Senior IT Security Analyst / Invincea Senior IT Security Analyst / Invincea ISSO Capitol Heights, MD Work Experience Senior IT Security Analyst / Invincea Invincea - Fairfax, VA August 2016 to Present * Responsible for Developing, Review CRM (customer responsibility matrix) established and updating Information Security System Policies, established security baselines in accordance with NIST, FISMA, and FIPS. * Perform vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple asset across the enterprise network. * Updates IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. * Conducting risk assessments, help review and update, Plans of Action and Milestones (POA&M), Security Control Assessments. * (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). * Monitors controls post authorization to ensure constant compliance with the security requirements. * Conducts Self-Annual Assessment based on NIST SP 800-53A. * Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). * Review and analyze Nessus Vulnerability and Compliance scans. * Assess systems of complexity and comprised of various technologies. * Create standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages * Provide weekly status reports on ongoing tasks and deliverables IT Security Analyst / Alpha Technology Systems Alpha Technology Systems - Springfield, VA July 2015 to August 2016 * Supported the Security Assessment and Authorization process of the clients' systems as a technical Security Analyst * Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. * Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple asset across the enterprise network. * Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. * Performed risk assessments, help review and update, Plans of Action and Milestones (POA&M), Security Control Assessments. * (SA&A) Security Assessment and

Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). * Monitored controls post authorization to ensure constant compliance with the security requirements * Documented findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). * Reviewed and analyzed Nessus Vulnerability and Compliance scans, WebInspect scans and DbProtect scans for possible remediation. * Provided DRAFT SAR for internal peer review. * Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages * Provided weekly status reports on ongoing tasks and deliverables IT Security Analyst Security Engineering - Falls Church, VA June 2014 to July 2015 VA * Assisted in conducting cloud system assessments * Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements * Supported Cyber Security analyst in conducting Vulnerability Management, Security Engineering, Certification and Accreditation, and Computer Network Defense. * Performed risk assessments, update and review System Security Plans (SSP) using NIST 800-18 (Guide for Developing Security Plans for federal information systems) Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration * Was responsible for conducting analysis of security incidents. Responsible for reporting findings and provide status to senior leadership. Perform escalations to Regional Computer Emergency Response Team (RCERT) when required. * Performed vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus SOC analyst Coastal International Security - Washington, DC October 2010 to June 2014 * Worked in a SOC environment, where I assisted in documenting and reporting vulnerabilities (Tier 1). * Assisted the SOC team in documenting and reporting vulnerabilities by utilizing Splunk. * Monitored personnel, equipment locations, and coordinate service and schedules. * Document incidents and activities. * Relayed complaint and emergency-request information to agency dispatchers. * Worked with callers to determine their locations, and the nature of their problems to determine type of response needed. * Received incoming telephone or alarm system calls regarding emergency and

non-emergency police and fire service, emergency ambulance service, information and after-hour calls for departments within a city. * Determined response requirements and relative priorities of situations, and dispatch units in accordance with established procedures. Education Bachelors of Science degree Delaware State University - Dover, DE May 2006 Skills security, Active Directory, access, Microsoft Office, Cisco

Name: Melissa Sherman

Email: zsullivan@example.com

Phone: +1-576-352-9248x77956