**Week5 Reflection on Cybersecurity**

Hang Yang

IS 5403: Cybersecurity

Prof. Jaime Martinez

April 13, 2024

**Week3 Reflection on Cybersecurity**

Dr. Mclver introduced his experience on the importance of Incident Response. The biggest takeaway I learnt from the video is that huge loss or system disaster could happen if incident response is ignored. We could not rely utterly on the security programs without any preparedness to the potential incidents on the security talents. The analogy used in the video is quite inspiring to see the incident response as the hospital ICU team. If the ambulances and the ICU doctors are not ready, people would die. The system could crash and cause huge loss if security breaches are captured but no reactions on them. On the other hand, we also need to train our security talents to handle the incidents carefully, not too slow and not too fast. My suggestions would be do some research on well-known cases and take some rehearsal practices in non-critical time. Another point worths mentioning is documentation. Always document the realistic procedures and actions we have done to fix the security breach. It’s not only a legal requirement, but also an efficient way to study and enhance our response tricks in future.

The videos by Prof. Jeff from IBM introduces two key methodologies in cybersecurity architecture: Detection and Response. The course provides a foundational understanding of both detection and response concepts. The detection step is an important component of cybersecurity together with prevention and response. It describes the process security professionals collect, analyze, identity and report the security incident. The introduction of detection tools place emphasis on SIEM (Security Information and Event Management) and XDR. SIEM excel in correlating and aggregating data to identify anomalies and similar alerts from the bottom up. On the other hand, XDR (Extended Detection and Response) introduces a contrary approach, initiating security feedback requests from the top down to individual domains. When individual domains receives the request from XDR, they would check and send results back if there are any specific security concern from the request. While each tool has its merits, they need not be mutually exclusive. Combining their strengths, if budget permits, can enhance the accuracy of security alert detection. In terms of response, it's worth mentioning that many initial attacks are difficult to control and prevent. However, the key is to detect of attacks as early as possible. Compared to traditional manual incident response methods, modern SOAR (Security Orchestration, Automation, and Response) tools offer automation that significantly reduces the gap between the start of an attack and awareness of it.

This week's Coursera course explains the crucial concepts of penetration testing, incident response, and forensics. Penetration testing acts as a valuable approach to assess the strength of a system's security defense. It's typically conducted during non-business critical hours, with careful planning involving stakeholders, and sometimes even the local security department. Forensics, a new concept to me, involves the meticulous process of identifying, collecting, examining, and analyzing data while ensuring data consistency and integrity. What surprises me most was the use of Python as a scripting language in this process. Data collection can be repetitive and laborious, making automation essential. Scripting languages, particularly Python, have become main approches to implement automation. Mastering Python can significantly enhance your capabilities in this domain. Overall, the course content is well-organized and coherent, providing a comprehensive understanding of incident response concepts and practical processes, including the utilization of specific tools.

**References**

IBM(n.d.). What is incident response? *IBM*. Retrieved from

https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit

Irei, A. & Shea, S. (n.d.). What is incident response? A complete guide. *TechTarget*. Retrieved from

https://www.techtarget.com/searchsecurity/definition/incident-response