Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - IBM Centreville, VA To obtain information security position as a team-player, in a fast-paced environment, where I can utilize my many years of general IT and SOC experience, along with educational background to achieve and maximize corporate goals in a challenging environment. Authorized to work in the US for any employer Work Experience Cyber Security Analyst IBM January 2017 to Present Manage the scoping, containment, remediation, reporting, and root cause analysis for all incidents on the IBM Cloud infrastructure. Assist Junior-level analysts on incident triage and disposition. Utilize data provided by malware and forensic analysis to search enterprise for additional indicators of compromise, lateral movement, or persistence of threat actors. Monitor threat feeds for indicators about recent attack vectors, defacements, malwares or phishing activities. Follow the daily security bulletins and advisories for new TTPs and attacks and perform an enterprise search for the applicable IOCs. Facilitate incident response and assessment process, including reporting and oversight of remediation efforts to address offenses. Provide real-time decision making for ongoing information security incidents as they occur to protect corporate and federal assets. Provide appropriate updates to upper management regarding security event handling, trends, analysis, incident response resolutions and lessons learned. Ensure that tools, documentations, procedures and run books are constantly tuned and maintained. Collaborate with the various technology vendors to evolve the tools, improving detection and response efforts and the security program capabilities as a whole. Utilize commercial and OSINT security tools for threat intel hunting. Continuously and pro-actively monitor for any indicators for early detection and prevention. Gather and validate observables from security bulletins and feed the indicators to security tools for signature detection. IT Coordinator Stratford University July 2014 to December 2016 Assist and guide users on the use of computer hardware and software, provide mobile device support. Monitor network for abnormalities using various toolsets such as network analyzer. Perform network troubleshooting to isolate and diagnose network problems. Responsible for overall network and systems health including systems backups, security updates, anti-virus updates. Create/Deploy virtual machines to students/instructors using Skytap. Maintain computers and printers in the classrooms and offices. Manage user accounts using Active Directory. Monitor/maintain student and admin computers using Windows servers. Reimage workstations using Clonezilla. Monitor security cameras that are in charge of overall building security. TECHNICAL SKILLS AND KNOWLEDGE SIEM tools - Splunk and QRadar. Security and threating hunting tools - Palo Alto, TruSTAR, ThreatStream, Autofocus, FireEye (NX, HX, AX), Wireshark, Security Center, and OSINT. Ticket Management Tools - Resilient, RTC, Jira, VSOC, PagerDuty, IMS and SCCD. Penetration testing life cycle and tools such as LCP password cracker, JPS virus maker, proRate. Forensic tools such as FTK Imager, Autopsy, Winhex, EnCase. Computer networking tools such as Cisco Packet Tracer. Software keylogger - Spyrix Microsoft Windows Active Directory Developing Access Control Lists (ACLs) as a modern method of controlling network security Education Master of Science in Cyber Security George Mason University January 2016 to Present Bachelor of Science in Information Security George Mason University January 2010 to May 2013 Skills Nist, Siem, Information Security, Cyber Security Certifications/Licenses CompTIA Security+ Comptia CySA+

Name: Susan Garcia

Email: davispenny@example.net

Phone: (354)615-7885x4665