Review the NICE Workforce Framework. Rank the categories based on how much they interest you. Write about why your top three categories interest you. In addition, write about your lowest ranked category and why you think it would interest you the least?

Janae Craig
05/16/2024

After spending time reviewing the National Initiative for Cybersecurity Education's (NICE) workforce framework. I've decided to rate them by the most interesting by placing them in the following order:

Investigate
Protect and defend
Analyze
Collect and Operate
Oversee and Govern
Operate and Maintain
Securely provision

The **"Investigate"** component of the NICE framework focuses on the investigation of cybersecurity events or crimes involving technology systems and networks, which piqued my curiosity because I have a minor in criminal justice and it entails conducting investigations into cybersecurity incidents or crimes. This could also include evaluating digital evidence. Cybercriminals use a variety of approaches, including malware and phishing assaults, social engineering, and insider threats. This variation guarantees that work remains fascinating and diversified. It also enables opportunities to collaborate with professionals from other fields and expand professional networks.

The **"Protect and Defend"** component includes planning and implementing security measures to protect against cyber threats, such as incident response, vulnerability assessment, and monitoring. This phase is crucial for enterprises to establish a strong defense posture, respond effectively to emergencies and safeguard sensitive assets against cyberattacks. I believe this is one of my top three because I have considered being a penetration tester.Working in such an area is appealing because it provides a feeling of purpose by directly affecting the safety and security of individuals, businesses, and organizations. It also helps you stay safe and up to date because you will know all the latest viruses, malware, and attacks.

The **"Analyze"** component includes evaluating incoming cybersecurity data to determine its intelligence value. It's fascinating because it shows how crucial data analysis is to cybersecurity operations handling these kinds of things. By analyzing this kind of data, you may be able to better understand cybercriminals' behavior, which will help you predict their next moves and build effective defenses. This section contains highly important jobs that could directly relate to the military or National security. You may encounter urgent threats or situations that require an effective response.

I put the **"Securely Provision"** section at the bottom of my list since, to me, it is the least fascinating area. Its concentration is on developing, putting into practice, and supervising secure IT services and systems. These tasks could include maintaining access restrictions, setting systems securely, and making sure security policies and laws are followed are all included. By including security measures into the creation and upkeep of IT systems, it is essential to laying a solid foundation for cybersecurity.

References

Bhattacherjee, A. (n.d.). Social Science Research: Principles, methods, and practices. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1002 context=oa_textbooks

Workforce Framework for cybersecurity (NICE framework). National Initiative for Cybersecurity Careers and Studies. (n.d.). https://niccs.cisa.gov/workforce-development/nice-framework