





IoT Security as part of a Digital Transformation Program

Cool Findings

Every product we tested was a technological innovation based on IoT and 5G. Our team had to stretch themselves to adopt new tools and techniques to find vulnerabilities across these products.

Some of these were:

-  Sensitive data exfiltration/tampering from an IoT device
-  Unauthenticated root access to the MongoDB database
-  User account takeover in a mobile application
-  Exploiting default credentials after reverse engineering the firmware

Objective

A leading telecom provider was running a multi-billion-dollar digital transformation program that included launching multiple IoT enabled technologies to enhance consumer experience and increase revenues. A key challenge was to ensure security was embedded into the product lifecycle to ensure faster go-to-market. After a detailed RFP process, the telecom provider selected Network Intelligence as its security partner for this journey.

Challenges

The key challenges in the project were:

- Coordinating with multiple vendors across different geographical locations
- Expertise in IoT testing, especially non-standard firmware and protocols
- Agility in working with multiple moving parts of the overall digital transformation program.
- Explaining risks of discovered vulnerabilities and working patiently with developers and architects to effectively mitigate them.

During the project, we had to adopt unique tools and techniques to identify a wide variety of IoT-enabled technologies. As a result, we identified many interesting vulnerabilities in IoT devices, product architecture, and the encryption protocols implemented by the product teams.

Solutions



Implemented cloud-native DevSecOps to address vulnerabilities early



Analyzed IoT device such as SmartCar using a car simulator to find security flaws



Summarized findings visually for clear, actionable insights



Adopted a partnership approach with product teams, business stakeholders, and security teams

Customer Benefits

- 1 Enhanced Security:** Reduced risk of security breaches in the newly launched IoT-enabled products and services.
- 2 Improved Reliability:** Ensured availability and smooth functioning of these products and services.
- 3 Faster go-to-market:** Worked closely with product and business teams to evangelize security issues and help them shift security left, thereby facilitating faster go-to-market.

