QUALITEST™

Leading News Agency Elevates Their Defense Posture with Shift-Left Cyber Security

When a leading news agency encountered significant challenges with a lack of a "shift-left" approach in their development pipeline, Qualitest defined a security-first approach to their testing needs.

Challenges

The organization had a lack of shift-left approach and automated security testing.

In addition, they did not have a consistent penetration testing approach or defined security test cases.

Solutions

Integrated security into SDLC by adapting and leveraging a "Shift Left" approach.

Implemented a standardized approach to penetration testing across all applications and created comprehensive security controls test cases tailored to the applications.

Results

Automated security testing significantly reduced the time and effort expended on application security.

Multiple critical and high vulnerabilities were identified and most of them were addressed, leading to a more secure production environment.

Client overview

Our Client is an American not-for-profit news agency headquartered in New York City. It is an independent global news organization dedicated to factual reporting. The agency today remains the most trusted source of fast, accurate, unbiased news in all formats and the essential provider of the technology and services vital to the news business.

Strengthening cyber defenses with a shift-left mindset and penetration testing

Our Client was primarily focused on penetration testing towards the end of their development life cycle. However, penetration testing isn't consistent and is usually conducted on a yearly or half-yearly basis, rather than rolling it out on all major releases.

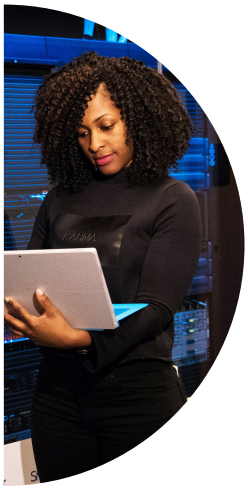
There was an absence of a "shift-left" approach or any integrated automated security testing in their development pipeline.

Our Client did not engage in any security testing at the infrastructure level. This resulted in critical systems and assets being exposed to potential vulnerabilities. Our Client also did not have any security non-functional requirements defined or any security-specific test cases designed. Without these, it is difficult to systematically identify and address potential vulnerabilities in their applications.

Qualitest was engaged to proactively identify and address security vulnerabilities in the initial stages of the development life cycle by integrating a 'shift-left' approach to security. This approach not only minimized the time and effort spent on application security, but also substantially reduced the overall risk associated with the applications.

It was important for our Client to:

- Establish a quality assurance partner with strong knowledge and experience on shift-left cyber security implementation.
- Understand the current tools and technologies used within their organization.
- Define best practices on their Secure Development Life Cycle including SCA, SAST and DAST, security controls, penetration testing and cloud security.
- Map their shift left and cyber security work with the three P's - people, process, and technology.
- Implement the solution and validate their requirements on all four areas they needed including the Secure Development Life Cycle, security controls, penetration testing and cloud security.



Implementing a shift-left approach for greater security coverage

To address our Client's requirements on cyber security, Qualitest segregated their requirements into four different areas:

- Secure development life cycle (SCA, SAST, DAST)
- Security controls testing (business-logic flaws
- Penetration testing (Release-Level)
- Cloud security audit

The requirements for all 4 areas were met through the following stages:

1. Define best practices
2. Map people, process and technology
3. Validate the requirements
4. Continuous improvement

Stage 1 – define best practices

This is the first stage in security testing which captures all the details on how to qualify a security testing requirement. They are broadly categorized into 2 main areas, which included a secure development life cycle and infrastructure security.

Stage 2 – map people, process and technology

Mapping people, process and technology took our Client's requirements from the define best practices phase and we worked towards selecting the tools, methods, technology, and the overall process of how the validation should be performed.

Stage 3 – validate the requirements

This is the final stage where the execution of all the security requirements took place. The result of defining best practices, mapping it against people, process and technology and validating these requirements happened in this stage.

The validation of the requirement includes all 4 areas i.e. secure development life cycle, security controls, penetration testing and cloud security.

Stage 4 – Continuous Improvement

Cyber security requires regular reviews, updates, and enhancements to address emerging threats, vulnerabilities, and the evolving technological landscape. This is all conducted as part of the continuous improvement stage.

In this stage we also ensured that the SCA, SAST and DAST tools are regularly updated. Once an application has been scanned with any genuine issues having been differentiated from the false positives, this is used as a baseline. Subsequent scans can then be compared to the baseline to identify any new issues, minimizing the repeated triage of false positives. We also ensured any existing vulnerabilities that were identified through security controls testing and penetration testing were converted into a DAST scan template and integrated into the CI/CD pipeline.

Key benefits

- 500+ vulnerabilities found with 50% of them fixed and classed as critical vulnerabilities through performing SCA (Software Composition Analysis) and SAST (Static Application Security Testing) on all the source code repositories.
- Real-time attack simulation was improved by 60% through automation via DAST (Dynamic Application Security Testing) scanning on multiple web applications and APIs.
- 100+ critical and high severity vulnerabilities were identified and fixed through the implementation of relevant security controls and penetration testing on multiple web applications and APIs covering advanced attacks and business logic flaws.
- A 40% improvement in the identification of vulnerabilities in applications for our Client was made to stop attackers from downloading content from their website without making any payment for it.
- A 30% improvement was made to the launch of a defect management portal and separate dashboard for logging vulnerabilities found and fixed. Additional security testing coverage was provided as part of DAST scans to identify automated vulnerabilities.