STRENGTHENING CYBERSECURITY IN SINGAPORE'S GOVT. HEALTHCARE ORGANIZATION THROUGH DEVELOPMENT TEAM'S SECURITY TRAINING

Security Awareness Training For Development Teams | Case Study

ABOUT THE CLIENT

The Client is a centralized system that stores & shares healthcare data electronically and allows only authorized professionals to access patient records from different healthcare providers. The system aims to improve care quality, reduce medical errors, and enhance patient safety.

BUSINESS REQUIREMENT

With the increasing prevalence of cyber threats and the growing complexity of software applications, the client sought to empower its developers with the knowledge and skills needed to write secure code and mitigate potential security risks proactively.

TOOLS COVERED

- Nmap
- Nessus
- Rapid 7
- Qualys
- Kali Linux
- Burp Suite Pro
- OWASP Zap
- Acunetix
- Microsoft Threat Modeling Tool
- Threat Dragon
- Wireshark
- SSL Scan
- Sqlmap
- Postman
- Semgrep
- Fortify On Demand
- Veracode

50% Faster Results

40% Lesser Costs

Comprehensive security training and awareness programs for the Development team

KEY FEATURES



Assessment of Training Needs: Our team assessed the development teams' training needs, evaluated skill levels, identified weaknesses & determined relevant security topics.



Customized Training Curriculum: A tailored curriculum was created, covering secure coding practices, common vulnerabilities, secure design principles & security best practices.



Interactive Training and Workshops: Conducted interactive sessions and workshops, engaging participants with practical exercises, real-world examples & hands-on learning.



Ongoing Support and Resources: Access to online tutorials, reference guides & security tools, for continuous learning and collaboration.

RESULTS

Increased Security Awareness: Raised awareness and understanding of security principles and secure coding among developers.

Improved Code Quality: Security integration in the SDLC improved code quality, with developers being able to proactively address vulnerabilities early.