cymulate

# Successful CTEM Depends on Validation

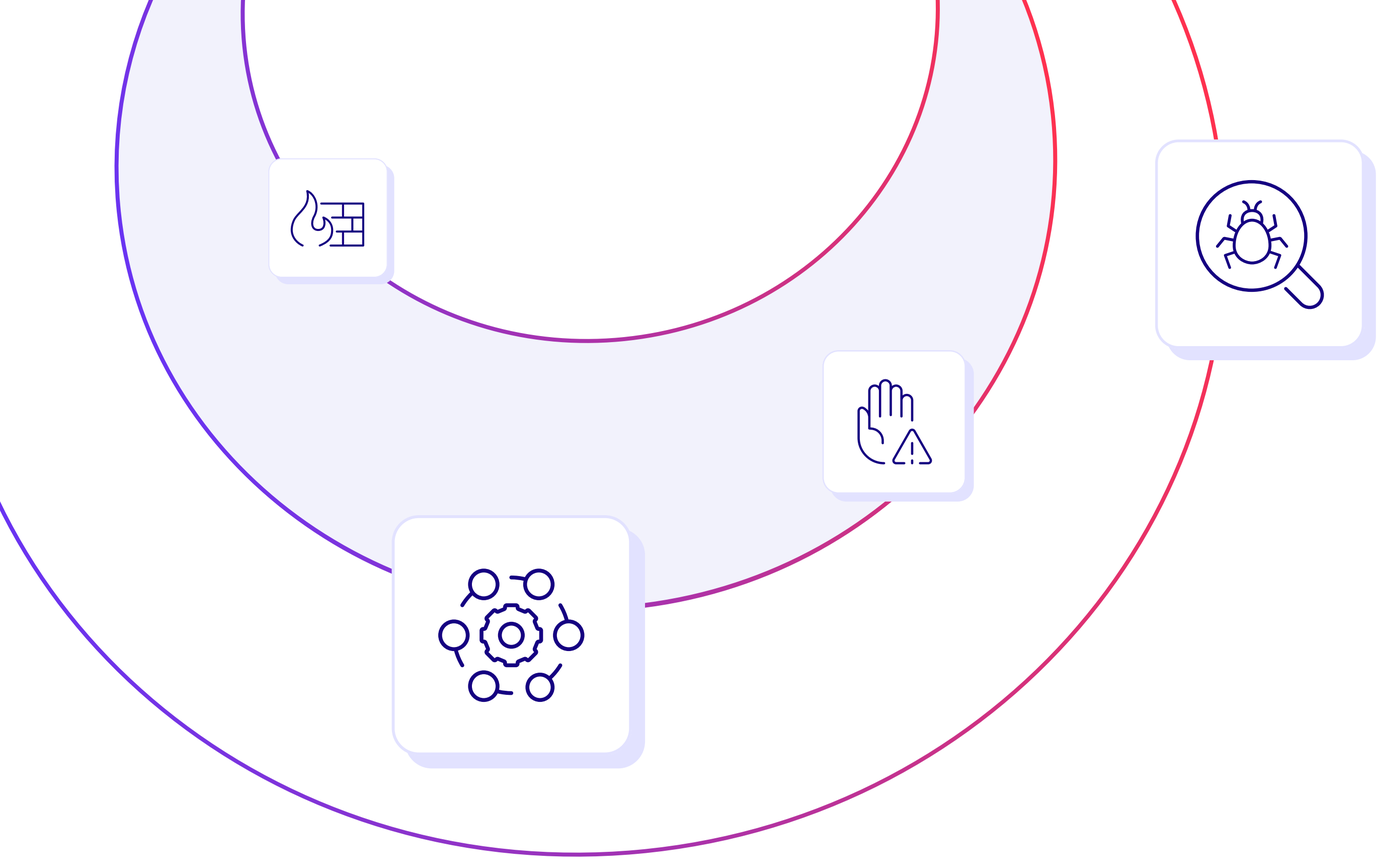
# INTRODUCTION

**The reality is clear:** reactive security methods are no longer up to the task of defending against the scale, speed and sophistication of today's threats.

We surveyed 1,000 CISOs, SecOps practitioners, and red and blue teamers across the globe to find out how they validate cybersecurity in their cloud, on-prem and hybrid environments.

The *Threat Exposure Validation Impact Report 2025* explores the role of AI, the rise in automation and the need to evolve legacy best practices – like manual penetration testing – into continuous, proactive processes. The report also explores the evolution – and challenges – of exposure management within SecOps teams.

Understanding the data and associated validation concepts can help you acquire what's truly needed for security tooling: proof.



# The State of Exposure Management

**98%**

**plan to invest in exposure management**

There are still significant questions around exposure management within SecOps – where it sits, how to effectively identify exposures and how to implement the right CTEM processes with limited resources. Yet, exposure management is a priority when it comes to security budget. And CISOs recognize that exposure management is an effective way to achieve actionable risk intelligence.

According to the research, almost all (98%) of CISOs say they plan to invest in exposure management in the future, with almost 9 in 10 (89%) stating that they plan to invest within the next 12 months.

# 90%

of organizations apply validation to their exposure management process at least once a month

### The Evolution to Exposure Management

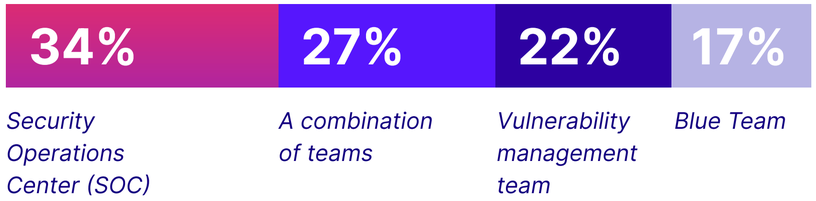
Exposure management is a proactive security measure that gives SecOps an attacker's view of security gaps and insight on how security controls and processes respond to threats and weaknesses. By implementing this proactive security measure into an ongoing process within a security program, organizations evolve into CTEM.

To build and execute a continuous effort to optimize both the short-term response and the long-term security posture, Gartner® created the CTEM framework that integrates scoping, discovery, prioritization, validation and mobilization.

### Resources are Lacking

Ultimately, there remains a lack of resources to properly adopt a robust exposure management program, which could result in major challenges when it comes to identifying and remediating vulnerabilities. This could also lead to a disconnect around who owns CTEM within an organization.

According to the research, exposure management is most likely to fall under the remit of an organization's SOC (security operations center) (34%), while 27% say it's spread across multiple different teams.




Further, while 32% say the role in charge of CTEM is responsible for prioritizing, 25% say validating, 24% say fixing and 19% say scoping.

## The Impact of Validating Exposure Management

Survey respondents recognize the importance of validating exposures in their environment as a means of assessing the impact of exploitation (45%), validating compensating controls (45%), testing the detection of exploitation attempts (43%) and validating that exposures are not a false positive (42%).

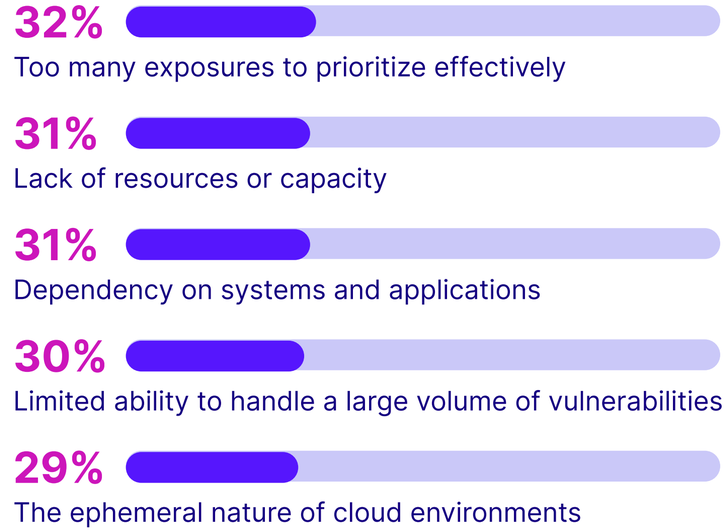
It's not surprising that 90% of security leaders say they apply validation in their exposure management process at least once a month.The more organizations apply validation to their exposure management processes, the more likely they are to experience a decrease in security breaches.

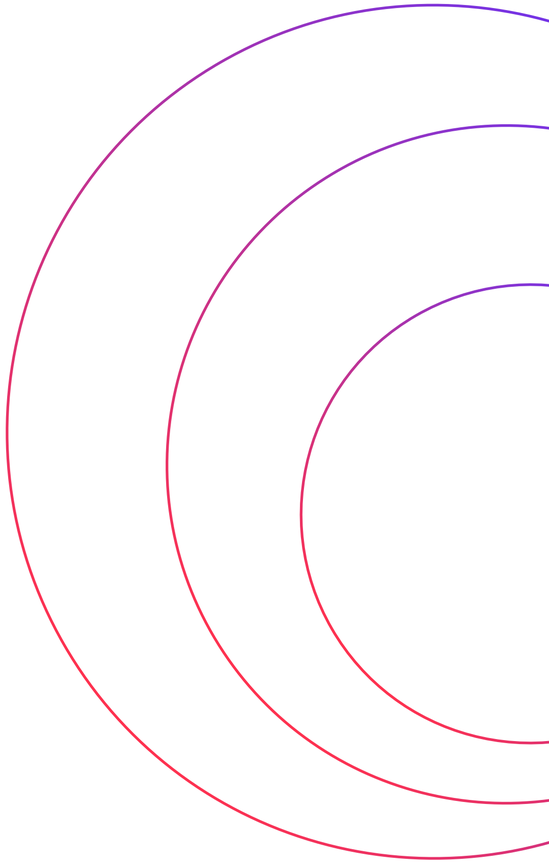
According to the research, respondents who say their organization experienced 4-9 breaches in the past year say they apply validation in their exposure management process 6 times per month. However, those that do this 10 times per month experienced just 1-3 breaches.

## Preparing for Exposure Management

While the majority of organizations have either adopted exposure management processes or plan to do so in the future, the research shows that security teams still face significant challenges and a lack of preparedness. For example, when remediating identified exposures, SecOps report that they experience challenges with prioritizing effectively (32%).

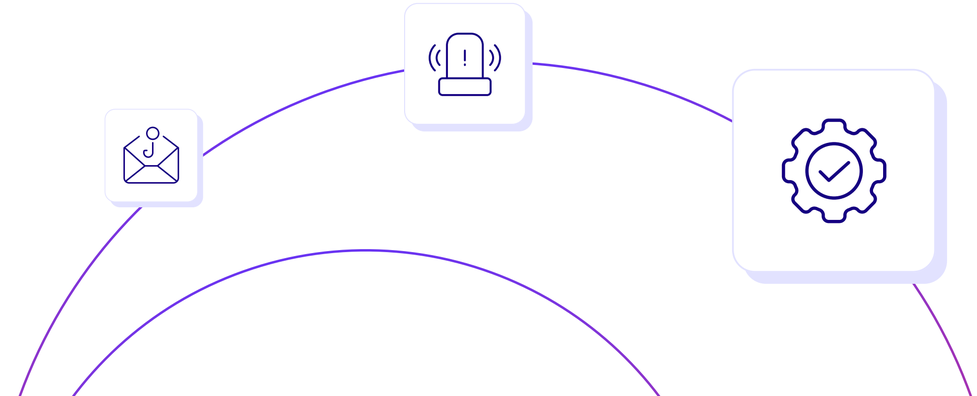
**Here are the biggest challenges facing SecOps when it comes to remediating identified exposures:**



**What's more, SecOps may be left with no choice but to ignore some vulnerabilities due to a lack of resources.** Just over 3 in 10 (31%) state that a lack of resources or capacity is one of the biggest challenges they face when remediating identified exposures, while almost half (49%) cite this as a factor that influences their decision to deprioritize exposure remediation.

Despite these challenges, organizations are employing a number of strategies to better prepare for exposure management, and to help them determine which vulnerabilities are most critical to mitigate. These include asset classification/business impact (35%), validating attack paths to critical assets (34%) and ensuring the effectiveness of controls to prevent or detect an exploit (34%).



**47%**

deprioritize exposure remediation due to the effectiveness of compensating controls to prevent or detect an exploit

## How do you determine which vulnerabilities are most critical to mitigate?

**35%** Asset classification / business impact

**34%** Validated attacks paths to critical assets

**34%** Effectiveness of controls to prevent or detect an exploit

**34%** Threat intelligence

**33%** Risk assessment

**23%** CVSS score

## THE BOTTOM LINE:

Exposure management is already playing a key role in security environments. Not only are organizations seeing a reduction in breaches as the result of implementing a CTEM process, but the vast majority are also planning to invest further in the coming year. However, most exposure management processes still don't have validation capability synchronized in the flow– and this is the critical step that proves exploitability of a vulnerability or other security gaps.

A full-context CTEM program will help you move beyond theoretical CVEs by validating what really matters most: proving whether a threat would succeed in your environment, today.

cymulate

### Schedule a Demo

Get a private demo to see the benefits for your organization

**Request a Demo**

## About Cymulate

Cymulate, the leader in security and exposure validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 1,000 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.

#### SURVEY DEMOGRAPHICS

Cymulate commissioned global market research consultancy, Censuswide, to survey 1,000 enterprise security leaders and practitioners (including CISOs, red teams, blue teams, IT security managers and vulnerability management) across the U.S., UK, Spain, Germany, France and Italy. Industry sectors included healthcare, manufacturing, education and financial services.