GAVS

CASE STUDY

Robust Application Security with DevSecOps

for Healthcare Improvement Company

Client Overview

The client is a leading healthcare improvement company uniting an alliance of several U.S. hospitals, health systems, and other providers & organizations to drive transformation in healthcare.

The Business Situation

The client has a large portfolio of 65+ healthcare products used by hospitals and other providers. Application security across these healthcare products was of primary concern. They required an assessment of the current state of application security, followed by an end-to-end solution to fortify their internal and external facing applications through continuous testing, monitoring, periodic enhancements, and proactive protection from security breaches.

The Solution

With extensive expertise and rich experience in cyber security and data protection solutions for the healthcare domain, GAVS provided end-to-end application security, threat mitigation, and proactive data protection through a multi-pronged approach. Given below are the different solution components:

- Integration of Security into the CI|CD Pipeline for scanning of all the different code components (DevSecOps)
- Static Application Security Testing (SAST) involving detailed white box testing to detect & address code level vulnerabilities
- Dynamic Application Security Testing (DAST) involving black box testing of the entire application stack
- Manual & Automated Roadmap for Interactive Application Security Testing (IAST)
- Enterprise-level Application Security Testing Scanners: Burp Suite Enterprise Edition, Black Duck by Synopsys (Software Composition Analysis), Checkmarx Enterprise Edition
- Testing Methodologies based on Global Security Frameworks: OWASP Top 10, SANS, NIST
- Continuous Updates & Enhancements in mapping of controls based on Governance, Risk & Compliance

To find out how GAVS can help your organization, please visit **www.gavstech.com**

Challenges

- Several security vulnerabilities across applications
- Lack of visibility into threat landscape
- Reactive approach to application security and data protection

Solution Highlights

- Integration of security into the development pipeline through DevSecOps
- Continuous testing for vulnerabilities at the code level and across the application stack
- Static, dynamic, and interactive application security testing
- Enterprise-level application security testing scanners
- Testing methodologies based on global security frameworks
- Periodic updates & enhancements in GRC-based mapping of controls

Solution Outcomes

- End-to-end application security: validation on internal & external facing applications
- Continuous testing & monitoring of security vulnerabilities at the code & application levels
- Proactive remediation of critical findings at the development stage itself
- Prevention of data breaches through continuous assessment
- Robust data protection & threat mitigation
- Regular security architecture reviews & enhancements through threat modeling