# Qualitest's Shift-Left Cyber Solutions Secure Cloud Infrastructure and SDLC for a Top Insurance Company

### Challenge

Secure the Client's cloud infrastructure.

Secure the SDLC from the earliest stages. Achieve full compliance with industry and government regulations.

### Solution

Defined best practices for cloud security based on AWS and Kubernetes, validated the cloud environment.

Identified best practices and performed SAST and DAST to detect security flaws at build and production stages. Identified PCI DSS compliance best practices.

### Results

Detected and fixed cloud environment security flaws.

Identified and corrected security flaws, compliance gaps and risks with shift-left approach and integrated DevSecOps tools. Framework for SSDLC, security and compliance can be leveraged going forward.

The Client is a leading service provider for personal and commercial insurance in the UK. Serving millions of policyholders, the company generates premiums worth billions of Euros.

The Client lacked the robust cyber security system imperative to handle massive amounts of sensitive customer data. Their approach--performing penetration testing at the end of the development lifecycle—was proving too expensive to fix issues and did not provide complete cyber security coverage.

## Robust Cyber Security Starts with a Robust Shift-Left Plan

The Client wanted consistency in their cyber security processes by addressing cyber security requirements as early as possible in the SDLC, but the requirements had not been properly defined. Qualitest helped the Client define requirements and then collaborated to build a robust cyber security plan that would secure the cloud infrastructure as well as the development lifecycle, and also satisfy compliance regulations.

The plan called for implementing cyber security testing solutions in the build pipeline and the cloud infrastructure in one key release, and then leveraging the solutions for subsequent releases and projects.

The Client wanted to:

- Establish a QA partner with strong knowledge and experience in shift-left cyber security implementation.
- Understand the current tools and technologies used.

> **“The Client wanted consistency in their cyber security processes by addressing cyber security requirements as early as possible in the SDLC, but the requirements had not been properly defined.”**

- Identify best practices for cloud security, secure the development lifecycle and meet compliance requirements.
- Map the process with people, process, and technology.

## Tackling Three Security Areas with a Three-Phased Approach

Qualitest divided the requirements into three areas: Cloud security, secured software development lifecycle (SDLC) and compliance security. The requirements for all three areas were met in three phases.

- Phase 1 – Discovery
- Phase 2 – Design & Preparation
- Phase 3 – Execution, Analysis & Reporting

## Phase 1 – Discovery

Qualitest engineers held technical workshops to gain a thorough understanding of the client's technology landscape, the tools being used and the current SDLC and SSDLC structure. At the end of this phase, we provided a detailed Gap Analysis report identifying where we saw gaps against best practices for each key area.

We also identified the key stakeholders with whom we would be working. Finally, we created a detailed test plan listing the activities to be performed.

## Phase 2 – Design & Preparation

Qualitest engineers came up with a detailed check-list for each area, based on the best practices relevant to the area.

### Cloud Security Checklist

- **AWS Infrastructure Best Practices**
  - Account monitoring and control
  - Users and groups management through IAM policies
  - Logging and monitoring
  - Networking - Virtual Private Cloud (VPC)
  - Managed services & continuous vulnerability management
  - AWS S3 & EC2
  - API gateway

- **Kubernetes Best Practices**
  - Limit direct access to Kubernetes Nodes
  - Create administrative boundaries between resources
  - Use authorized images

### Secure Development Lifecycle Checklist

- **Secure Coding Best Practices**
  - Authentication and Authorization
  - Input Validation
  - System Output
  - Data Storage
  - Services and websites
  - Logging
  - Unintended security disclosure requirements
  - Communication, Error Handling
  - Data Processing and Protection
  - File Management, Session Management and Memory Management

- **SAST (Static Application Security Testing)**

- **DAST (Dynamic Application Security Testing)**

- **Secure Build Pipeline**

### Compliance Checklist

- PCI DSS (Payment Card Industry Data Security Standard) Best Practices
  - Vendor-Supplied default credentials
  - Track and monitor network resource
  - Common code vulnerabilities
  - Payment Card Information

Additionally, in this phase we identified the tools we planned to use.

## Phase 3 – Execution, Analysis & Reporting

In the final phase, Qualitest engineers executed the checklists and the tasks prepared for the three areas that required Cyber QA.

## Cloud Security

- The checklist prepared was executed on the AWS environment.
- The Nexpose, Prisma Cloud and Splunk tools were leveraged for the execution.
- All the execution details were captured in Jira Tool.
- All the failed checklist items had a defect raised in Jira and assigned to the platform engineers to fix the vulnerability at the infrastructure level.

## Secure Development Lifecycle

- SAST
  - An open source tool was used for the SAST execution.
  - The rules and profiles defined were reviewed to get maximum coverage.
  - Leveraged security plugin for better cover age and mapping with the CVEs and CWEs.
- DAST
  - NeuraLegion Nexploit was leveraged for the DAST testing.
  - An opensource DAST scanning tool was leveraged as well for the DAST testing.
  - Micro services were scanned to cover Top 10 OWASP methodology for APIs through automated scanning.
  - Performed Fuzzing using open source DAST Scan tool.
  - All the vulnerabilities identified were raised on Jira and assigned to the developers to fix.
- Secure Build Pipeline
  - Open source Software Composition analysis and Git Secrets verification tools were identified to integrate with build pipeline.
  - Software Composition analysis was leveraged to identify if any components with known vulnerabilities are used in the development environment.
  - Git Secret verification tool was used to detect if any secret keys or other sensitive information was checked into the Git by calculating the entropy.
- Secure Coding Principles
  - Executed the checklist by leveraging the SAST and DAST tools.
  - Executed some of the checklist manually to identify vulnerabilities.
  - All the vulnerabilities identified were raised on Jira and assigned to the developers to fix.

## Compliance

- **PCI DSS**
  - The PCI DSS checklist prepared was executed on the AWS environment and Micro Services.
  - The Nexpose, Prisma Cloud, Splunk and OWASP ZAP tools were leveraged for the execution.
  - All the vulnerabilities identified were raised on Jira and assigned to the developers and Platform Engineers to fix.

# Results: A Reusable, Reliable Security Framework

The Client was pleased with the output of the cyber security Proof of Concept. Soon afterward we began discussions for a yearlong project to implement similar solutions for different projects.

## Key Benefits

- **Better definition of roles and responsibilities for engineering and security** resulted by the creation of a smoother interface between the two. This helped avoid requirements traceability issues, which was the most significant root cause of defects in the first wave of testing.
- **Identified vulnerabilities in build and production stages of the development lifecycle** by shift-left cyber security and performing SAST and DAST scan on the Micro services.
- **Secured the build pipeline and identified any vulnerabilities at the pipeline level** by integrating Software composition Analysis and the GitSecret verification tools.
- **Identified discrepancies in terms of secure coding principles** and pointed out possible vulnerabilities.
- **Created a defined, shift-left framework for cyber security** that could be easily utilized and leveraged for other projects.
- **Engineering and INFOSEC teams started to work closely together** to ensure solutions were designed to be secure with clear cyber requirements.

The Client now has a cyber testing service that is continually improving, is able to flex to demand and has mitigated significant cyber risk.

> **“The Client was pleased with the output of the cyber security Proof of Concept. Soon afterward we began discussions for a yearlong project to implement similar solutions for different projects.”**

QUALITEST

**Connect with Us**

www.qualitestgroup.com

https://www.linkedin.com/company/qualitest

https://www.instagram.com/lifeatqualitest

https://twitter.com/Qualitest

https://www.facebook.com/Qualitestgroup