

# Hardware and integrated systems pentesting: automotive

**Identify security issues on vehicles and gain recommendations to improve the systems at any stage of automotive development**

**The most trusted products, services, and brands are secured by NetSPI**

## The challenge




In 2023 critical and high vulnerabilities [in the automotive industry] accounted for nearly 80% of total Common Vulnerabilities and Exposures (CVEs), up from 71% in 2022.<sup>1</sup>

Today's automotive industry has reached a critical inflection point. Cybersecurity incidents have grown significantly in frequency as well as impact. The ability to identify security issues on vehicles at any stage of automotive development such as vehicle manufacturers, component suppliers, or OEM and aftermarket software and hardware providers is more important than ever before.

The technological design of a standard car contains multiple electronic control units (ECUs), with some luxury models containing hundreds of these units. Each one of these systems can contain up to 100 million lines of code. In an industry where a single mistake puts lives on the line, it is critical that organizations take a strategic approach to automotive cybersecurity – and related systems and applications – before malicious adversaries can cause harm.

## The solution

NetSPI's hardware and integrated systems pentesting includes a service specifically designed for use cases in the automotive industry, delivered on The NetSPI Platform. Our technology, process, and human intelligence help you discover, prioritize, and remediate what matters most. NetSPI security experts have decades of testing experiences as well as a deep understanding of the automotive Threat Analysis and Risk Assessment (TARA) methods to ensure the standards such as ISO 26262-1:2018, ISO/SAE 21434, R155, and R156 aren't just met, but exceeded.

-  Discovery of potential automotive security risks
-  Evaluation of attack vectors leveraging technology and human intelligence
-  Validation and prioritization of vulnerabilities

**"In 2023 the proportion of incidents with a high or massive impact dramatically doubled to nearly 50%"**

Upstream Global 2024  
Automotive Cybersecurity Report



## Identify potential exposures across your entire attack surface Leverage the deep knowledge of our security experts to identify risk

Our automotive penetration testers understand specific attack vectors for the automotive industry and will identify areas of potential risk that include:

- Misconfigurations in automotive software and potential hardware attack surfaces
- Unauthorized access points that may be hidden in debugging ports
- Potential network breach points including equipment control unit systems



## Pressure test your potential attack vectors with technology and human intelligence

NetSPI security experts understand and evaluate the potential threat vectors that matter most in the automotive industry including specific hardware and software systems including but not limited to:

- Vulnerabilities within car monitoring sensors and systems, including engine, and transmission control units (ECU/TCU) and tire pressure monitoring systems (TPMS) and on-board diagnostic systems (OBD-II)
- Potential risks within automotive infotainment systems, mobile applications, USB ports, Bluetooth, Wi-Fi, and other in-vehicle networks



## Focus on what matters with manually validated findings on The NetSPI Platform

The NetSPI Platform delivers better asset fidelity, data, and data visualization and our detailed manual triage and exposure validation helps your team prioritize remediation efforts. Our team manually validates and prioritizes each finding to allow your team to focus on remediation of the most relevant risks.

- Gain real-time findings and remediation support
- Document processes, exploitation evidence, and remediations
- Seamlessly integrate into existing ticketing system workflows with our open API

## You deserve The NetSPI Advantage



**250+ In-house  
security experts**



**Intelligent  
process**



**Advanced  
technology**

## Your proactive security partner

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), Attack Surface Management (ASM), and Breach and Attack Simulation (BAS).