WIZ + hackerone

Executive Summary of the Integration

The Wiz and HackerOne integration brings proven, exploitable findings from penetration tests, bug bounty, vulnerability disclosure, and AI red teaming programs directly into Wiz as Attack Surface findings, each carrying severity, proof of concept, and remediation guidance. Findings are automatically mapped on the Security Graph to the underlying cloud infrastructure, identities, and data flows, revealing the full blast radius. As a result, security teams have an extended view into the impact of risks, helping them better prioritize and remediate.

Market Challenge

Penetration test and bug bounty findings often live in isolation, disconnected from the cloud environments they impact. Without visibility into the underlying infrastructure, identities, and data flows behind an exploitable finding, security teams struggle to assess its true blast radius and prioritize accordingly. Findings get handed off to development teams and quickly buried in backlogs as feature work takes priority, leaving proven, exploitable risk exposed and remediation stalled.

Benefits of the integration

- **Full Blast Radius Visibility:** HackerOne findings, including severity, proof of concept, and remediation guidance, flow into Wiz and are automatically mapped on the Security Graph to the underlying infrastructure, identities, and data flows, revealing the true impact of each exploitable finding.
- **Accelerated Remediation:** Security teams can prioritize risk based on cloud context and route findings to the right owners within Wiz, closing the gap between discovery and fix.
- **Seamless Workflow Integration:** Researchers and program managers continue working in HackerOne while the broader security organization drives remediation in Wiz, no context switching or duplicate effort.

The “better together” story

HackerOne delivers proven exploitability from skilled security researchers who test like real attackers. Wiz delivers deep visibility into the cloud environments that those findings impact. Together, they connect what's exploitable with what's at risk, giving security teams the context to act decisively. Findings are no longer isolated reports—they're mapped to the infrastructure, identities, and data that reveal the full blast radius, so teams prioritize based on real impact, not guesswork.

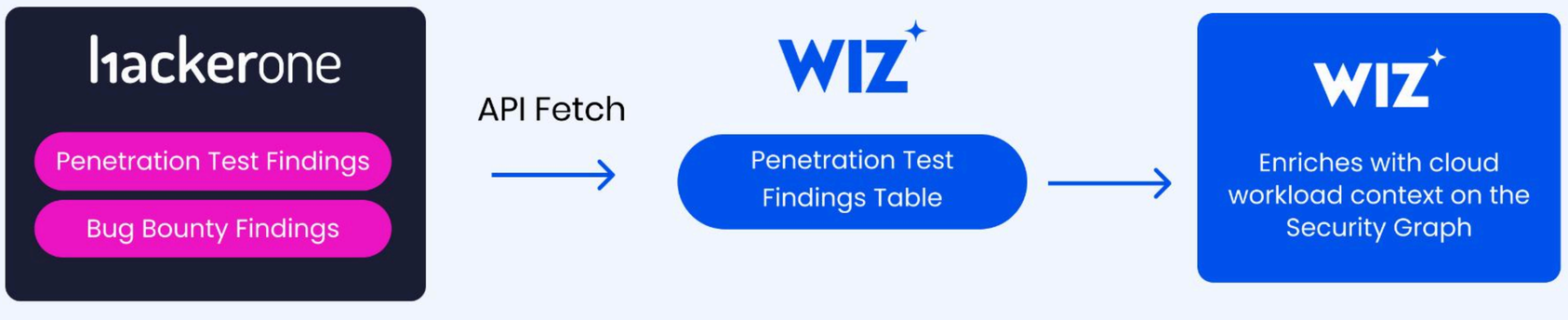
Use Case Overview

Use case: Tracing a Critical Finding from Bug Bounty Report to Cloud Blast Radius
A security researcher participating in a bug bounty program discovers unauthenticated access to an admin password reset endpoint in a customer-facing web application. The finding is validated in HackerOne with a proof of concept showing the attacker can reset admin credentials without authentication and gain full administrative access.

Challenge: The security team knows the vulnerability is exploitable—but the web application runs across multiple cloud environments. Which cloud accounts host the affected infrastructure? What data stores does the application connect to? What could an attacker with admin access reach beyond the application itself? The pen test report alone doesn't answer these questions, and manually tracing the path across cloud environments takes days.

Solution: The finding flows from HackerOne into Wiz as an Attack Surface finding. The associated host is automatically mapped on the Security Graph, immediately showing the security team that the vulnerable application runs on an EC2 instance connected to an RDS database containing customer records, with an attached IAM role that can access secrets in AWS Secrets Manager.

With the full picture quickly visible in Wiz, the security team can prioritize based on real impact and drive remediation with the right context: the exploitable entry point, the level of access gained, and the sensitive data at risk. What started as a single bug bounty report becomes a prioritized, contextualized remediation effort rather than another item lost in a backlog.



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 50% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.

About HackerOne

HackerOne is a leader in Continuous Threat Exposure Management (CTEM), combining AI-powered security solutions with the world's largest community of security researchers to help organizations identify and remediate vulnerabilities across code, cloud, and AI systems. Trusted by organizations including Goldman Sachs, Uber, and the U.S. Department of Defense, HackerOne helps enterprises continuously reduce cyber risk.