Pius Emmanuel Papka

(234)-812-666-6799 ● piusppk@gmail.com ● LinkedIn ● GitHub ● Portfolio Website ● Medium

SUMMARY

Cybersecurity Junior with a passion for digital forensics, threat hunting and incident response. Currently building my Security Analyst Skills through the use of various CTFs, certifications and projects/Labs.

CERTIFICATIONS

CCNA ● $(ISC)^2$ CC ● CyberOps Associate ● Splunk

EDUCATION

Modibbo Adama University Yola: Degree (BTech) In Computer Science *December 2023*

CYBERSECURITY PROJECTS AND LABS

Cybersecurity Detection and Monitoring Labs

- Designed a virtualized home lab network to test vulnerabilities and practice threat detection.
- Utilized Pfsense, Splunk, Kali Linux, Security Onions, and an Active Directory environment to simulate a small enterprise network.
- Simulated offensive and defensive tactics for adversary emulation and incidence response practice.

Azure Cloud Detection Lab

- Configured and deployed azure resources including Sentinel to detect attacker persistence on a virtual machine.
- Created a custom analytics rule to generate security alerts for virtual machine activity.
- Utilized KQL for log querying and MITRE Adversary TTPs and Mitigating Procedures

AWS Incident Response Lab

- Performed incidence response on a compromised AWS account using CloudTrail logs and JQ.
- Identified a compromised AWS Bucket, IAM User and other indicators of compromise.

Threat Detection with YARA Lab

- Created YARA detection rules by manual collection of simulated malicious document IOCs
- Utilized yarGen to generate YARA detection rules for simulated malicious documents.
- Tested YARA detection rules with Arya (a tool that creates pseudo-malicious files).

EXPERIENCE

American University of Nigeria ACIT ICT center *July 2021 till Date*

Security Operations Center Analyst

- Monitor and analyze security alerts using SIEM tools, actively participate in incident investigations and develop response strategies.
- Engage in real-time analysis of security alerts to detect threats and use threat intelligence sources to increase awareness.
- Conduct comprehensive vulnerability assessments, prioritize patching jobs, and work with IT teams to ensure strong system resilience.