Blueinfy

RUNNING AND ENHANCING APPLICATION SECURITY PROGRAM FOR AN INVESTMENT COMPANY

COMPANY OVERVIEW

ACME is a prominent investment company with a diverse portfolio, spanning three major business lines and over 50 brands. The company sought to implement a robust global application security program to safeguard its digital assets and enhance its overall security posture.

Existing Security Program
ACME's existing application security framework included:

Regular application penetration testing conducted by external vendors.
A program intended to manage and respond to reported vulnerabilities.

Despite these measures, ACME faced significant challenges:

The average time to resolve critical or high-risk vulnerabilities was 98 days.
The internal Application Security (AppSec) team consisted of only two members, one of whom left during the assessment period.

CHALLENGES IDENTIFIED

1. Inadequate Application pen testing quality
The external vendor's application pen testing was more like a Dynamic Application Security Testing (DAST) scans which even did not effectively manage false positives, compromising the integrity of the pen-testing results. This resulted in push back from brands which was very obvious.

2. VDP Scope Issues
The VDP program had inaccuracies in the domain list, and not all domains were included, resulting in incomplete vulnerability coverage.

3. Communication Gaps
There was a lack of clear communication and follow-ups with Business Units (Bus), leading to delayed responses and unresolved vulnerabilities.

4. Absence of Management Reporting
ACME management did not receive comprehensive management reports, affecting the visibility of security issues and progress.

5. Incomplete Pen-Test Scope
The scope of pen-tests was sometimes incomplete, with certain domains omitted from the assessment.

Obviously, there seems to be huge gap in application security program and one can say, the program was not in good shape.

STRATEGIC APPROACH BY BLUEINFY

To address these issues, Blueinfy was brought in to revamp ACME's application security program with a strategic and multi-faceted approach:

1. Building Stronger BU Relationships
Blueinfy established direct communication channels with BUs to ensure that critical and high-risk vulnerabilities were addressed promptly.
Implemented a structured process to enforce vulnerability fixes, leading to a remarkable reduction in resolution times from 98 days to just 4 days within the first year.

2. Enhancing Pen-Test Quality
Worked closely with the existing vendor to improve the quality and accuracy of pen-test results. This included refining the DAST scanning process and ensuring effective management of false positives.

3. Refining VDP Scope
Corrected inaccuracies in the VDP domain list to ensure complete coverage of all relevant domains.
Updated the VDP program to include all necessary domains, enhancing vulnerability management.

4. Improving Communication and Documentation
Created comprehensive documentation, including policies and FAQs, to provide BUs with clear instructions and improve communication.
Implemented a robust follow-up mechanism to ensure timely resolution of vulnerabilities and effective coordination with Bus.

5. Scope Verification
Worked with BUs to confirm and refine the scope of pen-tests, ensuring that all relevant domains were included in the assessments.

RESULTS ACHIEVED

Significant Reduction in Resolution Time
The time to fix critical and high-risk vulnerabilities was reduced from 98 days to 4 days within the first year, demonstrating a substantial improvement in response efficiency.

Enhanced Pen-Test Quality
Improved the accuracy and reliability of pen-test results through better management of false positives and refined testing processes.

Complete VDP Coverage
Achieved accurate and comprehensive domain coverage in the VDP program, leading to more effective vulnerability management.

Better Communication and Documentation
Established clear guidelines and improved communication with BUs, facilitating faster resolution of security issues.

Scope Accuracy
Ensured that pen-test scopes were complete and accurate, covering all relevant domains.

PROGRAM ENHANCEMENT IN THE SECOND YEAR

To further advance ACME's application security program, Blueinfy implemented the following measures:

1. Pen-Testing
Blueinfy took over the pen-testing process to deliver higher quality and more accurate results, leveraging Blueinfy's expertise.

2. Quarterly DAST Scans
Established a quarterly DAST scanning program, including false positive removal, to ensure ongoing security assessment.

3. Risk-Based Approach to save cost
Implemented a risk-based approach, where high-risk applications were prioritized for pen-testing, and medium/low-risk applications were scanned using DAST.
Optimized resource allocation by focusing efforts on high-risk areas and utilizing automated scans for less critical assets.

4. Management Dashboard
Collaborated with ACME's development team to create a management dashboard using Google Objects, providing better visibility and reporting on application security metrics.

5. On-Demand SAST Program
Implemented a Static Application Security Testing (SAST) program for on-demand code scanning, enhancing the ability to detect and address security issues early in the development process.

CONCLUSION

Through a combination of strategic improvements and tactical execution, Blueinfy successfully enhanced ACME's global application security program. The comprehensive approach led to substantial reductions in vulnerability resolution times, improved quality of pen-testing and scanning, and better overall management of application security. The ongoing program enhancements have positioned ACME to effectively manage its security posture and respond proactively to emerging threats, ensuring a robust defense against potential vulnerabilities.

Article by Hemil Shah

Web: www.blueinfy.com **Blog:** blog.blueinfy.com