Cymulate

Implementing Continuous Threat Exposure Management (CTEM)

Table of Contents

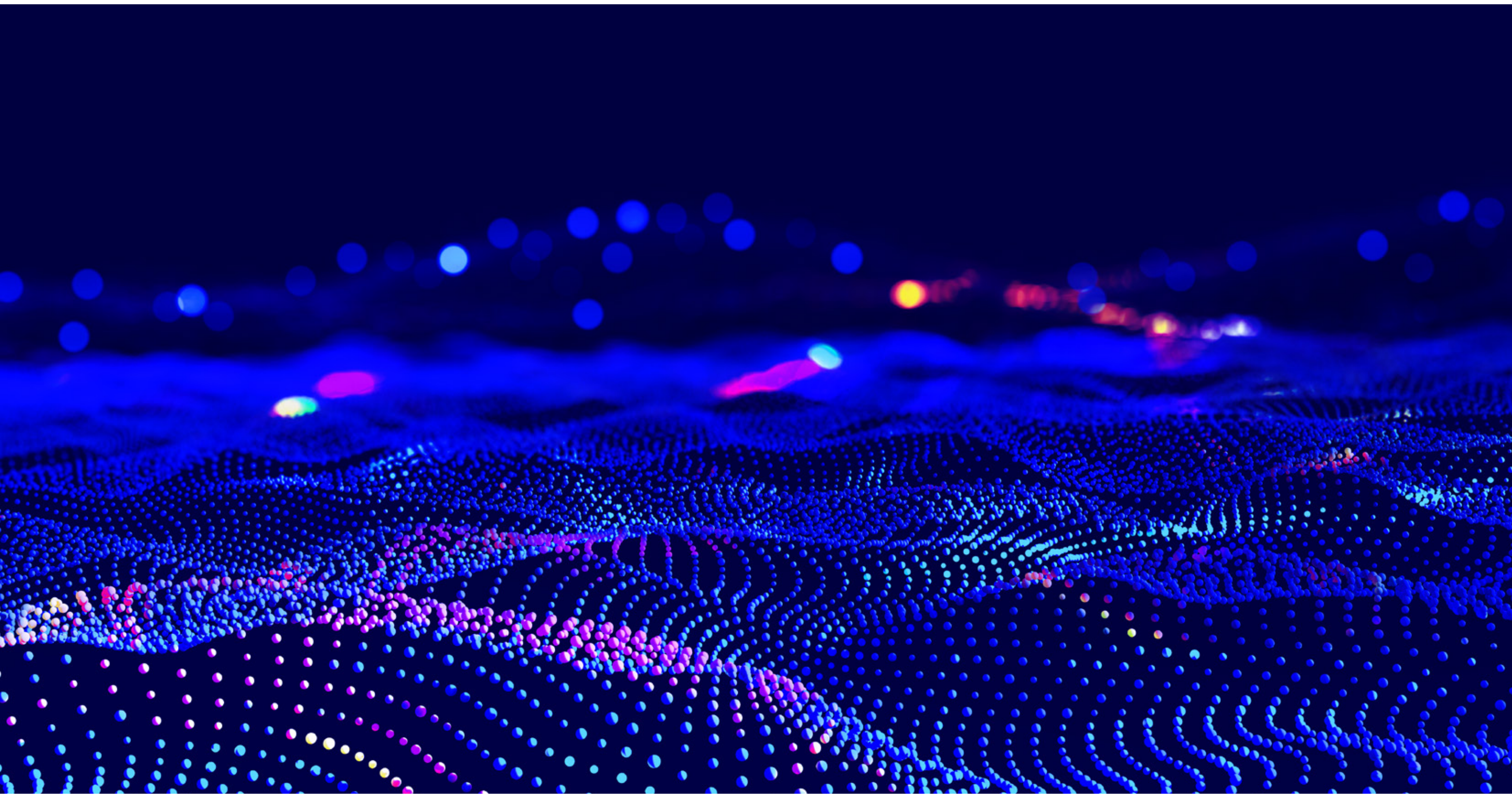
Introduction

Published in late July 2022, Gartner's Continuous Threat Exposure Management (CTEM) program is a new approach in the thinking process to achieve lasting and robust cyber resilience. When looking at the evolution of the threat landscape combined with the increased complexity of information networks, the ability to completely prevent cyberattacks is receding into the realm of dreams. This means that security practitioners' charter is to ensure that, when they happen, breaches are spotted, and threats are stopped or, alternatively, recover gracefully from a successful attack. The point is that preparations can be made ahead of time.

Continuous Threat Exposure Management is a concept that addresses the limitationof enterprise risk management frameworks by fostering proactive identification, evaluation, monitoring, and mitigation of vulnerabilities and security flaws across an organization's infrastructure in advance.

Expanding and refining the existing Threat Exposure Management approach, Gartner's CTEM is a recommended program aimed at shoring up resilience through the continuous management of threat exposure. Threat exposure can be defined technically, such as weaknesses in the infrastructure, or executively, such as a different understanding of business priorities and risk appetite/operationality ratio by the various departments. CTEM's goal is to reduce exposure by improving communication between technical, executives, and operational teams and ensuring that all technical findings are validated through adversarial procedures.

Cyber resilience is becoming the most likely future norm in planning information security strategies. It is already appearing in leading thought leadership platforms such as the World Economic Forum and updated compliance regulations such as the recent update to PCI DSS v4.0. The holistic nature of Gartner's CTEM program is designed to avoid inter-department communication gaps and addresses a comprehensive range of cyber resilience aspects. Implementing CTEM, if done correctly, is the optimal way to achieve and maintain lasting and robust cyber resilience.



Breaking Down CTEM

Practically, the Continuous Threat Exposure Management program is a repeating cycle of five successive steps spread over two main stages. The cyclic nature of CTEM is meant to ensure both comprehensive coverage of the entire infrastructure and continuous resilience improvement. Schematically, the cycle covers two main aspects: **Diagnose and Action.**

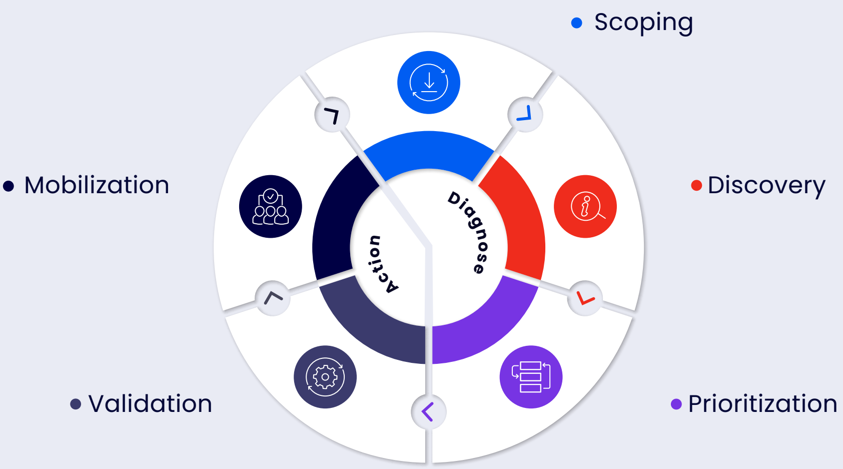
Though every cycle should cover each and every step, the trigger to initiate a new cycle might stem from a source related to any of the "Diagnose" stage's three steps – scoping, discovery and prioritization, and the "Action" stage, with the validation and mobilization steps.

A. Diagnose – This stage is when the identification and mapping of priorities and weaknesses take place:

- **Scoping** – Mapping the external attack surface, listing all digital assets, evaluating their operational values, and conveying that value to all stakeholders so that both technical and executives people understand which assets are defined as high impact.
- **Discovery** – Uncovering environments' security gaps (such as vulnerabilities and misconfigurations) and their risk profile, and, ideally, mapping them to assets for easy prioritization.
- **Prioritization** – Identifying and addressing the security gaps most likely to be exploited by cyber-attackers based on an adversarial perspective and correlating the findings to high-impact assets from an organizational or business point of view.

B. Action – This stage is when the security posture is tested, and corrective measures are taken:

- **Validation** – The validation step is tasked with a triple objective:
  - Assess attack success likelihood.
  - Evaluate the attack damage potential beyond gaining an initial foothold.
  - Verify the effectiveness of the detection and response existing array.
  - There are several methods to reach those objectives, including Attack Surface Management (ASM), Continuous Automated Red Teaming (CART), Attack Path Mapping, and Breach and Attack Simulation (BAS).
- **Mobilization** – Setting up and implementing a remediation program that combines automated and manual remediation and is defined in collaboration between tech and executive departments to ensure optimal coordination between operational and security needs.



Implementing CTEM with Cymulate

Gartner's CTEM approach is eerily like the line of thought that has been driving the Cymulate Platform since its inception.

What is the Cymulate Exposure Management and Security Validation Platform?
The Cymulate Platform, is a comprehensive security validation platform. In a nutshell, Cymulate runs an extensive array of off-the-shelf and/ or customized emulated attacks that test the resilience of an organization's security posture. Cymulate provides an exact percentage of attacks that evaded detection and/or mitigation compared with those detected and/or stopped by the existing defensive array. As a modular system, the Cymulate Platform can be integrated by organizations of a wide range of size or maturity levels but enables access for all to a quantified evaluation of the organization's security resilience.

Even though Cymulate's automations cover the entire MITRE TTPs list, its advanced purple teaming framework enables the easy creation of additional attack templates that can be created with an easy drag-and-drop type interface. Designed to facilitate communication between the board and the technical teams, the dynamic dashboards can be used to customize the data included in the automatically technical and executive reports and are even integrated with a ticketing system to accelerate mitigation.

What Makes CTEM and Cymulate a Perfect Fit?
This section will take a look at CTEM and its congruity with the Cymulate approach.

A **Diagnose** – Divided into three steps, CTEM's first stage aims to identify all relevant factors in a way that will facilitate communication between executives and tech people and ensure they speak a common language.

The diagnose stage is composed of three steps:

01 Scoping

The first step of Gartner's CTEM cycle is to define which infrastructure segments will be included in the process. Even though the CTEM cycle is designed to improve cyber resilience, the scoping process should not be defined exclusively by IT or SOC (Security Operations Center) teams. Still, it should be understood as the first step for cross-unit collaboration.

The scoping process is an opportunity for executives and security people to quantify risk appetite and establish security baselines that can be used to monitor trending in successive cycles. Ensuring collaboration between tech and non-tech teams at this stage is key to eliminating traditional communication issues and preventing interdepartmental tensions and conflicts. On the technical side, Gartner's CTEM recommends going beyond the traditional reactive approach and scoping from the attacker's perspective by mapping the external attack surface.

Cymulate's Attack Surface Management (ASM) is ideal for performing the technical part of scoping by discovering, documenting, and assessing the resilience of the organization's assets. The metrics ASM provides are also of considerable value for rescoping after the end of the first cycle. Equipped with quantified risk values that can be directly associated with relevant organizational segments and compared with each segment's risk tolerance level, the rescoping process is far more likely to adhere to the organization's overarching goals.

02 Discovery

The discovery stage is characterized by mapping the infrastructure and assessing its internal resiliency.

Once the CTEM scope has been defined in terms of business or organizational goals, the CISO or SOC leaders need to map the matching segment of the infrastructure, network, app, or data to cover:

- Drawing up a comprehensive inventory of all assets and components
- Mapping all the ways they are interconnected and all connections with other segments or outside the organization network
- Correlating the above with matching business implication

Again, Gartner insists that exposure discovery goes further than simply listing vulnerability and must include verifying the resilience of security controls and assets configurations and even phishing tests.

Cymulate's Breach and Attack Simulation (BAS) solution emulates a comprehensive array of attack scenarios, including all MITRE ATT&CK TTPs, to assess security controls resilience and map the existing detection and response tools' efficacy by shining a light on undetected or unmitigated emulated attacks. The Cymulate phishing solution identifies the people most likely to benefit from additional phishing awareness training.

03 Prioritization

Once the mapping process is completed, task prioritization and risk tolerance definition can occur.

Based on the business priorities defined in the scoping stage and the specifics of the information system segment or section covered, the CISO or the SOC leaders define mission-critical data and processes, their respective value or degree of sensitivity, and how essential they are to support the business objectives or any other criteria specific to the organization.

Again, the ability to evaluate risks for each considered segment based on accurate, validated, and quantified data facilitates the prioritizing process. Cymulate's assessment can be scheduled to run automatically at any frequency and does not require any business interruption. This means that the CISOs or SOC leaders have continuous access to the up-to-date security scores of each active module.

This continuously up-to-date data facilitates both affecting resources where they have the most significant impact and documenting the rationale behind the decision in terms easily understandable by non-tech people.

B Action

The Action Stage is composed of two steps.

01 Validation

The validation step collates all the information collected during the "Diagnose" stage steps. It requires implementing various techniques, from penetration testing or red teaming to breach and attack simulation and attack route mapping and analysis, to cover the complete attack gamut, from gaining an initial foothold to acquiring crown jewels or executing commands.

The Cymulate Platform is the only SaaS (Software as a Service) that unites all the technologies needed to achieve all CTEM validation objectives under a single pane of glass. The modular platform includes attack surface management, security control validation, full kill chain red teaming campaigns, purple teaming framework, and dynamic dashboards with customizable reporting and integrated ticketing for mitigation processes.

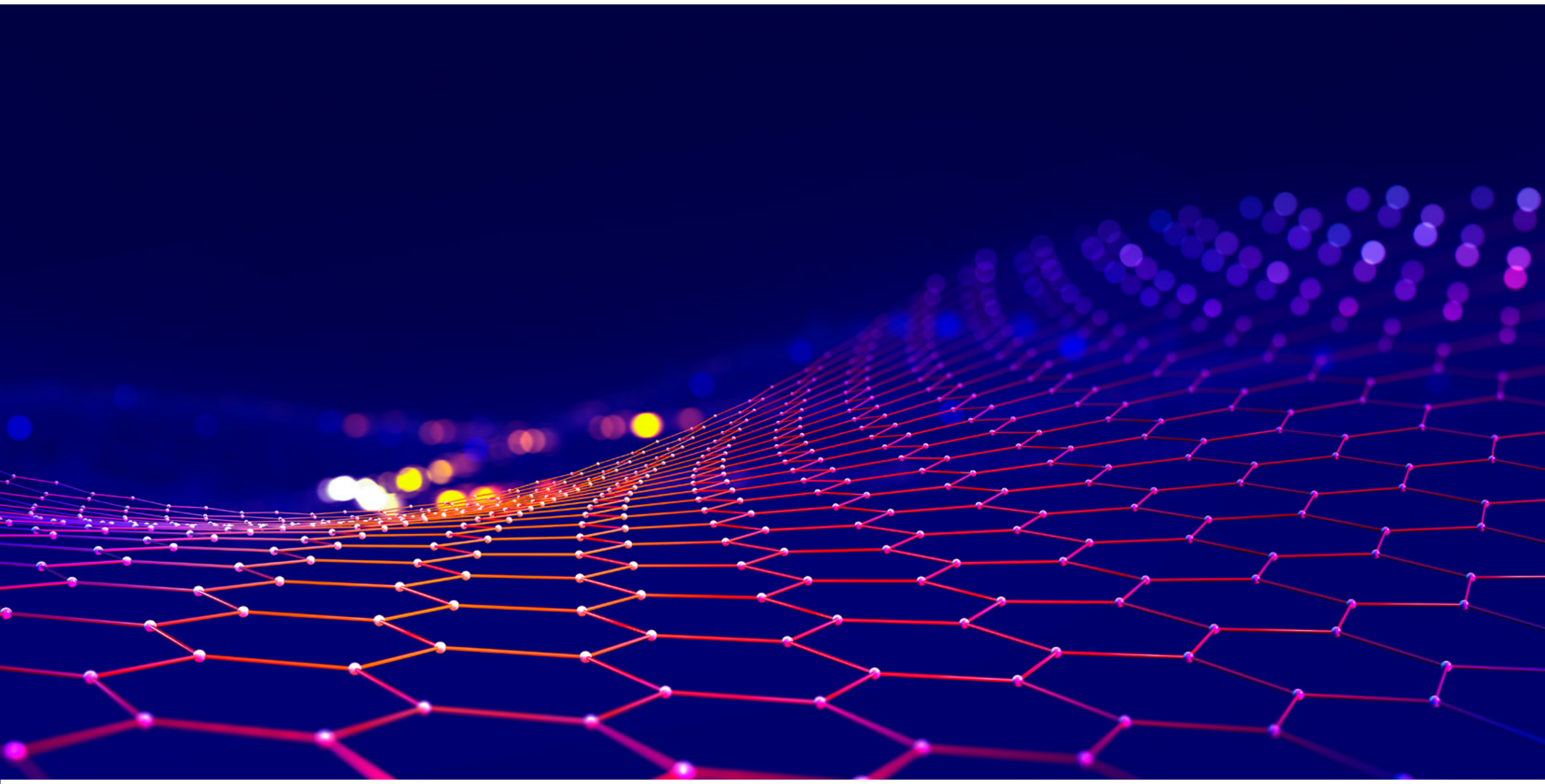
In addition, it includes an attack-based vulnerability management module to optimize vulnerability patching in terms of prioritization and workload reduction and maximize mitigation impact.

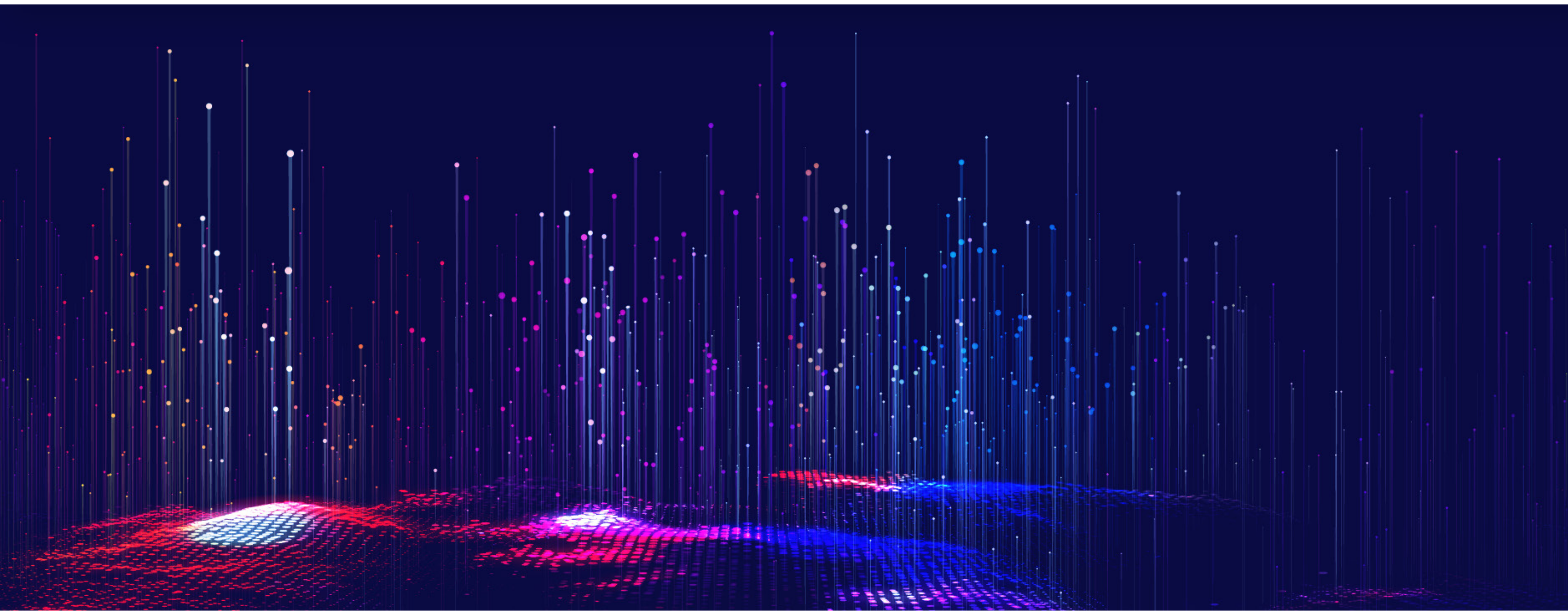
02 Mobilization

Gartner defines the mobilization step as the step during which corrective measures are taken. At Cymulate, for the validation stage to positively affect an organization's security posture, it is imperative to integrate the outcomes of the validation process into the mitigation process, so taking corrective measures must be as smooth and swift as possible.

The Cymulate Platform drastically accelerates the mitigation process:

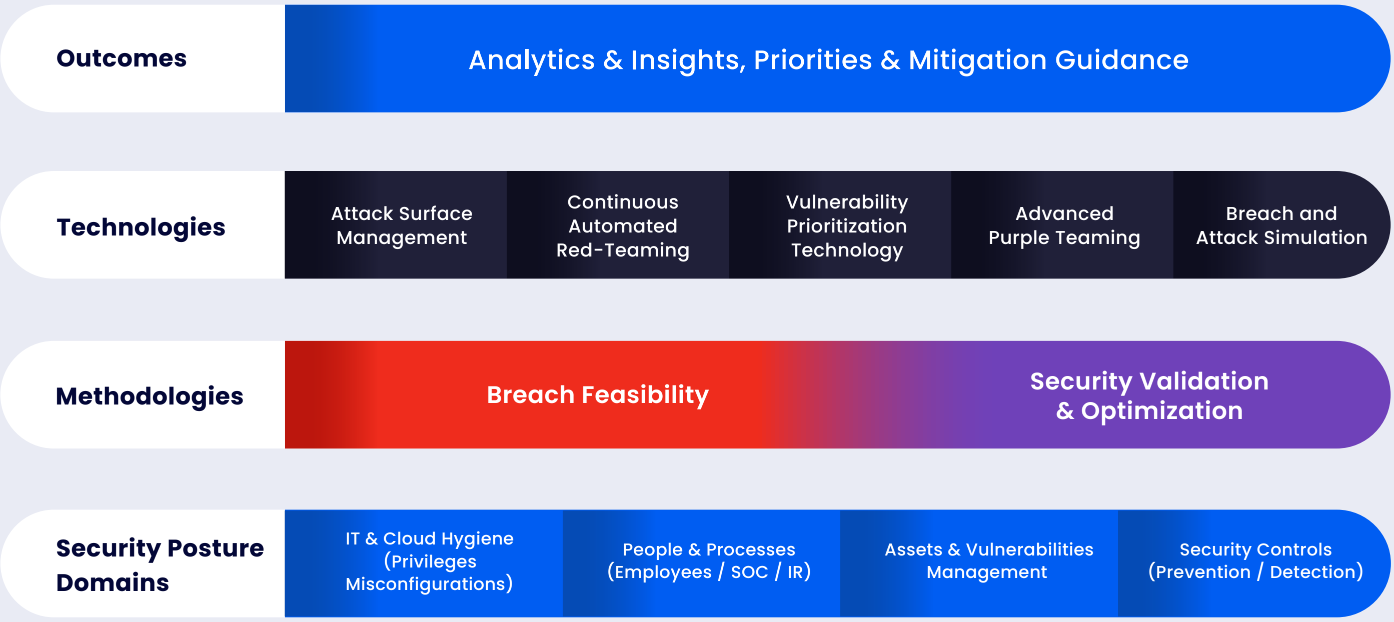
- The ABVM capabilities ensure optimal vulnerability patching prioritization and workload reduction.
- Validation of all used technologies outputs is displayed in Cymulate's single pane dynamic dashboards, giving an immediate view of the global and granular security posture.
- Actionable mitigation guidance, including pre-encoded sigma rules, is available for uncovered security gaps.
- Off-the-shelf analytic dashboards can be customized to include the sets of data relevant to the technical team or the executive board, and reports can be generated at a click.
- The integrated ticketing service makes communication between SOC and IT teams tasked with mitigation immediate and comfortable.





A Closer Look at Cymulate's Flow and How it Integrates with CTEM

Let's have a closer look at how the Cymulate Platform's basket of technologies is ideally suited to perform, or even outperform, the CTEM program. The visual above provides an immediate understanding of the breadth of the platform, aligning the different aspects both horizontally, in a listing fashion, and vertically to indicate how they relate to each other.



Outcomes

Analytics & Insights, Priorities & Mitigation Guidance

Technologies

Attack Surface Management

Continuous Automated Red-Teaming

Vulnerability Prioritization Technology

Advanced Purple Teaming

Breach and Attack Simulation

Methodologies

Breach Feasibility

Security Validation & Optimization

Security Posture Domains

IT & Cloud Hygiene (Privileges Misconfigurations)

People & Processes (Employees / SOC / IR)

Assets & Vulnerabilities Management

Security Controls (Prevention / Detection)

Let's break it down from the bottom up.

A Security Posture Domains

This layer describes the various security domains attackers can attempt to gain an initial foothold and escalate an attack through five main channels.

Security Posture Domain	CTEM Related Steps	Description
Security Controls	Discovery & Validation	Inadequately configured security controls can be leveraged by cyber attackers to either gain entry or to further their attack within an organization's infrastructure. With a continuously shifting environment due to business or organizational requirements that translate into frequent deployments, new misaligned configurations are at high risk of creeping in at any time.
People & Processes	Discovery & Validation	Poor response time during an incident and tool sprawl that clog down analysts' desks are only some of the issues that turn unoptimized processes and inadequately trained people into exploitable assets for cyber-attackers.
Vulnerabilities	Scoping, Discovery & Validation	The ballooning number of vulnerabilities, difficulties in patching them without business disruption, and IT man hours required for patching endemically lead to backlogs that put the organization at risk of attacks and fines for non-compliance.
Assets	Scoping, Discovery & Validation	Unmonitored exposed assets equate to a red-carpet inviting hackers to gain entry to an organization's infrastructure without being noticed, increasing the odds that they will be able to quietly escalate and achieve their goal.
Infrastructure, IT, Cloud, Privileges, Policy	Scoping, Discovery & Validation	As connections between on-premises and cloud infrastructure and IT multiply, the odds that improperly defined privilege and access policies can be exploited by attackers after gaining entry multiply.

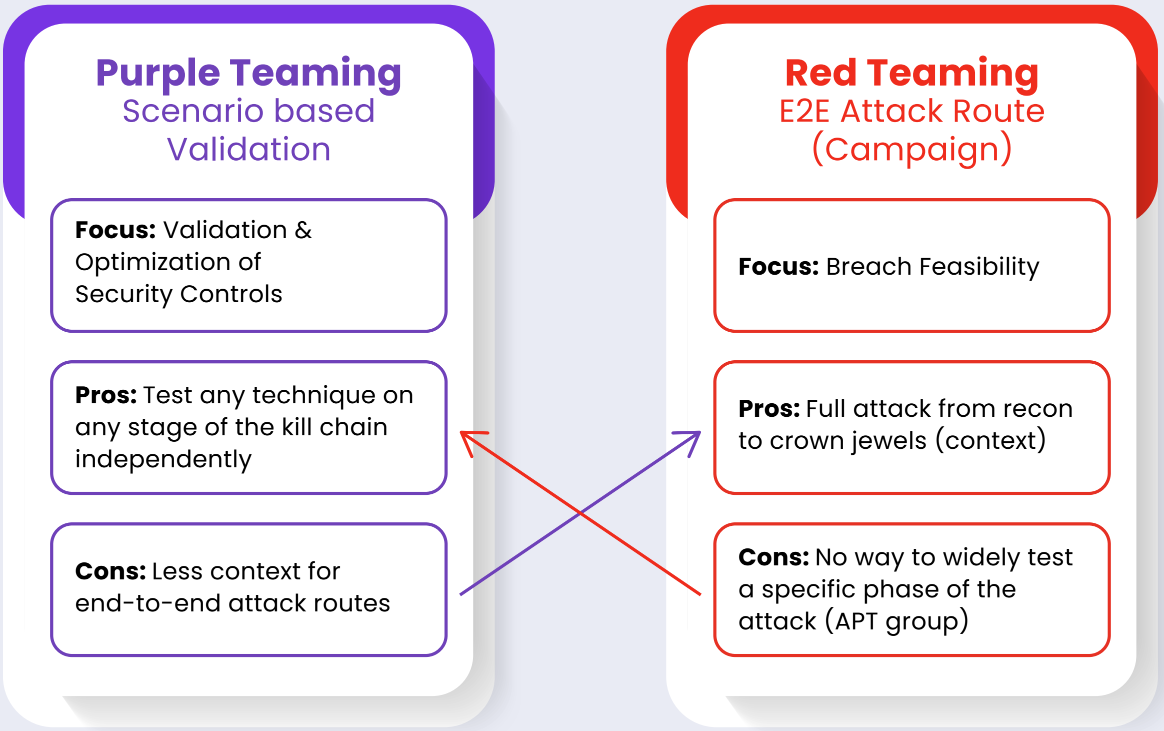
B Methodologies

There are two main methodological approaches to continuous security validation: with agents and without agents. In other words, from the inside or outside in. Each method has its pros and cons, and a holistic continuous security validation program should ideally include both.

Following the visual above, let's examine the implications of the two methodologies:

- **Security Validation & Optimization Scenarios – Purple Teaming**
  This covers agent-based technologies that launch production-safe emulated attacks to assess resilience against specific attack tactics, techniques, and processes if the attacker has already gained an initial foothold. This methodology is colored in purple to reflect the fact that using the related technologies (Breach and Attack Simulation (BAS), Zero code Advance Purple teaming, Attack Based Vulnerability Management (ABVM)) effectively enables a regular defensive blue team to operationalize automated offensive techniques with minimal adversarial skills required. This built-in blue team people red team ability combination effectively creates a purple team.

- **Breach Feasibility Campaign – Red Teaming**
  Breach feasibility can only be evaluated by attempting to launch an attack from the outside without an agent. When successfully gaining an initial foothold, the attackers attempt to progress laterally or vertically to achieve their goals.



Purple Teaming
Scenario based Validation

Focus: Validation & Optimization of Security Controls

Pros: Test any technique on any stage of the kill chain independently

Cons: Less context for end-to-end attack routes

Red Teaming
E2E Attack Route (Campaign)

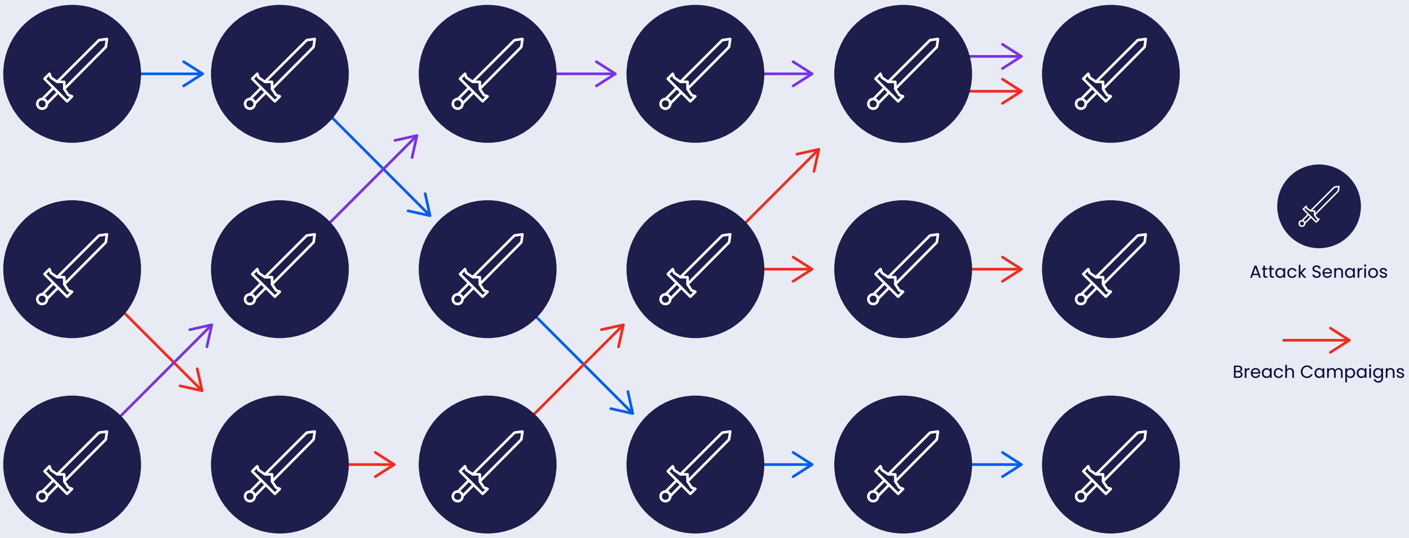
Focus: Breach Feasibility

Pros: Full attack from recon to crown jewels (context)

Cons: No way to widely test a specific phase of the attack (APT group)

Each approach has pros and cons, as shown in the figure above. Purple teamers can test any technique on any stage of the kill chain independently but lack the context to assess end-to-end attack routes. In contrast, red teamers can launch attacks from the recon stage to goal completion but lack the ability to assess specific segments of the attack kill chain.

By enabling purple teams to launch red team attacks from any attack stage, as shown below, Cymulate is unique in including the ability to combine the two methodologies in full kill-chain scenarios and campaigns.



* Figure: Create and customize end-to-end red teaming campaigns

C Technologies

The optimal way to cover all areas of security validation is to combine a number of different technologies and methodologies:

- **Breach Attack Simulation (BAS) - CTEM Discovery**
  Attackers are looking for gaps in security controls to find an entry point and expand their attack laterally and vertically. BAS tools answer the question: "How well are my security controls and processes performing?" It launches simulated attack scenarios out-of-the-box and correlates findings to security controls (email and web gateways, WAF (Web Application Firewall), Endpoint, or other) to provide mitigation guidance. These are primarily used by the blue team to perform security control optimization.

- **Zero Code Advanced Purple Teaming - CTEM Prioritization**
  Each organization has its specificities that no off-the-shelf automation can entirely cover. Purple teams expand BAS into creating and automating custom advanced attack scenarios. These tools usually extensively leverage the MITRE ATT&CK® framework, enabling advanced security teams to develop complex scenarios from predefined resources and custom binaries and executions. Custom scenarios can be used to exercise incident response playbooks, pro-active threat hunting, and automate security assurance procedures and health checks.

- **Attack-Based Vulnerability Management (ABVM) - CTEM Prioritization**
  Attackers' second favorite path to maximize their reach is taking advantage of unpatched vulnerabilities. The ever-growing volume of vulnerabilities is flooding IT teams with an unmanageable patching load, resulting in patching delays. Relieve the chronic vulnerability patching overload by drastically reducing the number of critical patches required. ABVM checks which vulnerabilities are effectively compensated for by the defensive array and deprioritizes them, focusing the patching effort on vulnerabilities that endanger the infrastructure.

  Note: This technology is relevant for purple and red teaming methodologies as both uncover vulnerabilities, but this technology filters discovered vulnerabilities to prioritize mitigation. It is the second stage of the validation process per se.

- **External Attack Surface Management - CTEM Scoping**
  Attackers are looking for unmonitored assets to stealthily penetrate an organization's digital infrastructure, emulating an attacker's reconnaissance phase, during which they comprehensively analyze their target organization. ASM (Attack Surface Manager) tools scan the domains, sub-domains, IP addresses, ports, and more for internet-facing vulnerabilities. It is also looking for Open-Source Intelligence (OSINT) that can later be used in a social engineering attack or a phishing campaign. This tool helps organizations understand how hackers might get an initial foothold.

- **Continuous Automated Red Teaming (CART) - CTEM Scoping & Discovery**
  Well configured Detection tools can detect and stop many known attacks but fail to emulate the creativity that is the hallmark of successful attackers. CART campaigns tools go beyond the ASM reconnaissance page to answer the question: "How can an adversary breach my defenses and internal segmentation?"

  These tools simulate an end-to-end campaign attempting to penetrate the organization by analyzing exposed vulnerabilities and autonomously deploying attack techniques that penetrate the network. For example, they can trigger the attack with a well-crafted phishing email. After gaining the initial foothold, the attack subsequently propagates within the network in search of critical information or assets.

D Outcomes

Each of the technologies mentioned above provides analytics, insights, priorities & mitigation guidance accessible from dynamic dashboards with off-the-shelf customizable automatically generated reports and an integrated ticketing system to accelerate mitigation management.

Conclusion

The transition from risk management to threat exposure management is in full swing, reflecting both compliance regulation updates and recommendations from think tanks ranging from Gartner to the World Economic Forum. Integrating with Cymulate assures environments against most threats, both existing and future, and puts ahead of the curve in terms of best practices.

Cymulate provides organizations with comprehensive security control validation and in-depth insights into breach feasibility. This modular solution addresses a wide variety of business and technical use cases and scales from out-of-the-box simulations to full customization for advanced attack simulations. With Cymulate, companies assess, optimize, rationalize, and prove their security program with minimal resource investment. Security professionals and business stakeholders leverage these insights to reduce cyber risk, justify investments, provide proof of security resilience to executive leadership, and to gain evidence for compliance and regulatory purposes.

Contact us for a live demo

Start Your Live Demo

info@cymulate.com | www.cymulate.com