Cymulate
Extended Security Posture Management

Boosting Red and Blue Team Effectiveness with Cyberattack Simulation

Cymulate

Table of Contents

01 | Two Sides, But the Same Team

One of cybersecurity pros' biggest fears is not knowing what they don't know. Even with the most comprehensive security controls and processes in place, it's difficult to know if they're working as expected. That's why many organizations are using blue team and red team exercises for security control validation.

Blue team exercises test the defending team's playbooks, workflows, defense controls and communication processes.

Red team exercises aim to challenge the organization's security controls by assuming an adversarial role and simulating a cyberattack from a threat actor's point of view.
The result of such activity is the identification of gaps and other vulnerabilities that could be exploited or were exploited during the exercise.

Although "adversaries" in teaming exercises, both are really on the same team—dedicated to defending the organization against real-world, malicious threats. Breach and attack simulation can turbocharge blue and red team effectiveness, as well as extend both teams' reach, save time, and ensure that the organization is relying on consistent, accurate information about its defenses.

35% respondents claimed that the **blue team** never or rarely catches the **red team**

68% of respondents believe **red team** testing is more effective than **blue team** testing

Most organizations see significant value in using blue teams and red teams to identify coverage gaps. Blue teams are usually internal security personnel, including IT staff or SOC analysts. Red teams might be in-house security personnel or outsourced, depending on the organization's resources.

A survey conducted at the Black Hat USA 2019 conference provides a snapshot of how respondents are using blue and red team testing.

72% conduct red team exercises:

- 23% monthly
- 17% quarterly
- 17% annually
- 15% bi-annually

60% conduct blue team exercises:

- 24% monthly
- 12% quarterly
- 13% annually
- 11% bi-annually

68% of respondents believe red team testing is more effective than blue team testing

- 62% of respondents said their blue team occasionally or often catches a red team
- 35% of respondents said their blue team rarely or never catches a red team
- 2% of respondents said their blue team always catches a red team

02 | Teams and Their Tools

Blue Teams

Blue team testing is designed to ensure that security teams understand and can effectively respond to cyber threats or attacks. These exercises test defense controls, such as firewalls (FWs), intrusion prevention systems (IPSs), endpoint detection and response (EDR) tools, as well as security orchestration, automation and response (SOAR) tools, security information and event monitoring (SIEM) tools, integrations, and configurations. No less important, they test the security team's behavior under pressure and their response to the chain of events, including resolution of the simulated cyberattack and remediation of identified gaps.
As such, blue teaming tests not only the incident response team's technology, but their practical knowhow, communications processes, playbooks and workflows.

To evaluate if their security controls are working effectively, blue teams require offensive security testing to be performed using human or automated attack simulations by red team personnel or automated red teaming tools.

Red team exercises may be launched overtly—providing advance notice to the defending team of the impending exercise, or covertly—with the blue team not even aware that a cyberattack simulation is about to take place, enabling them to experience the threat of a potential breach with all the adrenaline and pressure of a real one.
In this way, organizations can mimic such scenarios in the most realistic, true-to-life manner possible, thanks to the element of surprise.

In a blue team exercise, blue teams check whether the actions performed by the red team are in fact being identified as suspicious or malicious, and ensure that they are being caught and recorded by their SIEM. The latter serve as an all-encompassing detection tool responsible for picking up security events and alerts generated by the organization's various security controls in the event of risky activity.

Blue teams also verify that these alerts are being prioritized correctly, so that incident responders can tackle the riskiest activity first.

For example, as a response to communications taking place with a blacklisted URL or domain, various controls such firewalls, web gateways and IPSs may generate an alert that will be picked up by the SIEM. As a response to a simulated ransomware payload, behavior-based tools, such as EDRs, are expected to create an alert, that once again, should be caught by the SIEM.
If a red teamer attempts to exfiltrate sensitive data, such as PII or mock payment card details, the DLP should identify this activity as suspicious, and if configured to do so, also block and prevent it from leaving the network.
Once again, an alert about such activity should be reflected in the SIEM. And so on, across all the defense controls deployed to protect the organization against the entire cyber kill chain.

By ensuring that security controls are working properly during a red team exercise, blue teams can ensure that in the event of a genuine cyberattack, they will receive the appropriate alerts to enable them to resolve incidents in a timely and effective manner.

Blue teams need red teams and their associated expertise for effective security risk assessments.
If the organization has an in-house red team, then blue teaming can be performed at any time.
If red team testing is outsourced, it's likely to occur infrequently. In addition, testing outcomes can be difficult to assess if there is inconsistency in the scope and methodology of how blue team exercises are performed.

For example, depending on the approach taken in a red team exercise, the scope of the test may vary, the level of intrusiveness may change and the covered attack techniques or threat types may be different, as well.

Red Teams

Red teaming requires significant human resources and expertise. Red teams use techniques such as pen testing, spear-phishing and other social engineering techniques, multi-vector attack testing, vulnerability scanning, and reconnaissance to find and expose weaknesses in the security infrastructure and in the human element. Although many organizations rely on red team exercises, this approach has several significant limitations.

Red team exercises typically focus on just a few attack vectors—they don't test controls across the entire kill chain. They typically use a limited number of attack techniques, unlike real-world malicious attackers who use more than 290 attack techniques, as listed in the MITRE ATT&CK™ framework.

Performing red team exercises in-house also requires multiple testing instruments. Every attack vector and security control has its own dedicated testing tools, functionality and methodology.
For example, challenging email gateways uses different tools and techniques than challenging firewall settings or data loss prevention tools.
Running commands on these tools also requires the organization to have specific technical expertise.

Red team tools often lack the latest cyber threat intelligence, which means that they can only challenge controls against known threats, or else red team testers must perform some research in advance to ensure they are incorporating the latest threat intelligence in their testing. New malware variants emerge daily, which means you still must ensure that your controls can identify the newest attacks' Indicators of Compromise (IoCs), stealth techniques and behaviors.

As a result of these variables, it's difficult for CISOs and IT teams to make meaningful evaluations of security control effectiveness, across attack vectors for accurate security risk assessment. A lack of remediation guidance also makes it difficult to prioritize resources for mitigating identified weaknesses.

Without end-to-end automation, red teaming exercises are difficult to repeat consistently, hard to perform on a large scale and challenging to perform with a broad scope. For example, after running an exercise and fine tuning controls, you would want to repeat the same barrage of tests to make sure the adjusted controls work. This is especially important because IT environments change continuously. When red teaming is performed only periodically, SOC managers and security analysts cannot easily assess the security impact of changes to the environment and track security control effectiveness accordingly.

Examining Red Team Tools

Vulnerability management platforms

Vulnerability scans and pen tests deliver useful insight into your security posture at a specific moment in time. These scans are usually performed by proprietary or open source applications. They check for vulnerabilities that are already known to vendors and the industry, as well as for weaknesses that cybercriminals have already exploited.

Typically, scans look for vulnerabilities resulting from unpatched systems in networks and web applications, which require certain updates to be made to protect against known CVEs and other vulnerabilities. By scanning networks and websites for thousands of different security risks, vulnerability scans can automate security auditing and prioritize remediation. However, they cannot present a complete, continuous picture of an organization's security posture over time, nor do they deliver in-depth control data needed to defend against sophisticated, multi-vector attacks. Moreover, while vulnerability management platforms can identify the presence of a known vulnerability (CVE), they cannot check if the CVE can actually be exploited as they lack offensive testing capabilities that mimic threat actor behavior. For example, even if a machine is found to be vulnerable to a specific CVE, various policies and settings that are already implemented may inhibit the CVE from being successfully exploited.

Without end-to-end automation, **red teaming** exercises are difficult to repeat consistently, hard to perform on a large scale and challenging to perform with a broad scope.

03 | Using Breach & Attack Simulation to Boost Red and Blue Team Effectiveness

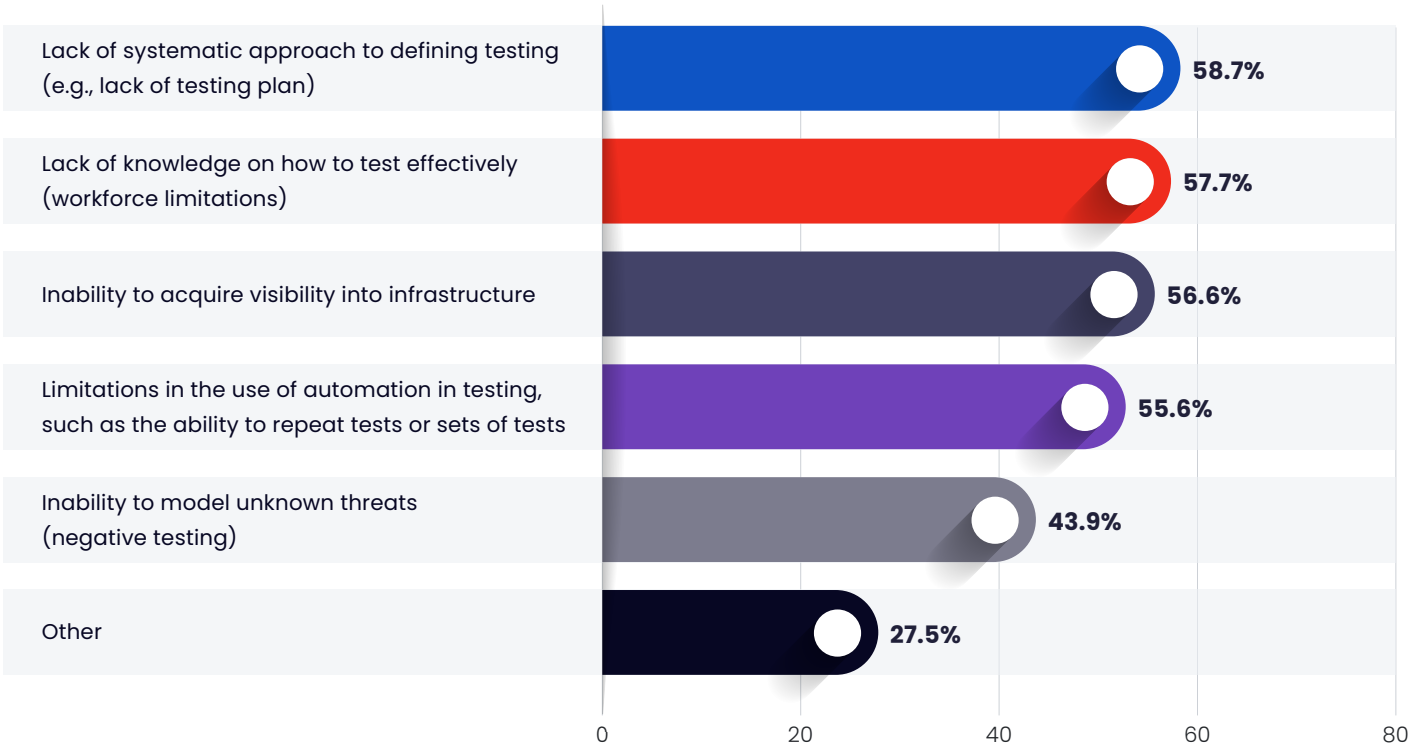
Automated Red Teaming Tools

There are a wealth of pen testing and red teaming tools out there, both paid and open source, to help you test your infrastructure, including MITRE Caldera, Red Canary Atomic Red Team and the Metasploit Framework, among others. However, they require some technical expertise to use, provide little remediation guidelines and cannot be used to prioritize remediation.

Blue and red teaming exercises are valuable components of many companies' security control validation strategies, but security teams still face barriers in maximizing their effectiveness. Figure 1 shows responses to a SANS survey on assessing control effectiveness.

> Lack of a testing plan is the top barrier cited by respondents to assessing control effectiveness.
>
> Source: SANS

What are your top three barriers to assessing control effectiveness?



A Breach and Attack Simulation (BAS) platform significantly boosts the effectiveness of both blue and red teams. Fully automated and customizable, comprehensive cyberattack simulation tests security controls across the full attack kill chain with thousands of simulated attacks. Able to test internal and external defenses, attack simulations show exactly where you're exposed and how to fix it—making security fast, continuous, and part of daily activities. BAS provides a systematic approach and testing methodology, deep visibility into the infrastructure and vulnerabilities, and automation for repeatability, fast results, and continuous coverage.

Cyberattack simulation tests security controls across the full attack kill chain with thousands of simulated attacks.

BAS Platform Capabilities

Proven framework

Offers a framework for testing an exhaustive range of attack vectors and threat scenarios, creating customized testing templates, and defining the testing scope.

Automation

Offers repeatability and continuous coverage, BAS enables you to automate testing, alerting and reporting to run daily, weekly, or on demand, for nonstop security control validation.

Industry-recognized threat modeling

Models threats based on the cyberattack tactics and techniques as described in the MITRE ATT&CK™ framework.

Remediation guidelines

Gain immediate remediation and mitigation guidelines for rapid, accurate response.

Complete coverage

Challenges controls across all vectors of the cyber kill chain, including pre-exploitation, exploitation and post-exploitation.

Metrics and reporting

Receive immediate auto-generated reports, that include metrics describing the full attack story and the techniques used. Benchmark control effectiveness against others in your industry and measure the impact of changes over time.

Threat intelligence

Enables incorporating daily threat intelligence on the latest cyberattacks seen in the wild, such asransomware, Trojans, APTs, cryptominers, worms or other threat types.

Enhanced Blue Teaming

The security team in a global financial services organization had traditionally developed and performed homegrown cyberattack simulations to test its security posture against specific threats. After implementing new technology, deploying a specific security policy, or updating the rule engine of a security control, the team would simulate specific attacks to ensure that they were blocked or detected and mitigated. However, as attack techniques become more sophisticated, operating across multiple vectors, and increasing in volume, building simulations in-house became more challenging. The development of each attack simulation is resource intensive, especially as they become more complex.

The security team above turned to BAS, which immediately increased their security control validation effectiveness. They no longer had to build or prepare manual frameworks to execute tests. They use BAS to augment periodic manual pen testing, and red team exercises, as well as to run frequent tests in response to vulnerability scans, emerging threats in the wild, or infrastructure configuration changes. Security control validation with BAS quickly shows them if defense controls identified the attack simulations and generated appropriate events and alerts in the SIEM.

The team can also run covert exercises simulating a full-blown advanced persistent threat (APT) across the kill chain. As shown in Figure 3, results are instantly available in a single-pane-of-glass view, with detailed breakdown of successful methods, progression of attack events, attack techniques, correlation with the MITRE ATT&CK framework, and specific mitigation steps that can be taken to reduce the attack surface. Everything is documented in the dashboard for future analysis and reference.

With BAS, security teams also gain the visibility needed to identify malware artifacts in security controls such as the SIEM, to ensure security controls are working as expected. They can search simulation results for unique strings appearing in the simulated malware file names, and verify that these artifacts appear in the relevant security control's alerts and events, for example, EDR, SIEM, etc.

BAS reports illuminate the full attack story, identifying how a simulated attack infiltrated the network, how it can exploit a target system or server and how it can accomplish threat actor objectives, such as encrypting files and folders or exfiltrate sensitive data. Delving into details, reports cover techniques used such as registry key manipulation, the creation of new folders and files, and PowerShell commands run.

How Cymulate Enhances Blue Teaming

- In-app visibility into SIEM and EDR's detection capabilities
- Comprehensive insights, analysis and mitigation guidelines
- Prioritization of remediation using exposure score
- Easy search of artifacts for log inspection
- Intuitive technical and executive-level brief
- Fully automated testing, reporting, and alerting
- Optional enrichment of workflows with Cymulate API

Figure 3. Blue teams can assess whether their SIEM and EDR are picking up alerts generated by attack simulations

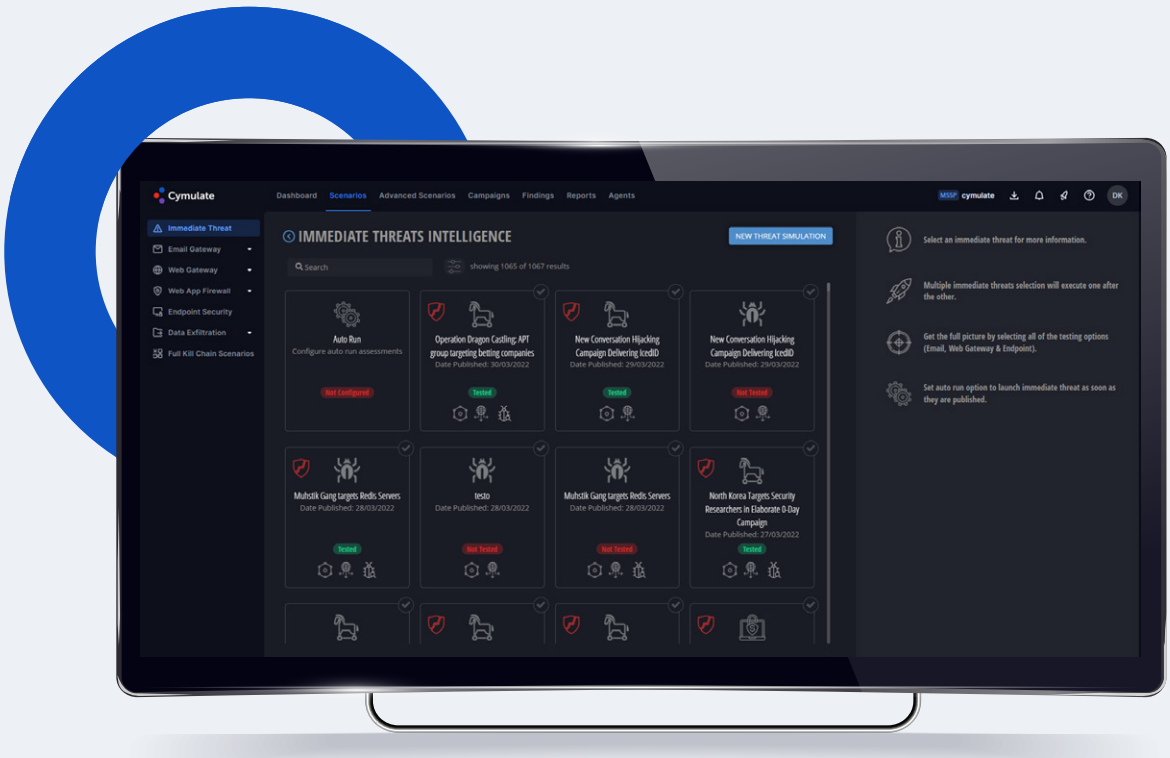


Figure 4. Red teams can automatically challenge controls against the very latest threats IoCs and techniques

Enhanced Red Teaming

With BAS, red teams can augment their capabilities to achieve comprehensive testing. They can test the IOCs and techniques deployed by the latest immediate threats seen in the wild, test across attack vectors, and challenge their security controls against the entire cyber kill chain.

BAS enables red teams to methodically test against all attack types—ransomware, worms, Trojans, C&C payloads, phishing, and others—using a variety of precompiled attack simulation scenarios and simulated payloads, as well as over 150 MITRE ATT&CK methods and techniques. As shown in Figure 4, they also can quickly and easily build their own attack simulation templates based on such precompiled attack scenarios, and MITRE ATT&CK techniques.

Understanding and identifying nation-state and other geopolitical actors are becoming increasingly critical for many organizations. The BAS platform identifies APT groups with their signature APT methodologies and techniques, enabling red teams to simulate targeted attacks relevant to their industry and geography.

How Cymulate Enhances Red Teaming

- In-app visibility into SIEM and EDR's detection capabilities
- Comprehensive insights, analysis, and mitigation guidelines
- Prioritization of remediation using exposure score
- Easy search of artifacts for log inspection
- Intuitive technical and executive-level briefs
- Fully automated testing, reporting and alerting
- Optional enrichment of workflows with Cymulate API

Cymulate

04 "Adversaries" Working Together

Using BAS, both blue and red teams can exponentially enhance their exercises and objectively assess performance of current controls supported by exposure metrics. Knowing where the organization's exposure is highest enables security teams to prioritize remediation and maximize the effectiveness of all security controls integrated with their SIEM. Blue teams gain immediate insight into security control effectiveness, together with helpful guidance on addressing new or complex threats.

Red teams can expand the frequency, volume, breadth and depth of their testing exercises to obtain 360° assurance that defenses either cannot be compromised or detected and remediated accurately. The winner? It's the organization that now can assure security control effectiveness and strengthen its security posture around the clock with consistent, accurate information about its defenses.

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 continuously 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

Request a Demo

Headquarters: Maze St 3, Tel Aviv 6578931, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632