CSIRT Security Analyst/Forensic Investigator CSIRT Security Analyst/Forensic Investigator CSIRT Security Analyst/Forensic Investigator Alpharetta, GA 3 + years of research-driven Information and IT security professional with solid knowledge in Risk management, Penetration Testing, CSIRT,Forensics and SOC analysis. Authorized to work in the US for any employer Work Experience CSIRT Security Analyst/Forensic Investigator Fiserv(Randstad Contract) - Alpharetta, GA December 2018 to Present Active member of Cyber security incident response team as a security analyst and Forensic investigator. Monitoring and responding both corporate and enterprise level assets from various level of attacks including DDOS, Phishing, Malware,,etc. Threat Hunting for protecting corporate endpoints using multiple sources and manually importing to the integrated - Anomaly threat stream. Assisting Malware analysis with Incident Triage using Carbon Black Response. Maintaining Email Security Using Fire Eye ESS, O365 Security Appliance. Creating Yara Rules to detect and stop Malware and Email threats. Incident handling using Service Now . IT security Intern Sanford Health - Sioux Falls, SD May 2018 to August 2018 SOC | SIEM | INTERNAL SELF RISK & Cyber- security ASSESSMENT Threat intelligence- Incident handling- Forensic analysis - Security Engineering. Maintaining technical proficiency in the use of tools, techniques, and countermeasures. Monitor social media, blogs, and vendor product websites for recently emerging Threats and presenting to the team. Configuring and Automating Backups for Nexpose box. Communicating tactical threat information to assist in defensive mitigations. Creating a comprehensive cybersecurity risk assessment tool by integrating NIST -800-53, ISO 27001:2013 and HIPAA Security Rule 45 for Internal, Vendor, and Meaningful usage. configuring and creating Vulnerability Reports in Nexpose, SIEM -Log monitoring and user behavior Investigations in LogRythm. Firewall administration and log investigation, IPS, Email Security using Industry Standard Software's and products. Third party Vendor management evaluation using Optiv Evantix. SOC analysis and Active protection on more than 70,000 assets in multiple platforms. Developed an Incident response Taxonomy and updated Incident Response policy for Efficiency and organized response. Penetration Tester Health Point, CAHIT, DSU March 2018 to May 2018 Scanning network infrastructure for security vulnerabilities. Exposing any

vulnerabilities in host network and analyzing risk rate. Documentation and testing of vulnerabilities found and report on safety measures to safeguard from attacks. Security audits and analysis of different branches of IT. Performing Social Engineering attacks using GoPhish. Freelance Ethical Hacker and Researcher June 2015 to July 2017 On-demand Security Awareness and services for Clients. Vulnerability Assessment and Secure Network installation. Risk Management with Risk Assessment and Risk mitigation On Demand. Penetration Testing of a system, Network and Web site. Information Security Jr. Technical Engineer/Intern Internettechies Solutions Pvt. Ltd - Chennai, Tamil Nadu January 2016 to April 2016 Worked on Vulnerability Analysis, Network Mapping, Port scanning, Penetration Testing in additional with documentation and customer service. For Network scanning used SolarWinds Network Topology Scanner and Nmap. Automatic network topology mapping and vulnerability scanning of systems using the network address is performed. Vulnerability Scanning App Nessus is used for performing Vulnerability Assessment and categorizing vulnerabilities according to risk - High (red), Medium (yellow) and low (green) in the report for exploitation. Based on Vulnerabilities loading the known payloads in the Metasploit for Successful exploitation and reporting. Training and Awareness exercises for Leadership of client. Completed my first Professional certification CEH v9. Information Security/Intern June 2015 to July 2015 Worked on Zen map (Nmap Windows Interface and commands), OS footprinting and Port Scanning. Training and Awareness about current threats. Acquired first-hand experience in Post scanning and Network mapping Acquired knowledge and understanding of the Secure practices in Information Technology. Education Master's in Information Assurance and Computer Security Dakota State University - Madison, SD August 2018 Bachelor's in Information Technology SRM University - Chennai, Tamil Nadu August 2012 to June 2016 Skills SECURITY (2 years), METASPLOIT (Less than 1 year), NESSUS (Less than 1 year), NEXPOSE (Less than 1 year), NMAP (Less than 1 year) Links https://www.linkedin.com/in/sai-puneeth-gundamraju-824891a1/ Certifications/Licenses Certified Ethical Hacker (CEH) April 2016 to April 2019 License ECCO3891429218 EC-Council Certified Security Analyst April 2017 to April 2020 License ECC45377105255 Additional Information TECHNICAL SKILLS Information and IT security:

Networking, Vulnerability Analysis, Risk Assessments, Penetration Testing, EDR, SOC Programming Languages: C, C++, Java, C# .NET, ASP .NET, HTML5, CSS3, PHP, JS, SQL Scripting languages: Python, power shell. Penetration Testing and other tools : Nmap, Nexpose, Wireshark, SolarWinds Network Topology Mapper, Nessus, THC Hydra, Metasploit, Gophish, the harvester, Magnet Axiom, Forensic Tool Kit. Logrythm-SIEM, Nexpose, Cisco Umberella, Cisco AMP for endpoints, Email Security Appliance, Ironport Firewall, Sourcefire, Cisco Visibility, Optive Evantix. Office tools: MSWord, MSExcel, MSPowerpoint, and Team management software - Slack. Operating Systems: Windows XP, 7,8,10, Kali Linux 1.0 and 2.0, Ubuntu 16, MacOS.

Name: Kathy Navarro

Email: corysanchez@example.net

Phone: +1-563-430-7767x437