Enterprise Security Analyst Enterprise Security Analyst Enterprise Security Analyst - Proxim Systems Work Experience Enterprise Security Analyst Proxim Systems - Pekin, IL March 2016 to Present Experience working in environment with regulatory compliance requirements (HIPAA, PCI, etc.) Assist in the development of security policies and standards to help ensure compliance. Review and develop internal security documents, controls, and procedures on a regular basis. Conducts and assists with the development of Security Awareness training material. Performs vulnerability scans and assists with the Vulnerability Management process using Qualysguard. Manage, monitor, and perform signature tuning for IDS/IPS infrastructure like Cisco SourceFire. Manage Security Information and Event Management (SIEM) tools like ArcSight Experience with Symantec Data Loss Prevention (DLP). Ensuring DLP & tracking the incident from inception till resolution. Maintaining rules and actions to the policies in DLP based on the discussions with various security teams within the enterprise. Managing the accuracy of DLP identification to lowering/avoiding false positives and negatives. Discovered risks & thereby implemented remediation processes in environments with DLP policy violations. Log analysis and responding to IDS/AV alerts and taking appropriate action like scanning endpoint systems. Experience in working with end-point security like Symantec Endpoint Protection and Anti-Virus. Provided Day to Day operational Support to resolve tickets related to Security Incidents like Phishing attacks. Recommends controls for reporting, analyzing, and reducing the impact of security incidents. Performs forensic investigations for security events and HR investigations. Conducts and assists in Vendor Risk Assessments based on the type of data handled and services provided by the vendor. Client1: United Health Group, Eden Prairie, MN Information Security Analyst Support the resolution of Audit, Compliance, or Risk Management related issues that could impact the confidentially, availability or integrity of data or processes. Conduct and manage vendor risk assessments and due-diligence reviews Creates and coordinates IT/business audit risk assessments; develops and executes IT/business audit testing plan; discuss results with Management and provides guidance on control issues and concerns. Tracks and manages audit issues to completion; ensures that clients' responses are received in a timely fashion, are in line with

recommendations, and have a reasonable estimated completion date using GRC tools like eGRC. Support the integration of the IT Risk Management practices into key Information Technology and business areas. Ensure vendor compliance to the business agreement, policies, procedures, & regulations along with ability to map controls and compliance requirements Play a leadership role on key projects and ensure that key IT risks are being adequately addressed. Provision assessment reports and executive summaries with recommendations & direction regarding remediation efforts and disposition of the third party Communicate, escalate, and track vendor progress on assessment remediation activities. Act as a liaison & SME(subject matter expert) for internal departments & vendors to successfully manage Vendor Risk Assessment Maintain current knowledge on information security topics and their applicability program requirements. Security expertise including knowledge on different security risk assessment frameworks (NIST/Octave), standards (SSAE 16/ISO27001/HITRUST). Information Security Intern Cyber Advanced Technology - Berkeley, CA August 2015 to December 2015 Design, configure and maintain applications for credit card authorizations. End-to-End hardware encryption of PINs all along the processing and facilitate secure printing of PIN mailers at the print facility. As part of the solution, the encryption of PIN data was upgraded to industry standard 3-DES algorithm, Hardware Security modules (HSMs) and distributed encryption services were installed to securely decrypt and print the mailers. Compliance to federal and internal standards for security and cryptography. Meetings with technology and business for proper understanding of requirements. Experience working in operations environment with commitment to procedurals ways of working, security disciplines, strict changes process and emphasis on availability of services. Planning, execution and testing of IT internal controls, performing quarter internal audit & maintaining the Asset Register. Evaluated Information Security & associated Risk Exposure. Setup policies to scan data for sensitive information like SSN, credit cards. Have experience handling data at rest and data in motion. Worked on complex and critical security and compliance issues. Log analysis & managing the accuracy to lowering/avoiding false positives and false negatives. Responded, investigated and reported IT security incidents. Provided day to day operational support to resolve remedy tickets

related to security incidents. Information Security Intern CloudPassage - San Francisco, CA May 2015 to August 2015 Full audits of files, review and cleanup permissions, audit of Halo policies (Firewall, CSM, FIM) Assisting Product Management team to help write CSM policies Following and writing end-user security guidelines which include Full Disk Encryption of Windows, Backing up codes, Laptop security, Firewalls setup, Installing Software Updates/ Security Patches, Password Manager, Antivirus, Web Browser security, Social Engineering guidelines. Enabling two-factor authentication for all the email accounts Providing physical security on front desk with the use of visitor sign-in system Backup all files on Git server. Installation and use of GAT(General Audit Tool) Making an inventory of all the softwares used on different system and associating a critical level with each of them. Responsible for handling day-to-day operational security tasks including responding to corporate security incidents, threat assessments, participating in incident management, collecting evidence, providing analysis for corporate investigations, reviewing and responding to user issues, and taking part in disaster recovery exercises. IT Intern Populus Brands - Los Angeles, CA January 2015 to May 2015 Experience working in operations environment with commitment to procedurals ways of working, security disciplines, strict changes process and emphasis on availability of services. Planning, execution and testing of IT internal controls, performing quarter internal audit & maintaining the Asset Register. Evaluated Information Security & associated Risk Exposure. Identified and documented potential risk on financial based application during remediation process. Experience in working with Remediation team on financial application. Maintaining the PCI Data Security Standards & Compliance status of user information & customer database storing essential Credit Card information. Information Security Analyst (Part-time) USC ITS January 2014 to December 2014 To speak and work with customers in person and over the phone. Alongside to troubleshooting complex technical problems and work independently to complete assigned projects. Experience working in operations environment with commitment to procedurals ways of working, security disciplines, strict change control process and emphasis on availability of service Worked on various enterprises security applications like Nessus and performed implementation, configuration, upgrading and policy creation. Monitored,

Evaluated & Responded to the vulnerability scanning of IT network and system using Nessus and remediation activity with responsible system administrator to resolve unauthorized activity within global computing environment. Discovered, analyzed, diagnosed and reported on malware events, files and vulnerability issues. Investigated the root cause for suspicious threats, analyzing the global threats in the IT environment and Solution designing. Developed policies and procedures to mitigate incidents for the entire computer network. Analyzed security risk and performed risk assessment for different applications. Monitored firewall logs for assessing security events and activity using log rhythm. Reviewed authentication, security event logging and monitoring of various servers. Network monitoring, Traffic capturing using Wireshark. Education MS University of Southern California - Los Angeles, CA December 2015 BE in Computer Science Panjab University - Chandigarh, Chandigarh June 2013 Certifications/Licenses Security+ July 2018 to July 2021

Name: Anthony Taylor

Email: dfoster@example.org

Phone: 874-418-7685