seemplicity

2026 State of Exposure Management

Operational strain, remediation bottlenecks and the evolving role of AI

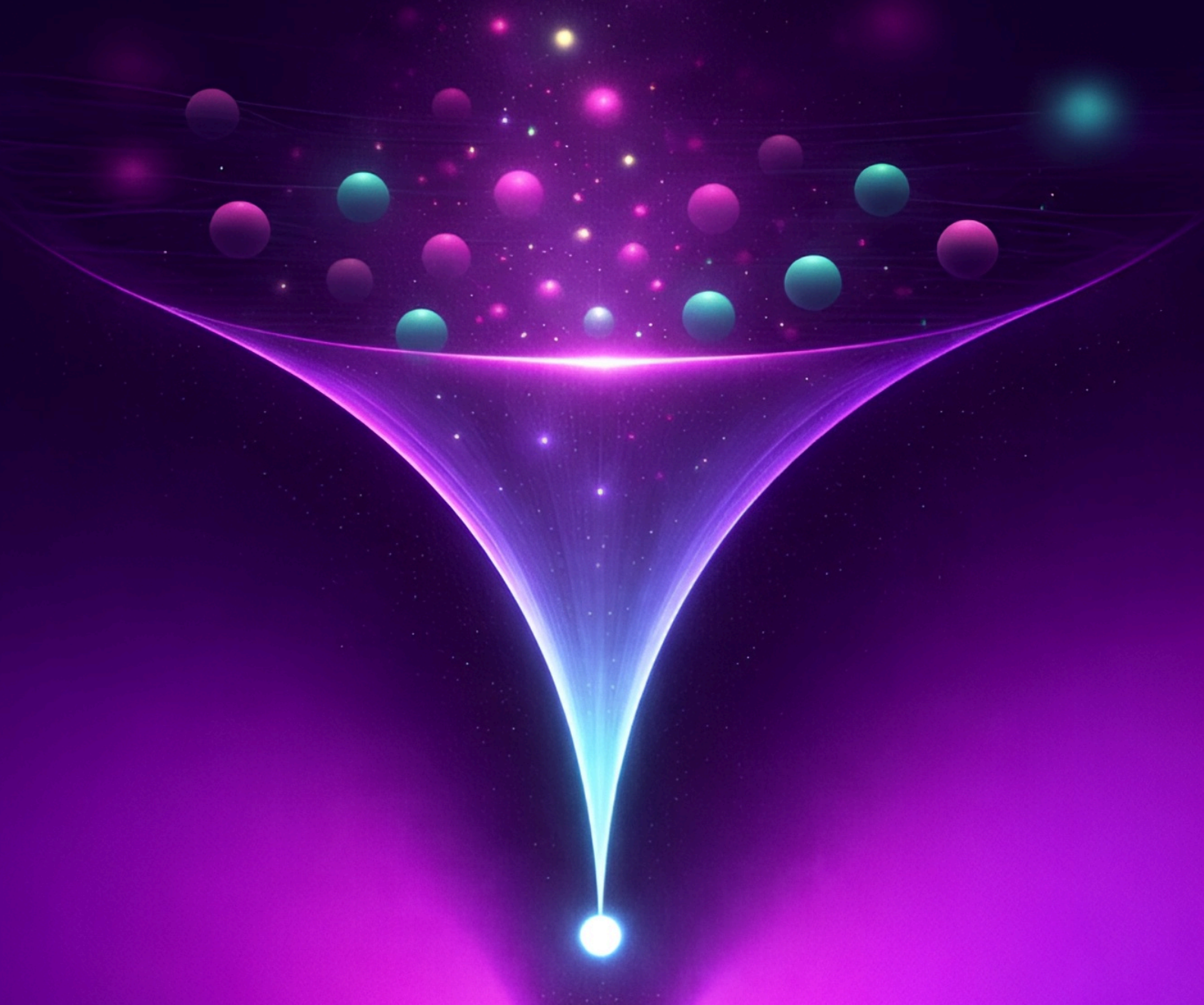


Table of Contents

The Execution Gap in Exposure Management

The security industry has largely succeeded in the first phase of exposure management: visibility. Through the widespread adoption of sophisticated scanning and asset discovery tools, enterprises now have an unprecedented view into their attack surface. However, this wealth of data has created a new operational crisis. The volume of identified exposures has reached a scale that traditional, manual remediation workflows were never designed to handle.

This report, based on a survey of hundreds of cybersecurity leaders across industries, examines the growing disconnect between the identification of risk and its resolution. The findings suggest that while organizations are increasingly confident in their ability to prioritize findings and report progress to the business, the actual mechanics of remediation remain the primary bottleneck. For many teams, exposure management has become as much an exercise in administrative coordination as it is in technical risk reduction.

This report explores the five critical dimensions of the current exposure management lifecycle:

1. **Baseline of High Volume:** Analyzing how a state of constant, high-volume findings has become the standard operational reality, leading to persistent remediation backlogs.
2. **Subjectivity of Prioritization:** Exploring why organizational confidence in risk focus remains high, even in the absence of standardized, industry-wide prioritization frameworks.
3. **The Coordination Tax:** Examining the hidden costs of execution, where security leaders spend a disproportionate amount of time on stakeholder alignment rather than risk analysis.
4. **Constraints of Automation and AI:** Investigating why high adoption rates for AI and automation have not yet translated into autonomous remediation, as human intervention remains a requirement for ownership and decision-making.
5. **The Outcome Mismatch:** Identifying the disparity between high reporting confidence and the lack of standardized processes required to verify consistent risk reduction.

Ultimately, the goal of this research is to highlight that exposure management is no longer a data problem, but an execution problem. By shifting the focus from identifying more, to fixing faster, organizations can move beyond the noise of high-volume environments and build a repeatable, scalable engine for risk reduction.

Key Findings

High-Volume Environments are the Operational Baseline

High-volume environments are now the baseline operational reality, with 54% of organizations managing a constant influx of findings that frequently outpace their capacity for resolution.

Prioritization Remains Subjective

While 95% of leaders report high confidence in their remediation focus, this sense of priority remains highly-individualized, as no single approach is used by a clear majority of the industry.

Coordination Stalls Execution

Remediation efficiency is constrained by administrative overhead. Half of all organizations now spend as much time, or more, on stakeholder coordination and manual alignment as they do on technical risk analysis.

AI Adoption Lacks Autonomous Trust

While 88% of organizations have integrated AI into their workflows, adoption has not yet led to delegated authority. Only 31% of leaders fully trust AI-driven recommendations without human oversight.

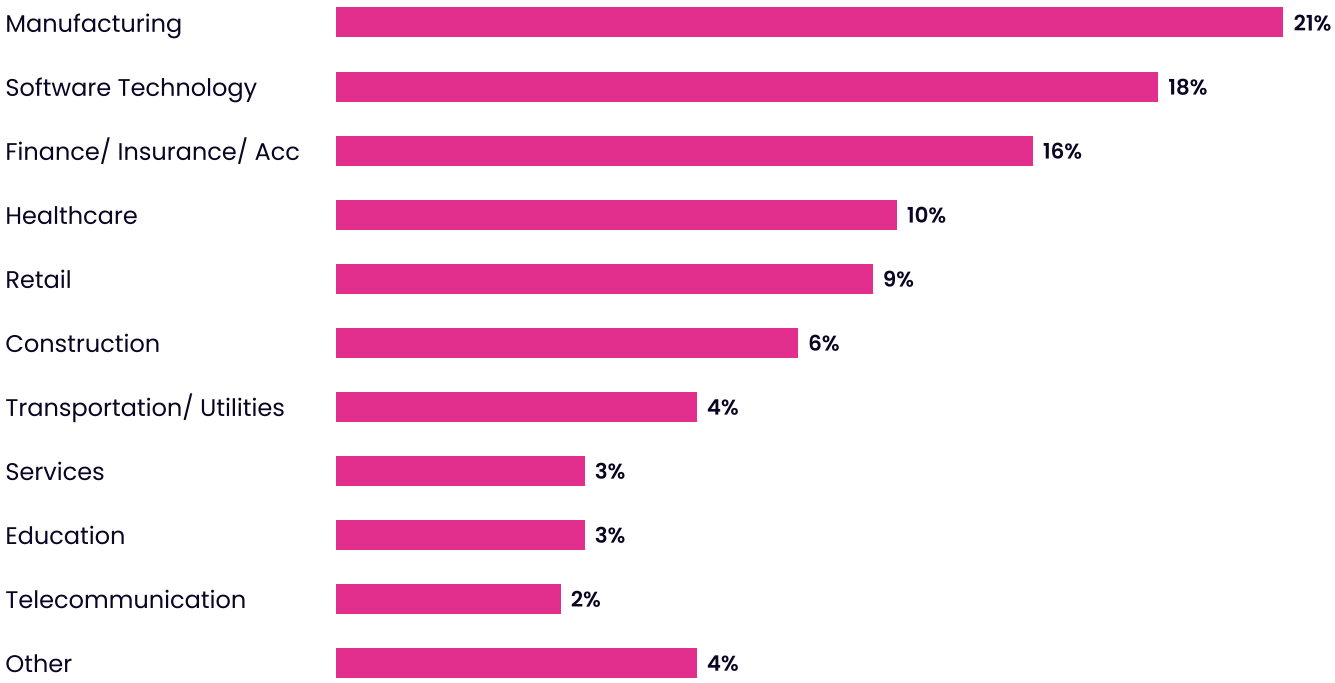
Confidence Exceeds Operational Maturity

A significant gap exists between outward confidence and internal maturity. Despite 94% of leaders feeling confident in their ability to report progress to the business, 43% acknowledge their internal processes remain inconsistent or ad-hoc.

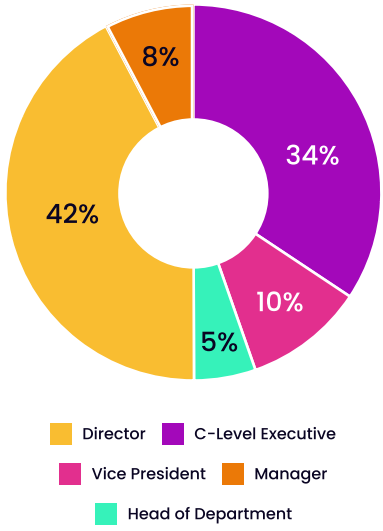
Methodology & About the Data

This report is based on a primary research study by Seemplicity. Seemplicity commissioned the research firm Sapio Research to capture responses from 300 cybersecurity and IT professionals based exclusively in the United States. The survey was conducted in January 2026. Percentages shown in charts and tables are rounded for presentation purposes. Consequently, aggregate totals may not equal 100%.

Industry

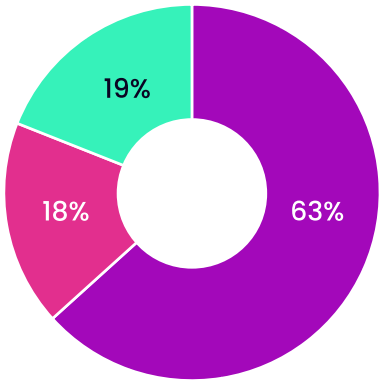


Job Role



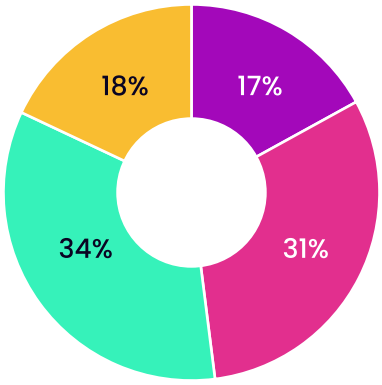
Organization Size

[No.of Employees]



Organization Size

[Annual Revenue]



A High Volume Environment is the Baseline

The primary challenge facing modern security operations is no longer a lack of visibility, but an overwhelming surplus of it. As organizations have expanded their security tool stacks across cloud, application and infrastructure environments, the number of security findings being generated has increased dramatically, creating a significant detection-execution gap. This "detection-execution gap" is further widened by attackers leveraging AI-driven techniques to automate reconnaissance and exploit vulnerabilities at machine speed. The data suggests that while security teams are more adept than ever at identifying potential risks, the sheer volume of these findings has outpaced the capacity to remediate them.

The Scale of the Exposure Challenge

The data reveals that a majority of enterprises are managing an extensive volume of security findings. Over half of all surveyed cybersecurity leaders (54%) describe their monthly volume of security findings as **high** or **very high** (Figure 1). Conversely, only 10% of respondents characterize their finding volume as **low** or **very low**, indicating that high-volume environments have become the baseline operational reality for the vast majority of security teams.

How would you describe the volume of security findings (i.e., identified vulnerabilities, misconfigurations, or other actionable security issues that require review or remediation) generated in your environment over a typical month? Select one

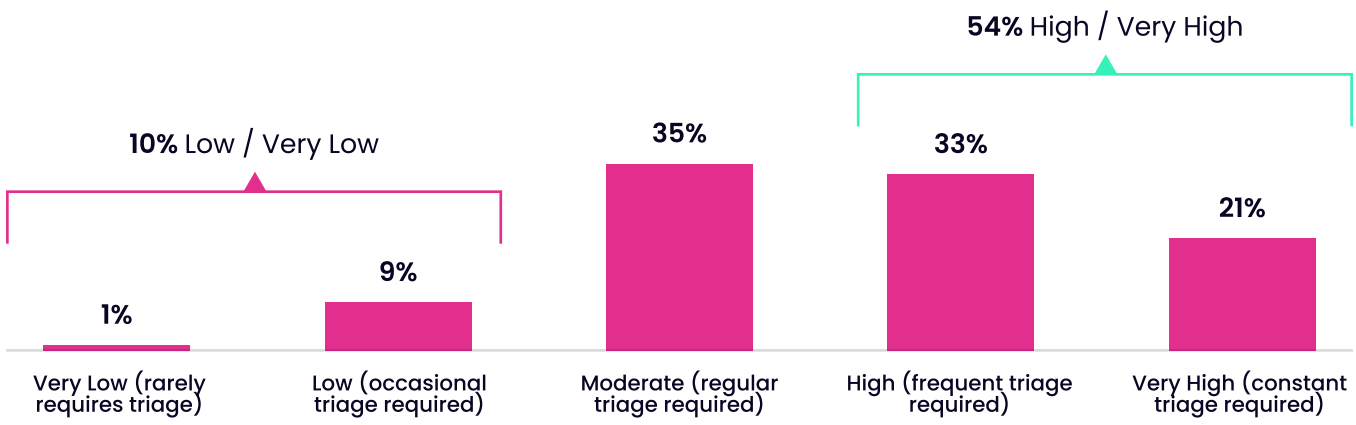


Figure 1: Monthly Security Finding Volumes Across Organizations

When a majority of security teams are operating in a state of constant high volume, it suggests that traditional methods of manual triage and spreadsheet-based tracking have become unsustainable. This data signals a systemic operational strain in which security teams are perpetually reactive, struggling to keep their heads above a continuous influx of vulnerabilities, misconfigurations and compliance gaps.

Persistence of the Remediation Backlog

The consequences of this volume are directly reflected in the scale of unresolved backlogs across the respondents.

How would you describe the current backlog of unresolved security findings in your organization? Select one

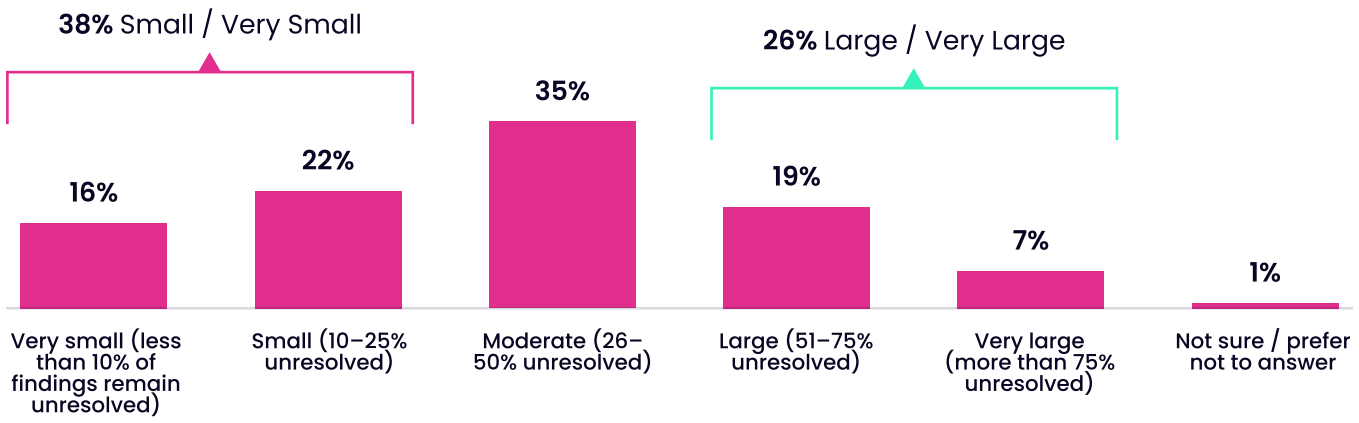


Figure 2: Current Backlog of Unresolved Security Findings

As illustrated in Figure 2, 61% of respondents report that more than a quarter (26%+) of their security findings remain unresolved in their backlog. Even more concerning is the density of this debt, with 26% reporting that more than half of all identified findings remain open. This level of exposure indicates that the rate of discovery is significantly outpacing the rate of resolution, further supporting the notion that organizations face a severe and systemic operational strain.

From Visibility to Velocity

These findings demonstrate that the industry has successfully optimized for visibility, but has failed to optimize for velocity. This imbalance creates a false sense of security. A high detection rate without a corresponding resolution rate simply provides a more detailed map of an organization's attack surface.

The detection-execution gap identified here serves as the foundational hurdle for exposure management. Addressing this operational reality requires a transition away from a detection-centric mindset toward a framework that emphasizes the systemic prioritization, routing and automation of the remediation lifecycle.

Subjectivity of Prioritization

Which statement best describes your organization's approach to prioritizing remediation work? Select one

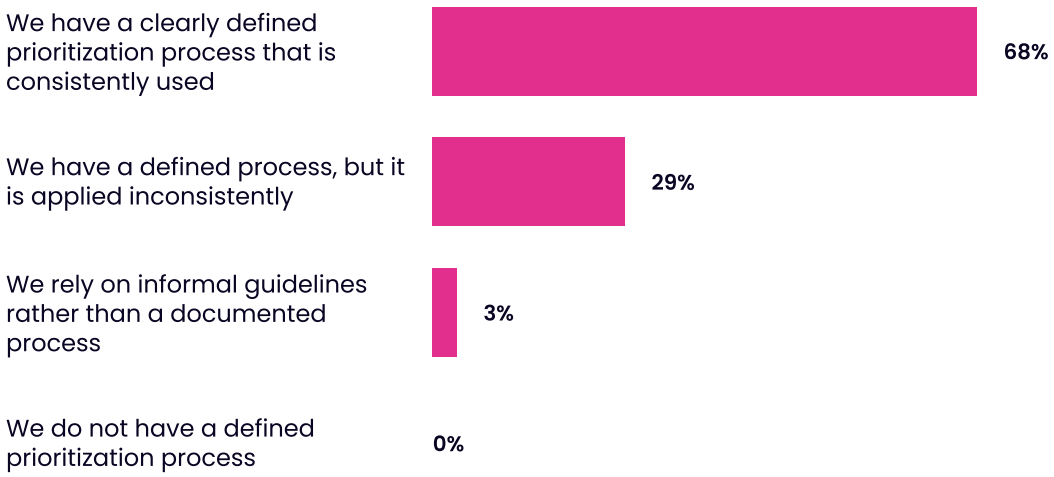


Figure 3: Organizational Approaches to Remediation Prioritization

On the surface, exposure prioritization appears to be a mature function. Figure 3 shows that a majority of respondents (68%) report having a clearly defined and consistently used prioritization process. This reported maturity is reflected in a high degree of confidence in remediation efficacy, with 95% of leaders saying they are **very** or **somewhat** confident that their remediation efforts focus on findings that materially reduce risk (Figure 4).

How confident are you that remediation efforts consistently focus on security findings that materially reduce risk? Select one

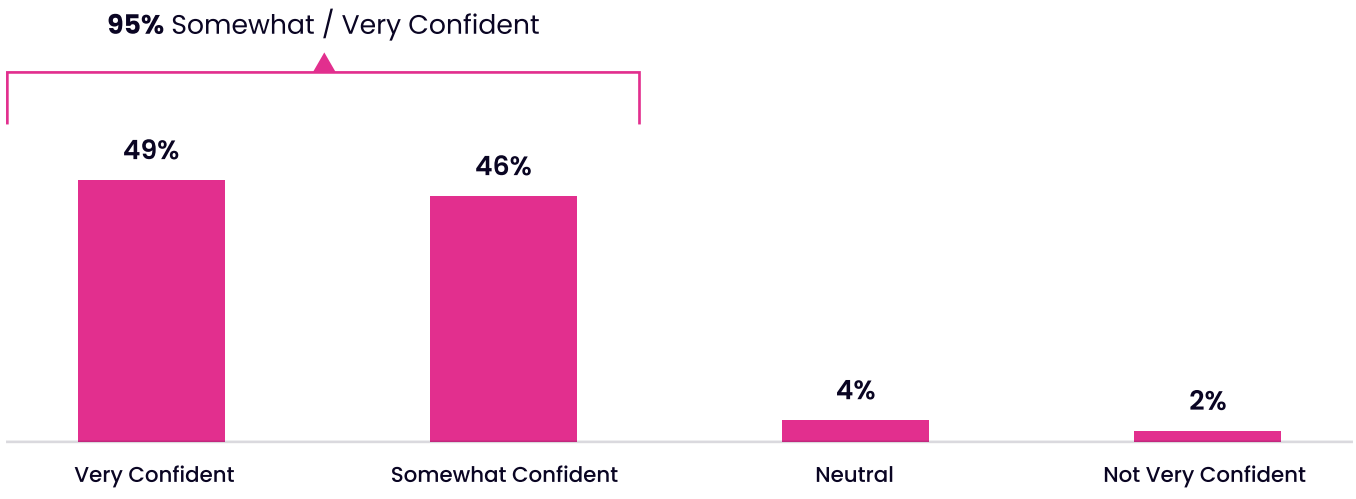


Figure 4: Leadership confidence in Risk-Based Remediation Focus

Interestingly, this high level of confidence remains prevalent even among organizations that lack a standardized approach. Of the 32% of respondents who acknowledge their prioritization process is either inconsistently applied or remains informal, 90% still report being confident that they are addressing material risks. This indicates that for the vast majority of security leaders, the sense of "focusing on what matters" is not strictly dependent on having a formalized or standardized process in place.

The Distribution of Prioritization Factors

When asked to identify their top three prioritization factors, the results show a distributed landscape of criteria. The most common inputs are **business criticality** (55%), s**everity scoring frameworks such as CVSS** (52%), and t**hreat intelligence** (50%) (Figure 5).

Out of the following, which factors are most commonly considered when deciding what to remediate first? Select up to three

Figure 5: Primary Factors Influencing Remediation Prioritization

It's telling that no single factor stands out as a clear majority. Even business criticality – widely considered a fundamental lens for risk – is not a top-three factor for nearly half of the respondents. This suggests that while organizations are looking at a range of technical and contextual signals, there is no industry-wide consensus on which specific factor(s) is most essential. Every organization is weighting these inputs differently to define their own version of priority.

Notably, operational factors are rarely prioritized at the same level as risk signals. Only 20% of respondents cite **engineering capacity** as a top-three factor. This indicates that for most organizations, the priority of a finding is determined primarily by the nature of the risk itself, rather than the practical resources available to address it.

The Performance Gap in Prioritization

Ultimately, a prioritization process is only as effective as the risk reduction it enables. Without a framework that consistently reconciles diverse risk signals with the practical reality of engineering capacity, organizations risk maintaining high levels of confidence while failing to achieve the scalable, repeatable outcomes required to keep pace with exposure volume.

The Coordination Tax of Remediation

The ultimate efficacy of an exposure management program is determined at the execution phase, in which remediation efforts actually translate into risk reduction. The research indicates that this critical phase is where operational efficiency often falters.

The Automation-Coordination Paradox

There is a notable disconnect between the reported automation of security workflows and the actual time spent on administrative tasks. A majority of leaders (66%) report that their routing processes – the mechanism for moving a finding from a scanner to a ticket – are **fully** or **mostly automated** (Figure 6).

How would you describe the level of automation used to route security findings to the appropriate remediation owner? Select one

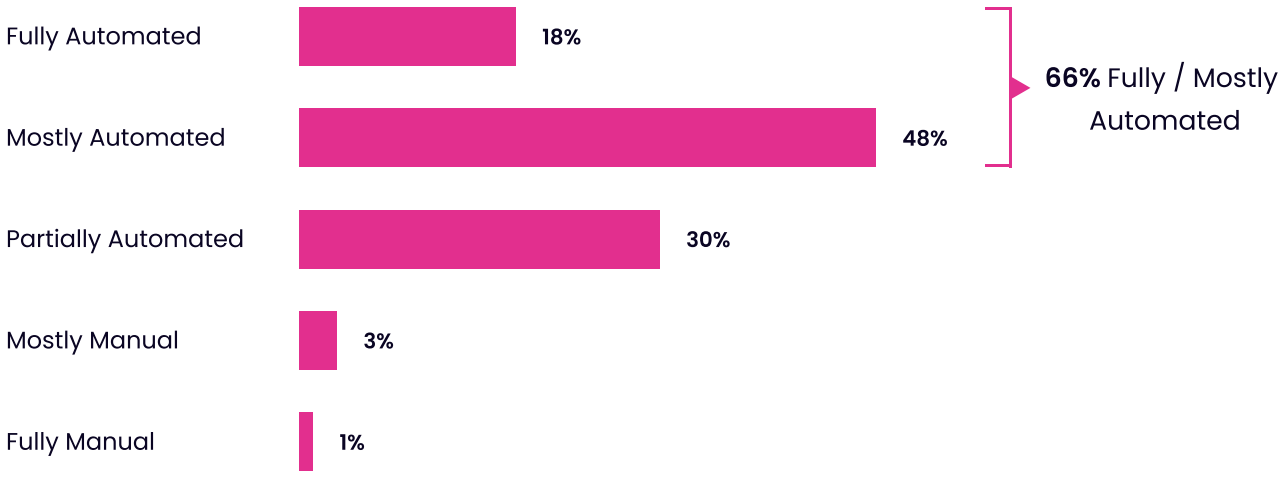


Figure 6: Automation Maturity in Remediation Routing

However, this automation has not yet translated into a significant reduction in human overhead. Only half (50%) of respondents are able to spend more time on risk analysis than on coordination (Figure 7). For the remaining 50%, the role of the security professional has shifted heavily toward administrative management: 34% state that time spent on coordination equals time spent on analysis, while 16% spend more time on coordination than on analyzing the risk itself.

Unsurprisingly, respondents who have fully-automated the routing of security findings to the appropriate owner report significantly more time spent on analysis: 78% of this group say they spend more time analyzing risk than coordinating remediation tasks.

In a typical week, how would you describe your team's time allocation between remediation coordination (e.g., identifying owners, assigning tickets, SLA compliance, etc.) and risk analysis? Select one

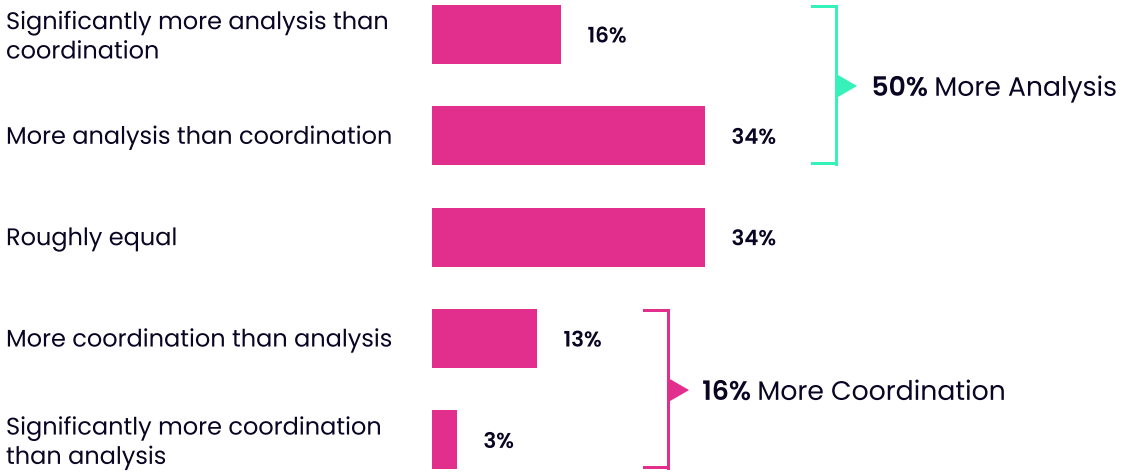


Figure 7: Time Allocated to Remediation Coordination vs. Risk Analysis

The Ownership Bottleneck

One such driver of the administrative drag appears to be the method by which remediation ownership is determined. While routing may be automated, the decision of who actually owns a fix remains largely manual and consensus-driven.

Figure 8 reveals that only 18% of organizations determine remediation ownership automatically via predefined rules. Instead, the most common practice is one of collaborative decision-making, utilized by 59% of respondents.

When a security issue is identified, how is remediation ownership typically determined? Select one

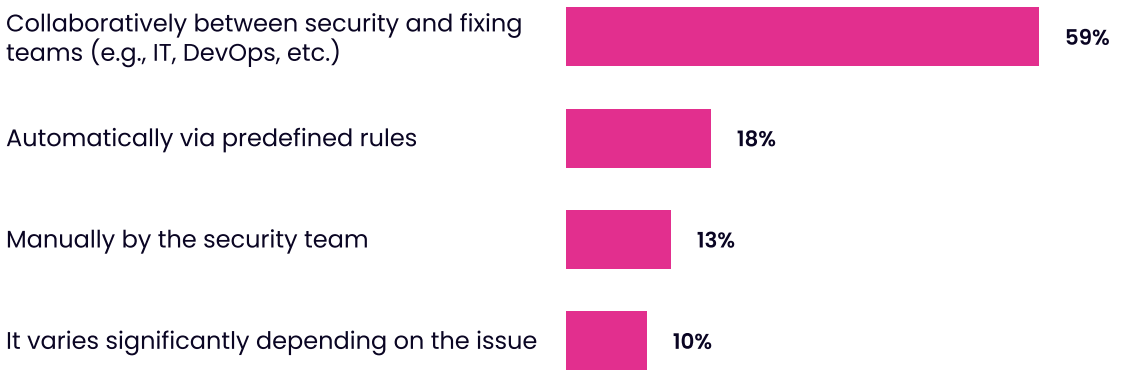


Figure 8: Methods for Determining Remediation Ownership

While collaboration is a necessary component of organizational alignment, its prevalence as the primary mechanism for determining ownership suggests a lack of automated, scalable mapping between security findings and the teams responsible for fixing them. In high-volume environments, relying on cross-functional negotiation to identify every remediation owner creates a coordination tax that directly competes with the time available for actual risk reduction.

The Hidden Cost of Collaboration

The data suggests that exposure management programs are currently hitting an execution ceiling. Organizations have successfully digitized the delivery of tickets, but they have not yet codified the rules of ownership.

The high percentage of teams spending equal or greater time on coordination than on analysis reveals a critical inefficiency. When collaboration is the default mechanism for determining responsibility, the administrative overhead scales linearly with the volume of findings. For an exposure management program to be truly effective, the focus must shift from simply routing data to establishing a clear, rule-based ownership model that removes the need for constant human intervention. Without this shift, remediation will continue to be restrained by the manual effort required to align disparate stakeholders.

AI as an Assistant, Not an Operator

Automation and AI have become central to organizational efforts to alleviate the manual overhead associated with exposure management. However, the data indicates that while baseline workflow automation is now deeply embedded, there is a distinct boundary between automated tasks and autonomous authority. This suggests that cybersecurity leaders maintain a cautious approach toward giving AI systems full responsibility.

The Scope of Process Automation

Automation is currently most prevalent in the data-heavy, administrative stages of the lifecycle. The most commonly automated activities include **tracking remediation progress** (66%), **aggregating findings from disparate tools** (61%), and **prioritizing findings** (60%) (Figure 9). However, the process in-between data management and operational execution remains a manual hurdle. Consistent with the ownership challenges noted in the previous section, only 44% of organizations have automated the process of **identifying ownership**.

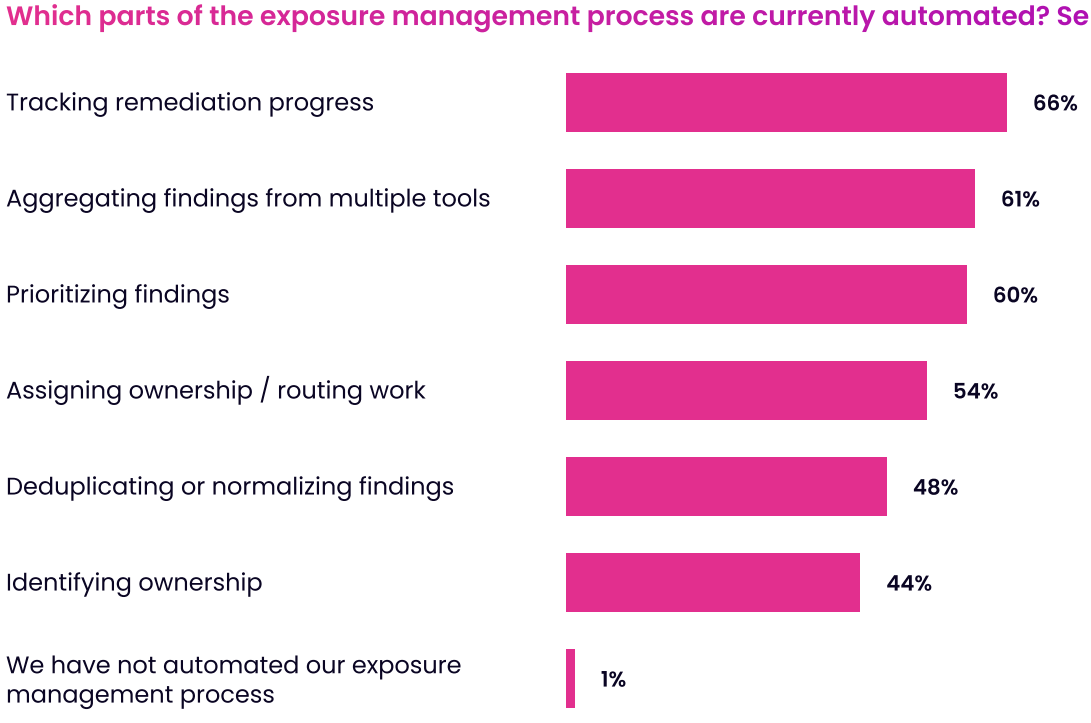


Figure 9: Levels of Automation Across the Exposure Management Lifecycle

AI Adoption and Enterprise Scale

The integration of AI within exposure management is widespread, as shown in Figure 10, with 88% of respondents reporting its use in some capacity. This adoption is split between organizations that **actively use AI to influence remediation decisions** (47%) and those **using it in more limited or experimental ways** (41%).

How, if at all, is AI currently used within your exposure management processes? Select one

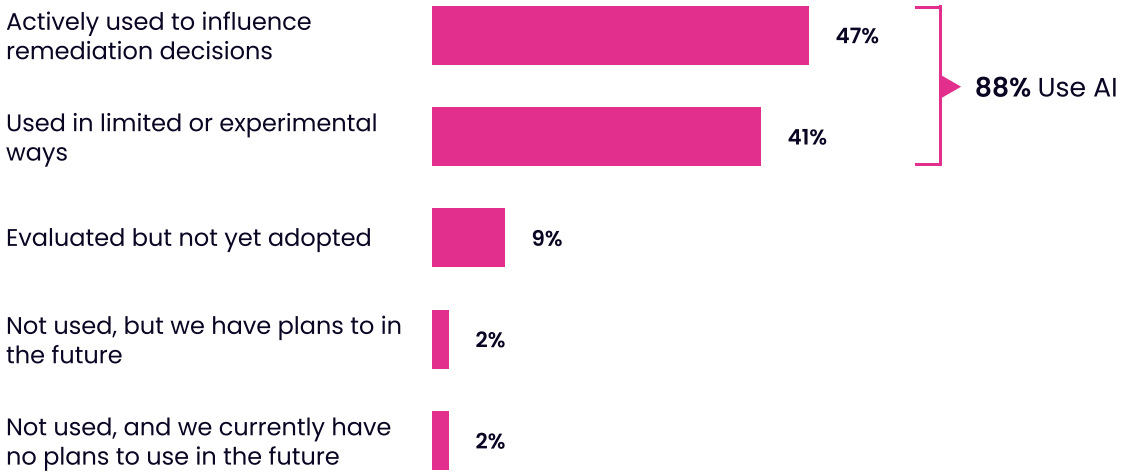


Figure 10: AI Implementation in Exposure Management Workflows

Notably, there is a correlation between enterprise size and AI usage, with adoption being highest in smaller enterprises (91%) compared to mid-sized (87%) and large enterprises (79%). This suggests that smaller organizations may be utilizing AI as an operational accelerator to compensate for smaller team sizes and fewer resources.

The Boundary of Trust and Autonomy

While a majority of organizations have integrated AI into their exposure management workflows, there is still industry-wide hesitation when it comes to full autonomy. When surveyed on their level of trust towards AI-driven recommendations (regardless of current AI usage), 80% of all respondents expressed confidence in AI's ability to influence prioritization decisions. However, only 31% reported full trust in these outputs (Figure 11).

This attitude persists even among the cohort of active AI users. Despite the confidence in AI rising slightly to 83%, the ceiling for **full** trust remains low at 34%. These figures indicate that while AI is increasingly viewed as a valuable support channel, a majority of leaders still require human oversight when it comes to prioritization decisions.

Whether you use AI or not, to what extent do you trust AI-driven recommendations to influence exposure prioritization decisions today? Select one

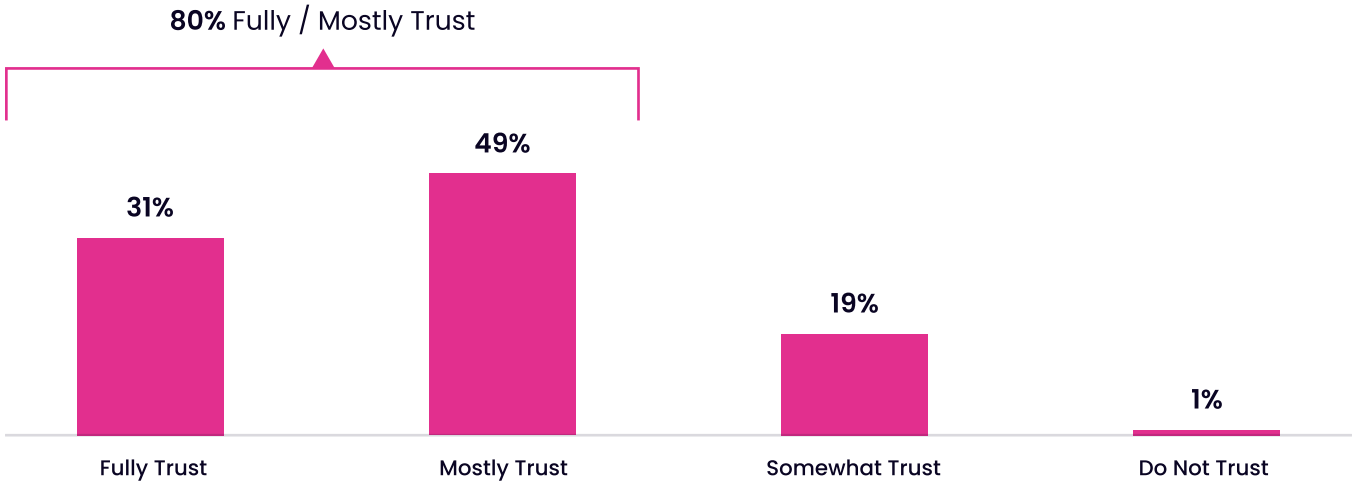


Figure 11: Levels of Trust in AI-Driven Exposure Prioritization

Acceleration Without Autonomy

The findings suggest that automation and AI are now well established within exposure management programs, but their role remains primarily supportive rather than autonomous. Organizations appear to be further along in automating data processing and workflow administration than in automating the more operationally complex parts of the remediation lifecycle.

A similar pattern emerges when it comes to AI. Adoption is widespread, yet trust in AI remains more measured when it comes to full decision-making authority. While most leaders are comfortable allowing AI-driven recommendations to inform prioritization, far fewer fully trust those outputs, indicating that human oversight remains standard practice.

Taken together, these findings suggest that automation and AI are currently functioning more as accelerators than autonomous operators. Organizations are investing in technologies that help them process information faster and support decisions at scale, but human control still governs key judgments and execution-related decisions.

Metrics of Exposure Management

A core component of an effective exposure management strategy is measuring progress and communicating that progress to the broader organization. The data shows that most organizations are actively tracking performance metrics and report high confidence in their ability to explain exposure management progress to non-security stakeholders. At the same time, the results reveal varying levels of operational consistency, suggesting that measurement, reporting, and process maturity do not always develop at the same pace.

The Dominance of Throughput Metrics

Measurement of exposure management performance in the current landscape is primarily focused on operational throughput. The most commonly tracked metrics are **time to remediation** (67%), **number of findings identified** (66%), and **number of findings remediated** (66%) (Figure 12). These indicators provide visibility into the speed and volume of the remediation pipeline, but they essentially just measure labor and movement rather than actual risk reduction.

Which metrics are regularly used to measure exposure management performance? Select all that apply

Figure 12: Most Common KPIs Used to Measure Exposure Management Performance

While 62% of organizations do track changes in exposure and risk over time, it remains the fourth most common metric, trailing the throughput-based indicators. This distribution suggests that for most organizations, performance is still defined by the efficiency of the process rather than the ultimate impact on the organization's security posture.

The Communication-Standardization Gap

There is a notable disconnect between how security leaders perceive their reporting capabilities and the actual maturity of their underlying processes. An overwhelming 94% of respondents report being confident in their ability to explain exposure management progress in business-relevant terms (Figure 13). This suggests that leaders believe they have successfully bridged the communication gap between technical security findings and executive-level stakeholders.

How confident are you in your ability to explain exposure management progress in business-relevant terms (e.g., risk reduction, business impact) to non-security stakeholders? Select one

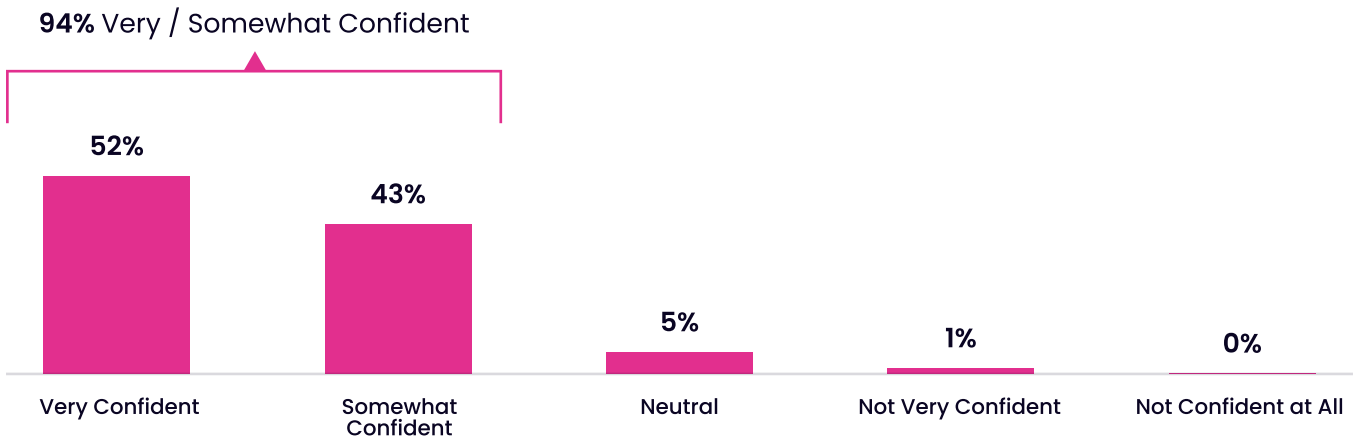


Figure 13. Confidence in Communicating Exposure Progress to Business Stakeholders

However, despite the high levels of confidence, the data reveals varying levels of process maturity. Only 57% of cybersecurity leaders state that their exposure management processes are well-defined and consistently followed across the organization (Figure 14). Conversely, 42% of respondents acknowledge that their processes remain inconsistent, ad hoc or reactive. This indicates that while leaders have mastered the translation of security activity into business language, the lack of standardized processes in many organizations challenges the underlying reliability of the data being reported to stakeholders.

Which statement best describes your organization's overall approach to exposure management today? Select one

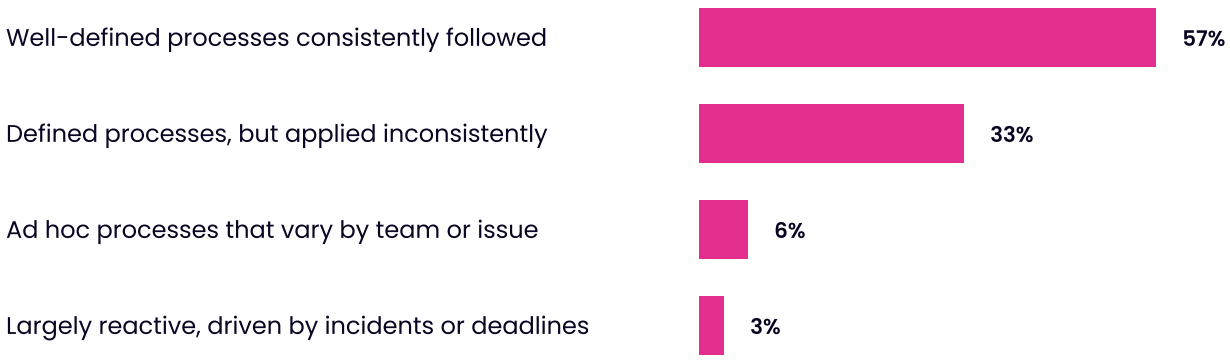


Figure 14: Organizational Maturity Models for Exposure Management

Activity vs. Outcome

The findings indicate that exposure management performance is currently being measured as a volume-based operational task rather than a risk-based strategic function. The reliance on throughput metrics reveals that organizations are optimizing for the speed of resolution and volume of activity. While this is a necessary response when there is a high volume of findings – which is the case for most organizations – it does not guarantee that remediation efforts are aligned with the highest-risk exposures.

The gap between high reporting confidence and the lack of process standardization suggests that the industry is in a transitional phase. For exposure management to move from an activity-driven model to an outcome-driven one, organizations must bridge the distance between their reporting and their operations. The goal is to ensure that the progress being communicated to the business is the result of a consistent, repeatable system that links day-to-day throughput directly to measurable risk reduction. Without this alignment, organizations risk optimizing for the speed of their workflows rather than the verifiable resilience of the enterprise.

From Visibility to Action

The findings in this research suggest that cybersecurity has largely solved the challenge of visibility, but the industry is still working to operationalize action. Security teams now have unprecedented insight into their environments, yet the volume of exposures being identified continues to outpace the systems designed to resolve them. Across the data, organizations demonstrate growing maturity in detecting, prioritizing, and reporting on risk. However, the operational mechanics of remediation – particularly ownership, coordination, and execution – remain the primary constraint preventing organizations from closing exposures at scale.

As exposure management continues to evolve, organizations will need to strengthen the operational side of the lifecycle. Key areas of focus include:

- **Establish Clear Ownership Models:** Define rule-based ownership for remediation so responsibility can be assigned automatically based on asset metadata and business logic, rather than through manual coordination.
- **Integrate Security and Engineering Workflows:** Embed remediation into existing development and infrastructure processes to reduce friction between identification and execution. Security should live where the work happens, not in a separate silo.
- **Extend Automation into Execution:** Move beyond automating data aggregation and ticket routing toward automation that supports ownership assignment and remediation coordination.
- **Measure Risk Reduction, Not Just Throughput:** Complement operational metrics like remediation speed and ticket volume with indicators that reflect actual business impact. Examples include reduction in true "Critical" exposures on high-value assets, decrease in average exposure window for exploitable flaws, and SLA attainment by business unit.

Ultimately, the next stage of exposure management maturity will depend on an organization's ability to translate security insight into consistent operational outcomes. In an environment where high volumes of findings are now the norm, the organizations that succeed will be those that can reliably convert visibility into action.

seemplicity

Learn more about Seemplicity's Exposure Action Platform at seemplicity.io