Amira Muaket

Professor Duvall

Internship Class, CYSE-368

3 April 2025

Reflection Journal #3

For the final 50 hours of my internship, it centered on Information System Security Officer (ISSO) training. One of my supervisors assigned me an online-based training program covering “ISSO Entry-Level Topics”. The online training program's total length was approximately 25-30 hours. I was required to write an extensive summary after each main topic and submit it to my supervisor. The training covered 12 main topics and each topic had its security innovation objectives/courses that aligned with the Commodity Future Trading Commission (CFTC) policies.

The first topic was “Risk Management Framework” and the objectives were Categorizing Systems and Information within the RMF, Selecting, Implementing, and Assessing Controls within the RMF, Authorizing and Monitoring System Controls within the RMF, Preparing the Risk Management Framework, and Essential Risk Assessment. The next topic is “Laws, Regulations, Policies and Ethics” and covers Confidentiality, Integrity, and Availability Requirements. “Cybersecurity & Privacy Principles” had both Fundamentals of Privacy Protection and Fundamentals of Security Information & Event Management (SIEM). I had prior knowledge of the first two topics, but I enjoyed how in-depth and detailed each topic was covered during the training.

“Cyber Threats & Vulnerabilities” had the most extended list of subtopics. It followed the Fundamentals of Ethical Hacking, Fundamentals of Secure Mobile Development, Fundamentals of Secure DevOps, Fundamentals of the PCI Secure SLC Standard, Introduction to the Microsoft SDL, How to Create Application Security Design Requirements, and Fundamentals of Threat Modeling. This part of the training was very technical heavy but extremely informative.

The next topic was “Risk Management Framework pt.2” - Selecting, Implementing, and Assessing Controls within the RMF, and ICS/SCADA Security Essentials. Out of all the topics, I enjoyed this portion of the training, especially selecting which RMF controls best-fit company/organization ideals and systems. “Encryption Algorithms” covered Essential Data Encryption, a topic I did not know of, so it was interesting to see how some ISSOs are encrypting certain data to keep their privacy. “Incident Response” covered Cybersecurity Incident Response, Essential Incident Response, and “Incident Response pt. 2” had Risk Management Foundations. This topic was an approach to creating a plan to be able to detect, respond, and recover data depending on certain incidents that may occur.

The “Server & Client OS” topic addresses the Fundamentals of Shell and Interpreted Language Security. “Zero-Trust” explains the Fundamentals of Zero Trust Security, which is enforcing a strict verification process when wanting access to applications. “Penetration Testing” subtopics include Penetration Testing Fundamentals and Infrastructure Penetration Testing. “Access Control” covered Essential Access Control for Mobile Devices and Fundamentals of Database Security. Finally “Creating Policies” has Essential Security Planning Policies and Procedures, and Essential Information Security Program Planning. The last topic revolved around decision-making, what are the right tools and protocols to add or remove depending on the current environment.

After completing the training, I found it to be a lengthy process. I took frequent breaks after each topic to gather my thoughts and notes. Despite the length, I did learn a lot about ISSO roles and responsibilities, both generally and the relation it has with CFTC policies and regulations. I hadn't realized that the role of ISSO had this much responsibility and it’s a crucial role played in protecting and managing data. This training course gave me insights into one of many roles in cybersecurity and a possible career path to follow.