

# Checklist for Extended Security Posture Management (XSPM) Solution



When shopping around for either Breach & Attack Simulation (BAS), Continuous Security Validation (CSV) or Extended Security Posture Management (XSPM) solutions, there are a few must-have features and characteristics to ensure you are getting most value.



## Deployment

Deployment may be happening only once, but the required deployment process says a lot about the XSPM solution agility and efficiency.

**As a rule, the deployment should be:**

**Simple:** Regardless of your organization's size, deploying an XSPM solution should not take more than one hour, two at most

**Light:** Low consumption of computing resources i.e, no latency or impact on business data transactions

**OS Agnostic:** It should work equally well on any Operating System, without requiring any tweaking

**Small Footprint:** One agent per environment should be amply sufficient.



## Security Validation

In order to be truly extended, a security posture management solution needs to cover a lot of ground. More specifically, an XSPM solution has to provide, at minimum, the following services:

### Breach and Attack Simulation (BAS)

BAS is a service recreating and emulating real-world attacks and launching production-safe attack campaigns against your environment.

Those are listed below in three categories covering the features and capabilities key to end-to-end security validation and Extended Security Posture Management – Deployment considerations, Security Validations and Management – these are summarized in a downloadable checklist table.

### A complete BAS service should:

**01** Continuously validate the security of your:

#### Email Gateway

Checks the resilience of email security controls preventing malware and email and security, policy enforcement and optimize email gateway configuration

#### Web Gateway

Challenges the secure web gateway and web proxy efficacy, identifies security gaps and provides mitigations recommendations.

#### Web Application Firewall (WAF)

Challenges WAF security resilience to web payloads and assists in protecting web apps from future attacks.

#### Endpoint Security

Tests endpoint security against all Mitre ATT&CK TTP scenarios, evaluates endpoint protection efficacy, and optimizes signature and behavioral detection-based endpoint security efficacy.

**02** Continuously validate that you are protected against:

#### Data Exfiltration

Launches production-safe attempts to exfiltrate synthetic sensitive and critical data through methods such as abuse of network services, cloud-based services, and USB/removable devices and optimizes data protection.

#### Emerging Threats

Leverages Immediate Threat Intelligence knowledge to launch simulated attacks with the latest uncovered methods and prioritizes vulnerability patching to match the vulnerability sensitivity to emerging threats.

### Full Kill Chain APTs

Simulates full kill chain APT attack scenarios of known APT groups and/or template-based custom-made scenarios to assess weaknesses and security gaps across the full kill chain that are vulnerable to APT attacks. Then provides detailed recommendations to optimize security controls and processes to detect and mitigate APT attacks.

### Continuous Automated Red Teaming (CART)

CART is the automation of the ethical hacking techniques formerly operated by red teams. It should comprise at least 3 modules:

#### Attack Surface Management (ASM)

The ASM module maps customer-owned assets exposed to the Internet and identifies security gaps such as CVEs, misconfigurations, data leak, darknet posts and more, any of which can be spotted by a hacker running a recon.

#### Phishing Awareness

This module launches phishing and spear-phishing campaign to evaluate employees phishing awareness and email gateway efficiency

#### Lateral Movement

This module deploys attack techniques, tools and methods used to gain access, elevate privileges, and spread across systems, following the initial compromise of a single endpoint. After assessing the attacker's ability to propagate within the network, it improves the resilience to lateral movement through a combination of segmentation enforcement, infrastructure misconfigurations correction and improved IT hygiene.

### Purple Team Framework

#### A purple team framework should:

- Enable Blue Team to test both SIEM/SOAR detection and security control efficacy
- Comprehensively cover Mitre ATT&ACK attack scenarios
- Instrumentalize both custom and template additional scenarios
- Correlate findings with SIEM/SOAR and security control solutions through API integrations

### Overall Characteristics

These validation features and modules should:

- Be capable of running continuously without disrupting operations
- Enable baselining and trending
- Include detailed and easy-to-follow remediation/mitigation recommendations

*“If you can't measure it, you can't improve it.”*

Peter Drucker



## Management

In addition to those services, it should include management tools to optimize the services use and maximize their potential outcomes, both in terms of security posture hardening and of reporting clarity, customizability and comprehensiveness. It should include.

### Attack-Based Vulnerability Management

Prioritizing the patching order of the vulnerabilities uncovered through the continuous security validation features is a critical part of Extended Security Posture Management. Automating and continuously updating the patching schedule requires analyzing uncovered vulnerabilities through the lens of the actual risk they pose.

### Automated detailed report generation

Timely reporting is crucial to maintaining and sharing up-to-date information. Automating the report creation to include relevant data requires report templates that can be customized to specific recipients. At a minimum, there should be 2 default reports templates: Technical and Executive.

### Analytics for Decision Support and Continuous Improvement

Evaluating the security posture and its improvement over time requires the ability to measure several factors:

- Percentage of attacks blocked
- Tool usage efficiency
- Overlap between solution
- Tool stack ROI
- Variance from baselines
- Other

### These measurements should enable:

- Evaluating the cybersecurity tool stack to know what tools to keep and optimize and what tools are missing
- Quantifying and documenting the existing risks and ways to reduce them
- Guarantying a graceful recovery




### 3rd party integration

To provide optimal results, your XSPM solution needs to easily integrate with existing solutions such as those used for SIEM, SOAR, EDR, DLP etc. Running a comprehensive assessment will surface gaps in processes and technologies that APIs

providing visibility, automation and prioritization are essential to quick remediation.

With a comprehensive Extended Security Posture Management solution, not only is the cybersecurity staff able to focus on real, immediate threats to the environment, they can also strategize based on accurate, precise data and optimize the use of exiting tools.

Download the attached checklist table for Extended Security Posture Management to ensure the solution you are looking at includes all the necessary capabilities and features.

 <h3>Deployment</h3> <ul style="list-style-type: none"> <li><input type="radio"/> Simple</li> <li><input type="radio"/> Light</li> <li><input type="radio"/> Low consumption of computing resources i.e., no latency or impact on business data transactions</li> <li><input type="radio"/> OS Agnostic</li> <li><input type="radio"/> Small footprint</li> </ul>	 <h3>Validation Features</h3> <ul style="list-style-type: none"> <li><input type="radio"/> Breach and Attack Simulation (BAS) <ul style="list-style-type: none"> <li>• Email Gateway</li> <li>• Web Gateway</li> <li>• Web Application Firewall (WAF)</li> <li>• Endpoint Security</li> <li>• Data Exfiltration</li> <li>• Emerging Threats</li> <li>• Full Kill Chain APTs</li> </ul> </li> <li><input type="radio"/> Continuous Automated Red Teaming (CART) <ul style="list-style-type: none"> <li>• Attack Surface Management (ASM)</li> <li>• Phishing Awareness</li> <li>• Lateral Movement</li> </ul> </li> <li><input type="radio"/> Purple Team Framework</li> </ul>	 <h3>Management Features</h3> <ul style="list-style-type: none"> <li><input type="radio"/> Attack-Based Vulnerability Management</li> <li><input type="radio"/> Automated detailed report generation</li> <li><input type="radio"/> Analytics for Decision Support and Continuous Improvement</li> <li><input type="radio"/> 3rd party integration</li> </ul>
--	--	--

## About Cymulate

With a Research Lab that keeps abreast of the very latest threats, Cymulate proactively challenges security posture end to end, automatically and continuously, allowing hyper-connected organizations in all maturity levels to avert damage and stay safe. Founded by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is trusted by hundreds of companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision to be the gold standard for security professionals and leaders to manage, know and control their Cybersecurity Posture. Today it's simple for anyone to protect their company with the highest levels of security. Because the simpler cybersecurity is, the more secure your company-and every company-will be.

Contact us for a live demo, or get started with a free trial

[Start Your Free Trial](#)