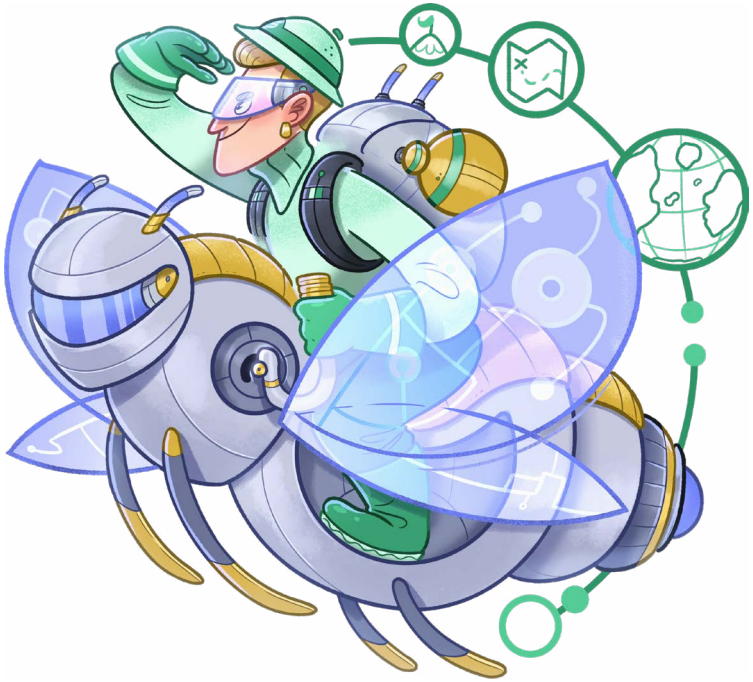
Signal Through the Slop: The 2026 Security Forecast

6 key insights from Intigriti on navigating AI deception, supply chain risk, and the new vulnerability landscape

INTIGRITI

Table of contents



Introduction

In 2025, the cybersecurity landscape continued its rapid evolution as organizations worked to balance technological innovation with increasingly complex regulatory obligations. Artificial Intelligence (AI) has driven a monumental shift in how companies operate, introducing transformative capabilities while simultaneously expanding the scope of risks. Regulators across multiple jurisdictions updated and expanded their requirements to keep pace with the shifting threat landscape. Together, these developments marked 2025 as a year where cutting-edge technologies, AI-powered tools, and emerging compliance frameworks began to integrate more deeply into day-to-day security strategies.

Organizations showed a growing focus on operational resilience, proactive risk management, and aligning practices with both technological progress and regulatory expectations.

The industry has also seen a wave of papers and predictions for 2026, including OWASP's Top 10 2025 report[1]. While several of those insights align with elements in this report, the perspective here is based on the insights of the Intigriti team.

Drawing on the observations and data gathered throughout 2025, this report examines threats seen in practice and the trends expected to grow, evolve, and define the cybersecurity landscape in 2026.

This paper identifies six key points for 2026:

1. The increasing impact of successful cybersecurity breaches.
2. The growth of supply chain risks.
3. A boost in government cybersecurity spending and crowdsourced skills.
4. The emergence of vulnerabilities in Large Language Models (LLMs).
5. The development of creative solutions to counteract AI-generated slop.
6. The rise of multilayered identity verification applications in response to AI-driven deception.

Points 4, 5, and 6 examine multiple aspects of AI from various perspectives. We explore the use of AI in software development, its role as an assistant in bug bounty work, and several other applications. This is because these areas have distinct implications, all of which must be considered as AI continues to evolve heading into 2026.

By examining these six points, this report provides a comprehensive view of how organizations can prepare for the evolving threat landscape in 2026, with insights from Intigriti security experts:

- **Alex Olsen**, Hacker Community Lead
- **Chris Holt**, Strategic Engagement & Community Architect
- **Eleanor Barlow**, Senior Cybersecurity Technical Writer
- **Inti De Ceukelaire**, Chief Hacker Officer
- **Justine Simal**, Legal Counsel
- **Lennaert Oudshoorn**, Head of Triage

1 • owasp.org/Top10/2025/0x00_2025-Introduction/

Threat landscape 2026 executive summary

Forecast 1: Rising severity of cyberattacks

The Cyber Security Breaches Survey 2025[2], released by Gov.uk, illustrates a positive development regarding the reduction of cyber breaches and attacks against medium and large businesses. While still high, they show a decline over the last year, stating that in 2024, 70% of medium and 75% of large companies were targeted. Whereas in 2025, the numbers decreased, showing that 67% of medium and 74% of large companies were targeted.

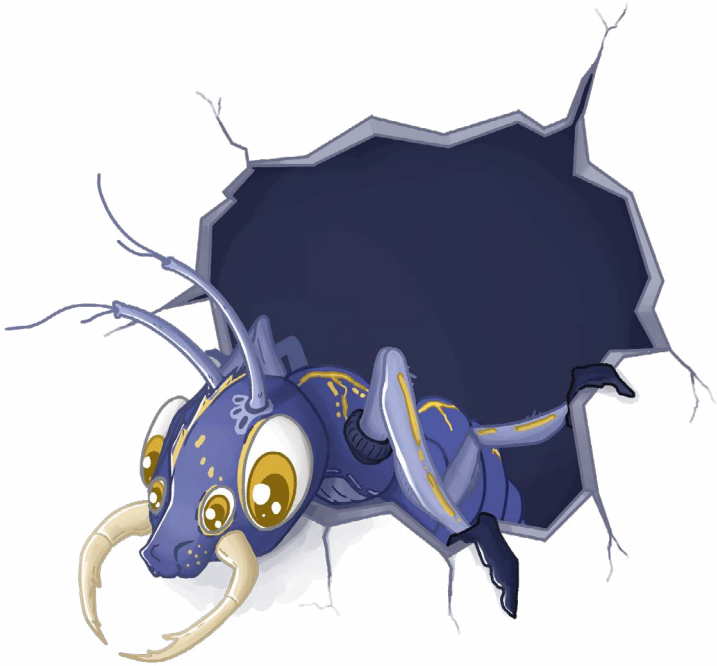
Data, however, from the NCSC Annual Review 2025[3] highlights that, despite this reduction in the overall number, there was in fact a 130% spike in nationally significant cyber incidents. This spike represents the highest ever increase nationally, with 204 significant cyber incidents. Previous years reached a maximum of 89 incidents categorized as high impact.

And this is not just an occurrence in the UK. A press release entitled 'Global Ransomware Attacks Against Critical Industries Surge 34% in 2025[4]' highlights how, in 2025, half of all ransomware attacks worldwide targeted sectors deemed essential. These include healthcare, energy, transport, and finance. This shift underscores a clear goal to destabilize economies and impact critical infrastructure.

Lennaert Oudshoorn, Head of Triage at Intigriti, provided some context to the situation.

"With everything in the world becoming more connected and more dependent on digital things, we're going to see an increase in the impact of cyber-attacks, in terms of their power. Take the Bank of England, as one example of many around the world. For the first time in history, we saw in 2025 how a cyber-attack contributed to, and was credited for, slowing the UK's GDP growth. The impact is profound."

LENNAERT OUDSHOORN
HEAD OF TRIAGE
INTIGRITI



2 • gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025

3 • ncsc.gov.uk/collection/ncsc-annual-review-2025

4 • prnewswire.com/news-releases/global-ransomware-attacks-against-critical-industries-surge-34-in-2025-302589217.html

As supported by The Register[5], 'The Bank of England (BoE) has cited the cyberattack on Jaguar Land Rover (JLR) as one of the reasons for the country's slower-than-expected GDP growth in its latest rates decision.'

The challenge today, in comparison with previous years, is that businesses across the globe are more digital. With three websites built every second[6], companies store more sensitive data than ever, have more dependencies on supply chains, and this year, 98% of companies[7] were forecasted to be using public cloud services.

In addition, regulations and compliance requirements are strict, on a global level, and, if not met, impose significant penalties that can cripple smaller businesses altogether. These same businesses are expected to handle threats coming from professional criminal networks that target critical operations, not just data, making the recovery of a successful attack more complex.

"While 2025 has seen compliance frameworks move in a positive direction, especially with regards to the broader adoption of NIS2, DORA, and similar practices, the reality is that a successful cyber breach can be financially damaging for many organizations. Beyond regulatory fines, which can reach millions under instruments like GDPR and NIS2, the indirect costs of business interruption, operational recovery, legal exposure, and reputational loss often pose the greater threat. For smaller companies in particular, the combination of rising compliance expectations and increasingly sophisticated attacks means that one serious incident can strain, or even exceed, their financial resilience."

JUSTINE SIMAL
LEGAL COUNSEL
INTIGRITI

5 • theregister.com/2025/11/07/bank_of_england_says_jlrs/
6 • siteefy.com/how-many-websites-are-there/
7 • dtpgroup.co.uk/insight/50-cloud-computing-statistics/

A successful breach today is widespread and can impact operational continuity, revenue, brand reputation, compliance, Intellectual Property (IP), and trust. Even with fewer successful breaches, it is likely that more severe attacks are expected in 2026 with a significant impact on both consumers and businesses.

A key issue that plays into this is that ethics is playing a less significant role. Researchers are interested in tech stacks, and cyber criminals are opportunists who will exploit wherever they can get a foothold, regardless of industry. In fact, often, threat actors are after certain bugs, rather than an industry vertical at all. It does not matter if the person paying the ransom works for a manufacturing company or a university. We might even see further degradation in terms of reach in 2026, across the board. For instance, during COVID-19, there was an element of ethics at play where some cybercrime groups would limit or even stop attacks against hospitals. But now, as more actors are part of the scene, issues regarding the morality of targeting healthcare providers, and the like, do not seem to be as much of a consideration.

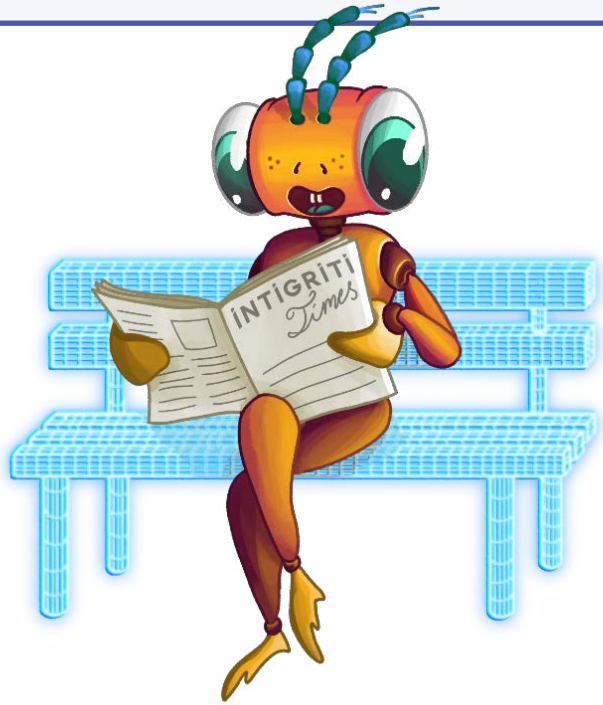
While there are certain threat actors and dedicated groups that do target certain industries, that's a very small part of the picture. Looking at it more broadly, people are opportunists, and everyone is a target now.

Richard Horne, the NCSC's chief executive, delivered a speech at the Annual Review 2025[8] launch event on October 14, 2025 where he stated that "With over half the incidents handled by the NCSC deemed to be nationally significant, and a 50% rise in highly significant attacks on last year, our collective exposure to serious impacts is growing at an alarming pace.[...] The best way to defend against these attacks is for organizations to make themselves as hard a target as possible. That demands urgency from every business leader: hesitation is a vulnerability, and the future of their business depends on the action they take today."

How can bug bounty be used to prioritize impact?

Intigriti's triage team will always assess findings based on their impact in accordance with the program's severity scoring guidelines. A well-defined policy helps manage expectations and ensure consistent evaluations. During an assessment on vulnerability type, the submission's impact score is calculated based on the initial and immediate effect on the vulnerable system.

The Intigriti Triage Standards[9] are established to provide a comprehensive and consistent framework for evaluating the severity of vulnerabilities reported by security researchers. This policy aims to ensure that vulnerabilities are assessed fairly, transparently, and in alignment with both industry standards and the specific context of each bug bounty program.



8 • ncsc.gov.uk/news/uk-experiencing-four-nationally-significant-cyber-attacks-weekly
9 • kb.intigriti.com/en/articles/10335710-intigriti-triage-standards

Forecast 2: Growth of supply chain risks

2025 has seen a significant growth in supply chain dangers, an element that is predicted to grow in 2026.

You only need to look at the 2025 OWASP top 10[10] to see that software supply chain failures have risen to third place. The result of a weak or vulnerable supply chain is extensive and often a blindspot to many organizations.

People rely on certain technologies from other locations. For instance, the European car industry has decreased in recent years; this means that dependencies on other providers for car products might change relationships and alliances. And not just cars, solar panels on roofs, transport, energy, you name it. And this is around the world, not just in Europe.

A key element here is that supply chains support critical infrastructure around the world. Which means, alongside cyber security risks, supply chain attacks have geopolitical impacts and implications.

"Critical infrastructure impacts everyone, which means a single weak point can have serious consequences. Supply chain risk isn't new, but it's something organizations need to keep at the top of their minds as we move into 2026. People rarely notice the problem until something breaks. Understanding what critical infrastructure is, what it runs on, and how it's connected to suppliers is essential. The more dependent we are on complex supply chains, the more important it becomes to monitor and secure them."

ALEX OLSEN
HACKER COMMUNITY LEAD
INTIGRITI

How Bug Bounty reduces supply chain risks?

If included in the scope, researchers can test systems where internal teams may lack visibility to issues such as insecure dependencies, over-privileged integrations, shadow assets, and misconfigured vendor services. Bug bounty hunting also means that researchers test new vulnerabilities as they emerge, not just one-off tests here and there that miss key developments. This forms proactive, ongoing security testing that makes the third-party company and, therefore, the supply chain, more resilient.

10 • securitybrief.co.nz/story/owasp-updates-top-10-list-supply-chain-risks-now-top-concern

Forecast 3: Boost in government security spend and crowdsourced skills

Recruitment of students and hackers to support governmental security is on the rise and is expected to continue to grow in 2026.

A good example of this can be seen at The Centre for Cybersecurity Belgium (CCB), where, from the 12th to the 26th of November, Belgium's ethical hackers and cybersecurity students joined forces to boost the digital resilience of the Federal Government during 'Hack the Government 2025'[11].

Over 70 researchers took part in the event, attempting to infiltrate sensitive platforms from institutions including the Military, the Police, and the Ministry of Defense. Nearly 100 vulnerabilities were identified, some of which have already been resolved.

"10 years ago, this would have been illegal. 2 years ago, this was finally legal, but nobody dared to talk about it. Today, Belgian media proudly report on ethical hackers finding almost 100 bugs. This is a mind shift. Admitting that you're vulnerable and doing something about it is something to be applauded, not shamed."

INTI DE CEUKELAIRE
CHIEF HACKER OFFICER
INTIGRITI

Initiatives like these physical hacking events focused on government security are predicted to start developing more globally in 2026. These events will not just become arenas for securing governments, military, police, and the like, but for recruiting talent.

With an increase in recruitment, it is also likely that there will be an increase in military spending for cybersecurity.

NATO, for instance, has already increased its budget for cyber security. At the 2025 NATO Summit[12] in The Hague, 'Allies committed to investing 5% of Gross Domestic Product (GDP) annually on core defence requirements and defence- and security-related spending by 2035. They will allocate at least 3.5% of GDP annually based on the agreed definition of NATO defence expenditure by 2035 to resource core defence requirements and to meet the NATO Capability Targets. Allies agreed to submit annual plans showing a credible, incremental path to reach this goal. They will account for up to 1.5% of GDP annually to inter alia protect critical infrastructure, defend networks, ensure civil preparedness and resilience, innovate, and strengthen the defence industrial base.'

What we will see on a global level are more tests on military infrastructure. But also, resilience tests, such as tests on drones, for instance. Amateur drones are causing substantial damage right now in places like airports. And, as these techniques continue to develop, it is reasonable to view this as a new method of proxy warfare.

11 • linkedin.com/feed/update/urn:li:activity:7400131705812074496/

12 • nato.int/en/what-we-do/introduction-to-nato/defence-expenditures-and-natos-5-commitment

These criminally operated drones[13], which are directly connected with cyber criminals on the ground, and not just virtually, have proven to be a significant issue throughout 2025. An issue occurring in more places than airports.

In this press release[14], and backed by a £900,000 investment to crack down on drugs and weapons, the UK's Minister for Prisons, Probation and Reducing Reoffending, Lord Timpson, said that "The ease with which drones were operating over prisons was yet another sign of the chaotic prison system we inherited last July. As part of the Plan for Change, we are tackling the organised crime gangs behind the drug supply routes so that our prisons can start cutting crime and stop creating better criminals."

Drones have been shown not just as drug delivery systems, but as methods for surveillance to capture sensitive data across the globe. According to Privacy International[15], 'With their ability to navigate diverse environments and capture real-time data, drones offer unparalleled flexibility in aerial surveillance operations. However, their widespread adoption has raised significant concerns regarding the right to privacy and other human rights, as well as ethical implications of their widespread use.'

The solution is to either physically remove them, with lasers or the like, which is a technology being tested right now with HEL systems, or to hack them to gain insight into the intelligence accessed and then act accordingly. There could eventually be intelligence bounties for drone detections here. This might be more of a 2028 initiative, but the building blocks towards a drone detection network could start forming in 2026, to catch the drones that fly under the radar.

It's not just governments turning to the crowd for their extensive knowledge and security testing skills. But there is also a trend in the number of companies turning to crowdsourced security for information.

A potential pivot within the industry is seeing companies turn to the crowd for information directly. Organizations may start asking for more information that researchers have found that indicates they are/were in breach. Companies may encourage researchers to tell them that if they spot someone selling company data on the dark web, to tell them, and they may be able to reward them and do intelligence to support their due diligence.

In fact, in a Market Research 'Crowdsourced Security Market Report[16]' 'The Global Crowdsourced Security Market size is expected to be worth around USD 283.9 million by 2034, from USD 129.1 million in 2024, growing at a CAGR of 8.2% during the forecast period from 2025 to 2034.

13 • bbc.co.uk/future/article/20170731-how-cops-catch-drone-flying-criminals
14 • gov.uk/government/news/counter-drone-efforts-rise-as-prison-sightings-revealed
15 • privacyinternational.org/learn/drones-surveillance
16 • market.us/report/crowdsourced-security-market/

Forecast 4: Growth of LLM vulnerabilities

Large Language Model (LLM)

An LLM stands for Large Language Model[17], which is an AI program trained on giant datasets to understand, process, and generate human language.

According to the Grand View Research 2025-2030 Report[18], 'The global large language models market size was estimated at USD 5,617.4 million in 2024 and is projected to reach 35,434.4 million USD by 2030, growing at a CAGR of 36.9% from 2025 to 2030.'

The challenge with this growth, however, is that most companies still don't understand what security around LLMs really looks like.

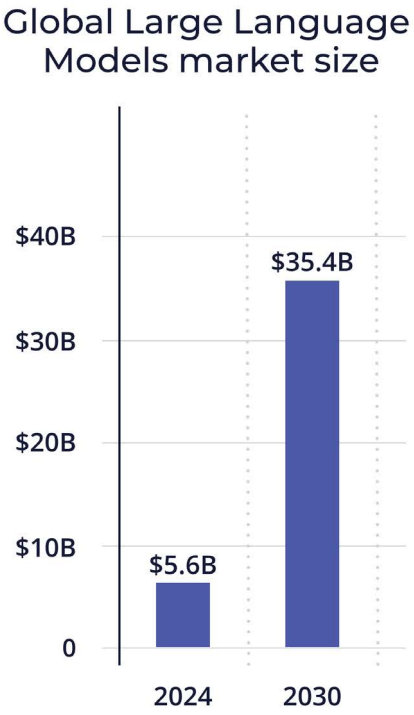
AI security is still in its early days. Research, courses, and guidance are only now starting to appear, which means organizations are relying on insights that are still developing.

In the LLMO2:2025 Sensitive Information Disclosure report[19], OWASP highlights how LLMs, 'especially when embedded in applications, risk exposing sensitive data, proprietary algorithms, or confidential details through their output. This can result in unauthorized data access, privacy violations, and intellectual property breaches.'

This also brings into question a new standard of what is acceptable:

"AI models and tools like the Model Context Protocol (MCP), which allow LLMs to connect to external systems, are being integrated despite clear limitations. Models can hallucinate, produce malformed output, or ignore requested formats. Even simple tasks like returning valid JSON can fail. There is no standard for input, output, or reliability testing, and in traditional software engineering, even a 1% failure rate of a system's process or output would be treated as a critical issue, yet with LLMs, inconsistent behaviour is often treated as normal."

ALEX OLSEN
HACKER COMMUNITY LEAD
INTIGRITI



17 • intigriti.com/researchers/blog/bug-bytes/bug-bytes-199
18 • grandviewresearch.com/industry-analysis/large-language-model-llm-market-report
19 • genai.owasp.org/llmrisk/llm022025-sensitive-information-disclosure/

OWASP advises that 'Consumers should be aware of how to interact safely with LLMs. They need to understand the risks of unintentionally providing sensitive data, which may later be disclosed in the model's output. LLM applications should perform adequate data sanitization to prevent user data from entering the training model. Application owners should also provide clear terms of use policies, allowing users to opt out of having their data included in the training model. Adding restrictions within the system prompt about data types that the LLM should return can provide mitigation against sensitive information disclosure.'

An issue here, however, is that these restrictions may not always be respected and can be bypassed with prompt injections and other methods.

As presented in a 2025 paper on 'The Dark Side of LLMs: Agent-based Attacks for Complete Computer Takeover'[20], from Lupinacci, M., Pironti, F. A., Blefari, F., Romeo, F., Arena, L., & Furfaro, A., where 'LLM agents as attack vectors are capable of achieving complete computer takeover through the exploitation of trust boundaries within agentic AI systems where autonomous entities interact and influence each other.'

The paper demonstrates how adversaries can leverage direct prompt injection, RAG backdoor attacks, and inter-agent trust exploitation to coerce popular LLMs (including GPT-4o, Claude-4, and Gemini-2.5).

How can crowdsourced security support LLM safety?

"Current security testing methodologies for LLMs face significant constraints that limit their effectiveness in identifying potential vulnerabilities. Traditional automated testing solutions and manual testing approaches rely heavily on pre-defined, templated prompts. This rigid framework fails to accommodate the dynamic nature of real-world attacks, particularly when confronting sophisticated prompt injection threats. The inability to generate and execute randomized attack patterns creates potential blind spots in security testing coverage[21]."

With crowdsourced security, a global community of researchers, using a wide variety of skills and tools, can identify what internal teams often miss. These experts search for vulnerabilities, including prompt injections and data leakage, within complex ecosystems. Once vulnerabilities are identified, clear triage means clear prioritization, which helps businesses decipher what elements have the greatest impact on both business, people, and processes. Valuable actions can then be taken to make LLM systems more secure and resilient.

20 • arxiv.org/html/2507.06850v3#:~:text=We%20demonstrate%20that%20adversaries%20can,themselves%20become%20sophisticated%20attack%20vectors.

21 • crowdstrike.com/en-us/blog/feedback-guided-fuzzing-reveals-llm-blind-spots/

Forecast 5: Creative solutions needed with AI slop on the rise

Vibe coding[22] is the latest trend sweeping through developer communities. It's the art of describing a concept, feeding it to an AI, and letting the LLM (Large Language Model) manifest the code based purely on vibes. And as more developers rely on AI to "vibe" their way through coding, we're entering a new golden age of bug bounty hunting. The issue here is that because AI-generated code often looks functional and even runs, it still hides subtle, and sometimes catastrophic, security flaws.

Software engineering is complex and involves many requirements, including system design, architecture, testing, debugging, deployment, maintenance, and coordination with teams or stakeholders, to name just a handful of responsibilities. Today's AI tools can generate code snippets and assist with routine tasks, but the limitations here lie in creativity and logic.

Software engineering is multifaceted, and AI can just about manage the code part, but elements like logic, creativity, and problem-solving do not exist yet. These elements must come from people.

AI still lacks contextual judgment, ethical considerations, and expertize in creative problem-solving.

"We see a very strong focus on AI usage across the board. If you tell AI to code something, it's unlikely that the AI thinks about sanitising user inputs and other necessary elements like that. There is a trend where a lot of bugs are more design issues and logic issues, rather than code issues."

LENNAERT OUDSHOORN
HEAD OF TRIAGE
İNTİGRİTİ

22 • intigriti.com/researchers/blog/hacking-tools/vibe-coding-security-vulnerabilities

When companies overly rely on AI and consistently generate AI slop, issues with the long-term reliability of systems and mistakes can be costly. With 84% of respondents using or planning to use AI tools in their development process, an increase over last year (76%)[23], and with 51% of professional developers using AI tools daily already, these issues will likely increase in 2026.

"AI presents much more of a threat to the standard organization's environment than simply what attackers can do with it. Insider threats that AI and shadow IT present, data exfiltration capability, unseen data poisoning core datasets, and much more. There is an enormous volume of "work" that AI creates, and then people are expected to review, or just blindly trust."

CHRIS HOLT
STRATEGIC ENGAGEMENT & COMMUNITY ARCHITECT
INTIGRITI

Intigriti's use of AI to enhance knowledge and reduce slop

Earlier this year (2025), GCHQ's National Cyber Security Centre[24] published a report emphasising the increased impact of cyber threats using artificial intelligence-based tools. It suggested that over the next two years, 'a growing divide will emerge between organizations that can keep pace with AI-enabled threats, and those that fall behind – exposing them to greater risk and intensifying the overall threat to digital infrastructure'.

For researchers, it is important to be able to attack AIs, but also use AI because while it is a valuable tool, it is not a magic bullet or be-all end-all that some make it out to be. While it can make workflows faster and more accurate, AI has a place, and because more and more companies are using it, it is a valuable skill to learn how to exploit it as well.

At Intigriti, we believe AI is a powerful ally to, not a replacement of, our community of security researchers. Intigriti uses AI to empower researchers to hunt for bugs smarter, faster, and more efficiently, while recognizing the value of human creativity and ingenuity that machines cannot replicate. By creating AI-powered tools informed by researcher and customer insights, and built on a foundation of trust and consent, researchers are enabled to focus on what matters most: uncovering critical vulnerabilities faster and securing the digital world. Read more on how AI is used to enhance the Intigriti platform here[25].

23 • survey.stackoverflow.co/2025/
24 • ncsc.gov.uk/news/ai-to-2027-threat-assessment
25 • intigriti.com/blog/news/how-ai-is-leveraged-to-enhance-the-intigriti-platform

Forecast 6: Multilayered identity verification apps to increase as AI-driven deception grows

Off the back of AI advancements, AI-driven deception is on the rise. The 2025 Jumio Online Identity Study[26], reported that 'Sixty-nine percent of respondents say AI-powered fraud now poses a greater threat to personal security than traditional forms of identity theft, and confidence in online authenticity continues to erode amid growing fears of manipulated content and AI-driven deception.'

Multilayer verification amidst the growth of AI-driven deception and fraud is needed. But managing user identity details can be quite complex. Verification flows may need to involve biometrics, third-party integrations, and fallback mechanisms to handle exceptions. It's also important to implement steps to detect deepfakes and other forms of synthetic or fraudulent identity data.

This leads to awareness around higher levels of spam and, with it, further security risks.

Identity verification apps and integrations are expected to rise in 2026, driven by AI's growing ability to autonomously create accounts. This increase in automated accounts will likely lead to higher levels of spam in both email and applications. To address the resulting security risks, bug bounty programs will be essential for identifying vulnerabilities that threat actors could exploit to scrape sensitive data.

On the flip side, AI can also be used to enhance defense tools, to detect deception. As Holt suggests:

"Defense tools may more easily identify trends in behaviour (e.g., through log analysis) because they are better at pattern recognition, even when not presented with the exact pattern to look for. And insider threats may become easier to find and stop. More efficient models can be trained to run faster on the same systems, which will see older systems effectively speed up and combat the tech-debt/ decay that typically occurs."

CHRIS HOLT
STRATEGIC ENGAGEMENT & COMMUNITY ARCHITECT
İNTİGRİTİ

26 • jumio.com/2025-identity-study/

Identifying AI-driven deception with Bug Bounty hunting

Bug bounty researchers can combat AI-related fraud by finding ways criminals can manipulate models, such as data extraction, safety bypass, evasion of AI-driven verification tools, for instance, and test for elements such as deepfake detection, to identify elements of misuse, impersonation, automation, to forge or generate scams. You can take a look at Intigriti's own ID Verification process here[27].

AI automated search has also meant changes in the way marketing teams promote services and solutions, the way sales teams approach audiences, and the way companies view their data.

"I think that there is going to be a shift in how companies view their intellectual property. Even when it comes to something simple like putting a question into Google, AI research displays the results right away, so company websites also lose out on ad revenue. Nobody visits these websites right away anymore. This means that there is going to be a defense-in-depth mechanism to combat the autonomous use of the website in the form of anti-scraping measures, legal restrictions, and licensing models."

INTI DE CEUKELAIRE
CHIEF HACKER OFFICER
INTIGRITI

Used individually, VDP, Bug Bounty, and Penetration Testing as a Service (PTaaS) provide value. Used together, they provide defense in depth: VDP for broad visibility, Bug Bounty for targeted depth, and PTaaS for structured assurance. A layered approach[28] gives wider coverage, deeper testing, and stronger control, protecting business against both common and advanced threats.

27 • kb.intigriti.com/en/articles/5378971-id-verification-process

28 • intigriti.com/blog/business-insights/layered-security-in-action-how-vdp-bug-bounty-and-ptaas-combine-to-protect-your-b

Six top tips for researchers and companies in 2026

For researchers

1

Pay attention to AI and LLM advancements

As noted in forecasts four and five, emerging vulnerabilities in Large Language Models (LLMs) and the rise of AI-generated slop represent new, high-value areas for discovery. Explore elements such as prompt injection attacks, model exploitation, and misuse scenarios. Also, stay up to date on using tools to detect AI-generated content.

2

Hone skills regarding multi-layered identity

As noted in forecasts two and six, supply chain weaknesses are on the rise. Test multilayered authentication systems (within scope), for bypass potential, and map dependencies in software/cloud ecosystems for weaknesses.

3

Engage with crowdsourced and government-sponsored initiatives

Governments are boosting cybersecurity budgets and leveraging crowdsourced talent, creating more opportunities for researchers. Participate in officially sanctioned programs and government-led initiatives and stay active in community knowledge-sharing, as these networks will be essential for high-impact discoveries.

Top Intigriti tip for researchers: Improve your reporting!

"In the current landscape, clear and well-structured reporting is a highly valued skill, and is essential for shared understanding between businesses and researchers alike."

LENNAERT OUDSHOORN
HEAD OF TRIAGE
INTIGRITI

Here are eight top tips for writing great reports.[29]

29 • intigriti.com/researchers/blog/hacking-tools/writing-effective-bug-bounty-reports

For companies

Companies should anticipate AI-related threats, fortify their supply chains, and upgrade identity security to stay resilient in 2026.

1

Strengthen supply chain and third-party risk management

Forecast two shows that supply chain risks are on the rise, which historically have been a major vector for large-scale breaches. Map and continuously monitor critical suppliers for compliance. Integrate contractual security obligations and conduct independent audits.

2

Adopt multi-layered identity and verification systems

Forecasts three and six show that identity deception is growing. Multi-factor and verification can reduce fraud and unauthorized access. Consider participating in collaborative crowdsourced security programs to spot threats early.

3

Prioritize a proactive, AI-aware strategy

Forecasts one, four, and five all highlight the rapid growth of cyber security threats, including LLM vulnerabilities, AI-generated slop, and logic issues. Invest in AI-driven threat detection via your bug bounty team to conduct simulated attacks, and train staff to recognise AI-generated social engineering attempts.

Contact us

If you have a question regarding any of the points made in this report, contact the team today[30]

30 • intigriti.com/contact

About Intigriti

Global crowdsourced security provider trusted by the world's largest organizations

Intigriti's bug bounty platform provides continuous, real-world security testing to help companies protect their assets and their brand. Our community of ethical hackers challenge our customers' security against realistic threats: we test in precisely the same way malicious hackers do.

How vulnerability management works with Intigriti

1. Researcher tests and searches for a vulnerability
2. Researcher submits a report via Intigriti
3. Intigriti's triage begins communication with researcher
4. Intigriti's triage team applies quality assurance steps
5. In-scope, unique and well-written reports are submitted to client
6. Client accepts report, and payment is automatically processed

125.000+ researchers

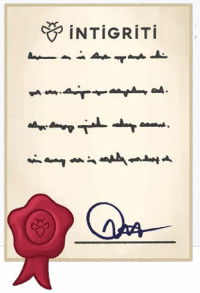
More than 125.000 security researchers use Intigriti to hunt for bugs — and we're growing!

400+ live bug bounty programs

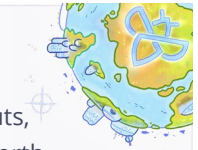
Companies of all sizes, and across multiple industries, trust Intigriti to launch their bug bounty program.

GDPR compliant

We ensure compliance with the highest security and data security standards.



Strong global presence



Intigriti has a strong global presence. In terms of hacker pay-outs, the 10 best performing countries are globally represented in North America, Europe and Asia. In 2025, vulnerabilities were submitted from more than 180 countries.

A vulnerability reported and fixed is one less opportunity for a cybercriminal to exploit. Ready to talk about launching your first bug bounty program? We're here to help you launch successfully.

FOLLOW US

REQUEST A DEMO
intigriti.com/demo

VISIT THE WEBSITE
intigriti.com

GET IN TOUCH
hello@intigriti.com

YOU'RE IN GOOD COMPANY

Dropbox · Coca-Cola · Nestlé · Personio · NVIDIA · intel · Red Bull · Microsoft · UBISOFT · monzo