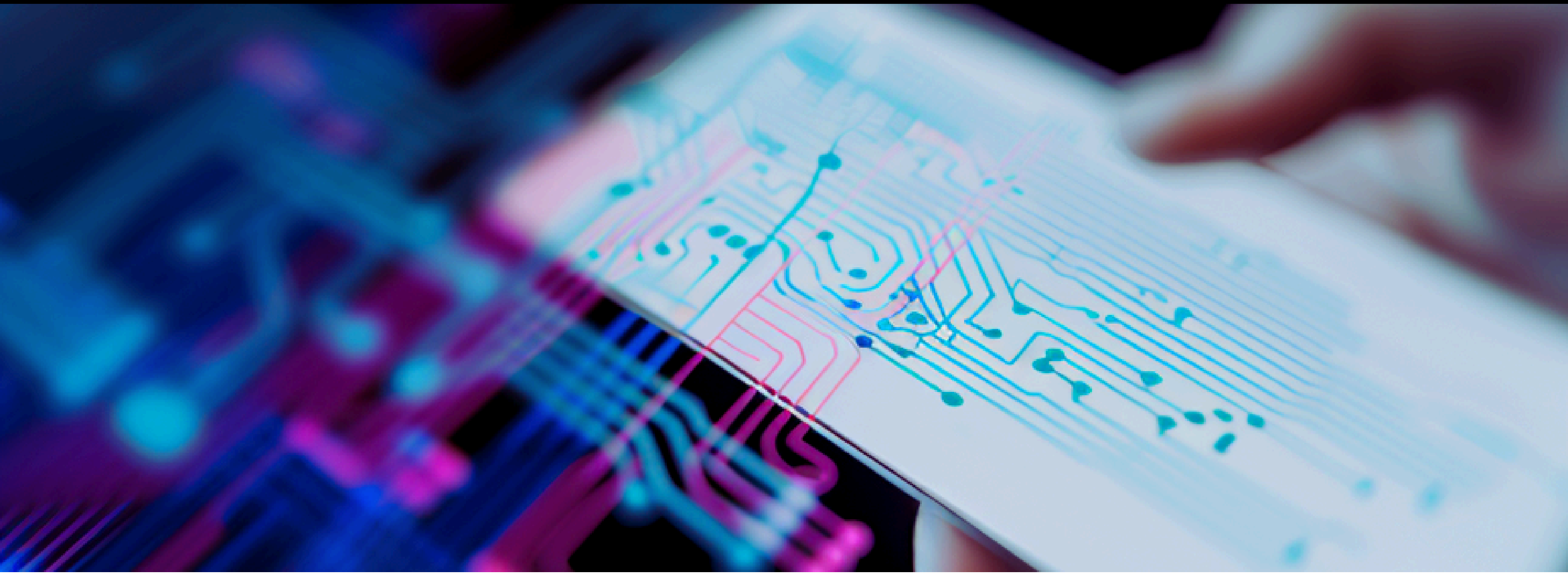
hackerone | AS Watson

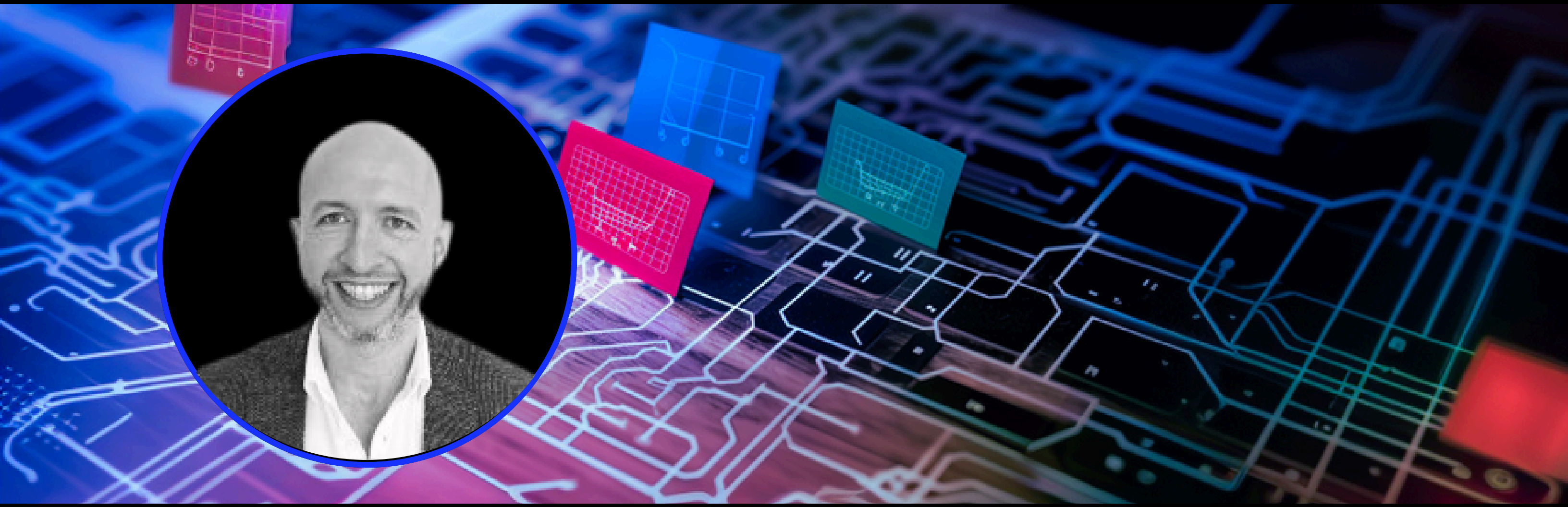


How Ethical Hackers Help AS Watson Address Digital Risk

Retail and e-commerce brands are seeing significant growth due, in large part, to the digital transformation occurring in the industry. In today's rapidly changing threat landscape, retailers are an attractive target for potential cybercriminals, with high amounts of customer data under their purview and a critical business need to deliver consistent customer experiences to the world's shoppers.

AS Watson Group knows this as well as anyone. As the world's largest international health and beauty retailer, they are in charge of the security for a footprint that includes more than 16,400 stores in 29 markets, 5.5 billion customers, and 130,000 employees. As part of their security strategy, they turned to HackerOne Bounty to help fortify their expanding digital presence and ensure that their assets remain as secure as possible as their attack surface changes.

We recently met with AS Watson's Chief Information Security Officer (CISO), Feliks Voskoboynik, to learn how ethical hackers have helped with digital transformation and enabled his team to harden their attack surface. Read on to learn Feliks' advice on including a bug bounty program as part of a security strategy, the lessons ethical hackers have provided, and what best practices he can share with other CISOs.



Q&A with AS Watson Chief Information Security Officer (CISO) Feliks Voskoboynik

Q: Tell us about AS Watson.

Feliks: Established in 1841, AS Watson Group is the world's largest international health and beauty retailer, with over 16,400 stores in 29 markets. In recent years, cybersecurity threats have been a growing concern that we cannot underestimate. The retail industry is a very attractive target for cybercriminals due to the retention of highly valuable customer information. We must protect this information from potential cyber threats, and that's where cybersecurity comes in. At AS Watson Group, our IT Security team strives to continuously strengthen the cyber defense in the organization. Our ultimate goal is to keep our organization safe and secure to enable employees and customers to work and conduct business in a safe environment.

Q: Do hackers help AS Watson with digital transformation goals?

Feliks: Every day, we strive to build a stronger international network and O+O (Offline plus Online / O plus O) platforms for customer connectivity. We focus on the O+O strategy, which makes seamless offline and online customer experiences. This digital transformation program induces a big attack surface for us, and our community of ethical hackers is helping us mitigate the risks and increase our security maturity. We wanted to have the possibility to invite a global hacking community because this is the easiest way to get top skilled hackers to assess the security of our assets.

Q: How do ethical hackers help identify vulnerability trends?

Feliks: Several times, hackers helped us with different types of vulnerabilities related to e-commerce. The creativity of the findings increased the security awareness of our product and development teams to release secure software. Security researchers help us with testing new security tools, as well as the way we configure and deploy them. One example of this was when we wanted to roll out an anti-credential stuffing tool, and hackers helped us find the weak spots and mitigate them.

Q: How do ethical hackers help harden your attack surface?

Feliks: The creativity of hackers is key to hardening our attack surface. When we receive a creative proof of concept (POC) from a hacker, we can use that process to review and verify that the specific vulnerability (or a similar one) is not reproducible on new assets. This approach gives us insights into where potential vulnerabilities might be and led us to introduce new cross-checking activities as part of the investigation and remediation process to verify a single risk on multiple components, such as inherited code into new assets.

Q: How do you use vulnerability insights to train internal teams?

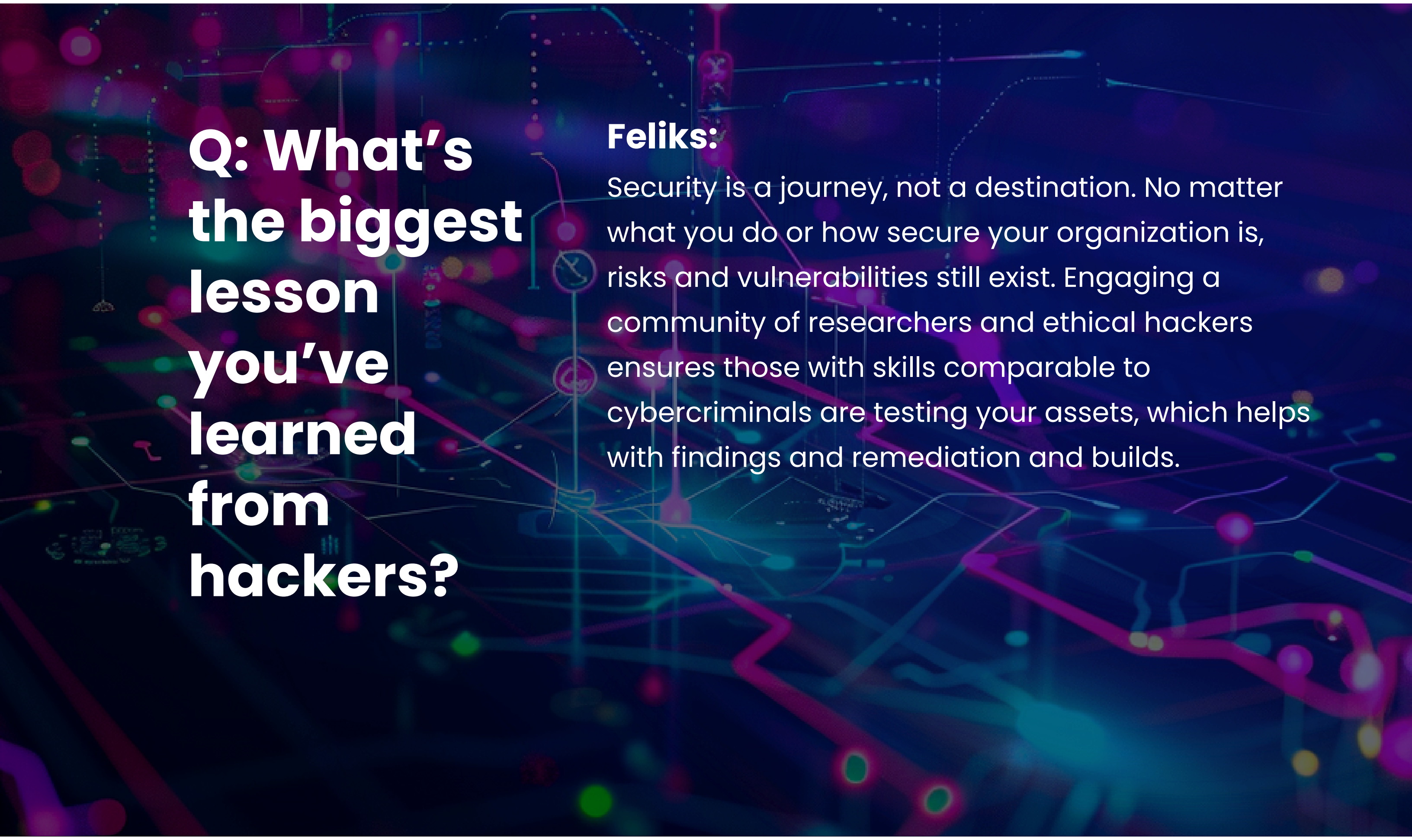
Feliks: Specific findings of hackers enabled us to build a new secure code training program for our development teams. We monitor the trends of vulnerabilities and leverage them to build a training baseline to reduce the risks to our assets. The training program has helped us increase the quality of the code and reduce vulnerabilities. It's also increased our prevention capabilities by shifting left as much as possible to secure the SDLC. We noticed a decrease in total valid reports over the years, and we lowered costs by remediating issues in live environments.

Q: How do you report on the value of working with ethical hackers?

Feliks: Considering our big attack surface, it's a challenge to scale up penetration testing teams, even with third-party engagement. Our first KPI was on the resources we were saving compared to standard, time-boxed penetration testing activities. We also developed an internal KPI on vulnerability trends on specific brands, remediation, risk reduction, and more. With the community, you have many different areas of expertise compared to a single resource executing a time-boxed penetration test.

Q: What ROI do you expect to see from your bug bounty program?

Feliks: The ROI comes from the fact that we rely on HackerOne to find and deliver critical issues every day. Therefore, the ROI is that HackerOne finds issues daily.



Q: What's the biggest lesson you've learned from hackers?

Feliks:

Security is a journey, not a destination. No matter what you do or how secure your organization is, risks and vulnerabilities still exist. Engaging a community of researchers and ethical hackers ensures those with skills comparable to cybercriminals are testing your assets, which helps with findings and remediation and builds.

Q: What advice would you give to other CISOs planning to start a bug bounty program?

Feliks:
Start with building a robust vulnerability management program to handle the reports properly and make the program scale. When you design the rules of engagement, you need to clearly understand the risks you want to prioritize and identify your risk appetite.

When you start a program, you will engage a community that requires your continuous commitment. Hackers are like customers, and they require time and effort to establish and maintain a relationship. It is crucial to properly manage the program KPIs, time-to-response, time-to-bounty, etc., which requires a proper team to handle it.

At AS Watson Group, we consider the community as an extension of our team. In addition, we organize and plan to do many different events and contests to keep the hackers engaged with our programs.

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

HackerOne has vetted hackers for organizations including:

gm

Lufthansa

ZEBRA

zoom

Spotify

citrix

PayPal

Uber

HYATT

U.S. Department of Defense

Google

reddit

Nintendo

Adobe

A.S. Watson Group

su mo

sumo logic

yahoo!

priceline

shopify

slack

yelp

salesforce

TOYOTA

Contact us