Information Security Officer Information Security Officer Information Security Analyst Lake Mary, FL I m an information security professional with hands-on experience in system administration, incident response, security engineering, and audits (PCI-DSS, RMF, SCA, SOC2, HIPAA, and HITRUST). Authorized to work in the US for any employer Work Experience Information Security Officer Therigy - Maitland, FL April 2019 to June 2019 Security Engineer II Data Dimensions - Lake Mary, FL September 2017 to March 2019 Create, maintain, and perform annual review of all security policies and procedures for the company Perform vulnerability scans and certify new systems for deployment via Tenable Nessus Gather evidence for annual SOC2, HIPAA, and RMF audits Manage multiple Trend Micro Anti-virus solutions across both physical and virtual environments (deployment, updates, configuration management, etc) Perform daily, weekly, and monthly reviews of various required reports generated through the Fortigate Fortinet program. Manage security-related incidents through the Black Stratus LogStorm appliance Manage the Visitor Management System for visitor tracking and auditing via TheReceptionist tablet-based solution Manage the Siemens Sipass physical security management system (creating access tables, schedule management, adding and removing badge access, etc) Review security video footage through ONSSI and ExaQ Vision applications for audits and security incidents requested by HR Successfully kicked off an Active Directory cleanup to clear over 2000 old accounts Helped the Sr. Security Engineer and the CISO to prepare company for HITRUST standards, including providing evidence during the initial gap audit Information Security Analyst HD Supply - Orlando, FL April 2017 to July 2017 ? Research/test/deploy enterprise-wide solution for password management and rotation with Thycotic Secret Server. ? Lead several PCI-DSS compliance efforts including Windows local administrator password rotation, compliance of PCI-scope remote endpoints, and creating SOPs for document redaction for in-scope employees. ? Used LogRhythm, VirusTotal, and Zscaler to research and manage proxy whitelist requests. ? Aid with vital threat research/analysis during multiple malware campaigns, specifically WannaCry and NotPetya. ? Use Tenable Nessus Cloud server to perform PCI-mandated vulnerability scans on in-scope endpoints. ? Coordinate ticket queue for Information Security department through ESMS and ServiceNow solutions. ? Created, modified, and managed various PCI-DSS mandated policies and documentation Cyber Secu Red Lambda - Lake Mary, FL November 2016 to January 2017 Develop plans to meet emergency data processing needs. Safeguard computer files against: accidental or unauthorized access. Pre-empt Accidental or unauthorized modification, destruction, and disclosure. Coordinate their implementation with inside personnel and outside vendors and conduct tests to ensure the functions of data processing activities and security measures are operational. If problems are identified, to modify the security files to incorporate new software, correct errors and change an individual s access status. Formally evaluate security features of information products and systems. Carry out and evaluate investigative work regarding potential threats. Take full responsibility for handling simulated and actual disaster scenarios. Ensure training in security matters is provided to all levels of staff. Proactively disclose and remedy actual or potential breaches and risks. Apply expert knowledge to initiate good security practices and planning. Take responsibility for arrangements for physical and logical security policy. Advise other professionals of necessity for security counter-measures. Information Assurance Engineer NCI, Inc - Orlando, FL April 2015 to November 2016 Audit new and existing information systems and applications to ensure that appropriate controls exist, that processing is efficient and accurate, and that systems procedures are in compliance with the appropriate standards. Assist in the development, implementation and enforcement of prudent systems security measures for entire network. Assist in deployment and implementation of anti-virus software on servers and PCs. Assist in providing troubleshooting processes and security methods associated with networked computer environments. Assist in certification and accreditation efforts utilizing DIACAP and RMF frameworks. Conduct security assessment scanning with approved tools, recommend remediation solutions, and reporting as necessary. Conduct varied compliance and/or vulnerability audits of all systems in accordance with DOD / Army regulations, instructions, guidelines, and local policies. Review, research, and provide recommendations on remedial action on security-related trouble calls. Assist on audits as directed by the Lead Security Engineer Assists, as directed by the Lead Security Engineer, with computer / data investigations. Assist with monitoring logs, auditing, and the management of system logs. Make recommendations to improve network functionality with backup documentation. Complete reports as required. Information Security Analyst (Contract) Nemours Children's Hospital January 2015 to April 2015 The main function of this role is investigating, removing, resolving malware issues using CLI, VMware, and Malwarebytes. Tickets are escalated from the help desk, from Quadrant security, and from internal executives. The secondary functions of this role is making exceptions to websites that employees are not allow to visit and ones that are blocked in Cisco WSA, making sure that these websites are deemed safe and are accessible to the respective employee. This includes looking at webpage source code for redirects or using tools like VirusTotal and Quttera Jr. Systems Administrator PowerDMS - Orlando, FL November 2013 to December 2014 Provide IT support to internal users and consult with C-level business leaders to discuss current IT environment. Manage hardware/software procurement and licensing, as well as provide full support and troubleshooting for all equipment and users. Managed user accounts via Active Directory 2008 and 2012. Manage Symantec and Comodo Endpoint migration and deployment. Work with System Engineer to develop Group Policy requirements for CJIS and SOC2 compliance. Systems Administrator Rosner Automotive - Fredericksburg, VA March 2013 to August 2013 Provided support for Microsoft Exchange 2010, Symantec Endpoint Protection server, Active Directory, Symantec Backup Exec, and Reynolds & Reynolds Contact Management system. Also provided all functions of hardware support, remote desktop administration, printer repair, and full assessment of security policies and procedures IT Systems Analyst DoD Office of the Inspector General - Alexandria, VA October 2011 to June 2012 Contracted through MSO Technology, Inc. to provide support for the Information Systems Directorate (ISD) division of the DoDIG. Provided multiple services such as help desk, change management, knowledge base management, Active Directory support, Exchange server support, network printer administration, and troubleshooting support for the Tier III server team. Influenced the development of Certification and Accreditation packages by testing image security and stability. Education Certificate of Completion in Network Security and Administration Central Technology Center - Drumright, OK August 2006 to May 2009 Skills Active Directory (10+ years), Microsoft Office (10+ years), Incident

Management (6 years), Vulnerability Management (5 years), System Administration (7 years), Information Security (7 years), Anti Malware (6 years), security Links http://www.linkedin.com/in/william-zacharias-51266b49 Certifications/Licenses Certified Information Systems Security Professional (CISSP) January 2015 to Present

Name: James Jordan

Email: lisa89@example.net

Phone: 200.271.3625