Senior Information Security Engineer Senior Information Security Engineer Senior Information Security Engineer - National Government Services, Indiana Indianapolis, IN Sponsorship required to work in the US Work Experience Senior Information Security Engineer National Government Services, Indiana August 2017 to Present Responsibilities: ? Managed and maintained various network security systems including firewalls, IDS systems, central authentication systems, application proxies, and general support systems ? Experience developing strategic plans for agency-wide implementation to address the operations of client services, product support, and quality assurance. ? Expertise in conducting investigations of Security violations and breaches and recommending solutions; preparing reports on intrusions as necessary and providing analysis summary to management. ? Expertise in conducting investigations of Security violations and breaches and recommending solutions; preparing reports on intrusions as necessary and providing analysis summary to management. ? Proven ability in identifying various network security vulnerabilities and explain in detail how to remediate the identified vulnerabilities. ? Designed and implemented Server management tools for monitoring system and network performance, file integrity, and IDS policy management ? Conduct periodic network, system, application, and physical security audits ? Maintain a set of policy documents, security standards, and process and procedure documents for the Technologies Division ? Responsible for monitoring and, providing analysis in a 24x7x365 Security Operation Center (SOC) using various SIEM(Splunk), IDS/IPS software tools. ? Assist in identifying breaches in a firm's security or tracking the source of an unauthorized intrusion. Recommend all infrastructure and applications patching and remediation be done. ? Stay knowledgeable of current advances in all areas of information technology concerning vulnerabilities, security breaches or malicious attack Identify vulnerabilities or weaknesses in systems ? Identify vulnerabilities or weaknesses in systems. ? Evaluate security policy, processes and procedures for completeness. ? Ensure that controls are adequate to protect sensitive information systems. ? Report to management on IT system vulnerability and protection against malware and hackers. ? Clearly document and define risks and potential impacts along with the statistical probability of such an event and identify systems affected by the defined risk. ?

Monitoring overall performance of system and services ? Assessed Health of ePolicy Orchestrator environment and defined corrective actions to bring the environment to standards define in best practices IT Security Sr. Analyst Nike, Oregon May 2016 to May 2017 Responsibilities: ? Assist in identifying breaches in a firm's security or tracking the source of an unauthorized intrusion. ? Identify defensive steps to take, including necessary firewalls, security software and data encryption. ? Facilitated changes in the overall organizational policies to ensure alignment with the industry standards. ? Keep the business units updated with the changes in the applicable policies, standards and procedures ? Summarize the risk with written reports to Nike Business Unit Leadership to facilitate informed information risk decision regarding the procurement of proposed vendor service or product. ? Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements and ISO 27001. ? Facilitate implementations of information security policies, account security policies and standards for logical and physical security by NIST as reference. ? Perform Risk Assessment, Gap analysis & create Risk Mitigation plan. ? Perform Internal & External Audits ? Responsible for conceptualizing and driving BCP as a culture, within the organization. ? Analyzing and assessing the detected vulnerabilities towards their legitimacy and guiding the respective teams to take required steps to complete the Vulnerability management process. ? Effectively communicate and partner with large number of teams, across various geographical locations to minimize risks and stay compliant. Security Engineer Accenture - IN January 2014 to December 2014 Responsibilities: ? Work closely with leadership to maintain Security requirements for operation of ArcSight systems. ? Supports the establishment, enhancement, and continual improvement of an integrated set of correlation rules, alerts, searches, reports, and responses. ? Monitoring and analyzing the security event arises through Snort, Cisco IPS/IDS, ASA/PIX, Check Point, Symantec, Palo Alto, Fortigate and IBM ISS. ? Analyzing attack logs in HP Arc Sight tool to protect client network. ? Providing proper remedy to fix vulnerability in the client network after analyzing security incident queries alerted by Arcsight. ? Recording detailed Incident Response and activities for future reference. ? Writing new rules and in Arcsight based on customer requirement and removing false positive alerts based on alert

investigation. ? Develop content for a complex and growing ArcSight infrastructure. This includes Dashboards, Active Channels, Reports, Rules, Filters, Trends, and Active Lists in support of Cyber Operations. ? Provide optimization of data flow using aggregation, filters, etc. ? Participate in the operation of ArcSight Security Information and Event Management systems to include ArcSight ESM, Connector appliances/Smart Connectors, Logger appliances, network devices and backups. ? Support life-cycle management of the ArcSight platforms to include coordination and planning of upgrades, new deployments, and maintaining current operational data flows. ? Apply Configuration Management disciplines to maintain hardware/software revisions, ArcSight content, security patches, hardening, and documentation. ? Coordinate and identify critical libraries and support monitoring of identified assets. ? Provide operational metrics and reports on assigned tasks. Security Analyst Nokia - IN May 2011 to December 2013 Responsibilities: ? Handled Design, Testing and Implementation of Endpoint Protection (using Symantec Endpoint Protection Manager) and Endpoint Encryption (using McAfee EEPC). ? Regular testing of definitions and deploying to production. ? Providing Advanced Application Support for Symantec Endpoint Protection Manger and McAfee ePO. ? Implemented and migrated Symantec endpoint protection Manager 12.1 RU2 in three major sites ? Upgraded the version of Symantec endpoint Manager from SEP 11.x to SEP 12.x series. ? Configuring policies, communication settings and other important features in Symantec endpoint manager 11.x and 12.x series. ? Exposure in customizing SEPM policies and its Infrastructure. ? Management and configuration of policies for McAfee endpoint protection using ePoilcy orchestrator 4.6. ? Installing McAfee endpoint protection components such as Virus Scan enterprise (VSE) and McAfee agent (framework service). ? Mitigating major virus incidents in the subscribed client environment. ? Preparing documentation for major upgrade/migration activities. ? Preparations of Root cause analysis (RCA) for major Virus incidents. Education Bachelor of Information Technology in Information Technology JNTU 2011 Masters in Computer Science UCM - Kansas City, MO Skills Information Security Certifications/Licenses Symantec Endpoint Specialist Mcafee DLP Specilaist Mcafee Endpoint Admin CCNA CCNA Security

Name: Tina Joyce

Email: samantha81@example.org

Phone: 311.209.0485