XM Cyber

The 2024 State of Security Posture Survey Report

January 2024

Table of Contents

Introduction and Key Findings

Introduction & Methodology

In recent years there has been a persistent surge in the frequency, volume, and impact of cyberattacks. Despite concerted efforts to detect and thwart these threats, attackers continuously innovate, finding novel ways to bypass detective controls. They exploit a diverse range of threats, which include Common Vulnerabilities and Exposures (CVEs) but also the misconfigurations, identity issues and active directory issues, i.e., exposures, which go far beyond CVEs, and are so often exploited in attacks.

Scrutiny of this issue from regulatory bodies, including the Securities and Exchange Commission (SEC), has intensified. Organizations now face additional obligations and requirements for prompt notifications when security incidents occur. This has placed considerable pressure on organizations to refine their incident response processes, emphasizing the need for transparency and the sharing of best practices.

For these reasons, addressing exposures and maturing their security posture has become increasingly crucial for security teams. Organizations must remediate exposures that attackers could use to move laterally in the early stages of their multi-step attacks to prevent their access to critical systems.

This survey explores the current state of the market concerning the effort to fortify security posture. We aim to assess how well exposures are being remediated, the level of effort invested in this undertaking, and the motivations behind such efforts. Through this research, we endeavor to provide a comprehensive view of the cybersecurity landscape, offering valuable insights for organizations striving to navigate the evolving threat landscape effectively.

Methodology

To gain insights into cybersecurity practices, we conducted a survey involving 300 full-time employees, including influential decision-makers such as CISOs, Directors, VP/Heads of Security, and other senior cyber professionals responsible for purchasing decisions. These participants were strategically sourced from 210 organizations in the US and 90 in the UK, all with 2,500 employees or more.

The survey, spanning the second half of 2023, was conducted in collaboration with Global Surveyz, an independent survey company.

Key Findings

1

87% of organizations intend to increase exposure remediation efforts

Our survey found that 87% of organizations acknowledge the pressing need to increase their commitment to vulnerability and exposure remediation in the next 12 months. Despite challenges such as overwhelmed security teams, a shortage of skilled personnel, and the struggle to fill critical positions, this finding reveals organizations' resolute commitment to allocating more resources and effort toward exposure management. Organizations clearly understand that proactive measures are essential in preventing cyberattacks.

2

82% of respondents acknowledge an increasing gap between the number of vulnerabilities and their ability to remediate them

As the number of vulnerabilities in their environments continues to rise, organizations face an uphill battle in addressing them comprehensively. The sheer volume of vulnerabilities makes them practically impossible to address, resulting in a widening remediation gap. Notably, this finding only measures CVEs, which represent just one type of exposure. Combined with other exposure types—such as misconfigurations of systems and applications and insufficiently managed identities—organizations are grappling with a multifaceted, growing threat landscape.

3

Exposure remediation comes at a high cost, involving 62% of IT and security teams

Exposure remediation efforts have a significant impact on operations. 62% of IT and security teams are involved in remediating an average of 12 exposures per week. Yet this resource allocation is still notably inadequate in the face of the thousands of CVEs created annually, not to mention other types of exposures. The stark contrast between the volume of exposures and the limited capacity to remediate underscores the formidable challenge organizations face in closing the remediation gap. As the problem continues to grow, there is an urgent need to explore innovative strategies that enable organizations to better prioritize the exposures that have the biggest impact on blocking attacker tactics.

4 99% of respondents acknowledge room for security posture improvement, with cloud environments biggest area in need

A substantial 45% of companies recognize the cloud environment as the primary area for enhancing their security posture, emphasizing the evolving nature of cybersecurity concerns. This shift underscores the need for organizations to address a broader spectrum of challenges, extending beyond the conventional focus on CVEs. As the significance of cloud environments continues to grow, organizations must adapt and prioritize strategies to fortify their security posture in this critical space.

5 Organizations struggle to articulate security posture, with 68% reporting need for better ways to communicate security posture to leadership and the board

Despite heightened cybersecurity efforts and a widening remediation gap, organizations face a significant challenge in effectively communicating their cybersecurity progress to leadership. We found that 68% of companies report that better communicating their security posture status to leadership and the board is very valuable. This suggests a pronounced discrepancy between the work done by taxed and overwhelmed security resources and their ability to convey this progress to leadership. This finding underscores the urgency for organizations to establish more effective communication strategies, ensuring that the efforts of their security teams are appropriately acknowledged.

6 90% of organizations frequently find themselves unable to remediate exposures due to purchased and legacy applications

Because of outdated legacy systems, 90% of respondents face challenges in addressing exposures. In grappling with the intricacies introduced by legacy systems, organizations confront three choices: accepting the risk, rewriting the application, or gaining a deep understanding of attack paths to remediate exposures and prevent potential harm to critical assets.

Survey Report Findings

Organizations' Plans for Vulnerability/Exposure Remediation in the Next 12 Months

87% of surveyed organizations expressed their intent to increase their commitment to vulnerability and exposure remediation in the next 12 months. This may be related to a variety of factors, including the fact that exposure management is becoming a strategic topic instead of being merely a checkbox item, or that Detection and Response tools continue to fail, forcing reliance on security posture.

Despite challenges such as overwhelmed security teams and a shortage of skilled personnel, organizations are prioritizing efforts to address cybersecurity issues. This commitment underscores the gravity of the cybersecurity problem and the determination to allocate resources for its resolution. Only a minimal 5% of companies plan to decrease their level of effort in vulnerability and exposure remediation, emphasizing a broad consensus on the importance of cybersecurity initiatives.

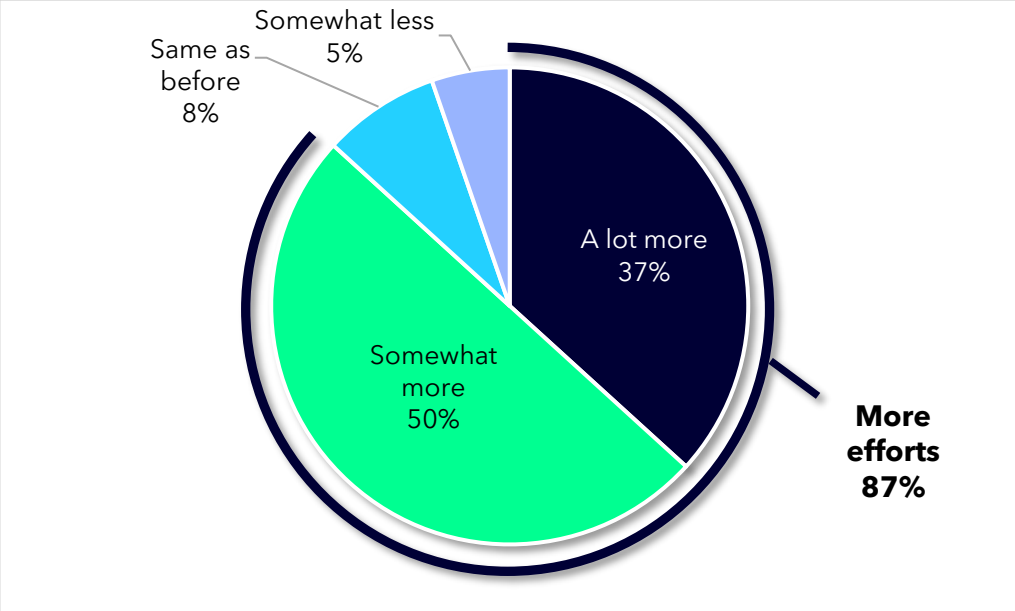


Figure 1: Organizations Plans for Vulnerability/Exposure Remediation in the Next 12 Months

Main Drivers in the Planned Increase in Remediation Efforts

27% of organizations attribute their plans to increase remediation efforts to a heightened priority given to security by company leadership. This shift is indicative of a broader trend in which security has ascended to a higher echelon of company priorities. The integration of security discussions at the board of directors level underscores a collective concern, particularly in public companies, about the significant impact that cyberattacks can have on business operations.

Other factors, such as the expanding attack surface (15%), compliance or audit-related considerations (15%), an increased pace of vulnerabilities discovered (13%), and increased concern about attacks going undetected (13%) also drive an increase in remediation efforts.

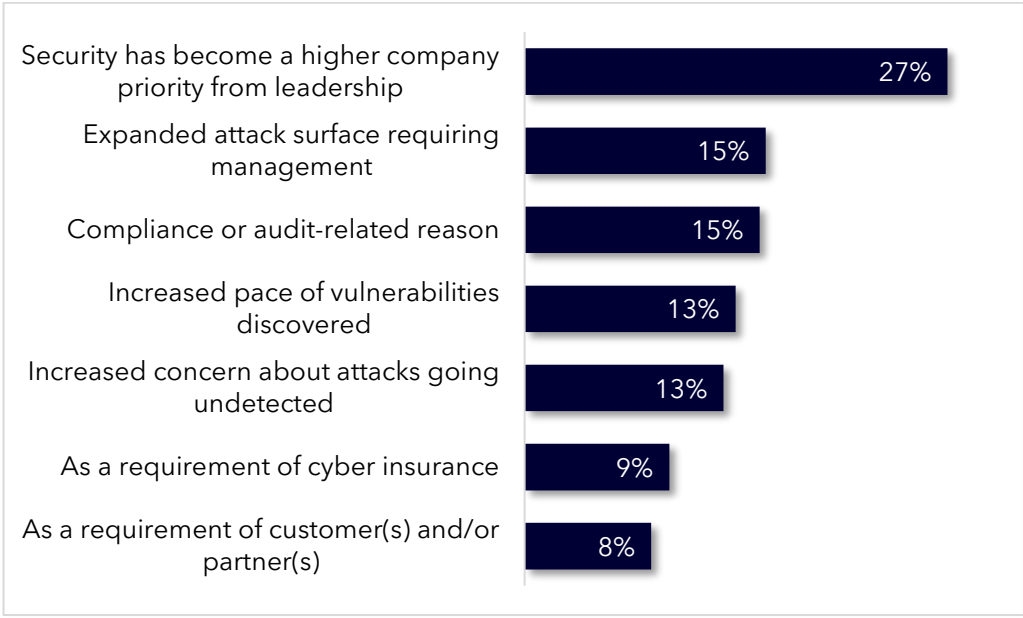


Figure 2: Main Drivers in the Planned Increase in Remediation Efforts

Percentage of Security/IT Teams Involved with Remediations of Exposures/Vulnerabilities

The survey findings reveal that, on average, 62% of security and IT teams actively engage in the remediation of exposures or vulnerabilities (Figure 3). This underscores the significance of this initiative, impacting a substantial portion of organizational personnel.

While this high level of engagement signifies the importance placed on cybersecurity measures, it also highlights the associated costs and the potential for increased efficiency. There may be an opportunity for organizations to optimize their approach to remediations, ensuring a balance between effectiveness and resource utilization.

Further, as company size increases, the percentage of security and IT teams involved in remediation efforts decreases. (Figure 4). This can be attributed to larger organizations having more extensive security teams with a higher degree of specialization, resulting in a smaller proportion actively participating in any particular activity. Yet even for organizations with 10,000 or more employees, 56% is still surprisingly substantial.

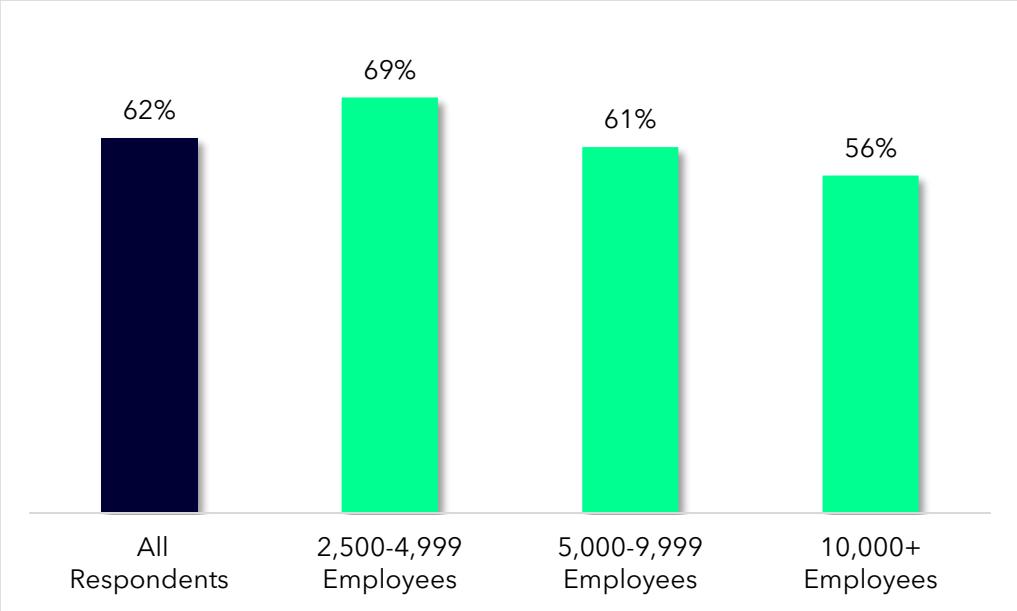


Figure 3: Average of Security/IT Teams Involved with Remediations of Exposures/Vulnerabilities, by Company Size

Gap Between the Number of Vulnerabilities/Exposures in the Environment and the Ability to Remediate Them

A striking 82% of surveyed companies reported an increase in the gap between the number of vulnerabilities/exposures in their environment and their ability to remediate them. This finding underscores the pervasive challenge organizations face in keeping pace with the growing number of vulnerabilities, making it increasingly difficult to address each one comprehensively.

Notably, Common Vulnerabilities and Exposures (CVEs) represent only a subset of exposures, in addition to issues such as misconfiguration and weak credentials, which are harder to count.

The acknowledgment of this widening gap by such a significant majority of respondents suggests the enormity of the issue. It's crucial to recognize that this figure might even underestimate the extent of the challenge, as those in the remaining 13% either might be unaware of the increasing gap or have successfully reduced it through substantial efforts.

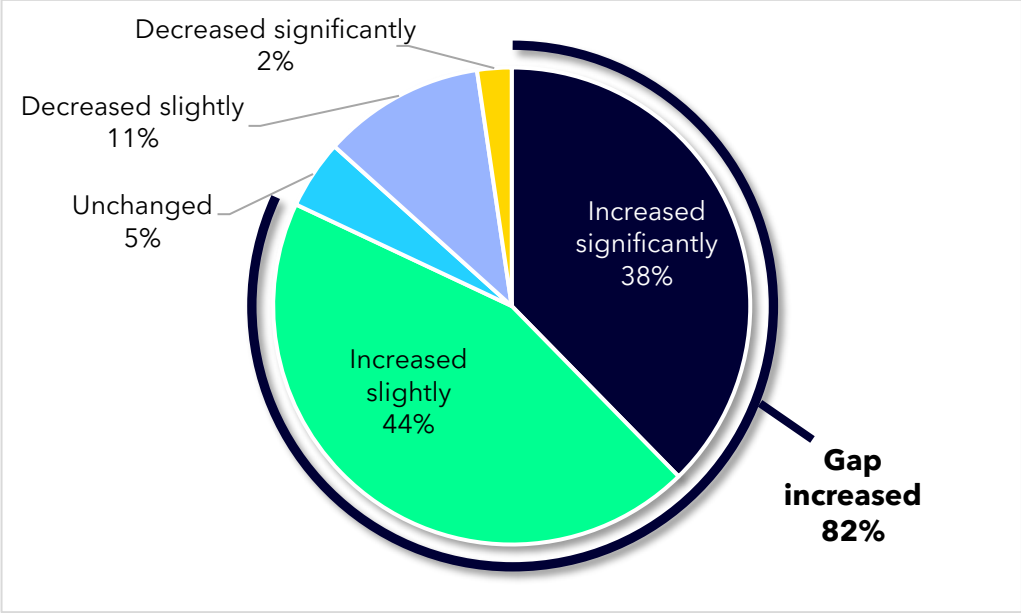


Figure 4: Gap Between the Number of Vulnerabilities/Exposures in Environment and Ability to Remediate Them

Number of Remediated Exposures in an Average Week

On average, companies reported addressing about 12 exposures per week. This figure is juxtaposed against the backdrop of an average of 10k-250k CVEs generated each year, not to mention other security issues.

The data points to a stark reality – organizations seem to be able to address only a fraction of the vulnerabilities and exposures within their environments. With thousands of new issues emerging annually, the current pace of remediation efforts exacerbates the widening remediation gap.

This underscores the critical need for organizations to explore innovative approaches to remediation, ensuring a more effective and scalable response to the growing challenges posed by an ever-expanding threat landscape. Without addressing this issue head-on, the gap between vulnerabilities and remediation efforts is poised to persist and potentially widen further, necessitating a strategic reevaluation of remediation approaches within organizations.

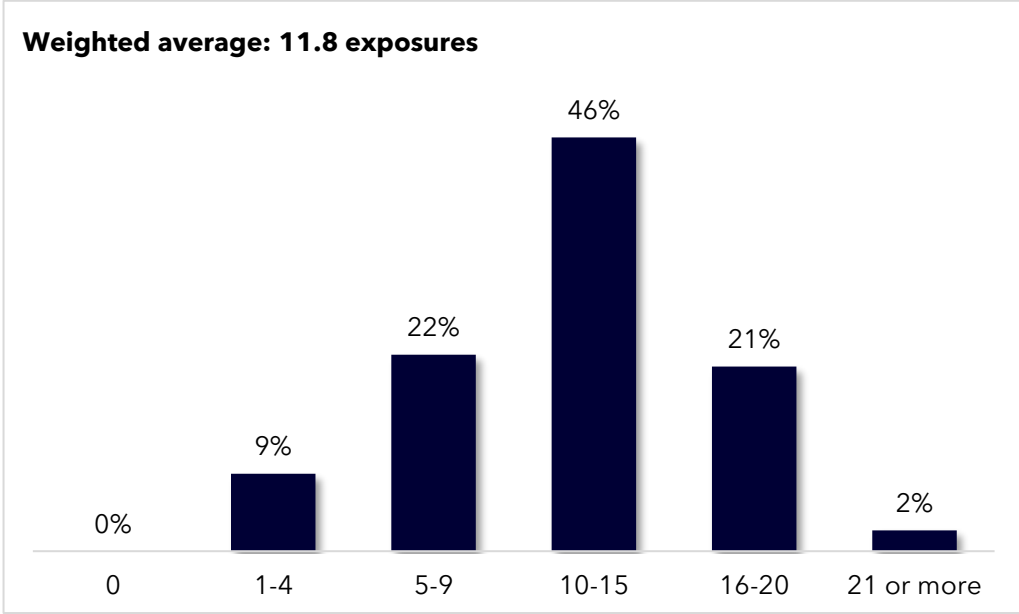


Figure 5: Number of Remediated Exposures in an Average Week

Value of Better Communicating the Security Posture Status to Company's Leadership and the Board

A substantial 68% of companies identify the ability to effectively communicate the current state of their security posture as highly valuable to company leadership and the board.

This finding reveals that many organizations, despite dedicating significant resources to bolstering their security postures, find themselves struggling to convey this progress to leadership and the board. This communication gap not only hinders the acknowledgment of the hard work done by security teams but also has broader implications, potentially contributing to high turnover rates within the security sector and impacting budgets. If organizations cannot effectively communicate their current status and progress, it becomes challenging to make a compelling case for an incremental budget necessary to reach an acceptable level of risk mitigation.

This highlights a need for improved communication strategies. Bridging this gap is crucial not only for required reporting, but also to recognize and reward the hard work of security personnel, as well as for fostering a positive and supportive cybersecurity culture within organizations.

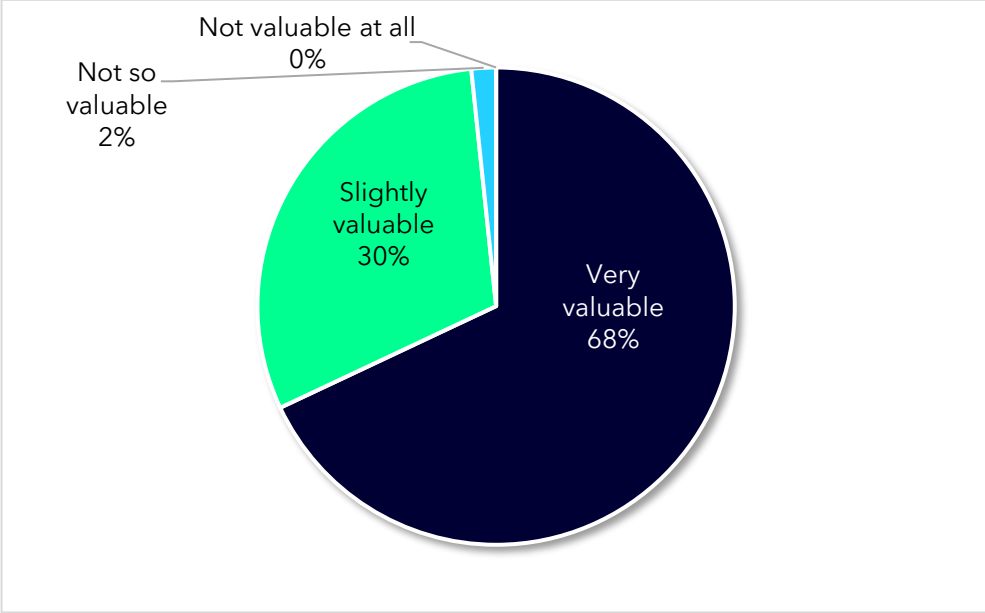


Figure 6: Value of Better Communicating the Security Posture Status to Company's Leadership and the Board

Companies' Vulnerability/Exposure Management Program

Considering the substantial efforts being invested in remediation, and the associated high cost of human resources, we posed the question, "How are companies managing exposures?"

We found that 61% of companies admit to operating reactively, addressing high-severity issues when they arise, while only 23% have formalized processes in place. This is remarkable given that basic vulnerability management has existed for 25 years.

Interestingly, the data reveals a notable trend when examined by job seniority. More senior roles in the company report having more formalized processes than Directors, who are closer to the frontline work.

The data suggests a need to investigate whether security teams have the necessary tools to establish and sustain an ongoing formalized process. It also introduces the possibility that there may be a communication gap between directors and their superiors, with those closer to the operational frontlines having a more nuanced understanding of the cybersecurity challenges faced by the organization.

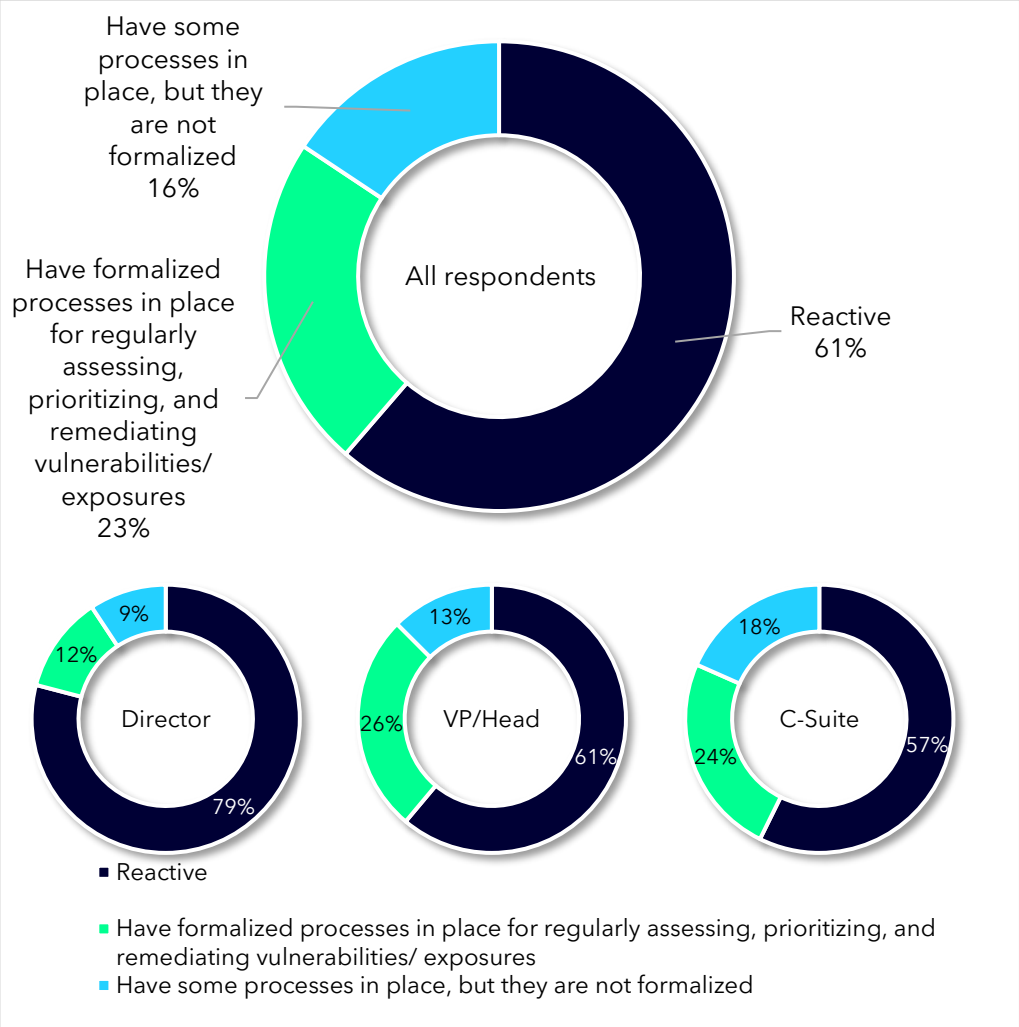


Figure 7: Companies' Description of their Vulnerability/Exposure Management Program

Companies' Processes for Addressing Exposures Across On-Prem and Hybrid Cloud Environments

The responses reveal that, in about half of organizations (47%), separate processes and/or teams are responsible for addressing exposures across on-prem and hybrid cloud environments.

In contrast, 42% of organizations manage exposures holistically, considering both on-prem and hybrid cloud environments as part of an integrated strategy. This means that the majority (58%) opt for ad-hoc or siloed approaches, relying on separate teams and processes for each environment. This puts organizations at a significant disadvantage in effectively combating the dynamic tactics of cyber adversaries, who often operate seamlessly across environments.

This suggests a need for organizations to assess their strategies for exposure management and consider whether a more integrated, holistic approach could enhance efficiency and effectiveness. The data highlights the ongoing challenge of aligning skill sets and tools across diverse environments, emphasizing the importance of strategic cohesion in managing exposures for both on-prem and hybrid cloud infrastructures.

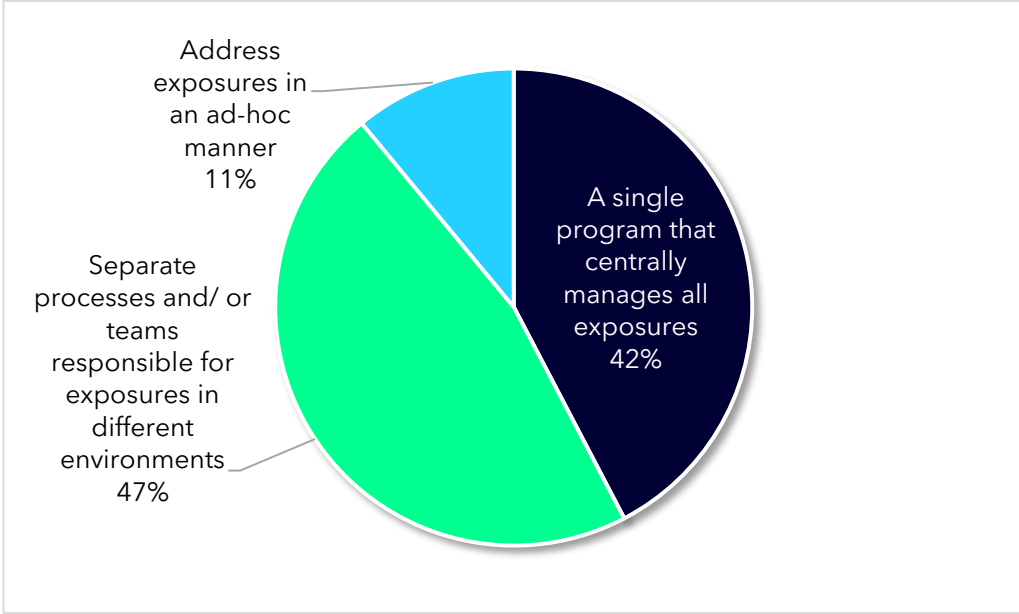


Figure 8: Companies' Processes for Addressing Exposures Across On-Prem and Hybrid Cloud Environments

Companies' Processes for Addressing Identity and Credential Related Exposures

About half of companies (51%) use a single program to centrally manage CVEs, misconfigurations, and identity-related exposures. The other portion (49%) uses ad-hoc or siloed processes.

The data also reveals that the use of single programs is more prevalent in smaller organizations, with larger companies (10,000+ employees) facing challenges in implementing such centralized programs. This may indicate that larger companies are potentially more sophisticated and integrated than medium-sized organizations, while the smallest entities might not be fully engaged in comprehensive exposure management practices.

The findings emphasize the need for scalable and integrated solutions, especially for larger enterprises, to effectively address identity and credential-related exposures and ensure a comprehensive security posture.

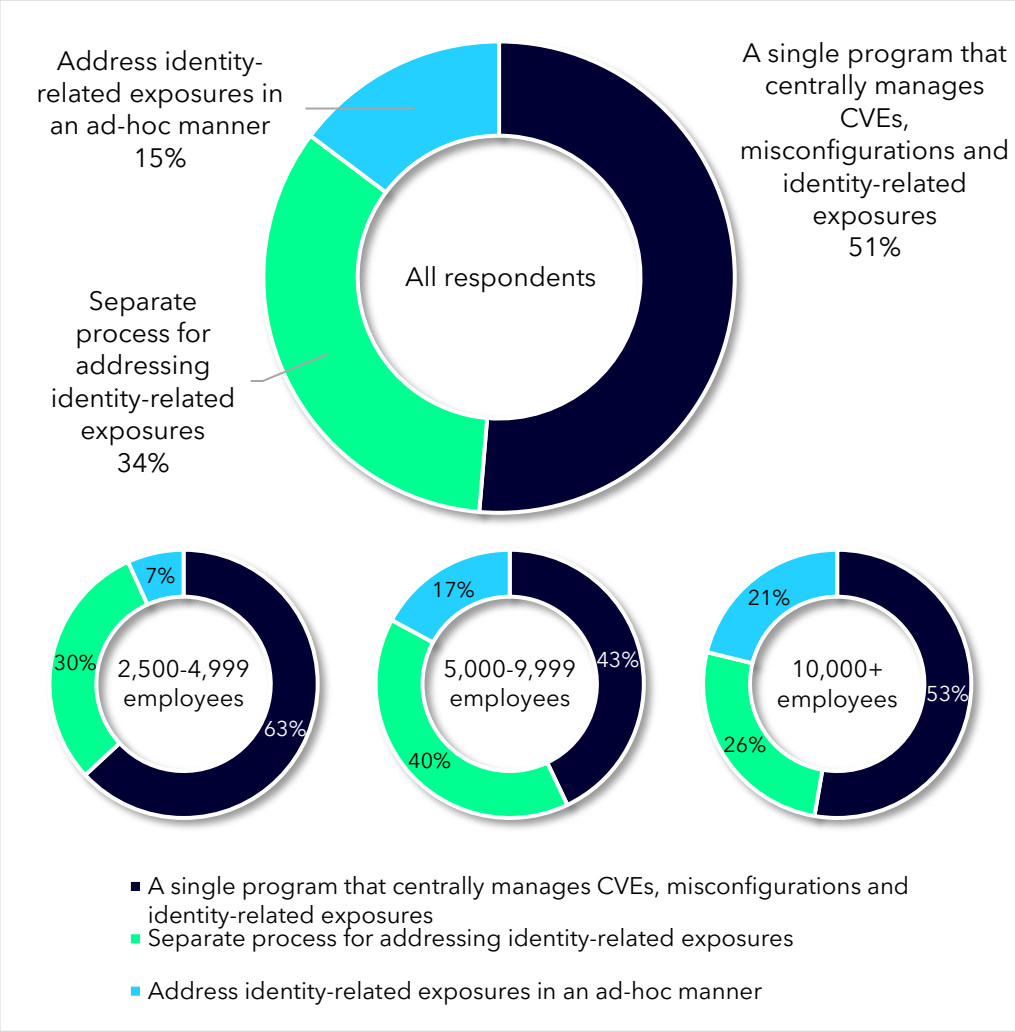


Figure 9: Companies' Processes for Addressing Identity and Credential Related Exposures

Biggest Opportunity for Improving Security Posture

A substantial 45% of companies identify their cloud environment as the most significant opportunity for improving their security posture. This perception reflects a concentrated focus on enhancing security measures within the cloud infrastructure.

In contrast, 23% of respondents believe that all environments are equally important for security improvements, highlighting a more balanced perspective.

Notably, a staggering 99% of companies acknowledge the potential for improving security posture in one or more environments. This sentiment underscores a widespread recognition of the evolving threat landscape.

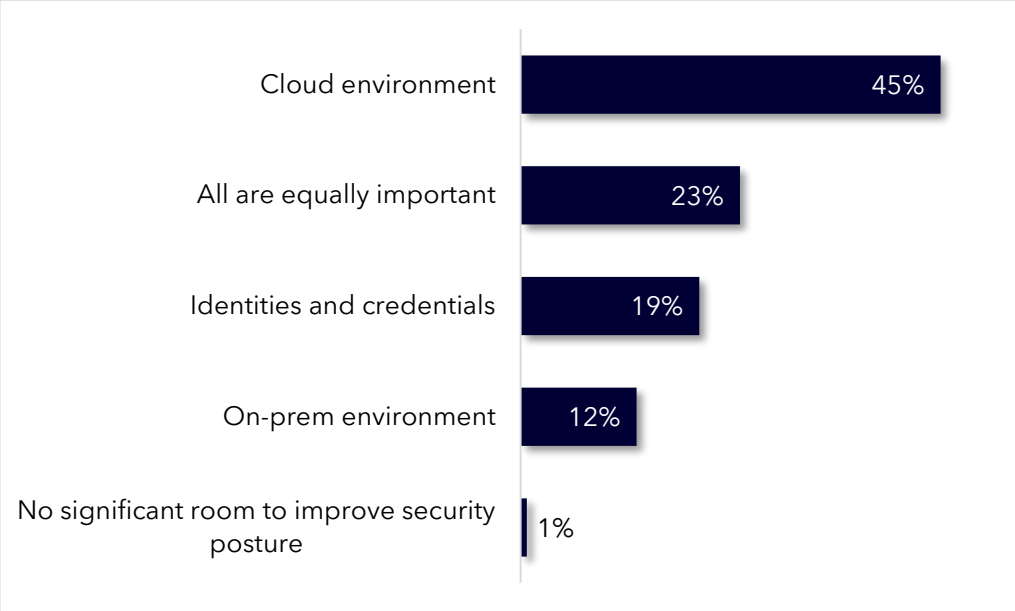


Figure 10: Biggest Opportunity for Improving Security Posture

Frequency of Inability to Remediate Exposures Due to Purchased Systems, Legacy Applications, Etc.

A striking 90% of companies frequently find themselves unable to remediate exposures due to factors like purchased systems and legacy applications.

To mitigate the impact of exposures that can't be remediated directly, organizations may consider alternative strategies. Understanding the attacker's potential actions and blocking them through alternative means becomes a crucial aspect of a proactive security approach. This can be accomplished through attack path modeling, which helps to visualize alternate remediation options when the most obvious ones are not viable.

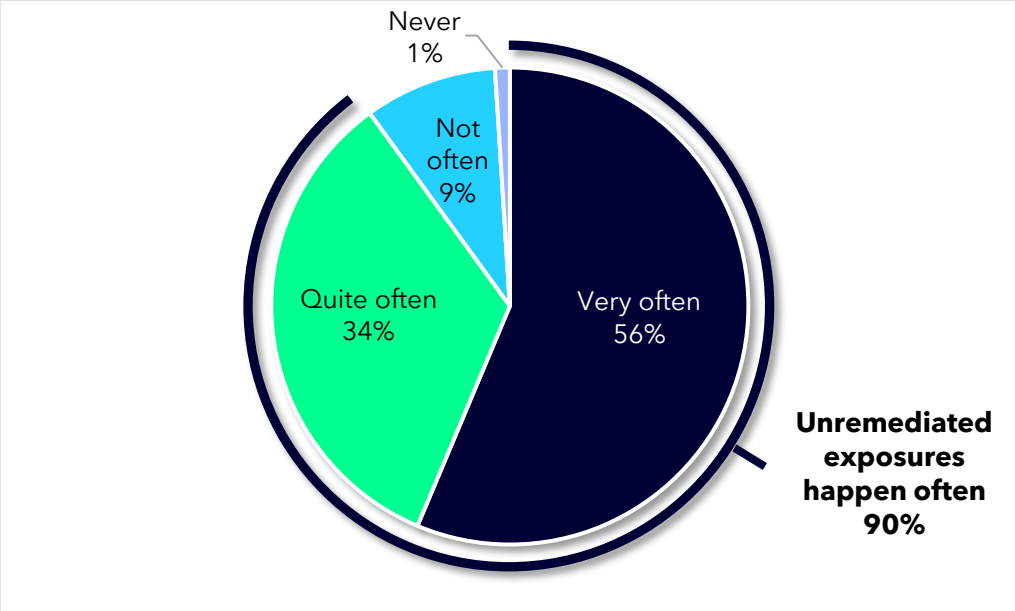


Figure 11: Frequency of Inability to Remediate Exposures Due to Purchased Systems, Legacy Application, etc.

Demographics

Country, Industry, Department, Job Seniority and Role

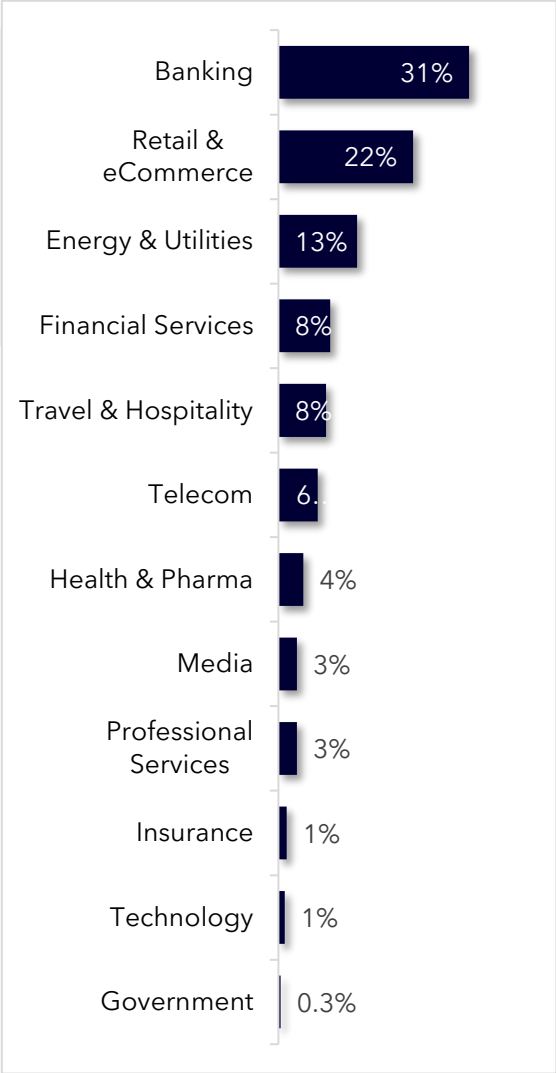


Figure 12: Industry

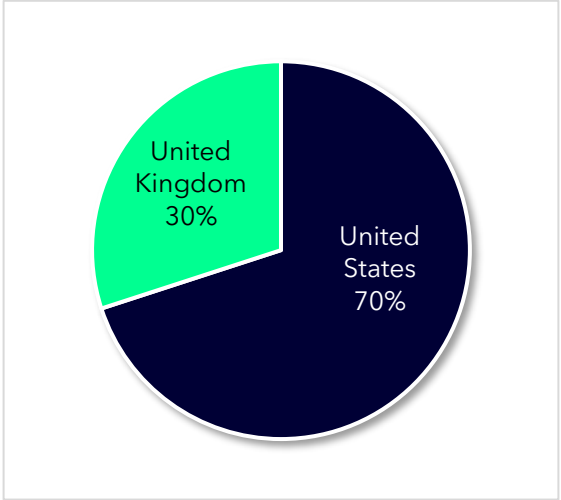


Figure 13: Country

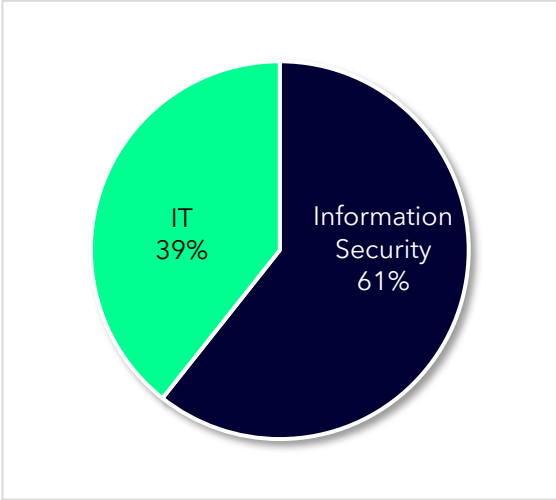


Figure 14: Department

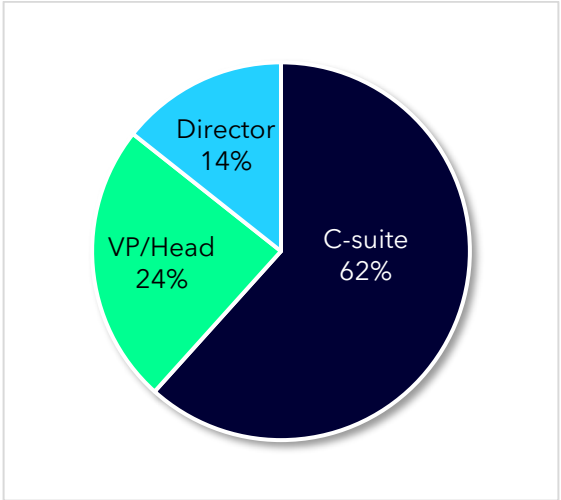


Figure 15: Job Seniority

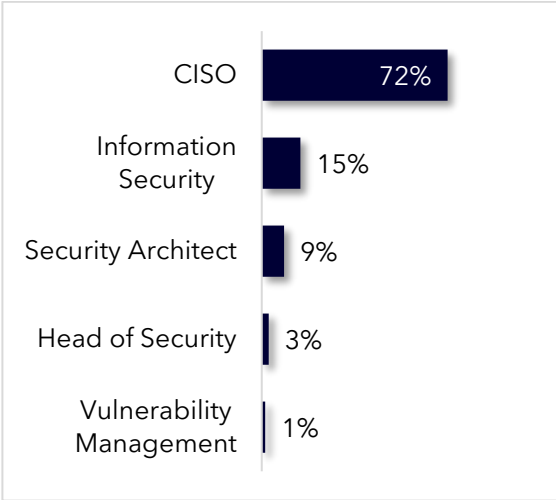


Figure 16: Role

Company Size and Role in Purchasing Cyber Security Products

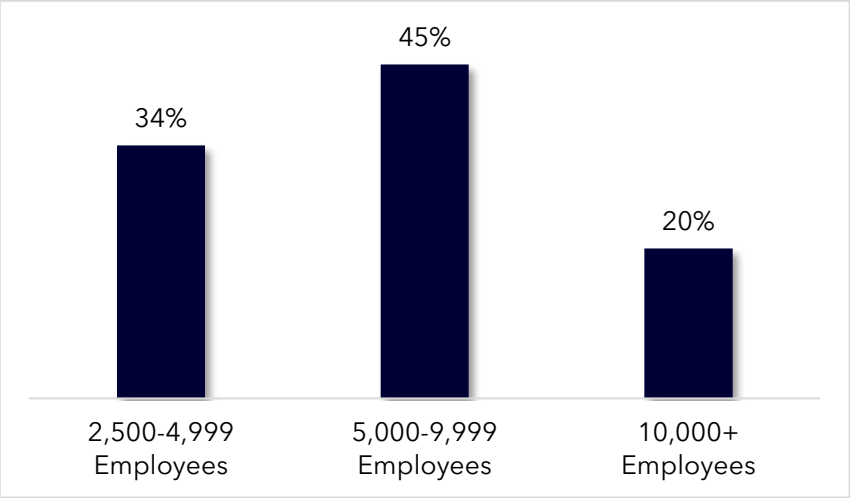


Figure 17: Company Size

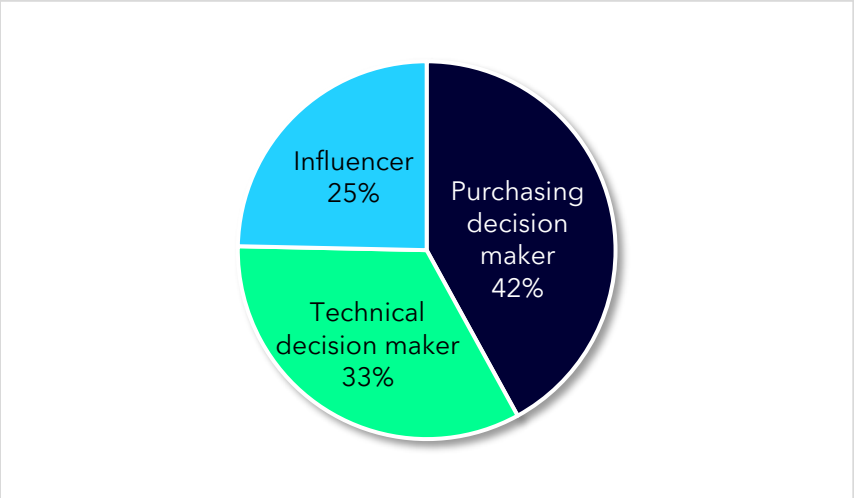


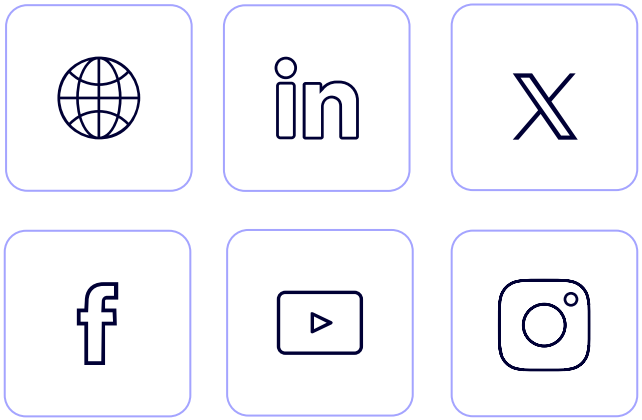
Figure 18: Role in Purchasing Cyber Security Products

About XM Cyber

XM Cyber is a leader in hybrid cloud exposure management that's changing the way organizations approach cyber risk. XM Cyber transforms exposure management by demonstrating how attackers leverage and combine misconfigurations, vulnerabilities, identity exposures, and more, across AWS, Azure, GCP and on-prem environments to compromise critical assets. With XM Cyber, you can see all the ways attackers might go, and all the best ways to stop them, pinpointing where to remediate exposures with a fraction of the effort. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia Pacific and Israel.

Request a Demo

For more information, please visit us:



info@xmcyber.com