Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Saint Paul Public Schools Talented IT Security specialist with three years of experience and expertise in Penetration testing, implementing, and troubleshooting network infrastructure and security Certified CompTIA Security+ Proven record of evaluating system vulnerability in order to recommend security improvements as well as improve efficiency while aligning business processes with network design and infrastructure. Strong hands on and exposure to IDS and Vulnerability scans on a regular basis Familiar and experienced with Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering) Experienced with Checkpoint Firewall Management station operations Experienced with implementing malware protection, policy control and analyzing logs Superior capacity to solve complex problems involving a wide variety of information systems Worked independently on large-scale projects, and thrive under pressure in fast-pace environments while directing multiple projects from concept to implementation. Experienced with extensive client interactions. SQL trained professional and performed few projects Authorized to work in the US for any employer Work Experience Cyber Security Analyst Saint Paul Public Schools February 2016 to Present Researched and analyzed known hacker methodology, system exploits and vulnerabilities to support Red Team Assessment activities Conducted onsite penetration tests from an insider threat perspective Performed host, network, and web application penetration tests Performed network security analysis and risk management for designated systems Performed APT to check backdoors in the network Configured rules and Maintained Palo Alto Firewalls & Analysis of firewall logs using various tools Penetrated network defense mechanisms externally utilizing various methods and techniques (withheld for operational security) Analyzed malware behavior, network infection patterns and security incidents using Tenable Security Centre. Analyzed approximately 10 classified network security intelligence reports on a daily basis Produced advisory reports regarding 0-day exploits, CVE vulnerabilities, current network Performed risk assessments to ensure corporate compliance Insured the security of different applications using standard encryption, decryption, and hashing with RSA and SHA-1 Managed Privilege Account Management using Cyberark. Conducted security event monitoring for corporate wide in-scope

applications with eGRC platform (RSA Archer) Performed application security and penetration testing using Metasploit. Provided up to ten on-site server maintenance visits on a monthly basis, troubleshooting various technical problems and performing operating system administration with Linux-based computer systems. Created written reports for compliance HIPAA, SOC type1 and 2 and PCI, detailing assessment findings and recommendations associated with HIPAA Compliance. Provided occasional, assistance with the development and maintenance of internal Red Team methodology, to include training program Managing the SIEM infrastructure Proposed remediation strategies for remediating system vulnerabilities using Nexpose. Developed Security Assessment Plan, Security Assessment Report, Security Assessment Questionnaire, Rules of Engagement, Kick off Brief, and Exit Brief templates Developed CVSS calculator to rate risk for vulnerability using Excel Created OWASP web application test cases and mapped them to associated NIST 800-53 Rev.4 security controls Monitored the security of critical systems (e.g., e-mail servers, database servers, web servers, etc.) and changes to highly sensitive computer security controls to ensure appropriate system administrative actions, investigate and report on noted irregularities Responsible for the Core Security of the Network. Managing the entire Network Security Products deployed in the network such as Checkpoint (GAIA R75.40/77.20) Developed Continuity of Operations (COOP) and Disaster Recovery (DR) operations and conducted evaluation of COOP and DR during annual incident response training Monitored Traffic and Connections in Checkpoint and ASA Firewall Ensured organizational compliance with CFCU information security programs Configured & Administered of the Checkpoint Firewall that includes creating Hosts, Nodes, Networks, Static & Hide NAT's Investigated potential or actual security violations or incidents in an effort to identify issues and areas that require new security measures or policy changes IT Security Analyst-Jr Anion Health Care - Hyderabad, ANDHRA PRADESH, IN May 2013 to December 2014 Penetration Tester Conducted incident prevention, detection/analysis, containment, eradication and aid recovery across IT systems until the company was acquired in 2013 Managed SIEM infrastructure Performed attack simulations on company systems and web applications to determine and exploit security flaws Identified attacks XSS, CSRF in the network

and prepared report by using Nessus and Metasploit Handled threats by SDL Threat Modelling Handled flows from "black box" to "grey box" to "white box" testing according to clients' needs Test form factors and technologies based on scopes of work Performed application and infrastructure penetration tests along with physical security reviews Defined requirements for information security solutions and perform reviews of application designs and source code Designed, developed and implemented penetration tools and tests and also used existing ones to handle penetration testing activities Document and discuss security findings with information technology teams with eGRC (RSA Archer) Worked on improvements for security services and provided feedback and verification about existing security issues Determined system and application flaws by indulging in approved hacks Conducted vulnerability tests and analyzed problems in a methodical manner Analyzed and reversed engineer codes to discern weaknesses and provided feedback to penetration testing teams Assisted in developing appropriate security measures for system flaws Maintained activities log for each penetration test administered and its outcomes Defined, established and managed security risk metrics and track effectiveness Coordinated with third parties to perform vulnerability tests and created security authorization agreements and standards Facilitated scrum ceremonies (grooming, sprint planning, retrospectives, daily stand-ups) Looked for ways for continuous improvement and was focused for the productivity of the Scrum security teams and the quality of the deliverables Empowered teams to self-organize and grow cross-functionality Educated business unit managers, IT development team, and the user community about risks and security controls Communicated with higher management, engineers, product owners and support specialists on product issues if found any The ability to balance risk mitigation with business needs Prepared detail practices and procedures on technical processes Analyzed security incidents and presented a quarterly report to the CIO Performed security research, analysis and design for all client computing systems and the network infrastructure Developed, implemented, and documented formal security programs and policies Monitored events, responded to incidents and reported findings Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention

(DLP), forensics, sniffers and malware analysis tools IT Security Engineer CTRLS Data Centric - Hyderabad, ANDHRA PRADESH, IN June 2012 to February 2013 Developed Black Box Security test environments & conducted tests as part of team for precautionary measures Helped onboard new members to organizational security practices and trained them in Cyber Security. Monitored and assisted with access controls and securing data of sensitive systems Conducted penetration test when required in the organization Collaborated with business units to determine continuity requirements Conducted business impact analysis for vital functions; document recovery priorities of the key processes, applications and data Established disaster recovery testing methodology Planned and coordinated the testing of recovery support and business resumption procedures while ensuring the recovery and restoration of key IT resources and data and the resumption of critical systems within the desired timeframe Provided technical support for hardware problems and specific applications Education Masters in Information Security and Intelligence Ferris State University - Big Rapids, MI May 2016 Bachelor of Technology in Computer Science Engineering Jawaharlal Nehru Technological University May 2013

Name: Frank Hall

Email: smithshawn@example.com

Phone: 001-845-469-8310x29850