Sr. IT Security Analyst Sr. IT Security Analyst Sr. IT Security Analyst - Bureau of Engraving Printing Abingdon, MD Authorized to work in the US for any employer Work Experience Sr. IT Security Analyst VariQ Inc / Bureau of Engraving Printing - Washington, DC January 2017 to Present Currently supporting US Department of Treasury - Bureau of Engraving and Printing (BEP), Enterprise Security Assessment and Authorization and Enterprise Continuous Monitoring Reauthorization (eCM-r) activities for multiple General Support Systems, Cloud Deployments and Major Applications. ? Developed and implemented secure and scalable FedRAMP - compliant information systems with successful ATOs on Salesforce PaaS, SaaS and BOX Content Management Cloud Platform which transitioned disparate collaboration tools into a cloud system where all parties can make permission-based updates and provide easier governance and collaboration while ensuring DLP is in palace. ? Served in the capacity of Bureau's Enterprise Cloud Security Expert and technical lead for designing Enterprise FedRAMP- Compliant cloud Infrastructure on Salesforce SaaS and PaaS for deployment of multiple applications that drive critical business processes for various Bureau offices. ? Developed a security architecture for defining control inheritance structure on Salesforce PaaS, simplifying authorization process for multiple applications and improving security posture. ? Attending important policy meetings and working with Agency's external partners Such as FRB, Treasury Department, Department of Homeland Security, Office of Management and Budget and National Institute of Standards and Technology on assigned government-wide projects such as Box.com, VMS, CDM, to improve agency's overall IT security posture and protections. ? Work with Chief Information Officers (CIO), Information Systems Security Officers (ISSO), and Security Administrators to define security and functional system requirements. This involve the development of security related documentation to include policy development, procedural testing, risk assessments. ? Coordinated and managed cloud security, developed detailed intelligence plans to satisfy cyber operations requirements within a Salesforce SaaS and PaaS General Support System (GSS). ? As Technical authority for Cloud solutions, developed and implemented auditable items in an event monitoring tool in collaboration with Project Managers, Development Team and Security Engineers. ? Developed and created

System Security Plans (SSP), Contingency Plans (CP), Contingency Plan Tests (CPT), Privacy Impact Assessments (PIA), and Risk Assessment (RA) documents per NIST 800 guidelines. ? Extensive knowledge in Salesforce cloud infrastructure, Microsoft Azure, Oracle Gov cloud and components employed to develop enterprise solutions and processes to collect and analyze data. ? Created Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) when required and include necessary language and policy to protect the organizational interest. ? Supporting Risk Management Framework (RMF) and Cybersecurity Framework ? Managed the software design security implementation for a Laboratory Information Management System (LIMS) project using agile development framework and methodology and ensured that systems security measures are taken to protect Personally Identifiable Information (PII) and improve data collection. ? Categorize the information system and information processed, stored, and transmitted by that system based on an impact analysis using guidance from FIPS 199 and NIST 800-60. ? Select an Initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions. ? Evaluated multiple systems, performs security reviews, identifies gaps in Agency's security architecture, and design a security risk management plan following the cybersecurity framework. ? Salesforce Cloud architecting security solutions and performing initial risk analysis, tracking IT project schedules, interfacing with customers and senior management both internal and external points of contacts, facilitating ongoing authorization for Agency systems and maintaining current documentation. ? Supported a data analytics strategy on Salesforce FedRAMP cloud that host multiple agency applications based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework. ? Performed over 50 different system analysis, present implementation recommendations, identify and track vulnerabilities, systems integration, and provide technical advice based on those reviews. ? Led a team effort geared toward IT infrastructure modernization to replace outdated tape backup solutions with modern Dell EMC cloud backup solution that essentially eliminated manual tapes. ? Detect and investigate policy violations, working with other teams for further investigation as appropriate. ?

Provide Continuous Diagnostics Mitigation (CDM) expertise to assist the Agencies to develop or improve organization-specific governance structures and policies. ? Provided oversight for Cloud security projects on salesforce cloud including API integration of audit tools, testing of tool functionality to ensure enterprise requirements are met. ? Collaborate with customer, clarify security procedures while designing and developing data extraction routines and queries. Research, gather and provide artifacts for audit request and data calls in a timely fashion that helped solved information quest pertaining to policy issues. ? Developed detailed intelligence plans to satisfy cyber operations requirements within a Salesforce SaaS and PaaS GSS. ? Led an initiative to develop agency-wide Enterprise Architecture plan that described new authorization boundary definition to enhance agency operation and improve the ATO process. ? Led team initiative to validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. ? Worked with Contracting Officer Technical Representative (COTR) to deliver tasks in a timely fashion including weekly project progress reports. Information System Security Officer (ISSO) VariQ Inc / US MINT - Washington, DC March 2018 to December 2018 US MINT ? As an ISSO, implemented agile methodology in developing applications and Tracking assigned project timelines for all A&A projects from inception through final authorization to operate (ATO) from Authorizing Official (AO). ? Spear headed a data lake initiative / data warehouse, application architecture systems project, web-based solutions, and developed a Contingency Plan including and facilitated a table-top test for the data lake solution. ? Led a team of three staff members in developing an enterprise Contingency Plan for a major data warehouse initiative, identified loop holes and apply mitigations to reduce risks. ? Managed multiple assigned projects concurrently while setting priorities to meet defined objectives within a tight timeline. ? Delegated work to team members on annual assessment of multiple systems that led to completion under a tight schedule. ? Performed Vulnerabilities Scanning using Nessus to scan network systems to ensure security and updated information is documented in the SSP in accordance with NIST. ? Prepared and facilitated high level meetings with Outside contractors and senior management to gather requirements and determine Security Impact on existing system and architecture. ? Extensive experience responding to multiple inquiries and data calls from both internal and external POCs and making sure needs are delivered expeditiously and on time. ? Expert hands-on experience with Enterprise Security Administration module. ? Experience with Data Loss Prevention (DLP) and User Behavioral Analytic (UBA) technologies and interface with incident response teams to build alert response procedures for these tools. ? Ability to exercise sound technical, interpersonal and organizational judgment while evaluating and solving complex problems. ? Experience in developing Splunk queries and dashboards targeted towards an information security, IT operations or business context. ? Experience in developing Splunk ES correlation searches or experience working with ES. ? Experience assign groups of users to the roles that best fit the tasks the users will perform and manage in Splunk Enterprise Security. ? Experience with the following cybersecurity areas: endpoint protection, network security, security operations, incident response policy, vulnerability management, FISMA compliance, and related areas. ? Ensures the confidentiality, integrity, and availability of IT systems through full compliance with FIPS, related NIST standards. ? Ensuring that Analysts receive and analyze alerts from various enterprise level sensors and determine possible causes of such alerts. ? Assist in implementing technical threat response actions. Detect adversary activity on the Network and provide a mitigation plan to defeat/detour the threat. ? Responsibilities include directing project-specific staff in support of customers and third-party teams. ? Helps protect government IT networks from cyber threats and enhances risk-based decision making by providing a consistent and proven set of solutions. ? Managing the SOC SharePoint and data repositories to improve cross communication, data sharing and situational awareness. ? Directly support Security Test and Evaluation/ Security Assessment activities; conduct vulnerability scans; document, deliver, and present results ? Develop Plan of Actions & Milestones (POA&M) in accordance with the IT Security Requirements. ? Knowledge and in Security Information and Event Management (SIEM), to include Splunk Enterprise Security. ? Experience with the following cybersecurity areas: endpoint protection, network security, security operations, incident response policy, vulnerability management, FISMA compliance, and related areas. ? Ensures the confidentiality, integrity, and availability of IT systems through full compliance with FIPS, related NIST standards, and agency IT security policies and directives. ? Understanding the true threat your organization faces from an Advanced Persistent Threat (APT) and FO (Focused Operators) are and how they work ? Experience working with data transmission protocols such as TCP/IP. ? Managed cyber incident requirements and resources to include identifying appropriate manpower and tools for each incident, e.g. type of breach, point of entry, tactical response and tools i.e. ArcSight, Sourcefire, Splunk, web content filter, Wireshark, firewall rule reviews etc. ? Responsible for the planning and development of plan of action and milestone and ensuring response stays within timelines by the team and the management receive timely updates. Information Technology Specialist/Engineer Boltos Solutions Inc - Laurel, MD February 2015 to December 2017 Coordinated with IT Program management teams on the requirements for operations related processes and act as a subject matter expert (SME) to provide advice and solutions for the development of related technical procedures in the operating system environment. ? Oversees and manages all security assessments and penetration testing activities. ? Developed and wrote jargon-free Standard Operating Procedures (SOPs) for configuring three database servers and cut down technical issues by 60%. ? Directed development of a disaster recovery plan for enterprise information system. ? Analyzed and configured information technology systems to ensure availability and security of information system to support over 2000 daily transitions. ? Documented database structure, changes, problems and issues for future references. ? Led a team of 5 on multiple assignments concurrently and met deadlines while preparing reports under tight schedules. ? Organized 35 database user accounts; developed, modified and deactivated user accounts; assigned and monitored user access rights ? Provided administrative, technical and program management support for services. ? Preventing Unauthorized Exposure of Confidential Data ? Work with business units to document and remediate computer security incidents ? Help desk actions - troubleshooting systems access, unlocking accounts, group policy, installation of updates and software, maintenance of computers, viewing vendor's sites for updates, market research for artificial Intelligence (AI) tools and technologies. Cybersecurity Analyst Innovative BI Solutions Inc January 2013 to January 2017 Responsible for in-depth analysis of network devices used in the Discovery and Counter Infiltration operations on specified networks and areas of interest at the team level. ? Ensure implementation of appropriate security controls across the organization. ? Identifying Confidential Data within an Organization ? Understanding of compliance reporting practices and methodologies ? In-depth experience with general IT security concepts, network security and monitoring practices/methodologies. ? Worked with internal and external professionals to support infrastructure and data solutions, ? Coordinated and managed IT projects for a team of 3 and provided planning and oversight of work deliverables, integrating schedules, and UAT testing and ensuring quality related to infrastructure requirements. ? Responsible for working in a 24x7 Security Operation Center (SOC) environment ? Provide analysis and trending of security log data from many heterogeneous security devices. ? Provide Incident Response (IR) support when analysis confirms actionable incident. ? Provide threat and vulnerability analysis as well as security advisory services ? Analyze and respond to previously undisclosed software and hardware vulnerabilities ? Investigate, document, and report on information security issues and emerging trends. ? Coordinate with Intel analysts on open source activities impacting systems. ? Integrate and share information with other analysts and other teams ? Ability to configure and develop an enterprise SIEM solution including signature tuning, development of correlation rules, reports, and alarms. IT Specialist Windsor Medical Center - Woodlawn, MD February 2012 to February 2014 Evaluated and Determined IT equipment and communications requirements and their compatibility requirement with other systems. ? Develops and implements IT security awareness programs to ensure that systems, network and data users are aware of and in synergy with privacy requirements. ? Information Assurance and risk mitigation of systems aid in the design and development of equipment and systems, and redesign of existing systems to fulfill the needs of customers ? Provide equipment and capability reports and acting as technical liaison. ? Provide expertise in business analysis, systems analysis, and project management. ? Launched a review and evaluation program and influenced replacement of two outdated systems. ? Designed web pages to present forms for download and decreased office wait time by 15% ? Supports the development and implementation of cybersecurity strategies across the functional areas to protect health information in accordance with HIPAA. ? Decreased cost of acquiring new Information Technology hardware from $12000 to $10, 500 ? Supervised transition from 50 racks of paper records to electronic medical records under budget. ? Trained three (3) office staff on how to use available technology and reduced support request by 60%. ? Demonstrate proficiency in attention to detail, customer service, oral communication, and problem solving while helping to protect information and information processing assets for Medical Record System. ? Negotiated with vendors and acted as a liaison between non-technical office staff and vendor technical staff during troubleshooting. Helped with transition from paper records to Electronic Medical Records ? Oversaw compliance with HIPAA in securing patient's data that led to improved security posture. ? Provided strategic and tactical Technology guidance for Health Information technology (informational and operational) projects, including the evaluation and recommendation of technical controls ? Demonstrated key Knowledge of computer threats, vulnerabilities, and risks to information system Education Bachelor's degree in Forensics University of Maryland University College - College Park, MD June 2016 Skills IT SECURITY (7 years), SHAREPOINT (5 years), Agile Project Management (6 years), HIPAA (4 years), FedRAMP Cloud Infrastructures (5 years), SQL (6 years), training (4 years), Microsoft Office, testing (5 years), Cloud Technology testing (6 years), Active Directory, Risk Assessment (6 years), access (4 years), Excellent Strategist (5 years), Exceptional Organizational Skills (5 years), Exceptional Communication skills (6 years), Information Assurance (8 years), HTML, Cisco Certifications/Licenses o CompTIA Security+ Present CompTIA Security+ o CompTIA Network+ Present Network o Oracle Database Certification (on Red HAT Linux). Present Oracle o CAP- ISC2 Certified authorization Professional - Pending Present In progress o Certified Information System Security Professional (CISSP) - in progress Present in progress Additional Information TECHNICAL PROFICIENCY Network / Operating Systems Linux * Microsoft Windows OS (Desktop & Server) *SmartCert 3.2.2 * SmartCert 3.4 * TFIMS * Ubuntu (Desktop & Server) * Web Content Filtering (WCF), Software Applications Blue Coat * Microsoft Visio * Microsoft Office Suite * Wireshark * BRO * Metasploit * Nmap * Nessus / ACAS * VMware/vSphere * SPLUNK *CDM tools *OpenVAS * Red Seal * Tripwire * Arbor * ArcSight * Oracle 12c database, Virtual Box, QRadar, Serena, Remedy, SharePoint and Office 365.   Skills FedRAMP Cloud Infrastructures * Cloud Technology testing *Agile Project Management * Privacy Impact Assessment (PIA) * Personally Identifiable Information (PII) * Requirements Gathering *Outstanding Communication * Risk Management Framework (RMF) * Security Control Assessment (SCA) * Security Assessment and Authorization (SA&A) * Business Impact Assessment (BIA) * Privacy Threshold Analysis (PTA) * Contingency Planning (CP) * Disaster Recovery (DR) *Risk Assessment, Policies and Procedures Implementation *FISMA, NIST SP 800 Series, FIPS 199, 140-2 & 200, * FedRAMP ATOs * Salesforce, Azure, AWS, Box.com *POA&M, HIPAA, SLA, MOU, Advanced Excel spreadsheet user.   AREAS OF EXPERTISE   ? EXCELLENT STR ATEGIST - excellent strategy model overcomes issues that commonly occur with traditional organizational cloud deployments of operational excellence and process improvement. ? EXCEPTIONAL ORGANIZATIONAL SKILLS - Offers accessibility to process documentation and standard operating procedures that impact the performance metrics; e.g., through a click of a mouse button in an organizational value chain. ? STRONG SENSE OF RESPONSIBILITY - Maintain a balanced and consistent performance. Solid professional standards; excellent record of dependability and responsibility. Maintain focus on achieving results and have the motivation to get the job done in a reasonable period while implementing solutions to meet diversity of needs. ? EXCEPTIONAL COMMUNICATION SKILLS: working and communicating in varied assignments with diverse staff members onsite and remote to exchange information, resolve problems and clarify issues.   TRAINING Searching and Reporting with Splunk6.x 2019 Creating Splunk Knowledge 6.x 2019 Using Splunk 6.x 2019 Scrum Master Agile Project Management course 2018 Certified Authorization Professional (CAP) onsite course 2018 CISSP complete online course (FedVTE) 2018

Name: William Watson

Email: garciacarl@example.net

Phone: 495-587-4690