Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst Tampa, FL Authorized to work in the US for any employer Work Experience Cyber Security Analyst NextEra, Plam Beach, FL October 2015 to May 2017 Working in Security Incident and Event Monitoring SIEM platform - IBM Qradar, McAfee ESM, and Splunk. Responsible for design and development of multiple security operations in SIEM and endpoint protection and data protection. Experience in IBM Qradar SIEM Integration. Experience in integrating the log sources with IBM Qradar. Creating Reports based on log sources integrated with Qradar for the Customer requirement. Experience in SIEM devices health monitoring and capacity management. Experience in developing & Fine-tuning SIEM rule alerts and reports. knowledge in creating, developing, and documenting SIEM implementation. worked with Qradar and having knowledge on investigations, building and tuning content. involved in operational expansion and tuning of developed systems as necessary. Technical expertise with security infrastructure architecture design and management. troubleshooting the log collection from networking devices, operating system, databases, security applications and more. knowledge in Rapid7 Vulnerability intelligence. Creating Vulnerability Assessment dashboard using Rapid7 that aggregates data across multiple services to identify critical threats and proactively mitigate risks. Consulted with Rapid7 in performing testing, targeting all assets along with social engineering. Developing processes and procedures around security event management. Performing investigation, analysis, reporting and escalations of security events from multiple sources including events like intrusion detection, Firewall logs, Proxy Logs, Web servers. Implementation and Integration of Servers (Windows, Linux and Unix), Security devices like Firewall, IPS, IDS, WAF, Nessus, McAfee Proxy, Symantec Endpoint Protection). Assist with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions. Experience in Information Security Platform by providing support on known/ unknown vulnerabilities/ threats found via security devices/ product. Experience in developing & creating SIEM Procedures (SOP) documentation. Network Security (IDS/IPS, N/W Sniffing, Wireshark, TCPDUMP, NMAP). Running vulnerability & compliance scan and report vulnerabilities mitigate risks associated with vulnerabilities reported. Expertise in windows server

administration along with windows architecture design. Worked on OWASP TOP 10 attacks like, XSS, SQL Injection, CSRF, PHP Injection etc. Interaction with customer regarding security alerts and attacks. Worked on DDOS mitigation and have good idea on different kind flood attacks. Experience in performing digital forensics and incident response using tools such as Mandiant Intelligent Response, FireEye Redline, Encase or other enterprise tools. Report/Track the vulnerability reports periodically and submit the report to management. Experience in Vulnerability management, implementing, executing, and monitoring vulnerability scans using Nessus, OpenVAS, and other vulnerability tools. Technical expertise in vulnerability assessment including vulnerability scanning and penetration testing with clear reporting, threat identification and action plans for remediation. Writing Snort Signatures, Tripwire (HIDS), and OSSEC (HIDS), Vulnerability assessment using NESSUS. IT Security Analyst, Hasting Mutual, Hasting, MI February 2014 to October 2015 working in Security Incident and Event Monitoring SIEM platform - RSA Envision. Monitor RSA envision dashboards to keep track of real time security events, health of SIEM devices. Hands on Experience with RSA envision centralized IPDB. Collecting the logs of all the network devices and analyse the logs to find the suspicious activities. Investigate the security logs, mitigation strategies and Responsible for preparing Generic Security incident report. 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. Analyse the Malware through static and Dynamic analysis with tools. Generating malware behavioural analysis report. Knowledge in analysing, detecting, preventing malware with security analysis tools and compliance tools. Experience with large enterprise environment and possesses both deep and wide expertise. Working knowledge of privileged account management with in large enterprise environment. Responsible to preparing the Root cause analysis reports based on the analysis. Responsible for maintaining McAfee IDS/IPS policies. Knowledge in Websense, NIPS, Symantec Antivirus, Checkpoint, Active Directory, Cisco switch & Cisco AC. Preparation of documents of all aspects of related efforts on intrusion analysis, which is submitted to higher officials to conduct audit and worked with various IT and business unit leads to ensure timely

and accurate reports. Implemented Zone Based Firewalling and Security Rules on the Palo Alto Firewall. Responsible for monitoring & acquiring data feeds from a variety of technologies for Splunk (Firewalls, BlueCoat proxy, Windows, Linux, RSA, etc) Setup Integration of FireEye alert in other security systems. Setup Automation of FireEye alerts to block infected devices in other security systems. Secured company internet access using BlueCoat proxies. Engineered BlueCoatpolicies to follow company's policy's & procedures. Knowledge in Group Policy Security (GPO) and AD policy. Constructed actionable reports & alerts from RSA Security Analytics. Conducted network vulnerability assessments to identify system vulnerabilities. Created custom scripts to save time & labour cost on attestation of 50,000 + accounts Collaborated with other departments in investigations for HIPPA & PCI violations Provide consultative services at the time of PCI audits & reviews. Installed and configured Symantec Enterprise Anti-Virus. logging, monitoring and response concepts and technologies for cloud networks, corporate networks, and hosts in all environments Created DLP role-based access controls, DLP device policies, DLP application file access protection. Worked with project managers to ensure incorporation of security activities in all ongoing projects and to identify security impact of new release. Develop, implement, and maintain employee database for multiple departments. Working with global security team for the Server Compliance and risk management. IT security Engineer Tamana Infotech March 2013 to January 2014 Worked on Multiple Education Bachelor of Engineering in Computer Science Anna University Masters in Information Security Sacred Heart university - Palo Alto, CA Skills LINUX (3 years), SQL (1 year), UNIX (1 year), C# (Less than 1 year), C++ (Less than 1 year) Additional Information Operating Systems: Windows 10/8/7/XP/NT/98, Unix, Linux- REMnux, Virtualization(VMware) Languages: C, C++, C#, HTML, Java, PL/SQL, Python, XML. Ticketing System: ServiceNow, Remedy.

Name: John Rogers

Email: parsonsmaria@example.com

Phone: (740)643-1493x9706