

Enhancing Security for QEPR's GPS Keyfob System



Client:
QEPR

Industry:
IoT and Consumer Electronics

Company Size:
11-50 people

Services Used:
Secure Architecture Development, Security Requirements, Penetration Testing, Bluetooth, NB-IoT, eSIM

Client

QEPR specializes in innovative loss prevention solutions, offering technology to protect personal items from being lost or stolen. Their flagship product, a hardware keyfob, combines cutting-edge technology with user-friendly design, providing a reliable and efficient way to track and retrieve lost items. With a focus on loss prevention and the fast return of lost smartphones, QEPR stands out with its complete, patented system, which includes a GPS-enabled keyfob, smartphone tag, and concierge member support.

Background

As QEPR prepared to transition from their prototype v1 to a robust v2 version, they recognized the critical importance of integrating security into their product development process. Protecting sensitive user data and ensuring the reliability of their loss prevention system were paramount. With complex technologies like Bluetooth, NB-IoT, and an embedded SIM card (eSIM) involved, QEPR faced the challenge of enhancing security without compromising the device's battery life and user experience.

The Challenge

QEPR approached Iterasec with multiple objectives:

- **Secure Architecture Development:**
Design a secure architecture for the keyfob device, mobile application, and web portal.
- **Implement Secure SDLC:**
Integrate security into their Software Development Life Cycle (SDLC) from the ground up.
- **Penetration Testing:**
Conduct comprehensive penetration tests on the mobile apps, web app, and the keyfob itself at various stages of development.
- **Optimize Security and Battery Life:**
Align security controls with battery constraints, finding compromises between security measures and energy consumption.
- **Technology Integration:**
Address security concerns related to Bluetooth, NB-IoT, and eSIM technologies.

The Solution

Iterasec provided a comprehensive range of cybersecurity services tailored to QEPR's needs.

Secure Architecture Development

We collaborated closely with QEPR to develop a secure architecture for their keyfob device, mobile applications, and web portal. This included:

- **Security Requirements:**
Defining detailed security and architecture requirements for all components of the system.
- **Battery Optimization:**
Designing security controls that balanced robust protection with minimal energy consumption to preserve battery life.
- **Technology Expertise:**
Leveraging our expertise in Bluetooth, NB-IoT, and eSIM technologies to address specific security challenges.

Secure Software Development Life Cycle (SDLC) Implementation

- **Security Integration:**
Embedding security practices into every phase of the development process.
- **Continuous Improvement:**
Establishing processes for ongoing security assessments and updates.
- **Developer Training:**
Providing training to QEPR's development team on secure coding practices and threat modeling.

Penetration Testing

- **Initial Testing:**
Identifying vulnerabilities in the early versions of the product.
- **Intermediate Testing:**
Assessing security after implementing initial fixes and enhancements.
- **Final Testing:**
Ensuring the product was secure before market release.

The Outcome

Our collaboration with QEPR led to significant enhancements in their product security and development process.

- **Robust Protection:**
Implemented a secure architecture that safeguarded user data and device integrity.
- **Vulnerability Mitigation:**
Identified and addressed critical vulnerabilities through thorough penetration testing.
- **Energy Efficiency:**
Designed security controls that did not compromise battery performance, ensuring the keyfob remained efficient and user-friendly.
- **Secure SDLC:**
Successfully integrated security into QEPR's development life cycle, promoting a culture of security awareness.
- **Confidence in Launch:**
Provided QEPR with the assurance their product was secure and ready for market release.
- **Team Empowerment:**
Equipped QEPR's development team with the knowledge and tools to maintain security standards independently.

Conclusion

Our partnership with QEPR showcases our commitment to delivering tailored cybersecurity solutions that address complex challenges. By integrating security into their development process and optimizing their product's security architecture, we helped QEPR bring a secure, efficient, and innovative loss prevention solution to market. Our collaborative approach ensured that QEPR could focus on their mission of protecting personal items, confident in the security and reliability of their product.