Module 5 Assignment

Joseph A. Brinkman

Omaha Metropolitan Community College

23SS_INFO_2123_HSA – Intro to SCADA Security

Mr. Gary Sparks

July 18th, 2023

Module 5 Assignment

CIS (Center for Internet Security) and NIST (National Institute of Standards and Technology) are two organizations that have developed frameworks for securing SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems).

NIST Cybersecurity Framework (CSF), is a voluntary set of guidelines designed to help organizations manage cybersecurity risks. The NIST CSF is developed through a collaborative process. Government agencies, industry experts, organizations, and stakeholders continually contribute to the CSF. As of April 25th, 2023, CSF 2.0 is the most recent framework. "The NIST Cybersecurity Framework was intended to be a living document that is refined, improved, and evolves over time. These updates help the Framework keep pace with technology and threat trends, integrate lessons learned, and move best practice to common practice. NIST initially produced the Framework in 2014 and updated it in April 2018 with CSF 1.1. Based on stakeholder feedback, in order to reflect the ever-evolving cybersecurity landscape and to help organizations more easily and effectively manage cybersecurity risk, NIST is planning a new, more significant update to the Framework: CSF 2.0." (NIST).

Comparable to the development process of the NIST CSF, the CIS benchmarks are also developed by a community of cybersecurity experts and practitioners who collaborate to define the best practices and security configurations for specific technologies, including SCADA and ICS. "Developed with our global community of cybersecurity experts, the CIS Benchmarks consist of more than 100 secure configuration guidelines for 25+ vendor product families. They remove guesswork from safeguarding systems against today's evolving cyber threats." (CIS).

The NIST CSF follows a five-step process: Identify, Protect, Respond and Recover. It provides high-level guidance and is organized around business functions and risk management principles. NIST CSF focuses on outcomes rather than specific technical details. Specific technical details are rather handled with security technical implementation guides, (STIG)s when using the NIST framework. By using both the NIST CSF and STIGS, an organization can meet DoD requirements and have ready access to technical guidance, eliminating problems such as guesswork and poor documentation.

CIS controls provided a prioritized list of 18 security actions that organizations should implement to protect their organization. CIS controls offer specific guidelines for securing various aspects of an organization's operations; network configuration, user access control, patch management, physical security, among others. The CIS benchmarks go into even greater technical detail on specific software, hardware, and operating systems than the CIS controls. Thereby providing even more granular insight into the products an organization uses to implement the controls. While the CIS controls and NIST CSF provide a framework an organization can follow to mitigate cybersecurity risk, the CIS benchmarks and STIGs provide the technical details on implementing and securing a product. For instance, CIS CISCO IOS 17.x Benchmark v1.0.0 is a downloadable 224 page pdf providing a table of contents, overview, and in-depth security recommendations across 3 different implementation groups that vary depending on the type of organization. There is also an available STIG for CISCO IOS versions.

Both NIST and CIS are widely adopted frameworks that are applicable to securing SCADA and ICS environments, but it is important to realize they each provide different approaches to mitigating an organization’s cybersecurity risk. NIST CSF focuses on a broader, risk-based approach with high-level guidance, while CIS offers more specific, technical

recommendations through its controls. STIGs are publicly available without needing an account, but an email address must be registered with CIS to obtain access to the Benchmark PDFs.

Reference

CIS. (2018). CIS. https://www.cisecurity.org/

NIST. (2019). *Cybersecurity Framework*. NIST. https://www.nist.gov/cyberframework

NIST. (2000). *National Institute of Standards and Technology | NIST*. NIST. https://www.nist.gov/

Editor, C. C. (n.d.). *security technical implementation guide (STIG) - Glossary | CSRC*. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/security_technical_implementation_guide