JOURNAL ENTRY 1

The National Initiative for Cybersecurity Education (NICE) Framework is a valuable tool that provides sets of standards for cybersecurity professionals and improves organizations' cybersecurity practices. It categorizes the duties and skills of cybersecurity workers, making it easier to understand their roles. The Framework helps in choosing the appropriate training and certifications for individuals in their desired or current cybersecurity positions. It consists of seven high-level categories that encompass various functions and roles in cybersecurity, ranging from technical specialities to management and leadership positions.

After reviewing the NICE Workforce Framework, my ranking of the categories based on my interest is as follows:

- OPERATE AND MAINTAIN
- PROTECT AND DEFEND
- OVERSEE AND GOVERN
- SECURELY PROVISION
- ANALYZE
- INVESTIGATE
- COLLECT AND OPERATE

Top Three Categories:

- **OPERATE AND MAINTAIN (Implementation and Operate)**

This category is my first interest choice because it entails ensuring that systems are effectively running and well secured. It offers me the opportunity to work with software, network configuration and hardware to ensure everything is efficiently running. I love the fact that this category is hand-on, which resonates with my attempts at maintaining my household devices. The work roles that appeal to me are network operations, systems administration, and database administration. The tasks in this category, like implementation procedure, maintenance, configuration, troubleshooting and improving performance are essential for keeping an organization's IT infrastructure secure and healthy. The aspect of addressing and resolving problems excites me, this practical approach aligns with my career goals and interest in specializing in this field.

- **PROTECT AND DEFEND (Protection and Defense)**

This category is my second interest choice because it focuses on the measures needed to safeguard information systems from cyber threats. It matches with my passion for security as it entails implementing measures to protect against cyberattacks. The roles that appeal to me are incident response, insider threat analysis, and threat analysis. The tasks in this category such as configuring firewalls, incident response, and intrusion detection systems, help to safeguard an organization's digital assets. What interests me about this category is the challenge and responsibility of defending systems from advanced threats; the concept of staying ahead of cyber attackers is thrilling. I'm excited to become a part of this, constantly adapting field that involves understanding threats, vulnerabilities, and the ability to respond swiftly to incidents.

- **OVERSEE AND GOVERN (Oversight and Governance)**

This category is my third choice because it involves managing cybersecurity strategies, governance, and policies of an organization's cyber work. This category is important as it ensures an organization's cybersecurity practices are aligned with its goal and laws and regulations set for privacy and security. The roles that appeal to me are security project management, technology program auditing, and cybersecurity curriculum development. It includes tasks such as compliance, cybersecurity policy-making, cybersecurity legal advocacy, and risk management, all needed for a strong cybersecurity framework. I am drawn to this category because an individual is allowed to impact and shape an organization's cybersecurity strategy at a senior level. It does not just involve technical expertise but also requires strategic planning, leadership, and knowledge of regulations. Creating policies and frameworks that protect an organization merge my passion for security with a wider perspective on organizational management and governance.

Lowest Ranked Category:

COLLECT AND OPERATE (Cyberspace Intelligence)

My lowest ranked category is "Collect and Operate" due to several reasons. Firstly, I prefer roles that don't focus solely on collecting and managing cybersecurity data. While I understand the value of data in cybersecurity, the tasks involved in this category, like gathering intelligence and planning operations, do not appeal to me as much as other tasks. What disinterests me about this category is that it seems more data-driven and analytical; I prefer to be hands-on and practical. I think my lack of interest in this category is partly because I don't fully understand the tasks included in it, but I plan to research and learn more about its role in cybersecurity operations.

In conclusion, after reviewing the NICE Workforce Framework, I have gained an understanding of the different roles and functions within the cybersecurity field that I wasn't previously aware of. The comprehensive categories have helped me clarify specific areas where my passion and interest lie. My ranking of the categories has given me insights into my career aspirations and the areas I would love to pursue. My top three categories: "Operate and Maintain”, “Protect and Defend”, and “Oversee and Govern” align with my interest in entering the cybersecurity field. I ranked “Collect and Operate” as the least interesting due to its data-driven and analytical nature. However, I recognize its importance and plan to conduct further research on the roles involved.

REFERENCES

GIAC. (n.d.). *NICE Framework*. GIAC Certifications. Retrieved May 16, 2024, from https://www.giac.org/workforce-development/niceframework/

NIST. (n.d.). *NICE Framework Resource Center | NIST*. National Institute of Standards and Technology. Retrieved May 16, 2024, from https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

Workforce Framework for Cybersecurity (NICE Framework) | NICCS. (2024, April 18). NICCS. Retrieved May 18, 2024, from https://niccs.cisa.gov/workforce-development/nice-framework