bugcrowd

Six steps to building a resilient security posture

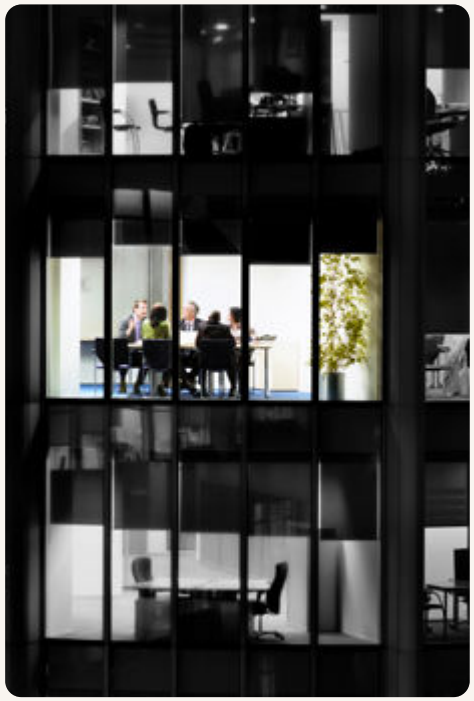
THE COMPLETE PROACTIVE SECURITY CHECKLIST

In 2024, Dropbox e-sign suffered a significant data breach that exposed millions of customers' information—including email addresses, phone numbers, hashed passwords, and MFA tokens. One concerning element of the breach was its scope: it impacted registered users *and* anyone who had received or signed a Dropbox document. The aftermath was a multimonth process, with teams working around the clock to coordinate with customers, regulators, and authorities.

This example underscores how digital-first SaaS and technology companies must remain vigilant against data breaches in today's complex threat landscape. Any technical disruption can be fatal to core operations or, worse, reduce customer trust and result in churn. These organizations must go beyond traditional security practices, like automated vulnerability scans, that only fix gaps after threat actors have exploited them.

Instead, technology and SaaS providers must embrace a proactive security model. In this model, organizations leverage practices like Managed Bug Bounty (MBB), Pen Testing as a Service (PTaaS), and Red Team as a Service (RTaaS) to ensure deep, continuous assessment of their entire technology stacks. These practices can pinpoint vulnerabilities that internal teams or standard tools might overlook. These practices can also help SaaS organizations reduce risk and more effectively meet compliance goals.

One of the most popular methods of guaranteeing proactive testing is crowdsourced security, where organizations partner with the ethical hacker community to identify critical vulnerabilities. Through this collaboration, SaaS and technology organizations can augment their security teams' capacities on demand while accessing specialized skills and diverse expertise. In this guide, we'll cover six best practices companies should follow when implementing proactive security testing, especially those centered on crowdsourced security.



1

Work with the right talent

To properly implement proactive security, you must build the right team that understands your goals and has the appropriate skills in your industry and target assets (e.g., LLM, cloud configurations, and applications). This can be a challenge for SaaS and technology organizations due to rapid growth bursts and an unrelenting pace of development. Recruiting and growing a security team to match this pace of growth is an impossible challenge.

Many organizations circumvent this issue by turning to crowdsourced security. This approach provides instant access to a large pool of external hackers, pentesters, and red team operators, offering thousands of extra eyes on your attack surface. Engaging with this community also helps organizations adopt an adversarial mindset—by thinking like threat actors, they find and fix critical vulnerabilities before attackers can exploit them.

For instance, consider cloud configuration security. As a first step, an internal team might assess your existing configurations against a list of known vulnerabilities, but this approach will miss emerging or novel vulnerabilities. Working with hackers can fill this gap and uncover new attack paths, resulting in more secure cloud systems.

The Bugcrowd Platform can help you draft the right team of hackers based on your unique use cases, timing, assets, and other requirements. Using the Platform, you can quickly increase your team's security capacity across various skill sets (API, IoT, AI, cloud configuration, etc.), enabling your security capabilities to scale alongside your product and company growth.

Crowdsourced security provides instant access to a large pool of external hackers, offering thousands of **extra eyes** on your attack surface.

2

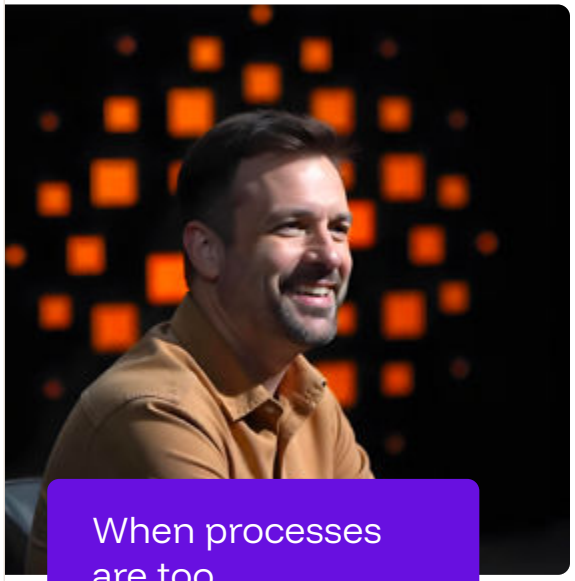
Streamline processes and aim for consistency

A key element of a successful proactive security program is standardized workflows, which ensures that the program produces reliable, consistent outcomes. Otherwise, you will waste time, get poor results, and struggle to scale your programs.

This is especially true in crowdsourced security, where clear processes are key to a healthy and productive partnership with hackers. Our annual hacker community survey showed that 58% of hackers hack to reduce risk for organizations—they're incredibly impact-oriented! To maximize hacker engagement, organizations should provide hackers and external testers with structured reporting and triage processes, consistent evaluation standards, straightforward submission procedures, and recognition for their contributions. When processes are too cumbersome or inconsistent, hackers disengage from a program. This results in lower-quality vulnerability reports and impairs your program's effectiveness.

Beyond vulnerability reporting, organizations should also streamline hacker vulnerability reports for DevOps teams to decrease time to remediation. We'll explore how to do this in a later tip.

The Bugcrowd Platform can help you implement efficient workflows that streamline program onboarding, promote communication between you and hackers, and expedite vulnerability submissions, triage, validation, and remediation. Through our structured submission form and our open-source Vulnerability Rating Taxonomy, organizations and hackers can efficiently share context and quickly address the most critical security issues. This approach delivers fast results. On average, Bugcrowd customers receive their first vulnerability within 7 days of launching their engagement.



When processes are too cumbersome or inconsistent, hackers disengage from a program, resulting in lower-quality vulnerability reports and compromising your program's **effectiveness.**

3

Consolidate vendors to bring efficiency at scale

SaaS and tech companies are constantly evolving—shipping new features, entering new markets, or iterating their business models. These shifts create ever-changing security requirements that complicate effective proactive security planning and implementation.

To address this challenge, it is important to consolidate security vendors rather than hire different specialists for each security initiative. This approach offers several advantages:

As you work consistently with a vendor, they'll develop a **deeper understanding** of your system architecture and business, enabling more relevant, tailored security solutions.

Save time

Teams don't need to spend months researching, evaluating, and onboarding new vendors; they can quickly spin up programs. Furthermore, using consistent communication channels and reporting formats streamlines program operations and saves time.

Personalized insights

As you work consistently with a vendor, they'll better understand your system architecture and business over time. This familiarity enables them to provide more relevant, tailored security insights and solutions.

Cost savings

Vendors typically offer discounts for multiple engagements, which can add up. Plus, you won't need to spend the time or money on onboarding and due diligence for different vendors.

By using a single vendor for crowdsourced security testing, organizations can easily increase capacity on demand and centralize operations. This helps them scale their security strategies efficiently as they grow.

Organizations can use the Bugcrowd Platform to launch and manage multiple crowdsourced security programs, including RTaaS, PTaaS, Vulnerability Disclosure Programs (VDPs), and MBB programs. For example, instead of hiring a separate consultant to pen test your cloud and LLMs, you can manage both through Bugcrowd. And, if you want to add LLM red teaming later, you can set this up on the same platform.

4

Don’t make triage and validation an afterthought

Separating genuine threats from false alarms is critical to successful and proactive security programs. Otherwise, you risk wasting company resources and missing critical vulnerabilities. That’s why effective validation and triage must be fundamental to your security program’s design.

Many crowdsourced security vendors attempt to address this problem by utilizing third parties to validate hacker submissions. However, this can result in inconsistent results or detrimentally leave reports untouched for days, which increases the risk of an attacker exploiting any vulnerabilities. To avoid this outcome, organizations must work with a platform that reduces bottlenecks in their triaging and validation processes by:

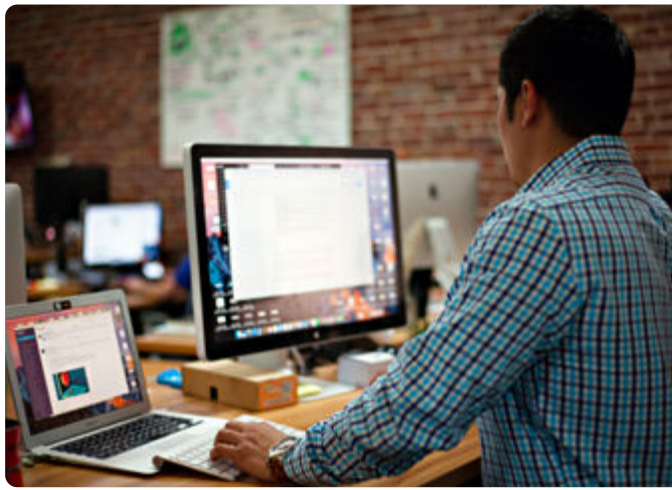
Meeting stringent Service Level Objectives more than 99% of the time

Employing in-house expertise across key parts of a technology stack

Adding critical context in each submission to reduce communication bottlenecks

The Bugcrowd Platform exemplifies this approach by treating validation and triage processes as a core priority, not an afterthought. Our global team of security engineers, with specialized expertise across mobile, AI, IoT, and other domains, enhances hacker submissions with crucial context, boosted by our massive security knowledge graph based on past experiences. We rapidly validate and prioritize vulnerabilities, handling the most important issues within hours, as demonstrated by how we meet our SLO more than 99% of the time.

Separating the signal from the noise isn’t straightforward—scanners are notoriously noisy, and triaging vulnerability reports requires **significant** time and skill.



5

Integrate with existing DevOps tools and processes

A good, proactive security strategy cannot exist in a vacuum—it must be part of a broader workflow that extends across DevOps tools and the software development life cycle (SDLC).

This is especially relevant for tech and SaaS organizations that frequently deploy new code, as each release introduces attack opportunities for threat actors to exploit. Over time, this transparency can help foster a more collaborative relationship between security and development teams, which leads to long-term security benefits like rooting out insecure coding practices.

Organizations don't have the resources, time, or incentives to build these integrations from scratch. That's why organizations must partner with vendors (especially for crowdsourced security) that have already built these integrations. At Bugcrowd, we have an end-to-end integration library featuring everything organizations need to quickly integrate platform workflows with existing DevOps tools and processes, including the following:

Integrating within a broader workflow that extends across DevOps tools and the SDLC is **crucial** for proactive security.

Event-based webhooks that enable event-based notifications with bidirectional functionality

A rich, easy-to-use API that provides many options for programmatic access to the Bugcrowd Platform, including version management

Prebuilt, easy-to-activate connectors for common security and DevOps tools like Jira, GitHub, ServiceNow, Qualys, Nucleus, and IBM Security

6

Leverage reporting and analytics for continuous improvement

When organizations don't have continuous insight into their proactive security programs, their performance declines or plateaus, especially as they scale their programs. This is especially true for crowdsourced security programs, where hacker engagement and program structure significantly impact security outcomes.

To harness the full potential of their security programs, organizations should use analytics and reporting to track program performance and brainstorm actionable improvements. Platform reporting and analytics should provide essential program-level metrics, comparative benchmarks, and detailed data breakdowns. With this information, organizations can make data-driven decisions that inform their security strategies' size, scope, and mix of programs.

Bugcrowd offers multiple data visualization options to help you monitor program health and implement improvements quickly. The Platform allows organizations to view a report on their overall security posture, track the performance of individual programs, and drill down into specific metrics to uncover new insights. Additionally, a dedicated Bugcrowd team member will actively monitor your metrics and identify new opportunities to boost your security outcomes.

To harness the full potential of your crowdsourced security programs, organizations must use **analytics and reporting** to track program performance and brainstorm actionable improvements.

Bugcrowd: Your proactive security partner

For SaaS providers, proactive security is a critical investment to lower their risk against breaches or technical disruptions. Crowdsourced security is the ultimate proactive security solution, enabling organizations to leverage the Crowd's expertise and uncover novel vulnerabilities.

Organizations can partner with Bugcrowd to implement proactive and crowdsourced security initiatives. Our unique solutions combine global expertise at scale, drawing on a vetted hacker community adept at uncovering hidden vulnerabilities across various SaaS platforms. Through transparent and actionable reporting and integrations with key DevOps workflows, Bugcrowd enables teams to swiftly validate, triage, and fix critical issues. Additionally, our programs support compliance with frameworks like SOC 2, ISO 27001, HIPAA, and GDPR.

For more information on how crowdsourced security programs can help elevate your SaaS company's posture, download our Ultimate Guide to Crowdsourced Security for SaaS Companies.

Or, if you're ready to kick off the conversation, talk to a Bugcrowd security expert today.

bugcrowd

PLATFORM TOUR

See the Bugcrowd Platform in action

Take a 5-minute tour to get an overview of how the Bugcrowd Platform connects you with trusted hackers to help you take back control and stay ahead of attackers.

Unleash Human Creativity for Proactive Security

TRY BUGCROWD