**11.2 Assignment: Information Security Continuous Monitoring (ISCM) Plan**

Alice Mace

Computer Information Systems, Bellevue University

CIS 608: Information Security Management

Professor Kayleen Amerson

May 29, 2022

Information Security Continuous Monitoring (ISCM) is defined as “maintaining ongoing awareness of information security, vulnerabilities and threats to support organizational risk management decisions.” (Luu) Implementing an ISCM in an organization is a major step in ensuring the safety of its networks and all components encompassing it. We’ll discuss incorporating an ISCM into Coffee Town Sherriff’s Office operations, how this assessment tool can work, and how to best action the information discovered in the process to make their network secure.

As has been detailed in prior assignments, the primary IT/cyber support for Coffee Town Sherriff’s Office is conducted by a third-party organization that is contracted with the county and state to provide support to smaller offices that do not have the bandwidth to encompass their own section for this maintenance. This group focuses primarily on event and incident management which “involves monitoring and responding to as necessary, observable occurrences in a network or system.” (NIST) There are multiple methods and resources that can be used to conduct this management, but we will focus on one of the primary methods used at the Sherriff’s Office, a real time automation type tool called Intrusion Detection and Prevention Systems (IDPS).

IDPS “typically are used to record information related to observed events, notify security administrators of important observed events, and automatically generate reports, with remediation actions performed manually after human review of the report.” (NIST) Coffee Town Sherriff’s Office network is supported by Check Point Quantum IPS which “provides both IDS and IPS functionality” by with features such as detailed and customizable reports, vulnerability detection, built-in antivirus, anti-bot and sandboxing, and blocks DNS tunneling. (Samson) By routing internal network traffic through the gateway as well, it scans and protects both new information coming in and existing data already within the network. Once Check Point generates reports, the third-party IT/cyber support group divvies up alerts and digs into them before actioning to ensure the threat is real and the depth of it is understood.

Once the IT/cyber team identifies/confirms a potential threat, they send out an office wide email informing of issue, what steps they need to take, what steps (if any) the user needs to take to repair the security of the network. If it will result in a system outage for any period of time, an approximate timeline for repair will also be included. If a substantial vulnerability was detected that may have resulted in the breach of system or data insecurity, a thorough investigation will be conducted and full report submitted to all parties whose data may have been compromised. The third-party group will retain all alert information and develop a detailed report upon repair for record/audit purposes. If a breach or substantial vulnerability was detected, they will brief the Sherriff’s Office leadership, as required, and they will determine any additional notifications needed based on the risk to their network and databases.

**References**

Luu, T. (2015, January 1). *Implementing an IS Continuous Monitoring Solution: A Case Study | ISACA Journal*. ISACA. Retrieved May 29, 2022, from https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/implementing-an-information-security-continuous-monitoring-solutiona-case-study#:%7E:text=%E2%80%9CInformation%20security%20continuous%20monitoring%20is%20defined%20as%20maintaining,security%20policies%20and%20exposure%20to%20threats%20and%20vulnerabilities.

NIST. (2011, September). NIST Special Publication 800–137. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

Samson, R., Jr. (2022, April 27). *Top 10 Intrusion Detection and Prevention Systems*. ClearNetwork, Inc. Retrieved May 29, 2022, from https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/

Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security* (6th ed.). Cengage Learning.