Information Security Analyst Information Security Analyst Information Security Analyst An energetic, dedicated and highly motivated professional with 4 years' experience working as an IT SECURITY ANALYST. I have acquired excellent practical skills in performance, development, implementation, and experienced in analyzing information requirements and delivering cost effective solutions. I am open to any IT Security position where I could utilize my versatile knowledge and skills to meet the organization's desired goals. Work Experience Information Security Analyst Solera Health Inc - Phoenix, AZ March 2018 to October 2018 Duties Included: Assisting in providing first level response to Security Incidents and events including but not limited to email spam/phishing attacks, malware infections, denial of service attacks, privileged account misuse, unauthorized access and network/ system breaches. Participating in conducting risk assessment on Solera's network partners and cloud vendors Analyzing security alerts, incidents, and requests; identifying root cause; determining and executes appropriate steps for resolution. Escalating security incidents/problems as required. Continuous monitoring and reviewing of Solera Health security information and event management (AlienVault SIEM) tool for high priority security alerts. Daily monitoring, patch management and vulnerability scanning using Qualys cloud based vulnerability scanner Consistently reviewing and adhering to Solera Health information security policies and procedures that meet HIPAA, HITRUST, Solera Health business associates and legal requirements

Assisting in implementing state-of-the-art information security software and hardware systems. Participating in auditing and reviewing of information security assets hardware and software inventory and recommend for change/upgrade through the change management process. Reporting and preventing with best efforts any harmful or suspicious activities known to Solera Health of a use or disclosure of ePHI in violation of HIPAA, HITRUST, Solera Health and/or a business associate's policies and procedures and/or Federal/State and Local Laws. Performing eDiscovery and quarterly DRP/BCP drills per company policies and procedures. Cooperating with the U.S. Department of Health and Human Services Office of Civil Rights, other legal entities, and organization officers in any audits or investigations Participating in the yearly review of all SaaS (AWS, MS Azure, SalesForce) applications by comparing it with other cloud vendors/competitors.

Attended HITRUST CSF training, information security training classes and conferences to improve awareness of the latest security threats and security defenses. IT Security Analyst Datalogic Solutions - Ashburn, VA January 2016 to February 2018 Duties Included: Supported enterprise security information and event management (splunk SIEM) system. Assisted in monitoring, detecting and isolating incidents happening in the organization's security products, network devices, end-user devices and systems. Using NIST to provide guidance in its NIST 800-37 RMF to comply with this FISMA requirement. Was able to categorize information system using FLPS 199, selecting security control using NIST SP 800-53 or FLPS 200, Implement security control using NIST 800-18 as a guide for developing of SSP, assisting in assessing security control using NIST SP 800-53A and continuously monitor using NIST SP 800-137 Reviewed security alerts, daily reports and followed up with investigation to remediation. Performed port scanning and full packet capture PCAP analysis using Wireshark. Participated in administering IDS/IPS and reviewing logs from IDS/IPS (Snort, Tripwire). Performed application, network, and system troubleshooting. Manually reviewed logs and provide documentation guidelines to business process owners and management.

Assisted in continuous monitoring of the A&A process by testing of security controls and vulnerability scanning. Assisted in conducting Risk Assessment (RA) using NIST 800-53A and NIST 800-30 as a guide. Reviewed and updated current security documentation, SOPs, networking maps, and system diagrams. Communicated effectively through written and verbal means to co-workers, subordinates and senior leadership. Reviewed POA&M and security controls Information Assurance Officer Siemens AG - Grand Prairie, TX December 2014 to January 2016 Duties Included: Applied current computer science technologies and Information Assurance (IA) requirements to the analyst. Design development, evaluation, and integration of computer/communication systems. Assisted in the SDLC, software debugging and input validation processes. Performed on-site security testing using vulnerability scanning and penetration testing tools such as Nessus, Nmap/Zenmap and kali Linux. Supported the SOC analyst in collecting security events from different security logs using SIEM tools and creating security incident ticket. Determined security controls effectiveness (i.e. controls implemented correctly, operating as

intended, and meeting security requirements). Worked with other team members in implementing SANS-20, ISO 27001 security controls and meeting PCI DSS compliances. Prepared and delivered oral IA-focused presentations to technical and non-technical groups. Assisted with security policies review, security alerts, guidance, regulations and technical advances in IT Security Management. Ensured that data, which contains PII, is continuously protected from unauthorized access, use, modification and disclosure. Education Masters of Science Vrije Universiteit (Free University of Brussels) - Brussels, IL September 2010 to September 2012 Bachelors of Science University of Buea October 2003 to July 2006 Skills FEDERAL INFORMATION SECURITY MANAGEMENT ACT (2 years), firewalls (Less than 1 year), FISMA (2 years), Mainframe (Less than 1 year), Network device (Less than 1 year) Additional Information Experience in vulnerability management and penetration testing tools (Nessus, Web Inspect, Qualys Wireshark, Kali Linux). Experience working with Nmap, Zenmap, protocol analyzers and other packet exploiting tools on both Linux and Windows OS. Experience in using ManageEnging ticketing and Change Management system.. Familiar in VMware and Virtual Machines technology. Experience in securing network devices (e.g. switches, firewalls, IDS/IPS, routers). Adequate knowledge of packet flow, TCP/UDP traffic, the OSI model, firewall technologies, IDS/IPS technologies, proxy technologies, antivirus/ anti-spam filtering, DLP and spyware solutions. Proficient in securing, managing data and databases. Proficient in handling PII, ePHI, conducting privacy assessments (PTA, PIA and SORN) and plans System Security Checklists. Adequate knowledge of the NIST RMF, HIPAA, ISO/IEC 27001, SOC 2 Type II and PCI DSS compliance. Excellent ability to work well in a group or team setting with exceptional analytical and communication skill Adequate knowledge on FISMA systems, FISMA Reporting Metrics TECHNICAL SKILL FISMA steps/process or C&A/A&A/ATO/SCA process POA&M (Plan of Action and Milestone) Operating system (platform): windows 2008, 2012, Mainframe servers Network device: firewalls, anti-virus software, Excellent verbal, written, and interpersonal communication skill

Name: Emily Grant

Email: chris29@example.net

Phone: +1-359-690-9649x55754