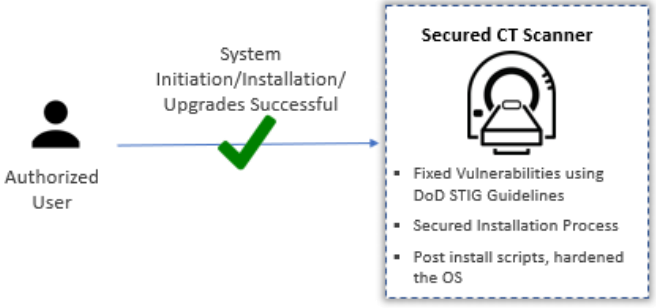
Case Study: Cyber Security of Medical Device (CT Scanner)

Client Requirements

Client is a leading medical device company. Client required assistance in meeting the US Department of Defense (DoD) and recommended FDA compliance on cybersecurity for its CT scan device.

Customer faced challenges with Authorized Device Dealers (ADD) installing unapproved software as freebies and top-ups and tampering customer software to win hospital/clinic purchase contracts.

CitiusTech was selected to provide the required assistance in the cybersecurity engineering of CT Scanner



Note: Any unauthorized user is not allowed into the CT machine due to the hardening of CT applications/OS, hence blocking the unauthorized access/hackers

Solution Schematic

CitiusTech Services:

- Developed Shell Scripts to strengthen OS security, as per DoD STIGs. Post- installation completion these scripts will be executed as post-installation security scripts
- STIG Compliance testing was conducted regularly to keep track of improvements in Security Posture
- Proposed near Ideal solution for secure Installation using Trusted computing and Public Key Infrastructure
- Developed best-fit Secure Installation process using GnuPG to ensure only customer signed patches are installed under Org constraints
- Knowledge sharing session on DoD RMF was conducted
- Assisted in categorizing CT Scanner from security perspective and identified list of all Security Controls applicable as a part of RMF

Value Delivered:

- Department of Defense's(DoD) OS level STIG compliance was met partially
- STIG Compliance testing helped in planning the next security development iterations
- Malicious Attackers, Distributor, Field Engineers, or Hospital staff will not be able to install unauthorized malicious software on the CT Scanner