# CIS-481: Introduction to Information Security

## Module 7 - Security and Personnel

## Exercise #10

**Team: 5**

**Participants: Sam Martin, Charles Degboe, Nicholas Zhang, Abril Beascoechea, Ricardo Portillo**

### Logistics

A. Get together with other students on your assigned **Team** in person and/or 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 and may impact your performance on assessments, especially with respect to the essay questions.

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** *(9 points)*

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?

Embedding the Information Security function within an IT department may lead to several potential conflicts of interest, given that IT's priority is normally focused on implementing as well as maintaining technology efficiently, which at times runs contrary to the rigid requirements of security protocols. This could mean favoring operational efficiency or cost over security measures. The issue of where the Information Security function should report is a balancing act among multiple factors.

Independence: The operation should be in a position to enforce security measures and not be overuled by operational priorities.Authority: Should report to a level in the organization that will allow it to effect meaningful change and have access to senior management.It must be independent enough, yet integrated enough, with IT and other departments to ensure practical security measures that are aligned with business operations.High visibility to the organization helps in emphasizing the importance of security and could be instrumental in garnering resources and support.

Common reporting alternatives to the IT department would be directly to the CEO or the Chief Risk Officer, or to a separate risk committee that provides the appropriate balance between independence and authority with requisite visibility.

**Problem 2** *(10 points)*

Exabeam (a SIEM vendor) has several excellent primers on modern Security Operations Centers (SOC). Learn more about SOC roles and responsibilities here:

https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/

Learn more about the role of SIEM solutions in a SOC here:

https://www.exabeam.com/explainers/siem-security/the-soc-secops-and-siem/

a) Compare and contrast the key qualifications and duties of the Tier 1-4 SOC analysts in a typical SOC (as noted in the table and shown in the figure in the first article). (*5 pts*.)

Similar to common business hierarchy, the higher the tier, the more qualifications are required, leading to bigger responsibilities.

Tier 1 is the most basic level requiring general technical skills and certifications such as CISSP or SANS SEC401. This level serves as the first level of defense by actively monitoring systems.

Tier 2 requires more skill and serves as a frontline response unit. Required qualification relates to incident response and analysis.

Tier 3 acts similarly to tier 2 but at a higher level due to a key requirement being the active defense against potential threats. Additionally, this tier handles similar situations as tier 2, but at a larger scale. Tier 2 and 3 can sometimes work together to handle major incidents.

Unilke the other tiers, Tier 4 is more of a management/command role that handles many of the non-technical aspects of the SOC. Interpersonal skills and communication skills are a key requirement here as this tier is responsible for hiring employees, reporting to upper management, and leading employees during major incidents. Other organizational and allocation skills are also a key part of this role as this position holds responsibility over the largest amount of people and resources compared to lower tiers.

b) As noted in the second article, “Advanced SOCs leverage next generation tools … which provide machine learning and advanced behavioral analytics, threat hunting capabilities, and

built-in automated incident response." Describe how the following next-gen tools help the SOC team find and deal with threats quickly and efficiently. (*5 pts*.)

· Next-generation SIEM: improves machine learning and behavioral analytics (reducing false positives and alert fatigue) and detects hard-to-detect events.

· Network Traffic Analysis (NTA): It's great at detecting unusual network behaviors, for example when wanting to investigate lateral movements by attackers already within the network.

· User and Entity Behavior Analytics (UEBA): Detects malicious insiders or those bypass security controls. Facilitates the detection of compromised accounts whether by external attackers or insiders.

· Endpoint Detection and Response (EDR): Offers protection against workstation or server compromises and helps manage the mobile workforce. It also provides the necessary data for historical investigation and track root causes.

· Web Application Firewall (WAF): Is positioned in front of web applications to inspect traffic and identify patterns that may be malicious activity. It minimizes false positives by learning acceptable URLs, parameters, and user imputs.

**Problem 3** *(6 points)*

Look up two (2) of the popular security certifications mentioned in Module 7 of the text and describe the requirements necessary to earn the certification and current associated cost for each.

CISSP- This exam is anywhere from 100-150 multiple-choice questions and you have 6 hours to complete it. The exam will be over the 8 domains of

1. Security and risk management,
2. Asset Security,
3. Architecture and engineering,
4. Communication and network security,
5. Identity and access management,
6. Security assessment and testing,
7. Security operations,

8. Development security.

You need to have a college degree and at least 5 years of work experience in at least 2 of the domains or 4 years of work experience in more than 2 domains. After you pass the test, you will have 9 months to get an endorsement from your employer to validate you work experience. After the certification is earned you will need to 120 hours of CPE every 3 years with a minimum of 20 hours per year. The cost for everything is expensive as the test is $749 and certified members must pay $125 annually.

SSCP- This exam has 125 multiple-choice questions and you have 3 hours to complete it. It will be over the 7 domains of

1. Access Controls
2. Security operations and administration
3. Risk identification, monitoring, and analysis
4. Incident response and recovery
5. Cryptography
6. Network and communications security
7. Systems and application security

This is a scaled-down version of the CISSP, however, the domains are not a subset of the CISSP, the content on this exam is slightly more technical. You will also need to continue pursuing CPE as well with this exam. The exam will cost $249 with a $125 annual fee.