US EPA Cyber Security Engineering Team Lead US EPA Cyber Security Engineering Team Lead US EPA Cyber Security Engineering Team Lead - GDIT Chapel Hill, NC Information Security professional providing security experience for a collaborative, technically progressive environment. Advising engineering solutions for business opportunities Ensuring confidentiality, integrity, and availability of information and information systems. Work Experience US EPA Cyber Security Engineering Team Lead GDIT April 2018 to Present SOC Security Engineer team lead; managing team of 8 engineers and developers. Translate business requirements into deliverables and milestones; ensure project tracking & completion Delegate work between engineering team; project tracking with stakeholders POAM & Milestone completion for FISMA, NIST standards; polices & procedures Roadmap long term cyber security goals and milestones for business posture Organize daily standups; fulfillment of Secure SDLC US EPA Senior Security Engineer GDIT September 2017 to April 2018 SIEM Administration - ArcSight including; O&M Log connector setup; patching & updates; etc. Symantec Bluecoat, FireEye, and NetApp Administration Cisco product administration including: AMP, Firepower, and ThreatGrid appliances Secure SLDC for DevOps team collaboration using AWS environment, including testing and QA phases. Cyber forensics using Encase to solve malicious activity on end user device Server & OS Hardening for Windows and Linux using CIS Standards Vulnerability management including patching and software updates for servers Vulnerability monthly scanning using Nexus, report generation. CDM Archer administration for user tracking, report creation PKI management and SSL creation for servers Architect cyber security environment as well as documentation of all technical procedures Ensure US EPA CSIRC meets NIST-800 frameworks, standard, and polices Lenovo - Senior Information Security Specialist North America Transitional June 2016 to September 2017 Application security lead for North America Transitional services, managing individuals and products Application security development for projects; UWC, LCD, LCMT, S2D - products with AWS environment Rapid7 SIEM (InsightIDR) rollout and administration, documentation compliant to NIST. VMware security architect for Lenovo's Ship2Desk project - created security polices for project. IPs/IDs security configuration, alerting, monitoring, and rule setup for OSSEC,

ModSecurity, Nginx+ Server and VM hardening for Windows and Linux using CIS standards Rollout of on-premise password manager Password Manager Pro - Documentation compliant to NIST Web Application Firewall setup (ModSecurity) - rule creation, and implementation to AWS instances Secure SLDC process including; static and dynamic scanning using Coverity Collaboration with DevOps team to ensure security within every process of SLDC Vulnerability scans monthly using Nexpose & Metasploit Vulnerability management and tracking followed by report on remediation and processes Penetration testing apart of SLDC during development phase, before and after development completion PKI encryption for services being deployed on web servers; including SSL certification creation Security technical documentation for all projects & whitepapers Developed security awareness training for NA Transitional services for DevOps team Senior Software Security Engineer January 2016 to June 2016 Security application admin for tools: Fortify, SecureAssist, Contrast, SonyaType, SecureAssist within PI Vulnerability scanning monthly of all IP range within PI Splunk admin for PI: data extraction, log management, configuration setup, alert and application alerting Splunk data aggregation, collection, alerting, compliance for PI. Collaboration with DevOps team to ensure Secure SDLC Malware analysis within FireEye - full pipeline process Packet Analyze using Wireshark & Nmap for incident response for security ticket escalation Penetration testing with Metaspolit on a product deployment basis and Ad-hoc basis Documentation of technical work plans on how to use tools Software Security Engineer SAS Institute May 2015 to September 2015 Data encryption via PKI certificate management for SAS products within AWS environment Collaborated on security architecture project "Walled Garden" for security intrusion protection Web development for "Walled Garden" within AWS environment Developed strategy to deploy automated Asymmetric PKI certificates for client login and data encryption Encase use for cyber forensics for client examination Developed security strategies for software development team for AWS EC2 instances Conducted security Reviews of OWASP Top 10 within SLDC SLDC Static and Dynamic code analysis IT Analyst Guys' & St. Thomas Hospital September 2014 to April 2015 Provided technical support to office including; troubleshooting, hardware, software setup, and patching AD and GPO for access

control policy review, user creation, windows administration Reviewed and created security polices for system and employee awareness Web Application development using JavaScript Data extraction and analysis from MySQL database Education Masters of Science in (MSc) - Computer Science & Security King's College London - London Bachelors of Science in (BSc) - Computer Science & Design University of Sussex - Brighton Skills AWS (2 years), Bash (Less than 1 year), Cisco (Less than 1 year), Encase (Less than 1 year), Git (Less than 1 year), HTML (Less than 1 year), IOS (Less than 1 year), Java (Less than 1 year), Jira (Less than 1 year), Linux (1 year), Metasploit (1 year), NetApp (Less than 1 year), Nexpose (1 year), Nginx (1 year), Python (Less than 1 year), Security (4 years), Splunk (Less than 1 year), Unix (Less than 1 year), Wireshark (Less than 1 year)

Name: Johnny Peck

Email: james60@example.org

Phone: (618)210-1847x8280