Cyber Security Technician Cyber Security Technician Cyber Security Technician - Novant Health UVA Health Systems Prince William, Medical Work Experience Cyber Security Technician Novant Health UVA Health Systems Prince William, Medical - Center, VA, US May 2011 to Present Ensuring Patients and employee data security against threats with data de-identification. Conducting data loss prevention with and implementing appropriate measures. Prioritizing data loss scan on repositories based on pre-defined criteria and policies. Analyzing potential privacy violations to identify false positives and policy violations with immediate remediation. Conducting SIEM analysis and generating dashboard/reports. Identifying vulnerabilities through scans and penetration tests to report the issues. Scanning and Identifying Indicators of Compromise (IOC's).

Performing threat intelligence and implementing Cyber Kill Chain defense against APT. Employing cyber modeling techniques to identify malicious threats and activities. Analyzing network traffic for malicious or abnormal activity for attack vectors. Identify adversary's Tactics, Techniques, and Procedures (TTPs) for technical mitigation strategies for preventing, controlling, and isolating incidents. Performing malware analysis using different malware analysis methodologies. Performing digital forensics to identify suspicious malicious content. Conducting intrusion detection and prevention. Performing log analysis and identifying malicious activities. Cyber Security Specialist DUANE READE - Manassas, VA August 2015 to January 2016 Analyzed compromised machines to provide explanation of break-in process Investigated email threats, fraudulent emails and copyright violations Researched in-progress attacks by use of network sniffers Analyzed pre-production systems for security vulnerabilities. Responsible for phishing mail box, blocking URL's and log analysis. Researched on an emerging threat, updated emerging threats, and detection capabilities. Analyzed most prevalent vulnerabilities, threats, attack methods, and infected vectors. Assisted SOC hire and training on Networking and Security fundamental of TCP/IP and other core Internet protocols. Monitored Security Information and Event Management (SIEM); Intrusion Detection System (IDS); Network Monitoring and Response Services. Managed global threat landscape by tracking changes in directing Manage services. Responded to evaluation-related queries from the evaluation facilities and assisted in resolving

evaluation-related issues. Network Administrator Uncommon Goods LLC - Brooklyn, NY May 2010 to July 2011 Managed all new install projects for servers, switches, and other network resources. Developed and updates documentation, appraising users and administrators of vital information. Provided adequate controls to ensure system security and access granted to users on a "Need to Know" basis. Administrated and maintained environment security. Involved with administering security alerts to staff and weekly data backups. Performed all levels of hardware and software systems support for over 200 dispatching computers. Performed hands-on administration, monitoring, and troubleshooting of Local Area network (LAN), resulting in optimum performance and minimum downtime. Designed, developed, and modified reporting processes in accordance with client specifications. Coordinated data transfer requirements between Organizational Maintenance Activities and all other automated information systems, such as ensuring all data stored on media transferred Established procedures for all systems recovery and contingency processes to include back fit processes. Established and maintained a system log, recording all down time, hardware failures, database saves, and all other system requirements established Education AS in Business Administration Southern New Hampshire University - Manchester, NH 2015 to 2018 AS in Business Administration Northern Virginia Community College - Annandale, VA 2012 to 2014 Skills CYBER SECURITY, FIREWALL, MALWARE, SSL, DATA LOSS PREVENTION, DLP, IDS, IPS, NESSUS, NMAP, SIEM, SNORT, SPLUNK, VPN, WIRESHARK, SECURITY, ACTIVE DIRECTORY, LDAP, TCP, TCP/IP, Comptia, Information Security, Network Security, Cybersecurity Certifications/Licenses Security+ CE July 2019 to July 2022 CPR/AED Associates in Business Administration August 2018 to Present

Name: Nicole Smith

Email: shartman@example.com

Phone: 272-851-7409