Security Consultant Security Consultant Security Consultant Pasadena, CA ? 6+ years of Information security experience on Security information and Event management (SIEM), Implementation, Operation Support, Vulnerability assessment, Development and implementation of IT processes aligned with business objectives for effective security management. ? 5+ years of extensive experience in Security information and Event management (SIEM) tools like ArcSight, Splunk, RSA Envision and QRadar. ? Experience working in Banking, Financial, Energy, Retail domain. ? Extensively worked on development and configuration of SIEM connectors for unsupported devices by ArcSight, Splunk and Qradar. ? Manage incidents for visibility, transparency and communication. ? Developed enerprise-wide Application Security Standards. ? Having extensive knowledge on regulatory compliance procedures related to SOX, PCI and HIPPA. ? Adept in conceptualizing, analyzing software system needs, evaluating end-user requirements, custom designing solutions & troubleshooting for complex software systems. ? Configured direct alerts and correlated alerts based on the devices in the client's network. ? Strategic Planning Framework to gauge an organization's current Info Sec maturity level and create roadmap for the future using COBIT 4.1&ISO 27000 standards ? Implemented Operating Systems, Applications, Users and Data migration projects ? Performed Proof of concept with Splunk, Tripwire, Qualys and RSA Envision tools ? Spearheaded ISO 9000 and driven system and policies for Customer Support division ? Developed tools and performed Risk Assessment on Network, Application, and Physical Security ? Have worked on security incidents as part of Incident Response towards forensic investgation. ? Prepare daily reports and security advisory for customer devices. ? Have Worked on Health monitoring of ArcSight database and manger. ? Work closely with other teams and third party vendors to conclude on the incidents. Authorized to work in the US for any employer Work Experience Security Consultant Greendot Corp December 2015 to August 2017 Environment: Hp ArcSight, Qualys, Splunk, IBM Guardium, RSA Envision, Windows, Linux Roles & Responsibilities: ? Administrated ArcSight components like ESM, Logger and collector appliances, ArcSight Management centre ? Identifed the unwanted users that are existing on ESM for report generation and removing those users from ESM reducing the overhead on ESM. ? Identifying the broken

resources and fixing the broken resources to make sure events are parsed and correlated for the rules to identify the true and false positives. ? Migrated the entire Legacy old logger and and collector appliances to latest appliances of loggers and collector appliances to balance the load, for retention purpose on loggers. ? Created the inventory for all the collector appliances by identifying the smart connectors and flex connectors inorder to migrate. ? Installed the smart connectors and also flex connectors so that events are parsed and sent to the ESM ? Configured most of the device logs into the ArcSight environment for monitoring ? Made the ArcSight environment simplified by reducing the number of legacy collector appliances and loggers. ? Administrated QRadar components like Console, Event Processors, Flow processors, Event Collectors, Flow collectors to NYPA Environment for Log collection and monitoring. ? Integrate Infrastructure devices and Securiy devices and also applications to QRadar SIEM. ? Integrated RSA and EMC solutions say Access manager, Authentication manager Symmetrix and made some recommendations for system and process improvement. ? Responsible for Configuration aligned to internal PCI and SOX controls by using RSA Envision. ? Involved in creating dashboards using RSA Security Analytics to improve the ability to spot the malicious activity. ? Responsible for transfer of log data to RSA Envision by collecting regular activities of source devices. ? Recommended and configure Correlation rules and reports and dashboards in QRadar Environment. ? Successful Integration of Palo AltoFirewall with the Panorama and Skybox, and implementation experience on Check PointFirewalls. ? Configure Network Hierarchy and Back up Rention configuration in QRadar SIEM. ? Extract customized Property value using the Regex for devices which are not properly parsed by QRadar DSM. ? Extract the logs, Perform real time log analysis using SIEM technologies and Forensics Analysis of logs as per the request. ? Performed scans on critical systems in the network for potential vulnerabilities using NMAP and Nessus. ? Responsible for planning and scheduling Nessus vulnerability scanning to run on regular intervals and on ad-hoc basis. ? Enhancement and fine tuning of Correlation rules on QRadar based on daily monitoring of logs. ? Recommended and Configure Daily and weekly and monthly reports in QRadar based on Compliance requirements. Security analyst Citizens Bank, Rhode Ishland December 2013 to December 2015 Environment:

RSA Envision, Windows Roles & Responsibilities: ? Integration and testing of multi-platform devices with RSA Envision. ? Configuring and testing of log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases and applications through the collectors (LC, RC). ? Categorize and test the messages generated by security and networking devices into the multi-dimensional RSA Envision schema. ? Integration of IDS/IPS to RSA Envision and analyse the logs to filter out False positives and add False negatives in to IDS/IPS rule set. ? Develop and testing of content for RSA Envision like correlation rules, dashboards, reports and filters, list. ? Debugging the issues which are related to RSA Envision performance, reporting, collection of logs from various devices. ? Develop and test UDS Connectors via XML for the RSA Envision un supported devices and Business applications. ? Attending weekly client meetings in that need to discuss about on boarding and content testing results status. ? Created installation and configuration and test case scenarios documents for each specific device Connectors. ? Recommended security strategies based on real time threats. ? Analyzed the Critical Infrastructure Protection (CIP) reliability standards of the North American Electric Reliability Corporation (NERC) to identify types of documentation needed for compliance. ? Analyzed evidence and documentation to evaluate compliance with the NERC CIP reliability standards. Security Engineer Land'sEnd, Wisconsin December 2012 to December 2013 Environment: ArcSight SIEM, Windows, Linux, Splunk, Qualys Scanner, Tcpdump, NMAP Roles &Responsibilities: ? Installation of Connectors and Integration of multi-platform devices with ArcSight ESM. ? Configuring log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases and apps. ? Integration of IDS/IPS to ArcSight and analyse the logs to filter out False positives and add False negatives in to IDS/IPS rule set. ? Categorize the messages generated by security and networking devices into the multi-dimensional ArcSight normalization schema. ? Creating alerts and reports as per business requirements and Threat modelling with specific security control requirements. ? Develop content for ArcSight like correlation rules, dashboards, reports and filters, Active lists and Session list. ? Created ArcSight asset modelling, it is used to populate asset properties in

Correlation rules and reports. ? Troubleshooting the issues which are related to Arc sight, logger and Conapps performances. ? Develop Flex Connectors for the ArcSight UN supported devices and Business apps. ? Configured 1200+ devices to ArcSight ESM for monitoring. ? Integration of different business data to Splunk Environment and also created dashboards and reports in Splunk. ? Created Vulnerability Assessment report detailing exposures that were identified, rate the severity of the system & suggestions to mitigate any exposures & testing known vulnerabilities. ? Performed scans on critical systems in the network for potential vulnerabilities using NMAP and Qualys. ? Responsible for planning and scheduling Qualys vulnerability scanning to run on regular intervals and on ad-hoc basis. ? Created installation and configuration documents for each specific device Connectors. ? Recommended security strategies based on real time threats. ? Have been a part of incident response team while investigating the logs using forensics. IT Infrastructure Engineer Systel Communications Pvt Ltd May 2010 to May 2012 Environment: Windows, Linux, LAN, WAN, Antivirus Responsibilities ? Install and troubleshoot operating systems - Windows 2000, XP, and Win7. ? Install, upgrade and troubleshoot MS-Office 2000, 2003, 2007. ? Installation and maintenance of Antivirus Symantec and McAfee. ? Responsible for data backup on weekly and monthly schedule. ? Configuring & Handling Outlook, Outlook Express and Data Backups. ? Implementing & troubleshooting network access LAN, WAN and Wi-Fi. ? Provide tier 2 remote support for all network & application related issues across the board. ? LAN/WAN design, implementation and optimization using Cisco routers and switches ? Installing, Configuring of Networking Equipment's: Routers and Switches ? Recommend and scheduling repairs to the LAN/WAN. ? Managing VLANs and inter VLAN routing. ? Configured VPN, ACL, and NAT in the Cisco ASA 5540 firewall to allow only authorized users to access the servers of the internal network ? Used Layer 3 protocols like EIGRP and BGP to configure Routers in the network ? Configure and Implement Remote Access Solution: IPSEC VPN, Remote Access ? Upgrade, install and troubleshooting networks, networking hardware devices and software. ? Involved in patch management and installation of critical systems. Skills LINUX (4 years), SECURITY (4 years), RSA (3 years), NMAP (2 years), QUALYS (2 years) Additional Information Operating Systems Microsoft:

Windows Server 2003/Server 2008; Linux: CentOS, Red Hat, Fedora, Ubuntu Server/Desktop, Web Technologies HTML, JavaScript, Microsoft.Net, Java OWASP/SANS Vulnerability XSS, SQL Injection, CSRF, Security Misconfiguration, Sensitive Data Exposure, Insecure Direct Object Reference SIEM Tools IBM QRadar,ArcSight,Splunk,RSA Envision Security Tools Qualys, Nessus, IBM AppScan, Wireshark, Snort, Tcpdump, Nmap Protocols Ethernet, LAN/WAN/MAN, TCP/IP, DNS, DHCP, FTP, TELNET, SMTP, POP3, SSH, UDP, ICMP, IPsec, HTTP/HTTPS, Database Activity Monitoring IBM InfoSphere Guardium

Name: April Coleman

Email: washingtonmorgan@example.net

Phone: 3445288950