CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #11

Team: Seven
Participants: Jackson Dillingham, Matt Jackson, Hilton Siaffa, Tabor Payne, Emily Wantland

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1
Though the Information Security function is often located in the IT department, many now argue that this is not the best place for it. Why? What factors need to be balanced when selecting the reporting structure of the Information Security function? *(8 points)*

- Though the Information Security function is often located in the IT department, many now argue that this is not the best location because both functions operate two diverse tasks. Recruiting the Information Security function in the IT department would create a conflict of interest and cause the two functions to struggle. IT professionals are concentrated on researching, developing, supporting and implementing information systems, while the objective of information security is identifying and thwarting threats to the information resources of an organization.
- The features that need to be balanced is shaping the difference between the duties of the IS function and the IT function. To evade confusion between the two functions, an organization should guarantee that there is a definitive separation of responsibilities for IT and IS functions. Additionally, the reporting construction must clearly designate the command structure of the IS function and how the CISO role will function in conjunction with the CIO role. By keeping the IT and IS function in different scopes, an organization is able to function with both roles peacefully coexisting.

Problem 2
Exabeam (a SIEM vendor) has an excellent primer on the modern Security Operations Center (SOC). Read it here: https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/ .
Compare and contrast the key qualifications and duties of the Tier 1-4 employees of a typical SOC. *(8 points)*

Alert Investigator

- Tier 1: Qualifications: The Tier 1 analyst should possess system administration skills, have knowledge in languages such as Python, Ruby, & PHP, and have CISSP or SANS SEC401 certifications.
- Tier 1: Duties: The Tier 1 analyst monitors SIEM alerts, manages and configures security monitoring tools, prioritizes alerts/issues and performs triage to confirm that a real incident is occurring.

Incident Responder

- Tier 2: Qualifications: The Tier 2 analyst should possess the same skills as a tier 1, but in addition they should have more experience dealing with incident response, advanced forensics, malware assessment, and threat intelligence.
- Tier 2: Duties: The Tier 2 analyst receives incidents and performs deep packet analysis, correlates with threat intelligence to identify threat actors, the nature of the attack, and affected data/systems. Moreover, they decide on strategy for containment, remediation, and recovery and act on these plans.

Subject Matter Expert/Threat Hunter

- Tier 3: Qualifications: The Tier 3 analyst should possess the same skills as a tier 2, but in addition they should have experience involving high-level incidents. Moreover, they should have experience with penetration testing tools, cross-organization data visualization, malware reverse engineering, identifying, and developing responses to new threats and attack patterns.
- Tier 3: Duties: The Tier 3 analyst conducts vulnerability assessments and penetration tests and reviews alerts, industry news, threat intelligence and security data. In addition, they actively hunt for threats that are on the network, as well as unknown vulnerabilities and security gaps. When the incident is major, the Tier 2 helps the effort to contain it.

Commander

- Tier 4: Qualifications: The Tier 4 must possess all the skills of a tier 3 analyst. In addition, they must have project management skills, incident response management training, and strong communication skills.
- Tier 4: Duties: The Tier 4 is responsible for hiring and training SOC staff. They are in charge of defensive and offensive strategy, managing resources, priorities and projects, and managing the team directly when responding to business-critical incidents. They are the point of contact for the business for security incidents, compliance, and other security.

At what levels of Security Maturity would an investment in a SOC become realistic? *(2 points)*

- The levels at which an investment would be worthwhile would be at level 4, which is considered advanced. These organizations will have an SEIM integrated with most areas, they will be considering analytics as a way to cut down alert fatigue, may be starting to think about tools that optimize incident investigation, looking to increase operation efficiency and maximize personnel output, and are intrigued by the idea of threat hunting.

Problem 3

Why would mandatory annual vacations for some (or all) employees be an important personnel control measure to consider? *(7 points)*

- Mandatory vacations are an important personnel control measure to consider because the vacation or paid time off an employee takes off work can simulate a situation in which that individual was unable to perform their duties if the employee were to be let go, placed on leave, etc. The time a worker spends off work can also allow other workers to momentarily fill their position and complete their normal job tasks.
- Furthermore, a mandatory annual vacation of at least one week allows the chance for the company to conduct an audit on the employee's performance. Employees who are embezzling from the organization or otherwise abusing information systems are generally unwilling to take vacations, for panic that their actions will be uncovered. This policy forces employees to contemplate the situation that they might be caught. Additionally, this method is efficient because it is a unique and non-threatening way of administering the

employee's customary job tasks and/ or duties without the employee thinking that they aren’t trustworthy.