# 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 ALIBABA CLOUD 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 global e-commerce and logistics company used Alibaba Cloud to host online marketplace, customer data, and payment systems. The company sought to secure its infrastructure from misconfigurations, unauthorized access, privilege escalation, and compliance violations, ensuring compliance with PCI DSS, GDPR, ISO 27001, and China's Cybersecurity Law (CSL).

## Challenges Faced

Key security concerns included:

- Over-privileged RAM roles and risk of privilege escalation
- Misconfigured OSS buckets exposing sensitive data
- Public ECS instances and unauthorized access risks
- Weak security in ApsaraDB for RDS, risking data leakage
- Insecure VPC configurations allowing unrestricted traffic
- Unprotected APIs vulnerable to exploitation
- Limited monitoring and logging for threat detection
- Compliance gaps with PCI DSS, GDPR, ISO 27001, and CSL

## Our Approach

We conducted a comprehensive penetration testing engagement, 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 Alibaba RAM, ECS, OSS, RDS, API Gateway, VPC, and Container Service for Kubernetes (ACK).
- Threat models specific to Alibaba Cloud, such as misconfigurations, privilege escalations, API vulnerabilities, and insider threats.
- Testing methodologies, including Black Box, Gray Box, and White Box testing.

## Security Testing Execution

- RAM Testing – Identifying excessive IAM permissions.
- OSS Testing – Assessing public access and data exposure risks.
- ECS Testing – Identifying insecure SSH/RDP access.
- Security Group & VPC – Reviewing firewall rules and access points.
- API Gateway Testing – Assessing API authentication flaws.
- ACK Testing – Evaluating RBAC and container vulnerabilities.
- ApsaraDB RDS Testing – Ensuring secure database access.
- CloudMonitor & Security Center – Ensuring proper logging and monitoring.
- Encryption & Data Protection – Evaluating KMS and encryption.
- Compliance Gap Analysis – Mapping findings to PCI DSS, GDPR, ISO 27001, and CSL.

## 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 Alibaba Cloud 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

## Remediation Support & Secure Coding Practices

- To ensure continuous security in Alibaba Cloud, we provided:
- RAM role hardening, enforcing least privilege access controls.
- OSS bucket access restrictions, preventing public exposure of sensitive data.
- Network segmentation and firewall improvements, securing ECS instances and databases.
- Secure API Gateway authentication and input validation, mitigating unauthorized API access.
- Alibaba Kubernetes Service (ACK) security enhancements, improving container security and RBAC policies.
- Implementation of Security Center and CloudMonitor 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 Alibaba Cloud security posture, reducing risks of data breaches and privilege escalations.
- Compliance readiness for PCI DSS, GDPR, ISO 27001, and CSL.
- 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

- Fixed all critical Alibaba Cloud vulnerabilities.
- Strengthened RAM roles and policies, reducing escalation risks.
- Secured OSS, RDS, and ECS instances, preventing unauthorized access.
- Applied cloud security best practices for ongoing 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 Alibaba Cloud Penetration Testing expertise, we helped the company proactively identify vulnerabilities, enhance Alibaba Cloud infrastructure security, and ensure compliance with industry regulations. Our structured approach, from threat modeling to remediation, ensured the Alibaba Cloud environment remained resilient against emerging cyber threats.

## COE Security LLC

COE Security is a leading cybersecurity services provider offering comprehensive solutions to address evolving threats. We help organizations mitigate risks, strengthen defenses, and recover from cyberattacks. Our experienced team possesses deep expertise in the latest technologies and best practices, delivering tailored solutions to meet unique security needs.

Given the complexities of cloud environments like Alibaba Cloud, specialized security testing is crucial.

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

*Joseph Henderson*

COE SECURITY