Extended Security Posture Management for Critical Infrastructure

Validate that your systems are protected from the next cyberattack

Cyberattacks have caught up to the critical infrastructure sectors and organizations today are vulnerable to attacks that can cause disastrous consequences for citizens, countries, and governments. For example, the well-known Colonial Pipeline ransomware attack impacted equipment that managed the pipeline, causing fuel shortages leading to high fuel prices, airline cancellations, and financial loss.

Cyber risk in these sectors are paramount and directly relate to:

This never-ending list of potential consequences takes a toll on organizations' security teams who are constantly fighting the next fire. Adding to the stress, an organization's security posture is affected by many different variables—both known and unknown. Between constantly changing threats, new and existing vulnerabilities, and the dynamic nature of today's enterprises, maintaining a robust security posture and keeping risk low seems to be a daunting task.

By switching from a reactive to a proactive approach, critical infrastructure organizations can predict if and how cyberattacks can evade their defenses and take measures to shore up the gap in a continuous and manageable fashion. They can mitigate risks, gain the maximum value of their cybersecurity spend, and clearly communicate to leadership the reduced risk trending over time.

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, critical infrastructure 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 nation state and criminal actor threats targeting the critical infrastructure sectors and others. By testing against these attacks and adversarial tactics and techniques, you can safely and comprehensively 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 the critical infrastructure sectors.

Security Posture Assessment

Attack Surface Management (ASM)

To challenge reconnaissance efforts, 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.

The critical infrastructure sector is especially susceptible to attacks because of the large attack surface that contains both Operational Technologies (OT) and Information Technologies (IT). These technologies increase risk because they are usually configured with legacy protocols and minimal security features that are easy to exploit.

Companies 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 or from leveraging the IT corporate network to gain access to the IoT and OT devices.

Infrastructure Resilience & Segmentation Policies

Cymulate's Lateral Movement module 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 validatio 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 critical infrastructure organization may segment or airgap 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. Alternatively, if a cybercriminal gains access to the corporate network, he can move laterally to the production network and wreak havoc on citizens, a government, or an entire country, depending on the sector of the organization.

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

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. By doing so, critical infrastructure companies can keep up with remediating vulnerabilities in their environment without the stress to personnel or 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.

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!

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