



INTIGRITI

Program types

Vulnerability Disclosure Programs (VDP) & bug bounty programs



intigriti.com



Vulnerability Disclosure programs (VDP) & bug bounty programs

Creating a stress-free and sensical way for ethical hackers to disclose security vulnerabilities to you is critical. Intigriti offers both VDP and bug bounty program disclosure routes through the platform. Below, you can understand the similarities and differences between them.

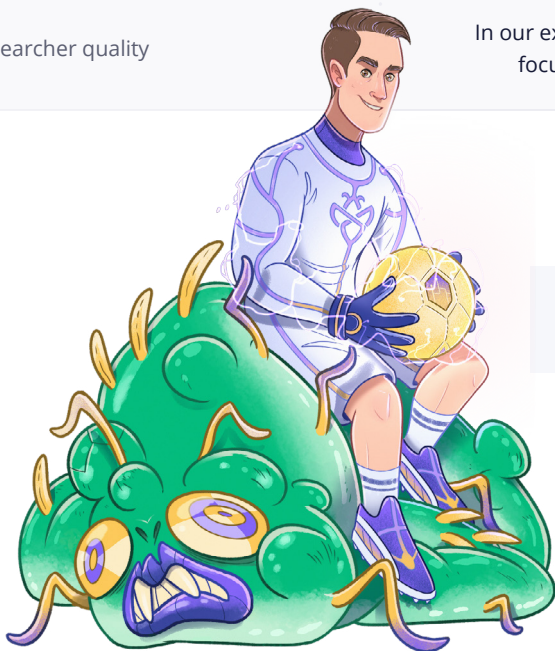
	VDP	Bug bounty
Compliance	Meets industry standards Supports ISO/IEC 29147:2018	
Legal considerations	Provides a legal framework Companies provide contributors with assurance that no legal action will be taken against them provided reports are made in good faith.	
Vulnerability management	Track submissions in real-time Companies can streamline the vulnerability disclosure process and keep track of submission security statuses in real-time, allowing them to obtain an accurate view of their security posture at all times.	
Communication	Centralised within the platform No need for sharing encrypted mails, the platform will allow communication in a safe and reliable way.	
Search culture	Say something, see something Allows people to report security issues when they notice them, without being afraid of legal repercussions.	Actively search & find something Security researchers are continuously activated through bounties, without being afraid of legal repercussions.
Reward system	No promises There is no promise for a reward, but a thank you is appreciated.	Rewarded for results Enables continuous security testing by incentivising the community through bounties. The size of the reward depends on impact (severity).
Researcher quality	A diverse community of security enthusiasts In our experience, beginner to intermediate security researchers tend to focus on VDPs, whereas bug bounties attract more experienced hacking talent.	
Quality assurance	Handled by Intigriti Intigriti's triage team provides a layer of quality assurance before escalating vulnerabilities to businesses. This means your security team only receives reports that are valid, unique, and in scope.	





Vulnerability Disclosure Programs (VDP) & bug bounty programs

Feature	VDP	Bug bounty
Supports ISO/IEC 29147:2018	✓	✓
Builds legal framework	✓	✓
Real-time vulnerability management overview	✓	✓
Centralised communication	✗ VDP follows a “see something, say something” culture	✓ Security researchers actively look for vulnerabilities
Active searching	✗ A “thank you” is appreciated	✓ Security researchers are rewarded or given a bounty for successful reports
Monetary incentive	✓	✓
Triaging service	✓	✓
Researcher quality	In our experience, beginner to intermediate security researchers tend to focus on VDPs, whereas bug bounties attract more experienced	



RESEARCHER
hack3r





About Intigriti

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

Intigriti's bug bounty platform provides continuous, realistic 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.



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 America, Europe and Asia.

In 2024, vulnerabilities were submitted from more than 180 countries.

TAKE YOUR FIRST STEPS

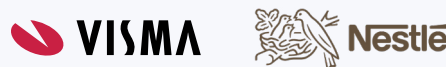
-  Request a demo www.intigriti.com/demo
-  Visit the website www.intigriti.com
-  Get in touch hello@intigriti.com



How vulnerability management works on Intigriti



You're in good company



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.

Speak to our team today.