**What did you do?**

I managed six assets of people, procedures, data, software, hardware, networking for asset inventory and Risk Assessment. According to the Asset Inventory and Risk Assessment Table Template, Dr. Jennex required to do the first 4 columns, which are ID, Asset Name, Description, system ID. For people, I managed 12 assets. I put them into System ID 1. For procedures, I managed 18 assets. I put them into System ID 2. For data, I managed 17 assets. I put them into System ID 3. For software, I managed 15 assets. I put them into System ID 4. For hardware, I managed 18 assets. I put them into System ID 5. For networking, I only managed 9 assets. I put them into System ID 6. Totally are 89 assets. During the inventory process, I grouped assets by their function and location within the organization. For example, all servers were grouped together regardless of their operating system or application, and all network devices were grouped together. Within each group, I further divided assets by their location, such as physical location or network segment. When dealing with assets that could be in multiple groups, I decided based on the asset's primary function or location. For example, a printer connected to a specific department's network was categorized as a department asset, even though it could also be considered a network asset. In cases where an asset was truly ambiguous or could not be easily categorized, I created a separate category for those assets and documented them accordingly.

**What were the results?**

The inventory of assets can help identify the potential attack surface of a system. Attack surface refers to the ways in which an attacker can exploit vulnerabilities in a system to compromise its security. By conducting an inventory of assets, we can identify the various entry points an attacker can use to gain access to the system and its data. For example, if the inventory includes a list of servers, applications, and databases, an attacker can target these assets to exploit any vulnerabilities in their security. Similarly, if the inventory includes a list of users and their access privileges, an attacker can target specific users to gain unauthorized access to the system. The inventory can also help identify any gaps or weaknesses in the system's security controls. For example, if the inventory shows that certain assets are not protected by firewalls or have outdated software versions, these assets can be considered vulnerable and should be prioritized for remediation. Overall, the inventory can provide valuable insights into the potential attack surface of a system and help organizations prioritize their security efforts to mitigate the risks.

**What did you learn?**

The results of an inventory and assessment can vary depending on the scope and depth of the analysis. It is possible that the attack surface is larger than expected, indicating that there are more vulnerabilities and risks present in the system. Alternatively, it is possible that the attack surface is smaller than expected, indicating that the system is more secure than anticipated.

It is essential to remember that risk is not solely determined by the size of the attack surface. Other factors, such as the nature of the assets, the value of the data, the level of access controls, and the strength of security measures, also play a significant role in determining the overall risk level. Therefore, it is crucial to consider all these factors in determining the level of risk present in the system.