Exposure Debt:

The Next Challenge in Cybersecurity



Security Research Report 2026

> 10th Edition | hackerone

Table of Contents

Section 1. 4
The Discovery Acceleration

Section 2. 6
Severity Is Rising as Researchers Lean into More Complex Vulnerabilities

Section 3. 8
The Exposure Debt Challenge

Section 4. 11
AI Is the New Frontier for Attackers and Researchers

Section 5. 13
Who's Responsible When AI Gets It Wrong?

Section 6. 15
The Human Layer

Section 7. 17
The Bounty Economy Is Splitting by Industry

Section 8. 20
Reducing Exposure Debt: Five Actions

Closing Remarks 22

Data Sources and Methodology 23

Letter from the CEO:



Fixing Got Twice as Fast. It Still Lost Ground.

For ten years, this report has tracked how security changes through the eyes of the people testing it. Through cloud, software supply chains, and now AI, one thing has remained constant: as technology evolves, security researchers evolve with it.

This year's data shows how far vulnerability discovery has come. Researchers are using AI to work faster and go deeper, moving into business logic, chained exploits, and the safety and security of AI systems. This is complex work where context and human judgment are decisive.

Validated findings reached an all-time high this year, and the volume they had to be found in grew faster still. Validation has not kept pace. Organizations have sped up resolution nearly twice as fast over the same period, and nearly 70% of the security leaders we surveyed still tell us findings enter their systems faster than their teams can close them. Fixing got faster. It still lost ground. The constraint is no longer discovery; it is everything between a report arriving and a risk being gone.

To close this gap, security teams need to know which exposures are genuinely exploitable, which pose the greatest risk, and where to focus limited resources. That is what a researcher does when they prove impact. They answer the questions that matter: Is this exploitable? How serious is it? What does it affect?

And the community is investing to stay ahead of the technology. This year, 85% of researchers told us they are actively upskilling in AI safety and security, and nearly three-quarters say AI has improved the quality and outcomes of their findings.

The value of that work is evident in rewards payouts. Researchers earned $47 million in the first half of 2026, up 26% over the same period last year. The number of researchers getting paid rose 36% over the same period, outpacing the pool. Widening that base is deliberate.

AI will continue to accelerate vulnerability discovery. The opportunity now is to match that speed in validation, prioritization, and remediation.

For security leaders, that means measuring success differently. Finding more potential exposures is not enough if the most consequential ones remain unresolved. Security programs must excel at identifying what is truly exploitable, fixing what matters most, and verifying that the exposure is gone, all continuously.

Finding more is progress. Continuously reducing cyber risk is the outcome that matters.



Kara Sprague
Chief Executive Officer, HackerOne

About the report

The 10th edition of the HackerOne Security Research Report brings together platform data, surveys of security leaders and researchers, and insights from practitioners. It examines how vulnerability discovery is changing, where resolution is falling behind, and how organizations can reduce Exposure Debt.

Platform findings cover July 2025 through June 2026, with comparisons across earlier years. Survey findings reflect respondents' experiences within their own organizations and research workflows.

Key Statistics

Up 11%
↑ 33% since 2021
Valid Reports at All-Time High

31%
of valid reports
Critical and High-Severity Findings at 5-Year High

131%
growth in 2 years
Open Valid Report Backlog

61%
↓ since June 2024
Average Resolution Time for Critical Findings

85%
↑ from 58%
Researchers Upskilling in AI in a Single Year

Nearly 5x
in 2 Years
Researchers selecting AI/LLM applications as a focus area increased from 9% to 42.5%

Up 91%
↑ 740% in 2 Years
AI-Related Bounty Payouts

$89M
↑ 18% YoY
Collective Bounty Payouts



Ten Years of Security Research

Over the past decade, the security landscape has transformed, and the scope of this research has grown with it. What has always been a record of hacker-powered security now also captures a broader picture, including the growing role of AI in what gets attacked, how vulnerabilities are discovered, and how organizations respond. The HackerOne Security Research Report reflects that broader lens, with the researcher community remaining at the heart of the research and our approach to security.



The report has documented the growth of vulnerability discovery for the last ten years. This year, it examines **Exposure Debt:** the growing gap between what organizations find and what they can fix.

Section 1.
The Discovery Acceleration

Valid Vulnerability Reports Rise

Valid vulnerability reports reached 92,194 by June 2026. That was an 11% increase year over year and a 33% increase since June 2021. May and June recorded the highest monthly volumes in a two-year monthly window. For security teams, that means more confirmed vulnerabilities to address, along with duplicates and other submissions that still require triage.

The most telling change is where researchers are looking.

Researchers Bring AI to Work

In our 9th Edition report, we profiled Bionic Hackers, researchers bringing AI into their work to accelerate common workflows, but also to dig deeper in their testing.

And this year, we see that **85% of researchers report upskilling in AI or machine-learning security**. Those focused on AI or LLM applications are now 42.5%, compared with 19% last year.

Researchers are also seeing results from using AI. Nearly three-quarters (74%) say it has moderately or significantly increased the quality and outcomes of valid findings they submit. Responses averaged 5.9 on a 0-10 scale measuring how extensively researchers used AI across the vulnerability research process.

Source code vulnerability reports climbed 239% YoY, now 5.1% of all valid reports.

Bigger Organization, Bigger Target

Enterprise programs carry nearly six times the valid report load of their smallest peers, compounding their Exposure Debt faster.

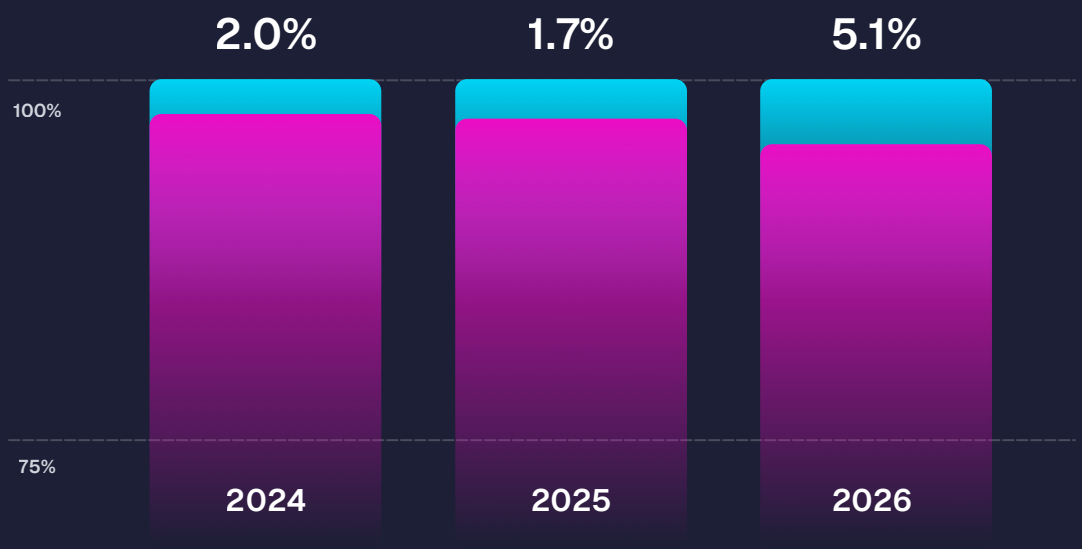
Programs at organizations with more than $10 billion in revenue averaged 84.2 valid reports in 2026, compared with 14.5 at organizations with $1 million to $5 million in revenue.

Security leaders are seeing changes in AI-assisted submissions as well:

53% report higher volume, and 60% report better quality.

More findings reveal more of an organization's exposure, but they also create an increased workload. Teams have to validate each submission, assign ownership to confirmed vulnerabilities, and implement mitigations or fixes.

Source Code Reports as a Share of Total Valid Reports





"Source code review historically took a lot of time, and in the world of bug bounty a hacker's success largely depends on finding a good ROI on our time. Putting time into reviewing source code manually was a risk because it meant investing considerable time with no guarantee of a bounty. Being able to guide AI to do this for us removes the risk while retaining all of the upside in the bounty amount."

— Douglas Day (archangel)

Section 2.
Severity Is Rising as Researchers Lean into More Complex Vulnerabilities

Security teams are handling more serious findings, both in number and as a percentage of valid reports. Critical and high-severity findings rose by 62% since 2021. After dipping to 27% in 2024, critical and high-severity findings reached

31% of valid reports, the highest percentage in five years.

AI Pushed Researchers Into Harder Territory

68% of surveyed researchers say AI has shifted their focus toward higher-complexity, higher-bounty bugs.

Business logic flaws are among the fastest-growing vulnerability classes in the research of 72% of respondents, while 56% point to chained authentication and IDOR vulnerabilities.

That growing focus puts researchers in territory where AI still struggles. Of those surveyed, 62.1% identified business logic flaws as one of the vulnerability classes AI tools are weakest at finding.

The Vulnerability Mix Continues to Change

Since 2021, improper access control reports have increased 104%, IDOR reports by 147%, and business logic errors increased 8%. Since appearing in 2022, misconfiguration reports have increased by 184%. Meanwhile, cross-site scripting (XSS) reports, which peaked in 2024, continue to decline, decreasing 14% this year.

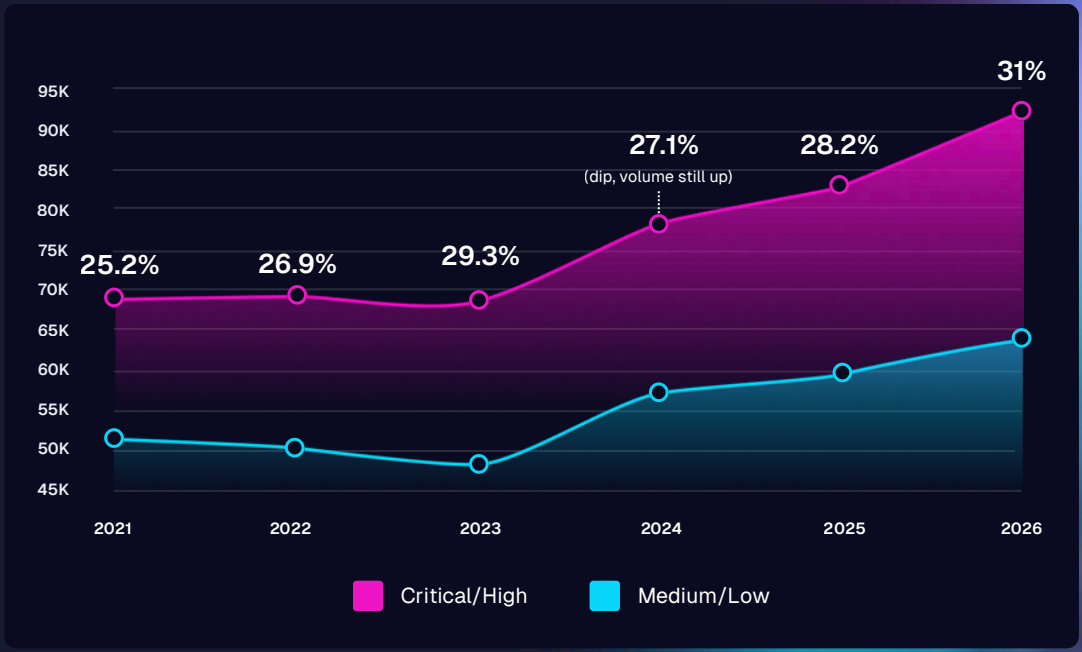
As automation handles more surface-level discovery, researchers are moving upstream into access control, IDOR, and business logic. These vulnerabilities depend more heavily on business context and coordination across systems, making them both more difficult to find and more difficult to resolve.

The findings accumulating in organizations' backlogs are increasingly complex, high-severity vulnerabilities that require teams to define intended behavior, establish ownership, coordinate fixes, and verify that unauthorized actions are prevented across connected systems.

The complexity of these findings also affects how teams prioritize them. Within a continuous threat exposure management (CTEM) program, prioritization needs to account for the business context: what the vulnerability puts at risk, which team owns the affected system, and what engineering needs to act.

Critical and high severity reports are now 31% of valid reports

Share of valid reports by severity, 2021 to 2026. Up from 25.2% in 2021.



Weakness Group Change from 2021 – 2026	
XSS	-14%
Improper Access Control	104%
IDOR	+147%
Misconfiguration	+184%
Business Logic Errors	+8%

Shares sum to 100%. Medium/Low includes unscored reports.



"To go where no one considered going before. Looking for issues that require extreme setup, are hard to reason about in context, or are at an impossible scale. Areas where researchers previously didn't see a return on investment – now there are no blockers to dig there."

— Johan Carlsson (joaxcar)

Section 3.
The Exposure Debt Challenge

Organizations are closing resolved tickets faster across every severity level, yet that velocity is being overwhelmed by incoming volume.

By June 2026, **92% of open valid reports were older than 90 days.**

The open **critical backlog grew 123%, high severity grew 152%, medium grew 149%, and low grew 119%** over the same time period.



Backlog counts show the amount of unresolved work, but they don't assign a financial value to the risk.

Security Leaders Confirm That Findings Are Outpacing Fixes

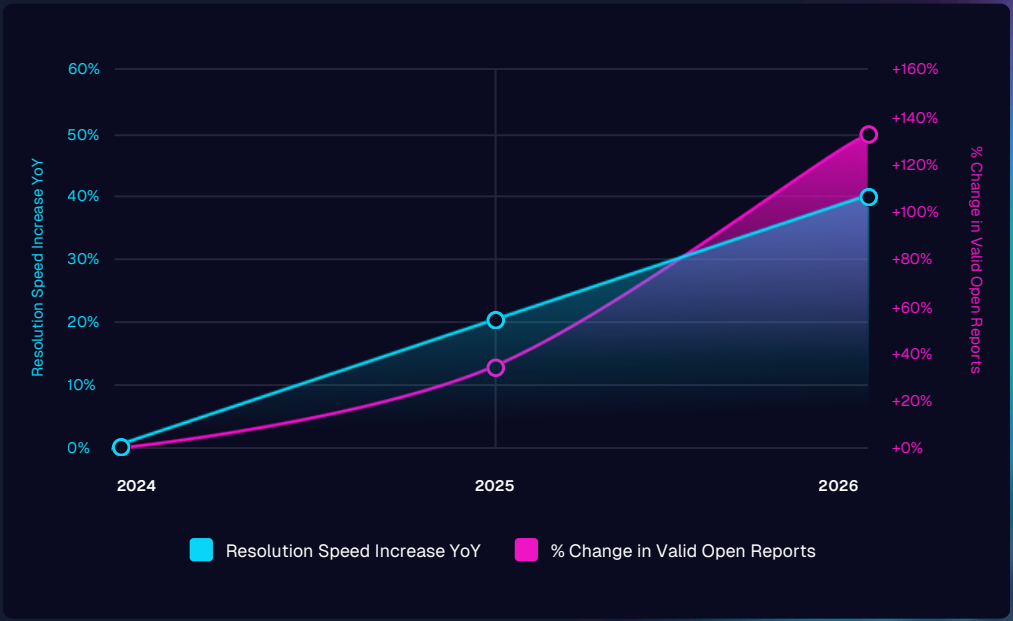
Nearly **70% of security leaders** say validated findings are entering their backlog faster than their teams can remediate them.

Asked how their backlog had changed over the past 12 months, **60% reported an increase of 20% up to 100%.**

Leaders also estimate that, on average, 21% of their unresolved backlog is more than six months old. These findings have already been validated as exploitable vulnerabilities posing real risk to the organization, so the longer they remain unresolved, the longer organizations carry the associated exposure.

Exposure Debt Growth is Outpacing Resolution Gains

2024 – 2026 Year-over-year performance



+54%

faster resolution
2026 vs 2024

+131%

more open reports
2024 → 2026

Competing priorities contribute to the delay: **58% say high- or critical-severity fixes are delayed by product delivery,** customer commitments, or other business priorities.

Even when a vulnerability is found and validated, the work isn't done. The final stage of a CTEM framework is Mobilization, where validated findings are translated into fixes. In practice, this is where Exposure Debt accumulates fastest. Even when findings reach the right team, they stall if the validation context doesn't come with them. Engineers need enough detail to make a safe fix and test it.

Exposure Debt continues to accumulate when validated findings remain open, whether they have been deprioritized or have reached engineering without being resolved.

Faster Closure Has Not Cleared the Backlog

Reports that reached resolution moved through the process faster: average resolution time fell from 135 days to 62 days across all severity levels over two years. But the number of valid reports still awaiting resolution grew 131% during the same period.

Resolution time measures completed work. It does not show how long unresolved findings have been waiting. To understand Exposure Debt, leaders also need to track the age and severity of open findings and identify where remediation has stalled.

The security leader survey measures two stages of the process separately. Respondents report an average of 30 hours to validate a critical finding and 16 days to remediate one.

Investment Isn't Going into Remediation

When security leaders ranked their investment priorities, proactive discovery, detection and response, and threat intelligence tied for first. Remediation was the first choice for only a tenth of security leaders.

Nearly seven in ten leaders say validated vulnerabilities are entering their backlog faster than their teams can fix them.

That difference is hard to ignore when nearly seven in ten leaders say validated vulnerabilities are entering their backlog faster than their teams can fix them. "The Verizon Data Breach Investigations Report 2026 found that software vulnerabilities had surpassed stolen credentials as the leading way attackers gained access, accounting for 31% of breaches.[1]" Verizon also reports that AI is shrinking the time required to exploit vulnerabilities from months to hours. The longer known flaws remain open, the more opportunity attackers have to use them.

Nearly all surveyed leaders say vulnerability metrics already reach leadership. Those reports can do more than show that a backlog exists. They can identify which high- and critical-severity findings have been open longest, who is responsible for remediation, and whether product commitments or limited engineering time are adding to the backlog. Some backlog growth is expected when expanded testing uncovers previously hidden exposure. The primary concern is what happens after a serious finding is validated and remains unresolved.



"AI is creating and finding these issues, and the speed gap is bigger than ever. What surprises me is that it's only gotten worse, even in the age of AI. It's getting applied to finding vulnerabilities fast. What we really need is to close the gap on validating, prioritizing, and remediating them faster."

— **Alex Rice,** HackerOne Co-founder, CTO, and CISO

Section 4.
AI Is the New Frontier for Attackers and Researchers

AI is being deployed faster than it is being secured. In a separate HackerOne study, we found that 94% of enterprise security leaders expanded their AI/ML footprint this year. That is showing up in vulnerability data now: valid vulnerability reports involving AI systems or AI-enabled functionality increased 53% year-over-year and surged 222% over two years.

At the same time, programs with AI assets in scope more than doubled since 2024.

Security teams also have a broader attack surface to test. Models, LLM applications, agents, and tool-connected workflows create new permissions, data flows, and dependencies that security programs need to cover.

Where AI Vulnerabilities Are Concentrating

Some of the fastest growth came from categories that had relatively few reports a year ago. System Prompt Leakage increased 557%, Misinformation increased 455%, and Improper Output Handling increased 264%. Prompt injection and sensitive-information disclosure still produced more reports overall.

The OWASP Top 10 for LLM Applications 2026 provides a current framework for understanding these risks. For security teams, the testing questions are practical: What information can the system reveal? What can it be made to produce? What happens when a connected tool acts on that output?

As models connect to more tools and business workflows, testing needs to cover the systems and data they can reach.

AI security vs. AI safety

AI security focuses on protecting AI systems, models, data, and connected infrastructure from attack or compromise. That includes risks such as prompt injection, sensitive information disclosure, data poisoning, model theft, excessive agency, and abuse of agentic tools.

AI safety focuses on unintended or harmful model behavior, including unsafe or unreliable outputs that can occur even without an attacker. The two areas can overlap, particularly around output integrity and agentic systems, but the distinction matters. AI security looks at how systems can be attacked or exploited. AI safety looks at how those systems can cause harm or behave outside their intended boundaries.

Where the Research Community Is Focusing Now

Researchers, including Commercial Community Members conducting security research through companies or other legal entities, are also adapting how they work as AI capabilities expand.

MCP Security Tops AI Skill Development, with 51% of Researchers Prioritizing It

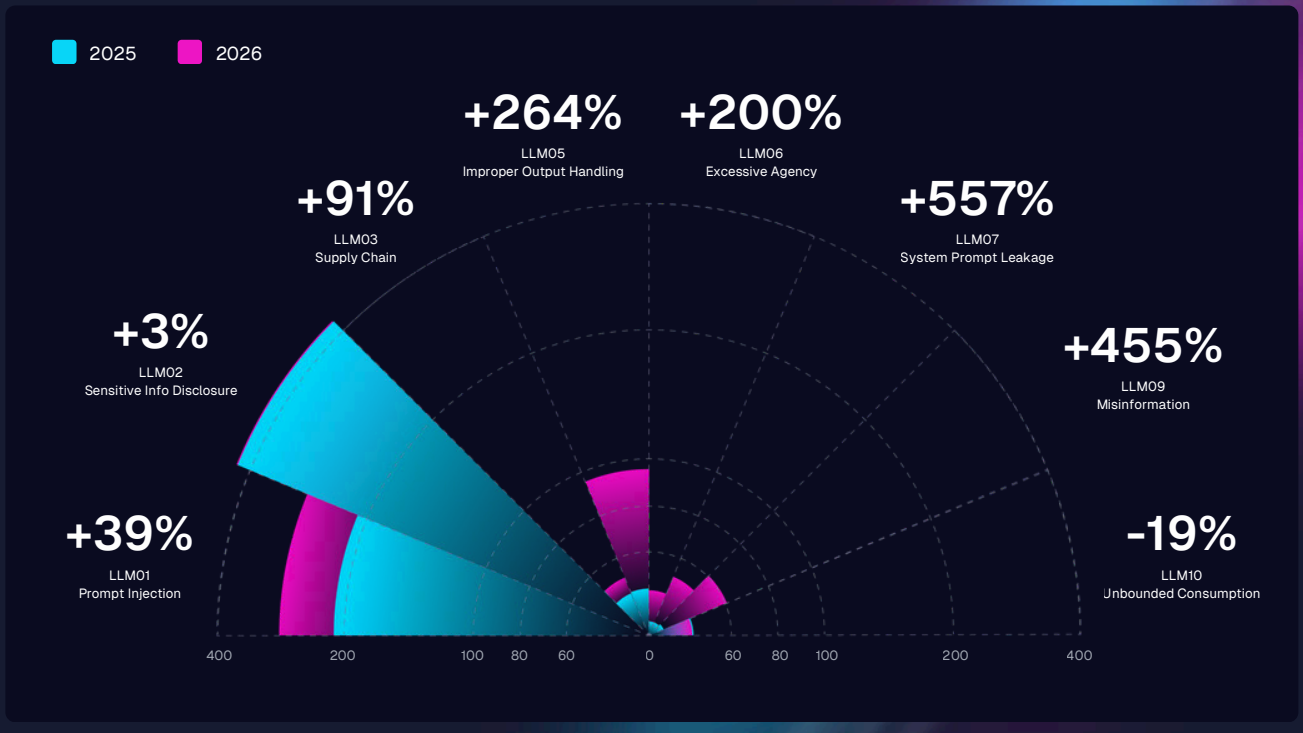
As AI systems connect to tools and workflows, researchers are building the skills to test those connections. Among the 343 respondents to the AI/ML skill-development question, 51% selected Model Context Protocol (MCP) security. Prompt injection, offensive AI tooling, and agentic security also ranked prominently.

68% of respondents have built or experimented with custom AI agents, MCP servers, or LLM pipelines. In a separate question, 68% said they use AI to chain vulnerabilities across multiple attack surfaces.

Testing one application at a time can miss risks involving tool permissions, identity, and downstream actions. Programs need to include these connections in scope.

Valid Reports Across OWASP

2025 – 2026 Year-over-year performance



Section 5.
Who's Responsible When AI Gets It Wrong?

When an AI-assisted tool incorrectly validates, prioritizes, or rejects a finding, responsibility most often falls to the CISO.

39% of security leaders selected the CISO as the role most likely to be blamed. Only 10% said responsibility would be distributed through a formal framework.

Organizations are delegating decisions to AI faster than they are defining accountability. Roles, escalation paths, and human review should be established before a bad decision puts them to the test.

AI Delegation: Accuracy Is the Top Concern

Security leaders report substantial concerns about delegating security decisions to AI. Their top concern is accuracy, specifically the risk that AI tools incorrectly validate, prioritize, or reject findings, producing false negatives that leave real vulnerabilities unaddressed. That concern was cited by 47% of respondents, followed by regulatory exposure (41%), loss of human oversight (41%), and adversarial manipulation of AI agents (37%).

In more than a third of organizations, executive leadership only partially understands the difference between discovery, validation, and remediation.

That makes accountability harder to assign. The AI tool may share in the tasks, but each decision should have an owner, record, and an accountable human. Those controls remain consistent when a finding moves from security to engineering.

The Next Wave for Security Leaders

Security leaders identified several top emerging challenges:

60%	AI-accelerated attacker capabilities
42%	Agentic AI and MCP security
41%	Identity-based attacks
37%	Supply chain compromise

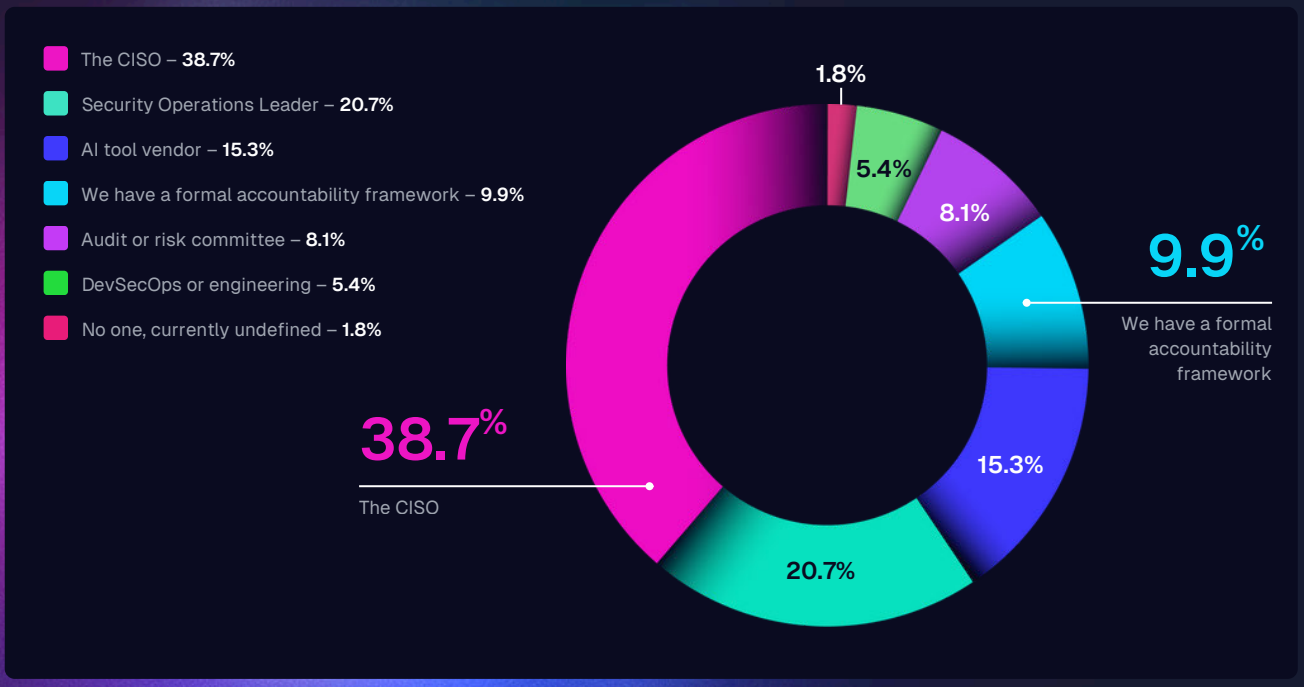
In a separate question, nearly half of security leaders cited faster exploitation of known vulnerabilities as AI's greatest operational threat.

The risks extend to how organizations use AI themselves. Excessive Agency vulnerabilities occur when AI systems can act beyond their intended limits. Reports of these vulnerabilities on the H1 Platform tripled from 2025 to 2026.

Autonomous agents need clear limits on what they can access and do, along with points for human review. The NIST AI Risk Management Framework provides a structure for this work through four functions: Govern, Map, Measure, and Manage. Organizations also need to decide who approves consequential actions and who is accountable when they fail.

The EU AI Act's Article 50 transparency obligations came into effect on August 2, 2026. The European Commission's guidance explains when people must be told they are interacting with AI and when AI-generated content must carry machine-readable markings, a requirement that applies from December 2, 2026 for systems already on the market. These requirements do not govern vulnerability accountability, but they reinforce the need for clear ownership and documentation.

Formal Accountability vs. Default Blame Assignment





"Accountability for any security program or tool should squarely fall on the security team, not the vendor. If you're getting false positives, that's on the security team to dig into. They need to own the tools, the process, and the experience end to end."

— Kyle Barry, CISO at CLEAR

Section 6.
The Human Layer

A business-logic flaw can look like ordinary product behavior until someone asks the right questions:

What should this account be allowed to do?

What changes if an attacker combines that permission with another workflow?

Can the result be reproduced?

Answering those questions takes judgment. It means learning how the product is supposed to behave, how permissions interact across systems, proving a path an attacker could actually take, and showing what that path costs the business. What makes the finding real is also what makes it hard to hand off: the exploit path, the surrounding context, and the steps that reproduce it have to reach the engineer who fixes it, intact.

Researchers Use AI for Scale and Judgment for Impact

Researchers use AI most for reconnaissance → **66%** and report writing **58%.** Manual exploitation ranks much lower, at **23%.**

AI's limits are clearest in more complex findings: → **62% of researchers say AI is weakest at identifying business logic flaws**, while 41% point to multi-step chained exploits.

Researchers are moving further into those areas. → Researchers are moving further into those areas. **72%** identified business logic flaws as one of the fastest-growing vulnerability classes in their own research, and **56%** selected chained authentication and IDOR. These are areas where human judgment remains central.

The Gap Between Finding and Fixing

Business logic flaws, chained exploits, and access control failures can span workflows, systems, and teams. Fixing them requires the context that made the finding possible, including the intended behavior, exploit path, and impact. When that context is lost between security and engineering, remediation slows and Exposure Debt grows.

Where AI is Strongest vs. Weakest

Researcher-reported areas of AI capability

AI STRENGTHS

Reconnaissance	66%
Report writing	58%
Escalating bugs	40%
Chaining bugs	35%
Large-scale scanning	34%

AI WEAKNESSES

Business logic	62%
Multi-step / chained exploits	41%
Race conditions	28%
Authentication bypasses	26%
Insecure design flaws	24%

Human contribution remains substantial even where AI tooling is active. Only 1 in 7 researchers describes their workflow as largely or fully autonomous. The other six are in the loop, finding things AI can't.



Section 7.
The Bounty Economy Is Splitting by Industry

Demand for AI security is driving up bug prices. HackerOne bug bounty programs collectively paid out $89 million between July 2025 and June 2026.

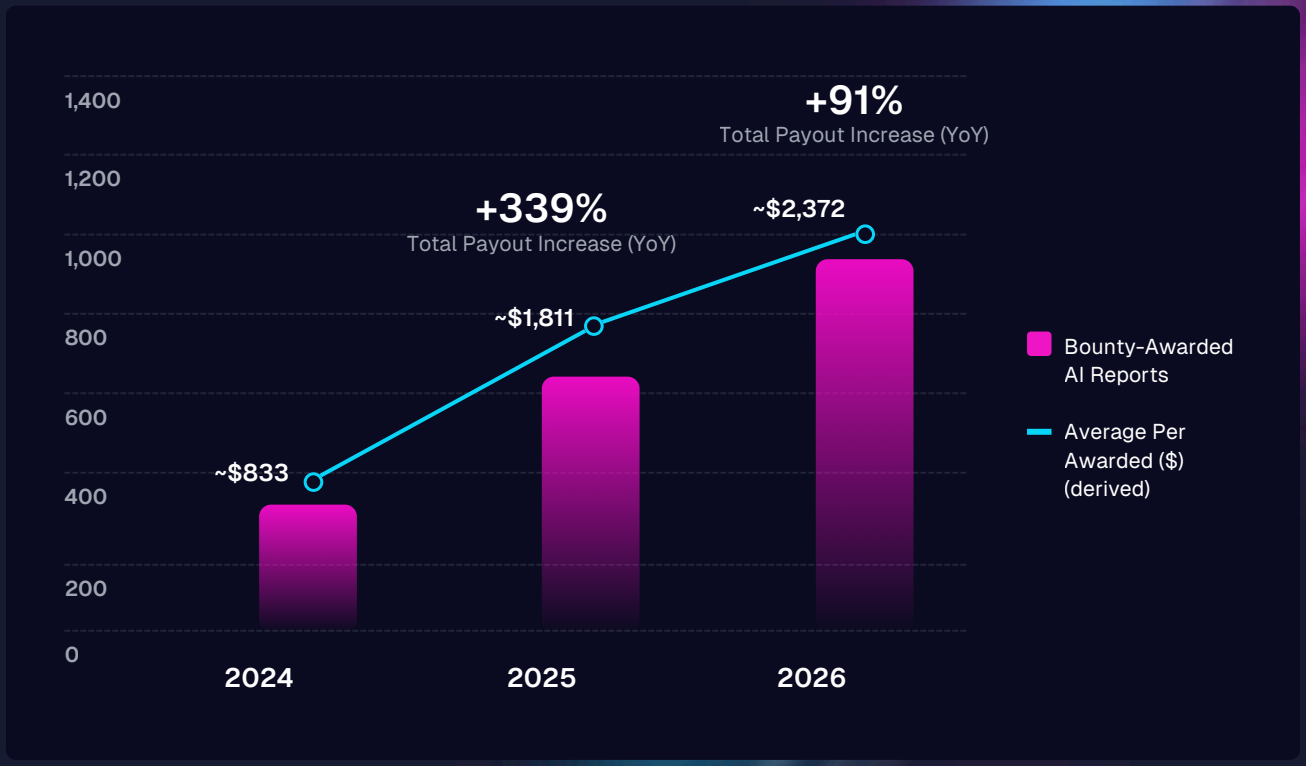
Valid AI reports grew 53% this year and total payouts rose 91%.

18% increase from the prior year.

That increased the average award per AI finding by 185% between 2024 and 2026, confirming that programs are placing a premium on complex AI vulnerabilities over routine bug classes.

Bounty-Awarded AI Reports

2024, 2025, 2026



Payout averages cover bounty-awarded reports. Published bounty benchmarks below describe offered award levels, rather than realized payments.

Bounty Economics and Backlog Pressure Vary

Technology / Computer Software

Computer Software is the largest industry on the H1 Platform. In the broader Technology/Hardware/Software Provider survey group, validated findings and AI-driven threats are creating significant pressure on security teams:

- **66%** say validated findings enter their backlog faster than their teams can remediate them
- **72%** cite AI-accelerated attacker capability as their top emerging concern – the highest of any industry
- **41%** cite Agentic AI and MCP security as a top concern

Financial Services

Financial Services respondents face some of the most demanding remediation challenges in the dataset:

- **38.5 hours average** time to validate critical findings – the longest of any industry
- **22.6 days average** time to remediate critical findings – the longest of any industry
- **68%** say validated findings arrive faster than their teams can remediate them
- **68%** cite AI-accelerated attacker capability as a top concern
- **53%** cite Agentic AI and MCP security – the highest of any industry

Technology/Computer Software		Financial Services
1,286	programs	502
$3,225	median critical bounty	$4,983

The Bounty Economy Split by Industry

Industry benchmarks

Technology/Hardware/ Software Provider		Banking/Financial Services/ Insurance
31.7 hrs	Average critical-validation time[1]	38.5 hrs
15.0 days	Average critical-remediation time[1]	22.6 days
66%	Findings entering backlog faster than remediation[1]	68%
$3,225	Median maximum critical bounty offered[2]	$4,983
$30,000	95th percentile maximum critical bounty offered[2]	$15,850

[1] Security Leader Survey, August 2026
[2] H1 Platform data, September 2026

Healthcare

- **Median Critical Bounty:** $5,000
- **Challenge:** Patching authorization and identity flaws across clinical systems without disrupting patient care or violating regulatory compliance.

Internet & Online Services

- **Median Critical Bounty:** $3,092
- **Challenge:** Fixing broken access controls and account-takeover vectors across fast-moving APIs without breaking live user traffic.

Cryptocurrency & Blockchain

- **Median Critical Bounty:** $90,000
- **Challenge:** Catching smart-contract logic and key-management flaws before deployment, where an exploit causes irreversible, instant loss of funds.

Section 8.

Reducing Exposure Debt: Five Actions

The data points to five actions security leaders can take to reduce Exposure Debt.

1. Increase Investment in Remediation



Detection and response remains the top-ranked security investment priority, while remediation was ranked first by only 1 in 10 security leaders overall. H1 Platform data shows the current bottleneck is at the fix stage, not discovery. Nearly 70% of leaders confirm findings enter their backlog faster than teams can remediate them. Add resources to fixing constraints: code ownership, developer sprint capacity, and cross-team dependencies.

2. Use Resolution Time as a Continuous Benchmark



Average resolution time improved from 135 days to 62 days across all severity levels, a 54% reduction that suggests meaningful progress is achievable. But resolution time only measures closed tickets. Organizations that have not seen comparable gains have a clear, measurable operational gap to close. Track resolution velocity alongside backlog age, severity distribution, and retest pass rates.

3. Update Program Scope to Include AI Assets and Agentic Systems



In this year's survey, 42.5% of researchers focus on AI and LLM assets, and 51% are actively developing Model Context Protocol (MCP) security skills. If your program scope has not expanded to cover where researchers are looking, your organization has an active blind spot. Bring AI models, autonomous agents, and tool integrations into scope, and make sure each asset has a designated engineering owner before findings arrive.

4. Treat Validation Speed as a Board-Level Metric

Security leaders report an average of 30 hours to validate a critical finding, with a median of 21 hours. That's 30 hours of open exposure on your highest-severity findings before remediation even starts. If that metric is not reaching executive leadership, it should be. Separate validation speed from remediation time to diagnose bottlenecks early.

5. Define AI Accountability Before an Incident Forces You

When an AI tool validates, prioritizes, or rejects a vulnerability incorrectly, 39% of security leaders say the CISO takes the blame. Only 10% of security leaders said responsibility would be distributed through a formal accountability framework rather than landing on an individual. The blame question is not the whole cost. When a valid finding is wrongly rejected or severity lowered, the person who loses is the researcher who found it. The hours are spent, the report is closed, and the researcher is not fairly compensated. Accountability has to cover both sides of that. Build the framework before an incident makes it urgent. Formally define the limits of automated tool decisions, where human review is mandatory, and who owns escalation.

That applies equally to HackerOne. On the H1 Platform, automated systems close reports as spam, duplicates, or out of scope. Severity and bounty amounts are set by customer program teams, with agent input advisory. When a researcher believes a closure or an amount is wrong, Mediation puts a person on it. Where mediation confirms that a report was closed in error, HackerOne works with the program to reopen it and have it assessed at the correct severity. How those systems work is published on our blog, Responsible AI at HackerOne.

Closing Remarks: From Discovery to Resolution

For much of the past decade, security programs focused on finding vulnerabilities across a growing attack surface. This report shows how far that has come. Researchers are finding flaws that span workflows, systems, and teams, and AI has changed how the work gets done at every stage.

The next challenge is resolving them.

Exposure Debt is the set of validated, exploitable vulnerabilities an organization already knows about and has not yet closed.

It does not shrink because discovery slows down. It shrinks when someone owns the fix, when validation is fast enough to be useful, and when the judgment behind a finding survives the handoff to the person who has to act on it.

That is work with three parties in it. Researchers prove what is real. HackerOne validates it, and owns the quality of that validation, including correcting it when our systems get it wrong. Customers close it. Discovery has not gotten easier. The next decade of this report will be about whether resolution got better.

Researchers have expanded what organizations can see. The priority now is giving teams what they need to act.

- Read: Fixing the Fix Gap to discover how H1 Remediation closes the gap.
- Download: The New Metrics That Matter to learn how to brief your board on AI-accelerated exposure.



"We've spent years making vulnerability discovery faster and more effective. But discovery without validation is increasingly meaningless. Security teams are drowning in findings, and volume without confidence just moves the problem downstream. The next challenge is tying discovery and validation together, then making sure resolution can keep up. Reducing Exposure Debt means bringing speed and intelligence to everything that happens after a finding is submitted, not just how fast you find it."

— Nidhi Aggarwal, Chief Product Officer at HackerOne

hackerone

Ready to reduce your Exposure Debt? Contact HackerOne.

Data Sources and Methodology

H1 Platform Data

- **Primary period:** July 1 through June 30. All annual comparisons in this report follow that convention. Comparisons use the full available period for each metric: backlog and resolution figures compare the periods ending June 30, 2024 and June 30, 2026; vulnerability mix trends use the period ending June 30, 2026 against five years prior where a longer view is more representative.
- **Scope:** Aggregated H1 Platform data used for valid vulnerability reports, severity, open-report backlog, resolution duration, AI-related reports, source-code reports, bounty measures, and program-level trends.
- **Privacy treatment:** Results are aggregated and anonymized for reporting.
- **Data-pull dates:** Core platform extracts used for the manuscript were pulled August 25, 2026. The industry bounty-table snapshot is dated September 1, 2026.

Security Leader Survey

- **Method:** Web-based survey conducted in August 2026.
- **Sample:** 111 security leaders at organizations reporting $100 million or more in revenue/budget across the United States, Canada, the United Kingdom, Australia, Singapore, and Germany.
- **Interpretation:** The sample includes multiple leadership roles and is referred to throughout as the Security Leader Survey. "CISO" is used only for actual CISO respondents or when quoting an explicitly named source.
- **Question bases:** Percentages use valid responses to the applicable question. Metric-specific bases should appear near industry or subgroup results where the valid n differs.

Researcher Survey

- **Method:** Online survey conducted from July through August 2026.
- **Sample:** 408 HackerOne security researchers overall; valid-response counts vary by question.
- **Interpretation:** Results describe the respondents to each question. Differences from prior survey years compare responding samples rather than tracking the same individuals over time.
- **Multi-select items:** Percentages may total more than 100%.

Methodological Comparability

The 2026 Security Leader Survey uses a broader, mixed leadership sample and is not limited to HackerOne customers. Earlier report surveys used different populations and methods. Cross-year survey figures should therefore be described as differences between samples, not as a longitudinal change in the same respondents.

Historical platform figures may differ from previously published counts where definitions or extracts changed.

Resolution-duration averages include resolved reports only. Recent unresolved reports may affect comparisons between periods.

External Sources

1. Verizon Data Breach Investigations Report 2026
2. Closing the AI Security Gap: Containing Risk Before It Scales, HackerOne

© 2026 HackerOne Inc. All rights reserved. HackerOne, H1, and the HackerOne logo are marks owned by HackerOne Inc. and are registered in the US and other countries. HackerOne owns other trademarks and service marks and may use the brands of third parties to identify their products and services. All third-party marks are the property of their respective owners, and their use does not imply any affiliation with, sponsorship by, or endorsement of HackerOne.

This report is provided for informational purposes only and does not constitute legal or professional advice. References to laws, regulations, and third-party frameworks describe their general subject matter as of the date of publication and may not reflect subsequent developments.