Cymulate

Extended Security Posture Management

How confident are you that your organization is protected from the next cyber-attack?

There are many factors to consider when answering this question: exposed digital assets, poorly configured security controls, immediate threats, newly discovered vulnerabilities, security gaps, architecture changes, and more. Your 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.

Cymulate empowers security leaders to maximize operational efficiency while minimizing risk exposure with a continuous security assurance program. With Cymulate SaaS-based Extended Security Posture Management, companies effectively manage their exposure to cyber threats, map and block possible breach routes, and validate security controls' performance.

With Extended Security Posture Management (XSPM) you can:

Manage organizational cyber-risk end to end

Rationalize security spend

Prioritize mitigation based on validated risk

Prevent environmental security drift

The Most Comprehensive Security Validation Technology

Cymulate's XSPM platform provides an end-to-end overview of an organization's security posture. This framework presents a comprehensive understanding of current levels of risk, exposure, drift, and even potential savings.

Security Controls Validation

Breach and Attack Simulation – Cymulate's Breach and Attack Simulation (BAS) technology was ranked #1 in innovation by Frost & Sullivan in the 2021 BAS Radar. Cymulate's BAS combines red (offense) and blue (defense) activities. It simulates thousands of attack scenarios and correlates them to security control findings through API integrations, as well as provides actionable detection and mitigation guidance.

- **Immediate Threat Intelligence** – Save time on threat research with prepackaged threat intelligence-led assessments that are updated daily, including samples, IoC's CVE's, detections, and mitigations.

Advanced Purple Teaming – Advanced Purple Teaming expands BAS into the creation and automation of custom advanced attack scenarios. Customized scenarios can be used to exercise incident response playbooks, pro-active threat hunting and automate security assurance procedures and health checks. Advanced Purple Teaming is primarily used by security practitioners with adversarial skills, including red teamers and pen-testers.

Attack-Based Vulnerability Management

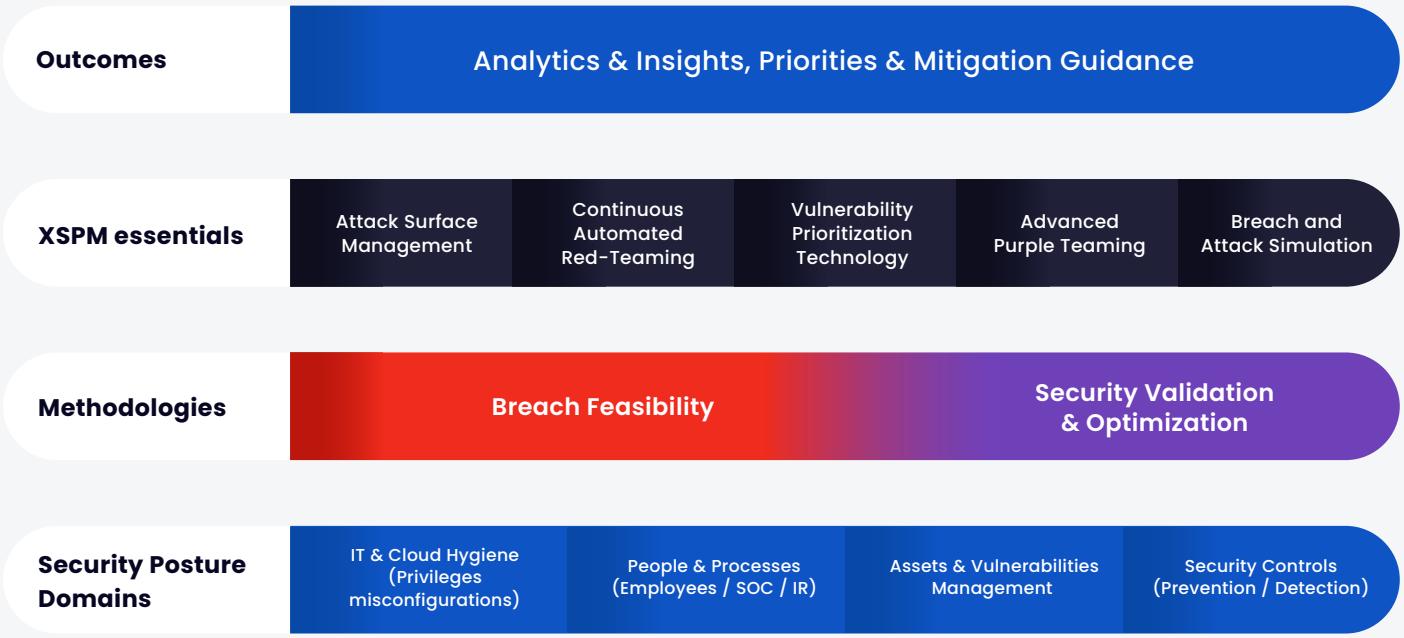
Cymulate's Attack–Based Vulnerability Management (ABVM) integrates with leading third-party vulnerability management solutions and cross-references information on vulnerabilities provided by these vendors, along with the analysis from Cymulate's ABVM, and offers a practical view of compensatory security controls over unpatched vulnerabilities in the network. Cymulate's ABVM enables organizations to accurately prioritize remediation and patching or reconfiguration of compensating security controls.

Breach Feasibility

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

Red Teaming Automation – Cymulate's red teaming automation capability amplifies attempts to penetrate the organization by deploying attack techniques that evade detection controls and gain an initial foothold within the network. It can also trigger the attack with a well-crafted phishing email. After gaining the initial foothold, the attack subsequently tests network segmentation policies by lateral movement within the network in search of a pre-defined objective. Blue teams leverage Cymulate's adversarial capabilities to assess their cybersecurity resilience, and companies that have in-house red teamers benefit from customization and automation to increase their operational efficiency.

Extended Security Posture Management (XSPM) Framework



Benefits

Optimize Cybersecurity Investments

To successfully allocate security funds in direct proportion to a company's priorities, security leaders need a clear picture of which security solutions are instrumental in protecting which business units. Cymulate enables you to quantifiably measure the effectiveness of security solutions, processes, and stuff workloads, to fine-tune your security spend to align with company priorities.

Reduce Risk Exposure

Cymulate assesses your current level of cyber-risk exposure from a threat actor viewpoint and draws a baseline to monitor how it trends over time. Doing so allows you to constantly validate your security controls against imminent threats, discover exposed assets and measure your employees' level of cyber awareness.

Measure and Communicate Value

Cymulate enables measuring and conveying cyber risk to executive leadership in simple words and with supporting data. Tracking and reducing your risk level over time, taking corrective measures, and optimizing defenses help demonstrate your security programs' impact on risk and ROI.

Why Cymulate?

01 **Fast Time to Value -** The Cymulate SaaS-based platform takes less than one hour to deploy, dramatically reducing risk within the first three months.

02 **End-to-End Validation -** Cymulate validates a company's security posture across the full cyber-attack kill chain, operationalizing the MITRE ATT&CK® framework, end-to-end.

03 **In-Depth Validation -** Cymulate utilizes various security tools and analytics to assess and validate an organization's true preparedness to handle cybersecurity threats effectively .

04 **Management and Analytics -** Combining aggregated findings from the entire Cymulate XSPM platform enables security leaders to create, customize, and export reports to gain unique holistic insights on their security posture and make data-driven decisions.

05 **Immediate Threat Intelligence -** Cymulate's Research Lab stays abreast of the very latest threats, updating the platform daily with Immediate Threat Intelligence so that organizations can rapidly assess their resilience against the latest threats.

Scaling Up Security for Every Maturity Level

Basic
Preventative Security Stance
Organizations who want to automate their security control validation & optimization, as well as operationalize threat intelligence.

Progressing
Detect and Respond Security Stance
Organizations who want to exercise incident response & threat hunting, rationalize security investments, and manage their attack surface, cyber hygiene, and prevent drift.

Advanced
Offensive Security Stance
Organizations who want to leverage & scale in-house red teaming, incorporate security validation into organizational risk management, and implement a continuous security assurance program.

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

Start Your Free Trial

Headquarters: Maze St 3, Tel Aviv 6578931, 7546302, Israel | +972 3 9030732 | info@cymulate.com | US Office: +1 212 6522632