Senior Information Security Specialist Senior Information Security Specialist Senior Information Security Specialist - CareFirst BlueCross BlueShield Hyattsville, MD I am a highly motivated IT professional, with extensive knowledge in PCI DSS 3.2, Security Assessment and Authorization (A&A/C&A), Risk Management Framework (RMF), System security life cycle and vulnerability management using Tenable Security Center and Nessus. Organized and detail- and goal-oriented individual and demonstrate professionalism, and ability to multi-task and coordinate with diverse teams to achieve a goal. Work Experience Senior Information Security Specialist CareFirst BlueCross BlueShield May 2018 to Present Develop and streamline the Vulnerability Management Program by creating a central CMDB, creating specialized reports for both management personnel and technical admins, developing metrics highlighting vulnerability remediation progress, and reviewing and updating the Vulnerability Management policies and procedures. Configure and conduct vulnerability, configuration, and compliance assessments on over 40,000 systems, including 5000+ Linux, Unix, and Windows servers, 7000+ workstations, mainframe, routers and switches, databases, virtual environments, firewalls, load balancers, appliances, physical security devices, printers, and other devices using Tenable Security Center and Nessus Scanners. Perform deep data analysis and data enrichment on the vulnerability scan results using macros to present the information to management and technical personnel in various meaningful and actionable formats Conduct weekly, biweekly, monthly, and ad-hoc meetings with over 40 admin teams to discuss vulnerabilities detected on the systems and applications they manage, and provide guidance on remediation and help develop remediation plans Collaborate with the Governance and Compliance team to discuss vulnerabilities that cannot be remediated, determine risk to the organization, record risk in the Risk Register for tracking purposes, and communicate risks to management. Engage with Audit teams to ensure the Vulnerability Management Program is compliant with SOC 2, PCI-DSS, NIST, and HIPAA regulatory frameworks as well as company policies. Patch and upgrade the Tenable Security Center application, as well as the Nessus Scanners and servers Cybersecurity Risk Analyst Washington Metropolitan Area Transit Authority (WMATA) - DC March 2017 to May 2018 Coordinated PCI DSS and HIPAA audit efforts and

conducted security control assessments on all enterprise systems and assets in scope. Configured and run vulnerability scans on over 20000 enterprise systems using Tenable Security Center and Nessus, in conjunction with MBSA and OpenVAS on newly built and allocated Windows and Linux servers in the QA, Dev, and Test environments Ran penetration tests on customer facing web applications using HP WebInspect and use NMAP to run ad-hoc penetration tests on selected servers for testing purposes Performed information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues using NIST SP 800-30 in conjunction with OCTAVE Risk Assessment methodology Registered and reviewed newly identified risks and areas of concern (AOCs) in RSA Archer Coordinate with different teams and developed necessary documentation needed to risk assessment kick-off meetings. Review information systems security environments to include all aspects of physical, technical and administrative security measures Monitor and evaluate a systems compliance with Information Technology security requirements in accordance with PCI DSS Provided analysis of system requirements relating to security/ Vulnerability reviews, risk, and contingency planning Review detailed descriptions of the controls, provide edits and feedback on their actionable quality, and based on the descriptions perform tests to prove the validity of these assertions through interviews, examining of evidence and either overseeing or directly running technical scanning tools against targeted systems Assist in conducting Security Assessments, Security Audits, and Security Awareness Presentations. Security Analyst Meso Scale Diagnostics - Rockville, MD August 2014 to March 2017 Conducted security control assessments using NIST 800-53 and 53A as part of the Security Assessment and Authorization processes. Ensured Information Systems are compliant to NIST Standards by ensuring controls were put in place using the SSP, Security Test and Evaluation Templates (ST&E) and reviewing applicable POA&Ms. Maintained and monitored identified POA&M items through completion with CSAM Used FIPS 200 as a guide for minimum security requirements for federal and information systems Performed Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), and E-Authentication with business owners and selected stakeholders Managed,

developed, maintained and communicated company policies, standards (FISMA, NIST 800-18, 53, 53A, 53 Rev4, 30, 37, 60, and 137) compliance, risk and business management, and configurations in accordance with industry standards and best practices. Junior Security Control Assessor/Risk Assessor Securitas - Washington, DC June 2012 to August 2014 Collaborated with a team of assessors to conduct security control assessments on all enterprise in-scope assets to ensure they were compliant with PCI-DSS, HIPAA, ISO, and NIST regulatory frameworks Scheduled meetings with the Senior Assessors, ISSO, and various system owners. Ensured all discussed items are accurately logged in the meeting minutes for recording keeping and tracking purposes Updated the Requirement Traceability Matrix to document if the assessed controls passed or failed. Assisted in developing Risk Assessment Reports based on the compliance of the controls to the different regulatory frameworks Reviewed architecture documents to ensure they were still current and valid Reviewed and update security policies and procedures Linux Administrator/ IT Technologist Support PepsiCo - Baltimore, MD June 2010 to June 2012 Installed, configured, upgraded, and patched Red Hat Linux servers Coordinated with the application teams to perform major OS upgrades on all servers Monitored system performance using system tools Installed and configured NFS, DNS, and FTP as well as maintain the ACLs and user permissions Created, modified, and deleted users and groups based on service ticket Answered incoming client and customer calls Troubleshoot software and hardware issue via phone Trained end users in the use of equipment and software Acquired and maintain expert knowledge of emerging desktop technologies and software applications Fully document all cases in call and ticket tracking software and escalate to appropriate queue Escalated support call to supervisor as necessary Assumed ownership of project-related tasks as needed or assigned Tools Nessus, Tenable Security Center, MBSA, OpenVas, HP WebInspect, NMAP, RSA Archer, CSAM, Microsoft Word, Project, Excel, Power Point, Visio Languages and Hobbies Spanish, French, German, Ibibio, Creole, Classical Piano, Reading Non-Fiction, Go Karts, Exploring New Cuisines, soon to begin learning Mandarin Chinese Education Master's Degree in Cybersecurity Technology University of Maryland University College - Adelphi, MD October 2016 to June 2018 Bachelors of Science degree

in Biochemistry University of Maryland - College Park, MD September 2008 to May 2014 Skills Cyber Security, Information Security, Nist, Network Security, Linux, Comptia, It Security, Siem, Cissp, Information Assurance, Cybersecurity

Name: Dana Terry

Email: todddrake@example.com

Phone: 818-738-9759x7146