# How Hacker-Powered Security Can Help Security Teams Become More Data-Driven

Jobert Abma (ghostwriter, Jenny Kanevsky)
Co-founder, Distinguished Engineer
September 14th, 2021

SHARE

As organizations face an evolving digital ecosystem, migrate to cloud environments, speed up development cycles, and normalize remote work business models, cybercriminals find new and creative ways to exploit these expanded attack surfaces. In 2020, the COVID-19 pandemic and rapid digital transformation—ready or not—meant

security teams faced significant strain on systems, often unprepared for these new challenges. At the same time, global cyberattacks grew exponentially. Not only did numbers increase, but so did types of attacks. How can security teams adjust?

**Challenges for Traditional Security Teams**

Traditional security teams are typically reactive. They're seen as change-resistant, out of sync with development, and unable to predict or understand risk. For teams to go from reacting to cyberattacks to strategically and tactically planning for risk reduction, they need to plan and prioritize. However, this is difficult because they lack the data insight to predict risk origin or risk importance.

A lack of alignment between security and development causes security issues. Security teams running traditional, annual pentests will be out of sync with development's rapid pace, which includes frequent, sometimes daily, patches, updates, and releases. As a result, security initiatives won't match current products, leaving the organization vulnerable. Security teams will lag behind a fast-paced development team without continuous monitoring, measuring, and iterating.

Today's security teams need data, insights, and industry trend input to inform planning, risk management, and decision-making.

They also need an understanding of emerging attack surfaces and new threats.

**Emerging Attack Surfaces and New Cyber Threats**

Cyberattacks continue to rise while traditional security teams struggle to keep pace with a changing digital landscape. According to Verizon's 2020 Data Breach Investigations Report, 43% of breaches involved web applications, and malicious hacking was the most common entry point for all breaches. HackerOne's data reports similar results from our database of 300,000 vulnerabilities. More importantly, the HackerOne hacker community found three new risk categories, including web application-related vulnerabilities:

- Remote access infrastructure
- Cloud migration
- Personal and office appliances

But what about additional risks? Every two minutes, our global ethical hacker community looks beyond traditional testing and web applications to find a new—often high-risk or critical—security vulnerability issue. These hackers, with significant expertise and specialized skills, can easily identify the exploitability of a given vulnerability and provide valuable feedback to improve vulnerability remediation process efficiency. In the first half of 2021, we saw an increase in the following

emerging categories, defined based on the number and severity of high and critical vulnerabilities discovered.

- **Privilege escalation vulnerabilities** - More system roles and an increased need for access lead to horizontal and vertical privilege escalation. Our data shows a 14% year-over-year increase in Common Vulnerability Scoring System (CVSS) industry-standard 8.0-10.0 vulnerabilities. (CVSS rates on a scale of 0.0-10.0, with 10.0 being the most critical.)
- **Improper authentication and access control**—The average asset has five improper authentication or access control vulnerabilities when first tested and after the first year, between one and two high or critical vulnerabilities, depending on the organization's security maturity. Last year, our hacker community reported an uptick of 20% per organizational asset.
- **Cloud misconfigurations—Vulnerabilities in this category tend to impact data confidentiality. Organizations store increasing amounts of data, and the number and variety of vulnerabilities reflect complex business needs. Our data reports that a 16% rise in cloud misconfigurations has led to organizational data leakage year over year**.

However, one of the biggest concerns is that time to remediation is slipping to an average of 3.1 days. This trend, combined with new vulnerabilities and emerging attack categories, increases security teams' pressure to keep pace with change. It's time for a new approach.

Today's security teams must become proactive and data-driven. First, they must mitigate risk by focusing on and driving down remediation time. Where traditional assessments and pentests give point-in-time reports, HackerOne Security Assessments deliver continuous testing, monitoring, and reporting. Access to this up-to-date information gives teams the insights and data points to plan and prioritize to reduce and prevent risk. In addition, forward-thinking organizations are adopting other security testing programs like bug bounties and Vulnerability Disclosure Programs (VDPs).

If you want to help your security team become more effective, proactive, and data-driven, empower them with the combination of threat category awareness, continuous insights, and feedback from internal testing and general industry trend data.

Working with HackerOne gives organizations access to a robust database, vulnerability trends, industry benchmarks, and the largest, most diverse hacker community in the world. Learn more here.