Cymulate

Responding to the Current Threat Landscape

Tips for answering tough questions about security validation and immediate threats

Table of Contents

01 Difficult Questions Require Complete Answers

For every organization, in every industry, cybersecurity resilience produces a continuous stream of questions.

A. How will an organization be attacked?

B. How can a security team defend against it?

C. How can they do it all again tomorrow? Next month? Next year?

While these questions can be difficult, the answers themselves must be straightforward, understandable, and accessible not only to the technology team but to the board and other business leadership, as well. Finding the right answers for an organization—and detailing those answers to all stakeholders—is something that Breach and Attack Simulation (BAS) can help with.

02 Testing Continuously and Comprehensively with BAS

Adversaries are relentless in their pursuit of a security gap or error. They simply never stop, knowing that time and human nature eventually work in their favor. Traditionally, organizations have been reactive—addressing vulnerabilities and threats after they are exploited or published in the media.

However, in today's adaptive and dynamic threat landscape, organizations have become more proactive with periodic pen testing, red teaming, and vulnerability scanning to test their teams and defenses. While these approaches are valuable, they are point-in-time approaches that require significant investments in time, talent, and budget.

Testing each security solution with its vendor's testing tools is also helpful for gaining detailed performance data, however, data collected from multiple systems and testing tools is difficult to correlate for meaningful action. Under continuous onslaught from cyber threats, organizations need defense strategies that are also continuous and comprehensive.

According to Gartner, "Security and risk management leaders should confront the threat landscape based on a continuous assessment of threat and business evolutions." Further, "The most rational approach would be to "engineer" the threat landscape, dissecting its components, analyzing each of them and prioritizing each factor based on the limited known business context. This approach is costly however, and takes time[1]."

Instead, organizations can turn to Breach and Attack Simulation (BAS) solutions to test their defenses. BAS is the practice of continually challenging, measuring, and optimizing the effectiveness of security controls using automated simulations to identify new security gaps as they emerge. Simulating with BAS provides organizations with an established framework to consistently assess security control efficacy. Unlike traditional pen testing or specific platform tests, security and risk management leaders use BAS to test their security posture from different angles.

[1] How to Respond to the 2019 Threat Landscape, Gartner, August 16, 2019

03 | 5 Tips for Responding to the Current Threat Landscape

BAS provides a powerful antidote to the unknown, delivering accurate, real-time insight into an organization's security posture—anytime and across all threat vectors. Here is how BAS directly addresses organizations' burning questions regarding threat actors.

Question: How do organizations stay on top of threat actors' common attacks?
Traditional threat vectors are still the most used—because they work. Hacking, malware, social threats, error, and misuse are the same top five threat vectors in 2022 as in 2013[2]. Threat actors still begin their efforts with the usual entry points, mainly using email or web-based attacks to deliver malware or establish command-and-control (C2) footholds.

Answer: Test the usual targets
Adversaries, whether external threats or rogue insiders, try to exploit the easiest avenues first. As shown in Figure 1, BAS enables organizations to simulate these threats against endpoints and test the effectiveness of endpoint protection platforms (EPPs), endpoint detection and response (EDR) solutions, antivirus, next-generation antivirus, web and email gateways, and other preventive measures.

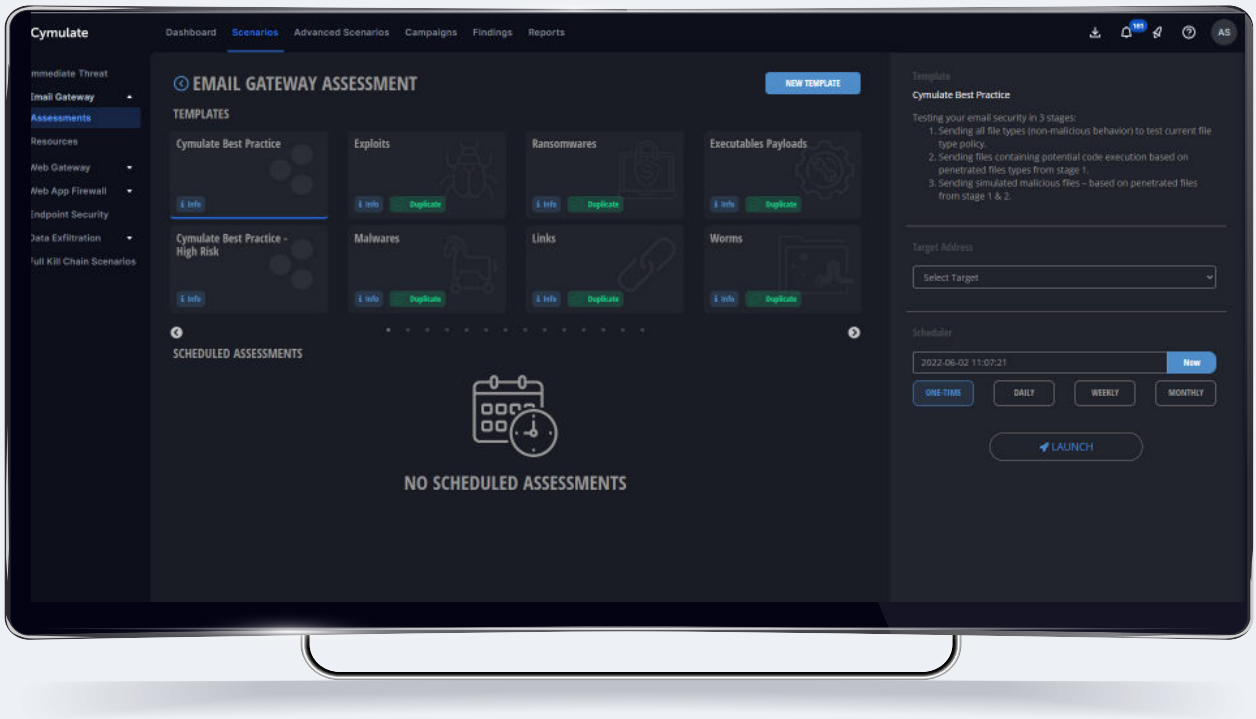

*Figure 1. Testing the most used attack vectors against known and the very latest threats

[2] 2022 Data Breach Investigations Report, Verizon

Question: How do security teams keep up with threat actors that are continuously adapting?
Attacks can, and often quickly do, adapt to bypass or overcome defenses and patches. A great example of this is the winding path of log4j. While log4j began as a straightforward exploitation of a weakness in a commonly used open source library, it didn't remain that way for long. When defenders found a way to block the attempt at exploitation, within a day threat actors began using a slightly modified form of the exploit which bypassed those filters[3]. Over the following months, threat activity around the exploit was found to impact everything from desktop apps to virtual desktop infrastructure[4].

According to Breach and Attack Simulation vendor Cymulate, when tested, 26% of organizations are vulnerable to an Emotet variant8[5]. Shodan statistics showed thousands of vulnerable hosts susceptible to proxynotshell weeks after patches were available, which proves to attackers that not all organizations keep abreast of the latest attack techniques[6].

This data points to the fact that preventive controls should continuously be updated with the latest indicators of compromise (IoCs) because as attackers adapt, organizations are exposed. Manually checking controls every day to make sure they can block the latest phishing sites, infection points, C2 servers, and other vectors is not practical for most organizations.

Answer: Surface the latest microtrends
BAS eliminates manual testing with simulations of the most current threats, allowing teams to immediately ensure that controls can detect the very latest IOCs and help them fine-tune defenses more quickly. Figure 2 shows how BAS delivers detailed immediate threat intelligence to keep defenses synched against the latest threats. BAS also tests preventive IoC-based controls that are are ineffective against signatureless and fileless attacks. With BAS, other machine learning and AI-based solutions' configurations are continually fine-tuned to enable faster detection.

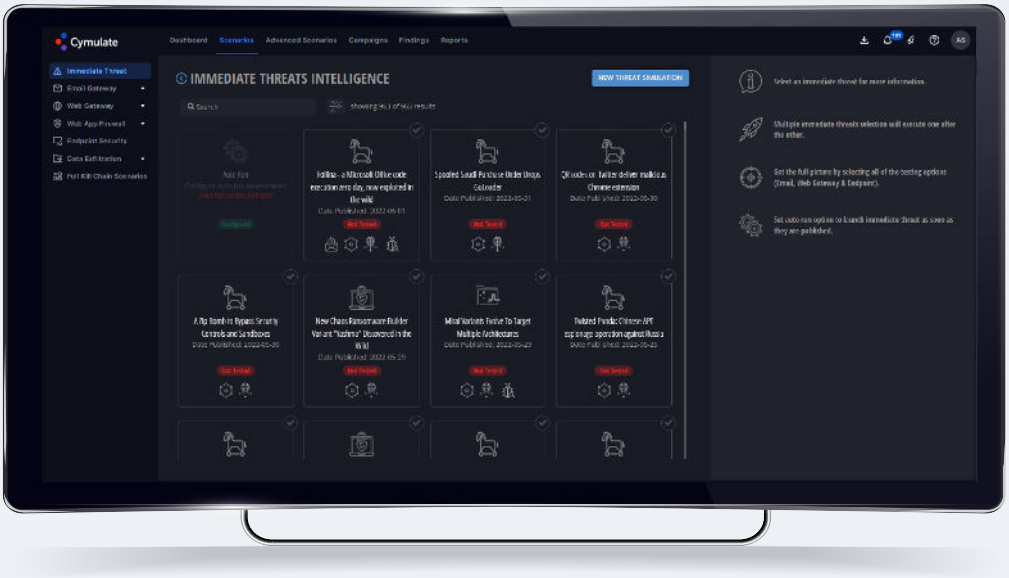

*Figure 2. Continuous security testing helps defend against the latest threats faster

[3] https://www.csoonline.com/article/3645431/the-apache-log4j-vulnerabilities-a-timeline.html

[4] https://www.rapid7.com/db/vulnerabilities/vmware-horizon-agent-cve-2021-45046/

[5] https://www.prnewswire.com/il/news-releases/cymulate-boosts-its-full-kill-chain-bas-platform-with-new-apt-simulation-to-id-gaps-in-network-defenses-300858901.html

[6] https://unit42.paloaltonetworks.com/proxynotshell-cve-2022-41040-cve-2022-41082/

Question: What if an organization's assets are extremely well-defended? Is there anything else the security team needs to worry about?

Adversaries also have changed their targets from executives to strategic low-level employees. Frequently, they will even target an organization's third-party partner to exploit connections that reach into their primary target. These links include everything from consumer-facing portals, health and scientific information exchanges, ordering systems, and payment gateways to shared collaboration tools.

In perhaps the most famous example from 2013, Target—a giant retail organization in the United States—found itself dealing with a massive breach of credit card data. Interestingly, the initial target of the attack was an environmental systems vendor which had only maintained a link into Target's systems for billing purposes. Using the access gained by breaching the HVAC vendor, the attackers hopped from system to system to eventually reach and breach the credit card Point-of-Sale systems[7].

In recent years there has been a consistent trend of threat actors targeting 3rd-party services or other low-priority targets to gain access to high-priority data. For instance, when Apple lost control of critical blueprints due to an attack against a hardware outsourcing firm[8].

Answer: Challenge defenses against anything that has access to an organization's systems

Using BAS allows teams to test these ports of entry, as well as internal controls that limit lateral movement. Figure 3 shows how BAS challenges internal network configuration and segmentation policies against different techniques and methods used by attackers to propagate within the network and control additional systems. It simulates an adversary that has control over a single, compromised workstation and attempts to move laterally within the organization. The result of the assessment is a visualization of all the endpoints that the simulated adversary was able to reach with a detailed description of the methods used. The assessment identifies infrastructure weaknesses and provides guidance to remediate them.

*Figure 3. Lateral movement assessment to test for propagation between network segments

[7] https://redriver.com/security/target-data-breach

[8] https://www.bloomberg.com/news/articles/2021-04-21/apple-targeted-in-50-million-ransomware-hack-of-supplier-quanta

Question: How does an organization make sure it is safe when there are constant changes to IT?
Nonstop changes to IT systems make it difficult to ensure that defenses keep up with attack surface changes. Even newly deployed security measures will fail without a way to continuously assess the impact of change on the organization's risk posture and adjust security measures accordingly. Organizations are at risk of being exploited through unknown loopholes, such as software vulnerabilities, poorly configured security controls, lax settings, and excessive permissions.

Answer: Close gaps created by IT change
With continuous BAS, security teams are confident that their controls provide nonstop coverage of their organizations' assets. In addition to challenging a constantly changing IT environment, BAS helps teams test the impact of new technologies on security posture. By testing solutions before they're deployed, organizations ascertain that their chosen solutions perform as expected, prevent unknown gaps, and function with other security controls. Purchase decisions can be made according to how well comparable technology performs in the face of attack simulations.

*Figure 4. BAS assessment for Advanced Persistent Threats (APTs) across the kill-chain

Question: With so many threat actors and so much automation, don't the attackers have an unfair advantage?

Nation-state attackers and adversary groups have a distinctly unfair advantage over most organizations' security and risk management teams. With vast amounts of money and skilled resources, they have all the time they want to conduct reconnaissance and identify new exploits. According to Gartner, "If nation states target your organization, they will get in. The challenge becomes recognizing these sophisticated attacks early, and disregard trying to find all the ways these attackers may enter[9]."

Answer: Automate security posture validation

Most organizations are out resourced by nation-states and other adversaries. However, even with a small team, continuous BAS effectively identifies gaps and simplifies remediation before the gaps can be exploited. Teams gain exponentially greater visibility into security gaps across the full kill-chain. Closing those gaps hampers all attackers' lateral movement, including those from state-sponsored threat actors.

In Figure 5, teams gain at-a-glance insights into specific TTPs and actions with the ability to drill down into much deeper levels of detail. Dozens of nation-state APT groups actively work for financial, political, and military gains and with BAS, organizations can continually test their ability to cope with techniques that APT groups are known to use. Figure 5 shows how an organization's controls fared against techniques that are documented to be used by APT groups.

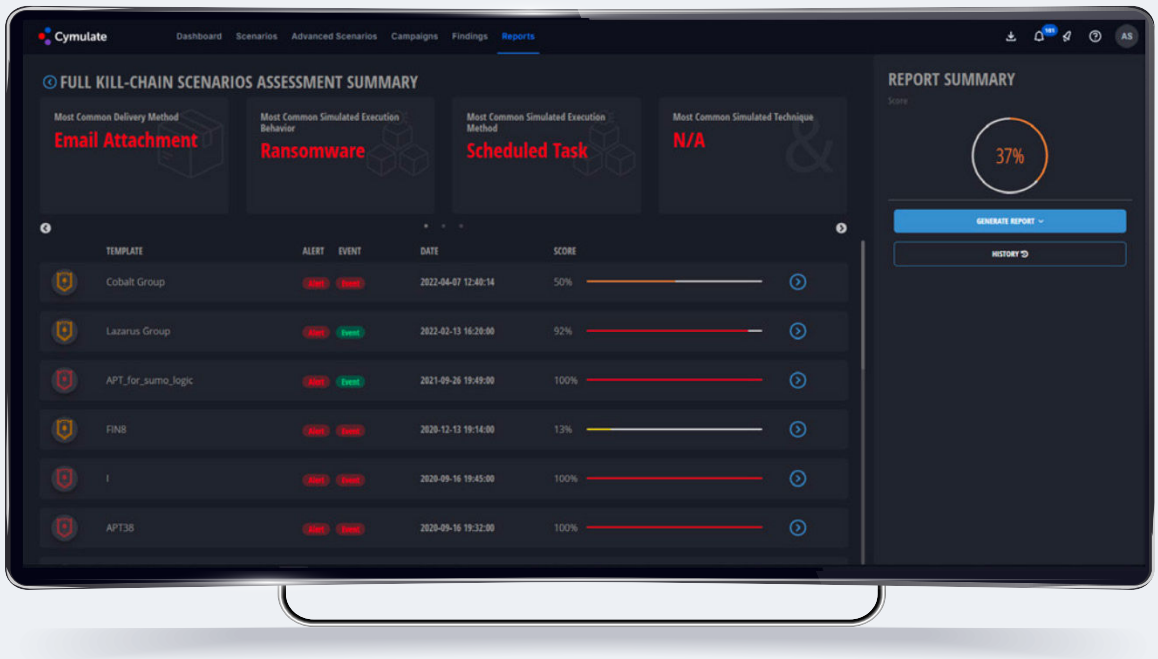

*Figure 5. Testing defenses against documented techniques used by APT groups to assess security control effectivenes

[9] How to Respond to the 2019 Threat Landscape, Gartner, August 16, 2019

04 Continuous Simulations for Continuous Improvement

Many security vendors have begun to provide performance metrics based on industry-recognized standards such as the NIST Risk Management Framework, MITRE ATT&CK™, Common Vulnerability Scoring System (CVSS), and Microsoft DREAD. Quantifiable metrics give security teams a starting benchmark for assessing control effectiveness in their specific environments. By continually challenging their security controls, uncovering weak spots, and tuning controls to improve their effectiveness, teams can shrink their attack surface.

BAS enables continuous, comprehensive testing to challenge, measure, and optimize cyber defenses with:

- Production-safe simulations that test across the full kill-chain
- Out-of-the-box simulations of the latest threats and TTPs, as well as customizable attacks for advanced users
- Scheduled, automated attacks for repeatability, accessibility, and consistency
- Techniques mapped to the latest MITRE ATT&CK matrix
- Actionable remediation guidance

While BAS is a pioneer in the automated security validation market, in the last few years additional technologies have emerged to address security posture challenges. Some security vendors offer these solutions as stand-alone products and others offer them as add-ons to their BAS. These technologies include:

External Attack Surface Management (EASM) – This technology emulates real attackers to identify digital assets (such as domains, IP addresses, and more) and assess their exploitability against an organization's security policies and solutions. With findings mapped to the MITRE ATT&CK® framework's TTPs (Tactics, Techniques and Procedures), companies can take the necessary mitigation steps.

Vulnerability Prioritization Technology (VPT) – This technology integrates with common vulnerability scanners to combine the data on found vulnerabilities with the results of BAS simulated attacks. It correlates the criticality of vulnerabilities with the value of assets so organizations can optimize patching prioritization and drastically reduce the patching workload.

Purple Teaming Framework – This solution operationalizes the MITRE ATT&CK® framework to create, launch and automate custom attack scenarios. Security teams craft or modify executions to create both simple and complex scenarios of atomic, combined, and chained executions.

Published in late July 2022, Gartner's Continuous Threat Exposure Management (CTEM) program[10] is a new approach to achieve lasting and robust cyber resilience. The suggested continuous planning and monitoring process reduces the level of risk and includes the executive departments. CTEM uses validation technologies that prompt prioritized remediation actions based on the business context. Through adopting technologies like those listed above, Gartner predicts that organizations will be far less likely to be breached.

[10] Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program, 25 July 2022, Jeremy D'Hoinne, Pete Shoard, Mitchell Schneider.

05 Re-Shuffling the Deck

It's not surprising that many organizations feel that the cybersecurity deck is stacked against them. Despite a constantly shifting threat landscape with known and new attack vectors, continuously evolving tactics and targets, and a distinct resource disadvantage—there is hope. Security teams now have the opportunity to re-shuffle the deck in their favor with BAS. Using continuous, comprehensive attack simulations, they can find—and close—potential exploitation avenues before attackers exploit them. Continuous security validation enables organizations to continually strengthen their security postures with measurable, documented improvement.

*Figure 6. Security Validation Platforms provide comprehensive attack simulations to help find and close potential exploitation avenues before attackers exploit them

About Cymulate

The Cymulate Security Posture Validation Platform provides security professionals with the ability to continuously challenge, validate, and optimize their on-premises and cloud cyber-security posture with end-to-end visualization across the MITRE ATT&CK® framework. The platform provides automated, expert, and threat intelligence-led risk assessments that are simple to deploy, and easy for organizations of all cybersecurity maturity levels to use. It also provides an open framework for creating and automating red and purple teaming by generating tailored penetration scenarios and advanced attack campaigns for their unique environments and security policies.