

# How Cyberattack Simulations Differ from Penetration Tests & Vulnerability Scanning

And why continuous security validation  
is key for the Financial industry



# Table of Contents

Glossary .....	3
01   Introduction .....	4
02   Vulnerability Scans .....	5
03   Manual Penetration Tests .....	6
04   Targeted Simulated Attacks .....	7
05   The Cymulate Approach .....	8
06   About Cymulate .....	10

# Glossary

APT | Advanced Persistent Attack

CISO | Chief Information Security Officer

GDPR | EU General Data Protection Regulation

CCPA | California Consumer Privacy Act

SIEM | Security Incident and Event Management

SOC | Security Operations Center

WAF | Web Application Firewall

# 01 | Introduction

The Banking industry places a lot of attention on cybersecurity as they continue to develop on-line services and adopt new technologies to cut costs and streamline operations. In addition to this, they must comply to privacy regulations such as European Union's General Data Protection Regulation and the California Consumer Privacy Act. These trends place even more emphasis on a Bank or other financial institution to protect their digital assets from threat actors and cybercrime, and continuously validate the effectiveness of their security controls and overall security performance. As we have seen in recent years, cyberattacks have become more sophisticated, making them harder to detect and mitigate. Current methods used by banks (and their CISOs) to verify that their systems and data are protected, are vulnerability scans and penetration tests.

As explored below, vulnerability scans and penetration tests are useful for getting insight into the security posture of an organization at a specific moment in time. However, they do not present the full picture of an organization's security posture; especially when it comes to more sophisticated, multi-vector attacks. The most effective way for an organization to test its resilience against the growing wave of cybercrime, is to opt for targeted attack simulations that use multi-vector simulated attacks.

These kinds of simulations are also known as Breach & Attack Simulations (BAS). Gartner has asserted that, "Security testing is so challenging for technical professionals focused on security operations that many don't try it. Breach and attack simulation tools help make security postures more consistent and automated."



## 02 | Vulnerability Scans

[Vulnerability scans](#) are performed by an application that may either be proprietary or open source. This app checks for vulnerabilities that are already known to vendors and the industry, or for weaknesses that have already been exploited by cybercriminals. Thousands of different security vulnerabilities in networks or host systems are scanned, such as software bugs, missing operating system patches, vulnerable services, insecure default

configurations, and web application vulnerabilities. The scans are used to assist automating the security auditing process of an organization's IT.

By scanning networks and websites for thousands of different security risks, vulnerability scans can automate security auditing and be a central part of an organization's IT security. The resulting list of vulnerabilities to be patched can be used to remediate them.



### Benefits

Automated, can be scheduled, easy to use

Detects known vulnerabilities

Fast, capable of producing results within a few hours

Does not require any special expertise

The latest exploits are uploaded

Could be more cost effective than pen-testing

Ability to perform multiple scans simultaneously



### Disadvantages

Lack of process overview. It provides only a snapshot, and does not give substantial insights

Cannot detect vulnerabilities that have not been mapped yet. The time between updates leaves organizations exposed


Produces a high rate of false positives [\(estimated at 30% - 60%\)](#)

It lacks an appropriate adversary model threat scenario

Uploads require internet connection

Meant for non-critical systems; far less for critical real-time systems.

Could put stress on the production environment which may result in downtime

 A vulnerability scan can only find a known vulnerability or threat. Since mitigation only entails updating and

patching the system, misconfiguration or misuse of the infrastructure and the security solutions will not be mitigated.

## 03 | Manual Penetration Tests

Manual [penetration testing](#) (or pen-testing) is conducted by human testers (in-house or outsourced to a 3rd party) 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, applications, devices, and/or people are attacked to check if a hacker would be able to penetrate the organization. The tests also reveal how deep an attacker could penetrate and how much data could be stolen or exploited.



### Benefits

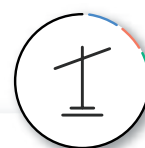
Identifies weaknesses that vulnerability scans do not detect

Identifies selected high-risk weaknesses

The pen-tester can learn about a new attack technique and test it the very next day

The assessment report can be used to mitigate weaknesses

Provides a training tool for network security



### Disadvantages

Success depends on the skill and expertise of each individual tester

Does not identify all weaknesses that threat actors exploit due to the limited testing environment

The tester cannot perform all the attack methods that he/she has learned during previous years

It takes a long time (weeks, sometimes even more than a month) to receive the assessment report

Does not provide 360° insight, since manual testing is unable to test all aspects of the system (e.g. lines of code, decompiled Assembly, web pages and parameters, web services, etc.), in contrast to automated tools

The results of manual pen-tests reflect a specific point of time. Often, they are not performed due to high costs

## 04 | Red Teaming

Targeted simulated attacks, also known as red teaming or attacker simulation, are gaining popularity - and for good reason. Letting you take a proactive approach, apart from identifying weaknesses in the organization's security posture, they can also provide valuable insights about your organization's ability to identify attacks in progress and

remove them from the environment. Multi-step attacks are used to simulate various types of adversaries, and for identifying gaps in information security controls through simulation optimization.



### Benefits

Mimics the tactics, techniques and procedures (TTPs) deployed by real attackers

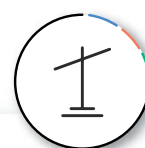
Prepares for real world cyberattacks by executing simulated attacks for given threat scenarios

Proactive approach

More cost effective than manual testing

Detects unknown issues at unknown locations

Enables evaluating security operations / monitoring capabilities



### Disadvantages

Simulations must be conducted regularly

Requires in-house or outside expertise

Extent of effectiveness may be difficult to assess by CISOs and IT teams due to lack of consistency between one engagement to another

Requires significant resources, wether outsourced or conducted in-house

Due to lack of end-to-end automation, exercises are difficult to repeat in a consistent manner

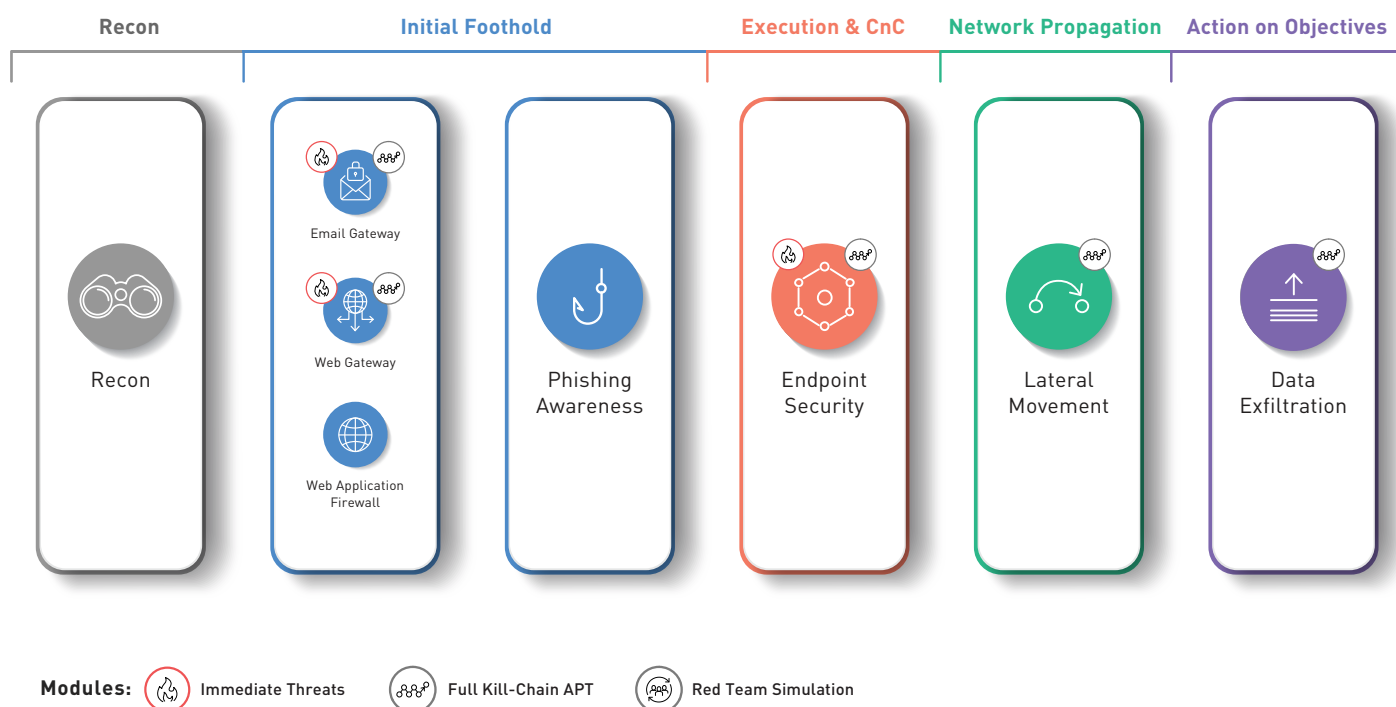
Diffucult to assess the impact of changes to the environment on posture and track security performance over time

# 04 | The Cymulate Approach

Cymulate's Breach & Attack Simulation (BAS) platform takes targeted simulation attacks one step further by measuring the organization's true preparedness to handle cybersecurity threats effectively. Using an offensive approach, Cymulate exposes critical vulnerabilities by simulating multi-vector cyberattacks from an attacker's perspective. This sophisticated plug & play platform simulates and tests attack vectors by impersonating

hackers, state-sponsored threat actors, and even rogue insiders before an actual attack takes place and exploits any weaknesses. The SaaS simulations can be run on-demand at any time and from anywhere without impacting the users or infrastructure. With Cymulate's Red Team capabilities, organizations can continuously test their cybersecurity posture against cyberattacks, global cybercrime campaigns and targeted [APTs](#).

## End to end security validation





## Features

## Benefits

### Pre-Exploitation



#### Immediate Threat

Test your organization's security posture against clear and present cyber danger



#### Email Gateway

Test your organization's security posture against clear and present cyber danger



#### Web Gateway

Test the organization's HTTP/HTTP Southbound exposure to malicious websites



#### Web Application Firewall

Test the organization's HTTP/HTTPS outbound exposure to malicious website



#### Recon

Perform continuous reconnaissance on your organization to identify exploitable information and weaknesses

Continuous security validation against the very latest in-the-wild threats

Simulates the broadest range of attack vectors in the industry, providing a comprehensive assessment

Provides 360° insight pre- and post-exploitation and awareness

SaaS solution, no hardware required

Remediate the intelligence and weaknesses an adversary can gather on your organization prior to an attack

### Post-Exploitation



#### Data Exfiltration

Test the organization's outbound critical data safely before sensitive information is exposed



#### Lateral Movement

Test the organization's Windows domain network configuration using a sophisticated lateral movement algorithm

Immediate results 24x7x365

Mitigates attacks before they happen

### Exploitation



#### Endpoint Security

Test if the organization's endpoint solutions are properly tuned to protect against the latest attack vectors



#### Phishing Awareness

Test employees' awareness of phishing campaigns with advanced, customizable simulations



#### Full Kill-Chain APT

Test the SOC team's incident response by launching pinpointed full Kill-Chain APT simulations

Excellent ROI and reduced TCO of the organization's cybersecurity investment

Immediate results 24/7/365

Fully automated and customizable blue-team exercises to assess effectiveness

## 05 | About Cymulate

Cymulate helps companies stay one step ahead of cyber attackers with a unique breach and attack simulation service that empowers organizations with complex security solutions to safeguard their business-critical assets. By mimicking the myriad strategies hackers deploy, the system allows businesses to assess their true preparedness to handle cyber security threats effectively.

Cymulate is trusted by companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision—to make it easy for anyone to protect their company with the highest levels of security. Because the easier cybersecurity is, the more secure your company - and every company - will be.



**Ready to Cymulate? Get started with a free trial**