YES WE H/CK

OVHcloud

OVHCLOUD

Public Bug Bounty Program

CASE STUDY

WHY DID YOU LAUNCH A BUG BOUNTY PROGRAM?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Security has always been a part of the OVHcloud DNA. It's inherent in our business as an infrastructure provider and all of the services that we offer. Our infrastructure security is a permanent focus, as well as a driver of our customers' trust. That security relies on physical and logical safeguards and oversight activities, scans, internal and external penetration tests, code and configuration reviews, and other security measures. Some of these safeguards are managed non-stop by our teams, while others rely on a partnership with trusted third parties.

We launched a bug bounty program for OVH with YesWeHack several years ago in order to add a layer of security to our existing systems. Our companies share the same core values and evolve in the same ecosystem; we share the same passion and the same European roots. It's partly for these reasons that we started with this platform: we were one of YesWeHack's first public program clients, and launched our program during a live bug bounty at the Nuit du Hack (Hack Night) event.

IS BUG BOUNTY STRENGTHENING THE TRUST YOU HAVE WITH YOUR CUSTOMERS?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Yes, definitely. OVHcloud works with different types of clients. Some of them manage their infrastructure themselves and are highly sensitive to technical communications. Our communication is therefore based on transparency and reliability. Other customers are more mindful as to our ability to bring in trusted third parties, such as certification auditors or external service providers. Bug bounty offers an added degree of trust for some of our customers who demand more than traditional security measures.

YesWeHack works with large strategic organisations such as OVIs (Operators of Vital Importance) and we also play in that market. YesWeHack bug bounty is part of this ecosystem of trust and is becoming a 'must have' for organisations like ours. It's also a question of reputation vis-à-vis the community of hunters, who are stakeholders in this ecosystem: through YesWeHack, we can interact with people who aren't always available via other channels.

> **Bug bounty puts us in touch with experts with knowledge that complements our teams across the entire spectrum of technologies that we use.**

WHAT DOES BUG BOUNTY OFFER YOU IN TERMS OF THE AFOREMENTIONED SERVICES (AUDITS, SCANS, PENETRATION TESTS, ETC.)?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

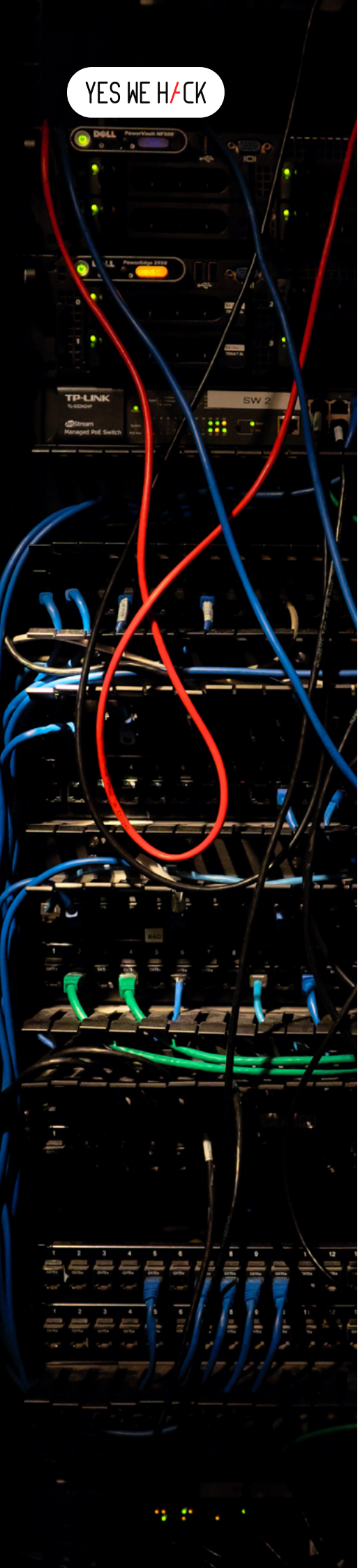
Bug bounty puts us in touch with experts with knowledge that complements our teams across the entire spectrum of technologies that we use. This includes OpenStack, Kubernetes, Machine Learning tools, and AI. It's impossible to find a team of penetration testers with advanced skills in all of these technologies.

YesWeHack gives us easy access to experts in these various technologies who say: "I'm a Kubernetes expert, so I'm going to take a look at all of these bug bounty programs with Kubernetes offers and dig deeper." This effectively completes our security approach by providing a perspective that complements that of our teams.

Bug bounty also offers a formal framework for vulnerability reporting. It allows us to provide a legally secure point of entry for the hunters. Even if it isn't the only OVHcloud channel for vulnerability reporting, we recommend to anyone that 'finds' vulnerabilities to use our program. This allows us to have one single inflow and a linked process for managing vulnerability reports. It's therefore a defining part of our CVD (Coordinated Vulnerability Disclosure).

Beyond the advantages of bug bounty as a model, I would highlight the YesWeHack platform, which has a very intuitive user interface. The OVHcloud team managing the bug bounty program gives us excellent feedback on the workflow management, report processing, and interactions with the hunters.

The APIs enable us to integrate useful information into our own tools and dashboards automatically. We can also track our bonus budget and the activity of each program. At a glance, we understand the status of our programs and can quickly report indicators to our management. Bug bounty is fully integrated into our global security strategy.



OVHcloud

WHAT ROLE DOES BUG BOUNTY PLAY IN YOUR AGILE DEVELOPMENT METHODOLOGY?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Our team of penetration testers oversees our bug bounty program: two managers are in charge of the program as well as leading the community of hunters. They then work with the various teams affected by the vulnerabilities so that we can integrate them into our management systems and ensure remediation.

Once the vulnerabilities are reported via the platform, we integrate them into our processes: we have an entire organisational structure that we call security management systems, as part of the ISO 27001 certification framework. Documented processes, roles, and responsibilities ensure that each vulnerability, incident, or potential threat is processed and monitored over time by our teams. It is also part of a detailed action plan whose application is verified according to the sensitivity of the product in question, and the associated level of requirement. Thanks to the YesWeHack API, we can easily integrate the bug bounty reports into this process. Everything is managed by tickets that are viewable on our dashboards and accessible to our external auditors.

> **We're in a relationship where we openly discuss findings on how to analyse a vulnerability. There is no other way to have such productive communication.**

YOU'RE IN A PUBLIC PROGRAM – HOW ARE YOUR EXCHANGES WITH THE COMMUNITY GOING?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Managing a bug bounty program is a real commitment to all stakeholders involved in making the internet safer. We have a responsibility to be rigorous and transparent in the management and resolution of reported vulnerabilities. This is made easier by the fact the platform provides a framework that facilitates relationships between customers and hunters, with very rich and very direct communication. We're in a relationship where we openly discuss findings on how to analyse a vulnerability. There is no other way to have such productive communication.

WHAT'S NEXT?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

We're working on standardizing the integration of tickets generated by vulnerability reports into our global risk management model. The goal is to unify our risk management regardless of the information source – whether it's a proven incident or a vulnerability report. It's about taking advantage of the full potential of APIs to further automate reporting.

We've also identified certain hunters who are particularly strong on our public program, with whom we have excellent relationships, or who have very specific skills. We plan to invite these experts onto programs dedicated to specific products. That will probably happen this year.

ABOUT

YES WE HACK

Founded in 2015, YesWeHack is a Global Bug Bounty & VDP Platform.

YesWeHack offers companies an innovative approach to cybersecurity with Bug Bounty (pay-per-vulnerability discovered), connecting more than 25,000 cybersecurity experts (ethical hackers) across 170 countries with organizations to secure their exposed scopes and reporting vulnerabilities in their websites, mobile apps, infrastructure and connected devices.

YesWeHack runs private (invitation based only) programs and public programs for hundreds of organizations worldwide in compliance with the strictest European regulations.

In addition to the Bug Bounty platform, YesWeHack also offers: support in creating a Vulnerability Disclosure Policy (VDP), a learning platform for ethical hackers called Dojo and a training platform for educational institutions, YesWeHackEDU.

⟶ CONTACT US

⟶ VISIT OUR WEBSITE

OVHcloud