Cybersecurity Analyst Cybersecurity Analyst Cybersecurity Analyst - Global Services & Consulting, Inc Baltimore, MD Security Analyst with over 8 years of experience delivering mission-critical IT security solutions. Proficient with Risk Management Framework methodologies, privacy/compliance, and continuous monitoring security strategies. Strong technical background in Unix/Linux Operating Systems. Excellent comment (verbal/writing) and customer service skills. Work Experience Cybersecurity Analyst Global Services & Consulting, Inc - Baltimore, MD Present Coordinate with the infrastructure teams to plan, develop, implement and test security controls that meet Federal regulations. Develop and maintain security documentation such as the System Security Plan, Privacy Impact Assessment, Configuration Management Plan, Contingency Plan, Contingency Plan Test Report, POA&M, and incident reports. Assess vulnerabilities and ensure systems are patched and security hardened at all levels. Monitor to ensure vulnerabilities are remediated as appropriate. Analyze and define security requirements for information protection. Monitor security breaches and participate in incident response activities and investigation of security breaches. Process and submit Plans of Action and Milestone (POA&Ms). Support IT Incident Response (IR) actions and reporting. Work with the infrastructure Incident Response team to move servers from Red to Blue Zone and back to production. Work with infrastructure and InfoSec teams to apply critical patches to assigned systems. Coordinate with infrastructure and networking team to resolve DNS issues, change IPs from dynamic to static IPs where required on assigned systems. Deployed Endpoint threat protection agents like FireEye, Symantec and Heat to various systems. Cybersecurity Analyst (RMF) CareFirst BlueCross Bs, Inc - Owings Mills, MD October 2016 to March 2019 Document and Review security plans, contingency plans, privacy impact assessments, and risk assessment documents per NIST 800 guidelines for various agencies Perform Security Privacy Threshold Analysis (PTA), Privacy Impact Assessment, E-Authentication with business owners and selected stakeholders. Experience mitigating controls with NIST 800, FIPS and FISMA. Responsible for actively monitoring internal and external cybersecurity threats and risks. Implements data security measures and controls to protect our client's information systems. Review and responds to security alerts, scans, and audits Coordinates security incident responses

with ISSO and security teams, report on information systems security status, standards, compliance, and deficiencies Responsible for planning and continuous monitoring of Cybersecurity and privacy policies, programs, compliance artifacts, and standards. Assist in establishing a continuous monitoring strategy to proactively survey, monitor, and track security-related defects and the status of their resolutions. IT Security Analyst Executive Consulting Inc - North Bethesda, MD November 2014 to September 2016 Coordinate with the infrastructure teams to plan, develop, implement and test security controls that meet Federal regulations. Develop and maintain security documentation such as the System Security Plan, Privacy Impact Assessment, Configuration Management Plan, Contingency Plan, Contingency Plan Test Report, POA&M, annual FISMA assessment, and incident reports. Assess vulnerabilities and ensure systems are patched and security hardened at all levels. monitor to ensure vulnerabilities are remediated as appropriate. Analyze and define security requirements for information protection. Monitor security breaches and participate in incident response activities and investigation of security breaches. Process and submit Plans of Action and Milestone (POA&Ms). Support IT Incident Response (IR) actions and reporting. Systems Administrator (Unix/Linux) Beyond Technologies - Sterling, VA August 2011 to October 2014 Building and integrating new servers (physical and virtual) using both interactive and automated methods (kickstart). Create, manage, and administer user accounts security on UNIX/Linux servers. Manage and troubleshoot user account issues. Harden Linux servers based on CIS benchmark recommendations; Nessus scan Performed software installations, upgrades/ security patches, troubleshooting, and maintenance on Linux servers Configure swap space to OS as needed. Manage file systems, storage, NFS, file permission (data security) using ACL permissions. Education Bachelor's in Arts UNIVERSITY OF YOAUNDE - Yaounde Cameroon September 2005 to December 2009 Master of Science in Cybersecurity Management & Policy UNIVERSITY of MARYLAND UNIVERSITY COLLEGE - Adelphi, MD Skills Security, Fisma, Incident response, Nessus, Nist, Nmap, Linux, Unix, Unix/linux, Sdlc, Security plan, System security, Risk management, Windows server 2008, Excel Additional Information AREAS OF EXPERTISE Risk Management Framework NIST SP 800 Special Publication Series FIPS 199/200 Management

FISMA Tenable Nessus Vulnerability Scans Nmap System Security Plan Incident Response and Contingency Plan Release Management (SDLC) Systems Administrator (UNIX/Linux) Operating Systems: UNIX/Linux OS RHEL:6/7 Windows Server 2008/2012R2

Name: Edward Fernandez

Email: cassandrabowers@example.net

Phone: 291.768.0088