Security Analyst Security Analyst Security Analyst - Archer Daniel Midlands Chicago, IL 8+ years of Information security experience on Network Security Integrations, 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 different Security Roles, Security information and Event management (SIEM) tools like ArcSight, Splunk, 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. Experience in performing detailed technical network security evaluations and recommendations via vulnerability Management. 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. Have worked on security incidents as part of Incident Response towards forensic investgation. Authorized to work in the US for any employer Work Experience Security Analyst Archer Daniel Midlands - Decatur, IL December 2018 to Present Environment: HP Arcsight , Windows,Linux ,Cloud app Security, Cofense,Symantec ATP Roles & Responsibilities: Created effective rules in SIEM ArcSight tool to capture real threat events and fine-tuned to avoid false positive alerts. Assisted with incident management response and analysis as a member of the computer security monitoring and incident response team providing analysis for the full scope and lifecycle of incident response. Real-Time Log monitoring in the Security Operations Centre from different devices Monitoring network traffic for security events and perform triage analysis to identify security incidents. Document track and escalate cyber- security incidents and respond to cyber incidents as defined in Handling procedures and local SOP Analyze Threat Patterns on various security devices and Validation of False/True positive Security Incidents. Regularly making recommendations to tune alert logic and reduce false positives. Cyber security training with other team members to promote security and operational awareness. Performed initial analysis and investigations into alerts as they are seen including anti-virus and phishing alerts

Respond to incidence of various types from malware incidents, website compromise, business

email compromise, phishing, credential harvesting to intrusions of various sorts Respond to phishing attempts and block emails or domains involved in these phishing attempts. Coordinate with users and scan systems targeted by phishing emails to eradicate the potential of any malware infection. Develop content for Arcsight like correlation rules, dashboards, reports and filters, Active lists and Session list. Correlation rules are created by making use of conditional logic, aggregation that is used to match the particular field for the required time frame. Rules are created using variables (Local, global) as and when required based on the necessity from the actions tab where variables are declared and made use inside the rule condition. Created the standards rules, light weight rules, pre persistent rules in arcsight in order for them to correlate and trigger the alerts Active lists and session lists have been created and made use to create the rules as and when needed. Security Administrator HCSC (Blue Cross Blue Shield) May 2017 to November 2018 Environment: Hp Arcsight, Advizor reporting tool, Splunk, Windows, Linux Roles & Responsibilities: Administrated Arcsight components like ESM, Logger appliances and collector appliances, Arcsight Management centre (ArcMc), Arcsight VM connectors Upgradation of arcsight ESM from 6.9 to 6.11 version has been performed after Linux OS has been upgraded to 6.8 RHEL. Arcsight Health monitoring has been performed by Monitoring the alerts, dashboards, reports for any SIEM health related issues that are found on ESM. Troubleshooted all he Hardware issues in case of appliances and software issues on VMs, worked with the vendor to resolve both the software and hardware issues. Troubleshooted the Anamoli threat stream Optilink software that runs on Arcsight connector that provides the threat fee data from Anamoli. Identified the storage and capacity levels and worked with the storage teams towards increment of space as per the requirment. Ensured that the SIEM is receiving the logs from the configured log sources from all the enviroments and are reporting to ESM Troubleshooted the log sources and the intermediate device specific issues, any threat feed issues with the vendor Anamoli Installed the smart connectors and flex connectors, modification of flex connector like parser, mapping, categorization etc, deployed the modified flex connectors in Production. Identified and Troubleshooted the connectors that are not being reported on ESM Creation of Dashboards,

alerts/Notifications, reports, co-relation rules etc has been done. Upgraded the SIEM components, applied the patches, Migrated the connectors to lesser utilized hardware for better performance. User account management has been performed like creation, modification and deletion of accounts on Arcsight ESM. Adminstrated the Security event visualization tool (Advizor) that would gather all the security relevant data on the front end, Monitored all the Advizor analyst and server components thats integrated to splunk via estreamer, performed all the upgrades on Advizor as per the Vendor instructions Security Consultant CVS Retail, Rhode Island January 2017 to April 2017 Environment: Hp Arcsight, Qualys, Splunk, IBM Guardium, Windows, Linux Roles & Responsibilities: Administrated Arcsight components like ESM, Logger and collector appliances, Arcsight Management centre (ArcMc). Migration of arcsight ESM from 6.0 to 6.9 version by exporting the packages and import into the 6.9 version 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 all the 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 loggers appliances with devicename and device vendors for the process of migration 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 Created the rules,filters,active lists, session lists, Dashboards and reports Configured 1800+ Devices into the arcsight environment for monitoring Made the arcsight environment simplified by reducing the number of legacy collector appliances and loggers. Security Consultant New York Power Authority, NY November 2015 to December 2016 Environment: QRadar, Tenable Nessus, Windows, Linux .Roles & Responsibilities: 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. Integrate Security Center Vulnerability

scanner to QRadar to populate vulnerability information to associate internal assets. Recommended and configure Correlation rules and reports and dashboards in QRadar Environment. 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 Monitoring of day to day system health check-up, event and flow data backup, and system configuration backup. 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 Nessus. Responsible for planning and scheduling Nessus vulnerability scanning to run on regular intervals and on ad-hoc basis. Analysis of Offenses created based on different device types of logs via Correlation rules. 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 Consultant Ameriprise Financial, Minneapolis January 2015 to October 2015 Environment: HP ArcSight SIEM, Splunk, Windows, Linux, Qualys Scanner, Wireshark, tcpdump, NMAP Roles & Responsibilities: Administrated Arcsight ESM, Connectors and Logger. Configuring log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases and apps. Categorize the messages generated by security and networking devices into the multi-dimensional Arcsight normalization schema. Installation of Connectors and Integration of multi-platform devices with Arcsight ESM, Develop Flex Connectors for the Arcsight Unsupported devices / Custom Apps Develop content for Arcsight like correlation rules, dashboards, reports and filters, Active lists and Session list. Creating alerts and reports as per business requirements and Threat modelling with specific security control requirements. Arcsight asset modelling implementation, it is used to populate asset properties in Correlation rules and reports. We on-boarded 1000+ devices to Arcsight ESM for monitoring. Integration of IDS/IPS to Arcsight and analyse the logs to filter out False positives and add True

Positives in to IDS/IPS rule set. Integration of different devices data to Splunk Environment and also created dashboards and reports in Splunk. Troubleshooting the issues which are related to Arcsight ESM, logger, Conapps performances. Collect network traces on system memory capture, process, activity data, and forensic disk images by using incident response forensics 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. Responsible in reporting the vulnerability assessment result to management, development and operations team. Performed port scanning on servers using NMAP and closed all unnecessary ports. Used Wireshark/tcpdump to capture live data packets from the network traffic and analyzed the same for any security flaws. Follow up and ensure the closure of the raised vulnerabilities by revalidating and ensuring closure. Leading operational activity including Log Analysis and Troubleshooting. Security Engineer Target Security Operation center, Minneapolis May 2013 to October 2014 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. Security analyst US Bank Security Operation Center February 2012 to April 2013 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. IT Infrastructure Engineer Apollo Hospitals Enterprise, Ltd December 2009 to January 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. Handling Norton Ghost for deploying OS to multiple PC's. Implementing & troubleshooting network access LAN, WAN and Wi-Fi. Provide tier 2 remote support for all network & application related issues across the board. Writing and keeping technical documentation up to date 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. Develop and documenting system standards for system and network devices. Involved in patch management and installation of critical systems. Education Bachelor's 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,Nexpose,IBM AppScan, Wireshark, Snort, Tcpdump, Nmap, Anamoli, Advizor, Threat StreamS,TTrend Micro, WAF 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 Firewalls PaloAlto, Cisco ASA,Cisco NGFW, IDS,IPS

Name: Sean Morrison

Email: corteztroy@example.org

Phone: 001-769-895-7508x6894