Information Security Analyst Information Security Analyst Information Security Analyst - InterVarsity USA A dynamic self-motivated Information Security Engineer with about 9 years of industry experience. Analytical, detail oriented, insightful and a problem solver who enjoys exploring new systems, tools and networks. Work Experience Information Security Analyst InterVarsity USA - Madison, WI April 2018 to Present Planning, implementing and upgrading security measures and controls to protect systems, networks and data; Maintaining data security access control processes and monitor security access levels for all applications Managing firewall system by updating, auditing rules and monitoring system logs. Conducting internal and external security audits and supervising remediation of key issues Monitoring of IDS/IPS systems, including end point security, wireless security access, data loss protection, threat protection, etc.; Performing risk assessments and testing of security measures for information processing systems; Creating, testing and implementing technology disaster recovery plans; Developing and maintaining an Incident Response plan and document / conduct analysis on any reported or detected security breaches to determine their root cause; Conducting security awareness training for the organization including simulated phishing attacks; Works closely with Development, IT Services Delivery, Desktop Support, Legal and Executive staff; Ensuring ongoing adherence to pertinent laws, regulations (PCI, HIPAA, GDPR), policies and procedures; Training IT staff on network and information security procedures and staying up-to-date with security methodologies and procedures. IAM Cloud Migration Architect Wells Fargo Bank - Glen Allen, VA October 2016 to April 2018 Successfully migrated over 500 banking applications with right entitlements in cloud Azure; Identified and evaluated security gaps and helped create security project plans; Liaised with internal team leads on security issues to find resolution and remediation plans; Investigated to identify potential issues related to access controls and propose solutions; Performed testing for PKI related to existing software, digital certificates and new software upgrades; Worked with related engineering teams to ensure controls like MFA are successfully integrated into applications; Demonstrated expert level skills in collaboration with different stakeholders, influenced decisions, and the ability to take strategic view of every situation at hand; Acted as IAM Solution Subject

Matter Expert (SME) for the Access Request & Approval service, while consulting with IAM stakeholders, LOB and technology partners, User Acceptance Testers, etc.; Worked closely with DevOps, application development and QA teams throughout the SDLC stages; Depicted complex ideas, issues and designs to varied audience; communicates project objectives, scope and status to other project teams. Cyber Security Engineer The Vitamin Shoppe - Ashland, VA May 2013 to October 2016 Periodic penetration testing and vulnerability assessment on internal network to check for the various vulnerabilities in the network and ensured to communicate the correct mitigation measures using Nessus; Conducted exams on compromised computers, servers, and other related hardware devices; Performed Active Cyber Threat Hunting using both manual and machine-assisted techniques to identify tactics, techniques and procedures of advanced adversaries or threat agents; Leveraged aggregated cyber threat intelligence, log, network flow, and anomaly data for analysis, research and the identification of potential compromise within applications; Implemented corporate security standards and procedures to ensure the security, reliability, and accessibility of data, applications, networks and infrastructure components; Ensured that all compliance and vulnerability management services are operating and performing within established program guidelines; Performed daily alert-based monitoring of information security events and initiate response procedures in accordance with established processes with SIEM tools; Analyzed server and firewall logs, scrutinizing network traffic, updating virus scans, and troubleshooting; Developed training programs on all security and information governance policies and determined the types of training that should be developed on critical policies, as well as, how often the training should be conducted; Provided input on Incident Response process definition and support the development and maintenance of documented play-book procedures, knowledge articles, and training material; Assisted with the development of processes and procedures to improve cyber incident response capabilities; Maintained awareness of shifts in business structure and strategy and possess the ability to recognize the impacts potentially has to the Cybersecurity organization position and risk threshold; Implemented new and manage existing security technology and remediation solutions, including server and software installations, configurations, and other related

deployment activities; Ongoing application of NIST Publications SP 800-18, SP 800-30, SP 800-37 rev 1, SP 800-53 rev 4, SP 800-53A, SP 800-60 and Federal Information Processing Standards (FIPS) - FIPS 199 and FIPS 200. IT Security Analyst Core-Tech Consulting - Stafford, VA November 2011 to May 2013 Worked on periodic and on-demand system audits, penetration testing, vulnerability assessments, and third-party security reviews to ensure that business partners, applications, networks, and infrastructure components adhere to security standards and policies; Performed root cause analysis to identify gaps and provided technical and procedural recommendations that will reduce Client's exposure to cyber-risks; Conducted risk assessments and collaborated with clients to provide recommendations regarding critical infrastructure, network security operations and Continuous Monitoring processes; Provided intelligence regarding intrusion events, security incidents, and other threat indications and warning information to clients and stakeholders; Assisted in vulnerability assessment, patch management, incident management and continuous monitoring; Managed and deployed endpoint detection and response solutions for a multi-tenant environment; Analyzed and remediated findings discovered during scheduled internal and 3rd party vulnerability; Served as a hands-on technical expert working directly with various teams to provide guidance and ensure the solutions they deliver adhere to security standards and policies; Researched and analyzed log sources for the purpose of security monitoring, particularly security and networking devices (such as firewalls, routers, anti-virus products, proxies, and operating systems). Education MSc. in Digital Forensics Council University 2018 to Present BSc. in Finance University of Ghana - Accra, GH 2007 to 2011 Additional Information SKILLS & CORE COMPETENCIES: Experience with SDLC Methodologies; Experience with Cloud Computing (AWS, Azure); Strong knowledge of Security Controls (NIST 800 Series, ISO, SOX, PCI, NIST CSF, HIPAA/HITRUST, DIACAP); Identity & Access Management; Penetration Testing & Vulnerability Assessments (Burp Suite, SPLUNK, AlienVault, Qualys, Nessus); Network Security and Threat Analysis (OWASP 10, Routers/Switches, Firewalls, TCP/IP, VPN, IDS/IPS, DLP, SSL/TSS); Software and Platforms (Linux/Unix, Windows, iOS, Android, Cloud Computing, C, JavaScript, Python, etc.).

Name: Victor Phillips

Email: lindseyholloway@example.org

Phone: (762)689-5964x7546