## CYBERSECURITY ANALYST AND ITS JOB POSTINGS.

A cybersecurity analyst is a professional who is responsible for protecting an organization's computer systems and networks from cyber-attacks. They are responsible for monitoring networks for security breaches, identifying potential threats, and developing strategies to protect the organization's data and systems.

They must have strong technical and analytical skills, as well as excellent communication and interpersonal skills. They must also stay up-to-date on the latest cyber threats and security trends. There are different types of cybersecurity analyst and they include:

1) **Security Operations Center (SOC) Analyst**
   - **Role**: Monitors and analyzes network traffic in real time to detect and respond to cyber threats using tools like SIEM (e.g., Splunk, Microsoft Sentinel). They investigate alerts, mitigate incidents, and escalate complex issues.

   - **Responsibilities**:
     - Monitor security dashboards for suspicious activity.
     - Respond to incidents like malware or phishing attacks.
     - Generate reports on security events.+.
   - **Skills Needed**: SIEM tools, log analysis, incident response. Online platforms like TryHackMe can help you practice.

2) **Vulnerability Management Analyst**

   - **Role**: Identifies, assesses, and prioritizes vulnerabilities in systems and applications through scans and penetration testing. They work to patch or mitigate weaknesses before exploitation.
   - **Responsibilities**:
     - Conduct vulnerability scans using tools like Nessus or Qualys.
     - Perform risk assessments and recommend fixes.
     - Collaborate with IT teams to apply patches.
   - **Skills Needed**: Vulnerability scanners, penetration testing, knowledge of CVSS scoring. Free tools like OpenVAS are useful for learning.

3) **Threat Intelligence Analyst**
   - **Role**: Researches and analyzes cyber threats, such as advanced persistent threats (APTs) or ransomware, to understand attacker tactics and inform defense strategies.

   - **Responsibilities**:

     - Collect and analyze threat data from sources like dark web forums.
     - Develop threat intelligence reports.
     - Advise on proactive defense measures.
   - **Skills Needed**: OSINT (Open-Source Intelligence), malware analysis, threat-hunting tools. Platforms like Recorded Future offer free training resources.

4) **Incident Response Analyst**

- **Role**: Leads the investigation and mitigation of security incidents, such as data breaches or ransomware attacks, to minimize damage and ensure recovery.
- **Responsibilities**:
    - Investigate breaches and determine root causes
    - Coordinate containment and recovery efforts.
    - Document incidents for compliance (e.g., NDPR in Nigeria).

- **Skills Needed: Forensics tool**s (e.g., Autopsy), incident handling frameworks, scripting (Python, PowerShell).

5) **Compliance and Risk Analyst**

- **Role**: Ensures organizational adherence to cybersecurity regulations (e.g., NDPR, GDPR) and conducts risk assessments to align security practices with standards.
- **Responsibilities**:
    - Audit systems for compliance with regulations.
    - Conduct risk assessments and gap analyses.
    - Develop policies and train staff on compliance.
- **Skills Needed**: Knowledge of compliance frameworks (ISO 27001, NIST), risk assessment tools, policy writing.

6) **Penetration Testing Analyst**
    - **Role**: Simulates cyberattacks to identify vulnerabilities in systems, networks, or applications, helping organizations strengthen defenses.
    - **Responsibilities**:
        - Perform penetration tests using tools like Metasploit or Burp Suite.
        - Report findings and recommend remediation.
        - Test web applications, networks, or cloud environments.
    - **Skills Needed**: Ethical hacking tools, scripting, knowledge of attack vectors. Free platforms like Hack the Box

## Key Responsibilities:

- **Monitoring and Detection**: Use tools like Splunk or Microsoft Sentinel to track network activity for threats, relevant for Nigerian banks and tech startups.
- **Incident Response**: Quickly address breaches, critical in Nigeria where cybercrime like phishing is prevalent.
- **Vulnerability Management**: Identify weaknesses in systems, important for Nigerian organizations adopting cloud services.
- **Compliance**: Ensure adherence to local regulations like the Nigeria Data Protection Regulation (NDPR) and global standards like GDPR for international firms.
- **Training**: Educate staff on cybersecurity best practices, key in Nigeria's growing SME sector.

## Cybersecurity Analyst Job Postings (Relevant for Nigerians):

1. **Cyber Security Analyst – New York City Department of Parks (New York, NY)**

    - **Source**: City of New York Jobs, posted January 31, 2025
    - **Description**: Involves implementing cybersecurity policies, conducting audits, and using Advanced Threat Protection (ATP) to secure data. This role suits Nigerians with international aspirations, as U.S. public sector jobs sometimes sponsor visas for skilled professionals.
    - **Key Responsibilities**:
        - Conduct security audits and manage IT inventory.
        - Implement citywide cybersecurity standards.
        - Use ATP to prevent data leaks
    - **Application**: Apply via cityjobs.nyc.gov, Job ID# 700528, by February 28, 2025.

2. **Cyber Security analyst – Delta group(Portsmouth Uk):**
    - **Source**: X post by @Deltragroup, June 4, 2025
    - **Description**: Focuses on enterprise security operations, using SIEM tools, identity management, and vulnerability assessments. The UK's tech sector is open to international talent, and Nigeria's Commonwealth ties can ease visa processes.
    - **Key Responsibilities**:
        - Monitor security events with SIEM tools.
        - Respond to incidents and manage vulnerabilities.
    - **Application**: Apply via the link in the X post.

3. **Cyber Security Analyst (Remote) – Bizoforce Inc. (India)**
    - **Source**: X post by @Bizoforceinc, June 9, 2025
    - **Description**: A remote role focusing on threat analysis, incident response, and SIEM tools for enterprise clients. Remote work is ideal for Nigerians, avoiding relocation costs.
    - **Key Responsibilities**:
        - Real-time threat analysis and incident response.
        - Use SIEM tools and manage vulnerabilities.
    - **Application:** Apply via the link in the X post.