Remote Information Security Analyst Remote Information Security Analyst Remote Information Security Analyst - Trinity Health Virginia Beach, VA Work Experience Remote Information Security Analyst Trinity Health - Virginia Beach, VA 2018 to Present Assist with onboarding services to Enterprise Information Security (EIS) Shared Services to include; Incident Response support, Risk Management support, Security Assurance Support, Remote Access Exceptions process, VPN configuration process, & continuous monitoring of some InfoSec controls Work backlog Information Security tickets in various RSO queues Compile metrics for all departments under the Enterprise Information Security Umbrella and make available for viewing on Huddle Boards Assists the business owners of various information resources with VPN security tickets Plans and implements security initiatives & resolves complex security issues Oversees specific projects to design, develop, engineer and implement solutions to security requirements Communicates advanced information security concepts with clients, peers, management and vendors effectively Establishes and operates information security reporting procedures to validate that security controls remain in place Acts as an advocate and resource on information security for various department areas or system-wide initiatives Works with business stakeholders to define Information Security processes Work with ServiceNow developers to automate Information Security request intake process in ServiceNow Process Information Security tickets and requests via ServiceNow Develop standard operating procedures for the EIS Shared Services department Provide metric reporting for the EIS Shared Services team based off ServiceNow reporting tool Build out processes for the EIS Share Services queue management function Effectively communicate with audiences of varying levels of technical experience from users to executives Remote IT Security Consultant UnitedHealth Group - Virginia Beach, VA 2015 to 2018 Serve as an escalation analyst on the Security Incident Response team Educate and train internal users on cyber security awareness Enforce and ensure compliance with company information security policies Create SAFE with Me information security awareness material in print and video format Respond to various types of Information Security incidents such as malware, unauthorized disclosures, policy violations, HIPAA violations, vulnerabilities, attacks, data leakage prevention, and insider threats Analyze incidents generated by

Symantec DLP (Data Loss Prevention) Handle Data Loss Prevention incidents containing sensitive information Track Data Loss Prevention incidents through remediation or user education activities Work with Data-in-Motion, Data-in-Use, and Data-at-Rest DLP incidents Work DLP incidents handling PII, Confidential, or Sensitive information Approve and provision or deny request to access cloud storage Box, OneDrive, and Dropbox Utilizes SEIM tool ArcSight and Kibana for log analysis needed for incidents Assist in the modification of UHG information security policies Manage IT security Risks in conjunction with the Risk Review Team using eGRC tool Make sound information security decisions keeping in mind the mission of the business Work in conjunction with HR & Ethics and Compliance team to investigate security incidents reported anonymously through NAVEx Global Ethics Point portal Handle incidents that deal with Optum Bank fraud in conjunction with Optum Bank team Write executive summary documentation for all high-level information security incidents Effectively communicate with audiences of varying levels of technical experience from users to executives Create and/or update Standard Operating Procedures for the Security Incident Response team Information Assurance Analyst Harris Corporation - Norfolk, VA 2014 to 2015 Serve as Cyber Security Analyst for the Commander Navy Installations Command Supports real-time detection of vulnerabilities and sophisticated attacks, discern and remove false positives, and analyze the information generated by McAfee ESM and HBSS monitoring tools Monitors and tracks down anomalies, non-compliant systems, and other observed events that are detrimental to the overall security posture of the CNIC IT infrastructure Perform packet capture analysis on hits received via SIEM tool McAfee Enterprise Security Manager Prepare daily report for management with analysis on all hits received in McAfee Enterprise Security Manager Supports remediation efforts to include: installation of software patches, changes of a configuration setting, and the removal of the affected asset Scan systems with ACAS for Information Assurance Vulnerability Alert & Bulletin (IAVAs, IAVBs, IAVMs) compliance Report systems that are not in compliance with current IAVA standards after scanning with ACAS Assist in the creation of POAMs for the Certification and Accreditation process Scan systems in preparation of ATO for the certification and accreditation process Write and maintain Standard Operating Procedures and policies for Cyber

Security Team Knowledge of FISMA & NIST Information Assurance Analyst Reliable Systems Group - Norfolk, VA 2013 to 2014 Serve as Cyber Security Analyst for the Commander Navy Installations Command Scan systems for Information Assurance Vulnerability Alert & Bulletin (IAVAs, IAVBs, IAVMs) compliance Monitor Non-classified (NIPR) Networks in real time with McAfee Network Security Manager and analyze alerts for viruses, attacks, and intrusions Prepare daily report for management with analysis on all hits received in McAfee Network Security Manager Utilize Vulnerator tool to create POAMs and filtered reports of vulnerabilities in assistance of Certification and Accreditation process Scan systems in preparation of ATO for the certification and accreditation process Monitor and report alerts received by McAfee Host Based Security System (HBSS)/ ePO Install patches required by Vulnerability Management System issuances (IAVAs, IAVBs, IAVMs) for IA systems Knowledge of FISMA & NIST Systems Analyst URS Federal Services - Virginia Beach, VA 2011 to 2012 Served as Circuit Management Team Lead for United States Fleet Forces under IT portfolio management Managed and tracked a portfolio of over 5,000 IT hardware circuits Led circuit discontinuation effort which resulted in a $10 Million cost avoidance to the Navy Elicited requirements from appropriate business stakeholders for the development of a circuit dashboard Documented requirements from business stakeholders Led and managed the development of Master Circuit Dashboard project from initiation to completion Established a baseline now considered USFF's Circuit Asset & Inventory Portfolio Managed development of USFF Review and Revalidation dashboard Performed Review and Revalidation of United States Fleet Forces circuits Created dashboard to analyze and track changes with USFF's discontinued circuits Tracked certification and accreditation statuses of circuits Trained other analysts on the circuit management team Education MBA in Cybersecurity Management Touro University 2019 B.Sc. in Computer Information Science ECPI University 2008 Skills SECURITY, SHAREPOINT, DLP, ACTIVE DIRECTORY, ESM, Cyber Security, Siem, Network Security, Nist, Information Security

Name: Ricardo Thomas

Email: carolchung@example.org

Phone: (563)623-5930