QBurst | A High AI-Q™ Company

Cloud Security and Compliance Modernization

A comprehensive cloud security modernization and compliance enablement program, upgrading the client's legacy infrastructure, integrating continuous monitoring, and achieving critical SOC 2 and ISO 27001 certifications.

Overview

- **Certification Achievement:** Successfully achieved both SOC 2 and ISO 27001 certifications within aggressive timelines, opening doors to new enterprise markets.
- **Security Modernization:** Upgraded critical legacy systems (Ubuntu 14, PHP 7.3, EKS) and implemented robust security processes, including SAST, DAST, and vulnerability management.
- **Enterprise Trust:** Strengthened the client's reputation and led to direct revenue growth attributed to compliance certification, attracting inquiries from Fortune 500 companies.

Client Profile

The client provides an end-to-end messaging platform for guest and property management in the hospitality industry.

Challenges

- **Crippling Technical Debt:** Core systems were running on critically outdated software (e.g., Ubuntu 14, PHP 7.3, old EKS clusters, and Jenkins), posing immediate security risks.
- **Missing Security Controls:** There was no formal security program in place, lacking essential tools like Static and Dynamic Application Security Testing (SAST/DAST), intrusion detection, and strict access controls.
- **Non-Compliance:** The absence of Multi-Factor Authentication (MFA), proper data safeguards (pseudonymization, masking), and a tested disaster recovery (DR) plan made passing compliance audits impossible.

- **Manual Auditing:** Lacked continuous compliance monitoring or automated vulnerability management, slowing processes and increasing administrative burden.

QBurst Solution: A Comprehensive Security and Compliance Modernization Program

We embedded security practices (DevSecOps) across the client's entire infrastructure, application layer, and governance framework to ensure audit readiness for SOC 2 and ISO 27001.

Key Components

- **Infrastructure Upgrade:** Completed a comprehensive migration of outdated EC2s, PHP backend, EKS clusters, and the Jenkins CI/CD pipeline to current, supported versions.
- **Code Security Integration:** Automated code security by integrating SonarQube for SAST and Detectify for DAST directly into the continuous integration pipelines.
- **AWS-Native Security:** Enabled and configured powerful AWS native security services, including GuardDuty (threat detection), Security Hub (compliance checks), and Inspector (vulnerability assessment).
- **Continuous Compliance:** Integrated Vanta to automate compliance monitoring, providing real-time visibility into controls and reporting.

Technical Highlights

- **Continuous Compliance Automation:** Deployed Vanta to automatically monitor security controls and gather evidence, vastly simplifying the auditing process.
- **Vulnerability Management:** Established a streamlined vulnerability management process with SLA-based patching cycles across all environments.

- **Data Protection & DR:** Implemented data pseudonymization, masking, enforced Multi-Factor Authentication (MFA), and established a fully tested disaster recovery plan.
- **Governance and Access Control:** Enforced a least-privilege access model using AWS IAM and ensured all security services were configured for real-time protection.

Impact: Ensuring Compliance, Security, and Operational Reliability

- **Certification Achievement:** Successfully achieved the required SOC 2 and ISO 27001 certifications, officially validating the client's security posture.
- **Increased Enterprise Client Confidence:** The certification and strengthened security led to increased enterprise client confidence, resulting in direct inquiries and revenue opportunities from Fortune 500 companies like Reliance and ITC.
- **Strengthened Security Posture:** The implementation of SAST, DAST, and AWS-native tools significantly strengthened overall security and resilience against cyber threats.
- **Improved Operational Reliability:** The modernization of the infrastructure and the tested Disaster Recovery plan improved operational reliability.
- **Direct Revenue Growth:** The compliance certification became a direct enabler for revenue growth by opening access to enterprise markets. It increased the rate of successfully closed enterprise deals by over 55%.