IT Security Analyst IT Security Analyst IT Security Analyst - MAHLE INDUSTRIES INC ? 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 ? Familiar with SSAE 16, ISO27002, Safe Harbor, Privacy Shield, General Data Protection Regulation (GDPR) ? 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 ? 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 ? Knowledge in shell scripting ? Hands on experience with Qualys Guard vulnerability management tool ? Perform Network and OS hardening to make premises secure ? Experience working on Palo Alto Firewalls ? Experience in adding Rules and Monitoring Checkpoint Firewall traffic ? Thorough knowledge in Solaris Administration ? Thorough knowledge in Cloud security ? Knowledge of OWASP top 10 vulnerabilities ? Configurations including AD integration and Management of Cyber Ark Enterprise Password vault ? Review risk and safety reports, risk scores and flagged high risk factors ? Antivirus McAfee Virus Scan Enterprise, Symantec, Endpoint Protection Suite Work Experience IT Security Analyst MAHLE INDUSTRIES INC - Farmington Hills, MI January 2017 to Present Responsibilities: ? Responsible for capturing security and privacy requirements for clients to be compliant with Payment Card Industry (PCI). ? Experienced with, DLP, Bluecoat websense, Proofpoint, Trend Micro, Nexpose (Rapid7) and Splunk Enterprise SIEM security tools to monitor network environment ? Assisted engineers with Splunk troubleshooting and deployment ? Created Splunk dashboards for

investigations ? Review risk assessments completed by security team based on National Institute of Standard and Technology (NIST) and International Standard Organization (ISO) by using its methodology is based on the PDCA cycle, which builds the management system that plans, implements cybersecurity, maintains, and improve the whole system. ? PKI/Certificate Authority (CA) support and implementation. ? Perform log analysis utilizing Splunk and various other security software and tools ? Manage Splunk configuration files like inputs, props, transforms, and lookups. Upgrading the Splunk Enterprise and security patching. ? Monitor client environment using Security Event and Information Management (SIEM) technology to centralize the storage and interpretation of logs; collect data into a central repository for trend analysis and provide automated reporting for compliance and centralized reporting, which provides more situational awareness and real-time analysis of security alerts. ? Responsible for monitoring and, providing analysis in a 24x7x365 Security Operation Center (SOC) using various SIEM, IDS/IPS software tools. ? Create policies, alerts and configure using SIEM tools ? Assist with vulnerability scans and reporting to clients and IT departments, use of Nessus scan and Report, Review the vulnerability scan that affects the assets and find critical devices that have critical vulnerability ? Work experience with IT policies, procedures, and standards are related to doing security review using the NIST standard specifically with NIST 800-53 and NIST 800-66 for HIPAA security rules. Review the Logs for malicious user activities ? Complete security project management to ensure that clients remain on track for their annual security assessments. ? Implement solutions as a part of the project support which include EventSentry SIEM, Nessus Vulnerability scanner and Palo Alto Firewall. ? Deploy EventSentry SIEM 3.3.1 from scratch for security log monitoring and alerting in production environment including switches, routers, firewalls, load balancers, VPN and expand the deployment to the corporate domain. ? Manage and Maintain Nessus Vulnerability scanner 6.11.0, add additional scan engine to a production environment and identify gaps in patching. ? Create dynamic groups for discovered assets by asset location and operating systems to run full system audit scans. Security Analyst HP Inc - Houston, TX March 2015 to December 2015 Responsibilities: ? Configure and Install Splunk Enterprise, Agent, and Apache Server for user and role authentication and SSO. ? 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) ? Successfully delivered RSA Archer Solutions in various SLDC stages including Analysis, Design, Development, Enhancement, Testing, Migration, Documentation and implementation of applications in Archer platform ? 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 in the Questionnaire Assessment Building from Scratch. The First Engagement was: Regulatory Compliance Risk Assessment Questionnaire ? Working on Numerical Fields Such as Inherent Risk Assessment Risk Rating Score calculation, Assessment Questions etc. ? Configuring and Performing Qualys Guard scans for all assets in the enterprise and evaluation of potential vulnerabilities ? Vulnerability Scanning and creating the reports using Qualys Guard ? Perform OS and Network hardening using different approaches ? Conduct regularly scheduled reviews of the organizations firewalls (rule sets, VPN). Using Splunk to extract useful data from syslog events and using this to formulate permit rules ? Extensive experience with the Palo Alto Panorama management console. Packet analysis with Wireshark. Configuration of Palo Alto firewalls, access policies, Application & URL filtering, Security Profiles, Global Protect VPN, Data filtering and file blocking ? 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 ? 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) ? Administration of User accounts, Group memberships, and Organizational Units

using Active Directory ? Perform migration user accounts into Password Vault using Bulk upload utility ? 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 Information Security Administrator Yujas InfoTech November 2012 to November 2015 Responsibilities: ? 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. ? Worked with Palo Alto Panorama management tool to manage all Palo Alto firewall and network from central location. ? 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. ? Implemented ISL and 802.1Q for communicating through VTP. ? Working with Client teams to find out requirements for their Network Requirements. ? Designing solutions for frozen requirements using Cisco Routers and Switches. ? Deploying the network infrastructure to meet the requirements. ? Monitor performance of network and servers (Microsoft and Linux) to identify potential problems and bottleneck. ? Real time monitoring and network management using Cisco Works LMS and Solarwinds. ? Provided technical support on hardware and software related issues to remote production sites. ? Responsible for LAN and internet connection file and print server. ? Maintained and installed new internet connections for customers. ? Handled installation of Windows NT Server and Windows NT Workstations. ? Handled Tech

Support as it relates to LAN & WAN systems. Skills SECURITY (4 years), SOLUTIONS (4 years), SIEM (4 years), BGP (3 years), CISCO (3 years) Additional Information TECHNICAL SKILLS DLP Websense, Symantec & McAfee End Point Security McAfee Suits (VSE, HIPS & HDLP), McAfee MOVE AV, Symantec IPS/IDS McAfee IPS, , SecureWorks IDS/IPS, SNORT SIEM , Splunk security manager, IBM QRadar, LogRhythm MSS Vulnerability Assessment, Content Filter, Antispam, IDS/IPS Management Vulnerability Management Tools Nessus, Nmap, Nexpose, Wireshark, Fortify Security Tools Splunk , McAfee Vulnerability management solutions, Nessus, Solarwinds, LogRhythm, Platforms/Applications Continuous Monitoring Vulnerability Management, Web Application Scanning, ThreatProtect, Policy Compliance, Cloud Agents, Asset Management, Governance, Risk Management and Compliance, Solarwinds, Nexpose, Rapid7 Event Management RSA Archer, Blue Coat Proxy, Splunk, NTT Security, LogRhythm, PenTest Tools Metasploit, Burpsuit, NMAP, Wireshark and Kali Security Software Nessus, Ethereal, NMap, Metasploit, Snort, RSA Authentication Networking LAN, WAN, Wi-Fi, DNS, WINS, DHCP, TCP/IP, ISCSI, 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 Operating System Windows , Linux, Unix Security Intelligence WhiteHat Web Security, iDefence, NTT Security, LogRhythm SIEM Splunk, Solarwinds, Nitro, IBM QRadar, LogRhythm Switches Cisco Catalyst VSS 1440 / 6513 / 6509 / 4900 / 3750-X / 2960 Routers Cisco Routers ASR 1002 / 7606 / 7304 / 7206 / 3945 / 2951 / 2600

Name: David Lucas

Email: sherriedwards@example.net

Phone: (835)265-3859x4521