Chioma Dibor

Nigeria | ambydibor@gmail.com | +2349067942965 | https://www.linkedin.com/in/chiomadibor/ | Blog

PROFILE

Dedicated cybersecurity analyst with hands-on experience. Skilled in threat intelligence, threat detection and incident response, using tools like Wireshark, Nmap, Splunk to ensure security and compliance. Committed to safeguarding critical assets and aligning cybersecurity strategies with organizational goals.

SKILLS

- Forensics Tools: FTK Imager, Autopsy
- Network Security Tools: Wireshark, Nmap
- Operating Systems: Windows, Kali Linux
- SIEM Tools: Splunk, Graylog, Wazuh
- Threat Detection and Incident Response
- Microsoft Defender XDR, Microsoft Sentinel
- Security Frameworks: MITRE ATT&CK, NIST, ISO 27001
- Compliance Regulations: GDPR, PCI-DSS
- Soft Skills: Communication, Presentation Skills
- Report Writing and Documentation

WORK EXPERIENCE

Cyber & Forensics Security Solutions, India **Aug 2024- Sept 2024**

Position: SOC Analyst Intern

- Analysed network traffic using Wireshark, Nmap to detect potential cyber attacks, identifying indicators such as port scanning, abnormal DNS queries and unexpected outbound traffic. Documented findings and proposed mitigation strategies.
- Performed log analysis and anomaly detection by collecting logs from Windows servers using Sysmon and imported them into Splunk. Developed queries to identify abnormal login attempts, such as multiple failed attempts in a short period.
- Implemented a comprehensive SIEM solution to detect and respond to invalid login attempts, including standardizing data fields, creating a responsive dashboard, filtering out noise and configuring alerts for improved security monitoring and incident response.

Cybersafe Foundation - CyberGirls Fellowship **Nov 2023 – Nov 2024**

Position: Cybersecurity Analyst

- Conducted threat analysis and incident response by investigating security alerts, analyzing logs, and identifying Indicators of Compromise (IOCs).
- Performed digital forensics on compromised systems, extracting artifacts from memory dumps and network traffic using Wireshark, Volatility, and Autopsy.
- Utilized MITRE ATT&CK framework to map adversary tactics and techniques, enhancing detection and response strategies.
- Collaborated with teammates on projects, achieving a 90% success rate in incident handling, and security challenges.
- Strengthened problem-solving and analytical skills by actively engaging in hands-on cybersecurity exercises and threat-hunting scenarios.

PROJECTS

- **Threat Intelligence & Malware Detection Using YARA & VirusTotal:**
  Developed a Python-based threat intelligence solution to identify malware from a dataset of SHA-256 hashes. Automated hash analysis using the VirusTotal API, extracted key threat details, and documented findings. Conducted in-depth research on the malware's lifecycle, attack patterns, and mitigation strategies. Created and tested a YARA rule to detect similar threats, enhancing proactive threat detection capabilities. Delivered a comprehensive threat intelligence report, emphasizing cybersecurity best practices.

- **Automated Patch Management for Remote Workers' Endpoint Applications in SMEs:**
  Developed and implemented an automated patch management solution tailored for remote workers in small and medium enterprises (SMEs), leveraging ManageEngine Patch Manager Plus from Zoho and Action1 to streamline patch deployment. The solution reduced manual intervention, improved compliance with security standards, and enhanced scalability. The implementation strengthened endpoint security, minimized vulnerabilities, and optimized patching workflows for better efficiency.

- **Comparative Analysis of OSI and TCP/IP Network Models:**
  Conducted an in-depth analysis of the OSI and TCP/IP network models, focusing on their layered structures, functionalities, and practical applications. Examined the abstraction levels within the OSI model's seven layers, compared them with the four-layer structure of TCP/IP, and evaluated key mechanisms like error correction, routing, and flow control.

- **Phishing Incident Response Playbook:**
  Developed a comprehensive phishing incident response playbook to streamline detection, analysis, and mitigation of phishing attacks. Conducted investigations using URL scanners, identified IoCs to trace malicious activity. Implemented containment strategies, including EDR isolation, firewall rules, and credential resets, ensuring rapid threat eradication. Enhanced overall security posture through post-incident reviews, awareness training, and continuous improvement of phishing detection capabilities.

EDUCATION

B.A, Philosophy, University of Nigeria Nsukka **March 2024**

- 2:1, Second Class Honours, Upper Division

CERTIFICATION

Certified in Cybersecurity Certification (ISC2) **September 2024**
Microsoft Security Operations Analyst (SC-200) **January 2025**
CompTIA Security+ **In progress**
Infosec Incident Response
Cisco Networking Devices and Networking Configuration
Cisco Endpoint Security

REFEREES

Available on request.