PRODUCT EBOOK

hackerone

The Role of Hackers in Security Assessments for Product Development

How hacker-driven security assessments can support product development and improve relationships between security and development teams.

For many organizations, quickly writing and shipping new code and features is essential to their businesses. However, securing new software at the current rate of delivery is a challenge. Traditional security practices slow down development, forcing developers to wait for security approval on code, often creating friction between the two functions.

This was less of a concern in the past because development released new code at a slower rate. Waiting weeks for penetration test results wasn't an issue when development teams only needed to release two to three software patches each year.

By contrast, some development teams work with a DevOps cycle of under 24 hours and frequently release substantial updates and new features throughout the year. Rapid deployment means adaptation to changing markets and greater efficiency at driving business results. A faster DevOps model can help organizations build a competitive advantage and better serve their customers, creating a security challenge.

Most traditional penetration test providers need weeks or months notice to arrange engagements, so penetration tests are seldom available on-demand. Instead, customers must book them significantly in advance, usually just once or twice per year. This approach doesn't fit most current development practices and often delays product and feature releases.

By rethinking the security assessment process, organizations can incorporate security into the development lifecycle and help development teams protect even the most aggressive roadmaps.

Results:

As a result, traditional penetration tests don't fit modern development practices and often lead to product and feature release delays. Rethinking the security assessment process incorporates security into the development lifecycle and helps development teams protect even the most aggressive roadmaps.

Lack of Alignment Between Security and Developers

Relations between security and development teams have often been difficult. For developers, security may be seen as a hindrance to development timelines. Meanwhile, security teams may feel as though developers aren't interested in security.

These challenges arise because security and development teams seem to have competing objectives:

- Developers want to meet their timelines and ship new features and fixes as quickly as possible.
- Security teams want to ensure live code is vulnerability-free, no matter how long that takes.

This conflict can lead to a breakdown in communication between the teams. Since fitting meaningful security controls into a rapid DevOps lifecycle is already a challenge, this can cause additional frustration and poor outcomes.

DevSecOps addresses this by integrating security practices into the DevOps cycle. By prompting developers to include security in their processes—and security teams to break away from traditional silos to support developers actively—DevSecOps incentivizes both teams to work together.

The diagram below demonstrates how different security practices fit into the DevSecOps lifecycle.

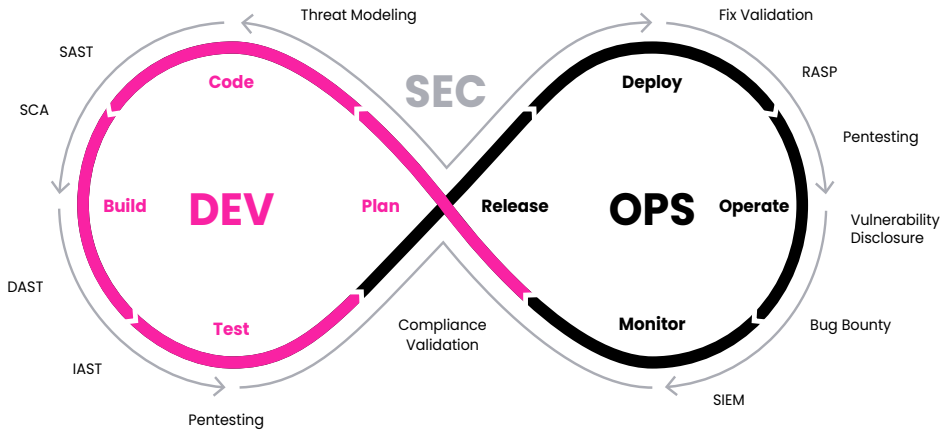

Figure 1: The DevSecOps lifecycle

Security Scanner Challenges

As DevSecOps has grown, static application security testing (SAST), dynamic application security testing (DAST), and interactive application security testing (IAST) tools have become integral to development programs. The speed of SAST tools and the real-time nature of IAST scanners allow them to fit directly into the lifecycle. DAST tools can take five to seven days to run, so they usually run alongside the DevSecOps cycle, providing feedback to improve future code releases.

Scanning tools provide security assurance and help mitigate the danger of basic vulnerabilities creeping into production environments.

However, scanning tools raise several concerns:

1. **They generate false positives.** SAST scanners, in particular, are known for providing high numbers of false positives and negatives. There's no way to know whether a result is a valid security issue or a false positive without a manual code review. Unfortunately, manual code reviews are time-consuming, putting pressure on developers. Investigating every result found in every iteration of the DevSecOps cycle is resource-intensive.

2. **They produce an overwhelming number of results.** False positives or not, SAST scanners (and DAST scanners to a lesser extent) often provide many results that lack context or prioritization. Again, time-consuming human intervention is needed to provide this crucial information.

3. **They run inside the development environment.** While scanners can effectively identify known technical vulnerabilities, they don't test new code in its final production environment. Even DAST scanners, which perform black-box testing against a compiled application, run inside the development environment. This lack of production testing presents a problem, as new security issues can quickly arise once code is released.

4. **They only find simple, technical security issues.** Combined, SAST, DAST, and IAST scanners effectively identify problems developers can solve with basic secure coding practices. Despite how good a development team is, these issues are inevitable, and scanners can help. However, no scanner can find more advanced issues like business logic abuse or multi-page sequence problems, which frequently arise in complex applications—and can be easy to exploit once code hits production

5. **Scanners lack speed.** For fast (five days or fewer) development cycles, DAST tools may not be quick enough for in-band testing. This forces development teams to rely on SAST and IAST tools, running the risk of vulnerabilities making it into production.

6. **They impact code performance.** While IAST tools come closest to providing a seamless source of vulnerabilities inside the DevSecOps cycle, they add to the instrumentation running inside the development environment. As with any other real-time tool, IAST scanners require additional resources and can affect code performance.

While scanning tools provide a measure of security assurance, they aren't sufficient to ensure new code is safe to deploy into a production environment.

Scanning Tools Raise Several Concerns:

1. **They generate false positives.**
2. **They produce an overwhelming number of results.**
3. **They run inside the development environment.**
4. **They only find simple, technical security issues.**
5. **Scanners lack speed.**
6. **They impact code performance.**

HackerOne Assessments:

HackerOne Assessments provide organizations with a single platform approach to security testing while still allowing them to benefit from the varied skills of a diverse pool of testers. This is one of the primary benefits of working with ethical hackers—the ability to work with the largest and most diverse global hacker community while retaining the business-oriented service of a traditional penetration test.

Improve Outcomes with Continuous Security Assessments

In addition to security scanners, many organizations use security assessments to identify software and other vulnerabilities. A security assessment is an in-depth study by a team of human testers, often hackers, to identify asset vulnerabilities. These assessments may take the form of a penetration test completed by an external service provider, which is usually designed to meet the requirements of one or more compliance frameworks.

Some organizations have treated security testing as an annual exercise as required by many compliance frameworks. Equally, security teams have often opted to switch vendors for each security assessment to expose software to various testing talent. While this reasoning is logical, the process makes it impossible to standardize testing and remediation, which is essential for rapid, consistent security outcomes.

Organizations should consider adopting a **continuous approach to security testing to resolve these issues.**

HackerOne Assessments gives organizations a single platform approach to security testing and the benefit of a diverse pool of testers. This is one of the primary advantages of working with the largest and most diverse global hacker community while retaining the business-oriented service of a traditional penetration test. All testing is completed in a staging environment, so there is no risk of disruption to live assets.

This approach provides seven key benefits:

1. **Diversity.** HackerOne Assessments provide access to a large community of background-checked hackers that can rotate across development projects. Unlike most security testing, this gives organizations the flexibility to expose assets to a range of testing talent with skills in various programming languages and operating systems all while keeping the business and process benefits of working with a single testing provider.
2. **Two-way communication.** The platform makes it easy for developers to communicate with security testers, ask questions, and seek to resolve reported vulnerabilities.
3. **Rapid reporting.** Rather than waiting weeks for results, developers receive new (and rigorously vetted) vulnerability reports as soon as the testing team finds them. Rapid reporting allows developers to investigate and resolve vulnerabilities immediately.
4. **Verification.** Unlike security scanners (and some penetration tests), assessments provide only vulnerabilities that have been replicated and verified by HackerOne. A false-positive rate of close to zero protects developers and security teams from wasting time and resources.
5. **Development roadmap support.** With such a vast pool of talent available, organizations can arrange assessments on demand whenever needed. This speed and flexibility are ideal for supporting rapid development roadmaps.
6. **Integration.** Like security scanners, HackerOne's platform integrates seamlessly with existing development workflows, including popular ticketing and incident management tools like GitHub, ServiceNow, and Jira. These integrations ensure every reported vulnerability goes directly to the right team, avoiding the risk of missed vulnerabilities and communication breakdowns.
7. **Instant retesting.** As soon as developers resolve a vulnerability, they can reach out in real-time to the testing team to ask for a retest ensuring it is thoroughly closed. This process can take weeks with a traditional penetration test

HackerOne Assessments:

1. **Diversity**
2. **Two-way reporting**
3. **Rapid reporting**
4. **Verification**
5. **Development roadmap support**
6. **Integration**
7. **Instant retesting**

The Process:

These process and outcome improvements help build better relationships between development and security teams and support a mutually beneficial outcome—improved product security.

Note:

For routine code updates, current DevOps cycles are extremely fast—sometimes under 24 hours per cycle. As a result, even the fastest human security testing doesn't fit inside the lifecycle. Instead, HackerOne Assessments sit alongside the lifecycle, providing vital vulnerability reports and intelligence that feed into future cycles, ensuring vulnerabilities are addressed earlier.

HackerOne Assessments provide the rapid vulnerability input needed to ensure each release is secure for larger code projects such as new products and features. In addition, DevOps cycles are typically much longer in these cases so that assessments fit directly inside the lifecycle.

Facilitating Communication Between Developers and Security

Competing objectives and poor testing outcomes lie at the heart of the conflict between developers and security teams. By providing a source of vetted and prioritized vulnerabilities, assessments support developers to ensure high product quality without overwhelming them with too many results or false positives.

These process and outcome improvements help build better relationships between development and security teams and support a mutually beneficial outcome—improved product security.

Supporting the DevSecOps Lifecycle

DevSecOps aims to integrate security into the development process to protect roadmaps while ensuring a higher security standard. HackerOne Assessments fit into DevSecOps by:

1. **Supporting development roadmaps for new products and features, which typically require rigorous human testing before release.** With traditional penetration tests, roadmaps are regularly delayed due to the challenge of arranging tests, slow provision of results, and difficulty communicating with testers after the engagement. As a result, a release can easily be delayed by weeks or months, particularly if the test reveals complex vulnerabilities that require back-and-forth communication between developers and testers.

   HackerOne can arrange assessments on-demand, provide development teams with immediate vulnerability reports, and support two-way communication and retesting throughout and following the engagement. This collaborative approach allows developers to benefit fully from each engagement in a far more condensed time frame.

2. **Helping development teams learn from each vulnerability and implementing controls to prevent the same issues from arising in future code.** Accessible two-way communication helps development teams gain a better understanding of each vulnerability. At the same time, the platform makes it easy to track the types of vulnerabilities found over time, so developers can see where primary issues lie. Then, using this information—along with the expertise of the testing team—earlier in the DevSecOps lifecycle, development teams can implement new controls to eliminate those vulnerability classes from future code.

3. **Helping ensure code releases are in line with business objectives.** Some forward-thinking development teams now consider vulnerabilities a quality issue and believe there is no point in shipping new code if it doesn't meet quality standards. By providing developers with comprehensive vulnerability reports, feedback, and ongoing discussion, HackerOne Assessments support developers in tackling security issues and ensuring new code releases are in line with quality standards.

   So, how does this translate in the real world?

   After working with customers from a wide range of industries, HackerOne saw how assessments could benefit organizations that rely on the speed and efficacy of their development roadmaps. Zebra Technologies came to HackerOne, let down by traditional security testing options, needing a faster, more collaborative alternative.

How Does this Translate in the Real World?

After working with customers from a wide range of industries, HackerOne saw how assessments could benefit organizations that rely on the speed and efficacy of their development roadmaps. Zebra Technologies came to HackerOne, let down by traditional security testing options, needing a faster, more collaborative alternative.

Better Together: HackerOne Assessments and Security Scanners

HackerOne Assessments are highly effective for supporting the DevSecOps lifecycle but don't have to be used in isolation. Throughout this guide, we have compared assessments to security scanners to illustrate their value. In practice, both are essential components of a healthy DevSecOps program.

For routine code updates, current development cycles are fast—sometimes under 24 hours per cycle. As a result, even the fastest human security testing doesn't fit inside the lifecycle. Instead, HackerOne Assessments sit alongside the lifecycle, providing vital vulnerability reports and intelligence that feed into future cycles, ensuring vulnerabilities are addressed earlier. Meanwhile, SAST and IAST scanners provide security feedback directly inside the DevSecOps cycle, identifying simple, resolvable issues before each release.

Development cycles are typically longer for larger code projects and new features. A full range of HackerOne Assessments, security scanners, and other testing can be run before release.

Zebra Technologies Case Study

How Zebra Technologies Ensures Secure-by-Design Product Development

Zebra Technologies builds enterprise-level data capture and automatic identification solutions that provide organizations with operational visibility. With over 10,000 partners across 100 countries, Zebra provides better visibility through industry-tailored, end-to-end solutions that intelligently connect people, assets, and data to help customers make business-critical decisions.

Zebra holds substantial quantities of sensitive information for its customers, so product security is essential to its business model. Security tests must help the company ensure secure-by-design product development while satisfying a host of compliance and internally mandated requirements.

In the past, Zebra relied on traditional penetration testing providers as its only source of external security validation. However, scheduling delays and lack of clarity into testing processes led the company to look elsewhere.

"To maximize the security of our products, we need to get testing into our development process as early as possible," explains Dr. Jasyn Voshell, Director of Product Security at Zebra Technologies. "With traditional penetration testing providers, we'd have to wait weeks to spin up an engagement live, so scheduling delays disrupt our release timelines."

The company also needed transparency in the testing process. Penetration testing providers often provide a black box service where customers have little visibility into testing methods and coverage. Looking for more flexibility and transparency, Zebra switched to HackerOne Assessments.

"To maximize the security of our products, we need to get testing into our development process as early as possible," explains Dr. Jasyn Voshell, Director of Product Security at Zebra Technologies. "With traditional penetration testing providers, we'd have to wait weeks to spin up an engagement. We have a requirement to test every product before it goes live, so scheduling delays disrupt our release timelines."

Dr. Jasyn Voshell
DIRECTOR OF PRODUCT SECURITY, ZEBRA TECHNOLOGIES

Zebra Technologies Case Study

ZEBRA

After standardizing all security testing into the HackerOne platform, the company can now schedule assessments faster and clarify the testing process.

"We can get a HackerOne Assessment up and running in five days, which is more in line with our product release timelines," continues Voshell. "The platform is great because we can communicate with testers during the engagement and even guide the testing in a specific direction. The process gives us more confidence that our products are being tested thoroughly."

The platform also gives developers real-time access to the testing team to ask questions about replicating issues and requesting instant retests for fixed vulnerabilities. This flexible approach to security testing makes HackerOne Assessments an ideal fit into Zebra's development processes.

Voshell explains:

"The top benefit for us is the speed of remediation. With other vendors, we couldn't even start to remediate until the end of each pentest. With HackerOne Assessments, we get vulnerability reports straight away, and we can request immediate retests for resolved issues. This allows us to fix issues much earlier in the development process and support our product release roadmaps in a way that wasn't possible in the past."

"We can get a HackerOne Assessment up and running in five days, which is more in line with our product release timelines," continues Voshell. "The platform is great because we can communicate with testers during the engagement and even guide the testing in a specific direction. The process gives us more confidence that our products are being tested thoroughly."

Dr. Jasyn Voshell
DIRECTOR OF PRODUCT SECURITY, ZEBRA TECHNOLOGIES

Protect Your Product Roadmaps with HackerOne

Launching products on time is a business imperative. However, traditional penetration tests don't provide the flexible and frequent testing needed to support today's development cycles. While product security is essential, it can't come at the expense of rapid-release roadmaps.

HackerOne Assessments can be tailored to meet specific requirements and support different stages of the development cycle. For example, HackerOne Application Pentest for AWS is a pentest engagement specifically for AWS customers, helping them understand and fix cloud vulnerabilities such as data leaks, subdomain takeovers, and unauthorized access. These engagements are conducted by AWS Certified hackers, who have the domain-specific expertise needed to uncover vulnerabilities in AWS applications, both live and in active development.

Assessments combine on-demand access to the world's largest and most diverse community of expert hackers with a platform that allows two-way communication, issue validation, and instant retesting. The platform integrates with existing workflows and incident management tools, ideal for feeding vulnerability reports into product development.

The diagram below shows where each HackerOne solution fits into the DevSecOps lifecycle.

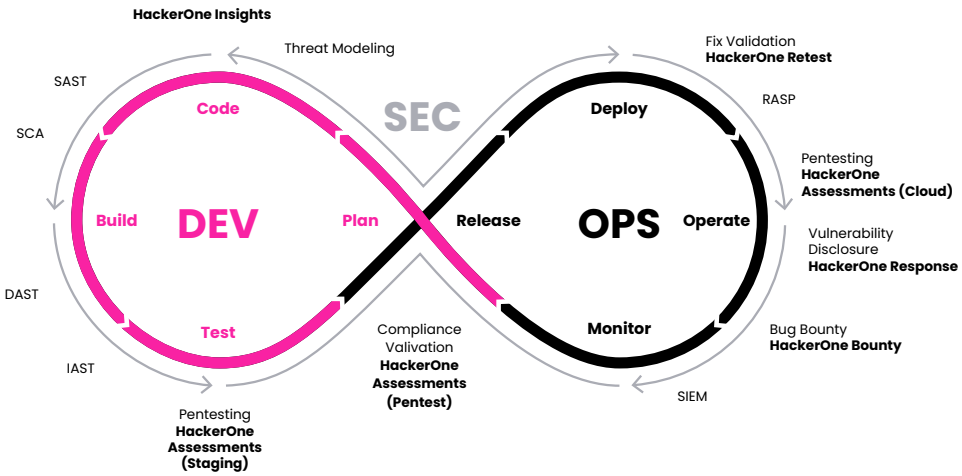

Figure 2: The HackerOne supported DevSecOps lifecycle

In addition to assessments, HackerOne provides a full range of testing solutions that support a true DevSecOps approach to product development. These include:

HackerOne Retest. All HackerOne solutions allow customers to instantly request retesting for patched vulnerabilities and enable easy two-way communication between developers and testers.

HackerOne Response. Invite the global hacker community to search for and report vulnerabilities in your assets via a Vulnerability Disclosure Program (VDP), and receive only validated, prioritized, and categorized vulnerabilities through a single platform.

HackerOne Bounty. Step up your response program by incentivizing hackers to help you find software weaknesses that elude conventional security tools and testing services. Manage your bug bounty program through the HackerOne platform and optionally allow us to manage the program for you.

HackerOne Insights. Build a better understanding of risk in your software by analyzing vulnerability trends in the largest dataset of exploitable vulnerabilities submitted by hackers and verified by HackerOne. Track program performance, prioritize vulnerabilities, and benchmark against industry peers.

Learn more about how HackerOne can improve your security, mitigate risk, and, with HackerOne Assessments, help your organization launch secure products without delaying release roadmaps. Contact us to learn more here.

hackerone

HackerOne has vetted hackers for hundreds of organizations including:




With over 2,000 customer programs, more companies trust HackerOne than any other vendor

Contact Us