

Henry Osei

Silver Spring, MD

nimako09@gmail.com • (240) 485-6732

TECHNICAL SKILLS

Programming: C, C++, JavaScript, CSS, Java, HTML 5, Swift, Python, SQL, KQL

Software: Office 365, Word, Jack the Ripper, Wire Shark, Logisim, VMware, Nmap, Microsoft Defender Security Center, MySQL,

Operating Systems: Linux, Mac OS, Windows XP, 7, 8, 9, 10

SIEM: Sentinel, Splunk

Cloud Computing Tools: Azure AD, Sentinel, Microsoft Defender Security Center, Cloud Application Security

EDUCATION

Bachelor of Science in Computer Science

December 2020

Towson University, Towson, MD

Related Coursework

Data Communications and Network; Data Structures and Algorithm Analysis; Cryptography; Database Management Systems; Operating Systems; Network Security; Operating Systems Security; Object-Oriented Design

WORK EXPERIENCE

Junior Cyber Security Engineer, X8 LLC, Hanover, MD

6/20 – Present

- Writing Power-Shell scripts to automate deployment, patching and playbook processes.
- Perform patch management 2 times a week using Qualys.
- Use KQL to write Sentinel monitoring alerts.
- Perform system and network log audits in pursuit of anomalous behavior.
- Handles phishing email testing internally to allow users to distinguish legitimate emails from phishing emails.
- Handles incoming alerts and perform internal investigations.
- Create and update procedures for working processes.
- Perform ongoing update to SIEM and other security tools with indicators of compromise discovered via open-source intelligence.
- Provided technical documentation for ongoing work processes.
- Handles technical onboarding of new employees.
- Handles security controls and security guidelines.
- Perform Security Assessments on assigned systems using the Risk Management Framework (RMF) guidelines.
- Use SIEM for real time system monitoring, analysis, evaluation, forensic investigation, and for enforcing the company's security policies compliance.
- Perform risk assessments, update and review System Security Plans (SSP) using NIST 800-171, Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration.
- Implements security guideline framework using NIST 800-171.
- Cooperates with team members for CMMC implementation and gap assessments to assess compliance.
- Implements advanced hunting queries to look for malicious processes; malicious activity within end-point users.
- Reviews Conditional Access Policies.

- During my tenure at Hughes, I gained a deeper understanding of satellite internet and associated concepts. I also expanded upon my understanding of secure networks, specifically VPN and IPSec, and firewalls including how traffic is handled and dealt with the white and blacklist.
- I gathered data from various team members and stakeholders on devices and their applicability in store settings. Through the data gathering and analysis, I was able to gain a better understanding of the store level network diagram as it relates to the devices.
- Analyzed and organized numerous customer traffic by source and destination.
- Managed Firewall Policies document with attention to configuration control
- Created and executed procedures for port forwarding.