CyStack

DATA SHEET

Managed Bug Bounty

Find vulnerabilities with WhiteHub before attackers do

Crowdsourced Security

In the context of internet users increasingly imposing high standards on the products they use, businesses are inadvertently pushed into the race to develop products fast enough, good enough, and still be safe in the operation. The more frequently the software is updated, the more likely it is to have security flaws.

The solution to this problem is that developers must be faster than hackers in finding and fixing vulnerabilities in their products. An advanced approach here is to use crowdsourced security.

Basically, this is an extended version of traditional security testing in terms of human resources. Instead of working with a team of 2-5 security testers, companies now can have a security researcher community of thousands of people who will help them to find out security issues.

When comparing crowdsourced security to traditional security methods, there are several advantages:

- Broader coverage: Crowdsourced security allows businesses to engage with a large number of security experts with diverse skills and expertise, which can help to identify vulnerabilities that may have been missed by internal security teams. Traditional security methods typically rely on a smaller group of in-house security experts.
- Fresh perspective: Crowdsourced security can provide a fresh perspective on security issues, as security experts from outside the organization may be able to identify vulnerabilities and attack vectors that internal teams may have overlooked.
- Faster detection and response: Crowdsourced security can help businesses quickly detect and respond to security vulnerabilities, as security experts are able to identify and report vulnerabilities in a timely manner.
- Cost-effective: Crowdsourced security can be a cost-effective alternative to traditional security methods, as it allows businesses to tap into a large pool of security experts at a fraction of the cost of hiring a full-time security team.
- Positive reputation: By launching a crowdsourced security program, businesses can demonstrate their commitment to security, which can help to build trust and improve their reputation.

Use Cases:

- Web Application Security
- Mobile Application Security
- Internet of Things (IoT) Security
- Network and Infrastructure Security
- Compliance and Regulations
- Third-Party Vendor Security
- Supply Chain Security
- Incident Response

How CyStack Helps

WhiteHub, the 1st and the biggest crowdsourced security platform developed by CyStack in Vietnam was born to thoroughly solve the mentioned problems. WhiteHub helps businesses to launch their own bug bounty program to find vulnerabilities effectively.

A bug bounty program is a type of crowdsourced security that incentivizes individuals or groups, known as "ethical hackers", to identify and report security vulnerabilities in a company's software or systems. Companies offer rewards, such as monetary compensation, swags, or recognition, to ethical hackers who are able to find and report these vulnerabilities.

The purpose of a bug bounty program is to identify and address security vulnerabilities in a timely and efficient manner, while also providing a safe and secure environment for ethical hackers to report vulnerabilities. This can help organizations to improve their security posture and reduce the risk of cyber-attacks and data breaches. Bug bounty programs can be used to test the security of a wide range of systems and applications, including web applications, mobile apps, and IoT devices.

Customer Benefits

WhiteHub is a bug bounty platform that allows organizations to manage and coordinate their bug bounty programs, and also provides a marketplace for ethical hackers to find and report vulnerabilities:

- **Customizable workflows**: WhiteHub allows organizations to customize their vulnerability submission forms and workflows, allowing them to define their own processes for handling vulnerability reports.
- **Centralized dashboard**: WhiteHub provides a centralized dashboard for managing and tracking vulnerability reports, including the ability to assign tasks, set priorities, and track progress.
- **Secure communication**: WhiteHub includes an integrated communication system for easy and secure collaboration between organizations and ethical hackers.
- **Reward system**: WhiteHub has an inbuilt rewards system for recognizing and incentivizing valuable contributions from ethical hackers.
- **Access to a global community of ethical hackers**: WhiteHub allows organizations to quickly and easily find and engage with security experts from around the world.
- **Integration with existing tools**: WhiteHub integrates with existing security tools and platforms, allowing organizations to easily integrate the platform into their existing security infrastructure.
- **Reporting and analytics**: WhiteHub provides comprehensive reporting and analytics, providing organizations with detailed insights into the effectiveness of their bug bounty program.

How It Works

A bug bounty program at WhiteHub typically works as follows:

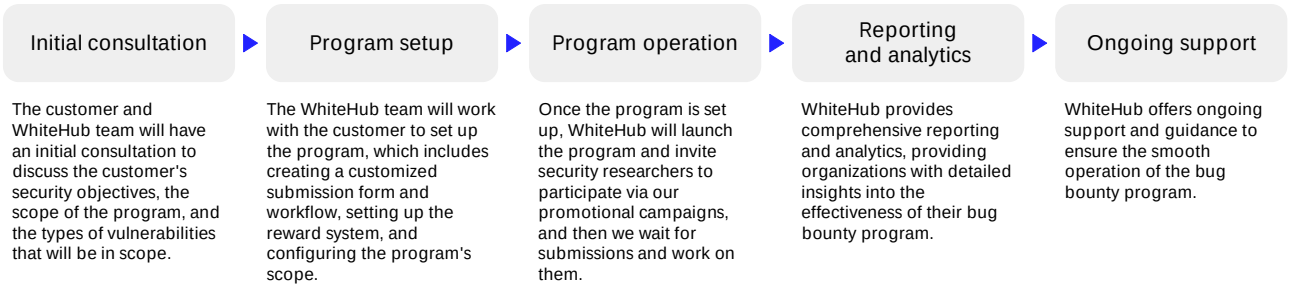
1. **Scope and rules**
   We work with the customer to define the scope of the bug bounty program, which typically includes the systems or software that are eligible for testing, as well as the types of vulnerabilities that are eligible for rewards. The rules of the program are also established, including the reward amounts, the submission process, and the timeline for receiving rewards.
2. **Program launching**
   We launch the bug bounty program in WhiteHub, announce it to the public, and provide details about the scope of the program
3. **Testing**
   Ethical hackers, also known as bug hunters from WhiteHub community, then try to find vulnerabilities in the defined systems or software. They can use a variety of techniques and tools to discover these vulnerabilities, including manual testing, automated scanning, and penetration testing.
4. **Reporting**
   When a bug hunter finds a vulnerability, they report it to WhiteHub and provide detailed information about the vulnerability, including steps to reproduce it and any potential impacts or risks it poses.
5. **Validation**
   We will verify the reported vulnerability to determine if it is a genuine security issue and if it meets the eligibility criteria for a reward.
6. **Reward**
   If the reported vulnerability is valid and eligible for a reward, the bug hunter receives a payout according to the reward structure established in the program. The reward amount can vary depending on the severity of the vulnerability, the impact it could have on the company or its customers, and the level of effort required to discover it.
7. **Fixing**
   The customer then fixes the vulnerability and may reach out to the bug hunter for additional information or assistance in verifying that the fix is effective.
8. **Public disclosure**
   Once the vulnerability is fixed, the customer may publicly disclose the issue and credit the bug hunter for their contribution to the security of their systems.

Plans

WhiteHub offers 2 plans for customers: Vulnerability Disclosure Program and Managed Bug Bounty. The below table describes the differences between them:

	Vulnerability Disclosure Program	Managed Bug Bounty
Suitable for	Businesses that have an in-house security team who can manage a bug bounty program	Businesses that don't have an in-house security team or have one but don't want to spend more human resources on bug bounty managing
Vulnerabilities Triaged by Who will discuss with the reporters and verify the submission	The client	The WhiteHub team
Branded Domain The program is hosted at a domain/subdomain of the client, not the WhiteHub domain	No	Yes
Number of Programs The maximum number of programs a customer can launch	Up to 2	Up to 4
Program Visible to Who can see and join the program	Everyone	Everyone, or only invited researchers
Program Policy Built by How the program policy is built	The client, based on the basic policy	The client, with consults from the WhiteHub team
Promoted via Channels used to promote the programs	Free channels (social networks, chat groups, etc.)	Both free and paid channels (advertising, newspapers, etc.)
Pre-Assessment WhiteHub team will perform security tests before launching the program	No	Vulnerability assessment and penetration testing
Support Channels The channel to get support from the WhiteHub team	Ticket, chat	Ticket, chat, phone, and prioritized support
Researchers Selected Based on Rules to select security researchers for the program	No specific criteria	Skillset, reputation points, certificates, NDA
Triage Analysts Rules to assign a triage analyst to work on a new finding	Predetermined	Predetermined, Random, or Round-robin

Flow To Work With Clients



The customer and WhiteHub team will have an initial consultation to discuss the customer's security objectives, the scope of the program, and the types of vulnerabilities that will be in scope.

The WhiteHub team will work with the customer to set up the program, which includes creating a customized submission form and workflow, setting up the reward system, and configuring the program's scope.

Once the program is set up, WhiteHub will launch the program and invite security researchers to participate via our promotional campaigns, and then we wait for submissions and work on them.

WhiteHub provides comprehensive reporting and analytics, providing organizations with detailed insights into the effectiveness of their bug bounty program.

WhiteHub offers ongoing support and guidance to ensure the smooth operation of the bug bounty program.

About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net

CyStack