Technical Graduate Assistant Technical Graduate Assistant Technical Graduate Assistant Chicago, IL Seeking for Cyber Security Analyst/Engineer Position Develop, implement, monitor and support information systems security programs Around 5 plus years of experience as a Cyber Security Analyst with proficient and thorough experience and a good understanding of information technology. Have a deep knowledge in identifying and analyzing suspicious event. Versatile, bilingual professional and ability to manage sensitive materials. Able to use various security tools to perform logs and packet analysis. Finally, can perform malware analysis with the overall objective to ensure confidentiality, integrity and availability of the systems, networks, and data. Authorized to work in the US for any employer Work Experience Technical Graduate Assistant Chicago State University, IL - Chicago, IL June 2018 to May 2019 Responsibilities: Responsible for handling department website Technical system support. Help resolve system related issues. Trouble shooting. Awareness of social engineering and guide through common security tips. Maintains applications and/or virus protection measures. Checking status of databases and servers. Monitors network performance and make adjustments, connections and/or changes as necessary. IT Security Analyst Kaiser Permanente, US (Cognizant Technology Solutions November 2016 to August 2017 Responsibilities: Provided 24*7 support for all security operations. Conduct proactive monitoring, investigation, and mitigation of security incidents. Responsible to scan Internal and External IPs to find vulnerabilities. Built a Process involved Mapping, Scanning, Reporting and exception form/remediation control. Scan the IP's in Qualys using authenticated Scan, Qualys agent for the vulnerabilities. Report the vulnerability scan and details of it to server team so that they can fix the vulnerabilities and rescan it after the proper remediation is done. Used the Web application Scanner to scan the URL's and identified the potential threats and exploited vulnerabilities like Cross site scripting and SQL injections. Obtained a detailed report of Scanning and provided to server team and got it fixed. Provided the solutions through Qualys web application scanner to the appropriate team to work on and make sure that the systems are protected by any attempts of hacking. Used CrowdStrike to protect our internal assets by installing falcon CrowdStrike sensor on the servers, Validate Machines in CS portal. Used host

management strategy for creating policy, create group, add machines to group. Designed the Prevention policy for the organization Perform threat hunting using the search capabilities of CrowdStrike. Implemented OpenDNS on network and end points. Block Malicious URL's provided by Sec Ops team investigation. Perform Firewall Risk Assessment using AlgoSec. Offline import and Live connect to capture the current state risk of Firewall. Connected life connect to firewall by using credentials for having the routing capabilities on the same network. 2 IT Security Analyst CNO Financial Group USA May 2015 to November 2016 Responsibilities: Created and established complete security awareness training program for Cognizant employees working for CNO client. Carry out Phishing test campaign to get the analysis on how much percentage of users are prone to email frauds. Generate reporting metrics to show the statistics and progress. Perform risk assessments how much percent of users are prone to email risk driven by metrics. Introduced phish alert button to make users reporting of fraud/phishing emails easy in just 'one click'. Responsible to make sure Crowd strike agents are installed. Threat hunting and detailed analysis of a critical/High detection. Responsible to perform risk exposure assessment in an event of vulnerability break down/disclosure. Administer the platform for version upgrades and troubleshoot issues if any. Investigate for any malware/virus found by Crowd Strike and take appropriate remediation. Block URLs which are malicious in nature. Threat Intelligence by Umbrella. Deploy agents to End points and Network. Restrict access to non-business-related website. IT Security Analyst Cognizant Technology Solutions - IN April 2014 to May 2015 Responsibilities: Investigate the emails reported by the users for any malicious link or an attachment. Perform detailed analysis on malicious attachments and take remediation steps accordingly. Block HASHES in CrowdStrike and malicious URLs in OpenDNS. Generate Monthly metrics on reported fraud/phishing emails. Performed Header analysis, Blacklist check for IP, Hyperlinks, analyze encoded html files etc. Work with legal team to take down fake domains that impersonate the real client domain. Identify suspicious/malicious activities or codes. Search firewall, email, web or DNS logs to identify and mitigate intrusion attempts. Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based

on analysis. Perform Firewall Risk Assessment using AlgoSec. Information Technology Trainee Uclid IT - Hyderabad, Telangana July 2013 to March 2014 Responsibilities: Continuous monitoring and interpretation of threats using the IDS and SIEM. Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis. Rescan mitigated systems for further infections. If none, commission systems back to the network. 3 Conduct research on new and evolving threats and vulnerabilities using security blogs. Research new and evolving threats and vulnerabilities with potential to impact the monitored environment. Identify suspicious/malicious activities or codes. Monitoring and analysis of security events to determine intrusion and malicious events. Search firewall, email, web or DNS logs to identify and mitigate intrusion attempts. Education Master of Science in Computer Science Chicago State University - Chicago, IL Bachelor of Technology in Technology Jawaharlal Nehru Technological University - Hyderabad, Telangana Skills FIREWALL, CSS, SECURITY, QUALYS, SIEM, SPLUNK, SQL, VISUAL STUDIO, HTML, XML, OPEN SOURCE, INCIDENT RESPONSE, REMEDY, TIVOLI, JAVA, BMC, TRACKIT, RISK ASSESSMENT, FRAUD INVESTIGATION, METRICS

Name: William Wilson

Email: anthony30@example.org

Phone: 001-773-873-8892x2441