ASIMILY ProSecure

Problem Statement – Why ProSecure?

Risk assessments of networked systems and devices that collect, transmit, and/or store private data are required by The Joint Commission (TJC) and the Office of Civil Rights (OCR).

Across the supply chain, and healthcare technology in general, this remains a challenge for program compliance and governance, often the weakest link in the organization's risk management programs.

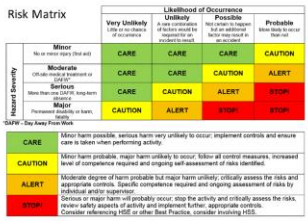
What process ensures risk assessments on new technology are defined, documented, and include follow through to implementation.

Current State:

Typically, today, risk assessments are resource intensive in terms of people and time. Across health delivery organizations (HDOs) there are numerous approaches and in virtually every instance people are addressing the problem with,

- Excel spreadsheets, manually created risk & control profiles not well-suited for medical devices
- Manual analysis of a manufacturers disclosure statement for medical device security (MDS2)
- Manual analysis of controls, vulnerabilities, devices to provide a one-off risk approach, subjective results
- Many stakeholders, lack of continuity across facilities & platforms for uniform configuration & deployment
- Lack of expertise and knowledge of the application of risk management to connected medical devices

Anecdotally, customers state risk assessments take 20-80 hours, per device, start>finish with inconsistent outcomes.



REDUCE OPERATIONAL INEFFICIENCIES & INCREASE COMPLIANCE

ASIMILY ProSecure provides community sourced, data driven risk assessments to develop concise Configuration Control Plans (CCPs); support deployment and sustainment of medical devices from a platform/fleet approach.

PLATFORM SPECIFIC

Every healthcare organization is different, with unique networks and available controls. ASIMILY ProSecure leverages medical device manufacturer data sources to provide dynamic insights to each unique device platform and policy.

SINGLE PANE of GLASS

ASIMILY ProSecure solves for a variety of use cases across asset inventory, cybersecurity, and operational controls to provide comprehensive Configuration Control Plans (CCPs).

INFORMATION SHARING

ASIMILY ProSecure risk assessment report supports each unique healthcare eco-system with specific Configuration Control Plans (CCPs) to address consistency of controls across the organization.

ASIMILY
440 N Wolfe Rd
Sunnyvale CA 94085
info@asimily.com

ASIMILY ProSecure

How ASIMILY ProSecure solves the problem:

ASIMILY ProSecure, permits clients to tackle medical device risk assessments with a new paradigm…a paradigm of risk modeling and platform configuration that can be standardized and implemented consistently across an organization. Each device platform can be implemented with a documented risk assessment with control and configuration plan (CCP) that ensures a standard risk profile.

ASIMILY ProSecure addresses four primary use cases for risk assessment and CCP development:

1) Legacy devices that need a standard configuration and control plan
2) Shadow IT, unconnected devices with network interface cards, may connect
3) New devices being considered and needing a risk assessment and CCP
4) Ad hoc development of CCPs based on local needs, assets, and policies

ASIMILY ProSecure combines all the knowledge of every platform across our installed base to create an anonymized, community sourced data set of the best configuration and control plan. Every ASIMILY customers is gaining the insights and advantages of ASIMILY's artificial intelligence (AI) and machine learning (ML) backend. **ASIMILY ProSecure** fills the missing gap, completing the risk assessment puzzle.

ASIMILY ProSecure clients can create and evaluate risk, optimal configurations, and best security controls as part of contractual requirements and implementation criteria. Clear, documented requirements to ensure consistency across medical devices as a fleet, or platform, instead of every installation being a one-off and different.

Who?

Healthcare - All healthcare organizations looking to enhance management of connected devices with a fleet-based risk assessment and Configuration Control Plans (CCPs) approach.

What?

Assess, Procure, and Configure - Which connected devices are most critical, have highest risk, and how to consistently deploy and configure to reduce risk. Provide control requirements to supply chain for inclusion in purchase contracts.

When?

Prior to purchase and before deployment – Documented risk assessments provide controls to include in purchase contracts; provide clear deployment requirements for installation.

Where?

Anywhere - Easy to deploy, secure browser-based web application permits broad access with role-based access controls, virtually accessible from anywhere for all stakeholders.

Why?

Compliance and risk management – Have documented risk assessments for connected devices on the network. Manage connected devices consistently across the organization to optimize life cycle costs and mitigate risk.

ASIMILY
440 N Wolfe Rd
Sunnyvale CA 94085
info@asimily.com