Bellevue University

Eric Wellmaker

Week 11.3 Writing Assignment

Information Security Mgmt

February 24th, 2022

NIST SP800-137 is a good tool for assisting InfoSec professionals to develop an ISCM strategy. For this assignment I will explain how I will maintain situational awareness of all network systems across an organization, assess security protocols, and provide actionable communication of security status across all tiers of an organization. In the second section I will identify two security automation domains, plan for aggregation & analysis and explain the use of an automation tool.

Situational Awareness of ongoing Threats

The National Institute of Standards and Technology (NIST) special publication 800-137 explains that in order to effectively address ever-increasing security challenges, a well-designed ISCM (Information Security Continuous Monitoring) strategy is necessary to addresses monitoring and assessment of security controls for effectiveness, and security status monitoring (Dempsey et al., 2011 p.12). This means that having a well-prepared system that's being continually tested will provide the results needed to maintain situational awareness of threats and threat activities. ISCM can be defined as consistent awareness of InfoSec resources, vulnerabilities, and the threats to support organizational risk management decisions (Dempsey et al., 2011 p.51). Using the ISCM protocol, I would maintain situational awareness of systems by Red Hat testing of network systems to gather any pertinent data that would notify any vulnerabilities within the network system. I would Implement routine training once a quarter to ensure employees understand network systems, how to handle & classify InfoSec assets. Depending on the classification level of the asset, I would consider implementing a Zero Trust network for those asset(s). And finally, have continuous monitoring so I can have real-time information to make well informed decisions based on the level of risk

(Whitman, M. E., & Mattord, H. J., 2018 p.425). The continuous monitoring of a security assessment program is an essential component of any security program. The security assessment can be used to satisfy standards specified in the Federal Information Security Management Act (FISMA) for accessing security controls in information systems. (Whitman, M. E., & Mattord, H. J., 2018 p.577). In the next section, I will discuss security automation domains that support continuous monitoring.

Security Automation Domain

Security automation can be defined as an information security area that includes a collection of tools, technology and data. The information from the network is sampled, analyzed and reported to display the security status of the organization (Dempsey et al., 2011 p.64). Asset and Network Management are two of the eleven security controls from the NIST SP800-137. Asset Management can be summed up as a tool to keep an accurate count of hardware and software inside an organization (Dempsey et al., 2011 p.69). Utilizing asset management software will help an organization by tracking an assets service life. Network configuration management has a series of tools for continuous monitoring. These tools include host discovery, inventory, change control & performance monitoring (Dempsey et al., 2011 p.69). My plan for aggregation and analysis is to utilize the security information and event management (SIEM). This tool can gather vulnerability scanning information data which can be used to make a risk assessment decision (Dempsey et al., 2011 p.72).

Automation tools are helpful to InfoSec professionals by reducing the time required for conducting taskings and improving in areas that need human monitoring and thought

processing. While the system is looking for trends in data, the employee can focus on other taskings required of their job description (Dempsey et al., 2011 p.19).

Software Assurance Protocol (SwAAP) is an automation tool which can assist with continuous monitoring. SwAAP has been developed to identify and classify all software weaknesses. SwAAP automation can assign a vulnerability score & identify attack patterns (Dempsey et al., 2011 p.19). This automation has many advantages and benefits for the InfoSec professional.

The Information Security Continuous Monitoring Plan is a sound strategy for helping InfoSec professionals. As mentioned in the above sections, a well-planned system that's consistently tested for system faults will provide the data necessary to maintain awareness of vulnerable network systems. My network plan consists of penetration testing, training personnel and implementing Zero Trust networks. Asset and Network Management on the other hand are automations which identify trends while InfoSec personnel can focus on other taskings. SIEM is another tool which can help with accessing risk and making a decision. Following NIST SP800-137 will help ensure vulnerabilities are identified and mitigated.

References

Dempsey, K., Shah Chawla, N., Johnson, A., Johnston, R., Clay Jones, A., Orebaugh, A., Scholl, M., Stine, K., (2011). NIST Special Publication 800-137. Computer Security Resource Center. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

Whitman, M. E., & Mattord, H. J. (2018). Management of information security (6th ed.). Cengage Learning.