IT Security Analyst IT Security Analyst IT Security Analyst - Charter Philadelphia, PA ? Information Security Officer (ISO) Information Security, GRC Consultant with experience in Governance, Risk, Compliance & Audit ISO 27001, PCI, HIPAA, SOX etc. Information Security & Network security functions. ? 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. ? Perform Risk Assessment, Gap analysis & create Risk Mitigation plan. ? Perform Internal & External Audits ? Deliver niche technology projects such as DLP and forensics to catch and prevent fraud, manage overall operational aspect of DLP. ? Oversee Vulnerability assessment /penetration testing of scoped systems and applications to identify system vulnerabilities. ? Responsible for conceptualizing and driving BCP as a culture, within the organization. ? Ensure IS policies are updated & reviewed. ? Experienced in CyberArk installation and implementation ? Manage relationships in all areas of IT and the lines of business. ? Subject matter expert (SME) for DLP, Firewall, VPN, Archer, Vulnerability Management solutions, IDS/IPS/WIPS, SIEM and Endpoint Security. Authorized to work in the US for any employer Work Experience IT Security Analyst Charter - St. Louis, MO October 2016 to Present Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements and ISO 27001. ? Working with McAfee ePO for managing clients workstations for providing end point security. ? Facilitate implementations of information security policies, account security policies and standards for logical and physical security. ? Working as Device Management in-charge to provide technology support, install, maintain, upgrade, and troubleshoot server's issues, networks, other security products, providing solutions to complex hardware/software problems. ? Vulnerability Assessment and Management (Nessus & Qualys) ? Installation and configuration of CyberArk Vault, Password Vault Web Access (PVWA), Central Password Manager (CPM) and Privileged Session Manager (PSM) in Prod and DR ? Working on the Security tools like Deep Security, HIPPM, Nessus, Symantec Control Compliance Suite 11. ? Perform Risk Assessment and drive the closures of identified risks. ? Working with EPO and other end point security tools and technologies

to run On Demand Scans as well as maintain the End Points across the infrastructure up to date. ? Daily monitoring of Solarwinds, FortiSIEM (AccelOps), Splunk, LogRhythm, Vectra (AI), Cylance, ESA, WSA, Umbrella, and Proofpoint ? Managing a Team for performing Release Management functions. Assessing the new releases, performing VA & Secure Code Review prior pushing them to Production Environment. ? Reviewing HLD & LLD from Security perspective. ? Security risk analysis & reporting using SPLUNK. ? Malware / Threat Analysis (WASC) ? Incident handling and analysis ? Creates and tracks internal and external incident reports ? Researches and assesses new threats and security alerts ? Log Monitoring & Analysis ? Coordination with external stakeholders ? Assists with documentation and procedural updates Security Analyst Bed Bath & Beyond, NJ 2016 to September 2016 Worked on tools like Active Directory and Group Policy, Symantec Data Loss Prevention, Symantec End-Point Protection Manager, Symantec Endpoint Encryption, Windows Server Update service, Bluecoat Proxy, Syslogs, GFI ? Frame works used ISO 27001 ISMS, PCI DSS, SSAE16, OWASP, SANS ? Experience on Nessus VA and BurbSuite PT ? Monitor their organization's networks for security breaches and investigate a violation when one occurs ? Install and use software, such as firewalls and data encryption programs, to protect sensitive information ? Prepare reports that document security breaches and the extent of the damage caused by the breaches ? Conduct penetration testing, which is when analysts simulate attacks to look for vulnerabilities in their systems before they can be exploited ? Research the latest information technology (IT) security trends ? Help plan and carry out an organization's way of handling security ? Develop security standards and best practices Cyber Security Engineer TechDefence - IN May 2012 to July 2013 Assisted on forensic analyses using forensic tools to find case specific information ? Reviewed Digital Forensics evidence using EnCase ? Implemented Web and Network Security ? Performed Network vulnerability analysis using different security tools ? Examined Foot Printing Methodologies ? Implemented IDS and IPS ? Implemented Web Application Firewall ? Monitored and update security systems from time to time ? Prepared and maintained necessary documents relating to data security systems ? Determined OWASP TOP 10 vulnerabilities on web application like SQL injection, XSS, session hijacking, etc. Education Ganpat

University September 2013 to October 2015 Skills SECURITY (3 years), ISO (2 years), ISO 27001 (2 years), NESSUS (2 years), GOVERNANCE (1 year) Additional Information Technical Skills: Platforms/Applications ? Continuous Monitoring: Vulnerability Management, Web Application Scanning, ThreatProtect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management and Compliance, Solarwinds, Nexpose, Forcepoint, Rapid7 ? Event Management: RSA Archer, Blue Coat Proxy, Splunk, NTT Security, LogRhythm, HP Arcsight ? PenTest Tools: Metasploit, NMAP, Wireshark and Kali ? McAfee Email Security Gateways GUI & CLI (1 year), ? McAfee Network Data Loss Prevention (2 years), McAfee NITRO SIEM - Security Information and Event Management (1 year), ? Carbon Black Endpoint Security - Threat & Process Analysis (1 year), ? McAfee EPO (ePolicy Orchestrator) - GUI (Less than 1 year), Securonix Analytics & Intelligence Tool - GUI (Less than 1 year), ? Security Software: Nessus, Ethereal, NMap, Metasploit, Snort, RSA Authentication ? Frameworks: NIST SP 800-171, ISO 27001/31000, HIPPA, HITRUST CSF, PCI DSS ? Security Intelligence: WhiteHat Web Security, iDefence, NTT Security, LogRhythm ? SIEM: Splunk, Solarwinds, ArcSight, Nitro, IBM QRadar, Forcepoint, Rapid7 Nexpose ? Switches: Cisco Catalyst VSS 1440 / 6513 / 6509 / 4900 / 3750-X / 2960 ? Routers: Cisco Routers ASR 1002 / 7606 / 7304 / 7206 / 3945 / 2951 / 2600 ? Firewalls: Check Point, ISA 2004/2006, Palo Alto PA 3000/5000 ? Networking: Conversant in LAN, WAN, Wi-Fi, DNS, WINS, DHCP, TCP/IP, ISCSI, Fiber, Firewalls/IPS/IDS ? Routing: OSPF, EIGRP, BGP, RIP-2, PBR, Route Filtering, Redistribution, Summarization, Static Routing ? Switching: VLAN, VTP, STP, PVST+, RPVST+, Inter VLAN routing & Multi-Layer Switching, Multicast operations, Layer 3 Switches, Ether channels, Transparent Bridging ? Protocols: TCP/IP, L2TP, PPTP, IPSEC, IKE, SSL, SSH, UDP, DHCP, DNS ? Hardware: Dell, HP, CISCO, IBM, SUN, CheckPoint, SonicWall, Barracuda Appliances, SOPHOS email appliances ? VPN: ASA 5520, Cisco Concentrator 3030, Nortel Contivity Extranet 1500 ? NMS: NAM, Sniffer, Solarwinds NPM, Cisco Secure ACS 5.2, CiscoWorks ? Operating Systems: Windows, Unix, MS-DOS, RHEL, CentOS, Kali Linux

Name: Craig Foley

Email: garciasamantha@example.net

Phone: 488-704-0427x6167