Sr. IT Security Analyst Sr. IT Security Analyst Sr. IT Security Analyst - Express Scripts Inc Atlanta, GA Experienced Security Consultant with 6+ years of IT experience with a focus on designing and developing security solutions. Skilled & technically proficient with multiple firewall solutions, network security, and information security practices. Manage SOX and PCI compliance program, controls and remediation efforts Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools. Advanced Knowledge in IPSEC VPN design connection and protocols, IPSEC tunnel configuration, encryption and integrity protocols. Knowledge of Intrusion Detection, DMZ, encryption, IPsec, proxy services, Site to Site VPN tunnels, MPLS/VPN, SSL/VPN Trouble shoot various appliances on the SIEM platform via various Linux commands and Knowledge of capacity planning and Linux performance. Worked on Bluecoat proxy to analyze and scan malwares to protect the infrastructure Configuration and maintenance of SIM/SIEMS tool - QRadar, Splunk &Arcsight Onboard new log sources with log analysis and parsing to enable SIEM correlation. Implemented multiple tools including Symantec DLP, and QRadar SIEM Implementation and Management for Qradar SIEM and Sourcefire IDS Establish roadmaps for implementing policies and standards to align with COBIT Managed Security Expertise in Gathering and analyzing metrics, key risk indicators and maintain scorecards defined within the area of information security to ensure our information security program is performing effectively and efficiently. Familiar with general security risk management principals and best practices. Supported the information security audit and third-party assessment initiatives during planning, execution, and remediation phases, as well as coordinating and tracking remediation activities. Full knowledge of vulnerability management Worked on files integrity monitoring continuously tracks changes to file and identifies who made changes to which files using McAfee control. Strong knowledge of PKI concepts, patterns and practices Lead the definition and implementation of POCs around PKI and other certificate related technologies Performed routine network startup and shutdown procedures, data backups, and disaster recovery operations on secured and unsecured networks, Monitored security aspects of various operating systems (UNIX, LINUX, MS

Windows, Netware) commercial, freeware, and government-owned security tools and firewalls. Experience analyzing McAfee DLP events and reports Experience with McAfee global threat Intelligence and McAfee threat Intelligence Exchange to provide global and local reputation of files and applications. Liaison between the audit/assessment teams and Information Security management. Familiar with threats and vulnerabilities, latest trends and risks and be able to understand the technical remediation action steps or plans and communicate them effectively to teams within the organization Managed policy exceptions with Business Unit requestors and coordinate the annual exception review process. Configured scripts to run and pull backups of Firewall configurations Worked directly with various teams to document exceptions, identify compensating controls, and remediation action plans accordingly. Support security compliance initiatives and assessments including responses to client security organization audits, questionnaires. Experience working on Linux, Centos, shell scripting (VIM, VI, nano). Provided process improvement suggestions for more effective management and review of exceptions. General knowledge in the areas of IT management, acquisition and maintenance of systems, system operations and Information security control activity. Experienced in the design and deployment of Palo Alto, SourceFire, Checkpoint Firewalls & Blue Coat Proxy Knowledge in planning, design, implementing and troubleshooting, complex networks and advanced technologies.

Been a focal contact for departments client Policies and Standards based Audit for ISO/IEC 27001:2013 Standard. Used per defined scripts as well as custom script to administer Windows 2008 server using power shell. Experienced in design, installation configuration, Administration and troubleshooting of LAN/WAN infrastructure and security using Cisco routers/Switches/firewalls.

Monitored and researched Cyber Threats with a direct & indirect impact to the organization internally. Assisted in Symantec HIDS/NIDS Setup using HPSA implementation and provided status reports. Experience in Security Information and Event Management Tools like IBM QRadar, Splunk and RSA Archer. Understand PKI and SSL key management Advanced knowledge in Cisco Switches and Routers Configurations. Advanced knowledge in TCP/IP suite and routing protocols, such as OSPF, BGP, and EIGRP. Conduction of Security Awareness and Network

training for NOC and SOC staffs. Drafted and installed Checkpoint Firewall rules and policies. Experienced in conducting Disaster Recovery drills and following best practices for network operations and security. Expertise skillset includes solutions for clients in the financial, retails, chemical & technology services domain. Extensive experience in balancing Information Security requirements by having a broader perspective on the business process of security administration. Hands on skills include end-to-end security management (security aspects in all stages of product development) and end-to-end product development (from functional design of the system to testing and deployment). Work Experience Sr. IT Security Analyst Express Scripts Inc November 2017 to Present Responsibilities: As a threat hunter continues Monitoring External Feeds information, existing correlated offences, and End Device Logs Source, Real time log threat abnormality activity, and further investigation triage. Generated IR workflow security documentation, including security assessment reports, contingency plans; and disaster recovery plans. Establish a bridge call between corresponding members during high incident handling. SIEM tools experienced QRadar/ArcSight Utilized Security Information and Event Management (SIEM) - ArcSight, QRadar, Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP). Provided high level analysis on security data to identify significant activity. Observed and analyzed traffic in order to learn valuable lessons from known malicious actors and to determine countermeasures against such threats. Provided detailed status updates on existing cyber security incidents daily to include follow up with client/customer to ensure satisfactory resolution. Interacted with cyber intelligence analysts conducting threat analysis operations as well as numerous IT professionals performing varying technical roles within the client organization. Conveyed verbal briefings to management on pending cyber incidents as well as coordinate with CERT and AV Vendors as necessary to convey incident information. Acted as alternate shift lead as necessary, mentor new associates on process and procedure, manage group mailbox, and open tickets for new incidents. Monitoring security patch levels of the servers, workstations and network environments, and anti-virus systems.

Make recommendations to senior management on results of analysis and work closely with other Information Technology groups to refine and enhance security controls. Conducted base level

analysis to determine the legitimacy of files, domains, and emails using tools such as Wireshark, Snort and a Linux Toolkit as well as online resources such as Virus Total, URLVoid, IPVoid, and Robtex. Security Dashboard monitoring, Reporting tool Remedy, Service Now. Manage and maintain Arc sight, RSA, Nitro System health Performed shift lead roles and responsibilities in support of SOC/CIRT on an enterprise level. Involve in Content Creation to fine-tune the incoming events for effective monitoring. Create SOP's related to event validation and escalation, and system health issues. Created and configured management reports and dashboards using Splunk

Performed Secure Network Architecture review for New Branch office and upcoming Vendor/Client's network. Performed vulnerability assessment for Web Application & Network and leads to be closing of all the findings. Identifies new security threats by conducting penetration testing, log analysis and vulnerability assessments; evaluates and recommends on procedures used to mitigate risks. Connectivity check between end devices of Agent and log collector used tool Infoblox, And of Dashboard. Personal interest experienced forensic in my personal lab tools used (FTK, Burp Suite). Created custom and cloned applications for 6 modules in the Archer eGRC tool suite for audit, compliance, incident response and policy management. Verified compliance with information security requirements derived from organizational missions/ business functions, federal legislation, directives, regulations, policies, and standards/guidelines. Monitored sources of security intelligence, drafted security event notifications to be distributed to agencies, stake holders and business partners, to distribute notifications to the appropriate groups. Conducted Tenable Nessus, IBM Appscan vulnerability scanning for all endpoints, servers, and web applications. Ensures knowledge and control of changes to organizational systems and environments of operation; and maintains awareness of threats and vulnerabilities. Interpreting scan results, validating test scans, and work with developers to identify code changes required to address vulnerabilities identified by the tests. Conducted analysisand disseminated scan results to senior management and provided patch management recommendations. Information Security Specialist American Express - Phoenix, AZ September 2016 to October 2017 Responsibilities: Responsible for the Governance, Risk, and Compliance solution for all security operations, risk assessment, and

cyber risk register procedure. Responsible for the administration, management and upgrade of modules for the Archer eGRC tool. SIEM technology used in the organization is RSA Envision, where I am responsible for event analysis and escalation with remediation process as a Admin. Provide security monitoring, event analysis, and countermeasure proposals for the security incidents using RSA Envision, Packet capture tools (WireShark, Microsoft Network Monitor) Continuously monitored, analyzed and identified security alerts information from all approved security devices, collection techniques and designated system logs. Read Symantec logs and make sure ISSO is aware of any anomalies and odd behavior on the network. Performed analysis on security incidence that is required to learn valuable lesson about attack and implement changes proactively based on knowledge learned Using BMC Remedy tool and mail system to assign the incidents to the respective supported technology team. Acted as alternate shift lead as necessary, mentor new associates on process and procedure, manage group mailbox, and open tickets for new incidents. Coordinate with the internal technology teams regarding any incident aging and ensure SLA timings.

Firewall rule creation to restrict unauthorized social sites (Model -NSA 2400 Sonicwall Firewall, PFSense). Installing, administration and maintaining various (applications / operating systems) and hardware devices. Managing devices like Routers & Switches, Wireless Devices & configuring them as per network requirement. Network monitoring planning, monitoring, maintenance & trouble shooting activities to ensure maximum uptime. Scanned internal Network with different tools (MBSA, Nexpose, Metasploit, Nmap, Qualys). Cyber security Analyst Ocean Web Technologies Pvt. Ltd October 2013 to April 2016 Responsibilities: Served as the main point of contact for over 100 employees regarding IT. Responsible for IT efforts from start to completion, including projects, overhauls, implementations, and network upgrades. Established entire Endpoint Protection (antivirus) implementation to include Symantec SEP, Cloud management and critical systems protection. Revamped security standards to include a changeover to a more robust firewall and Intrusion protection/prevention implementation. Restructured Active Directory to reflect best practices for security groups and need-to-know access to certain areas and documents within the company Developed and suggested security standards for Windows security Audits.

Created procedures and guidelines in performing vulnerability assessments. Provide training to freshers on Information security policies and conduct awareness sessions to other departments in the organization. Evaluate emerging technologies that might enhance the overall security posture of the organization while ensuring compliance to regulatory requirements. Experienced on service delivery, managing project requirement, customer relationship, allocating work, conducting status meetings and customer reviews, technical support and system administration. Provided security assessment/approval for all internal projects; performed security assessments for production/testing/development environments IT Security Analyst RD Technology - IN January 2012 to September 2013 Responsibilities: Coordinate and manage team activities during assessment engagements. Troubleshot LAN related issue of Enterprise Customers in terms of switching and connectivity. Provided support for BGP configuration related issues for customers. Optimized the network with Traffic Switch Over techniques. Configured and troubleshooting DHCP issues on Switches. Created of Network diagrams on Visio. Install and configure the Qradar SIEM including all its components, local & or remote log collectors. Worked on SIEM tool Qradar for reporting and data aggregation Used SIEM tool Qradar on adding the newly build windows and Linux log servers and creating policies for different alerts Security Audit, Budget Violation, Operational Violation, Best practice check in client AWS environment. Cisco Routers, Switches IOS upgrades with latest IOS (12.X till 15, x) version as per company standards. Coordinated with Network Administrator regarding BGP/OSPF/EIGRP routing policies and designs, worked on implementation strategies for the expansion of MPLS VPN networks. Troubleshooting the Network Routing protocols (BGP, MPLS EIGRP and RIP) during the Migrations and new client connections Participate in meetings to discuss system boundaries for new or updated systems to help determine information types for categorization purposes. Determine the classification of information systems to aid in selecting appropriate controls for protecting the system. Education Bachelor's Degree in Electronics and Communication Engineering Jawaharlal Nehru Technological University 2009 to 2013 Skills WIRESHARK (2 years), SECURITY (3 years), RSA (2 years), LINUX (2 years), OPERATIONS (2 years) Additional Information Technical Skills Platforms/Applications Qualys

Continuous Monitoring: Vulnerability Management, Web Application Scanning, Threat Protect, Policy Compliance, Cloud Agents and Asset Management Event Management: RSA Archer, Blue Coat Proxy, Norse, Splunk, NTT Security, LogRhythm PenTest Tools: Metasploit, NMAP, Wireshark and Khali Frameworks: NIST SP 800-171, ISO 27001/31000, HIPPA, HITRUST CSF, PCI DSS Security Intelligence: WhiteHat Web Security, iDefence, NTT Security, LogRhythm. 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 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 Languages: C / C++, Bash, Python, Core Java, Shell script, JavaScript, HTML, UNIX, PowerShell, Ruby. Protocols: TCP/IP, L2TP, PPTP, IPSEC, IKE, SSL, SSH, UDP, DHCP, DNS Nexus: Nexus 7010 / 5548 UP / 5020 / 2232 PP / 2248 TP / 1000 V UCS: Fabric Interconnect 6248/6120, IOM 2208/2204/2104, B200 M2, HP VC FLEX-10 ANS: F5 BIG-IP LTM 6900/6400, Array APV 5200/2600/TMX 5000, Cisco CSM, CSS VPN: ASA 5520, Cisco Concentrator 3030, Nortel Contivity Extranet 1500 NMS: NAM, Sniffer, Solarwinds NPM, Cisco Secure ACS 5.2, CiscoWorks Operating Systems: Windows, NT, Windows 98/XP/2000/2003/2007, MS-DOS, Linux. Networking: Conversant in LAN, WAN, Wi-Fi, DNS, WINS, DHCP, TCP/IP, ISCSI, Fiber, Firewalls/IPS/IDS Hardware: Dell, HP, CISCO, IBM, SUN, CheckPoint, SonicWall, Barracuda Appliances, SOPHOS email appliances

Name: Jeffery Norman

Email: msullivan@example.net

Phone: 363.747.2642x78447