10/4/2025

**MODUPE FELICIA KPOKPOGBE**

**1057398**

**BSC. INFORMATION TECHNOLOGY**

ITE1100 ASSIGNMENT

PURSUING A CAREER IN CYBERSECURITY ANALYST

**CYBERSECURITY ANALYST: SAFEGUARDING THE FUTURE OF DIGITAL INFORMATION**

**Career description**

A cybersecurity Analyst is essential in protecting an organization’s digital systems from threats like data breaches, malware, phishing, and unauthorized intrusions. The primary role is to understand company IT infrastructure in detail, to monitor it at all time and to assess potential threats that may compromise the network’s access. The cybersecurity analyst is responsible for configurating tools which may take effect in form of virus software, password protectors and vulnerability management software. Reporting every detail that is occurring in the network and evaluate its strengths is one of the skills needed is learning to read these reports. The cybersecurity Analyst also examine system weaknesses because no network is fully secure, but the goal is to make it as secure as possible. It is essential to continuously test all company network and find weaknesses before external threats can compromise them.

Technologically, scripting involves writing code that automates specific tasks or controls the behaviour of a program. The difference is that coding is static, whereas scripts can make images and text move around. Learning to create tools and automate repetitive tasks using languages like Python or PowerShell enhances efficiency as analyst. Knowing how to use detection of security breaches software, security information and event management (SIEM) products, intrusion detection system (IDS), and intrusion prevention system (IPS) enables to quickly suspicious activity or security violations.

Professional skills are also very important. Cybersecurity professionals must be able to communicate both written and verbally and capable of making fast, informed decision under pressure. Collaboration with other team within the company (legal, IT, public relations) might be necessary or share findings with other organizations or the greater cybersecurity community.

Cybersecurity professionals can work in variety of environments, including corporate IT teams, government agencies, specialized cyber defence firms and even remote Security Operations Center (SOC). As the field evolves, positioning cybersecurity at the core of modern IT disciplines focused on the secure handling of data and information.

**Personal motivation**

My interest in cybersecurity began four years ago when my business WhatsApp account was hacked after i unknowingly clicked on a suspicious link sent by a stranger. Shortly after, i lost access to my account, and the attacker began messaging my contacts while impersonating me. They demanded 200,000 naira, claiming it was an emergency and asking my friends and family to lend me the money. The experience was both alarming and eye-opening, as i saw firsthand how easily someone’s digital identity could be misused. It sparked a deep curiosity in me to understand how such attacks happen and how to prevent them, ultimately inspiring my decision to pursue a career in cybersecurity.

Also, cybersecurity is essential across all types of organizations and is highly recognized on a global scale. It is a broad and challenging field, especially as modern institutions such as banks, schools, hospitals and government agencies increasingly rely on technology to operate. These organizations depend heavily on reliable digital security to protect sensitive data and maintain trust, making cybersecurity a critical component of their operations and is a lucrative career opportunity.

Moreover, I consider myself to be patient, thoughtful in decision making, kind and eager to learn new things. These traits align well with the demands of the cybersecurity field, making it a suitable career path for my personality.

**Steps to professionalism**

To establish myself as a respected cybersecurity analyst, i am committed in gaining knowledge and skills in key areas such as network security, cryptography, risk management, compliance, incident response, and threat analysis. This aspiration led me to pursue further education in University of Guyana after completing my Associate degree in Nigeria. By earning a Bachelor’s degree in Information Technology, i aim to build a strong and versatile foundation that will prepare me for both career entry and long-term advancement in the cybersecurity field.

To enhance my expertise and career prospects, i intend to earn the following industry recognized certifications:

* Certified Ethical Hacker (CEH) which focuses on ethical hacking techniques used by malicious hackers and would enable me to learn how to defend against them.
* CompTIA Security+ is an entry level certification that provides a global benchmark for best practices in IT security which would help me build a strong foundation in cybersecurity principles.
* CISSP would demonstrates my ability to effectively manage security in a business environment and is highly esteemed in the cybersecurity field due to its comprehensive coverage of key areas like communications and network security.

Additionally, i intend to apply for internship in IT department to get more job opportunities on LinkedIn jobs, Indeed, Jobberman and more in the industry and also have a practical learning experience which would builds my knowledge. I also intend to join cybersecurity communities like Cybrary, infosec institute, women in cybersecurity (WICYS) and platforms like TryHackMe or Hack The Box for mentorship.

The only i anticipate in pursuing a career in cybersecurity is the financial cost. Gaining access to quality training, certifications, tools, and practical labs can be expensive, making it difficult for many aspiring professionals, including myself, to fully explore the field. Despite this, i am determined to find alternative learning paths, utilize free resources, and seek opportunities that can support my growth, such as scholarships, mentorship programs, and open-source platform. This challenge is one the reasons my aunt chose to sponsor my education at the university of Guyana, after recognizing my determination and commitment to pursuing my career in cybersecurity.

**Application of skills and society contribution**

Beyond personal growth in career, i strongly believe cybersecurity can be a force for good. In Nigeria and the whole of Africa, the application of cybersecurity skills is becoming essential to protect national infrastructure, foster digital trust, and enable sustainable growth.

After my degree at the university of Guyana, i intend to return to my country Nigeria and contribute to Nigeria’s digital transformation by building trust in digital services, supporting innovation, enabling a digital economy, reducing digital inequality and enhancing National security.

**References**

* Coursera. (2025). Cybersecurity skills. Retrieved from https://www.coursera.org/articles/cybersecurity-analyst-skills
* SentinelOne. (2025). Cybersecurity 101: cybersecurity challenges. Retrieved from <https://www.sentinelone.com/Cybersecurity-101/cybersecurity/cyber-security-challenges/>
* CISSP. (2024). Certification provided. Retrieved from https://www.isc2.org/research
* Mordor intelligence. (2025). Nigeria cybersecurity market report

**972 words**