Senior Cyber Security Analyst, Shift Lead Senior Cyber Security Analyst, Shift Lead Senior Cyber Security Analyst, Shift Lead Laurel, MD To pursue my studies at University of Maryland University College to major in Cyber Security. My interest includes ethical hacking, risk/threat assessments, information assurance, computer investigations, disaster recovery plans. I desire to build innovative technologies, mitigate threats and implement countermeasures in order to protect the confidentiality, integrity, and availability of systems. I am determined to provide assurance to the protection of information systems and highly sensitive networks. Authorized to work in the US for any employer Work Experience Senior Cyber Security Analyst, Shift Lead Kidwell Dr - Vienna, VA August 2013 to September 2015 Support customer with performing Cyber Incident Response Team (CIRT) operations as a shift team lead. Duties are composed of managing a team of analysts, lead cyber security investigations amongst IDS/IPS systems, analyzing network traffic, correlating security events, and referencing open source information to detect and report threats against customer networks. Coordinate with development and production organizations to ensure security tools have full operational capabilities. Meet project deadlines and ensure quality control of project stages. Produce reports and metrics to identify significant security events as required by management. Propose with recommendations for mitigating risk. Develop effective training and procedures for investigating events accordingly. Lead Computer Security Analyst, Level TASC, Inc August 2011 to August 2013 Supported National Security Agency (NSA) TAO division, Mission Infrastructure Operations Center - Security Operations Center (MIOC-SOC). Served in the role as a senior lead analyst providing leadership, oversight, shift continuity, training amongst 4 rotating shifts teams, and ensuring a secure IT infrastructure that must be accessible and available at all times. My mission focus is to detect anomalies in network traffic, intrusion detection base-lining, long-term traffic analysis, and respond according to mitigate the abnormal activity. In order to protect TAO's information assets against cyber-attack and exploitation, I've utilized cutting edge cyber security technologies to perform mission essential network analysis and practices through 24x7 security monitoring. My knowledge and initiatives has improved the security of critical mission IT systems in order to ensure mission success for NSA's TAO. I.T. Security Specialist Department of Justice

January 2010 to March 2010 I've briefed Information Technology Management officials and staff on FISMA (Federal Information Security Management Act) regulations initiated by Office of Budget and Management, ensuring that all federal systems are certified and secure against daily threats, both imminent and minor. I have also served as a security control validator, in which I ensured information assurance of all systems are implemented properly within domains such as management, operations, physical security, access control, disaster recovery exercises, etc. based on FISMA and NIST standards. Risk Manager I.T. Problem June 2009 to August 2009 I've designed senior level processes for addressing Information Technology related issues by using ITIL, COBIT, and Gartner Research best practices. This is used for managing IT service life-cycles and either mitigating, or eliminating any risks discovered within standard asset systems to an acceptable level. I've developed the processes and procedures for reporting any problems discovered in After Action Reports, Root Cause Analysis, Quality Assurance Plans, Information Assurance Policy, and Risk Assessment plans to Senior Information Assurance Directorates within the OCIO Service Delivery branch and INFOSEC branch. Relevant Coursework and Skills: I am ISC(2) CISSP certified; EC-Council CEH and ECSA/LPT certified; CompTIA A+, Network+, Security+ certified. I am also certified by the Information Assurance Criteria Review Board (IACRB) as a Data Recovery Professional. I have a firm understanding in concepts of penetration testing, reverse engineering, vulnerability assessments, firewall technologies, intrusion detection/prevention systems, and hardware-based data recovery. I have applied these concepts to proactively determine how sensitive and vulnerable networks are to cyber attacks in a proactive manner; in addition to incident response and handling if an OPSEC/COMPSEC breach occurs. I've worked with Microsoft Windows 7/Vista, along with Linux distributions such as Backtrack and Ubuntu. I have attended/participated in conferences sponsored by the NSBE (National Society of Black Engineers), Black Hat Technical Security Conferences, and SANS Institute. Education Cyber Security University of Maryland University College June 2016 to 2017 Skills Incident Management, Incident Management (6 years), Cyber Security, Cyber Security (7 years), Packet Analysis (7 years), Splunk (4 years), FireEye (3 years), Solera (2 years), HIDS/NIDS, HIDS/NIDS (Less than 1 year), HIDS/NIDS (7 years)

Certifications/Licenses CISSP May 2018 Security+ September 2020 Network+ Network+ 2023 Network+ September 2020 CDRP April 2026

Name: Elizabeth Diaz

Email: amy61@example.net

Phone: 6929068161