INTIGRITI

BEAT APTs TO THE BREACH

A guide to scaling vulnerability discovery across your attack surface with bug bounty

Continuous, real-world threat simulation by motivated ethical hackers

EBOOK

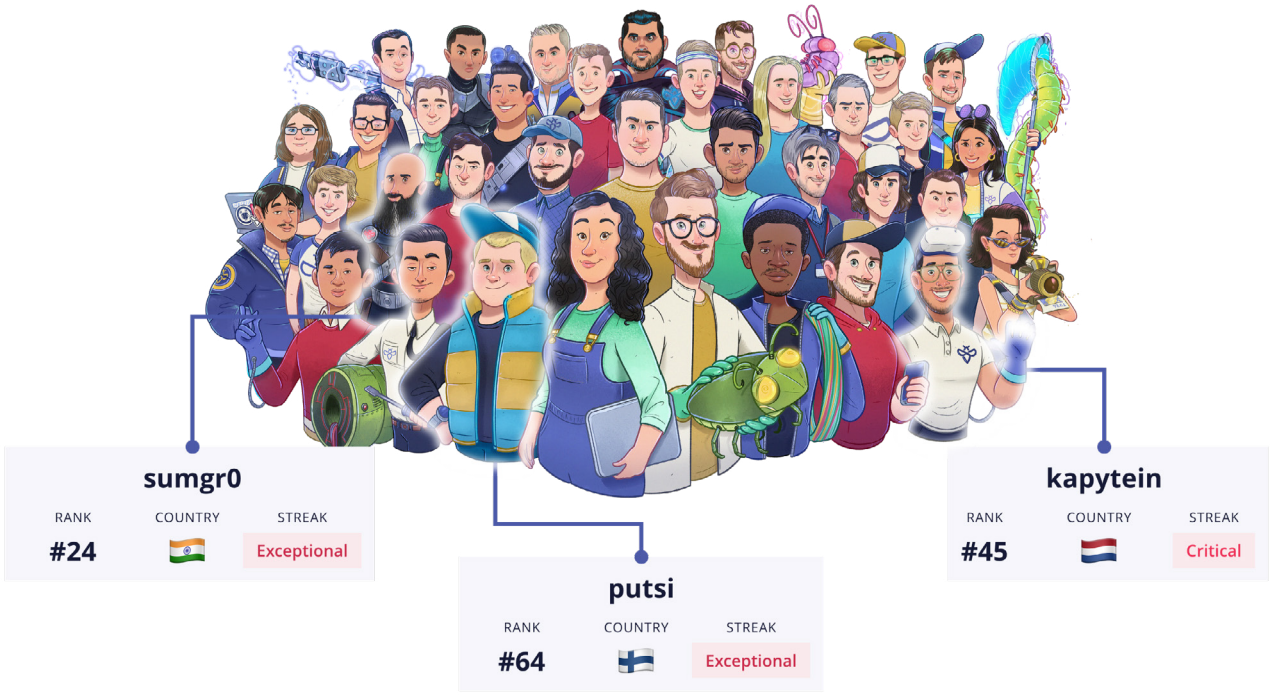
Table of contents

Introduction

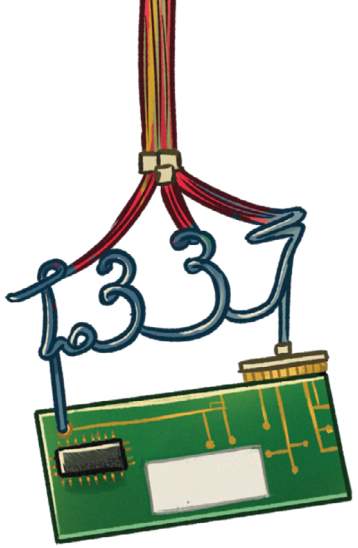
The cybersecurity landscape is undergoing a dramatic transformation, influenced by rapidly evolving technologies and increasingly sophisticated threat actors. In 2025, the importance of robust cyber defense mechanisms has never been more pronounced.

Organizations face numerous challenges, most notably the understanding that no one is completely immune to cyberattacks. Cybercriminals have adapted their tactics and strategies to exploit vulnerabilities in organizational infrastructures, emphasizing the need for continuous adaptation and robust security measures.

This report synthesizes insights from various perspectives on the cyber threat landscape, examining current trends, the expanding attack surface, and the role of bug bounty programs in enhancing security. By leveraging the skills of ethical hackers, organizations can better mitigate risks and optimize their defenses against a diverse range of threats.



Understanding the current cyber threat landscape



Key cyber threats

Cybersecurity professionals are operating in a dynamic environment shaped by ever-evolving threats. Noteworthy trends include:

Ransomware

This major threat has escalated, with attackers forming partnerships to enhance their capabilities. A recent report from ENISA indicates that 60% of organizations affected by ransomware have made ransom payments. The potency of ransomware attacks is bolstered by the speed at which attackers can exploit vulnerabilities and the complexity of the malware used.

Malware

In 2023 alone, there were 97 zero-day vulnerabilities exploited, illustrating the rapid pace of malware development. Zero-day vulnerabilities are particularly dangerous as they are unknown to developers and unpatched, offering attackers critical openings.

Social engineering

Attackers have refined their tactics to exploit human vulnerabilities. Sophisticated social engineering strategies make it increasingly difficult for victims and security systems to recognize manipulation.

Threats to availability

Disruptions to services, especially through Denial of Service (DDoS) attacks, have become a significant concern, exemplified by the July 2022 DDoS attack that targeted critical infrastructure in Europe.

These threats are compounded by the use of emerging technologies, such as artificial intelligence (AI), which can serve both defensive and offensive purposes. AI's potential for malicious use, including the development of harmful language models, represents a new frontier in cybersecurity threats.

Evolving attack techniques and tactics

Today's cybercriminals employ advanced strategies that continuously evolve, making it crucial for organizations to stay alert and adaptive. Key tactics include:

Supply chain compromise

Attacks through third-party vendors present unique challenges, as seen in high-profile breaches where trusted partners have been exploited to infiltrate larger networks.

Exploiting zero-day vulnerabilities

Attackers can operationalize these unknown exploits rapidly, necessitating real-time response measures from organizations.

Ransomware-as-a-Service (RaaS)

This model enables less skilled actors to execute sophisticated ransomware attacks by providing access to pre-made tools, thereby increasing the volume and variety of attacks.

Advanced social engineering

Attackers now use tactics like voice phishing and business email compromise, leveraging deep insights into their targets' behaviors and relationships.

Expanding attack surface

The challenges of modern technology

The rapid proliferation of new technologies has significantly broadened the attack surface organizations must protect:

IoT devices

The use of Internet of Things (IoT) devices has surged, introducing new vulnerabilities. Many IoT devices lack fundamental security measures, making them prime targets for attackers. For example, botnet attacks that exploit insecure IoT devices can disrupt services or infiltrate corporate networks as seen in the 2016 Mirai botnet attack.

Cloud and hybrid environments

While cloud computing and hybrid environments offer flexibility and cost savings, they also introduce challenges related to misconfigured settings and weak access controls. High-profile incidents, such as the Capital One data breach in 2019, highlight the risks associated with improperly secured cloud infrastructure.

Remote work and mobile devices

The rise of remote work has further decentralized corporate security. Employees working from home often rely on less secure networks, making them susceptible to targeted phishing attacks mimicking IT staff. Organizations must reinforce security policies that protect remote workers while ensuring robust cybersecurity practices.

RESEARCHER
tamaytandiran

Building a proactive cybersecurity strategy

In light of the evolving threats and expanding attack surface, a proactive approach to cybersecurity is essential.

Strategies to enhance cybersecurity

Organizations need to adopt comprehensive cybersecurity strategies that encompass:

- **Continuous risk assessment:** Regularly identify and evaluate potential threats and vulnerabilities within the organization.
- **Robust security policies:** Establish clear guidelines for cybersecurity practices and incident response protocols.
- **Layered security controls:** Implement a diverse range of technical and administrative controls to safeguard systems and data.
- **Incident response planning:** Develop and test incident response plans to minimize damage when security breaches occur.

Components of a cybersecurity strategy

Utilizing established cybersecurity frameworks, such as NIST and ISO 27001, can provide structured guidance for building a robust security program. Key components of an effective strategy include:

- **Threat Intelligence:** Leverage threat intelligence services to stay informed about new vulnerabilities and emerging threats.
- **Employee training:** Regular training programs to enhance awareness of cybersecurity best practices.
- **Adoption of the zero trust model:** Assume that all users and devices accessing the network could be threats, and verify their identity continuously.

The role of bug bounty programs in modern security

As traditional cybersecurity measures face challenges in keeping pace with evolving threats, bug bounty programs have emerged as a vital strategy for enhancing organizational security.

Importance of bug bounty programs

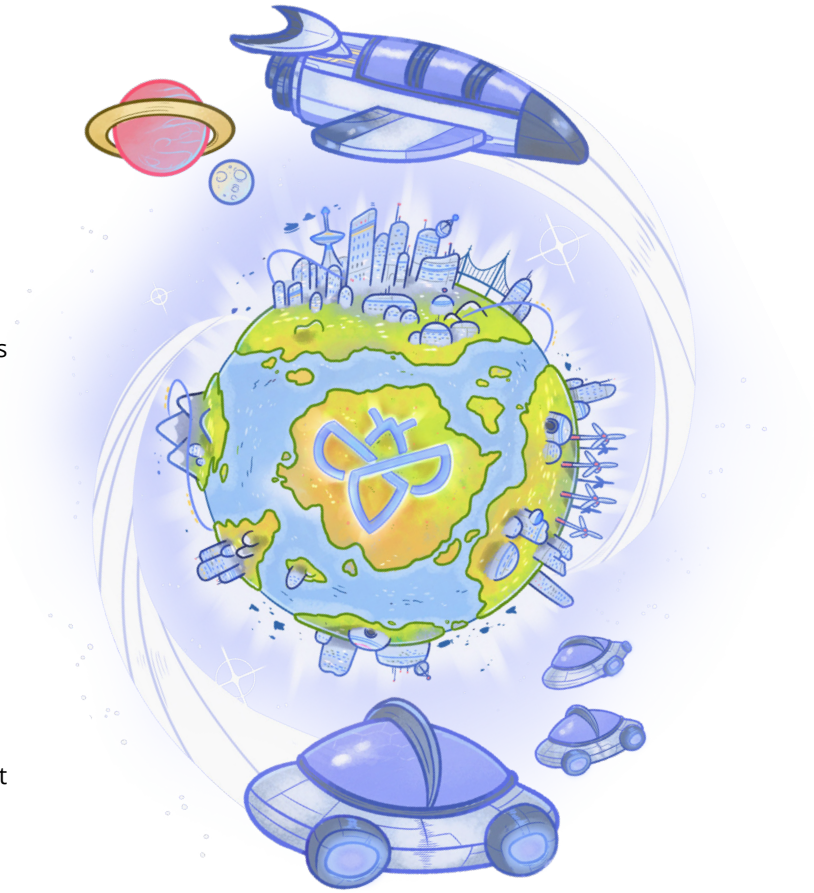
Bug bounty programs tap into the skills of a global community of ethical hackers, providing several advantages:

- **Ongoing cybersecurity testing:** Organizations benefit from continuous vulnerability identification and remediation through real-time testing.
- **Diverse perspectives:** The collective experience of a diverse group of security researchers can uncover vulnerabilities that internal teams often overlook.
- **Encouraging knowledge sharing:** Bug bounty platforms foster collaborative interactions among researchers and organizations, leading to improved security practices.

How bug bounty programs mitigate risks

Bug bounty programs effectively address various cyber threats:

- **Identifying vulnerabilities:** Ethical hackers actively search for weaknesses that cybercriminals might exploit, allowing organizations to patch these vulnerabilities proactively.
- **Simulating real-World attacks:** The tactics used by bug bounty hunters closely resemble those of real attackers, providing organizations with a clearer picture of potential vulnerabilities.
- **Fostering quick recovery:** By continuously monitoring for vulnerabilities, organizations can respond to threats in real time, improving incident response and minimizing damage.



Cyber threat actors and their motivations

To effectively combat cyber threats, organizations must understand the diverse motivations and techniques of their adversaries.

Types of cyber threat actors

Cyber threat actors range from amateur hackers to highly skilled, state-sponsored groups:

- **Script kiddies:** Typically less skilled, they use pre-packaged tools to exploit known vulnerabilities, often targeting low-hanging fruit.
- **Insiders:** Threats can arise from individuals with legitimate access to information who may misuse this access, whether maliciously or through negligence.
- **Hacktivists:** Motivated by ideological beliefs, these attackers often target organizations perceived as unethical or oppressive, using tactics such as data leaks or DDoS attacks.
- **Cybercriminals:** Primarily profit-driven, cybercriminals employ methods like ransomware and data exfiltration, frequently targeting small to medium-sized businesses.
- **Advanced persistent threats (APTs):** These state-sponsored groups engage in long-term, strategic intrusions aiming for espionage or sabotage.

How bug bounty programs counteract threats

Bug bounty programs can effectively counteract the strategies employed by different threat actors:

- **Script kiddies:** Researcher-led programs identify and remediate known vulnerabilities quickly, reducing opportunities for opportunistic attacks.
- **Insiders:** Bug bounty initiatives can help detect misconfigurations and weak access controls that could be exploited.
- **Hacktivists and cybercriminals:** Proactively identifying weaknesses in applications and networks reduces the risk of successful attacks.
- **Advanced persistent threats (APTs):** A robust bug bounty program can serve as an ongoing initiative to expose vulnerabilities that advanced attackers might exploit.

The future of cybersecurity

As technology continues to advance, cybersecurity will increasingly intertwine with emerging innovations.

Emerging technologies and security implications

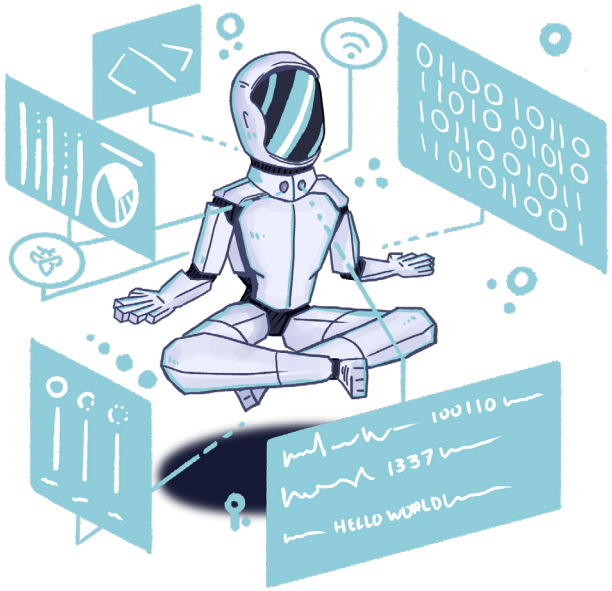
Emerging technologies, including AI, blockchain, and quantum computing, offer both opportunities and challenges in cybersecurity. Organizations must be wary of:

- **AI:** While it enhances threat detection, AI can also enable new forms of automation for cyber threats, such as sophisticated phishing attacks.
- **IoT devices:** The growing number of IoT devices expands the attack surface, necessitating robust security measures for operational technology.
- **Quantum computing:** Although still developing, quantum computing poses potential risks to current encryption methods, requiring future-proofing strategies.

Preparing for future threats

Organizations must adopt a forward-thinking approach to cybersecurity:

- **Continuous learning:** Stay informed about emerging threats, vulnerabilities, and mitigation strategies.
- **Invest in advanced security technologies:** Leverage innovations in AI and machine learning for predictive security capabilities.
- **Build resilient architectures:** Ensure that organizations are prepared for evolving attack vectors by implementing robust defenses against future threats.



Conclusion

The cyber threat landscape is complex and continually evolving, with new challenges arising daily. Organizations must adopt a proactive approach to cybersecurity that incorporates comprehensive strategies, including bug bounty programs, to effectively defend against an array of threats.

Investing in bug bounty programs allows organizations to harness the creativity and expertise of ethical hackers to uncover hidden vulnerabilities and strengthen their defenses. By proactively identifying and addressing potential threats, organizations enhance their resilience and safeguard their operations in an increasingly interconnected world.

If your organization is ready to enhance its cybersecurity posture through comprehensive strategies, including a bug bounty program, contact us today to learn more about how we can help you navigate the complexities of the cyber threat landscape.

About Intigriti

Intigriti is a rapidly growing cybersecurity company that specializes in crowdsourced security services to help organizations protect themselves from cybercrime.

Founded in 2016, Intigriti now has a global team of 100+ employees spread across Belgium, the United Kingdom, the Netherlands, and South Africa.

Information from Q1/2025. We are constantly growing, so please contact our sales department or see our website for an accurate number.

What to expect as an Intigriti customer

Conquer the limitations of traditional security testing

Continuously test your digital assets for vulnerabilities by leveraging the expertise of Intigriti's 125,000+ registered security researchers.

Industry-leading support

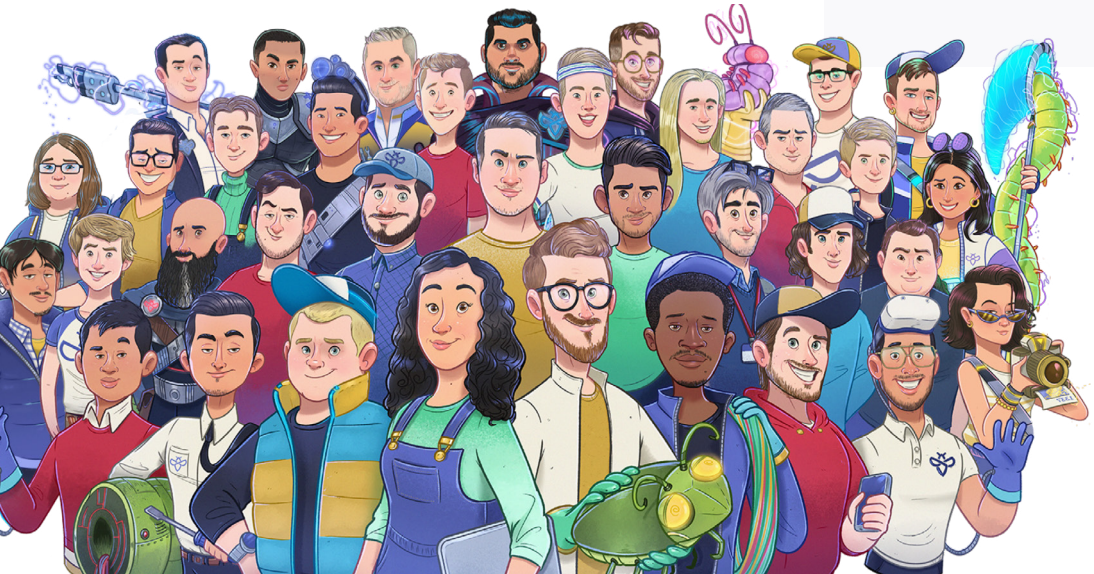
Receive only unknown, unique, valid, and in-scope vulnerabilities through our "pay for impact" model—only pay for valid vulnerability submissions. Our expert triage team rigorously evaluates every report before sharing it, allowing your team to focus on critical tasks. Comprehensive support includes triage, account management, customer success, technical support, and more.

Reduced risk

On average, Intigriti clients receive 53 vulnerability reports within one week of launching a bug bounty program through our platform. Intigriti's support empowers organizations to identify and remediate risks quickly.

Customized pricing

We provide a scalable model that aligns with customer aspirations and program expansion. Clients of all sizes and from various business sectors use our services.



Trusted by the world's largest organizations

Microsoft intel VISMA Red Bull

Nestlé UBISOFT Coca-Cola

Contact us

Need some help getting started with ethical hackers?
Our experts can help you maximize the success of your bug bounty program. Get in touch today to connect with the brightest and most experienced researchers across the globe.

www.intigriti.com

hello@intigriti.com

Intigriti hackwithintigriti @intigriti Intigriti Intigriti