Information Security Administrator Information Security Administrator Information Security Administrator - Lender Service Provider, LLC Chantilly, VA Authorized to work in the US for any employer Work Experience Information Security Administrator Lender Service Provider, LLC - Fairfax, VA November 2017 to Present - Lead the security operations service to ensure accurate and rapid response to critical security event. - Advise and consult with customers on risk assessment, threat modeling and vulnerability management. - Perform packet analysis/ monitor traffic logs using Nmap and Kiwi Syslog. Analyzed and mitigated security vulnerabilities, hacking attempts, and other realized risks. Stopped leakage of sensitive information and prevented damage to the company's reputation on numerous occasions. - Collect and analyze technical network activity for anomalies that could indicate potential threat issues from current and previous employees, contractors or partners. - Conduct periodic review to ensure compliance with established configuration management procedures, ensuring all software, hardware and firmware changes recorded as required. - Assisting management with business Continuity, Disaster Recover, Contingency Plan and Business Impact Analysis. - Responsible for annual review/updating company IT security policy. - Performed security baseline and risk assessment for IT projects, using business and customer requirements to perform security specification, development, testing and launch. - Conducted internal IT pre-audit to achieve 100% SOC1 type II compliance including user access review, network protection, third party management, change management and back up management process. - Conducting quarterly security user awareness training for new hires within IT and provided quarterly phishing test and training courses utilizing Knowbe4 for clients - Assisting manager with security analysis utilizing using SIEM tools such as Splunk Enterprise Security - Configure, maintain and support network equipment such as end point protection, patches firewalls and IDS, assisting with implementation of countermeasure and mitigating controls. - Conduct and support vulnerability scanning program (Nessus) including the scheduling of scans, production of reports and interpretation of results for all clients. - Assessed security and advised on any detected vulnerabilities in the infrastructure including software, hardware and networks. - Respond to security incidents raised by user community including phishing attempts, malware outbreaks, and

unauthorized access attempts. - Capture, document and report discovered or suspected security, privacy and confidentiality incidents to the management - Review configuration changes for the system and the impact of change. Ensuring all software, hardware and firmware changes are recorded as required by established configuration management procedures. - Perform research and make recommendations on cyber security best practices, new technologies and protection capabilities. Provide advice and recommendations for IT device hardening while maintaining current security equipment with latest software and patches. - Assisting manager in the presentation of the security capabilities to clients to remediate and mitigate findings. - Maintain up to date knowledge of IT security industry, including awareness of new or revised security solutions, improve security process, and the development of new attacks and threat vectors. IT security Analyst SNC Systems LLC - Fairfax, VA February 2010 to October 2016 - Performed enterprise- wide internal and externa vulnerability testing and scanning monthly to assess the company's security posture using Tenable Nessus - Prepared reports on scanning results monthly and recommended solutions to mitigate risks. - Participated in project planning sessions with customers, suppliers and team members to review and refine business requirements and assess feasibility of the solutions or system enhancement. - Analyze network traffic and various log data to determine the threat/impact against the network, recommended appropriate countermeasures and assess damage. - Responding to and remediating all cyber security incidents within the timeframes defined by applicable SLAs. - Leads efforts in the improvement and development of process/procedure manuals and documentation for incident response, threat intelligence, advanced persistent threat detection and vulnerability analysis. - Create, update and approve operational cyber security workflows and internal documentation. - Documentation, development and testing of Splunk dashboards and alerts. - Assist with the development of a cyber- security awareness program and security training; assisting management to get updates on their information assurance knowledge constantly because changes of their position, duties, overall risk environment. - Assisting management in the assessment of project risk and controls by providing analysis of system requirements relating to vulnerability reviews, and risk &contingency planning. Education Bachelor of Science in Business

Logistics University of Maryland College Park - College Park, MD Certifications/Licenses Associate CISSP CEH CCNA Security CCNA switch and routing ITILv3 Security+ Additional Information Strong communication skills and ability to engage with customers to understand their requirements - Advanced analytical and problem solving skills, multitasking in a fast-paced environment. - Ability to work well independently as well as follow detailed instructions for completing tasks. - Solid foundation in networking with a deep understanding of TCP/IP and other core protocols. - Understanding of security related technologies including encryption, IPsec, PKI, VPN, firewall, and authentication protocols such as TACAS+ and RADIUS. - Experience with and knowledge of packet flow, TCP/UDP traffic, firewall technologies, (Cisco ASA firewall), IDS/IPS technologies and antivirus, spam and spyware solution. - Experience identifying, coordinating and communicating and system vulnerabilities leveraging a vulnerability management tool such as tenable Nessus - Experience with SIEM architecture, enterprise class logging and monitoring solution, such as Splunk and kiwi Syslog. - Ability to conduct detailed research and evaluation of security issues and products as required. - Familiarity with industry standard and regulations such as, ISO 27001/27002, NIST SP 800 series (800-37, 800- 53), ITIL, assisting management to manage internal control, risk assessment and business process. - Develop information security policies and procedures using clear, concise and accurate statements

Name: Christopher Mitchell

Email: martinraymond@example.net

Phone: (514)221-7228x327