Cymulate

APT-Ready in Four Steps: Your Action Plan

How to Establish a Continuous, Repeatable System to Defend SMB and Enterprise Networks

Table of Contents

01 Introduction

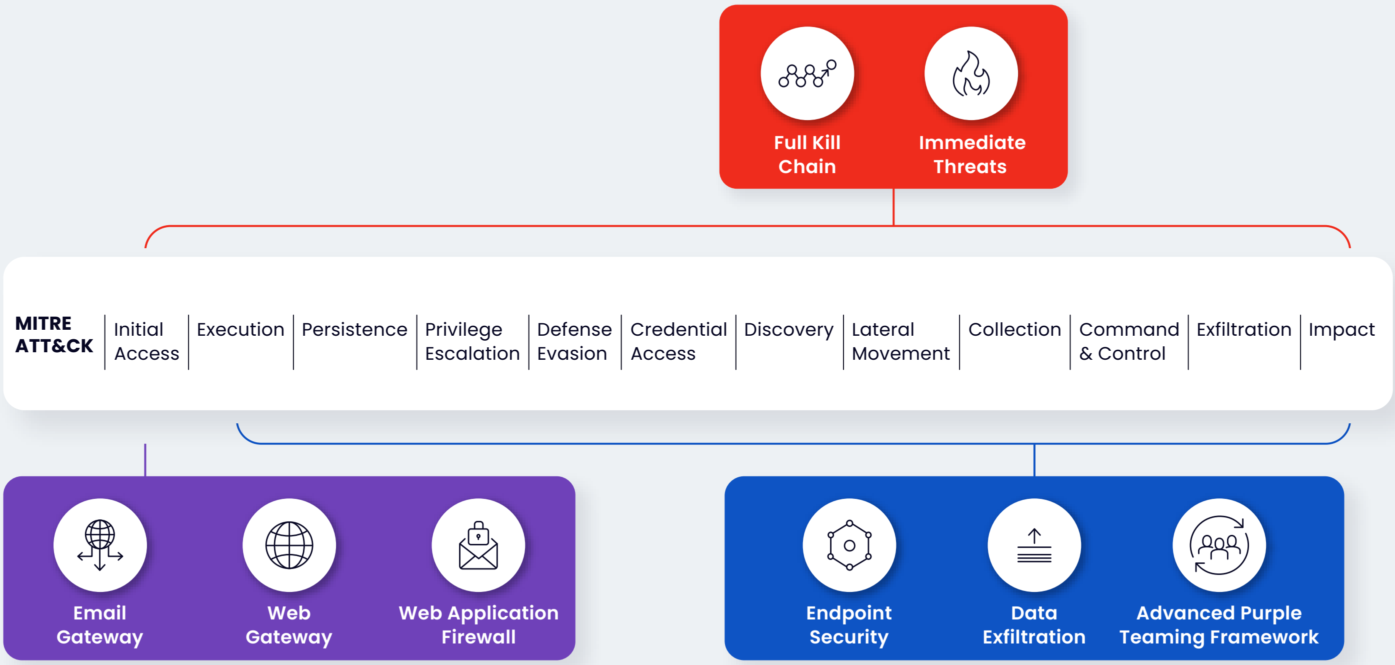
The term "Advanced Persistent Threat" (APT) strikes fear into any security professional's heart. An APT is a cyberattack executed by criminal groups or nation-states intending to steal data, perform high-value financial fraud or monitor the target organization's systems over an extended period of time. APT perpetrators have specific goals, and they spend extensive time and resources to identify vulnerabilities and design attacks that will escape detection for as long as possible. Attacks are "advanced" because they're specifically tailored for the target organization and carried out in phases over multiple attack vectors.

Unlike opportunistic threat actors, APT attackers are patient—willing to wait weeks or even months to find a security gap that enables them to move laterally in the network toward strategic servers and databases. Ultimately, they're looking for sensitive personal, payment, or protected health information; intellectual property and trade secrets to steal or monetize; executive, strategic and financial information for competitive advantage; or national military or infrastructure information for political advantage.

Large enterprises used to be the primary targets of APT attacks. Today however, APT groups also target small and medium-sized business, because they often have fewer security resources. This document discusses how APT actors work, how to evaluate your security defenses in light of these attacks, and how to increase the effectiveness of your security controls to better defend against APT threats.

02 Stealthy and Difficult to Detect: 3 Phases of an APT Operation

There are three phases of an APT operation: attack delivery or pre-exploitation, system compromise exploitation, and "action on objectives" or post-exploitation activity.



Pre-exploitation

To get inside a network, APTs use pre-exploitation tactics like phishing, water holing, or drive-by downloads. For example, an attacker can bypass a third-party hosted email gateway and deliver malicious email directly to a company's Office 365 account, or an attacker can bypass a web gateway by encrypting malware payloads. Organizations that lack policies to control and manage encrypted traffic are at higher risk. Web application firewalls (WAFs) protecting consumer-facing applications may be inadequately configured, enabling attackers to inject commands, gain a foothold in the network, compromise an application's database, and manipulate or steal sensitive data.

Phishing and spear-phishing campaigns have become much more sophisticated than in the past. Using easily available social media, attackers tailor spear-phishing emails to specific individuals, luring them with information that isn't common knowledge or simply looks innocuous. Humans are still the weakest link in the security chain, and attackers use that knowledge to their advantage.

Exploitation

Exploitation techniques are used to compromise systems, establish command and control (C2) access, and maintain presence in the network while avoiding detection. Attackers might modify registry keys to reference and execute malicious files; create "masquerade" registry entries that look like they are associated with legitimate programs; inject a malicious Dynamic Link Library (DLL) to escalate privileges or manipulate accounts by changing permissions, modifying credentials, or modifying authentication processes. Access to network administrator credentials can mean that an APT attacker now has the privileges needed to change critical controls and assets such as firewall configurations, user accounts, DNS servers, IP routing, listening ports, or system services.

Attackers also have a wide variety of defense evasion techniques.A rootkit can provide continued privileged access to a computer while actively hiding its presence. An APT might disable security tools, such as antivirus software, to prevent detection or interfere with normal security processes. Backdoors, or Trojans, are often installed on systems and used to install additional malware, exfiltrate data,or communicate with an attacker's system. Backdoors ensure that the attacker can come and go in the network, even if the captured log-on credentials are changed.

Post-exploitation

Once inside, APTs dwell in the network undetected for weeks and months using custom code for their dirty work. They move laterally within the network from their initial point of entry toward their ultimate goal—a server, database, or other critical assets. Common techniques for taking the next step in the network include authentication using Pass the Hash and hijacking a remote desktop protocol or Windows Remote Management (WinRM) session. Data is often collected and can be exfiltrated from the victim organization to the attacker via alternative protocols (DNS, Telnet, and others), email, and cloud services such as Dropbox and Slack.

03 | How Well Do Your Security Controls Actually Work?

There's no question that attackers will get into a targeted network. The better question is how well do your deployed security controls actually work? If you don't know, you're not alone.

Pros and Cons of Current Security Testing Methods

Vulnerability scanning, penetration testing, and Red Team exercises have traditionally been used to uncover an organization's security gaps. While each has its strengths, they also require a high level of expertise, time, or cost to perform. For these reasons, even large organizations use them infrequently, which means that they can only provide limited insight into a vast attack surface for a brief time.

- **Vulnerability Scanning**
  Vulnerability scanners help organizations identify systems that have not yet been patched with the appropriate software updates. However, they do not check for misconfigured security controls or poorly defined policies.

- **Red Teaming**
  Red Team exercises must be conducted regularly to have an impact on an organization's detection and response capabilities. Their added value is that they pit an adversary against the organization's security controls, infrastructure, and human element, providing a more thorough evaluation of a company's security posture. Yet, Red Team exercises only provide a snapshot of an organization's security posture because they are not continuous. In addition, they require a lot of manpower, must comply with security and compliance policies mandated by various regulations, and it can be difficult to assess their effectiveness.

- **Manual Pen Tests**
  Although manual penetration testing helps answer the question "can they get in?" they are usually limited in scope. The pen tester can try out the very latest tactics and techniques, but they rarely check all attack methods and results are highly dependent on the tester's skill. Like red teaming, pen tests offer point-in-time results, and it can take weeks to get an assessment report. Even after the organization remediates needed gaps, organizations rarely repeat pen tests to validate their effectiveness because that would require another costly engagement with a for-hire pen tester or consulting firm.

04 | A New, All-inclusive Paradigm

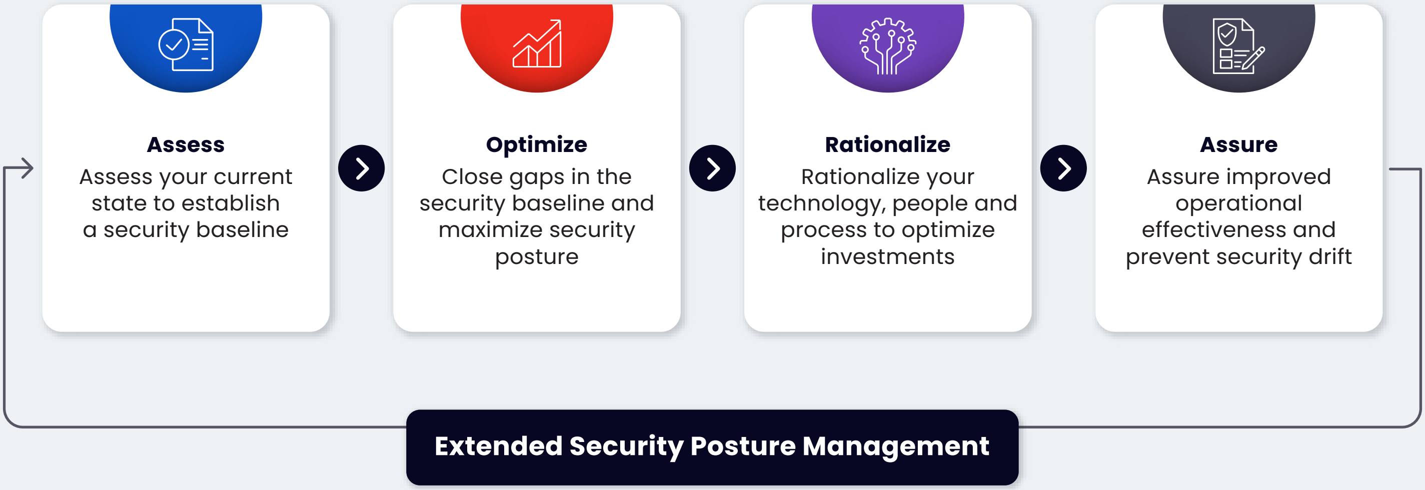
If attackers can continuously identify and exploit vulnerabilities across multiple threat vectors, shouldn't their targets be able to do the same thing? Targeted organizations also have the advantage of already knowing exactly which assets are critical to the business and how they are protected. It's time that security testing delivers continuous, on-demand visibility of cyber posture—including internal and external controls. Organizations need clear metrics that demonstrate weaknesses and the capability to quantify them to better assess risk and prioritize remediation. In addition to uncovering vulnerabilities, the testing solution should also help mitigate them.

A new testing paradigm is able to achieve these goals and enable organizations of all sizes to accurately know how well existing security measures are working—or not. Continuous security assurance solutions, which test the effectiveness of your organization's security via attack simulations, operate from an attacker's perspective to proactively challenge your defenses and validate your security framework.

Just as real APTs target attack vectors sequentially, security effectiveness testing solutions should also align against the pre-exploitation, exploitation, and post-exploitation phases of an APT-simulating attacks across the entire kill-chain. Anyone on your security team can continuously simulate attacks to assess, optimize, rationalize, and assure your organization's security posture. In four steps, you can make your environment significantly more APT-ready. Here's how.

Continuous Security Assurance Process

Operationalizing continuous validation and optimization



Assess
Assess your current state to establish a security baseline

Optimize
Close gaps in the security baseline and maximize security posture

Rationalize
Rationalize your technology, people and process to optimize investments

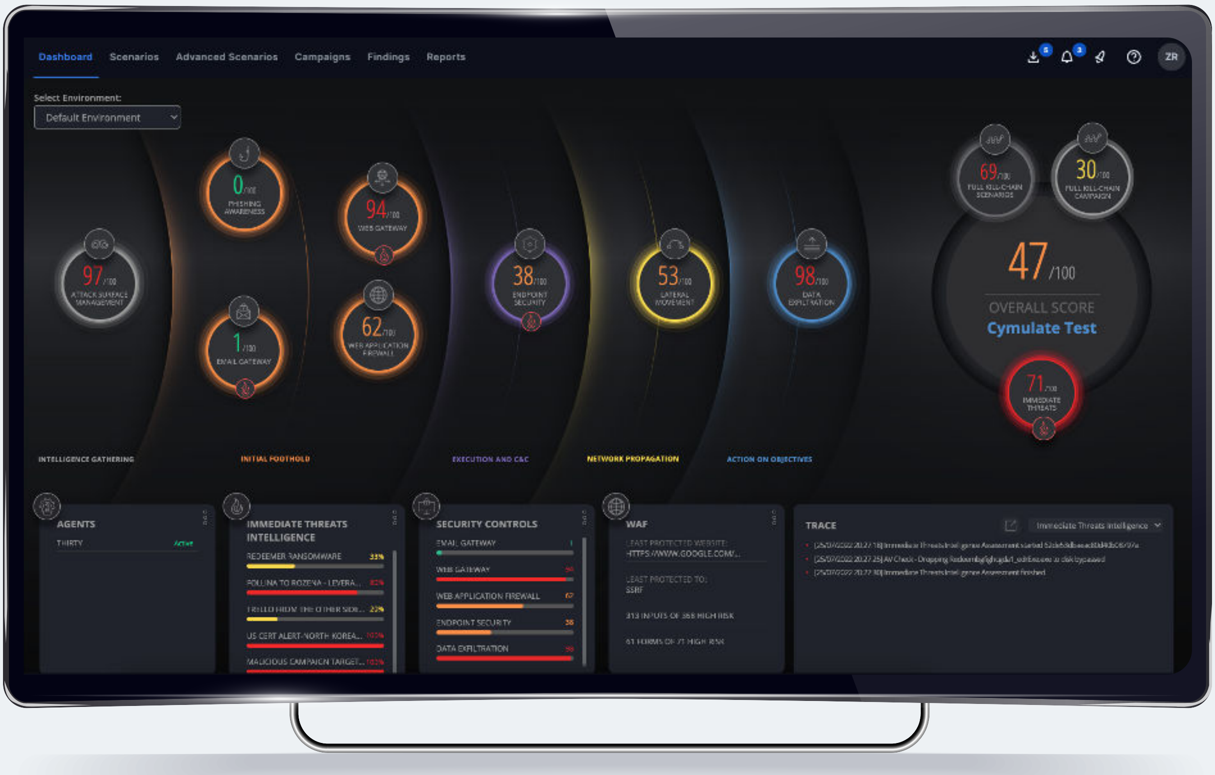
Assure
Assure improved operational effectiveness and prevent security drift

Extended Security Posture Management

Step 1: Assess

Continuous security assurance solutions test controls across all vectors in a single assessment, as shown in Figure 1. With just a few clicks, thousands of simulations targeting pre-exploitation, exploitation, and post-exploitation controls are launched. By mimicking countless threats—both common and new—you can challenge both internal and external defenses to assess your current security posture and establish a baseline to track your security performance.

Ideally, simulations should utilize real-world APT tactics used by well-known APT groups. For example, groups like Fancy Bear, OilRig, Lazarus Group, Ocean Lotus, and Dragonfly 2.0 have characteristic modus operandi. The simulation tool should also automatically update their simulations to emulate the latest threat trends and tactics.



Select Environment: Default Environment

AGENTS

THIRTY Active

IMMEDIATE THREATS INTELLIGENCE

REDEEMER RANSOMWARE	33%
FOLLINA TO ROZENA - LEVERA...	82%
TRELLO FROM THE OTHER SIDE...	22%
US CERT ALERT-NORTH KOREA...	100%
MALICIOUS CAMPAIGN TARGET...	100%

SECURITY CONTROLS

EMAIL GATEWAY	1
WEB GATEWAY	94
WEB APPLICATION FIREWALL	67
ENDPOINT SECURITY	38
DATA EXFILTRATION	98

WAF

LEAST PROTECTED WEBSITE: HTTPS://WWW.GOOGLE.COM/...

LEAST PROTECTED TO: SSRF

313 INPUTS OF 368 HIGH RISK

61 FORMS OF 71 HIGH RISK

TRACE

Immediate Threats Intelligence

```
• [25/07/2022 20:27:18] Immediate Threats Intelligence Assessment started [illegible]
• [25/07/2022 20:27:25] AV Check - Dropping [illegible] to disk bypassed
• [25/07/2022 20:27:30] Immediate Threats Intelligence Assessment finished
```

Figure 1 – Testing controls across the full kill-chain

A Identifying Pre-exploitation Weaknesses

APTs usually target email gateways, web gateways, and WAFs to gain entry and a foothold in the network. Security effectiveness testing will challenge these and other controls to uncover weaknesses.

Email Gateway

When operated with default configurations, email gateways may permit a wide range of file formats to land in employees' inboxes. Most gateways lack the ability to inspect nested files—a spreadsheet link inside a Word file inside a PowerPoint presentation, for example.

Web Gateways

These controls often cannot filter URLs or identify shady domains. By attempting to connect to known malicious URLs, attack simulation tools test policies across the web gateway, firewall, and network based IPS and IDS solutions to uncover vulnerabilities. Simulation tools can ensure safer browsing to prevent drive-by downloads, payload dropping, and C2 communications.

Web Application Firewalls (WAFs)

Web-based application vulnerabilities can allow attackers to execute arbitrary commands on the server side of an application, and if that server is part of the enterprise network, the attacker can then move laterally from the application's backend server to other sensitive assets. Many WAFs lack the ability to detect malicious requests. Misconfigurations are also common, so the WAF might be mistakenly running on monitoring mode instead of blocking mode, for example. And attackers can use techniques such as SQL injection, XSS, and command injections to bypass the WAF and dump databases containing sensitive information, such as personally identifiable information (PII), payment card details and protected health information (ePHI).

B Uncovering Exploitation Attempts

As mentioned previously, attacks are often successful at outmaneuvering gateways, WAFs and individual users, leading to the compromise of a server or workstation in an enterprise network. APT simulations can assess external attack surface management, user awareness, and endpoint security resiliency to overcome poor configuration settings or a mistaken click.

External Attack Surface Management

Emulate real attackers to automatically identify externally accessible digital assets (such as domains and IP addresses) and assess their exploitability against an organization's security policies and solutions.

Phishing Awareness

Simulate phishing attacks on users and assess employees' abilities to detect suspicious emails and not click.

Endpoint Security

When a user inevitably clicks, a threat simulation tool will demonstrate how well your endpoints catch signatures and suspicious behaviors.

Using MITRE ATT&CK™ techniques, security teams can easily create customized malware scenarios and run specific commands to test the effectiveness of controls, such as the ability of endpoint security solutions to detect malicious PowerShell commands, identify process injections, hooking, etc. By running simulations of techniques spanning defense evasion, infection, execution, credential access, privilege escalation, persistence, and more, security teams can ensure their security testing are sufficiently comprehensive, while gaining the ability to automate and shorten testing cycles.

Alternatively, threat simulations may comprise of scenarios that mimic the behavior of real ransomware, banking Trojans, cryptominers, worms and other threats; again enabling teams to assess the efficacy of their existing endpoint protection solutions and subsequently take the appropriate mitigative steps to reduce the organization’s threat exposure.

Behavior-based detection controls can be tested using precompiled executables with execution methods and behavior-based scenarios exhibited by common types of malware. Examples include DLL injection used to execute a payload, exploiting the Regsvr32 utility for payload execution, and dropping a malicious MS Word macro, among many others.

To test the effectiveness of AVs to catch the latest threats’ IoCs, tailored attack simulations may focus on dropping malicious payloads on an endpoint and then testing for the ability of the AV to detect it.

These attack simulations challenge EDRs, endpoint protection platforms (EPPs), antivirus, next-gen antivirus (NGAV), and host-based intrusion detection and prevision solutions (IDS/IPS) to ensure that they detect and stop threats.
Security validation tools also can test settings to ensure that endpoint solutions are actually blocking or quarantining files rather than just monitoring them.

C Testing for Post-Exploitation Vulnerabilities

Once inside the network, an APT has a multitude of Tactics, Techniques, and Procedures (TTPs) available to compromise systems and move laterally or exfiltrate data.
Attack simulation solutions should have the depth to match.

Lateral Movement

A threat simulation tool should be able to emulate attacks that exploit weak policies and might enable lateral movement, including policies applied on next-gen IPS systems and firewalls, as well as endpoint security solution such as EDR, EPP, AV and NGAVs.
Threat simulations can uncover misconfigurations and gaps in security controls, such as not implementing the principle of least privilege, and find weaknesses typically associated with flat networks, such as lack of segmentation and communication ports that unnecessarily permit communications over rarely used protocols.

Data Exfiltration

Testing your Data Loss Prevention (DLP) solution should enable you to validate settings, such as uncovering inabilities to detect data exfiltration performed via certain file types (e.g. JPG, PNG) and detecting exfiltration methods such as sending data to email, saving it to a thumb drive or using services such as Dropbox and Slack, etc.

Step 2: Optimize

Once you've conducted a simulation—what did it reveal? Your attack testing solution should provide scoring metrics that clearly show the areas of greatest risk, based on the number and types of simulated attacks. Scores should be calculated based on industry-recognized standards, such as the NIST Risk Management Framework, Common Vulnerability Scoring System (CVSS) v3.0 Calculator, Microsoft DREAD, or the MITRE ATT&CK Framework.

Simulation results should be easily understandable and explainable to non-technical individuals. Each simulation step and its results are displayed, showing control strengths and vulnerabilities. An exposure score accounts for the potential impact, infection success rate, and probability of encounter for simulated APTs. Higher scores reflect the magnitude of potential threats to target systems or resources—the higher the score, the greater the potential impact.

Remediation and mitigation guidelines, provided at the end of each simulation, enable IT and security teams to implement appropriate countermeasures and optimize an organization's security posture by closing gaps in the security baseline. KPI metrics deliver quantifiable security posture benchmarks and inform prioritization of remediation efforts and resources.

Pre-exploitation
By following the mitigation tips provided by your simulation tool, you can significantly improve the effectiveness of your email and web gateways or web application firewalls. Gateways or sandboxes that analyze files and file attachments, or malware analysis tools used for this purpose, can be adjusted to inspect email file types and nested files, along with content disarm and reconstruction tools used to sanitize suspicious items. Mitigation might also mean closing gateway configuration gaps or dozens of other possible steps based on your specific systems and vulnerabilities.

Exploitation
Improve security hygiene by disabling automatic macros, limiting privileges of user accounts, identifying and blocking unnecessary system utilities, restricting the execution policy (e.g. for PowerShell and CMD) on certain systems and taking steps to improve user awareness.

Post-exploitation
Mitigation guidance might include tips to improve DLP configuration or to limit or prevent lateral movement. Your simulation tool might recommend strengthening controls by applying principles of least privilege, removing unused or misused credentials, limiting the communication protocols available, or hardening systems.

Step 3: Rationalize

Once you optimize your controls, you can also identify redundancies or gaps and remove, replace, or add new tools. Attack simulation enables you to evaluate new products within your actual environment so you can reallocate budget, as well as rationalize your resources and spend to achieve operational efficiency.

Step 4: Assure

APTs rapidly adapt to an organization’s attempts to remove them from the network, and they frequently target the same victim again if access is lost. If you’ve been breached, you are much more likely to be targeted again and possibly suffer another breach.

Even if you have never been breached, our organization’s security posture is affected by many different variables—both known and unknown—that are constantly changing and causing perpetual drift. Maintaining a robust security posture and keeping risk low requires you to continuously monitor your security program’s performance, end-to-end.

A continuous security process is the only thing that will keep you and your organization safe. Schedule your security effectiveness tests to automatically and regularly simulate individual attack vectors to validate security controls, run simulations of the very latest threats detected in the wild, or test your security arsenal across the entire kill-chain.

Additional Benefits of Continuous Security Effectiveness Testing

A continuous security assurance process and attack simulation tools not only deliver immediate visibility into potentially damaging security gaps, but they also provide critical insights for strengthening an organization's overall security posture. They give your security team control over testing so they can make the most informed decisions for tailoring defenses to the organization's most pressing needs. Additional benefits include:

- **Security posture at a glance:** Get immediate visibility into your cyber stance across the digital estate—on demand or continuously—without waiting for reports.
- **Rationalize security investments:** Use objective metrics to benchmark and compare the effectiveness of different security solutions. Prioritize budget allocation and spending based on risk metrics and potential impact.
- **Test effectiveness:** Measure the impact of policy changes, software updates, and new or prospective technology purchases to avoid creating vulnerability or opening a gap.
- **Executive and technical stakeholder buy-in:** Effectively communicate quantifiable security gaps to the board, executive team, IT staff, and users
- **Continuous optimization:** Complement or replace manual and homegrown testing methods with fully automated, repeatable sets of tests that can be run across your infrastructure at any time.
- **Validate compliance:** Quickly and easily ensure that your organization remains compliant by assessing potential exposure across your infrastructure—without having to wait days or weeks for assessment reports.
- **KPI metrics:** Gain quantifiable benchmarks for an immediate, objective understanding of vulnerabilities and exposure levels. Metrics also provide a way to measure security control performance over time and compare your organization to others in your industry.

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.

With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.

Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

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

Start Your Free Trial