# CASE STUDY

"At COE Security, we build, operate, and transfer world-class security solutions, empowering businesses with resilience and trust."

Joseph Henderson

COE SECURITY LLC

USA | BRAZIL | UAE | INDIA

## CASE STUDY

# CASE STUDY FIRMWARE PENETRATION TESTING WITH COE SECURITY

COE SECURITY

# Measurable Impact Our Security in Numbers




- 1,500+ Global Engagements
- 95% Client Satisfaction
- 10+ Years of Cybersecurity Excellence
- 15K+ Critical Vulnerabilities Identified
- 1M+ Security Incidents Managed
- $350M+ Costs Saved
- $2.5B+ Transactions Secured
- 24/7/365 Threat Monitoring & Response
- Proactive Threat Hunting
- Cutting-Edge Security Technologies
- Dedicated Security Advisors
- Zero-Day Exploit Mitigation
- Incident Response Planning & Execution
- Security Awareness Training
- Customizable Security Solutions

## Client Profile

An IoT manufacturer developing smart devices and embedded systems for various industries, including healthcare, retail, and logistics

## Challenges Faced

As an innovator in the IoT space, the client faced growing concerns over the security of their devices, particularly around vulnerabilities in firmware that could be exploited by attackers. The client recognized the importance of securing their embedded systems before they went to market. However, with the rapidly evolving landscape of cybersecurity threats and limited internal expertise in firmware security, the client required expert assistance in identifying and mitigating potential risks

- Firmware Vulnerabilities Identifying and assessing security flaws in firmware that could be exploited
- Device Integrity Ensuring that the devices were secure from manufacturing to deployment
- Risk Mitigation Developing remediation strategies to address identified vulnerabilities before products were released
- Continuous Monitoring Ensuring ongoing protection and regular testing to stay ahead of emerging threats

We're Hiring!

COE SECURITY

# Compliance & Regulatory Mastery


- ISO 45001
- HIPAA & HITRUST
- NIST & NIST 800-171
- ISO 27001
- PCI DSS
- CMMC
- CIS Controls
- SOC 2
- CCPA & NYDFS
- EU CRA
- FedRAMP
- GDPR
- UK Cyber Essentials
- Essential Eight - Australia

## Our Approach

The IoT manufacturer partnered with COE Security for a comprehensive firmware penetration testing engagement. Our team of security experts employed advanced testing techniques to identify vulnerabilities in the firmware of the client's devices, providing actionable insights and tailored remediation strategies

## Phase 1 Firmware Analysis and Vulnerability Assessment

- Conducted thorough penetration testing of the client's firmware, simulating real-world attack scenarios to uncover vulnerabilities
- Identified potential attack vectors and weaknesses in the system, including unauthorized access points and insecure communication protocols
- Provided a comprehensive report outlining discovered vulnerabilities and prioritized risks

## Phase 2 Exploitation and Risk Analysis

- Attempted exploitation of identified vulnerabilities to assess the real-world impact on device functionality and security
- Performed additional testing to determine the potential for attackers to compromise device integrity or exfiltrate sensitive data
- Analyzed the potential long-term impact of discovered flaws on device security and company operations

We're Hiring!

COE SECURITY

# Our Cybersecurity Arsenal: Beyond Protection- We Build Resilience

- Application Penetration Testing (Thick/Thin)
- Mobile Application Penetration Testing
- API Penetration Testing
- Network Penetration Testing
- Operational Technology Security Testing
- Cloud Penetration Testing
- AI & LLM Security Audit and Pen Testing
- Red Teaming & Social Engineering Services
- Product & Hardware Penetration Testing
- IoT Security
- Security Operations Center Services (24/7)
- Custom Security Services

## Phase 3 Remediation Strategies and Patch Development

- Provided detailed recommendations for addressing the vulnerabilities identified during testing
- Assisted in developing firmware patches and updates to mitigate risks and enhance device security
- Worked closely with the client's development team to integrate security improvements into future device iterations

## Results

With COE Security's expert guidance, the IoT manufacturer was able to significantly enhance the security of their devices, resulting in

- Strengthened Device Security Early identification and remediation of firmware vulnerabilities before product release
- Risk Reduction Mitigated potential threats that could have led to data breaches, financial loss, and reputational damage
- Operational Efficiency Streamlined development processes and improved security integration throughout the product lifecycle
- Market Confidence Enhanced customer trust and confidence by demonstrating a commitment to security and product integrity

We're Hiring!

COE SECURITY

# Industries We Protect with Cutting-Edge Security



- Financial Services
- Healthcare
- Retail
- E-commerce
- Government
- Cryptocurrency
- Blockchain Technology
- Automotive
- Transportation/Logistics
- Energy & Utilities
- Hospitality/Tourism
- Entertainment/Media
- Manufacturing
- Education
- Telecommunications
- HiTech & Information Technology

**We're Hiring!**

## Results Achieved

- Within six weeks, the company successfully:
- Eliminated all critical vulnerabilities, reducing cyber risks significantly.
- Strengthened access controls, preventing unauthorized access.
- Hardened network infrastructure, making it resistant to attacks.
- Adopted a proactive cybersecurity strategy, enhancing overall resilience.

## Client Testimonial

Partnering with COE Security for firmware penetration testing was a game-changer for our product development. Their thorough testing and expert guidance helped us identify and fix critical vulnerabilities, ensuring our devices were secure and ready for market. We now have confidence in the security of our products and the trust of our customers.

"Peace of mind in a world of cyber threats. That's what we deliver."

*Joseph Henderson*

COE SECURITY