CASE STUDY

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

Joseph Henderson

CASE STUDY

SECURING CI/CD PIPELINES THROUGH DEVOPS 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

We're Hiring!

Client Profile

A leading software development company with a DevOps-driven CI/CD pipeline relied on cloud-native infrastructure, containerized applications, and automated deployments to deliver software at scale. With rapid development cycles and multiple integrations, the company needed to ensure its DevOps environment was secure from misconfigurations, privilege escalations, supply chain threats, and insider risks.

Challenges Faced

Before undergoing DevOps Penetration Testing, the company identified several security concerns:

- Misconfigured CI/CD pipelines, allowing unauthorized code execution and privilege escalation.
- Hardcoded secrets and API keys, exposing sensitive credentials in repositories and build logs.
- Weak access controls in DevOps tools, enabling unrestricted access to critical environments.
- Unverified dependencies, introducing supply chain vulnerabilities in containerized applications.
- Insecure Kubernetes and Docker configurations, increasing risks of container breakouts and privilege escalation.
- Compliance concerns with ISO 27001, SOC 2, PCI DSS, and NIST DevSecOps guidelines.

Our Approach

To strengthen DevOps security, we conducted a comprehensive DevOps Penetration Testing engagement, identifying vulnerabilities and providing remediation strategies.

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:

- Scope of testing, including CI/CD pipelines, cloud environments, Kubernetes clusters, repositories, and DevOps tooling.
- Threat models specific to DevOps environments, such as insider threats, supply chain attacks, and privilege escalations.
- Testing methodologies, including Black Box, Gray Box, and White Box testing.

Security Testing Execution

Using MITRE ATT&CK for Cloud, OWASP DevSecOps, and NIST 800-190, we assessed:

- CI/CD Security – Testing Jenkins, GitHub Actions, and GitLab CI/CD.
- Secrets Management – Detecting exposed credentials and API keys.
- Container Security – Evaluating Docker, Kubernetes RBAC, and escape risks.
- IaC Security – Reviewing Terraform, Ansible, and Kubernetes YAML.
- Cloud Security – Testing IAM roles, S3 buckets, and network segmentation.
- Supply Chain Risks – Analyzing dependencies and package managers.
- Runtime Security – Identifying privilege escalation and attack paths.

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 misconfigurations and privilege escalations.
- 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

We're Hiring!

Remediation Support & Secure Hardware Development Best Practices

- Secure CI/CD pipeline configurations, enforcing least privilege and role-based access control (RBAC).
- Implementation of secrets management tools, such as Vault, AWS Secrets Manager, and GitHub Secrets.
- Container hardening recommendations, including non-root users, minimal base images, and runtime protections.
- Automated security scanning tools, like SAST, DAST, IaC security checks, and dependency scanning.
- Cloud security best practices, ensuring secure IAM policies, encryption, and network segmentation.
- Re-testing of critical vulnerabilities, ensuring proper remediation.

Results

Within six weeks, the company successfully:

- Eliminated all critical vulnerabilities, reducing the risk of cyber-physical attacks.
- Strengthened SCADA and PLC security, ensuring safe industrial operations.
- Hardened network architecture, preventing unauthorized access and lateral movement.
- Adopted a proactive OT security strategy, enhancing overall resilience.

Compliance & Continuous Security

- Stronger DevOps security posture, reducing risks of unauthorized access and supply chain threats.
- Compliance readiness for SOC 2, ISO 27001, PCI DSS, and NIST DevSecOps best practices.
- Improved monitoring and logging, ensuring real-time threat detection.

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 DevOps Penetration Testing expertise, we helped the software company proactively identify vulnerabilities, strengthen CI/CD pipeline security, and ensure compliance with industry regulations. Our structured approach, from threat modeling to remediation, ensured the DevOps environment remained resilient against modern 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