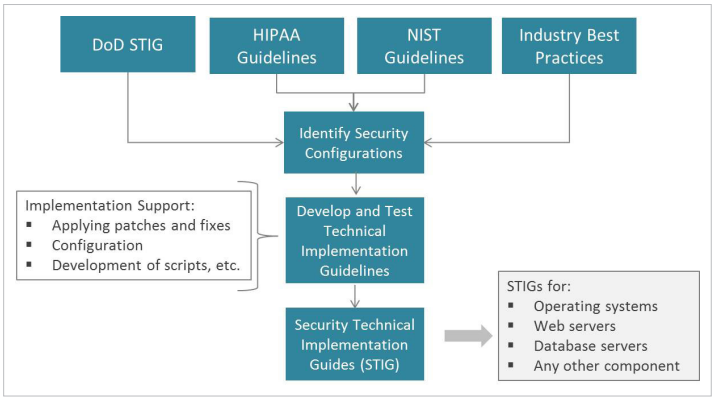
Case Study: Security Testing and Management for Medical Devices

Client Requirements

Client is a leading provider of medical diagnostics systems. Client required assistance in meeting US Department of Defence (DoD) and FDA compliance on cybersecurity for its CT scan devices. Client faced challenges with Authorized Device Dealers (ADD) installing unapproved software as freebies and top-ups and tampering client software to win hospital/ clinic purchase contracts.

CitiusTech was chosen to design and develop a secure installation process. CitiusTech enabled the client to achieve the latest industry and government mandates, improve overall security and compliance by implementing Security Technical Implementation Guides (STIGs), considering the type of systems under scope. To meet the FDA guidelines (Post Management of Cybersecurity in Medical Device), CitiusTech was also assigned the task of developing security patch management process.



CitiusTech Solution

Requirement Analysis

NIST guidelines for Risk Management Framework (RMF) were throughly analyzed with reference to system under scope. List of applicable security and privacy controls were identified and tailored for balancing device performance with cybersecurity risk. Analysis ensured that residual risk was acceptable with overall low cost of developing security and privacy controls. Secure installation involved in-depth understanding and literature survey of various strategies based on Public Key Infrastructure (PKI), Trusted Platform Module (TPM), OpenPGP and OpenSSL.

CitiusTech team studied FDA guidelines, 'cybersecurity for networked medical devices containing off-the-shelf (OTS) software and industry best practices including 'Information Technology — Security Techniques — Vulnerability Handling Processes to engineer Security Patch Management Process.

Solution Design

- Provided consulting service with implementation support for DoD STIGs configuration standards
- Performed security assessment of the STIGs including automated and manual testing
- Finalized a secure installation strategy and developed and tested security scripts
- Designed and tested patch management process
- Deployed security updates phase-wise
- Provided Linux OS hardening vis-à-vis FDA and DoD guidelines and Shell Scripting to automate the system hardening process

Value Delivered

By partnering with CitiusTech, the client was able to:

- Leverage CitiusTech's strong expertise in security testing and automation
- Comply with new cyber security expectations from DoD/ FDA for their diagnostic medical devices
- Ensure that no ADD or field engineer installs unapproved software
- Develop resuable security scripts for different product lines using similar version and flavour of Linux OS
- Streamline security patch management process
- Ensure sync between its security architecture for next-gen medical devices and Trusted Platform Module (TPM) chip, delivering higher level of security at low cost

All product and company names mentioned herein are trademarks of their respective owners

About CitiusTech

CitiusTech is a specialist provider of healthcare technology services and solutions to medical technology companies, providers, payers and life sciences organizations, with over 2,700 professionals worldwide. CitiusTech's services and solutions include healthcare software development, healthcare interoperability, regulatory compliance, BI/analytics, consumer engagement, care coordination and population health management. CitiusTech helps customers accelerate innovation in healthcare through a number of solutions and accelerators for clinical quality reporting, healthcare big data, cloud computing, mobile health and predictive analytics. With cutting-edge technology expertise, world-class service quality and a global resource base, CitiusTech consistently delivers best-in-class solutions and an unmatched cost advantage to healthcare clients worldwide.