Blueinfy

IMPLEMENTING COMPREHENSIVE APPLICATION SECURITY PROGRAM FOR ACME – PHARMA COMPANY

BACKGROUND

ACME is a global pharmaceutical company overseeing more than 30,000 domains. The company operates a diverse portfolio, including critical applications related to vaccine sales and lower-priority platforms like cafeteria surveys. The new CISO faced a significant challenge: determining how to best allocate resources for application security amid a lack of compliance requirements, no existing pen-testing program, and a general absence of strategic focus. Additionally, ACME had limited knowledge about its technology stack and faced issues with SSL certificate configurations.

CHALLENGE

1. Resource Allocation Dilemma

The CISO needed to decide whether to invest more in securing high-value applications like those related to vaccine sales or lower-priority ones like cafeteria surveys, which might not pose immediate risks but could still impact the brand.

2. Lack of Structured Security Program

ACME lacked a strategic approach to application security, resulting in reactive rather than proactive measures. Without regulatory compliance driving security practices, there was no structured pen-testing or regular scanning in place.

3. Knowledge Gaps and Technology Issues

The company had limited understanding of the technology stack used across its domains. Even an inconsistent SSL certificate configurations across domains posed potential security risks.

4. Inadequate Scanning Practices

Scans were performed on-demand by the application team without a comprehensive strategy, leading to incomplete vulnerability management.

SOLUTION

Blueinfy was enlisted to create and implement a detailed multiyear application security program to address ACME's multifaceted challenges.

Phase 1: Comprehensive Domain Profiling and Risk Assessment

1. Domain Profiling through Data Collection and Public Data Analysis

Blueinfy conducted an in-depth profiling of all 30,000+ domains (which was collected as part of DNS dumps and proprietary methodologies which gathers information from public domains). This involved collecting 60 different data points, including information about the technology stack and SSL certificate status.

2. Asset Base Reduction

Identification of expired or non-essential domains allowed ACME to streamline its application asset base, focusing on domains that required attention.

3. Risk Assessment

Blueinfy worked closely with ACME to assign risk levels to each domain (High, Medium, Low) based on predefined criteria such as handling PII, PHI, login functionalities, and e-commerce.
A new policy was developed, mandating regular scans and pen-testing based on the risk rating of each domain, ensuring that high-risk domains received prioritized attention.

4. Vulnerability Discovery

The profiling identified domains hosting viruses due to sub-domain takeover vulnerabilities.
Numerous SSL certificate-related vulnerabilities were discovered, including expired certificates and misconfigurations.
Numerous domains were discovered where admin interface were accessible with default credentials.
Phase 2: Implementation of DAST Scanner and Pen-Testing

1. DAST Scanner Evaluation and Implementation

Blueinfy assessed various DAST (Dynamic Application Security Testing) scanners to find the best fit for ACME's needs.
The chosen DAST scanner was implemented, with Blueinfy assisting in configuring and fine-tuning scan profiles to enhance accuracy and effectiveness.
Detailed evaluations were conducted to eliminate false positives and ensure actionable results.

2. Pen-Testing

Comprehensive pen-testing was performed on all high-risk domains identified during Phase 1. This included manual and automated testing to have comprehensive security review to uncover complex vulnerabilities and actionable report with zero false positives.

RESULTS

1. Enhanced Security Posture

The structured approach led to significant improvements in the security of ACME's application assets, with critical vulnerabilities being addressed and mitigated.

2. Strategic Resource Allocation

ACME was able to make informed decisions about where to allocate resources, ensuring that high-value applications received the necessary protection while reducing the focus on lower-priority domains.

3. Improved Security Measures

The implementation of a DAST scanner and pen-testing processes established a more robust security framework, leading to better management of vulnerabilities and improved overall security.

4. Operational Efficiency

The reduction of domains and optimized scanning practices led to more efficient operations and a more manageable security environment.

CONCLUSION

By partnering with Blueinfy, ACME successfully addressed its application security challenges with a well-structured phase wise plan. The comprehensive profiling and risk assessment in Phase 1 provided a clear understanding of the security landscape, while the implementation of a DAST scanner and pen-testing in Phase 2 enhanced the company's security posture. The approach not only optimized resource allocation but also established a strategic focus on application security, positioning ACME to better protect its diverse range of domains and applications.

Article by Hemil Shah