Cymulate

A Practical Guide to Exposure Management

A Cymulate eBook to introduce exposure management and identify the pragmatic steps to break cybersecurity silos and implement an exposure management program

Exposure Management Overview

Exposure management presents a cardinal shift for security operations and their ability to reduce cyber risk with proactive security. Exposure management takes a proactive approach to identify, validate, prioritize, and mitigate the vulnerabilities, configurations, control gaps, and other weaknesses that create exposure risk.

To answer the key question “how exposed is the organization,” exposure management integrates silos of the cybersecurity program to increase cyber resilience with a focus on the risks that present the biggest potential impact to the organization.

> *Proactive security is all about getting ahead of threats – seeking out and mitigating weaknesses before they are discovered and exploited by adversaries.*

Omdia

Proactive Security: Cyber-Resiliency’s Innovation Wave, Omdia, 2023.

Exposure Management & the Attacker's View

To answer this critical question of "how exposed is my organization," exposure management provides the framework for cybersecurity programs to view their cyber assets and supported processes from the attacker's view of the organization.

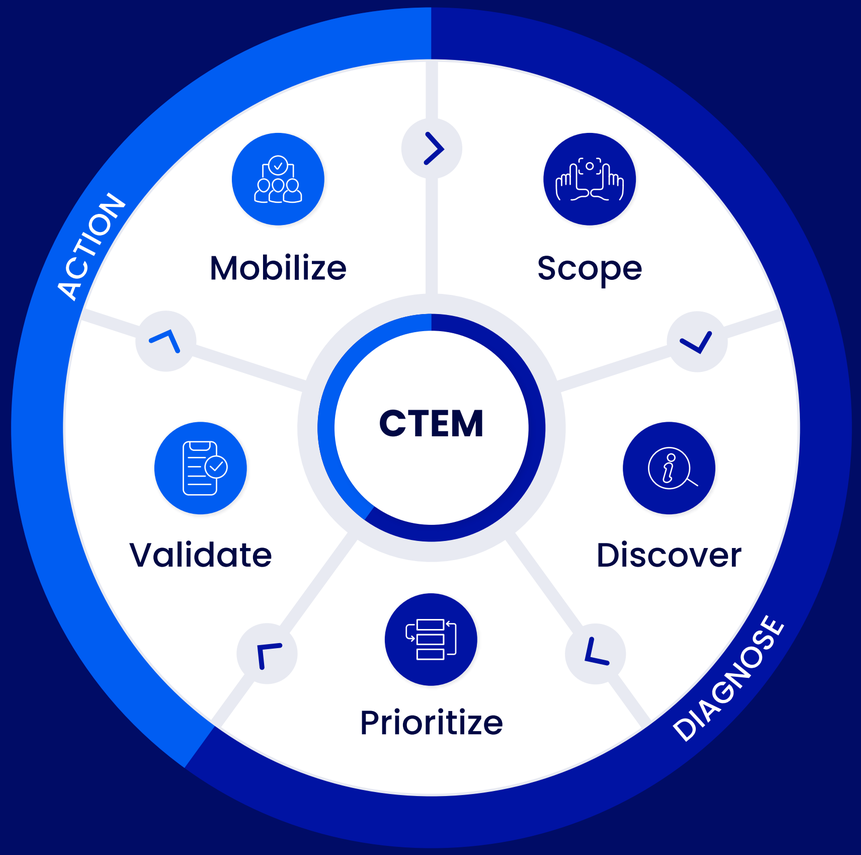
Understand weaknesses and gaps

Test and validate the security controls, defenses, and incident response

Know the configurations across networks, systems, clouds, applications, data, SaaS and controls that make the organization vulnerable to attack

This eBook explores the concept of exposure management and highlights the key responsibilities, tasks, and outcomes required.

Continuous Threat Exposure Management



Operationalize Exposure Management

Gartner introduced continuous threat exposure management (CTEM) to operationalize the practice of exposure management, with five integrated phases of scoping, discovery, prioritization, validation, and mobilization.

While some may see exposure management as a logical evolution of vulnerability management, Gartner's concept of CTEM draws a clear distinction that exposure management must be both forward-looking to potential threats and aligned to organization needs for defending against business disruption.

Cymulate

Exposure management goes well beyond traditional vulnerability management to include requirements for scoping, validation, and mobilization. To implement these steps, security organizations must transform from traditional scan-patch processes to a more integrated program that aligns to business priorities, includes offensive testing for validation, prioritizes based on risk, and understands that mitigation is more than just a simple tactical fix but an optimization of security posture.

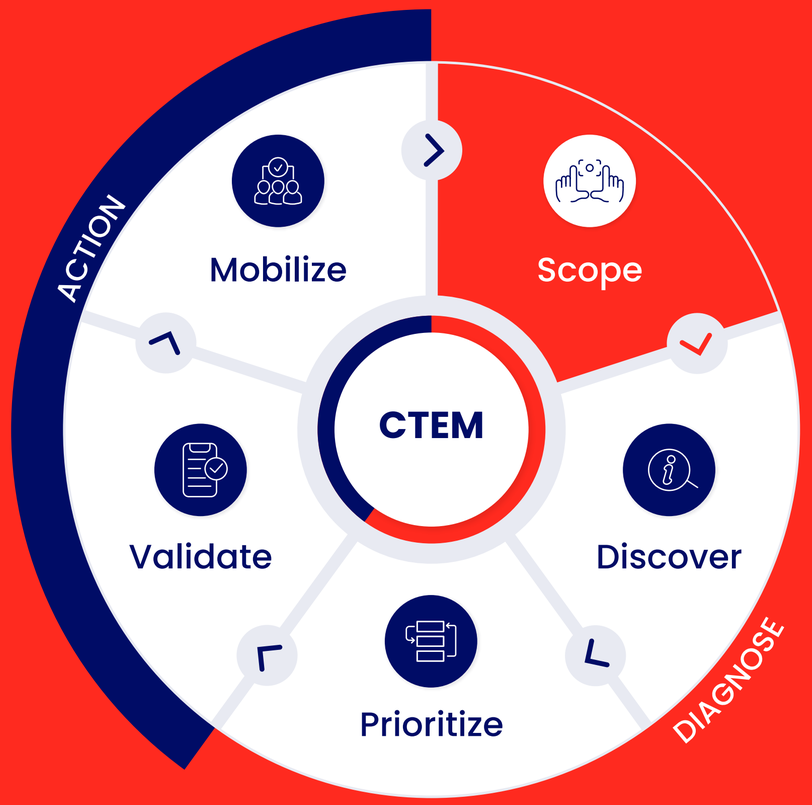
With increasing pressure from boards to treat cybersecurity as a business risk, security leaders can look to exposure management to:

- Create common non-technical language to define acceptable risk
- Drive agreement when unacceptable risk requires mitigation that may disrupt business operations
- Justify budgets/projects to achieve goals
- Measure outcomes with tangible results

> *Continuous threat exposure management is a pragmatic and effective systemic approach to continuously refine priorities and walk the tightrope between two modern security realities. Organizations can't fix everything, nor can they be completely sure what vulnerability remediation they can safely postpone.*

Gartner

How to Manage Cybersecurity Threats, not Episodes, Gartner, 2023.



Scoping
Overview

Scoping provides the foundation for successful exposure management programs by aligning the cyber program with business risks, defining a clear focus, and establishing measurable goals and objectives. Following Gartner's guidance, continuous threat exposure management should run in concurrent cycles of focus, which allows for iterative improvements.

For each cycle, scoping allows the organization to define what will fall under review during the current cycle, reducing the number of variables involved while defining the business context and establishing criteria for success.

Cymulate

SCOPING: JOBS TO BE DONE

Identify Business Operation Risks

While the scope of exposure management may be technical (cloud, data, SaaS, etc.) or focused on a critical organization function, the scope must always consider potential impact to business operations.

Supporting Technologies
For large or regulated organizations, security teams should leverage the already risk registries already documented in Governance Risk & Compliance (GRC) systems.

Baseline Security Posture

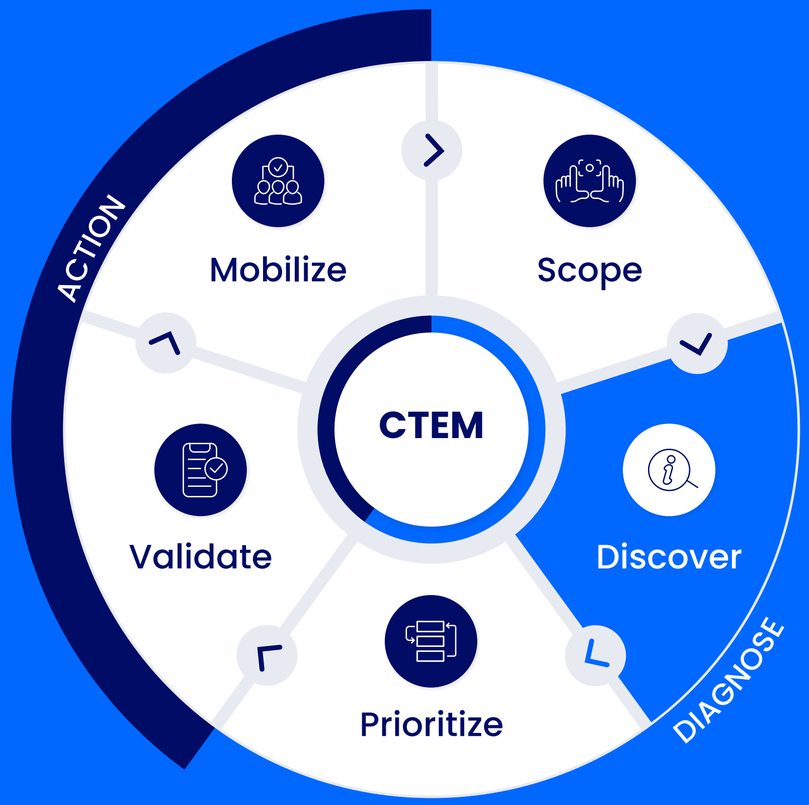
To deliver measurable results, exposure management must start with an understanding of where you are today. The baseline considers the full attack surface in scope (such as assets, clouds, systems, etc.) and correlate with the business risks.

Supporting Technologies
Cyber Asset Attack Surface Management (CAASM) provides an aggregated view of controls and attack surface mapped to business risks.

Define Risk Tolerance

Exposure management programs recognize that many vulnerabilities cannot be patched and remediation often involves business disruption. Alignment with the business on risk tolerance sets the criteria and foundation for mitigation action and acceptable of disruption or risk.

Supporting Technologies
This is a business and strategy function that can be potentially be supported by tools that measure risk.



Discovery
Overview

While scoping defines the business process itself, discovery asks what systems, applications, and other resources support that scope—even when those objects may not appear to fall within the scope themselves. This is the attack surface.

The discovery phase creates a risk-profiled asset inventory of both the internal and external attack surface through the identification of the assets, classification of their business context, and understanding of potential cyber risk.

External Discovery

Exposure management applies the attacker's view to understand how the organization appears to the threat actor. This requires a complete scan and discovery of the external attack surface including:

- Web domains
- IP addresses
- Web applications
- Databases supporting web applications
- Asset libraries and other code components visible to the outside world

Supporting Technologies

Attack Surface Management (ASM) or sometimes referred to specifically as external attack surface management (EASM) scans the organization's public-facing Internet assets to inventory known and unknown assets.

Dark Web Discovery

Discovery also extends to the dark web to identify stolen data, confidential business information, sensitive personal data, or fraudulent products.

Supporting Technologies

Attack Surface Management (ASM) should include dark web threat discovery that searches for compromised data and monitors hidden forums and marketplaces to uncover stolen data and credentials.

Digital Risk Protection Services (DRPS) provide similar level of dark web monitoring as a managed service that also include response services such as data recovery and removal information from the dark web.

Internal Discovery

The goal of internal discovery is to identify vulnerabilities and exploitable assets that create exposure risk. This requires scanning the internal attack surface to identify exploitable assets that an adversary can leverage to propagate from a foothold to crown jewels.

Identify Vulnerabilities And Misconfigurations

Discovery must also include the identification of vulnerabilities and misconfigurations across external and internal systems that make the organization vulnerable to attack.

Supporting Technologies

Internal asset discovery and vulnerability identification is traditionally accomplished with Vulnerability Scanners that actively scan the network and probe each IP address on the network and analyze the response from active devices for known common vulnerabilities and disclosures (CVEs) and device information, such as open ports.

For a more complete discovery, Attack Surface Management (ASM) takes a broader view to discover assets, systems and details of the configuration:

- Active Directory and Azure AD objects
- Clouds such as AWS, Azure, Google Cloud
- On-prem physical and virtual resources
- APIs

For specific domains such as clouds, data, and applications, domain-specific Security Posture Management tools offer specialized integrations to the specific environments for more granular details of the cloud, data, or application.

DISCOVERY : JOBS TO BE DONE

Identify Control Weaknesses

Control weaknesses and gaps can be just as damaging as an unpatched CVE. Security programs that have already adopted to control testing and validation should include those findings in the discovery phase of exposure management.

Supporting Technologies
Production-safe offensive security tools like Breach and Attack Simulation (BAS) assess the efficacy of existing security controls through attack simulation to highlights weaknesses attackers could exploit.

Map Attack Paths

Attack path analyses model potential lateral movement trajectories across external and internal environments, illuminating risks from chained exploitation of discrete vulnerabilities.

Supporting Technologies
With visibility to internal and external assets and their configurations that make them vulnerable, Attack Surface Management (ASM) simulates an attacker's techniques with a broader view to discover and map the attack path for each asset.

DISCOVERY : JOBS TO BE DONE

Consolidate Exposures & Create Risk-Profiled Asset Inventory

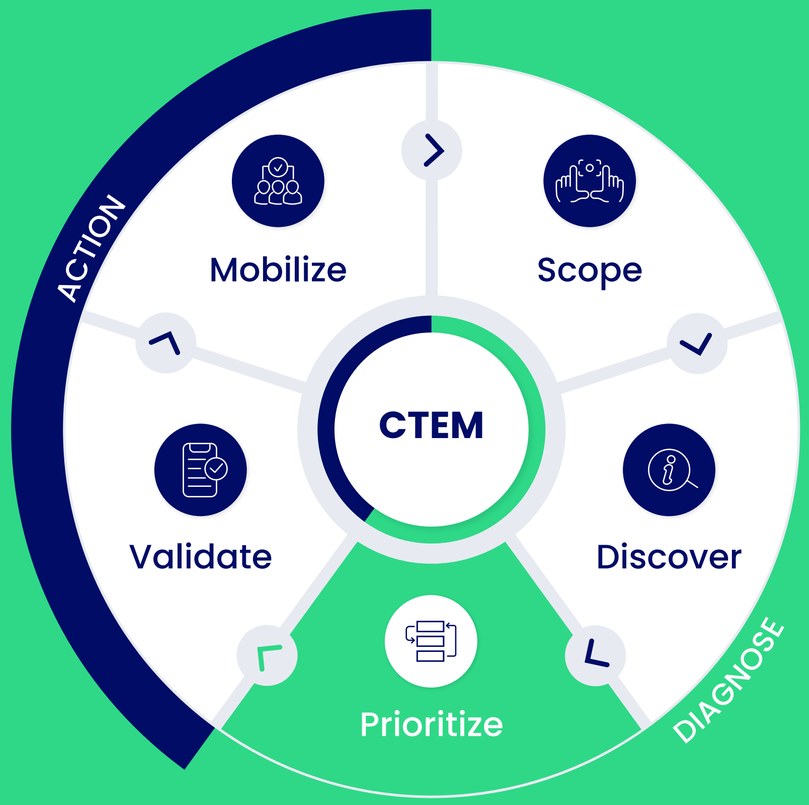
Discovery should include the aggregation and analysis of all discovery findings into a single view of exposure risk. With this consolidated view of assets and exposures, organizations should create risk-profiled asset inventories that also considers the business context of the asset.

Supporting Technologies
For the aggregated view of assets and findings, Cyber Asset Attack Surface Management (CAASM) integrates with the other technologies to create to create consolidated view of all assets and findings.

"When combined with EASM and DPRS, CAASM forms the foundation for a more complete automated attack surface management process and supports development of effective continuous threat exposure management programs."

Gartner

Emerging Tech: Security – Successfully Cross the "CAASM", Gartner, 2023.



Prioritization

Overview

With a goal of mitigating the threats that your organization is most likely to face, prioritization within an exposure management program differs greatly from traditional vulnerability management. While typical vulnerability prioritization considers external factors such as Common Vulnerability Scoring System (CVSS) severity scores and potentially threat intel, exposure management requires prioritization that also considers internal factors such as compensating controls, business context, and the availability of mitigation.

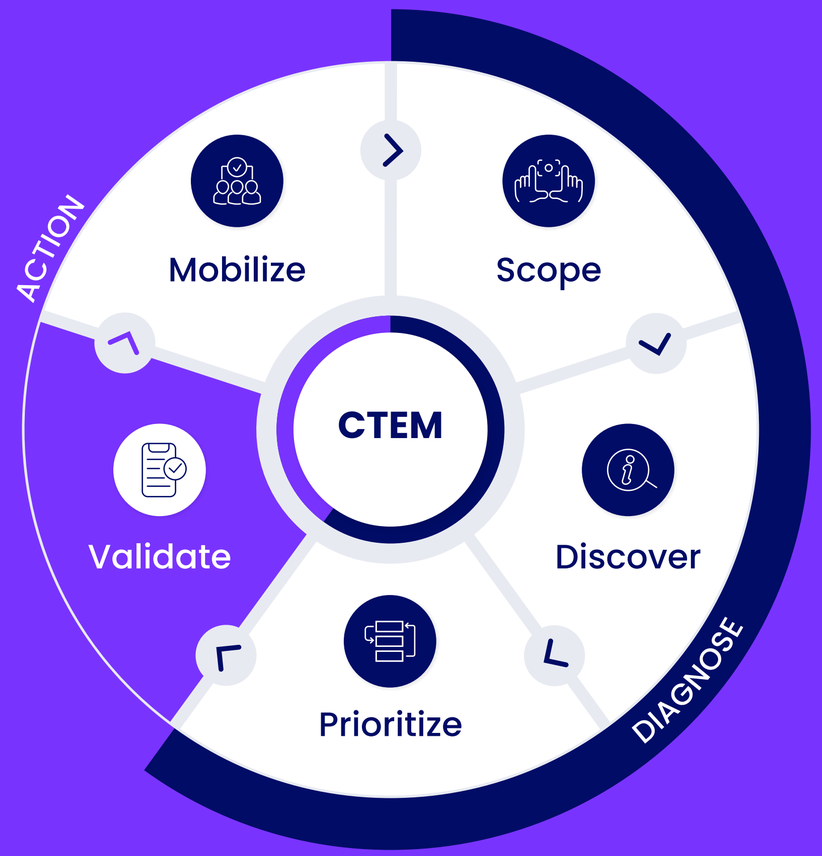
PRIORITIZATION: JOBS TO BE DONE

Stack Rank Exposures

Effective prioritization requires a stack rank of all exposures based on key factors such as risk, potential impact to business operations, and threat intel to active campaigns and targeted industries. While prioritization has long been a challenge for vulnerability management, concepts like risk-based vulnerability management can be applied to all exposures as long as organizations start with the consolidated list and risk-profiled asset inventory.

Supporting Technologies
With exposure risks aggregated and a complete risk-profiled asset inventory, Cyber Asset Attack Surface Management (CAASM) provides the correlation and analysis for advanced exposure prioritization.

> *"CAASM can aggregate multiple vulnerability sources into a single view and can overlay them against assets rather than organizations having to pull them together manually."*
>
> **Gartner**
>
> Emerging Tech: Security - Successfully Crossing the "CAASM", Gartner, 2023.



Validation
Overview

The inclusion of validation is one of the biggest advantages of exposure management over traditional security operations programs like vulnerability management. Validation provides the confirmation of exposure risk by assessing the likelihood of attack success and identifying the potential impact of successful attacks.

While some argue you cannot do proper prioritization without validation, Gartner analyst Pete Shoard describes them as separate functions where prioritization provides the “sort” function while validation provides the “filter.” With this filter on validated risk, security teams can focus their remediation efforts on exposures that present the greatest risk.

Legacy approaches to validation relied on periodic penetration tests and skilled red teams. Exposure management recognizes the need for continuous assessment which demands technologies for automation with broad coverage of the attack surface.

VALIDATION: JOBS TO BE DONE

Validate Controls & Response

Controls validation and response optimization is one way exposure management improves security posture over time. Specific to exposure risk, validation tests the ability of existing controls to mitigate attacks that target the exposure. For threats not mitigated, assessments test the response processes and ability to contain the threat. Exposures mitigated with compensating controls present a substantially lower risk.

Supporting Technologies
Offensive security tools like Breach and Attack Simulation (BAS) provide production-safe automation for continuous assessment of existing security controls and response processes through attack simulation.

Validate Threats

The disclosure of new high-severity vulnerabilities or the report of new exploits or active campaigns from threat actors often requires urgent testing to validate the risk to the organization.

Supporting Technologies
In the past, threat validation was limited to organizations with dedicated red teams. Now technologies like Breach and Attack Simulation (BAS) and Automated Red Teaming provide the offensive testing to safely assess cyber resilience to specific threats and campaigns.

> *Expanding and automating a cybersecurity validation (CyVal) approach via CTEM is key to a successful exposure management program. One approach to starting CyVal is to implement breach and attack simulation (BAS) or automated penetration testing tools, and expand progressively to a workflow of systematically taking the attacker's view to validate whether an attack would be successful.*

Gartner

Top Strategic Technology Trends for 2024, Gartner, 2023.

VALIDATION: JOBS TO BE DONE

Validate Attack Paths

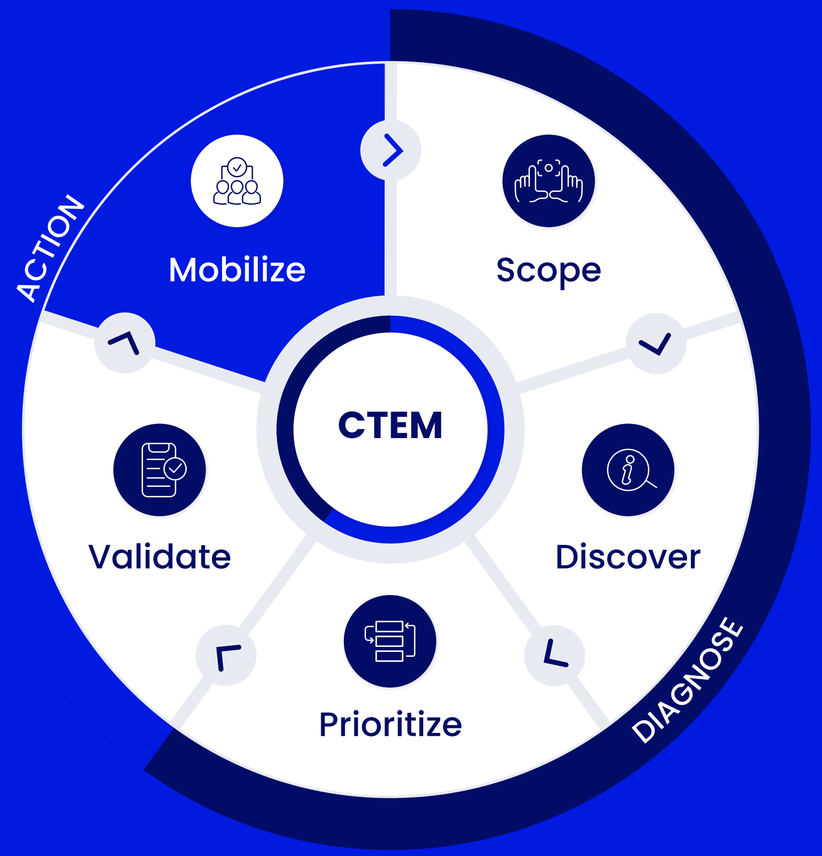
Attack path validation shows how each exposure and vulnerability can be exploited and the consequences of a compromised asset, including lateral movement and privilege escalation. By validating attack paths, security teams confirm attack viability and gain insights into the aggregate potential damage inflicted by a successful attack.

Supporting Technologies
While Attack Surface Management (ASM) identifies potential attack paths, Automated Red Teaming provides the offensive testing to confirm and validate the attack paths with real-world attacks on an organization's systems, networks, clouds, applications, and more.

> *Organizations with establishing cybersecurity validation programs use BAS technology primarily to ensure consistent, yet improved, security posture over time and across multiple locations … Integrate BAS in a cybersecurity roadmap, as part of a continuous threat exposure management (CTEM) program. Don't run BAS in isolation.*

Gartner

Hype Cycle for Security Operations, Gartner, 2023.



Mobilization
Overview

The mobilization phase is the action-oriented step of any exposure management program. It focuses on executing concrete steps to reduce organizational risk and improve security posture based on the insights gathered throughout the process.

The effectiveness of the implemented fixes should be validated to verify that they achieved the desired reduction in exposure and identify any remaining security gaps.

Plan Remediation

Response is not always straightforward, so more complex remediations must be planned with collaboration and alignment across teams. To effectively mobilize teams to action, the remediation plan must consider:

- Business impact of exploited threat
- Tradeoffs of remediation vs. mitigation (and the options for each)
- Disruption introduced by remediation
- Technical requirements of proposed actions.

Supporting Technologies

Cyber Asset Attack Surface Management (CAASM) provides the consolidated analysis to build remediation plans that consider all options and provide guidance for ops teams to perform the remediation.

Automate Configuration Updates

When possible, automated remediation and mitigation in the form of configuration and control updates provides a fast and effective response, leaving scarce human resources more time to focus on more complex remediation processes.

Supporting Technologies

Security Orchestration Automation and Response (SOAR) allows organizations to streamline security operations responses with automated actions along defined playbooks. Even if responses are not fully automated, the defined playbooks provide a framework for responsibility, acceptable interruptions, and timely action.

Managing Remediation Process

The final step is to create and assign specific remediation tasks to designated owners. Accountability is critical to drive execution.

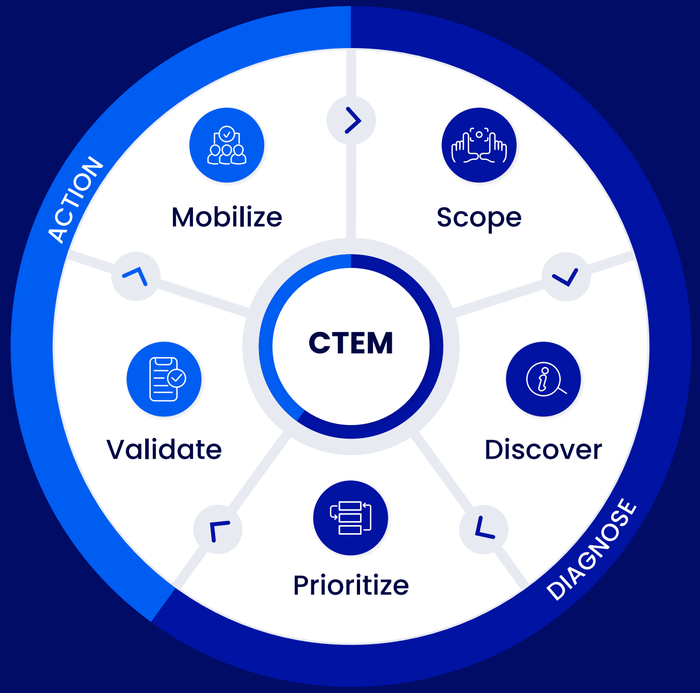
Tracking completion of assigned tasks through metrics and dashboards. This enables following through to ensure risk reduction.

Supporting Technologies
Ticketing systems like IT Service Management (ITSM) provide system of record to create, assign, and track individual remediation actions.

Validate Remediation

After remediation and mitigation actions have closed, secops teams should then validate the action has reduced exposure risk. This often requires rescanning the environment, re-testing controls, and reassessing attack paths.

Continuous Threat Exposure Management



Exposure Management: Outcomes

Strengthen Cyber Resilience

Exposure management aligns the people, process and technology toward a common goal of improving the security posture ahead of potential threats. Exposure management provides a framework for unifying security operations and fostering collaboration with a shared understanding of security priorities and clear direction for action that reduces exposure risk.

Align Cyber Program to Business Needs

Exposure management not only elevates an organization's security posture but also empowers CISO to be more effective in their roles. This approach enables CISOs to:

- Focus initiatives and remediation with context to business
- Apply common non-technical language to define acceptable risk
- Drive agreement when unacceptable risk requires mitigation that may interrupt business operations

Execute with Measurable Results

Exposure management provides a way to measure the outcomes of cybersecurity efforts with tangible results, such as reduced incidence of successful attacks and improved compliance with regulatory standards. These metrics are vital in demonstrating cybersecurity investments' value to stakeholders and continuously improving security practices.

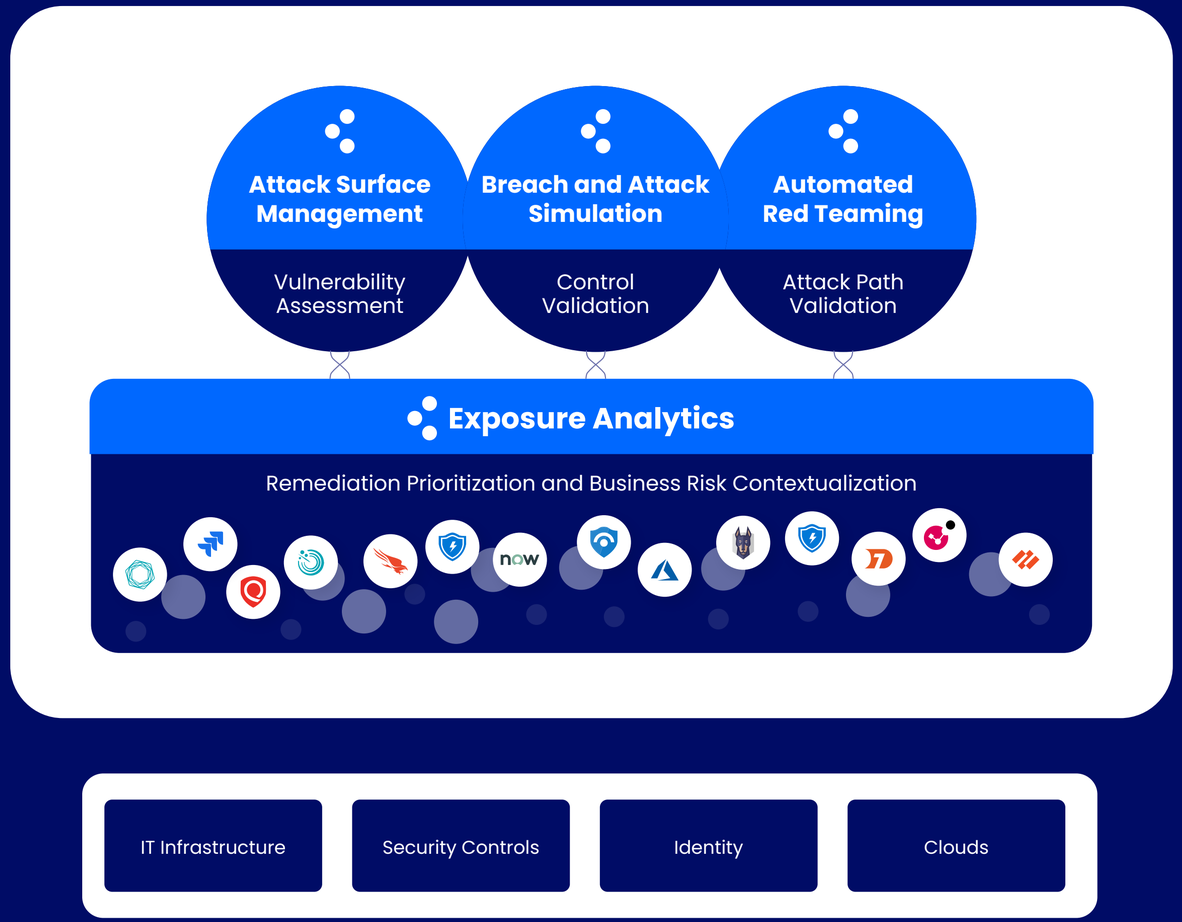
Cymulate

Cymulate Exposure Management & Security Validation Platform

Cymulate recognizes the need to integrate silos of secops functions with supporting technologies to support the exposure management program from scoping through to mobilization. To support security teams on their journey to exposure management, the Cymulate Exposure Management and Security Validation Platform combines critical technologies:

- Attack Surface Management
- Breach and Attack Simulation
- Automated Red Teaming
- Exposure Analytics (generically referred to cyber asset attack surface management

Cymulate Exposure Management & Security Validation Platform



Why Cymulate

Most Trusted Security Validation

Cymulate combines the offensive testing of Breach and Attack Simulation and Automated Red Teaming with the visibility of Attack Surface Management to validate controls, attack paths and threats. More than 500 enterprises use Cymulate to:

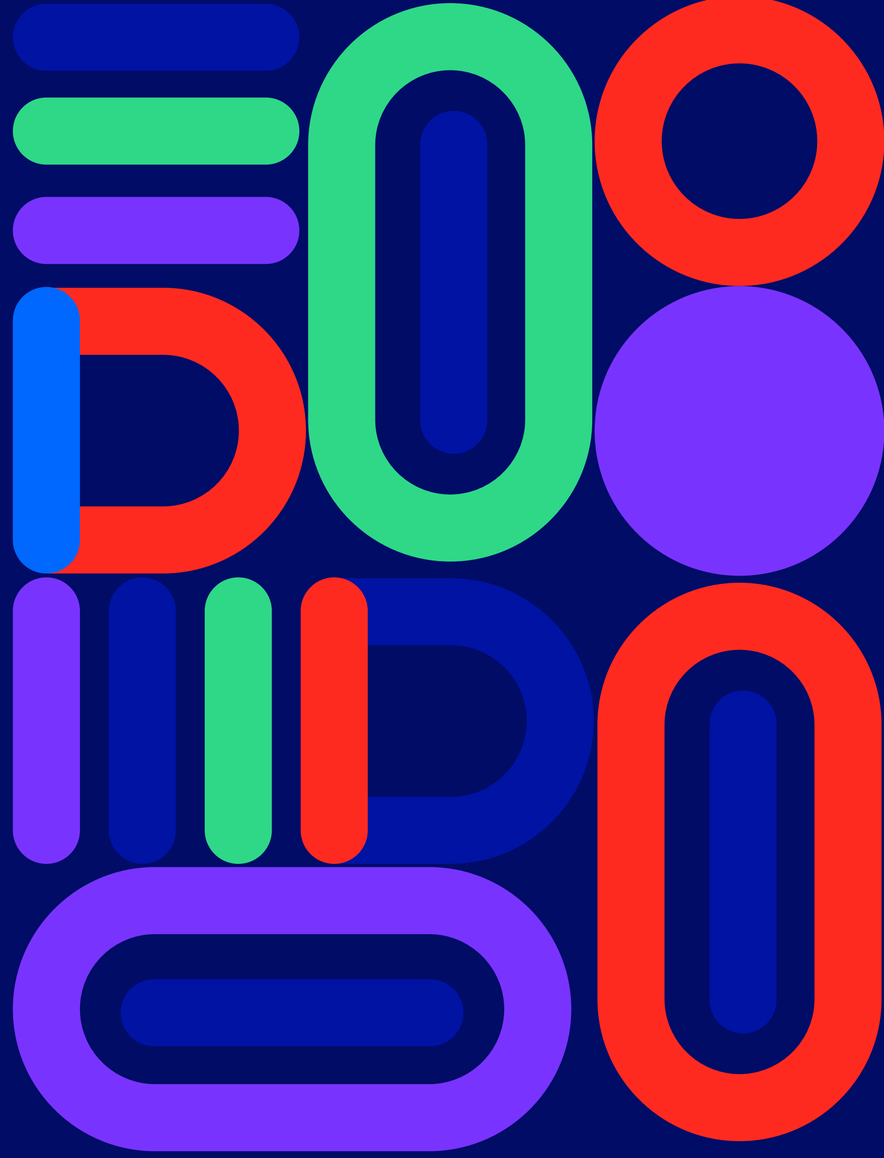
- Identify and control security drift
- Assess and optimize their security operation centers
- Test emergent threats with daily updates
- Automate network pen testing

Analyze Exposure Risk

Cymulate automates the attacker's perspective to assess attack paths for each exposure while correlating other exposures and business context of affected assets, systems, applications, cloud deployments, etc.

Open Platform Manages Exposure Process

The Cymulate Exposure Management and Security Validation Platform provides the technology and integrated solution to drive exposure management from scoping to mobilization.



Learn More About Exposure Management

Whitepaper

Continuous Threat Exposure Management (CTEM)

From Theory to Practical Implementation

Download Now

Webinar

So You Want to Envolve Your Security Operations into Exposure Management

Watch Now

Request a Demo

Schedule a Demo

Get a private demo to see the benefits for your organization

Contact Us

About Cymulate

Cymulate, the leader in exposure management and security validation, provides a modular platform for continuously assessing, testing, and improving cybersecurity resilience — before an attack occurs. More than 500 customers worldwide rely on the Cymulate platform to drive their threat exposure management programs from scoping through discovery, prioritization, validation, and mobilization. The Cymulate platform automates the attacker's perspective to help organizations of all sizes understand threat exposure, how controls and processes respond to threats, and the improvements they can make to mitigate exposure risk. For more information, visit www.cymulate.com.

Appendix

Glossary of Supporting Technologies

- **Attack Surface Management (ASM)**
  ASM technologies facilitate the ongoing process of discovering points within data systems that could be used to attack the organization (servers, applications, services, cloud components, workstations, etc.) and defining and implementing remediation strategies to address gaps.
- **Automated Red Teaming**
  Technologies that automate and aid in the continuous testing of traditional red team exercises to validate entire attack paths from infiltration to actions on objectives. The simulations attempt to breach an organization by autonomously deploying attack techniques that penetrate and gain an initial foothold within the network.
- **Breach and Attack Simulation (BAS)**
  Offensive testing technologies that simulate cyber-attacks on systems and networks to identify weaknesses in their security posture. BAS helps organizations proactively identify and address security issues before an attack occurs. It also ensures they are better prepared to defend against real-world threats.
- **Cyber Asset Attack Surface Management (CAASM)**
  Technologies that identify and manage cyber assets, both internal and external, primarily through API integrations with existing tools.
- **Digital Risk Protection Services (DRPS)**
  Managed services that monitor the cyber presence of an organization across surface web, social media and dark web to identify threats, discover leaked data, and protect organization brand. DRPS often includes the remediation services to facilitate the take down of organization data across social media and dark web.
- **Governance Risk & Compliance (GRC)**
  Integrated suite of software capabilities for managing governance, risk management, and compliance with industry and government regulations.
- **IT Service Management (ITSM)**
  Technologies that enable IT teams manage the end-to-end delivery of IT services through ticketing systems that enable repeatable workflows.
- **Security Orchestration Automation and Response (SOAR)**
  Technology that helps coordinate, execute and automate tasks between various people and tools to assist in threat and vulnerability management, security incident response, and security operations automation.
- **Security Posture Management**
  Technologies that identify and remediate risks through security assessments and automated compliance monitoring. Tools are typically focused on dedicated domains, such as clouds, data, applications or SaaS.
- **Vulnerability Scanners**
  Tools that identify and inventory of IT assets while attempting to identify operational details, such as the operating system it runs and the software installed, in order to discover security vulnerabilities in their computer systems, networks, applications and procedures.