

## CASE STUDY

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

Joseph Henderson



## CASESTUDY

### ACHIEVING ISO 45001 CERTIFICATION FOR A MANUFACTURING COMPANY

COE SECURITY LLC

USA | BRAZIL | UAE | INDIA



# 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

**We're  
Hiring!**

## Client Profile

A mid-sized manufacturing company specializing in industrial equipment, with 500 employees across two manufacturing facilities and one corporate office.

## Challenges Faced

A manufacturing company sought ISO 45001 certification but lacked the expertise to navigate the process. Key challenges included:

- Gap Analysis & Pre-Audit Readiness – Identifying OH&S gaps and preparing for certification.
- Risk Assessment & Mitigation – Implementing risk controls for workplace hazards.
- Documentation & Implementation – Developing policies, procedures, and training.
- Internal Audits & Management Review – Ensuring system effectiveness through audits and reviews.

## Solution:

Partnering with [Your Cybersecurity Consulting Firm Name], we provided:

1. Gap Analysis & Pre-Audit Review – Assessed compliance gaps, created an action plan, and conducted a mock audit.
2. Implementation & Remediation – Developed policies, improved hazard controls, and trained employees.

Our expertise ensured a seamless certification process, enhancing workplace safety and compliance.

## Implementation and Remediation

- Documentation Development – Created and implemented essential policies, risk assessment procedures, emergency plans, and training materials.
- Hazard Mitigation – Worked with the safety team to enforce effective controls, including engineering solutions, administrative measures, and PPE.
- Employee Training – Provided training on new OH&S procedures, emphasizing the importance of active participation.



# 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

## Security Testing Execution

Leveraging industry-standard frameworks like OWASP Top 10 and NIST SP 800-115, we conducted a comprehensive application penetration test, covering:

- Recon & Intelligence Gathering – Mapping application structure, identifying exposed endpoints, and assessing attack vectors.
- Automated & Manual Testing – Using Burp Suite, OWASP ZAP, and Kali Linux to uncover and validate vulnerabilities.
- Authentication & Authorization – Detecting weak authentication, privilege escalation, and session mismanagement.
- API Security – Identifying BOLA, IDOR, and rate-limiting flaws.
- Injection & Input Validation – Testing for SQLi, XSS, and command injection.
- Business Logic Flaws – Analyzing transaction workflows for exploitation risks.
- Mobile App Security – Evaluating data storage, reverse engineering threats, and insecure API calls.

## Findings & Risk Assessment

Following the penetration test, we compiled a detailed report highlighting:

- Critical, High, Medium, and Low-risk vulnerabilities along with their potential business impact.
- Proof-of-Concept (PoC) exploits demonstrating how attackers could exploit weaknesses.
- A prioritized remediation roadmap to help the company fix vulnerabilities efficiently.

**We're  
Hiring!**





# 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

## Internal Audits and Management Review

- o An internal audit program was established, and internal auditors were trained on conducting effective audits.
- o We facilitated management review meetings to evaluate the OH&S management system's performance and identify improvement opportunities.

## Certification Audit Support

Ongoing support was provided throughout the certification audit, addressing any questions or concerns raised by the certification body.

Results: With our guidance, the manufacturing company successfully achieved ISO 45001 certification. The implemented OH&S management system resulted in:

- **Reduced Workplace Incidents:** A 25% reduction in workplace incidents within the first year.
- **Improved Employee Morale:** Increased employee engagement and a stronger safety culture.
- **Enhanced Regulatory Compliance:** Demonstrated compliance with relevant OH&S legal and regulatory requirements.
- **Improved Operational Efficiency:** Reduced downtime and improved productivity due to fewer work-related injuries and illnesses.
- **Competitive Advantage:** Enhanced reputation and competitive advantage by demonstrating a commitment to employee well-being.

**We're  
Hiring!**





# 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 critical vulnerabilities, including authentication bypass and insecure API endpoints.
- Strengthened its web and mobile applications against cyber threats.
- Integrated security best practices into its software development lifecycle (SDLC).
- Established a regular penetration testing cycle, ensuring ongoing security improvements.

## Client Testimonial

"Partnering with COE Security LLC was instrumental in our successful ISO 45001 certification. Their expertise and support were invaluable throughout the entire process."

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

*Joseph Henderson*

