



HOW WIND RIVER TIGHTENS ITS SECURITY POSTURE WITH HACKERONE PENTEST

Wind River's solutions power many of the world's most mission-critical systems and infrastructure. With sensitive customer data and IoT infrastructure in mind, the company decided to implement a more robust security program around ISO 27001 and needed a leading security testing partner to support its ambitious plans.

Customer Story

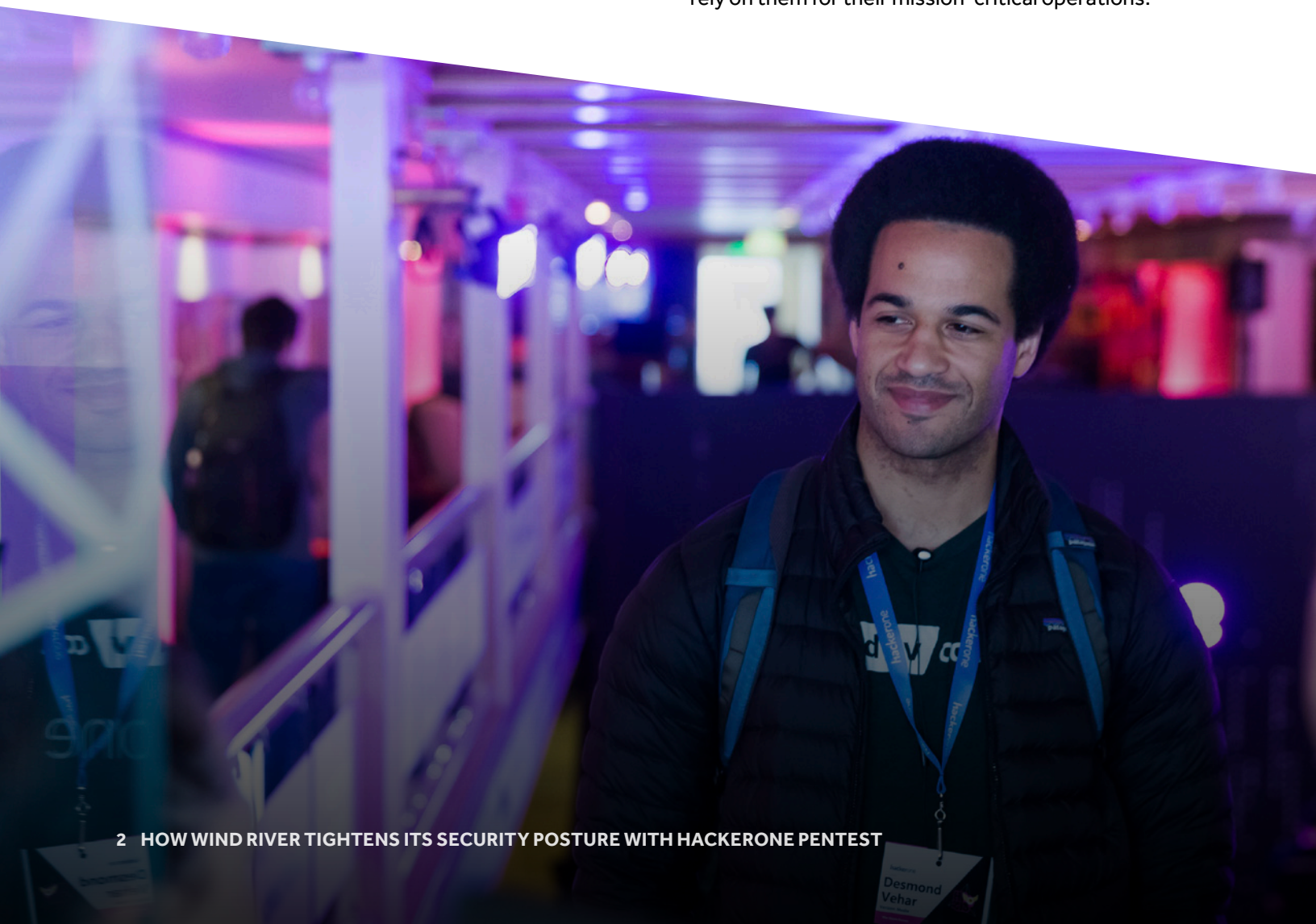
WINDRIVER

Wind River is a global leader in software for the intelligent edge. Its technology powers billions of connected devices and systems across market segments ranging from aerospace to industrial, defense to medical, and telecommunications to automotive. As an integral part of the connected world matrix, security is of paramount importance to Wind River.

Wind River customers rely on the company's software and services to power mission-critical operations and process highly sensitive information. With customers including many of the world's largest and most prominent organizations — from NASA to Ford Motor Company — ensuring world-class security across the board is essential.

Rich Kellen, Vice President and Chief Information Security Officer at Wind River, explains:

"Connected intelligent edge devices now play a pivotal role in operations across all industries. And as uptake increases, there has been a huge spike in cyberattacks targeting the systems that power those devices. As the leader in powering these systems, we have to make sure our products are hardened against cyberattacks so our customers can rely on them for their mission-critical operations."



KEY STATS

Solution	Engagement Length	Outcomes
H1 PENTEST	2 WEEKS	<ul style="list-style-type: none">→ HARDENED ATTACK SURFACE→ SATISFIED ISO 27001 TESTING REQUIREMENT→ INSTANT RETESTING→ CUT ISSUES FROM FUTURE CODE

BUILDING TRUST THROUGH SECURITY AND COMPLIANCE

Wind River helps the world's technology leaders power generation after generation of the safest, most secure devices in the world. The company's software runs the computing systems of the most important modern infrastructure across a diverse range of use cases — from collaborative robots to commercial and military drones, connected cars to the connected factory floor — as well as the communication networks that support these mission-critical intelligent systems. The company is now expanding to a Software as a Service (SaaS) delivery model for its offerings. While the systems and operations Wind River enables remain the same, the software used to power intelligent connected systems will now also be delivered remotely.

Security is not only a number one priority for the customers the company serves, it's a top priority for Wind River as well. To ensure their systems remain

secure — and maintain customer trust — Wind River decided to implement a new, more robust security posture. The company's security program is now based around ISO 27001 — an international information security framework designed to help organizations protect the confidentiality, integrity, and availability of sensitive information.

As part of this program, the company needed a comprehensive penetration test of its web-based assets and Internet-facing IP addresses to ensure its systems were fully hardened against cyber threats.

HUNTING DOWN SERIOUS VULNERABILITIES WITH HACKERONE PENTEST

Historically, the security testing tool of choice to satisfy compliance requirements was traditional pentesting. However, while Wind River needed to fulfill the testing requirement of ISO 27001, the real aim was to improve security. As the threat landscape has evolved, traditional methodology-based penetration testing has become less effective at uncovering serious vulnerabilities.

To ensure its assets were tested with the necessary rigor, Wind River opted for a HackerOne Pentest.

"We aren't just looking to satisfy compliance requirements," explains Rich Kellen. "Traditional penetration tests might have been OK ten years ago, but they don't provide the intensity and range of testing skills we need to make sure our assets are watertight. We need a testing partner that goes beyond a pre-planned methodology to find issues a hacker could find and exploit in the real world."

HackerOne Pentest provides the guaranteed coverage of a traditional penetration test with the creativity and diverse testing capabilities of expert hackers. Hackers from the HackerOne community were hand-picked for the two-week engagement based on their skills and experience. This ensured Wind River's assets were exposed to rigorous testing by hackers with domain-specific expertise — something that isn't guaranteed with a traditional penetration test.

"With a traditional penetration test, you book your engagement months in advance, and you get whichever testers are available at the time," continues Rich Kellen. "They might be great testers, but if they aren't experienced at working with your types of assets, that's a problem. HackerOne selected a team to make sure we had a diverse range of testing skills and that our testers were experienced at working with assets like ours. That's a service you just can't get unless you go crowdsourced."

During the engagement, the hacking team focused on identifying high-risk vulnerabilities that were at risk of exploitation. By focusing on the tools and techniques they each specialize in, the team realistically simulated the attacks Wind River's assets could face in the real world. The engagement also included a methodology-driven component to meet compliance, business, and risk management needs.



FUTURE-PROOFING SECURITY

Wind River's end goal was to build a more robust security program based around ISO 27001 to protect sensitive systems and information from a new breed of cyberattacks. Through HackerOne Pentest, the company tapped a global community of hackers to uncover serious vulnerabilities in its systems before they could be exploited in the real-world.

"Compliance and security aren't the same thing," explains Rich Kellen. "If you want to achieve both, you have to choose your framework wisely and use it in a way that genuinely improves security across your organization. HackerOne Pentest helped us fulfill the testing requirements of ISO 27001. But more importantly, it uncovered issues and vulnerabilities we didn't know about that could have caused serious problems for our customers and us."

HackerOne Pentest also enabled Wind River to collaborate with hackers throughout the engagement. This allowed the company's security and engineering teams to:

- Discuss reported vulnerabilities and seek guidance on how to resolve them.
- Request retests for fixed vulnerabilities to ensure each issue was resolved.

"Being able to have issues retested during the same engagement is a game-changer," explains Rich Kellen. "That's something that hasn't been available in the past because traditionally, you didn't receive the results of a penetration test until after the engagement was over. By having each issue retested after we have applied a fix, we can be sure our efforts have been successful, and nobody can exploit that issue in the wild."

After the engagement, Wind River received a summary report of the vulnerabilities discovered, with clear remediation guidance. After analyzing each vulnerability's root causes, the company's engineering and security teams put procedures in place to eliminate entire classes of vulnerabilities from future code. This proactive approach is part of Wind River's plan to future-proof the security posture of its assets.



"The threats we face now are much more sophisticated and varied than they were just a few years ago," concludes Rich Kellen. "To combat a higher class of threats, you need a higher class of security testing, and you need to take a more proactive approach in responding to the issues and vulnerabilities found. HackerOne Pentest gives us the comprehensive and diverse testing we need to protect against advanced threats and ensure our products meet the rigorous security standards we've set over the last 40 years."

RICH KELLEN

**VICE PRESIDENT AND CHIEF INFORMATION
SECURITY OFFICER, WIND RIVER**

HACKERONE HAS VETTED HACKERS FOR HUNDREDS OF ORGANIZATIONS INCLUDING:



Lufthansa



UBER

HYATT



Google



HBO



yahoo!

priceline



verizon
media



With Over 2,000 Customer Programs,
More Companies Trust HackerOne
Than Any Other Vendor

CONTACT US