

## CASE STUDY

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

Joseph Henderson



## CASESTUDY SUPPLY CHAIN SECURITY REVIEW: STRENGTHENING THIRD-PARTY RISK MANAGEMENT & CYBER RESILIENCE

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 multinational manufacturing and logistics company with a complex supply chain network involving global suppliers, vendors, and partners. The organization needed a proactive security strategy to mitigate risks associated with third-party dependencies and ensure compliance with industry standards.

## Challenges Faced

With increasing cyber threats targeting supply chains, the organization encountered several security risks:

- Third-Party & Vendor Security Gaps Limited visibility into supplier security postures exposed the company to potential breaches.
- Regulatory & Compliance Risks Needed to align with NIST, ISO 27001, GDPR, and industry-specific cybersecurity frameworks.
- Supply Chain Disruptions from Cyber Threats Rising ransomware, data breaches, and operational disruptions posed critical threats.

## Solution

The organization partnered with COE Security to implement a Supply Chain Security Review, ensuring comprehensive risk assessment, continuous monitoring, and compliance enforcement.





# 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

## End-to-End Supply Chain Risk Assessment

- Conducted third-party risk assessments to evaluate vendor cybersecurity maturity and vulnerabilities.
- Implemented automated supply chain risk scoring and continuous security monitoring.
- Identified weak links in the supply chain that could be exploited for cyberattacks.

## Threat Intelligence & Incident Response for Third-Party Risks

- Integrated real-time threat intelligence to detect and mitigate supply chain threats proactively.
- Established incident response playbooks for supplier-related security incidents and data breaches.
- Implemented network segmentation and access control measures to limit third-party exposure.

## Regulatory Compliance & Security Governance

- Ensured compliance with ISO 27001, NIST, GDPR, and industry-specific cybersecurity standards.
- Conducted supplier security audits and enforced cybersecurity clauses in vendor contracts.
- Developed security frameworks for third-party risk management and vendor accountability.

**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

**We're  
Hiring!**

## Security Awareness & Resilience Training

- Provided cybersecurity awareness training for procurement and supply chain management teams.
- Conducted red team exercises to simulate supplier-related cyberattack scenarios.
- Implemented best practices for secure data sharing, authentication, and vendor risk mitigation.

## Results

With COE Security's Supply Chain Security Review, the organization achieved:

- Stronger Third-Party Risk Management Identified and mitigated vulnerabilities within the supply chain ecosystem.
- Real-Time Threat Detection & Response Implemented proactive security monitoring for supplier-related risks.
- Regulatory Compliance Assurance Maintained adherence to ISO 27001, GDPR, and industry cybersecurity frameworks.
- Enhanced Supply Chain Cyber Resilience Strengthened security controls for vendors, partners, and suppliers.
- Improved Incident Preparedness Established robust response strategies for mitigating supply chain disruptions.





# 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!**

## Client Testimonial

COE Security's supply chain security expertise helped us uncover vulnerabilities in our vendor ecosystem and implement a proactive defense strategy. Their real-time monitoring, compliance support, and risk mitigation framework have been invaluable in strengthening our cyber resilience

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

*Joseph Henderson*

