

Information Security Analyst Information Security Analyst Information Security Analyst - Coca-Cola Consolidated Inc Charlotte, NC Information Security Analyst with broad-based hands-on skills in system implementation, support and updates. Including user and system provisioning within Active Directory using Group Policy and Access Management Solution Systems. Proven ability to perform Risk Assessments and take the proactive steps necessary to ensure the safety and security of corporate data. Authorized to work in the US for any employer Work Experience Information Security Analyst Coca-Cola Consolidated Inc May 2019 to Present Lead Vulnerability Management efforts Design, configure, and deploy logical network scans for internal and external network Provide monthly threat and vulnerability assessment reports, i.e. CVE assessment, attack analysis Technical support in the areas of risk assessment, network security, product evaluation, and security implementation. Responsible for designing and implementing solutions for protecting the confidentiality, integrity and availability of sensitive information. Participates in design of information system contingency plans that maintain appropriate levels of protection and meet time requirements for minimizing operations impact to customer organization. Conducts testing and audit log reviews to evaluate the effectiveness of current security measures. Works with Managed Security Service Providers (MSSP's) to remediate deficiencies and issues. Coordinate efforts with Operations team as needed. Work with DevSecOps team to ensure secure practices are being implemented in cloud environments Coordinate efforts with Training Partner for Security Awareness Training campaigns and phishing tests Information Security Analyst Wells Fargo - Charlotte, NC January 2019 to March 2019 As the Information Security SME on the Data Analytics and Controls Team, within Enterprise Information Security, duties are to engage "The Top 50" metric stake holders from Application Security, Business Process IS, Cyber Defense, Data Protection, Identity Access Management, IS Risk, IT Infrastructure Risk, Third Party Management, Vulnerability Management, and Workforce Accountability domains, to refine existing metrics' information and ensure domain alignment with "The Top 50" goals Analyze and assess current and proposed portfolio metrics produced by EIS covering all ten domains. Identify "Gaps" in metric coverage by comparing Wells Fargo Information Security Policy Standards to industry standards such as NIST,

CIS, and ISO Mappings. Outline the proper steps to eliminate metric gaps required to validate all Information Security Policies used at Wells Fargo Information Security Analyst Wells Fargo - Charlotte, NC March 2018 to October 2018 Participate in intelligence sharing session to review cyber threat deliverables, intelligence gap support requests, guide analytic discussions and nominate topics to be covered during the calls. Gather and evaluate cyber threat business intelligence requirements for the LOBs by having regular discussions with key line of business personnel (e.g. operational risk personnel, technology managers, information security leaders, etc.).

Effective Vulnerability Management via creating Threat Models for Wells Fargo applications and processes, i.e. determining attack vectors, compensation controls, and residual threat score justifications. Recommend usable cyber threat business intelligence products designed to ensure the LOBs maintain situational awareness and can make informed business decisions. Facilitate and maintain relationships with LOB contacts by managing and supporting the delivery of cyber threat business intelligence products and services. Solicit feedback for the LOB to improve cyber threat intelligence products. Develop and further relationships with personnel at other financial institutions, government agencies, and other appropriate organizations Perform cyber threat analysis and reporting on information from both internal and external sources and appropriately manages and communicates relevant cyber threat intelligence to partner teams within Enterprise Information Security. Analyze cyber threat data and correlate with existing understanding of cyber threats impacting the financial services sector. Conduct research and write papers based on the identification of trends, up-and-coming threats, and tailor products to intended customers. Actively monitor and research cyber threats on the Internet and Dark web with a direct or indirect impact/relevance to financial services, business operations, technology infrastructure and client trust. Initiate and participate in cyber threat intelligence exchanges with the Wells Fargo LOB partners to include the full range of intelligence lifecycle activities. Information Security Analyst TIAA - Charlotte, NC June 2017 to March 2018 As a member of TIAA Entitlement Review Team responsible for facilitating access certifications for approx. 300 high-risk corporate apps Administrator on the RSA IDM/Governance and Lifecycle System (a.k.a. Aveksa) Daily monitoring

of open reviews (certifications) and engagement with reviewers who need assistance completing reviews. Processing of entitlement rejections from reviews including engagement with application access administrators in cases where de-provisioning activity is performed manually Provide support to end users by resolving issues and data submissions questions. Data submissions must be manually processed for consumption by the entitlement review tool. Follow-up with participation application teams for deliverable such as: periodic role attestations, manual reviews (when needed), updates to stale data, etc. Installing, Monitoring, Upgrading and Decommissioning of servers, which includes server installation, provision within the correct Domain, Organizational Unit, and applying appropriate Group Policy measures (all within Active Directory) Publication of monthly dashboards related to program effectiveness including compliance with the mandatory certification program requirements. Patch Management Security Analyst Sealed Air - Charlotte, NC September 2016 to June 2017 Configuration and monitoring of SEP on enterprise servers During the deployment phase of IDS Cylance, work in conjunction with the Infrastructure Teams (Server & End-User Computing) to assess, document and deploy LANDesk and Cylance, on all servers within the scope of the project (2100+ servers) Post Cylance Deployment Project design the execution of the Patch Management Project As a part of the Cyber Threat Team, researched potential threats on the horizon and assist in the execution of defensive measures to prevent attacks from occurring Identified, prioritize, and remediate security weaknesses. Conduct and manage vulnerability scanning via SIEM System Qualys Review Cylance to ascertain that no false positives or false negatives exist during post installation of application Use the Cylance logs to white-list and black-list individual applications as needed Information Security Analyst Wells Fargo - Charlotte, NC October 2015 to September 2016 IDM Reconciliation SME - support reconciliation duties in accordance with corporate governance regulations Vulnerability Management via minimizing Cyber Threats by enforcing strict cyber security policies which prevented internal users from becoming victims of aggressive external cyber threats, i.e. Insecure Third-Party Services and Business Email Compromise (BEC) Administrator on the Oracle IDM System During weekly Audit Team meetings, validate remediation or provisioning of user privileges, with documented

approvals gathered from request log files, SQL Server Reporting Services (SSRS), and Crystal Reports    Monitor the health of the Oracle IDM Solution- produce metrics, look for issues, monitor operational reports and follow-up with users of the solution    Answer questions escalated from Level 1 and 2 IDM Solution Support Team    Record submit and track IDM solution problem tickets from users numbering over 10,000    During application onboarding, educate new users of corporate security governance policies and how they apply to them IT Infrastructure Administrator - Server Team Camso Inc - Charlotte, NC March 2015 to September 2015 Exchange Migration Engineer, Team Lead LPL Financial - Charlotte, NC July 2014 to March 2015 IT Support Administrator Ei SolutionWorks - Kannapolis, NC January 2014 to April 2014 Lead System Support Specialist Monarch - Albemarle, NC December 2011 to September 2013 PC/LAN Analyst Wells Fargo - Charlotte, NC May 2010 to November 2011 Education B.A. in Psychology in Psychology University of North Carolina - Charlotte, NC January 1992 to May 1996 Skills Information Security (5 years), Ids (7 years), Ips, Qualys (3 years), Splunk, Active Directory (8 years), Security Controls, NIST, CIS, ISO (1 year)

Name: Victor Gilmore

Email: marypetersen@example.net

Phone: 285-353-5350x96155