Interview Assessment #3

Name of Professional: Jose Pasillas

Profession: Sinor Manager of Incident Response

Company: Vanguard

Date of interview: 2 / 2 / 24

Assessment:

My third interview was with Jose Walker, a Sinor manager at Vanguard, a well-known cybersecurity company. From our meeting, I understood the difference between the red and blue teams in cybersecurity and the vast possibilities that could be found in the blue cybersecurity sector.

The interview began by understanding how a managing job in the cybersecurity field works; since that was my original field of study, I found it interesting and informative to see that professionals that are in a managing role can either be in that position but working in that field and working up, or hired. Mr. Pasillas explains how he started, saying that he began with no experience and was “given a chance,” through that chance, he could begin at Verizon as an implementation manager tier 1 and then work up to tier 2. From there, he stayed at Verizon and worked as a tier 2 IT security Analyst. From there, he was given an excellent opportunity to work at NTT Data Services. However, he has to start at a tier 1 Information security advisory. Since Mr. Pasillas saw the opportunity in the risk, he took the position and started working his way up. In around two years, he grew and became an endpoint security Portfolio Leader, which deals with security engineering =, risk assessment, regulatory requirements, and threat management.

In less than ten months, he was promoted to become a top-tier security analysis advisor. From there, he started exploring bank security. He took on the position of Vice president, also known as Senior Business Information Security Officer, at Citi Bank for two years. From there, he had another opportunity to work as the Security operations center Senior Manager, also known as the Vice president. After a short period, he was hired at Vanguard as a 3rd Party Incident Response Senior Manager and has worked there until now.

Moving from there, we started discussing the difference between penetration testing and incident response because they sounded very similar based on our discussion. From there, he explained the difference between the red and blue teams in cybersecurity, where the blue team is defense. While red is offense, penetration testing will fall under the blue team since it protects against what is happening now. At the same time, incident response is a red team because it occurs before the penetration testing stage.

Through the discussion, I started explaining what my Original work product was and what I was planning on doing for my Final Product since I would like a professional opinion on the idea. That is when we make an agreement and assume that when it comes to incident response, it is like putting a puzzle together. It seems complicated; however, it is simple when the picture comes together. We discussed the difficulty of explaining cybersecurity to the public. And that was when Mr.Pallisis “It takes a normal person to create a complex person. However, it takes a complex person to create the idea,” from there I came to an agreement that even though cybersecurity is very complex, the only way the public can protect themselves would be to make it less complicated, in other

words, more straightforward. From there, we discussed having an event that would target both the new and old generations since they are most likely to fall for malicious attacks.