Senior SOC Analyst Senior SOC Analyst Senior SOC Analyst - Verizon Austin, TX Over 6.5+ years of experience, in field of SIEM Information Security with expertise in Implementation and Operation phases of the project. Work profile includes END to END planning & Implementation of Various Network Devices and Business Application with the SIEM Device -QRadar/Splunk Expert level understanding of SIEM Implementation & its Integration with other N/W devices and Applications and the troubleshooting work. Real Time Log monitoring in the Security Operations Centre from different devices such as Firewalls, IDS, IPS, Operating Systems like Windows, UNIX, Proxy Servers, Windows Servers, System Application, Databases, Web Servers and Networking Devices. Analyze Threat Patterns on various security devices and Validation of False/True positive Security Incidents. Expert Understanding to develop the complex Use Cases, Universal device support Modules on the QRadar SIEM and Splunk Expert level knowledge on creating the UDSM parser for the logs normalization in the SIEM tool. Expertise in customizing Splunk for Monitoring, Application Management and Security as per customer requirements and industry best practice. Headed Proof-of-Concepts (POC) on Splunk ES implementation, mentored and guided other team members on Understanding the use case of Splunk. Expertise in customizing Splunk for Monitoring, Application Management and Security as per customer requirements and industry best practice. Expertise in Installation, Configuration, Migration, Trouble-Shooting and Maintenance of Splunk, Passionate about Machine data and operational Intelligence. Knowledge in Authentication, End Point Security, Internet Policy Enforcement, Firewalls, Database Activity Monitoring (DAM), Data Loss Prevention (DLP), Identity and Access Management (IAM) solutions Hands on experience with Change Management working on the incidents and Change Request and coordinating with the APP teams during the cutovers. Experience in planning, developing, implementing, monitoring and updating security programs, and advanced technical information security solutions, and sound knowledge in SOX and PCI compliance requirements and understanding of NIST and ISO standards. Maintain QRadar components like Console, Event Processors, Flow processors, Event Collectors, Flow collectors for Log collection and monitoring. Integrate the devices like Juniper Network Secure Access, Aruba Mobility Controllers, Bluecoat, Fire

Eye, ISS site protector, Checkpoint, Palo Alto, Source fire, VMware Vcenter, Symantec End Point, AD servers with QRadar SIEM. Integrate Qualys guard scanner to QRadarto populate vulnerability information to associate internal assets. Provide expert analysis of events discovered by Junior Analysts Ensuring SLA adherence; follow up with the asset owners and ensure that the call raised is closed on time. Develop Operational processes and procedures to appropriately analyze, escalate, and assist in remediation of critical information security incidents. 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. Implemented workflow actions to drive troubleshooting across multiple event types in Splunk Monitoring of day to day system health check-up, event and flow data backup, system configuration backup. Analysis of Offenses created based on different device types of logs via Correlation rules. Integrate different feeds to Splunk Environment. Enhancement and fine tuning of Correlation rules on QRadarbased on daily monitoring of logs. Integration of different devices data to Splunk Environment and also created dashboards and reports in Splunk. Recommended and Configure Daily and weekly and monthly reports in Qradar and Splunk based on Compliance requirements.
A thorough understanding of the Software Development Life cycle (SDLC) including various concepts such as Requirement Gathering, Experience in the development of Client-Server and Web-Based Application Work Experience Senior SOC Analyst Verizon - Austin, TX September 2018 to Present Responsibilities: Initial set-up, installation and implementation of new SIEM solution (QRadar). Migrating existing Reports and Alerts from RSA envision to QRadar. Aggregate, correlate, and analyze log data from network devices, security devices and other key assets using QRadar. Created SIEM dashboard for QRadar and reconciliation with Storage, Database Server, Workstation and Server and Network Devices. Deploy new ESM, Loggers, SmartConnectors / FlexConnectors as required to collect data feeds Assist in the proper operation and performance of QRadar ESM, Loggers and connector Provide ad-hoc training to analysts focusing on specific client missions, including generic QRadar training sessions and Custom Use Case training sessions

Evaluate relative QRadar product advancements and provide recommendations to the customer Identifies security risks, threats and vulnerabilities of networks, systems, applications and new technology initiatives Provides technical support in the development, testing and operation of firewalls, intrusion detection systems, and enterprise anti-virus and software deployment tools Knowledge in Authentication, End Point Security, Internet Policy Enforcement, Firewalls, Database Activity Monitoring (DAM), Data Loss Prevention (DLP), Identity and Access Management (IAM) solutions Hands on experience with Change Management working on the incidents and Change Request and coordinating with the APP teams during the cutovers. Experience in planning, developing, implementing, monitoring and updating security programs, and advanced technical information security solutions, and sound knowledge in SOX and PCI compliance requirements and understanding of NIST and ISO standards. Responsible for performing administrator duties for IBM Infosphere Guardium (V9.x, V10.x) on more than 130 appliances. This includes building and configuring new appliances as well as migration of V9.x appliances to V10.x. Develop strategic plans for agency-wide implementation to address the operations of client services, product support, quality assurance, and information security training. Administers Guardium to detect threat vectors, vulnerabilities, and access to confidential data that may pose potential breach to Scripps data assets. Monitors internal access to data assets to determine potential theft. Automate the manual jobs using automation clients or the jump server by shell scripting the Guardium Installations Manager using HPSA Conducts complex security architecture analysis to evaluate and mitigate issues Develops implements, enforces and communicates security policies and/or plans for data, software applications, hardware and telecommunications Assist multiple security projects with the goal of exceeding compliance objectives. Responsible for maintenance, administration and configuration of the log aggregation solution. Along with creating custom views, reporting and automated alerting for both operational and security use using QRadar. Assisted with management and tuning of our perimeter Intrusion Prevention Solution. Network traffic visualization to facilitate monitoring and trending analysis. Responsible for maintaining availability, reporting and communication of the SIEM between it, its event-sources and the endpoints.

Responsible for the creation of the logic to correlate attacks across multiple event sources and attempt to make a determination of the possible outcome. Implemented forwarder configuration, search heads and indexing on splunk. Created Dashboards, report, scheduled searches and alerts, SIEM searches and alerts Metrics Identify threats through log analysis and perform risk mitigation. Log Source Configuration (Supported DSMs and Unsupported DSMs using scripts). System performance and health monitoring ofQRadar (Created a SIEM Webpage using VBScript on IIS Server). Monitored events, responded to incidents and reported findings. Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools. EPS and Utilization monitoring ofQRadar Develop comprehensive security event reports to address current and potential security concerns and meet Audit Requirements. Experience with programming languages; or scripting languages such as Shell and Python Experience in handling clients reported cyber-attacks and incidents. Security Analyst Capital One - Tampa, FL January 2018 to August 2018 Responsibilities: Participated in the product selection and installation of QRadar Security Information Event Manager SIEM consisting of multiple collectors and a high-performance MS SQL database Designed and implemented enterprise SIEM systems: centralized logging, NIDS, alerting and monitoring, compliance reporting, based on QRadar 7.0 SIEM. Responsible for QRadar SIEM monitoring and configuration aligned to internal PCI and SOX controls Manage the day-to-day log collection activities of source devices that send log data to SIEM QRadar Managed and monitored McAfee EPO 4.6. Installed Linux/Windows agents and VirusScan Enterprise Recommended WebSense Internet proxy and Web Security Gateway Anywhere to manage corporate Internet proxy traffic and supporting infrastructure Access control for browsing, Authentication for all hits from browsing on proxy servers, maintenance of proxy logs for forensic purpose Maintain McAfee antivirus applications and appliance, including ePolicy Orchestrator, VSE 8 and 8.5, and Secure Content Manager SCM 3200 SPAM, Virus, and content filtering of web and email traffic. Develop Knowledge base of various challenges faced in implementing SIEM solution and maintaining it. Dashboard / Enterprise dashboard customization for various team

based on the log source type requirements. Maintain and enforce Log Retention Policies. Developed process to store and forward log data to IBM Big Insights for forensic analysis. Identify current product management issues and developed best practices process to efficiently manage the Security Information and Management tool. Developed internal Change Configuration Management for SIEM. Cleaning up log sources auto-discovered in QRadar by identifying duplicates, correcting mis-identified log sources, and identifying log sources from their logs. Expertise in Universal Device Support (UDSM) Development for unsupported log sources. Customization of existing Device XML and also Creating New Device. IT Security Analyst Walmart - Bentonville, AR September 2016 to December 2017 Design, implementation, management, and investigations using a variety of information security products including Imperva WAF, Imperva Database Activity Monitoring, Splunk, QRadar SIEM, Websense web proxies,Websense email proxies, Websense Data Security (DLP), ANUE aggregation switches, and Big Fix Endpoint Manager. Investigations of incidents generated through various security technologies including Imperva WAF and DAM, Snort IDS, Splunk, QRadar SIEM, and Websense. Managed these technologies through planning, development, and implementation. Monitored file integrity and system changes using NNT. Configuration, troubleshooting, and management of Websense Web proxies. Configuration, troubleshooting, and management of Websense Email proxies. Configuration, troubleshooting, and management of Websense Data Security (DLP). Ensured compliance with PCI audit controls and support audit activities. Design, implementation, and management of a variety of information security products including RSA envision, RSA DLP, Cisco IronPort WSA, Cisco IronPort ESA, Cisco ASA firewalls, and HP Tipping Point IPS. Expertise with network security management functions, protocols and standards. Proficient in typical IT infrastructure technologies. Proficient with Cisco ASA firewalls. Expertise with network-based and host-based IPS/IDS (McAfee, HP Tipping Point, Juniper) Expertise in McAfee and RSA DLP (Data Loss Prevention). Expertise in Q1, SolarWinds, and RSA SIEM (System Information and Event Management). Expertise with web content filtering products (Cisco IronPort). Expertise with virtual server technology (VMWare, ESXi, VSphere). Proficient with Linux, UNIX. Expertise

with Microsoft Windows servers and desktops. Complete understanding of escalation, incident management and change management processes and procedures. Understand network performance analysis and capacity planning best practices. Thorough understanding of performance impact of network security configuration options. Able to provide technical leadership to less experienced personnel either individually or as part of a team. Information Security Analyst CipherCloud Hyderabad January 2015 to August 2016 Working in Security Incident and Event Monitoring SIEM platform - RSA Envision. Security Incident raises according to the alerts and follow-up. Monitoring various event sources for possible intrusion and determine the severity of threat. Hauling Ad hoc report for various event sources and, customized reports, and scheduled reports as per requirements. Collecting the logs of all the network devices and analyze the logs to find the suspicious activities. Monitor RSA envision dashboards to keep track of real time security events, health of SIEM devices. Investigate the security logs, mitigation strategies and Responsible for preparing Generic Security incident report. Hands on Experience with RSA envision centralized IPDB. Analyze the Malware through static and Dynamic analysis with tools. Skills Qualys, Snort, Splunk, Ssl, Vpn, Wireshark, Dns, Security, Websense, Cisco, Netcool, Networking, Tcp/ip, Bsd, Linux, Red hat, Shell scripts, Unix, Unix shell, Unix/linux Additional Information TECHNICAL SKILLS: Splunk Splunk 5.x and 6.x, Splunk Enterprise, Splunk on Splunk, Splunk DB 2 Connect, Splunk Cloud, Hunk, Splunk IT Service Intelligence, Splunk Web Framework Operating Systems Windows 2000, XP, Win 10, Windows Server, Unix/Linux (Red Hat), Free BSD Security / Vulnerability Tools Snort, Wireshark, Websense, Bluecoat, Palo Alto, Checkpoint Symantec,Qualys Vulnerability Manager, FireEye HX, Sophos, Sourcefire RDBMS Oracle 11g/10g/9i/8i, MS-SQL Server 2000/2005/2008, Sybase, DB2 MS Access, Mysql Networking Protocols and Tools TCP/IP, HTTP/HTTPS, SSH, SSL, DNS, SNMP Routers, Switches, Load Balancers, Cisco VPN, MS- Direct Access, Programming Language C, C++, Java with Big Data, Python, UNIX shell scripts Monitoring Tool Netcool,Dynatrace,tealeaf

Name: Joshua Pierce

Email: jacquelinemurray@example.com

Phone: 7078345857