Security Analyst III Security Analyst III Security Analyst III - Anthem, Inc Work Experience Security Analyst III Anthem, Inc August 2017 to Present Manage the assessment process and program support for over 1000 Anthem vendors. Served as a liaison between external vendor partners and internal stakeholders for Anthem vendor security objectives per the WISP guidelines. Support Chief Information Security Officer (CISO) third party vendor risk management initiatives through promoting HITRUST compliance with vendors, document collection, and performance of remote and onsite assessment per HITRUST, SOC, PCI, NIST, and HIPAA frameworks. Assist VSRM leadership in the following tasks: ? Overseeing Team Daily Stand - Up Meetings to help shape the agenda for the week. I help drive team attendance and participation by reporting on attendance and encouraging accountability among team members. In this capacity, I have the opportunity to address issues, train team members, and get feedback on areas of opportunity to improve team performance. ? Leveraged organizational tools such as SharePoint and excel reporting to assign and manage workloads to team of analysts ? Influence processes by driving team discussion through strategic meetings and documenting system requirements for technical SMEs (specifically assisting in the development of team's Archer solution) ? Lead meetings with external vendors partners and internal business contacts ? Lead vendor remediation efforts and planning ? Meet with internal partners such as procurement and legal to discuss process improvement opportunities ? Represent Anthem Security at Vendor Facility during onsite assessment and meetings with existing and potential vendor partners. ? Prepared reporting for upper management regarding metrics of completed assessments through the Aging Dashboard. ? Create Reports for internal business contacts Information Security Analyst McKesson February 2016 to February 2016 Managed the Infrastructure Vulnerability Management process which involved scanning the infrastructure using Tenable Security Center, meeting with internal stakeholders to drive timely remediation of vulnerabilities, and preparing weekly reports for upper management and business stakeholders. Assisted InfoSec Director in successfully achieving enterprise wide initiative of increasing timely remediation / patching of critical and high vulnerabilities and lowering the number of policy exceptions approved. Educated internal stakeholders of security risks of their assets and the importance of system maintenance to drive down security incidents. Worked closely with several internal teams to assist the business with compliance initiatives by performing the following tasks: ? Drive timely remediation and patching through regular follow up meetings with internal business contacts, system owners, and internal technical contacts ? Performing system differentiated control audit ? System Scanning using Tenable Security Center ? Asset Tracking and Inventory using Archer GRC tool ? Generating weekly business reports for upper management ? Meeting with technical stakeholders to discuss creation and execution of remediation plans and policy exceptions ? Data analysis of parity between identified vs. outstanding vulnerabilities ? Submitting and Reviewing Policy Exceptions Senior Information Security Analyst, Sr Dell Secureworks August 2015 to August 2015 I actively monitored and initiated the triage for security events and incidents on our clients' network. As part of the analysis team, I reviewed logs and events from client networks and alerted them on events that were actual threats to their security objectives. This required that I identified common attacks such cross sites scripting, malware and other threats to customer networks. Once these threats were identified, I engaged the client via their preferred method of escalation, call tree, and incident management program. Some common tasks that I performed in my role include: ? Network monitoring ? Incident Response through use of Remedy Ticketing Systems ? Event/Packet Analysis ? PCAP and system log reading ? Event Correlation ? Performing IP Shun/Block ? Using Regular Expression (REGEX) to write alert rules ? Provide customer service via the telephone. ? Using Windows/Linux based tools. IT Security Steward Center for Disease Control and Prevention - Atlanta, GA June 2012 to June 2012 Managed the recertification and accreditation process and served as a liaison between internal audit and internal stakeholders. Assisted Information System Security Officer (ISSO) and Security Stewards in Certification and Accreditation (C&A) and recertification process of more than 80 systems and their annual assessments. C&A and recertification is in compliance with NIST SP 800-37, NIST SP 800-53/53A and FIPS 199/200. Also adhere to OMB, FISMA, FIPS, and HHS/CDC guidelines and policies. Assist Information System Security Officer (ISSO) and Security Stewards in the following tasks: Recertification and Accreditation of Systems ? Determine system information types ?

Review Documentation annually and for initial certification ? Conduct Privacy Impact Assessments ? Conduct Risk Assessment from application/host scans ? Document System Baselines ? Provide network diagrams in relation to system ? Manage and document system weaknesses Manage Change Request ? Help to manage Change Requests for systems ? Help to process Change Requests. Perform Software Installation ? Perform installation of McAfee/Imation software on staff desktops ? Perform installation of SCAP software Work With ITSO Technician ? Performed troubleshooting work with NCHHSTP ITSO Technician. ? Complete disk formatting and load software to begin re-image process with CDC ITSO profile. Review Vendor-submitted Security Controls and Documentation ? Review submitted controls for compliance with NIST SP 800- 53 A ? Check for references and documentation of policies and controls ? Prepare documentation for review by OCISO Conduct System Security Plan Reviews ? Conduct Analysis of Systems' Security Controls to note errors and updates ? Conduct System Search in Trusted Agent for Non-Applicable, Users Non-Applicable, and also Non Satisfied (NS) controls. Prepare Privacy Impact Assessments(PIA's) ? Evaluated and categorized as low, moderate, or high impact systems based upon the sensitivity of data collected. ? Evaluated to ensure compliance with Privacy laws and CDC policy. ? Submitted the PIA to the Security Steward for subsequent submission to the CDC Chief Information Security Officer. Prepare and Update Business Continuity Plan (BCP) ? Prepared BCP with the name and contact information of individuals responsible for the system. ? BCP Tabletop Test Plan is prepared for moderate and high systems ? Training is provided in order to recover the system quickly, usually within 24-48 hours from the time of disaster or outage. Incident Response Team Member ? Member of the NCHHSTP Incident Response Team (IRT). ? Responded to incidents forwarded from the CDC Security Incident Response Team. ? Notified and counseled users that they have been infected with a virus or malicious code. I ? Initialized ITSO workstation/laptop re-image request. ? Updated or closed the incident using the OCISO Risk Vision database. Document and complete Center Change Management Requests ? Created and documented system changes using the CDC OCISO Information System Change Management (ISCM) Standard Operating Procedures (SOP). ? Coordinated with System Owner/Business

Steward and Technical Lead for change information and approval signatures. ? Ran applicable IBM Watchfire Application Vulnerability Scan to insure that changes did not add security vulnerabilities.

Initialize Security Computer Automated Protocol (SCAP/FDCC) ? Performed SCAP test on software requested by internal customer. ? Performed baseline analysis of the system at its normal state. ? Downloaded and installed requested software. ? Scanned the system to measure or note any changes in the system compared to the baseline. Perform Commercial-Off -The -Shelf(COTS) level III evaluation for requested software ? Complete COTS level III documentation to process requests for software to be installed on local workstations used for business purposes. ? Ran SCAP test to get a baseline configuration and then test against the baseline for any abnormalities after software installation. ? Forwarded Change Request for proper signature from System Owner, Security Steward, ISSO, and others. Issue Encrypted McAfee and Imation USB Drives ? Initialized the drives, ? Assisted the client with setup of a CDC approved password ? Assisted the client with scanning biometrics used to access information on the drive ? Explained how to use drives. Education Masters of Business Administration in Information Systems and Accounting in Information Systems and Accounting Georgia State University, J. Mack Robinson College of Business - Atlanta, GA May 2018 Additional Information Results-oriented security professional with capabilities to serve as a Team Lead as well as individual contributor. Extensive experience in relationship management of both internal and external stakeholders / partners to achieve business initiatives. Detailed-oriented and data driven. Summary of Qualifications include: ? Certified Information Security Professional (CISSP) ? Experienced with Information Security domains and security controls frameworks(NIST, HITRUST, SOC, PCI) ? Risk Assessment/ Asset Management / Vulnerability Management experience ? Relationship Management Experience with Internal and External Stakeholders ? Third Party Vendor Risk Management experience ? Experience working with industry tools Archer, Tenable Security Center, IBM AppScan, Remedy, McAfee Encryption Products, EnCase, and etc. ? Cybersecurity, Security Operations Center experience ? Programming / coding experience ? Security Clearance

Name: Phillip Sparks

Email: erica74@example.net

Phone: 406-344-4516x6362