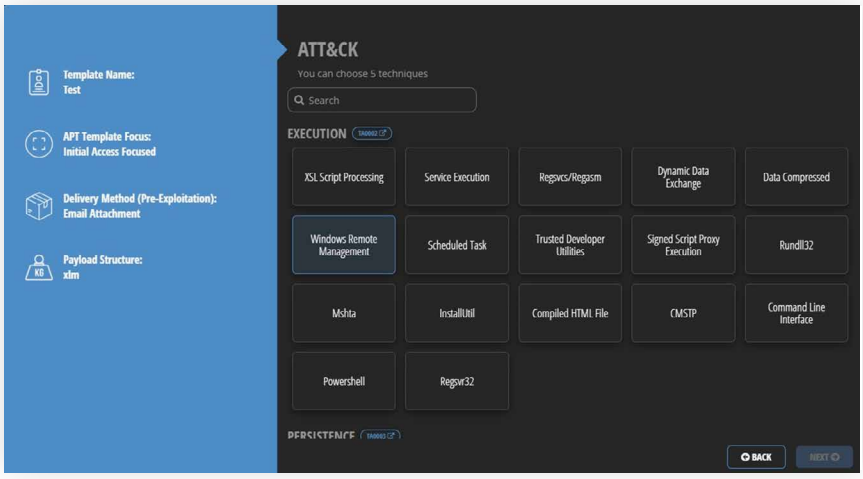
You can drill down to extensive underlying detail to help focus your simulations.

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



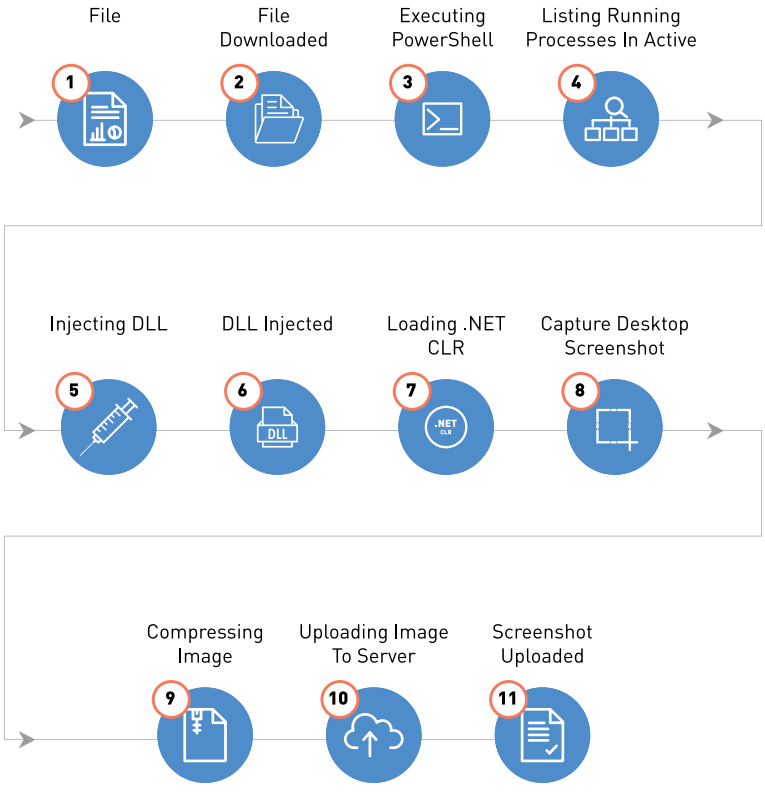
04 Dynamic Simulation

Cymulate

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

Headquarters: 2 Nim Blvd., Rishon LeZion, 7546302, Israel | +972 3 9030732 | info@cymulate.com
US Office: 31W 34th Street, 8th floor, New York, New York, 10001 | +1 212 6522632