PRAETORIAN

SURVEY REPORT

Continuous Offensive Security Outlook 2026

Get Started >

TABLE OF CONTENTS

03 Introduction

04 Respondent Demographic Summary

05 Executive Summary

07 Cybersecurity Controls and Processes

10 Tracking IT Asset Inventories

12 SecOps Teams Face a Heavy Vulnerability Workload

15 Risk Detection Through Multiple Sources

17 A Shift to Continuous Offensive Security

21 Conclusion: The Imperative for Continuous Offensive Security in 2026 and Beyond

23 Appendix

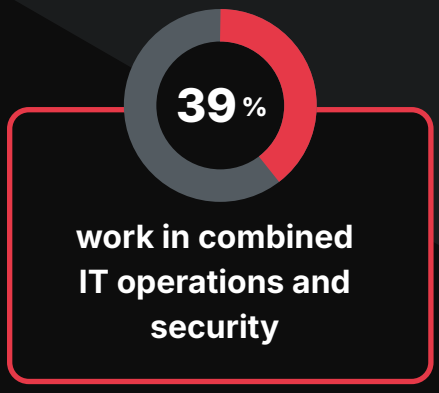
Introduction

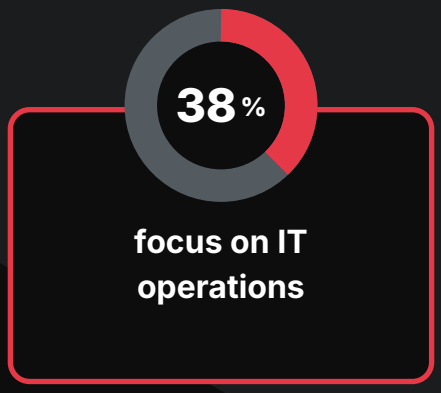
As we look to 2026, enterprises face mounting security challenges: an abundance of disconnected tools creating more noise than clarity, teams drowning in alerts, and critical vulnerabilities left unnoticed and drowned out by the sheer volume of alerts. The traditional security playbook isn't simply showing its age – in many cases it is actively holding companies back.

This report was built after surveying 263 leading enterprise IT and security professionals through an agnostic 3rd party research firm, which revealed the challenges were even more widespread than expected. Security teams are exhausted from managing an ever-growing collection of point solutions that operate in isolation, each adding to the onslaught of alerts while critical threats hide in plain sight. Meanwhile, CISOs struggle to demonstrate the real value of their security investments. Through this report you will discover how today's leading organizations are tackling these challenges and the continuous approach that shows a promising path forward. Whether you're looking to consolidate your security tools, improve threat detection, or better demonstrate security ROI, you'll find practical insights to help guide your strategy.

Respondent Demographic Summary

The survey respondents represent a diverse cross-section of IT and security leadership across enterprise organizations. Their roles break down as follows:





All participants work at large enterprises with revenues exceeding $1 billion:

The respondents are evenly distributed across key industries, with financial services, healthcare, and manufacturing each representing 14% of participants. For complete demographic details, please refer to the Appendix.

Executive Summary

As 2026 approaches, enterprises are reaching a critical inflection point. Traditional, point-in-time security strategies cannot keep pace with the realities of today's dynamic threat landscape. Leading organizations are shifting toward continuous offensive security—an approach that continuously tests and validates defenses in real time. Our research shows growing momentum for this forward-looking model, with CTEM (Continuous Threat Exposure Management) serving as one example of how enterprises are beginning to operationalize this shift.

Crisis of Confidence in Security Controls

Organizations express deep concerns about their security effectiveness. Despite heavy investment in security tools and processes, 64% report low to moderate confidence in their controls, and less than half believe their current approach performs adequately. Most see only modest improvements in their security posture, highlighting traditional approaches' limitations. The burden of manual processes weighs heavily, with 30% actively seeking solutions to reduce security workloads.

Vulnerability Management Burden

Despite quick response times to individual vulnerabilities, teams struggle with volume. Organizations maintaining backlogs of 100-999 unresolved vulnerabilities (41%) face difficult prioritization decisions, with 65% lacking confidence in their ability to assess business impact. Tool sprawl compounds this problem, as 37% attempt to coordinate between 6-19 different vulnerability scanning and asset discovery tools.

Asset Inventory Management Challenges

A dangerous disconnect exists between asset changes and monitoring capabilities. While half of organizations experience daily or weekly changes in their public-facing assets, only 15% express confidence in their ability to track all IT assets. More concerning, just 17% conduct daily inventories and 24% weekly inventories, leaving critical assets potentially exposed.

Multiple Risk Detection Hurdles

Security teams struggle to achieve comprehensive threat visibility. Nearly one-third cannot effectively correlate data across multiple sources, while 48% cite growing system complexity as their primary challenge. The infrequency of external vulnerability scanning—conducted only quarterly or annually by nearly half of organizations—further compromises security effectiveness. Despite recognizing these issues, 64% report only modest improvements in their risk detection processes.

EXECUTIVE SUMMARY CONTINUED

Strong Market Interest in Continuous Offensive Security

Organizations clearly recognize the need for change, with only 18% considering their current security tools sufficient. Half of the respondents prioritize enhanced threat intelligence capabilities, indicating a desire for more proactive security approaches. While interest in CTEM is high, organizations seek solutions that address both implementation complexity and budget constraints.

These findings point to a clear need for more integrated, automated approaches to threat exposure management. As organizations grapple with expanding attack surfaces, tool proliferation, and resource constraints, Continuous offensive security approaches emerge as promising solutions to transform security operations from reactive to proactive, enabling more efficient and effective threat management.

Cybersecurity Controls and Processes

To begin, each organization was asked how confident they are in their current security controls. 64% of respondents expressed significant concerns about the effectiveness of their cybersecurity efforts.

Level of Confident in the Effectiveness of Security Controls

The challenge of maintaining comprehensive visibility has become particularly severe as organizations expand their digital footprint. When asked further about confidence in their monitoring coverage:

- **38% expressed minimal to no confidence**
- **44% reported moderate confidence**
- **Only 14% felt highly confident in their ability to avoid monitoring blind spots**

These findings reveal a troubling reality: 82% of organizations recognize potential gaps in their security monitoring coverage. This lack of confidence potentially stems from several factors:

- **Rapid infrastructure changes outpacing monitoring capabilities**
- **Siloed security tools creating visibility gaps**
- **Growing complexity of environments**
- **Insufficient integration between security solutions**
- **Internal resource constraints limiting monitoring scope**

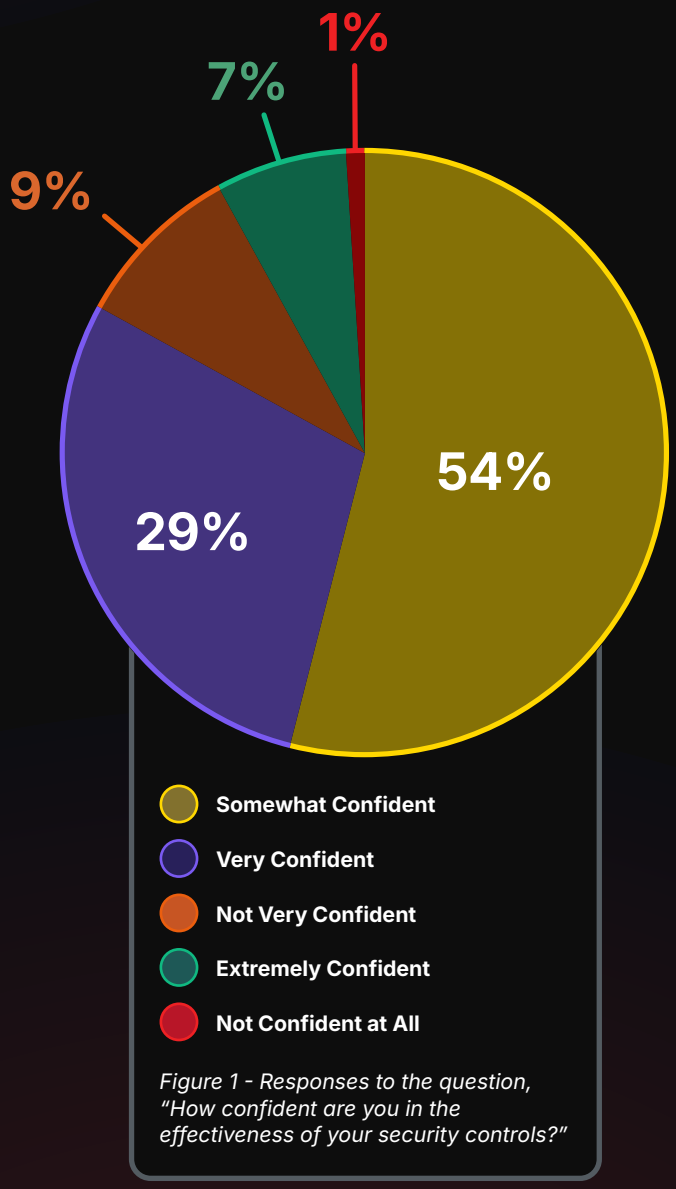
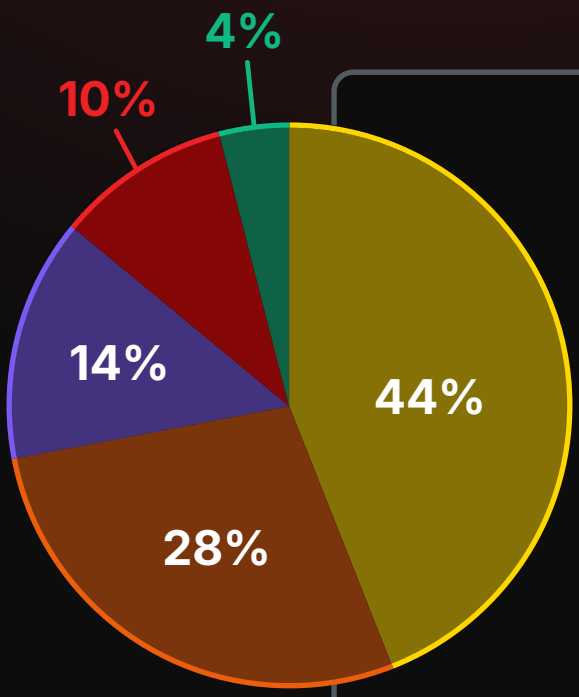


Figure 1 - Responses to the question, "How confident are you in the effectiveness of your security controls?"

The prevalence of blind spots represents an alarming gap in current security approaches, potentially leaving organizations exposed to undetected threats for extended periods.



How Well Current Security Approaches Anticipate New Attacks

However, respondents did note their security posture showed modest gains from the previous year. 62% said their organization's security posture had "improved somewhat" over the past year, with a further 17% saying it "improved significantly." An equal number said posture neither improved nor declined.

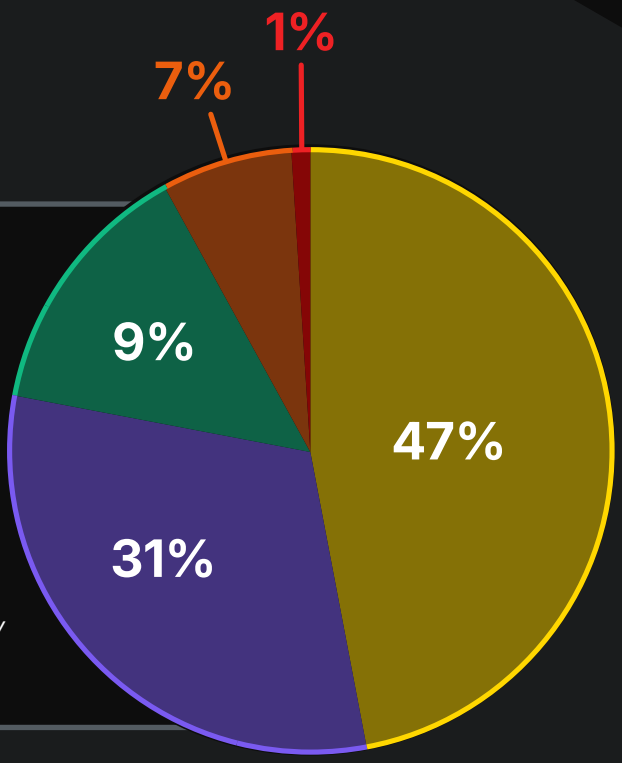
- Somewhat Confident
- Not Very Confident
- Very Confident
- Extremely Confident
- Not Confident at All

Figure 2 - Responses to the question, "How well does your current security approach anticipate new attacks?"

How an Organization's Security Posture has Changed Over the Past Year

- Moderately Well
- Not Very Well
- Fairly Well
- Very Well
- Not Well at All

Figure 3 - Responses to the question, "How has your organization's security posture changed over the past year?"



Possible explanations for the minimal improvements in posture were brought to light when respondents were asked what would motivate them to consider a new security solution.

- **30% seek substantial reduction in manual security workloads**
- **29% want significant improvements in threat detection**
- **29% desire more comprehensive visibility across their attack surface**

The consistent distribution across these factors suggests that organizations face multiple, equally pressing challenges in their security operations.

Organizations seek solutions that address both implemenation complexity and budget constraints.

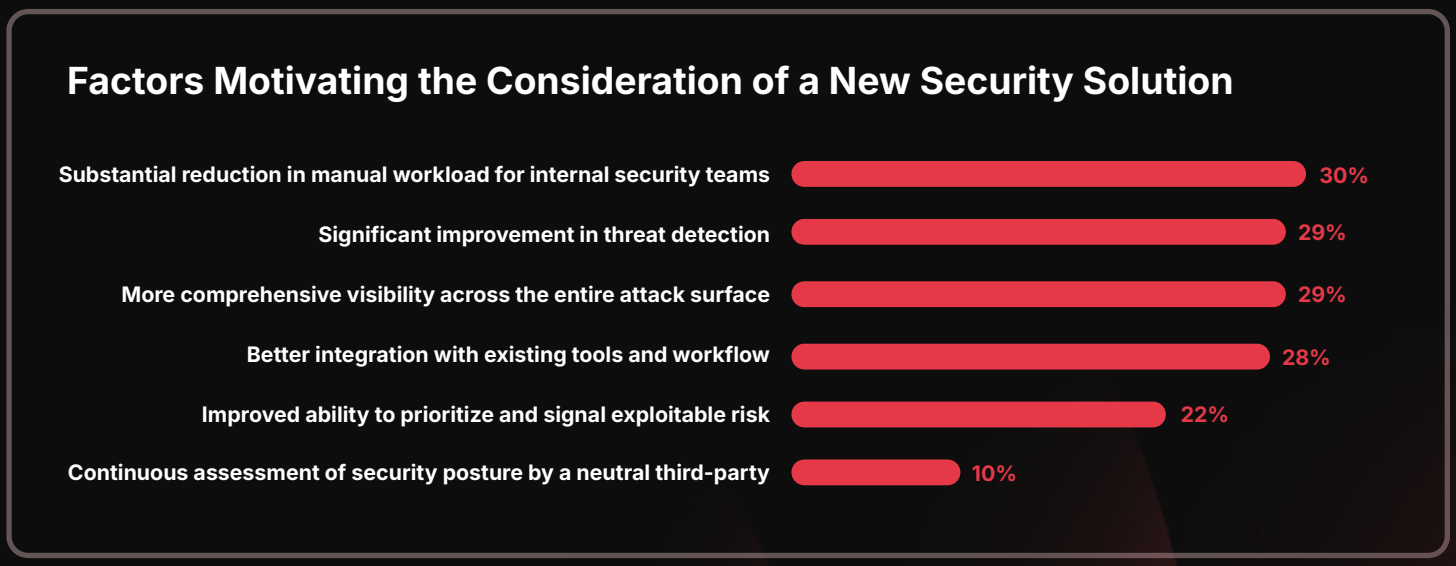


Figure 4 - Responses to the question, "Which of the following would most motivate you to consider a new security solution?"

Tracking IT Asset Inventories

Defending the attack surface poses a fundamental challenge: organizations struggle to track their IT assets effectively. When asked about their ability in identifying all assets across their IT ecosystem, 15% of respondents admitted they were either "not very confident" or "not confident at all." This represents one in six organizations that cannot reliably identify their complete IT asset inventory—a significant security vulnerability. Furthermore, 49% reported being only "somewhat confident" in their asset identification capabilities. Combined, these findings reveal that nearly two-thirds of organizations lack strong confidence in their ability to maintain comprehensive visibility of their IT assets.

Asset tracking challenges stem largely from the rapid pace of change in IT environments. Half of all organizations report that their public-facing IT assets change daily or weekly.

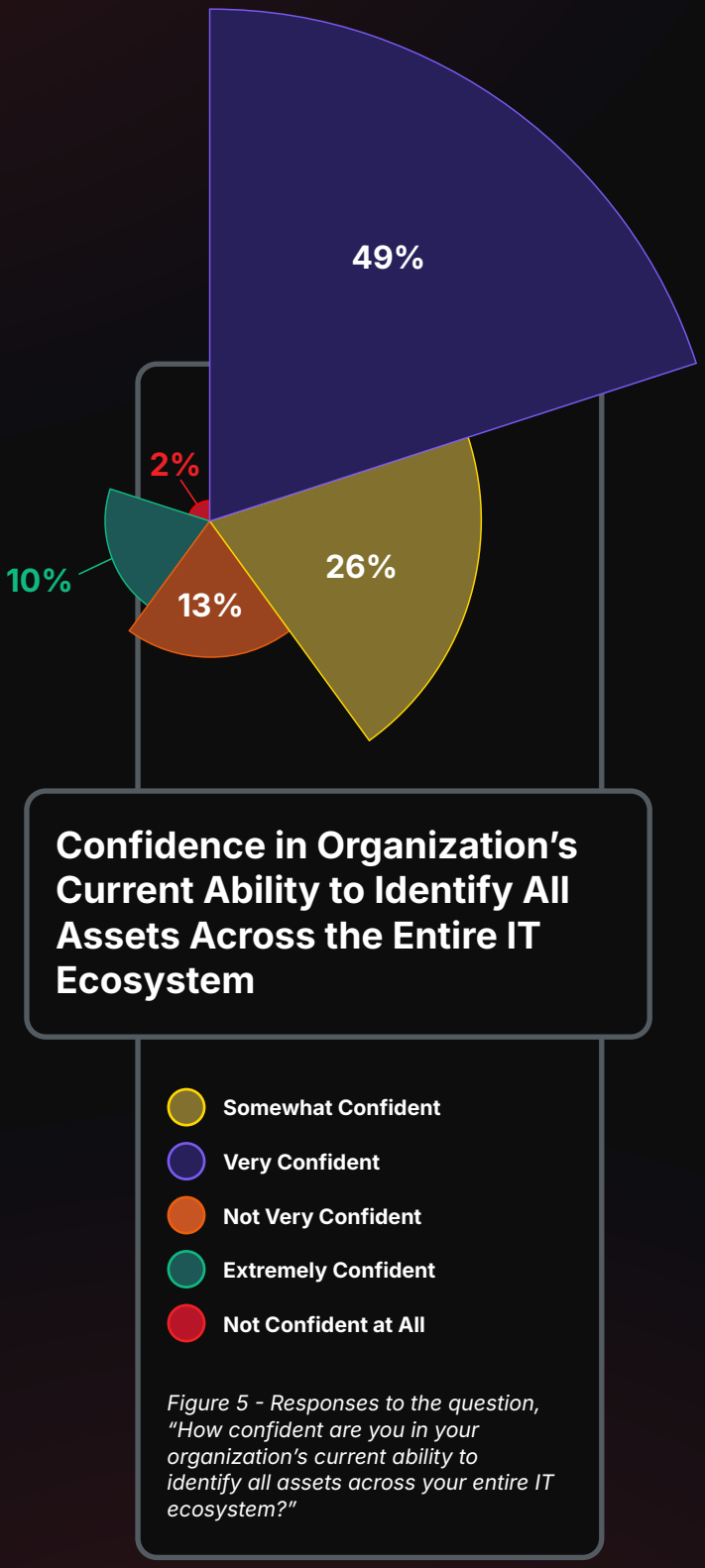


Figure 5 - Responses to the question, "How confident are you in your organization's current ability to identify all assets across your entire IT ecosystem?"

Rate of Change for Organization's Public-Facing Assets

Figure 6 - Responses to the question, "How often do you believe your organization's public-facing assets change?"

With the rapid rate of change in mind, the infrequency of asset inventory practices becomes particularly highlighted. Only 17% of organizations conduct daily inventory of their complete asset landscape, while 24% perform weekly checks. Six in ten organizations rely on monthly, quarterly, or annual inventory cycles.

These extended gaps between inventories significantly compromise an organization's ability to defend their attack surface effectively. In an environment where threats evolve daily and assets change constantly, periodic asset inventory approaches leave organizations exposed to unnecessary risk.

Despite 77% of organizations using automated asset tracking tools, most conduct inventories infrequently. The relationship between automation and confidence reveals a surprising pattern: respondents who reported the highest confidence in asset identification rarely use automated tools. Conversely, those with the lowest confidence levels are more likely to lack automation. This inverse relationship suggests that current automated solutions may not be delivering their intended benefits.

Frequency of Complete Asset Inventory

Figure 7 - Responses to the question, "How often do you take inventory of your complete asset inventory?"

The impact of automated asset tracking tools on confidence in ability to identify all assets.	Use automated asset tracking tools	Do not use automated asset tracking tools
Extremely Confident	5%	0
Very Confident	17%	3%
Moderately Confident	45%	46%
Slightly Confident	24%	37%
Not Confident at All	8%	14%

SecOps Teams Face a Heavy Vulnerability Workload

The survey findings reveal widespread challenges with vulnerability management, particularly within Security Operations (SecOps) teams. While 63% of organizations rely on SecOps for vulnerability management, only 20% maintain dedicated vulnerability teams.

Responsibility for Asset Discovery and Associated Vulnerabilities

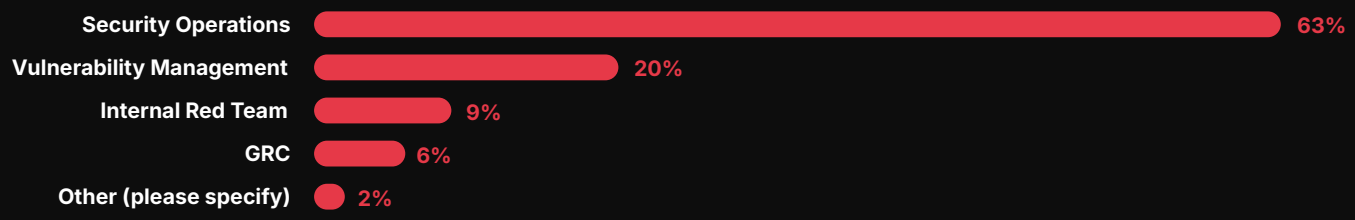


Figure 8 - Responses to the question, "What group in your organization is responsible for discovering assets and associated vulnerabilities in your infrastructure?"

SecOps teams demonstrate strong capabilities in detecting novel zero-day vulnerabilities, though this speed must be viewed within a broader context. While 30% can identify these threats within 24 hours, and 39% detecting them within 24 to 72 hours, rapid detection alone doesn't tell the complete story. This detection capability, while impressive, faces several critical challenges:

- Detection speed doesn't always translate to successful remediation
- Teams often struggle to prioritize zero-days among existing vulnerability backlogs
- Fast detection can be undermined by slow patch deployment
- Resource constraints may delay response despite quick identification
- The growing sophistication of zero-days can complicate even rapid detection

Average Time to Detect and Respond to New Vulnerabilities

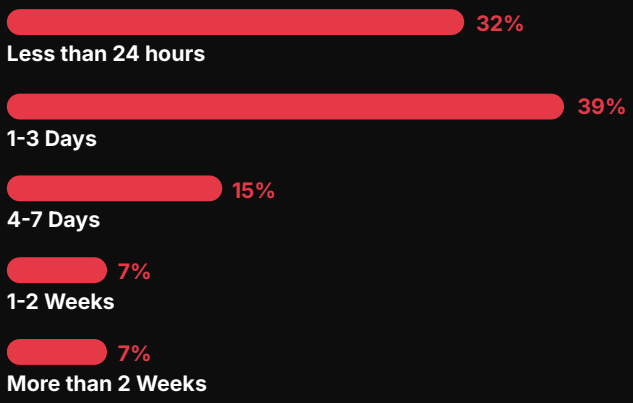


Figure 9 - Responses to the question, "On average, how long does it take your organization to detect and respond to new vulnerabilities?"

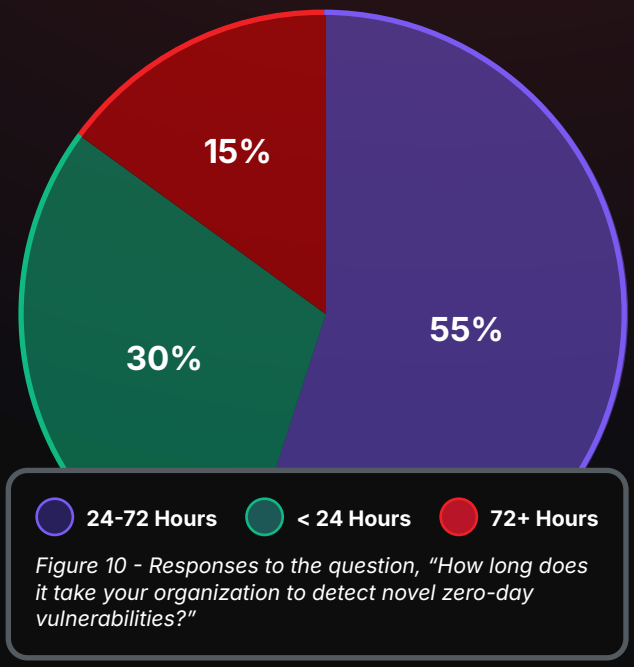


Figure 10 - Responses to the question, "How long does it take your organization to detect novel zero-day vulnerabilities?"

Time Required to Detect Novel Zero-Day Vulnerabilities

Despite reasonable detection and response times, vulnerability remediation backlogs have reached unmanageable levels. 41% of organizations carry between 100-999 unresolved vulnerabilities, while 27% face backlogs of 1,000-10,000 vulnerabilities. More alarming still, **one in ten organizations reports backlogs exceeding 10,000 vulnerabilities.**

The sheer number of backlogged vulnerabilities creates a dangerous scenario where attackers have an extensive menu of potential vulnerabilities to exploit. Even with strong detection capabilities, organizations carrying thousands of unresolved vulnerabilities remain exposed to potential compromise.

Number of Vulnerabilities Carried in Triage Backlogs

Figure 11 - Responses to the question, "How many vulnerabilities do you carry in your triage backlog?"

Organizations continue to face vulnerability prioritization battles: the inability to effectively assess security issues based on contextualized business risk rather than solely relying on a standardized scoring system. Nearly two-thirds of organizations (65%) lack full confidence in their ability to make these crucial prioritization decisions, with 12% expressing minimal or no confidence in their approach.

Nearly two-thirds of organizations lack full confidence in their ability to make crucial prioritizations decisions.

68% of organizations face backlogs of 100-10,000 untriaged vulnerabilities at any given time without strong prioritization abilities.

The problem is compounded by tool sprawl. 37% of organizations juggle between 6 and 19 different Asset discovery tools, undermining the traditional narrative of vulnerability management through a "single pane of glass."

The combination of extensive backlogs and tool sprawl creates a self-perpetuating cycle: more tools generate more alerts, further overwhelming SecOps teams' ability to effectively prioritize and address vulnerabilities. This cycle continues to widen the gap between vulnerability discovery and remediation efforts, leaving organizations increasingly exposed to potential compromises.

Number of Tools Does Leveraged for Vulnerability Scanning and Asset Discovery

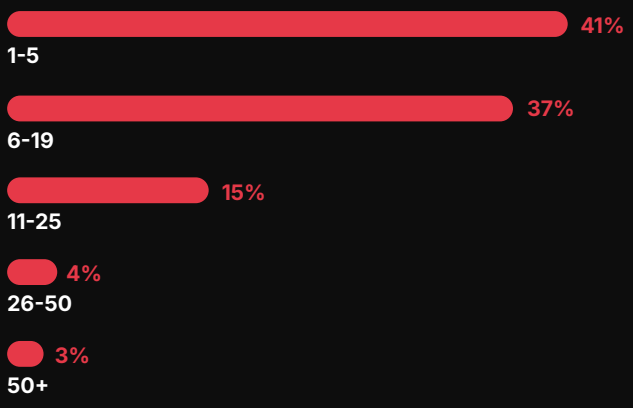


Figure 13 - Responses to the question, "How many tools does your organization leverage for vulnerability scanning and asset discovery?"

Ability to Prioritize Vulnerabilities Based on Real-World and Business Impact vs. CVSS

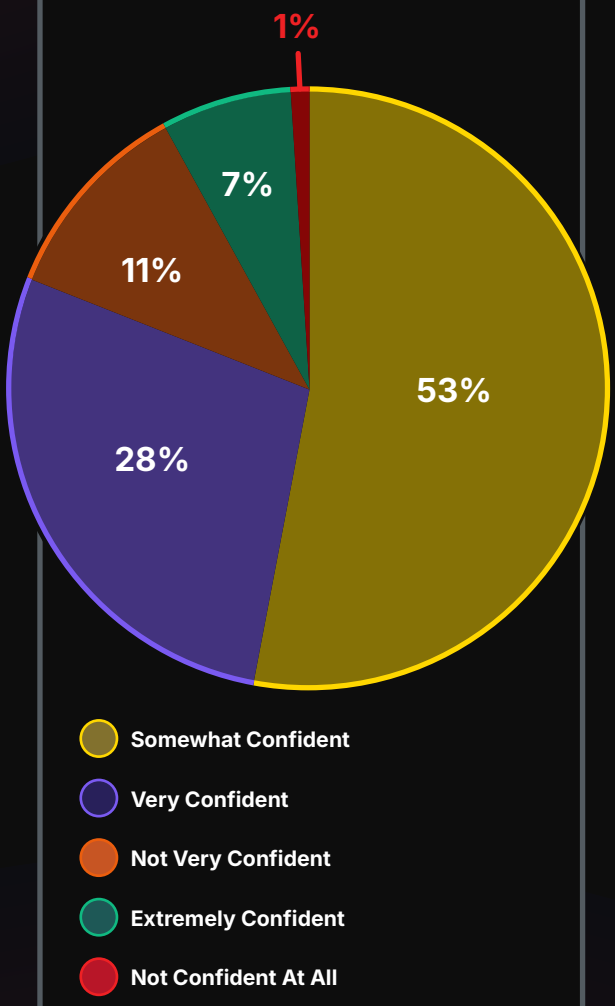


Figure 12 - Responses to the question, "What is your level of confidence in your organization's ability to prioritize vulnerabilities based on real-world and business impact as opposed to a CVSS? (Common Vulnerability Scoring System)"

Risk Detection Through Multiple Sources

SecOps teams face several key battles combating risk detection. When asked about their most frustrating aspects of threat and vulnerability management:

32% cited difficulty correlating data from multiple sources as their primary challenge. Alert overload ranked second at 19%, while 17% pointed to a lack of actionable insights.

These compounding challenges explain the extensive triage backlogs and low confidence in risk prioritization plaguing many organizations. Without the ability to effectively correlate data, filter unnecessary alerts, and generate actionable insights, security teams find themselves in a reactive cycle, continuing to fall further behind.

Most Frustrating Aspects of Current Threat and Vulnerability Management Processes

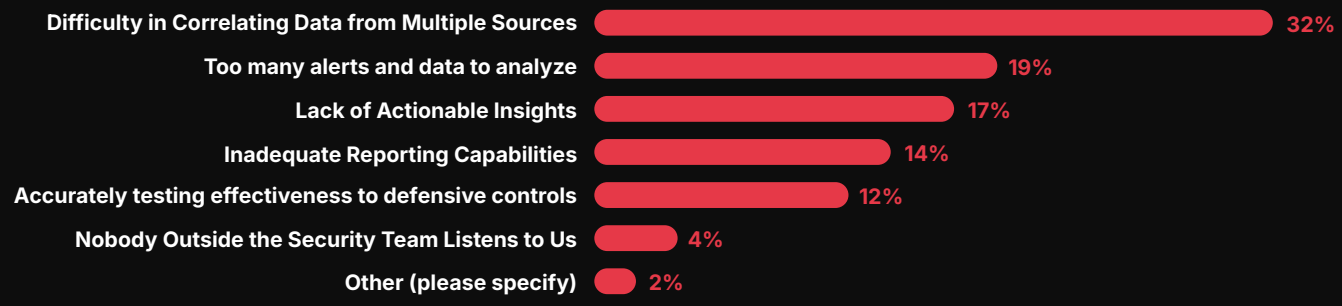


Figure 14 - Responses to the question, "What is the most frustrating aspect of your current threat and vulnerability management process?"

Complexity stands out as the dominant challenge in managing evolving threats, with 48% of respondents identifying it as their most significant obstacle. Insufficient threat intelligence follows at 17%, while resource constraints and alert fatigue each affect 15% of organizations. Together, these challenges reveal a fundamental lack of visibility into the threat landscape.

Most Significant Challenges in Keeping up With the Evolving Threat Landscape

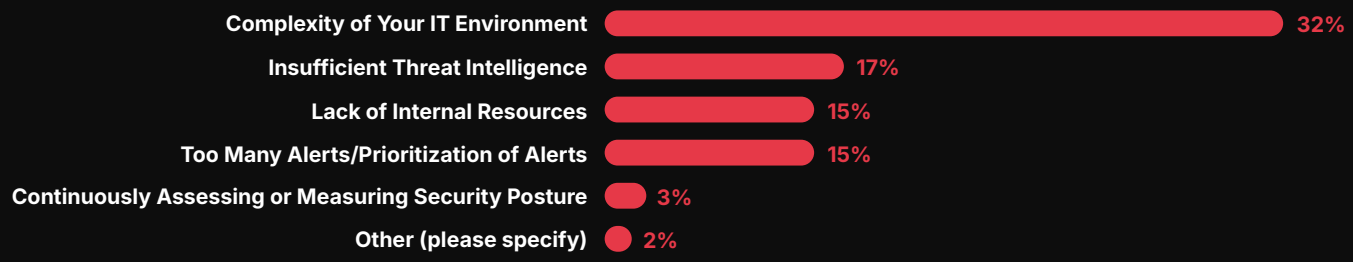


Figure 15 - Responses to the question, "What is the most significant challenge your team faces in keeping up with the evolving threat landscape?"

Frequency of Vulnerability Scanning Externally Facing Applications

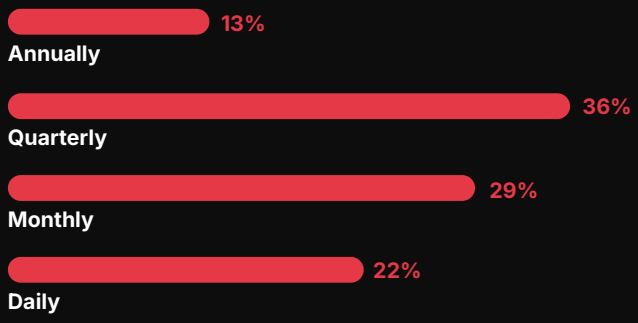
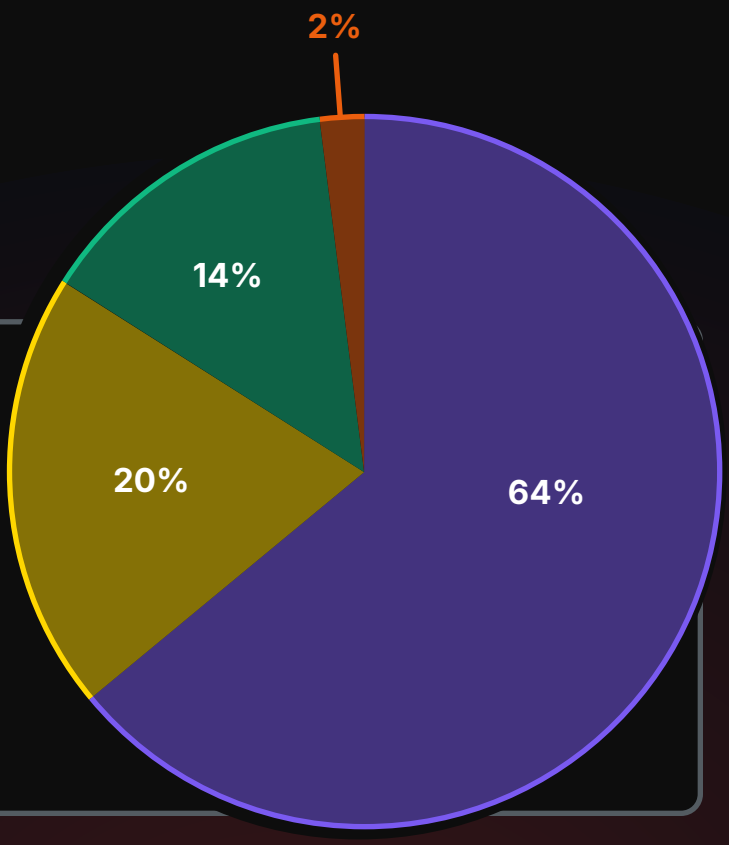


Figure 16 - Responses to the question, "How often does your organization scan its externally facing applications and infrastructure for security vulnerabilities?"

The infrequency of vulnerability scanning amplifies these challenges. Nearly half of organizations conduct security scans of their external applications and infrastructure only quarterly or annually. This scanning cadence falls dangerously behind the rapid pace of infrastructure changes.

Improvements in Processes for Detecting Risks Changed Over the Past Year

Figure 17 - Responses to the question, "How has your organization's process for detecting risks changed over the past year?"



A Shift to Continuous Offensive Security

Organizations overwhelmingly recognize the need for continuous threat testing and management, with 90% of respondents believing their security would benefit from such an approach. This strong interest has naturally led to increased awareness of Continuous Threat Exposure Management (CTEM) solutions, with 58% of security professionals now aware of the approach.

However, understanding of CTEM's distinct advantages over traditional vulnerability management remains uneven. While 40% of respondents report moderate familiarity with these differences, 23% acknowledge only slight familiarity. This knowledge gap is understandable given CTEM's emergence as a newer paradigm in security management. As organizations move beyond conventional periodic scanning and reactive security measures, many are still learning how CTEM's continuous, proactive approach can transform their security operations.

Familiarity with Differences Between Continuous Threat Exposure Management (CTEM) and Traditional Vulnerability Management

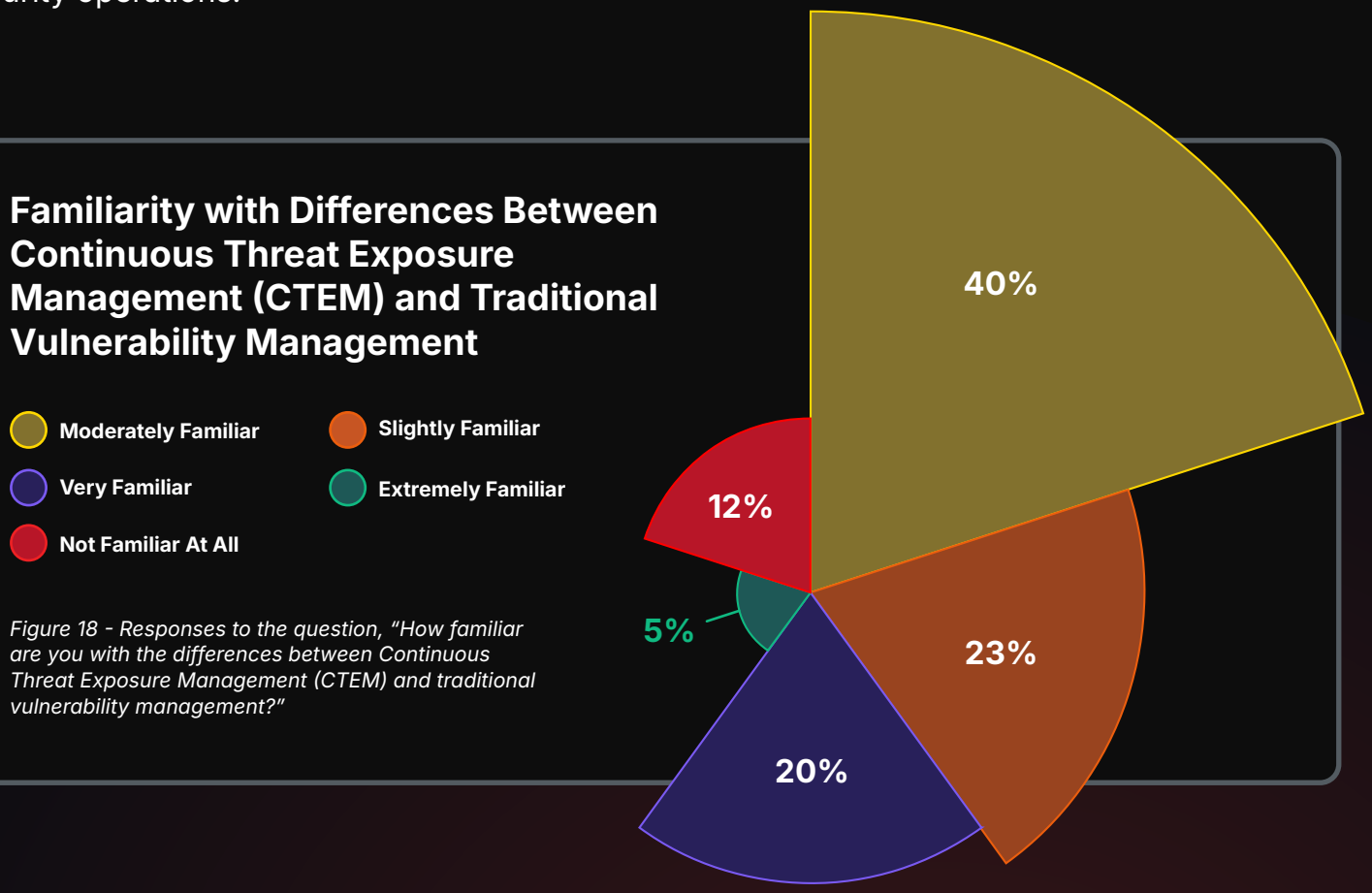


Figure 18 - Responses to the question, "How familiar are you with the differences between Continuous Threat Exposure Management (CTEM) and traditional vulnerability management?"

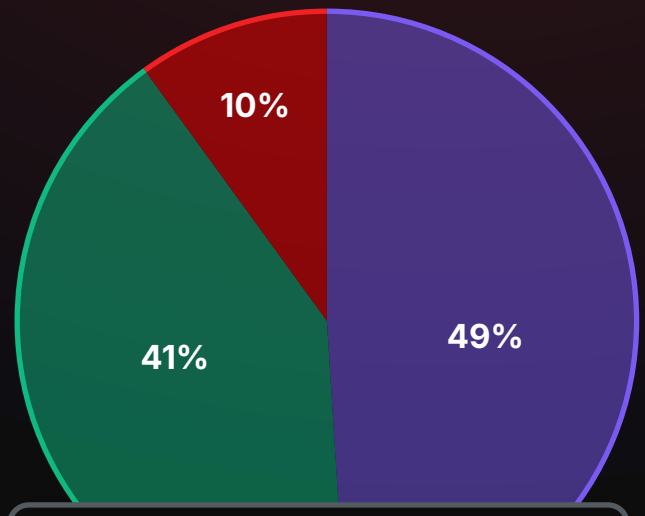


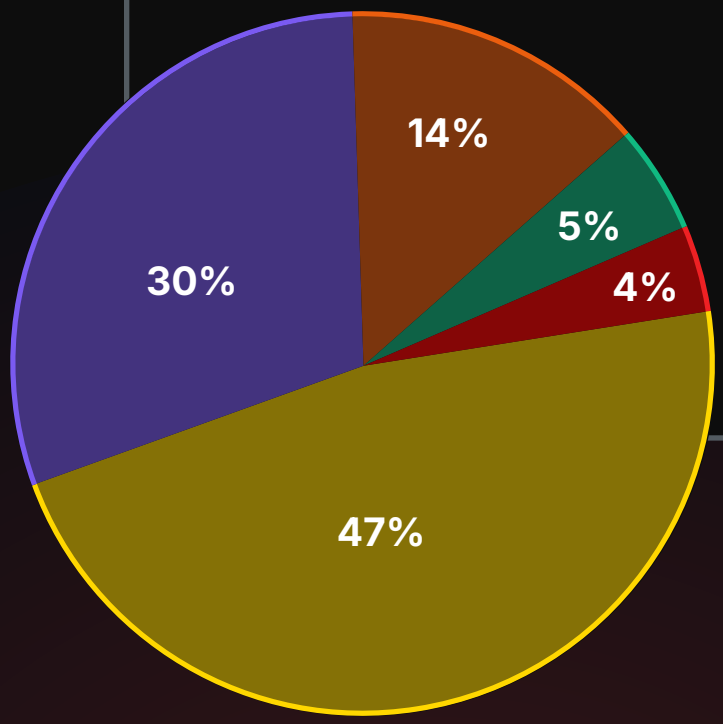
Figure 19 - Responses to the question, "Would you and your organization benefit from service where your company's threat exposure was tested and managed continuously?"

Perception of Benefit from Continuous Monitoring and Management of Threat Exposure

Organizations' strong interest in continuous threat monitoring reflects a growing recognition that current security approaches fall short as **nearly two-thirds of organizations recognize fundamental inadequacies in their current security approach.**

Perceptions of current security tools vs the need for future-focused continuous offensive security solutions in 2026.

Figure 20 - Responses to the question, "To what extent do you believe your current security tools and processes are sufficient, reducing the need for a CTEM solution?"



Organizations have clear priorities for their desired threat monitoring capabilities. When ranking preferred features, three key capabilities emerged:

Threat intelligence leads the requirements, with 50% of respondents ranking it as their top or second choice. Organizations also prioritize actionable insights and remediation guidance (37%) and vulnerability prioritization (34%).

These desired capabilities directly align with core CTEM functionality, suggesting that organizations increasingly recognize the value of integrated, intelligence-driven security solutions. The emphasis on actionable insights and prioritization reflects a growing desire to move beyond basic threat detection and towards a more strategic security management solution.

Ranking of Capabilities When Selecting a Product or Service that Continuously Monitors Threat Exposure

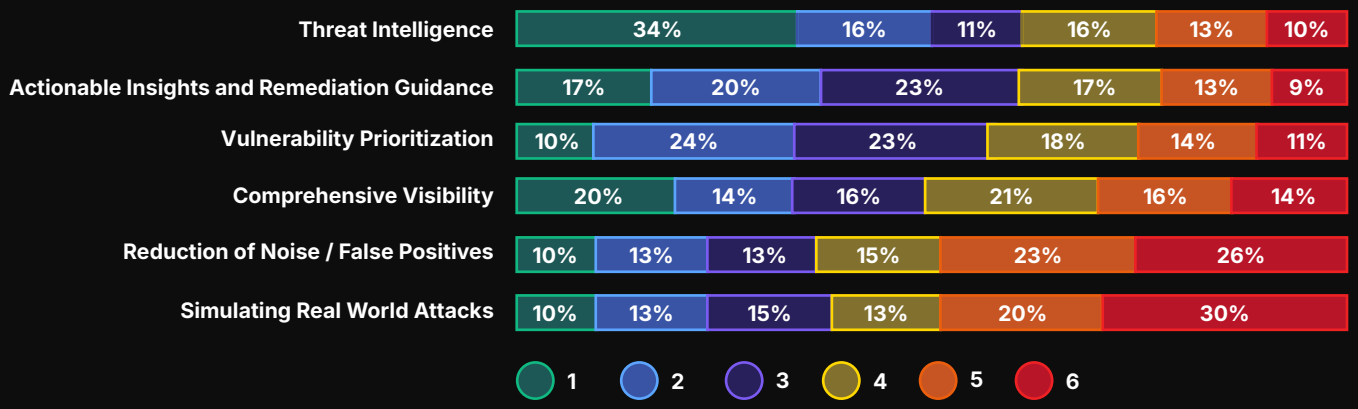


Figure 21 - Responses to the question, "How would you rank these capabilities when selecting a product or service that continuously monitors your threat exposure?"

The survey reveals strong momentum toward CTEM adoption in the coming year. A majority of organizations (52%) indicate they are "somewhat likely" or "extremely likely" to implement CTEM solutions within 12 months. While one-third remain neutral, only 15% express reluctance toward adoption.

The high proportion of organizations planning CTEM adoption, combined with low resistance, suggests the security industry is approaching a significant transformation in how organizations manage their threat exposure.

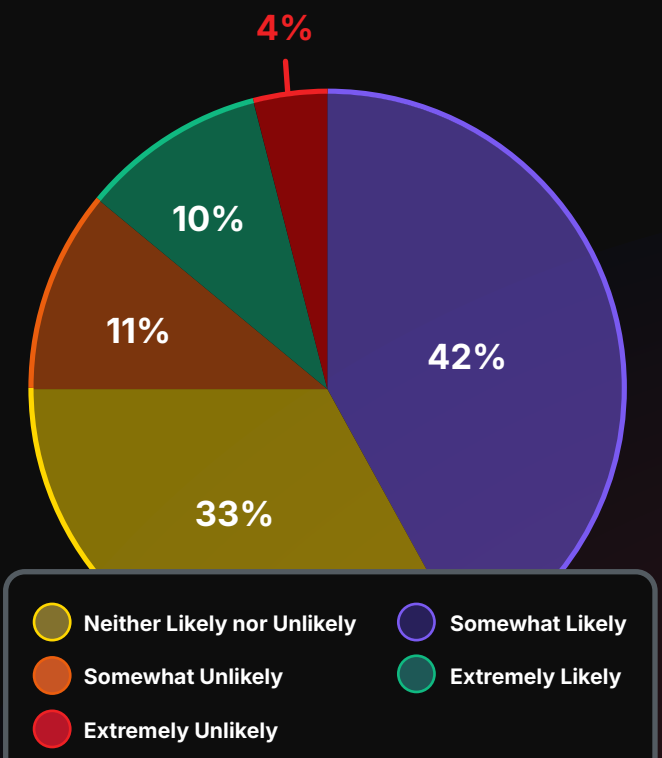


Figure 22 - Responses to the question, "How likely are you to consider adopting a continuous offensive security threat exposure management approach in the next 12 months?"

Projected Likelihood of Adopting Continuous Offensive Security Approaches in 2026

Despite strong interest in CTEM, organizations face several significant barriers to implementation. Implementation complexity emerges as the primary concern, with 63% of respondents ranking it as their first or second most significant obstacle. This reflects the challenges of integrating new security approaches into existing environments while maintaining operational continuity.

Budget constraints present the second major hurdle, cited by 43% of organizations. Other key implementation challenges include:

- Potential disruption to current operations (36%)
- Lack of skilled security personnel (30%)

These obstacles reveal broader industry challenges:

- Organizations struggle to balance security advancement with operational stability
- Security teams face resource constraints while threats continue to evolve
- The cybersecurity skills gap impacts adoption of new security approaches
- Many organizations need guidance on how to implement CTEM without disrupting existing security operations

Understanding these barriers is crucial for successful CTEM adoption. Organizations need clear implementation roadmaps that address complexity concerns, demonstrate ROI for budget justification, and minimize operational disruption.

Projected Obstacles to Implementing Continuous Offensive Security Solutions in 2026

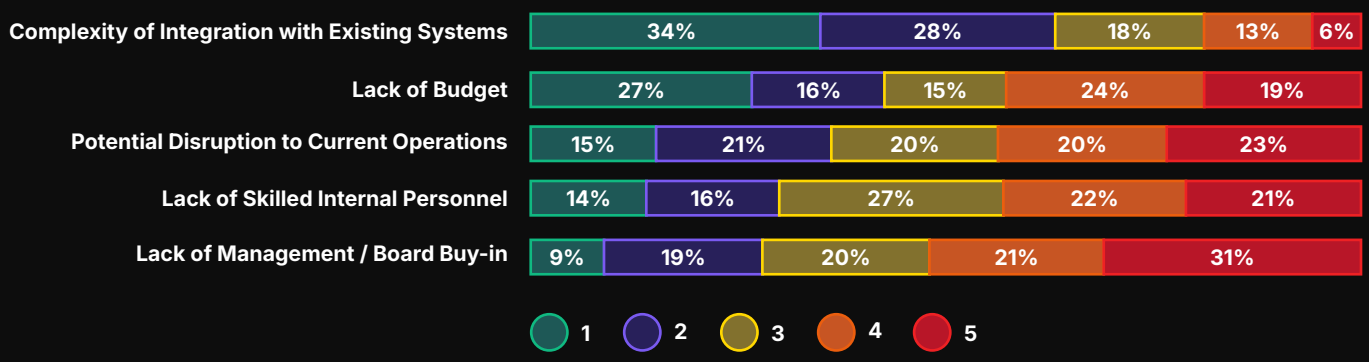


Figure 23 - Responses to the question, "How would you rank these obstacles to implementing a Continuous Threat Exposure Management solution in your organization? (Drag / drop choices in the order of most difficult to least)"

Conclusion: The Imperative for Continuous Offensive Security in 2026 and Beyond

The cybersecurity landscape has reached a critical inflection point. Traditional security approaches—marked by periodic assessments, reactive responses, and siloed tools—can no longer effectively protect organizations against today's dynamic threats. Through this study a few key findings came to the forefront:

- Security teams lack confidence in their current controls and capabilities
- Attack surfaces are expanding faster than traditional tools can monitor
- Asset inventory processes fail to keep pace with infrastructure changes
- Vulnerability backlogs continue to grow despite increased resources
- Tool proliferation creates complexity rather than clarity

Continuous offensive security—whether through CTEM or other continuous approaches—represents a fundamental shift in security strategy, enabling organizations to move from reactive defense to proactive risk reduction. This approach integrates:

- Continuous IT asset monitoring
- Comprehensive Attack Surface Management (ASM)
- Intelligence-driven vulnerability management
- Regular breach and attack simulation
- Integrated threat intelligence
- Ongoing penetration testing

The strong market interest in CTEM—particularly its threat intelligence capabilities—reflects growing recognition that security must evolve. As organizations face increasingly sophisticated threats across ever-expanding attack surfaces, CTEM's integrated, continuous approach offers a clear path forward for both SecOps teams and their IT partners.

The time for transformation is here. Organizations that will thrive in 2026 and beyond are those that move beyond static, fragmented programs and embrace a continuous offensive security mindset—where CTEM and other continuous methodologies serve as tools within a broader transformation.

Now what? Security leaders must act decisively:

Reevaluate

Audit your current program and identify where point-in-time testing or siloed tools create blind spots.

Restructure

Prioritize integration, automation, and continuous validation across your attack surfaces.

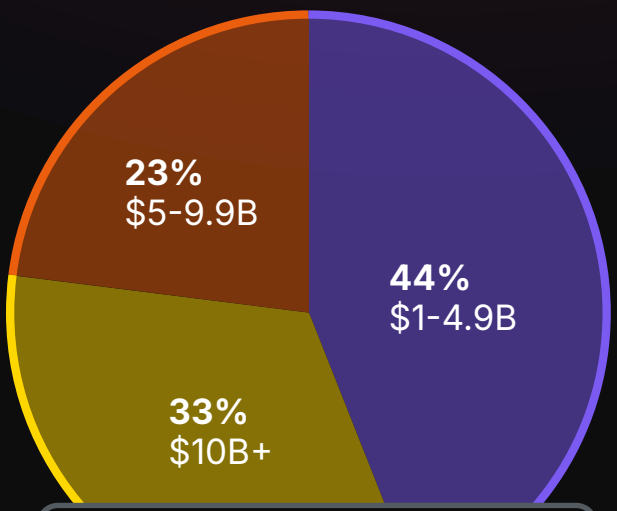
Reposition

Elevate board-level conversations from tool spend to measurable reduction of material risk.

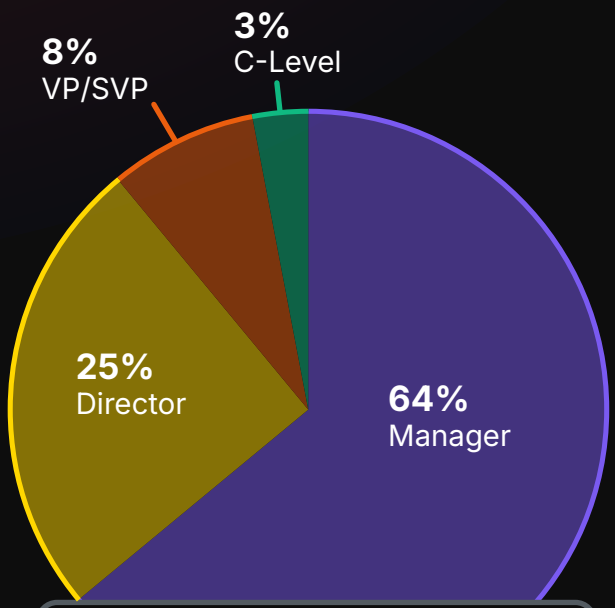
The mandate for 2026 is clear: enterprises must adopt continuous offensive security as their operating model, not an add-on. Those who lead this shift will set the standard for resilience in the years ahead.

For more information, please visit praetorian.com

Appendix: Respondent Demographic Detail

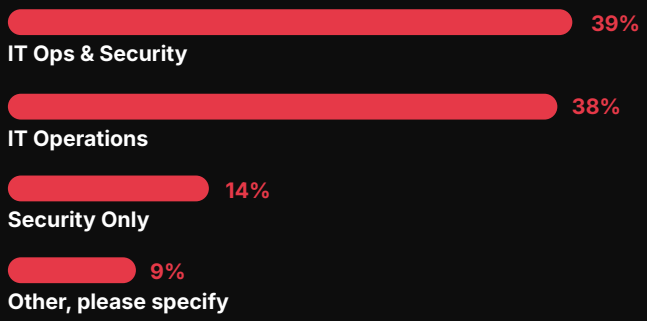


Company Size



Role with Organization

Job Role/Function



Primary Industry