CASE STUDY

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

Joseph Henderson

CASE STUDY

STRENGTHENING ENTERPRISE SECURITY THROUGH NETWORK PENETRATION TESTING

COE SECURITY LLC

USA | BRAZIL | UAE | INDIA

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

A large-scale manufacturing company with multiple offices, data centers, and cloud environments relied on an extensive IT infrastructure to manage operations, supply chain logistics, and customer data. Due to increasing cyber threats, the company needed to assess its internal and external network security to prevent unauthorized access, data breaches, and compliance violations.

Challenges Faced

Before undergoing Network Penetration Testing, the company identified multiple security concerns:

- Unpatched vulnerabilities in firewalls, routers, and servers, increasing the risk of exploitation.
- Weak access controls, allowing potential unauthorized access to internal resources.
- Misconfigured network devices, leading to exposure of critical services.
- Lack of segmentation, making lateral movement easy for attackers.
- Potential insider threats, with employees having excessive privileges.
- Compliance concerns with ISO 27001, PCI DSS, NIST 800-53, and CIS Controls

Our Approach

To enhance network security, we conducted a comprehensive Network Penetration Testing engagement, identifying vulnerabilities and providing remediation strategies.

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

We're Hiring!

Scoping & Threat Modeling

We collaborated with the client to:

- Define the scope of testing, including IoT devices, cloud integrations, APIs, and mobile apps.
- Identify threat models specific to industrial IoT environments, such as denial-of-service (DoS), man-in-the-middle (MITM) attacks, and firmware manipulation.
- Determine testing methodologies (Black Box, Gray Box, and White Box testing).

Security Testing Execution

- External Testing – Assessing firewalls, VPNs, and web servers for vulnerabilities.
- Internal Testing – Simulating insider threats and lateral movement risks.
- Vulnerability Exploitation – Identifying and exploiting unpatched systems.
- Firewall & IDS Evasion – Testing security controls against advanced attacks.
- Wi-Fi Security – Evaluating encryption, rogue APs, and access risks.
- Network Segmentation – Ensuring proper isolation of critical systems.
- Privilege Escalation – Identifying paths for unauthorized access.
- Social Engineering – Simulating phishing and credential attacks

Findings & Risk Assessment

- After completing the penetration test, we provided a detailed security report, including:
- Critical, High, Medium, and Low-risk vulnerabilities, with business impact analysis.
- Proof-of-Concept (PoC) exploits, demonstrating how attackers could exploit weaknesses.
- A prioritized remediation roadmap, helping the company fix vulnerabilities efficiently.

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

Remediation Support & Secure Coding Practices

- To ensure the network remained secure, we provided:
- Firewall hardening recommendations to block unauthorized access.
- Network segmentation strategies, limiting lateral movement.
- Patch management guidance, ensuring systems remain up-to-date.
- Secure Wi-Fi configurations, preventing unauthorized connections.
- Zero Trust Network Architecture (ZTNA) implementation, reducing attack surfaces.
- Re-testing of critical vulnerabilities, ensuring proper remediation.

Compliance & Continuous Security

- After implementing security fixes, the company achieved:
- A more resilient network, eliminating critical security risks.
- Compliance readiness for ISO 27001, PCI DSS, NIST 800-53, and CIS Benchmarks.
- Improved threat detection and incident response capabilities.
- Implementation of continuous network monitoring, ensuring long-term security.

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.

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!

Conclusion

By leveraging our Network Penetration Testing expertise, we helped the manufacturing company proactively identify vulnerabilities, strengthen security controls, and achieve compliance with industry regulations. Our structured approach, from threat modeling to remediation, ensured the network remained resilient against cyber threats.

COE Security LLC

COE Security is a leading cybersecurity services provider, offering comprehensive solutions to address the evolving threat landscape. We have a proven track record of helping organizations of all sizes mitigate risks, strengthen defenses, and recover from cyberattacks. Our team of experienced cybersecurity professionals possesses deep expertise in the latest technologies and best practices, enabling us to deliver tailored solutions that meet your unique security needs.

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

Joseph Henderson

COE SECURITY