SOFTPROM

Cymulate
Extended Security Posture Management

Exploring the Cymulate Edge

How Targeted Cyberattack Simulations Differ from Penetration Tests & Vulnerability Scanning

Table of Contents

01 | Introduction

Organizations of all shapes and sizes are fighting a war against threat actors. As we have seen in recent years, cyber-attacks have become more sophisticated, making them harder to detect and mitigate.

Today, vulnerability scans and penetration tests are the main methods relied upon by CISOs, and organizations in general, to verify that their infrastructure and their data and IP are protected. The risk assessment these methods generate might satisfy compliance regulators, but they fail to accurately picture the organization's actual security posture, especially against emerging threats, multi-vector attacks and APTs.

To effectively protect the infrastructure against the rising tide of cyber-attacks, the best option is to integrate comprehensive offensive testing and run a wide range of production-safe simulated targeted attacks. Those simulated attacks can focus on the infrastructure's security control or the entire kill chain resilience.

Modules running attack scenarios designed to test security controls are known as Breach and Attack Simulations (BAS), described by Gartner as a "tool that helps make security postures more consistent and automated."

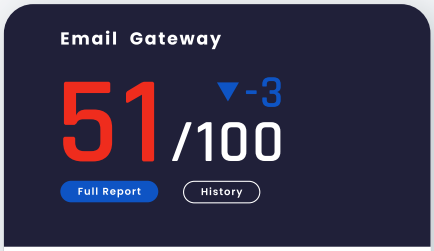
Module checking the full kill chain ability to detect, block or mitigate penetration, lateral movement, and escalation from the initial foothold to command execution, are Continuous Automated Red Teaming (CART).

Organizations with highly complex infrastructures and unique security needs can complement these two modules with a purple teaming framework that enables customizing attack scenarios and campaigns templates to cover atypical areas.

How it works

Cymulate facilitates managing your security posture 24X7X365 within minutes and based on facts, in just three simple steps:

1 Simulate
Simulate attacks across any vector.



2 Evaluate
Know where your company is exposed.

3 Remediate
Fix your security gaps.

02 | Classic Detection Techniques

Classic detection techniques still have some use, but as they are rooted in a time that precedes the adoption of AI/ML techniques by cyber-attackers, they can at best be contributing element to a comprehensive security framework or should be replaced by a better performing tool carrying out the same task in a more comprehensive and resource effective manner.

01 Vulnerability Scans

Performed by proprietary or open-source applications, vulnerability scans check the environment for vulnerabilities.
However, their search capabilities are limited to vulnerabilities already known to vendors and the industry, and to weaknesses already exploited by cyber-attackers. Vulnerability scanners typically scan networks and systems for thousands of security vulnerabilities of any variety, from software bugs and missing operating system patches to vulnerable services, insecure default configurations, and web application vulnerabilities.
They then generate a report listing all the detected vulnerabilities, ideally affecting a risk score to each uncovered vulnerability. These scores are typically based on CVSS scores.

A patching schedule based on these scores and on define risk tolerance baselines is then passed on to the IT team to apply the required patches.

Pros

- Automated, can be scheduled, easy to use
- Detects known vulnerabilities
- Fast, results available within a few hours
- No special expertise required
- Includes latest exploits
- Possibly more effective than pen testing
- Option to run multiple scans simultaneously

Cons

- Only detects known vulnerabilities or threats
- Fails to detect misconfigurations or misuse
- No comprehensive process overview. Resulting snapshot lacks substantial insights
- High rate of false positives – 30% to 60%
- No adversary threat scenario
- Uploads require Internet connection
- Designed for non-critical system - Insufficient for critical system
- Potentially causes downtime

02 Manual Penetration Tests

Pen testing is conducted by human testers (in-house or outsourced) who attempt to evaluate the security of an organization's infrastructure by safely exploiting vulnerabilities. Those vulnerabilities may be present in operating systems, services, or applications, resulting from faulty configuration or caused by careless end-user behavior.

In other words, the corporate network, application, devices, and/or people are attacked to check whether a cyber-attacker would be able to penetrate the organization. The tests reveal how deep an attacker could penetrate and if the attack payload could be executed, i.e., data exfiltration, file or system encryption, infrastructure disablement or destruction.

Pros

- Identifies security gaps missed by vulnerability scans
- Can identify full kill chain attack path
- Possibility of testing specific emerging threats on-demand
- Report can be as detailed as required
- Can be used for training purposes

Cons

- Performance linked to individual skills
- Test scope limited
  - Pen testers select which tactics and techniques to test – no comprehensive testing
  - Manual process
  - Unable to test every aspect of the system (e.g., lines of code, decompiled
- Snapshot of a point in time – no continuous evaluation
- Assessment report delivered up to 2 months after test
- Costly

03 Red Teaming

Red teamers are running simulated attacks across the full kill chain, including through using seemingly unrelated exploits. Their pro-active goal based adversarial actions provide a view of the organization infrastructure from the perspective of an attacker. Multi-step attacks are used to simulate various types of adversaries, and for identifying gaps in information security controls. They also provide valuable insights about your organization's ability to identify attacks in progress and remove them from the environment.

Pros

- Mimics the tactics, techniques, and procedures (TTPs) deployed by real attackers
- Simulates real threat scenarios
- Proactive
- More cost effective than penetration testing
- Can identify unknown vulnerabilities
- Gives insights into security posture, and into SecOps and monitoring efficacy

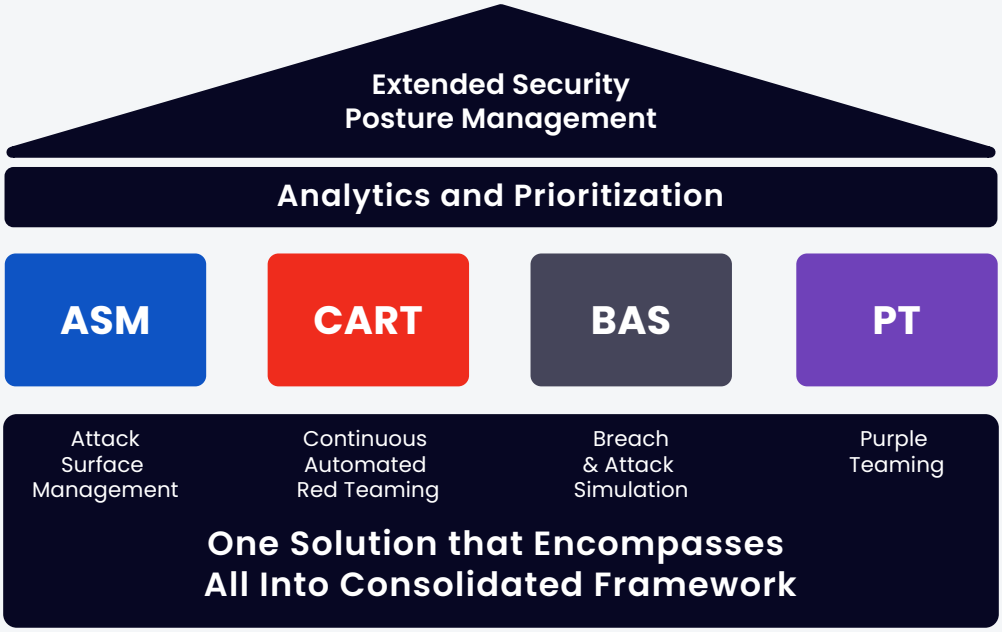
Cons

- Resource heavy
- Requires in-house or outsourced expertise
- Typically conducted annually or bi-annually unable to reassess security posture in sync with environment updates or modifications
- Manual process might lead to inconsistencies
- Inconsistencies between testing routines affects assessing security posture performance over time

03 | The Extended Security Posture Management (XSPM) Approach

Cymulate's Extended Security Posture Management (XSPM) approach combines Breach & Attack Simulation (BAS) and the Continuous Automated Red Teaming (CART) advantages and enriches them with a purple team framework that provides customizable attack templates to fine-tune testing further when appropriate. While BAS provide insight into security control misconfigurations and security gaps with the help of a lightweight single agent per environment,

CART uses an outside-in approach providing a 360° view from an attacker's perspective across the full kill chain and including for operationalized Immediate Threats Intelligence campaigns.
Cymulate's platform interactive single-pane-of-glass dashboard includes actionable mitigation recommendation, the possibility to visualize the attack on a MITRE or NIST Kanban view and access to granular detailed information about each finding.



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 constantly 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