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 AWS CLOUD INFRASTRUCTURE THROUGH 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 fast-growing fintech company relied on AWS cloud infrastructure to host its customer-facing applications, databases, and payment processing systems. As the company scaled, it needed to ensure its AWS environment was secure from misconfigurations, unauthorized access, privilege escalations, and compliance violations. Given the sensitivity of financial data, achieving a robust AWS security posture was critical to meeting PCI DSS, SOC 2, and GDPR compliance requirements.

Challenges Faced

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

- Over-permissioned IAM roles and policies, increasing the risk of privilege escalation.
- Misconfigured AWS S3 buckets, potentially exposing sensitive customer data.
- Publicly accessible EC2 instances and databases, increasing risks of unauthorized access.
- Unrestricted security groups, allowing unnecessary inbound/outbound traffic.
- Weak encryption settings, leaving data at risk of exposure.
- Insecure API Gateway configurations, leading to unauthorized API access.
- Lack of centralized logging and monitoring, making threat detection difficult.
- Compliance gaps with AWS Security Best Practices, PCI DSS, ISO 27001, and NIST 800-53.

Our Approach

To enhance AWS security, we conducted a comprehensive AWS Penetration Testing engagement, identifying vulnerabilities and providing tailored 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 AWS IAM, EC2, S3, RDS, API Gateway, Lambda, CloudTrail, Security Groups, and VPC configurations.
- Threat models specific to AWS, such as misconfigurations, unauthorized privilege escalations, insider threats, and API security flaws.
- Testing methodologies, including Black Box, Gray Box, and White Box testing.

Security Testing Execution

Using industry-standard frameworks, we conducted in-depth AWS security testing, covering:

- IAM Security – Identifying weak policies and privilege escalation risks.
- S3 Security – Detecting misconfigurations and data exposure.
- EC2 Security – Assessing insecure access and vulnerabilities.
- VPC & Security Groups – Reviewing firewall rules and open ports.
- API Gateway Security – Evaluating authentication and input validation.
- Lambda Security – Assessing permissions and environment risks.
- Database Security – Ensuring access controls and encryption.
- CloudTrail & Logging – Validating monitoring and anomaly detection.
- Encryption & Data Protection – Reviewing KMS and data security.
- Compliance Gap Analysis – Mapping gaps to PCI DSS, SOC 2, and NIST.

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 AWS misconfigurations and escalate privileges.

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 Coding Practices

- IAM role and permission hardening, enforcing least privilege access controls.
- S3 bucket access restrictions, preventing public exposure of sensitive data.
- Network segmentation and firewall improvements, securing EC2 instances and databases.
- Secure API Gateway authentication and input validation, mitigating unauthorized API access.
- AWS Lambda function security improvements, reducing exposure to event-triggered attacks.
- Implementation of AWS Security Hub, GuardDuty, and CloudWatch for real-time threat detection.
- Re-testing of critical vulnerabilities, ensuring proper remediation and security hardening.

Compliance & Continuous Security

After implementing security fixes, the company achieved:

- Stronger AWS security posture, reducing risks of data breaches and privilege escalations.
- Compliance readiness for PCI DSS, SOC 2, ISO 27001, and NIST 800-53.
- Improved real-time threat monitoring and alerting, ensuring early detection of security incidents.

Results Achieved

Within six weeks, the company successfully:

- Eliminated all critical AWS security vulnerabilities.
- Hardened IAM roles and security policies, reducing privilege escalation risks.
- Secured S3 buckets, databases, and EC2 instances, preventing unauthorized access.
- Implemented cloud security best practices, ensuring ongoing AWS security resilience.

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 AWS Penetration Testing expertise, we helped the company proactively identify vulnerabilities, enhance AWS infrastructure security, and ensure compliance with industry regulations. Our structured approach, from threat modeling to remediation, ensured the AWS environment remained resilient against emerging 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