IT Security Analyst IT Security Analyst IT Security Analyst - Altice USA York, NY Information Security Analyst/Engineer with experience in analyzing security incidents, Vulnerability and Penetration testing, Network Monitoring, Information Security & Network security functions. Experience with industry recognized SIEM (Security Information and Event Management) solutions such as NITRO, Splunk, Forcepoint and many other tools. Hands on experience with security consulting and research Hands on experience with HP Arcsight, IBM QRadar, Rapid7, Forcepoint Hands on Experience with RSA Authentication Solid understanding of working with NIST 800-53 framework Hands on experience with Incident Handling, Documentation and log analysis Experience and better understanding of scripting languages, command shells and regular expressions such as Python, Perl, visual basic Hands on experience with Fireeye Network(NX), Email(EX), Malware analysis(AX), Host (HX) and packet capture(PX) series Assess and evaluate business and technology risks, internal controls which mitigate risks, and related opportunities for internal control improvement Hands on Experience with Security frameworks such as NIST, HIPAA, PCI-DSS Excellent consulting and partnership skills in a large organization Experience on the technical delivery side of Governance Risk and Compliance (GRC) projects Troubleshoot issues and perform many tasks related to technologies such as RSA Authentication Hands on Experience with Rapid7 Nexpose, Metasploit and ForcePoint Experience with identity and access management solutions such as LDAP, Active Directory, XAML, SAML and multi factor authentication Worked in SOC department to analyse security incidents and log analysis Implementation of a GRC utility (from POC, through evaluation, selection, and implementation) Solid understanding and implementation of Firepower and identity service engine for big organizations Experience with 802.1x implementation and support Solid working knowledge of ethical hacking and testing of cryptographic algorithms Solid Knowledge of Linux, RHEL, CentOS, Windows, Unix Operating systems Identify the threat vectors and security events by analyzing signatures Perform Risk Assessment, Gap analysis & create Risk Mitigation plan. Experience configuring and deploying McAfee modules and products like McAfee ePO, McAfee VSE, McAfee HIPS, McAfee Endpoint Encryption, McAfee Network DLP, McAfee DLP Endpoint, McAfee SIEM. Oversee Vulnerability assessment /penetration testing of scoped systems and applications to identify system vulnerabilities. Having good experience SAST and DAST applications using different tools HP Fortify and IBM AppScan. Excellent knowledge of FISMA, HIPAA and NIST Compliance usage, rules and regulations Hands on experience with creating Regular expressions for any signatures Use Splunk Security Manager to identify threats and assigned category. Solid Understanding of IBM QRadar, Palo alto NGFW Provided technical security proposals, security presentation, installing and configuring Checkpoint and Palo Alto firewalls, VPN networks and redesigning customer security architectures Researched, designed, and replaced aging Checkpoint firewall with new next generation Palo Alto appliances serving as firewalls and URL and application inspection Familiar with SSAE 16, ISO27002, Safe Harbor, Privacy Shield, General Data Protection Regulation (GDPR) Performed upgradation of Palo Alto firewall from old platforms to new platforms 6.1.5 to 6.1.10 Configured Palo Alto Next-Generation Firewall mainly VSYS according to client topology Specialist in Consulting of different security solutions for all phases of solution cycle: Planning, Architecture, Design, Implementation, Deployment, Troubleshooting & Support, Handover and Documentation. Strong understanding of DLP Architecture, Rules and Policies and its implementation Hands on experience in administering and managing network and server infrastructure technologies and devices including firewalls, routers, switches, servers etc. Knowledge & Experience of OWASP top 10 vulnerabilities Experience in Network security design, proposal, solutions development and solutions architecture Excellent Project Management skills and adaptable to work in any work environment Assist in the creation of an end-to-end technology strategy for SIEM to address current and future security concerns, emerging threats, regulatory compliance and alignment with technology and the business Strong understanding of communication protocols (SSL, TLS, IPSec) Provide support in security architecture, design, developing, monitoring and supporting enterprise infrastructure environment Excellent security management and auditing experience. Antivirus: McAfee Virus Scan Enterprise, Symantec, Endpoint Protection Suite DLP: Websense, Symantec & McAfee End Point Security: McAfee Suits (VSE, HIPS & HDLP), McAfee MOVE AV, Safeboot IPS/IDS: McAfee IPS, HP Tipping Point, Cisco IDS, SecureWorks IDS/IPS SIEM: RSA Envision, Arcsight, Splunk security manager, IBM QRadar MSS: Vulnerability Assessment, Content Filter, Antispam, IDS/IPS Management Vulnerability Management Tools: Foundstone, QualysGuard, Nessus, Nmap, Nexpose, Wireshark Security Tools: Splunk ES, McAfee Vulnerability management solutions, Burpsuite, OpenVAS, Nessus, Qualys, Solarwinds, ForeScout Preparing for CISSP certification and will get it in November Specialization Governance, Risk & Compliance: GRC Archer, Risk Assessment, Compliance Tracking, Audits- ISO 27002, SSAE 16 PCI, GDPR, NIST, FISMA, Network Security: NIPS/NIDS, Firewall, VPN (IPSec, SSL), DLP, Endpoint Security / Information Security: Antivirus, HIPS, Encryption, HDLP, Malware Analysis, Advance Threat Protection Content Protection: Email Security, Web Security, Application Security SIEM Tools: McAfee SIEM, Splunk SIEM, HP ArcSight Work Experience IT Security Analyst Altice USA - Hicksville, NY December 2017 to Present An Information Security Analyst with focus on Cyber security, continuous monitoring, access control and compliance. Performed advanced cyber security operational monitoring and analysis of security events Ex: Security information monitoring tools, network and host based intrusion detection tools, system logs such as windows, mainframes applications and databases with different security technologies i.e., SIEMS (McAfee, RSA) cisco, IronPort proxy, McAfee endpoint such as VSE, HIPS, McAfee encryption, remediation of workstation and servers for antivirus with ePO. Daily assessment of Vulnerabilities identified by Dell Secureworks Firewall and IDS/IPS System through RegEX McAfee ePolicy Orchestrator, McAfee VirusScan Enterprise, MCP and HIPS Monitoring and troubleshooting of security threat event, intrusion detection, Virus/Malware outbreaks. Configuration of McAfee Antivirus products on end-points (Clients/Servers). Hands on Experience with Metasploit exploit techniques Solid understanding of RSA authentication and Rapid 7 technologies and ForcePoint Assist in developing procedures for monitoring, detecting, reporting, and investigating information security breaches Manage all evidence collection activities for PCI DSS compliance. Mature the PCI DSS evidence collection process and streamline evidence collection procedures. Analysed information security data from network and applications security logs and tools such as firewalls, proxies, application vulnerability scanners, network flow data, external data sources and cyber threat intelligence to identify potential compromises. Static Code analysis using HP Fortify to identify the vulnerabilities in the applications. Frame works used ISO 27001 ISMS, PCI DSS, SSAE16, OWASP, SANS Worked on SOC department which runs 24*7 days and able to analyse all security incidents Conducted network penetration tests and implemented vulnerability assessments Have solid experience working with FireEye HX, NX, EX, AX series Worked with GRC technology and have better understanding on it Implemented critical infrastructure projects including the development and design of a variety of essential network and endpoint security solutions such as: Entrust PKI, AAA services, BMC Control-SA, and perimeter security design with Cisco network devices, Websense, netForensics, and DNS Worked with Embedded system technologies to remediate attacks on them Participated in courses for password cracking and attack technologies Solid understanding of OWASP top Vulnerabilities and other software security best practices Familiarity with security and testing tools such as Burp Suite, Nmap, Zenmap, OpenVAS, Nessus Experience with penetration testing against a wide variety of application layer platforms, including web, mobile, and thick client above and beyond running automated tools Create and manage documentation necessary to accelerate the RFP response process. Solid experience with Ethical hacking and testing/development of Cryptographic Algorithms Resolve Incidents while investigate & troubleshoot root causes when escalated Experience with network layout, topology and configuration Real time analysis of security events or threats which is generated by network hardware and applications through SIEM tools such as HP ArcSight Conducting Security assessment of various security events through Splunk, Secureworks platform Hands on experience with AWS and Azure cloud management Used remediation techniques for all collected vulnerabilities and if it is very high severe vulnerability then ticket escalate to the higher authority Responsibility for the planning and controlled execution of releases into the managed environment Performed vulnerability scanning on web applications and databases to identify security threats and vulnerabilities. Conduct FISMA complaint security control assessments to ascertain the adequacy of management, operational, technical and privacy controls. Conducted system security assessments based on FISMA, NIST and HIPPA/PCI DSS

Compliance. Excellent knowledge of Compliance documentation (FISMA, NIST, HIPPA etc.) Other contracts involved assessing threats to resources by identifying vulnerabilities to loss of resources, and protecting from threats/reducing the risks/exposures by utilizing appropriate security design, strategy, & architecture. Perform Risk Assessment and drive the closures of identified risks. Vulnerability Management: Configured Qualys, Nessus Guard Tool for Vulnerability Analysis of Devices and Applications. Monitored them constantly through the dashboard by running the reports all the time. Experience on administrating and maintaining Red Hat Enterprise Linux system Responsible for identifying the cause of security incidents, monitor user activity, thwart data breaches and meet regulatory compliance requirements and mitigating advanced cyber threats. Worked with other team members to complete special projects and achieve project deadlines. Conduct analysis, cyber threats, the discovery of IT vulnerabilities, monitoring for cyber intrusions, troubleshoot and response to security incidents detected from HP ArcSight and related SIEM. IDS/IPS, and other security applications Conducting security workshops and presentations for the clients. Cyber security Analyst CTS - Windsor, CT January 2017 to November 2017 Configure, upgrade and fine tune the DLP policies to meet the changing needs & improve Security Metrics Responsible for Monitoring and enforcing information security program and policies Responsible for developing information security risk identification, classification, triaging and mitigation Worked with the enterprise architecture team, Security Governance, and Policy team Good understanding of administering and implementing SIEM, DLP, Web sense, Advance malware detection program, vulnerability assessment, and prevention, Had to deal with SIEM solutions such as Rapid7 Nexpose, Forcepoint, Splunk Maintaining Microsoft Active Directory, routers, switches, and Symantec backup Performed penetration testing on internal website using OWASP top 10 Vulnerabilities. Good understanding of IT security concepts with an emphasis on Security Operations, Incident response, Vulnerability Management, PKI encryption, network security control tools and functionalities. Managing Security Operation Centre Services, Information Security Transitions, Security Controls Gap Analysis, Service Assurance Programs, help team for Internal and External IT Audits, Security Consultation, Information Risk Assessment for various processes

Performed Static Application Security Testing (SAST) using tools such as HP Fortify. Entrust PKI and Security management, penetration testing and website protection with mitigation and remediation of Intrusion Prevention Systems (IDS/IPS). Executed the PCI Data Security Standards (PCI DSS) assessments for all controls, including communication of key milestones, gap remediation consulting/tracking, and guidance on compensating controls Solid Knowledge of TCP/IP and OSI models Worked with all Metasploit Exploitation techniques Conducting security workshops and presentations for the clients. Duties involves participation in managing technologies, evaluating new technologies, continuous improvement of SLA, customer meetings, implementing new solutions as asked by customer. Performing Vulnerability Assessments and taking the required counter actions and measurements to ensure the security of the IT infrastructure / systems. Analysis and documentation of network & information security requirements and define security policy for enterprise client and business critical servers. Jr. Security Analyst Ahinsa Systems - IN January 2013 to July 2016 Assessed and built a data protection program through data classification skills and a clear understanding of privacy standards and regulations Data Loss Prevention suit, Symantec DLP Product - Implementation and deployment as the champion team Deployment of Data loss prevention across the network - Data in motion, Data in Use & data at Rest servers Reviewed encryption logs and DLP logs to regulate use base technological risk violations Gained experience with Symantec DLP Software: DLP Cloud Prevent for Microsoft Office 365, DLP Cloud Storage, Cloud File Sync and Share, and security product capabilities Deployed in the cloud and on-premises using Amazon Web Services (AWS) and Single- Server support Analyzed Symantec DLP events and reports Lead and perform the annual SOX Audits and PCI assessments Performed tuning of Symantec DLP to reduce false positives and improving detection rates Network Access Control - Implementing a secure solution to identify network devices and profiling the Network devices to allow or disallow access based on the device type Signature Updates Deployment on the Management Components and all the Individual IPS/IDS devices Intrusion Prevention System - IDS/IPS Implementation and Upgrade for SiteProtector Refined IPS Policy and Creating Rules according to the Security Standard Analyzed the Network

Attack, blocks, detects and regular Health Checkups in the real environment Prepared the Knowledge Transfer document of Process and Technical specifications guide for the Transition/Internal purpose Ensured smooth transition for all the Security Applications, Preparing Team Metrics report and Project status report weekly/monthly presenting to the Customer. Client facing role and Understand the Customer requirement. Determined OWASP TOP 10 vulnerabilities on web application like SQL injection, XSS, session hijacking, etc. Contributed in providing Secure environments for our clients regarding PCI compliance. Education Bachelor's Skills IDS (5 years), IPS (5 years), METASPLOIT (1 year), PCI (5 years), SECURITY (5 years) 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 Networking Protocols: FTP, SNMP, Telnet, HTTP, SSH, DNS, DHCP, DHCPv6, ICMP, ICMPv6, SMB Event Management: RSA Archer, Blue Coat Proxy, Splunk, NTT Security, LogRhythm, HP Arcsight PenTest Tools: Metasploit, NMAP, Wireshark and Kali Security Software: Nessus, Ethereal, NMap, Metasploit, Snort, RSA Authentication Frameworks: ISO 27001, PCI-DSS, SSAE 16, FedRAMP, SOC 2, UEBA, ISAE 3000, HIPAA, NIST. 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, FTP, SNMP, Telnet, HTTP, SSH, DNS, DHCP, DHCPv6, ICMP, ICMPv6, SMB, WINS, 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: Dawn Ritter

Email: samanthashaffer@example.com

Phone: 493-373-3444