IT Compliance Analyst/Information Security Analyst IT Compliance Analyst/Information Security Analyst IT Compliance Analyst/Information Security Analyst - ROSS Stores Inc Jersey City, NJ 6+ years of Experience in designing, architecting, deploying and troubleshooting Network & Security infrastructure through network based intrusion detection system, advance cyber security techniques and firewalls of various vendor equipment Experienced in SIEM tool such as ArcSight to manage security events and big data analytics Installed Connectors and integrated multi-platform devices with ArcSight ESM, developed Flex Connectors using Regex for the ArcSight Unsupported devices / Custom Apps Implementing CISCO NIDS security policies to avoid malicious attacks in the network Create security policies in CISCO NIDS to avoid and detect network intrusions Monitoring the network to avoid intrusions and apply mitigation techniques using NIDS Responsible for applying latest Symantec standards on various platforms (Windows,Unix,Middleware, AIX,etc.) through Symantec control compliance suite tool Implemented FireEye security to avoid malwares and cyber-attacks on the system Hands on experience on FireEye NX,EX,HX, PX,and IA Configured Data leakage and protection policies to prevent data leakage of end client Configured Tenable security center with latest version of Nessus scanner Configuring rules and Maintaining McAfee ePO(AntiVirus) policies for host based protection Troubleshooting on the high severity issues related to McAfee ePO and McAfee end-point products to avoid any business impacts Involved to configured Netflow Integrator tool which converts processes data in Syslog from various networks equipment such as edge routers, switches and firewalls Hands on experience in Splunk to create various application based dashboards Configured and involved to set up architecture several internal tools such as vulnerability tracking reporting tool with including various ETL processes to monitor intrusion events and identify latest vulnerability Work Experience IT Compliance Analyst/Information Security Analyst ROSS Stores Inc - Dublin, CA October 2018 to Present Responsibilities: Responsible of administrative role and duties of cyber security applications like FireEye, Network intrusion detection system, McAfee epolicy orchestrator, Symantec data leakage and protection, ArcSight, Symantec control compliance suite, Netflow integrator Integrated IDS/IPS to ArcSight ESM and analysed the

logs to filter out False positives and add False negatives in to IDS/IPS rule set Responsible for applying standards for each platform (Windows, Unix, Middleware etc.) with application like Symantec Control Compliance Suite Created installation and configuration and test case scenarios documents for each specific device Connectors Configured Nessus Scanner with latest security center version Integrated different devices data to Splunk Environment and also created dashboards and reports in Splunk Monitored and identified any suspicious events using the ArcSight ESM console and raise a ticket Responsible to implement and deploy Symantec DLP, McAfee ePO and NIDS policies to protect organization against latest threats Responsible to monitor traffic status, appliance and server health check to verify functionality Entirely responsible to perform production changes/upgrades via informing to all responsible teams and stakeholders Involve in weekly and monthly meeting with other teams to review and discuss about upcoming production changes and policy modification Versed in PCI-DSS, HIPAA, ISO-27001/ 2, NYSDFS, GDPR, COBIT, CIS Controls, and ABA Cybersecurity compliance regimes. Maintain and responsible to assess compliance score of each network asset in the infrastructure to align with government configuration policy Create Policies, Procedures, Reports, Metrics, and provide network and host-based security to each host within the organization Work under the direction of the Team Leader to maintain security devices and show practical experience in managing SIEM environments, FireEye standalone devices such as NX, EX and HX, NIDS, UNIX servers, and packet capture devices Analyse logs and events from the solution and provide threat analysis reports and Build custom security policies and application signatures Review and ongoing assessment of malware analysis techniques, intrusion detection/intrusion prevention, SIEM, application access control, Antivirus, and other network component policies Configure, implement and maintain all security platforms and their associated software, such as Linux based standalone devices, windows servers, UNIX servers, intrusion detection/intrusion prevention, SIEM Ensure network security best practices are implemented through auditing: database servers, traffic analyser sensors, firewall rules, change control, and monitoring. Configured Intrusion policies, health policies and system policies in for network traffic analysis Worked and configured Netflow

Integrator tool which converts processed data to Syslog from edge routers, switches, firewalls then sends to Splunk Cyber security admin Aujas Network April 2017 to December 2017 IT Security Analyst Responsibilities: Working as a POC (Point of contact) for the devices which Symantec mange for the Clients. Attend the troubleshoot call with Symantec, McAfee and the local DC team to resolve the McAfee IDS and OOB issues Review and configure polices for McAfee agent 4.8, 5.0 Assisting the users with all the related issues in regards to McAfee Agent, VirusScan enterprise Documenting for all the changes and procedure for existing McAfee ePO environment Troubleshooting on the high severity issues related to McAfee ePO and McAfee point products to avoid any business impacts Processing the users/ application owners requests in providing the required exclusions Reviewing the policy exclusions request based on the vendor recommendations Responsible for the end to end policy development and deployment process to confirm the issues are fixed Deploying Agent and VSE package from the ePO console in regards to pushing the latest packages or in process of remediating the non-compliant assets Troubleshooting on the DAT and signature update issues on the endpoints Successfully upgrade ePO sever from 4.6 to 5.1 Actively working with various internal teams in remediating the non-compliant agents on both workstations and servers Ability to assess information of network threats such as scans, computer viruses Documenting all the standard operating procedures which will help the internal team members to assist in mission critical incident Monitoring and setting policies in EPO servers based on applications Working closely with Cyber threat intelligence team to enhance the policies and to mitigate the known risks to the entire environment Performing the reconciliation activities on all the ePO environments as part of AUDIT requirements Implemented Fire Eye security to avoid malwares and cyber-attacks on the system Used Fire Eye for malware detection and prevention in the network Prevention of email based cyber-attacks by providing fully integrated security solution in FireEye Implemented Fire Eye security to avoid malwares and cyber-attacks on the system Mitigating and detecting the advanced cyber-attacks like spear phishing using Fire Eye Creation of the IDS design documents for all the external and internal supporting clients Updating the Latest Signature set in all the Cisco IDS by using Cisco

Security Manager (CSM)Configuration of checkpoint firewall mainly IPS (Intrusion Prevention System) module according to client topology and checkpoint MDS Implementing CISCO NIDS to add security policies to avoid electronic attacks on the system Monitoring the network to avoid intrusions and apply mitigation techniques using NIDS Creating security policies in CISCO NIDS to avoid and detect network intrusions Experience on Endpoint security SME with McAfee Endpoint Analyse security landscape and technologies to ensure data protection Worked on McAfee ESM (Enterprise Security Manager) & IPS appliance which handled both SIEM/Correlation and Log Management Extensively used Security Information Management (SIEM) solutions for security event correlation, risk analysis and incident response Network Security Engineer IBM May 2016 to April 2017 Responsibilities: Configured, implemented and troubleshooting issues on Checkpoint R77.10 Gaia, R75, Cisco ASA 5540 and Palo Alto firewalls for the client environment Involved in implementing malware protection, policy control, analysing logs and different reports using Palo Alto PA-5020 Configured Cisco ASA and Checkpoint firewall layers securing existing Data Centre infrastructure Managed corporate Checkpoint Firewall management and operation and implementing security rules and mitigating network attacks Configuring rules and Maintaining Checkpoint Firewalls & Analysis of firewall logs using various tools Deployed and configured network based Cisco IDS/IPS v5 Provide 24*7 supports for day to day global operational activities including Change Implementation, Handling Work order access Request, High Priority incident handling/troubleshooting for Security Devices Exposure to wild fire advance malware detection using IPS feature of Palo Alto Configuring rules and Maintaining Palo Alto Firewalls with IPS module & Analysis of firewall logs Implementation of analysis, optimization, troubleshooting and documentation of LAN/WAN networking systems Modified internal infrastructure by adding switches to support server farms and added servers to existing DMZ environments to support new and existing application platforms Worked extensively in Configuring, Monitoring and Troubleshooting Cisco's ASA 5500/PIX security appliance Plan Design and assist in deploying enterprise wide Network Security and High Availability Solutions for ASA Installation & configuration of Cisco VPN concentrator 3060 for VPN tunnel with Cisco VPN hardware & software

client and PIX firewall Experience with implementing and maintaining network monitoring systems (Cisco works and HP Open view) and experience with developing complex network design documentation and presentations using VISIO Identify, troubleshoot, and resolve LAN/WAN network problems (DNS, DHCP, TCP/IP and a variety of hardware and other networking issues) Designed and implemented complex routed and switched LAN and WAN using Ethernet Technology

Used Network monitoring tools to ensure network connectivity and Protocol analysis tools to assess and pinpoint networking issues causing service disruption Network Engineer Wipro April 2015 to April 2016 Responsibilities: Configured and troubleshoot firewalls like PIX 520, ASA 5510, 5520 and FortiGate 420D through CLI and GUI. Also, VLAN management, port security and basic configuration of Access- list, NAT and Static routes. Work with tools such as FireEye, Damballa, Guardium, CyberArk, CyberArk Privileged Threat Analytics, SEP, Palo Alto, Checkpoint, Cisco ASA, F5 ASM, Imperva WAF, LanCope Stealth Watch, Brightmail, IronPort, Blue Coat Implemented and troubleshooting the Virtual firewalls (Contexts) solutions in ASA Responsible for installation, troubleshooting of firewalls (Cisco firewalls, Checkpoint R70 firewalls and Juniper firewalls,) and related software, and LAN/WAN protocols. Troubleshooting the VPN tunnels by analyzing the debug logs and packet captures Configuring failover for redundancy purposes for the security devices. Implemented the stateful & serial failover for PIX/ASA firewalls, Checkpoint Clustering and load balancing features. Responsible for implementing Data Center Security best practice, audit and compliance (PCI/SOX/DOD) requirements. Used F5 BIG-IP Local Traffic Manager (LTM) and provided a flexible, high-performance application delivery system to increases operational efficiency and ensures peak network performance for critical business applications. Automation of security operations and optimizing the usage of infrastructure. Responsible for managing Network & Security Engineering implementation that architect, design, builds, manages and supports Network and Security Infrastructure and Data Centres. Maintain the periodical software update on security devices depends upon the bugs fixed with the new software releases. Network Engineer April 2014 to October 2014 Responsibilities: Handled L1 network issues: VLAN management, port security, host machines LAN connectivity and monitoring of routers and

switches. Worked on Active Directory, DNS, DHCP, and Group Policy. Managed LAN connectivity issues and troubleshoot WAN routers like 2800/3800 series of local and remote sites. Installed NT server 4.0/2000 on NTFS partition with DHCP/DNS&WINS Creation of user accounts for authentication with rights to files & folders. Installing & configuring Microsoft TCP/IP Installing & configuring Remote Access Server (RAS) Installing Backup Domain Controller (BDC) to provide for PDC failure. Installations & troubleshooting of windows 95/98 & NT workstation 4.0 Clients logging onto NT server. Installation & troubleshooting of network printers Create & manage partitions Define a custom subnet mask & define a range of valid IP addresses. Installation of IIS 4.0 on server and loading appropriate files and folders, for the intranet website. Monitoring of website performance and in charge of backups. IT Security Specialist February 2013 to March 2014 Responsibilities: Executed hardware installation and testing Upgraded operating system and maintenance Managed physical security Helped in hardware troubleshooting Managed access for various role Implemented different patches on different systems 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 Education Bachelor's Skills credit, Powerpoint, Sales, Microsoft Office, Typing Additional Information Technical Skills FireEye: CMS, NX, EX, HX, IA, PX Network intrusion detection system: Cisco FMC1500, FMC2000, FMC3500 Symantec data leakage and protection: endpoint protection, web protection, network protection SIEM: ArcSight console 6.5 Security compliance tool: Symantec control compliance suite 11.1 Packet capture: Netflow integrator Network security: Cisco NIDS, IPS Antivirus: McAfee ePO 5.1 Vulnerability analysis: Tenable

Name: Amber Oliver

Email: andre62@example.com

Phone: 211.522.4992x13846