Cybersecurity Senior SOC Analyst Cybersecurity Senior SOC Analyst Cybersecurity Senior SOC Analyst - Synchrony Financial, Stamford New York, NY Authorized to work in the US for any employer Work Experience Cybersecurity Senior SOC Analyst Synchrony Financial, Stamford May 2017 to Present Highlights: Successfully Trained 26 HYD(India) new SOC analyst to the SOC Environment with The Tools and Process and Created new alerts (10) ? Working with Splunk in ES for incident review and validation ? Working with Sourcefire to co-relate events in ES and tuning alerts to decrease false positives. ? Active Hunting using RSA Net witness during Blue or Red team hunting exercise. ? Use Tanium dynamic search query and IOC/Trace module to identified vulnerable host and processes. ? Built several Tanium signal to alert on several vulnerable process and IOCs to the Splunk ES quueu. ? Using Forescout Full NAC solution to detect Rogue/Unmanaged devices on network and remediate it ? Proactively using Joesandbox Phishme-Triage and Blue coat and Proofpoint for Dynamic Email analysis to gather threat intelligence to actively respond to phishing email both internally and externally. ? Using Symantec SEP scan as host remediated for malicious software. ? Using Qualys to identify host based on Vulnerabilities, QIDs, Patch level and generating executive report. ? Using Exabeam to monitor User behaviour for lateral Movement activities. ? Acted as a mentor for the tier one analysts to assist them when issues arise. Selected as one of the escalation points when incidents occur above Analyst I capabilities ? Advised junior staff with challenging technical and customer service situations. ? Worked with multiple customer environments both on-premise and virtual from a remote location ? Assisted clients to harden their environment based on security suggestions. ? Created scripts in python to help simplify some of the tasks we perform ? Recently, tested and implemented products to enable automation in response to indications of compromise Senior IT Security Analyst Rackspace - Dallas, TX October 2015 to April 2017 Working on SIEM, Threat and Vulnerability management. ? AWS security, checking for any configuration change in the AWS resources using SPLUNK. ? Creating POC for different security tools. ? Network Security (IDS/IPS, N/W Sniffing, Wireshark, TCPDUMP, NMAP). ? Running vulnerability & compliance scan and report vulnerabilities/compliance to the environment owners. ? Plan, implement and manage vulnerability scanner environment. ? Act as subject matter expert and answer questions related to vulnerability scanner. ? Conduct senior level log analysis, proactive monitoring, mitigation, and response to network and security incidents. ? Investigate and handle security incidents create tickets and reports. (Incident Reports) ? Analysis of PCAP, capture, analyze and detailed reports using Wireshark. ? Analyze security event data from the network (IDS sensors, firewall traffic). ? Identify suspicious and malicious malware Both static and dynamic analysis ? Continuous monitoring and interpretation of threats through use of intrusion detection systems, firewalls and other bound ? Monitoring Snort (writing rules, monitoring BASE), creating the CASE of unknown alerts, Splunk Writing Snort Signatures, Tripwire (HIDS), and OSSEC (HIDS), Vulnerability assessment using NESSUS. Working on Backtrack UNIX. Shell Scripting. Application/Web Security (OWASP). Audit & Compliance (ISO27001). Wireshark, TCPdump, Ettercap, Cain & Abel, Ettercap, C|EH Modules. s IT Security Analyst Ameriprise Financials - Detroit, MI November 2012 to October 2015 Network monitoring and server compliance check. ? Worked on Data Loss Prevention (DLP), Deploying, configuring, and monitoring. ? Evaluated & architected IT Security solutions for the enterprise to improve the IT Security defence in depth. ? Provided leadership & mentoring to security Operations personnel. ? Optimized current security programs for efficiency & effectiveness. ? Developed & maintained operational configurations of multiple IT security solutions. ? Created DLP police to prevent loss of data "in motion/at rest" ? Created DLP effectiveness by reducing false positives by proving policies. ? Produced custom Splunk "TA's" FOR Forwarders, Search Peers & indexers ? Responsible for monitoring & acquiring data feeds from a variety of technologies for Splunk (Firewalls, BlueCoat proxy, Windows, Linux, Imperva, RSA, etc) ? Secured company internet access using BlueCoat proxies. ? Engineered BlueCoat policies to follow company's policy's & procedures. ? Constructed actionable reports & alerts from RSA Security Analytics. ? Conducted network vulnerability assessments to identify system vulnerabilities. ? Developed remediation plans & security procedures ? Provide consultative services at the time of PCI audits & reviews. ? Installed and configured Symantec Enterprise Anti-Virus. ? Administered and managed SEP Client deployments to Workstations and Servers. ? Set up policies for servers with specific policies for apps running on servers. ? Performing DLP inventory scans. ? Created DLP role-based access controls, DLP device policies, DLP application file access protection. Network Security Consultant Linux Administration & Security January 2011 to February 2012 Implemented SNMP-based networking monitoring tool CACTI, Creating Graphs, Templates, adding CAMM for TRAP Configuration, Setting Threshold. ? Implemented BACULA as a backup server and Scheduling backup jobs. ? UNIX/Linux Administration & Security. ? Perform investigations and evaluations of network traffics, read & interpret log, sniffer packets, and PCAP analysis with RSA Security analytics and Wireshark ? Collaborate with technical and threat intelligence analysts to provide indications and warnings, and contributes to predictive analysis of malicious activity. ? Identify and ingest indicators of compromise (IOC's) (e.g., malicious IPs/URLs, etc.) into network security tools/applications. Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis. IT security intern C-DAC November 2010 to January 2011 Worked on Multiple Operating Systems Environments likes Windows (2003, 2008) and Linux (Redhat, fedora, Debian), Virtual Infrastructure. ? Foot printing, Scanning, Sniffing and monitoring Network activities by using Open source & commercial tools like (Wireshark, Nmap). ? Conducting cyber forensics activities to check the process of cyber forensics after cyber-crime was conducted successfully by collecting evidence and securing the evidence. ? Conduct penetration testing & Auditing of the organization network by using tools. Education Masters of Science in Information Assurance in Information Assurance St. Cloud State University 2015 to 2017 Skills Data Entry, access, Microsoft Office, Management, database

Name: Aaron Ross

Email: christinajohnson@example.org

Phone: +1-208-443-9441x080