Sr. Security Operations Analyst Sr. Security Operations Analyst Sr. Security Operations Analyst - Dell Secureworks Atlanta, GA Authorized to work in the US for any employer Work Experience Sr. Security Operations Analyst Dell Secureworks - Atlanta, GA August 2015 to Present Assist Dell Secureworks in providing excellent customer service to clients by providing information systems support and security to protect assets. My current role includes fulfilling goals and objectives such as maintaining 98% client retention by providing speedy and excellent client service as defined within client's service level agreement. My daily job activities include consulting with businesses regarding their system security, monitoring network traffic by using monitoring tools, alerting clients of threats to their systems, and assisting clients in business continuity goals. Some daily tasks which I perform to help clients meet information system security needs include: Shunning/Blocking IP addresses ? Per client request, Linux based application is used to connect to network device to block malicious IP addresses Reviewing logs of devices such as Check Point, Palo Alto, Fortinet, Fortigate, Barracuda, Cisco, and other types of firewalls, routers, and other devices. ? Log packets are inspected for suspicious host headers, suspicious URL paths which might indicate attacks such as directory traversal, SQL injection, and other common attacks Correlating logs from different devices in order to recreate events for informational purposes ? Logs are correlated to find the true source of an exploit Monitoring network and verifying alerts to identify true positive threats vs. false positives ? Working in Security Operations Center environment and Providing excellent customer service to client in accordance with client policy and needs for their particular business. IT Security Steward Center for Disease Control and Prevention - Atlanta, GA June 2012 to March 2015 Assist 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 ? Create NIST Based System Security Plans ? 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. ? Review Third Party 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. ? Perform Software Installation ? Perform installation of McAfee/Imation software on staff desktops ? Perform installation of SCAP software ? 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 (AppScan) 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. ? Performed SIEM activities ? 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. ? 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. Business Systems Support Analyst (Co-Op) Center for Disease Control and Prevention - Atlanta, GA January 2013 to May 2013 Atlanta, Georgia As a Business Systems Support Analyst for Financial Services, I provide support and help increase productivity of staff (also called internal customers) through the following activities: ? Develop software applications to support financial services department and staff ? Use ASP.NET and other programs in .NET framework to create applications that interface with the database to make database navigation simpler for non-technical employees. Used C#, Java, JavaScript, and Visual Studio. ? Make website more efficient by removing click here links and creating JavaScript code which allows for automatic onloading and redirecting of users to the appropriate page(s) using single sign on. ? Respond to Incidents ? Provide support to internal customers who require password recovery, troubleshooting, and other technical needs. ? Perform SIEM activities ? Pro-actively suggests solutions to improve efficiency and productivity ? Monitor users for most frequently used links and websites ? Create manual with common links, websites, and system directory to help customers navigate online environment (Citrix). ? Monitor media which customers use to report incidents and create more efficient means of communication through updating website incident directory to ensure the incident gets to right person in a timely manner. ? Maintain database ? Use SQL to make tables and link tables to promote relational database structure which allows for more meaningful data. ? Use Access and Visual Basics to maintain legacy databases Education MBA in Information Security and Accounting Systems Georgia State University, J. Mack Robinson College of Business - Atlanta, GA May 2016 Bachelor of Business Administration in Computer Information Systems and Information Security Georgia State University, J. Mack Robinson College of Business - Atlanta, GA May 2013 Additional Information ? About 3 years of experience working with Center for Disease Control's C/I/O's as IT Security Steward ? 1 year experience in IT policy and project management ? 5 months experience working as Business Systems Analyst at Georgia Pacific helping to develop and support financial services applications ? 3 months experience in Security Operations Center environment ? Several years working experience in Sales ? Associate of (ISC)2 ? Masters of Business Administration, Computer Information System and Accounting, 3.7 GPA SKILLS Computer ? McAfee Encryption software ? IBM Watchfire Application Vulnerability Scan ? Microsoft SQL Server Management Studio ? MySQL ? Java ? Eclipse ? Netbeans ? Access ? Outlook ? Microsoft Office (Excel, PowerPoint, Project Manager) ? Visio ? Bizagi ? Citrix ? SharePoint ? Windows7 OS Language ? French (conversational)

Name: Scott Curry

Email: hernandezjoshua@example.org

Phone: +1-343-771-8537x9651