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 GCP SECURITY 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

Client Profile

A large healthcare technology company relied on Google Cloud Platform (GCP) to host its electronic health records (EHR), AI-driven diagnostics, and patient management systems. As the company expanded its cloud footprint, it needed to ensure its GCP environment was secure against misconfigurations, privilege escalations, unauthorized access, and data breaches. Given the highly sensitive nature of healthcare data, achieving HIPAA, HITRUST, and SOC 2 compliance was a top priority.

Challenges Faced

Key security concerns included:

- Overly permissive IAM roles and service accounts.
- Misconfigured Google Cloud Storage (GCS) buckets exposing PHI.
- Publicly accessible Compute Engine instances.
- Insecure Cloud SQL configurations leading to data leakage.
- Weak API Gateway authentication mechanisms.
- Unrestricted firewall and VPC rules.
- Limited security logging visibility.
- Compliance gaps with HIPAA, HITRUST, SOC 2, and ISO 27001.

Our Approach

To strengthen GCP security, we conducted a comprehensive GCP Penetration Testing engagement, identifying vulnerabilities and providing tailored 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

Scoping & Threat Modeling

We collaborated with the client to define:

- Scope of testing, including IAM, Google Cloud Storage (GCS), Compute Engine, Cloud SQL, API Gateway, VPC configurations, and Kubernetes Engine (GKE).
- Threat models specific to GCP, such as misconfigurations, privilege escalations, API vulnerabilities, and insider threats.
- Testing methodologies, including Black Box, Gray Box, and White Box testing.

Security Testing Execution

- Using industry frameworks, we conducted GCP security testing covering:
- IAM – Identifying excessive permissions and escalation risks.
- GCS – Detecting public access and data exposure.
- Compute Engine – Assessing insecure access and vulnerabilities.
- Firewall & VPC – Reviewing open ports and unauthorized access.
- API Gateway – Evaluating authentication and input validation.
- GKE – Assessing RBAC and container security.
- Cloud SQL – Ensuring secure access and encryption.
- Logging & Security – Validating monitoring and anomaly detection.
- Encryption – Reviewing KMS and data security.
- Compliance – Mapping gaps to HIPAA, HITRUST, SOC 2, ISO 27001.

Findings & Risk Assessment

- Critical, High, Medium, and Low-risk vulnerabilities, with business impact analysis.
- Proof-of-Concept (PoC) exploits, demonstrating how attackers could exploit misconfigurations and escalate privileges.
- A prioritized remediation roadmap, helping the company address security issues efficiently.

We're Hiring!

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

- To ensure continuous security in GCP, we provided:
- IAM role and service account hardening, enforcing least privilege access controls.
- GCS bucket access restrictions, preventing public exposure of sensitive data.
- Network segmentation and firewall improvements, securing Compute Engine instances and databases.
- Secure API Gateway authentication and input validation, mitigating unauthorized API access.
- GKE security hardening, implementing role-based access control (RBAC) and workload identity.
- Implementation of Security Command Center and Chronicle SIEM for real-time threat detection.
- Re-testing of critical vulnerabilities, ensuring proper remediation and security hardening.

Compliance & Continuous Security

- Stronger GCP security posture, reducing risks of data breaches and privilege escalations.
- Compliance readiness for HIPAA, HITRUST, SOC 2, and ISO 27001.
- Improved real-time threat monitoring and alerting, ensuring early detection of security incidents.
- Proactive cloud security management, establishing continuous security monitoring and risk management practices.

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.

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