Network Security Engineer Network Security Engineer Network Security Engineer/ Analyst, B.S. Cybersecurity | C|EH | Sec+ | CySA+ | Server+ Woodbridge, VA Skilled and detail-oriented Cybersecurity professional with over 4+ years of hands-on experience with diagnosing network infrastructure issues, assessing security controls, and hunting for potential threats on network systems. Well-versed with several network security tools to efficiently and effectively isolate system deficiencies. Clearance: Top Secret Certifications: Certified Ethical Hacker CE ComTIA Cyber Security Analyst + CE CompTIA Security + CE CompTIA Server + Education: University of Maryland University College- B.S. Cybersecurity Dec 2018 SANS Incident Response Certificate Program Jul 2019- Sep 2020 Cybersecurity Skills: Skilled user of SIEM, McAfee ESM, Snort, Kibana (ELK), endpoint protection (HBSS), vulnerability scanner (ACAS & Tenable Nessus), Tcpdump, Wireshark, Crowdstrike (EDR), and Kali Linux. Experienced with multiple raw data analyzing tools. Work Experience Network Security Engineer Office of Naval Research - Arlington, VA May 2019 to Present Responsible for deploying a fully operational SOC environment to provide continuous visibility into active cyber threats and risk, actionable analysis to proficient investigations, and remediation orchestration. Ensures operational health of McAfee ESM (SIEM) that includes comprehensive data log ingestion from multiple receivers, such as firewalls, IDS, routers, switches, databases, virtual boxes (VMware), access points, and endpoint security (HBSS) Provides cyber threat analysis and remediation procedures to client, develops dashboards for better threats and risk visualization, and integrates open source threat intelligence to McAfee ESM Supports creating incident response playbook and SOPs Detects, identifies, and investigates cyber threats using the McAfee ESM Network Defense Analyst Tier II Army Research Lab - Adelphi, MD May 2018 to May 2019 Responsible for detection, identification, and investigation of active cyber threats and alerts through routine analysis within SIEM tool and raw data pcap examination utilizing tcpdump and other raw data analyzing tools. Performs real-time proactive network security monitoring and reporting with various security applications, such as SIEM, Snort, endpoint protection (HBSS), vulnerability scanner (ACAS), and Full Packet Capture Conducts threat profiling, retrospective analysis, and intrusion detection attempts investigation using SIEM, Snort, BRO log files, and deep

packet analysis of raw data (pcap, string, hexadecimal, and binary) using TCPDUMP and other analysis tools Monitors and investigates false positive alerts in cloud sensors using Kibana (ELK) Fine-tunes IP Watchlist, string search, domain list, and Snort through SIEM Provisions security initiatives through predictive and reactive analysis through articulating emerging threats and trends Generates Intel Reports to clients using open source and commercial threat intelligence research to determine IOC's, new vulnerabilities, and other attacker TTPs Appropriately informs and advises management on events, incidents, and incident prevention and if necessary, issues IP block Reports confirmed incidents to ARCYBER, AFNOSC, NCDOC, and DoD CERT Joint Force Headquarters Security Control Assessor FDIC - Arlington, VA March 2018 to May 2018 Conducted Independent Verification and Validation (IV&V) assessments on Government systems by successfully helping clients go through the four steps to C&A and A&A, such as planning, certification, accreditation, and continuous monitoring. Evaluated overall security compliance of Government systems and applications by utilizing OpenFISMA to ensure compliance to NIST 800 series, FISMA, FIPS 199, and FIPS 200 Analyzed security functions for design weaknesses and technical flaws by testing against NIST 800-53 and by using Tenable Nessus Vulnerability Scanner and Burp Suite to verify system vulnerabilities Coordinated with PenTesting Team to properly assess public facing websites, SSPs, POAMs, and AORs to adequately advice the clients of the necessary countermeasures on how to mitigate the risks found Conducted verification and validation for security compliance of low and moderately complex information systems, products, and components Performed re-testing of system security compliance to ensure that proper security controls are in place to mitigate previously specified risks and weaknesses IT Analyst FDIC - Arlington, VA October 2017 to March 2018 Responsible for providing Information Technology support to Federal Deposit Insurance Corporation to ensure service usability, availability, and security. Provided support to McAfee security related issues, VPN configuration, VDesk, and Jump Host problems Administered, provisioned, and removed user accounts to multiple applications to ensure implementation of principle of least privilege (PoLP) and potential privilege creep Utilized Active Directory, Bomgar Remote Access Tool, and Citrix Mainframe Receiver to

support client Information Technology related issues Identified, verified, and escalated security related issues to CSIRT, such as unauthorized use of FDIC device overseas, phishing emails, and reported anomalous workstation behavior Senior Airman- Systems Analyst US Air Force - Andrews AFB, MD March 2011 to March 2017 Responsible for the system analysis and security of the USAF's Logistics Readiness program. Collected and maintained data within On-Line Vehicle Integrated Management System (OLVIMS) and ensured that data is clearly defined Properly provided systems administration support for Windows systems including server and workstation upgrades Supported compliance for specific STIG requirements Performed daily backup operations, ensuring all required file systems and system data are successfully backed up to the appropriate media Administered creation, modification, and deletion of user accounts per request Conducted periodic performance reporting and system metrics to support audit requirements Followed patch management best practices to appropriately apply patches and upgrades on a regular basis Education B.S. in Cybersecurity University of Maryland University College December 2018 Skills Cisco, Vmware, Office 365 Military Service Branch: United States Air Force Rank: E-4 Certifications/Licenses ComTIA Cyber Security Analyst (CySA+) Certified Ethical Hacker (C|EH) CompTIA Security + CompTIA Server+

Name: Paige Spencer

Email: blakeaguirre@example.net

Phone: (586)982-3084