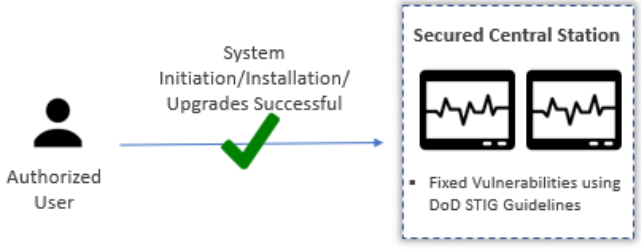
Case Study: Securing Central Station

Client Requirements

Customer is a leader in medical device industry and medical device systems.

Customer engaged CitiusTech to perform vulnerability assessment for OS and all SOUP items of Central Station (SOUP items are third party software's installed in medical devices), carryout STIG compliance testing, orient the Monitoring Solution's Engineering team with DoD RMF process.

Central Station receives data from multiple bedside monitors in the ICU. Nurses can remotely monitor patient data/status from one central station, thus increasing efficiency.



Note: Hardening of Central station secures any unauthorized access as per the DoD STIG guidelines

Solution Schematic

CitiusTech Services:

- CitiusTech carried out OS Vulnerability assessment and found 35+ OS level vulnerabilities. Identified, analyzed & deployed all required OS patches
- CitiusTech carried out manual vulnerability assessment for all SOUP items. Found 145+ vulnerabilities. Identified and addressed all vulnerable SOUP items
- CitiusTech conducted knowledge sharing session on DoD RMF and trained 35-40 Engineers with DoD RMF processes
- CitiusTech conducted STIG Compliance testing and found 150+ non-compliant implementations which needed to be addressed prior to releasing the product

Value Delivered:

- All identified Items were successfully upgraded addressing critical system level security vulnerabilities
- Provided a detailed assessment on how the existing vulnerabilities could be exploited by malicious actors to compromise the patient care process.
- Sensitized the engineering leadership to conduct similar assessments across the entire product portfolio