Princess Osei-Adubofour

E-mail: posei_adu@yahoo.com

Professional Summary & Technical Skills

- Cybersecurity professional with strong knowledge of SOC Operations, Network, Email, & Endpoint security, and Information Security and Assurance.
- Expansive understanding of the MITRE ATT&CK framework & Cyber Kill Chain model, Operating Systems
- (Windows/ Unix) logs, Windows disk and memory forensics, Computer Networking (TCP/IP), Firewalls, Proxies, Intrusion Detection/Preventions Systems (IDS/IPS), APT groups, Breach Investigation
- Well versed: ArcSight (ESM, Logger), Splunk ES, Open-Source Intelligence (OSINT) search tools, Mcafee Epo, RSA Netwitness, Trellix HX/NX/PX/Helix, Wireshark, Sourcefire, Cisco Ironport, Crowdstrike, Tippingpoint IPS, Imperva (Incapsula, SecureSphere), Archer, Remedy, Service Now, Qualys, Nessus, Nmap, several proprietary Custom tools (e.g., data enrichment; automation; etc.)
- Knowledge of common cyber-attack vectors such as port scans, man-in-the-middle, DoS, DDoS, Trojans, viruses, ransomware, web application attacks, etc.
- Proficient in Microsoft Office [Word, PowerPoint, Excel, Publisher, Access, Outlook], Linux Command line, Snort, Yara, Regex
- Effective investigative skills, time management, and exemplary communication + interpersonal skills that demonstrate the ability to work efficiently and accurately, meet goals, and manage multiple duties independently and within a team setting

Professional Certifications

CompTia Security+ce | CompTia CySa+

Education

Old Dominion University-Norfolk, VA
Bachelor of Science-Cybercrime — Anticipated Dec. 2025

Work Experience

Google — **June 2022- Present**
Cyber Security Analyst-Mandiant Managed Defense Services-Remote

- Monitors security appliances and provide advanced detection and response service though security event analysis and review
- Performs live response data collection and analysis on hosts of interest in an investigation
- Collates and analyzes relevant events from host and network device log files
- Performs incident response and basic malware analysis to investigate incidents
- Helps determine the scope of the compromise, activity associated with any malware, and assess customer impact
- Maintains current knowledge of tools and best-practices in forensics and incident response and an understanding of advanced persistent threats, including tools, techniques, and procedures of attackers

Bae Systems — **September 2019- June 2022**
Cyber Analyst II- Global Security Operations Center- Reston, Va

- Responsible for monitoring and investigating DMZ, proxy, email, & host-based alerts from a SIEM as a part of the corporate Global Security Operations Center [GSOC] team for more than 7+ global markets

- Detects and prevents Advanced Persistent Threat and generic malware infections, web application attacks, and others cyber threats.
- Performs dynamic analysis of malware using VirtualBox, Wireshark, and Remnux to discover and track C2s and artifacts for the creation of network and host-based signatures of APT and generic malware.
- Vets & enriches IoCs through intel platforms to immediately change SIEM alerting behavior
- Escalates & facilitates incident response for spear phishing emails, mass phishing campaigns, and infections and monitors remediation efforts ensuring all incident response steps have been adhered to
- Provides guidance and training for lower tier analyst

Perspecta (Contracted via Apex Systems) **October 2018-August 2019**
Security Analyst- U.S. Public Sector Delivery SOC-Herndon, VA

- Performed network security monitoring and incident response for 5+ government customers across 30+ programs in a managed security service provider (MSSP) team
- Maintained records of security monitoring and incident response activities, utilizing case management and ticketing technologies.
- Monitored and analyzed network, host, and application logs in a security information and event management (SIEM) tool to identify security issues for remediation.
- Recognized potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information
- Communicated alerts to agencies regarding intrusions and compromises to their network infrastructure, applications, and operating systems.
- Consolidated and conducts comprehensive analysis of threat data obtained from classified, proprietary, and open source resources to provide indication and warnings of impending attacks against unclassified and classified networks.
- Generated end-of-shift reports for documentation and knowledge transfer to subsequent analysts on duty

Noblis **April 2017- June 2018**
Cyber Fraud Analyst- Cyber Fraud Analytics and Monitoring (CFAM)-Lanham, MD

- Assisted the client [Internal Revenue Service, IRS] collaboratively with data analytics architects, data scientists, and the insider threat team to strengthen their security posture against fraudulent transactions through detailed and accurate forensic cyber analysis and reporting
- Triaged and interpreted system/ website/ application logs to detect fraud through analytic methodologies; working to prevent unreasonable release of user Personally Identifiable Information (PII) in identity theft cases, account take-overs, tax/refund fraud
- Operated as security watch personnel and incident responder utilizing big data security analytics software on a 24/7 team, working non-traditional hours (evenings and nights)
- Collaborated with client's cyber fraud watch and monitoring tool developers to recommend improvements for the detection of fraudulent behavior through analysis of data
- Developed visualizations dashboards and indicators that identify anomalous activities
- Analyzed business processes and synthesize potential fraud scenarios, fraud patterns, and risk indicator

Prior experience
Navy Federal Credit Union **December 2013- Feb. 2017**
Fraud Investigation Specialist- Security Operations Center (SOC)-Vienna, VA