# Extended Security Posture Management for Manufacturing

## How confident are you that your organization is protected from the next cyberattack?

Cyberattacks have caught up to the manufacturing industry and organizations today are concerned about production shutdowns resulting from these attacks, Intellectual Property (IP) theft, new vulnerabilities being announced daily, and making sure to implement compliance requirements. Meeting these demands takes a toll on manufacturers' security teams who are constantly fighting the next fire and have no time to reevaluate and optimize their cybersecurity posture. However, to stay ahead of cybercriminals, manufacturers would like to take a proactive approach to cybersecurity and predict if and how cyber-attacks can evade their defenses.

An industrial company'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 cybersecurity leaders to continuously monitor their program's performance, end-to-end.

### The top four security concerns of manufacturers are:

- Production shutdown resulting from a cyberattack
- Intellectual Property (IP) theft
- Vulnerability management
- Implementing compliance requirements

### Assess, Validate, and Manage End-to-End

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

## Security Controls Validation – Breach & Attack Simulation (BAS) and Advanced Purple Teaming

Cymulate enables you to orchestrate simulated attack scenarios that validate email, web, web-application, endpoint, and DLP security controls either individually or by simulating the flow of an APT across the full attack kill-chain. Out-of-the-box scenarios make it simple to launch various assessments. The platform is updated daily with new threats, attacks and adversarial tactics and techniques for you to simulate the latest scenarios and validate the current effectiveness of your security controls against emerging threats.

**Cymulate's security controls validation ensures the right controls are in place to prevent a ransomware attack, IP theft, or confidential data exfiltration, and tests against the latest attacks targeting production companies.**

## Security Posture Assessment

### Attack Surface Management (ASM)

Cymulate's Attack Surface Management (ASM) technology emulates real attackers to identify digital assets and assesses their exploitability against the organization's security policies and solutions. With findings mapped to the MITRE ATT&CK® framework's Tactics, Techniques, and Procedures (TTPs), 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.

Industrial businesses are especially susceptible to attacks because of the large attack surface that contains both Operational Technologies (OT) and Information Technologies (IT). These technologies also increase risk because they are usually configured with basic security features that are easy to exploit.

**Manufacturers can use Cymulate's ASM and Red Teaming Automation to discover misconfigured IoT and OT devices or any other vulnerabilities in their security controls. Once exposed, the organizations can implement Cymulate's mitigation guidance to prevent threat actors from leveraging them as an entry point to the corporate IT network.**

### Infrastructure Resilience & Segmentation Policies

Cymulate's Lateral Movement vector emulates a hacker that has gained an initial foothold in a company's network and moves laterally in search of valuable assets. It applies hacking tactics and techniques to uncover infrastructure misconfigurations and weaknesses. Cymulate decouples infrastructure lateral movement validation from endpoint security validation (worm malware) so that each vector can be measured and optimized independently.

In the case of network segmentation, Cymulate enables the continuous evaluation of the efficacy of security policies for separate units within the same company. For companies with a complex infrastructure, Cymulate can ensure that there is no opportunity for lateral movement between networks.

A production organization may segment its production network from its corporate IT network, but a misconfiguration or security drift can leave it vulnerable to lateral movement. If this is the case, once a cybercriminal gains access to the production network, he can move laterally to the corporate network and exfiltrate confidential documents or activate ransomware.

**Cymulate continuously discovers discrepancies and provides remediation guidance so that manufacturers can reduce risk by closing gaps and ensuring there is no way to move from the production network to the corporate IT network.**

### Attack-Based Vulnerability Management

Cymulate's Attack–Based Vulnerability Management (ABVM) integrates with leading third-party vulnerability management solutions to enable organizations to accurately prioritize remediation and patching or reconfiguration of compensating security controls. Manufacturing companies can't keep up with remediating all the vulnerabilities in their environment—many do not have the personnel or the resources.

**Cymulate's Attack-Based Vulnerability Management helps these companies prioritize their vulnerabilities so they can save time and effort wasted on remediating vulnerabilities that can't be exploited in their environment.**

Cymulate

## Compliance Enablement

Cymulate enables organizations to comply with ISO 27001, GDPR, PCI and other federal or industry regulations requiring regular security testing. By proactively assessing their resilience to cyber-attacks and breaches, production companies can meet compliance mandates while becoming less dependent on manual testing methods. Every test is documented, effortlessly providing auditors proof of compliance to security testing mandates.

## Scaling Up Security for Every Manufacturing Organization

### Basic
(Prevent Security Stance)

**Simple to deploy and use**

- Automate security control validation and optimization
- Operationalize threat intelligence
- Prescriptive mitigation guidance

### Progressing
(Detect & Respond Security Stance)

**Comprehensive**

- Exercise incident response and threat hunting
- Rationalize security investments before and after
- Manage the attack surface, cyber and IT hygiene and prevent environmental drift

### Advanced
(Offensive Security Stance)

**Customizable**

- Leverage and scale in-house red-teaming
- Incorporate security validation into organizational risk management
- Continuous security assurance program

Cymulate's holistic approach with Extended Security Posture Management quickly delivers high value to industrial companies; the platform is simple and customizable for all skill levels. Cymulate helps prevent production shutdown, stop IP theft, manage efficient vulnerability patching, and meet compliance requirements. **Remove assumptions, prove you're secure with Cymulate XSPM.**

### 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