VULNERABILITY DISCLOSURE PROGRAMS

FROM LUXURY TO NECESSITY

87% of organizations have discovered at least one critical vulnerability through a VDP!

VS

CONSEQUENCES OF *NOT* HAVING A VDP

Unknown Vulnerabilities

Leaves org insecure, while the total number of security issues growing over time

Security Breach Risk

High reputational damage and financial repercussions

Researchers Unable to Report Findings

Vulnerabilities may be disclosed publicly via social media or other channels before remediation

No Secure Process

No secure environment or organized process for submission and acceptance of prioritized vulnerabilities

Potential Noncompliance

Inability to meet compliance requirements or government directives

Loss of Confidence

Customers/citizens and other stakeholders lose confidence after a breach

A VDP MANAGED BY BUGCROWD

Reduce Risk

Securely accept, triage, and rapidly remediate valid vulnerabilities submitted from the security community

Improve Security ROI

Visualize and prioritize your entire threat landscape, so you can stay ahead of cyber attacks

Accelerate Digital Transformation

Digitize workflows and align security testing with your release cycle so you can ship secure code faster

Drive Better Decisions

Deliver context for risks and systems on your entire internet footprint with actionable intelligence for risk management

Increase Transparency

Demonstrate transparency to the security community and improve customer confidence

Gain Confidence

Identify vulnerabilities while building a stronger security brand

bugcrowd

Organizations of all kinds have transformed their approach to security using Bugcrowd VDP. Get the scoop in The Ultimate Guide to Vulnerability Disclosure