Jr cybersecurity analyst Jr cybersecurity analyst Jr Cyber security Analyst - Dover Corporation Chicago, IL I am a Security Analyst with 3 years of experience scanning and analyzing vulnerabilities and threats in large scale networks. I have been using Splunk for Security incident and event monitoring and Qualys for threat vulnerability management in an enterprise environment of over 25K employees for over a year at Dover Corporation. I also performed malware investigation, Email header analysis and provided remediation. I have excellent communication skills and obtained a master s degree in Information Systems and Security. Authorized to work in the US for any employer Work Experience Jr cybersecurity analyst Dover corporation - Downers Grove, IL January 2018 to March 2019 Dover Corporation, IL 01/2018 03/2019 Jr. Cyber Security Analyst involved in variety of Cyber Security initiatives and primarily responsible to drive following projects: Project 1: Threat Vulnerability and Management project: Tools used: Qualys, MS Excel. Perform Risk assessment on Internal and External assets. Work with respective operating company to solve their internal and external vulnerabilities based on severity level. Generate monthly report on vulnerabilities. Create custom reporting dashboard to show the trending. Track vulnerabilities exception through exception form and make sure to follow the TVM process. Monthly calls with operating companies to track the status and explain the report. Provide generic remediation of the vulnerabilities. Analyze the risk exposure of Dover in the event of a new vulnerability break down/release. Perform deep analysis in identifying the risk exposure and provide appropriate remediation steps. Project 2: Security Awareness Training and Test campaigns Tools used: Knowbe4, SecureAuth (LMS). Created and established a complete Security awareness training program for Dover Corporation. Roll out Security Awareness training to all end users in the form of videos and posters. Carry out Phishing test campaigns to get the analysis on how much percentage of users are prone to email frauds. Introduced Phish alert button to make user reporting of fraud/phishing emails easy in just one click . Generate reporting metrics to show the statistics and progress. Perform risk assessment on how much percent of users are prone to email risk driven by metrics. Project 3: End Point Protection Tools used: Crowd Strike, Cylance. Responsible to make sure Crowd Strike agents are installed across Dover Corporation. Monitor

alerts from Crowd Strike depending on the severity Level. Threat hunting and detailed analysis of a Critical/High detection. Responsible to perform risk exposure assessment in an event of Vulnerability break down/disclosure. Blacklist malicious hashes. Check for false positive alerts. Administer the platform for version upgrades and troubleshoot issues, if any. Investigate for any malware/virus found by Crowd Strike and take appropriate remediation. Project 4: URL Filtering Tool used: OpenDNS. 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. Project 5: SIEM ( Security Incident and Event Monitoring): Tool used: Splunk. Implement a solution to mitigate the risk across Dover. Experience in configuring, implementing, analyzing and supporting Splunk server infrastructure across Windows, UNIX and Linux. Experience with a variety of Operating Systems, Protocols and Tools depending on the type of platform or application to be administered. Upgrade and Optimize Splunk setup with new discharges. Extensive experience in deploying, configuring and administering Splunk clusters. Expertise in Actuate reporting, development, deployment, management and performance tuning of Actuate reports. Created Splunk app for Enterprise Security to identify and address emerging security threats through the use of continuous monitoring, alerting and analytics. Helping application teams in on-boarding Splunk and creating dashboards, alerts, reports etc. IT Security Analyst Intern Efusion solutions - Barrington, IL September 2017 to January 2018 Tools used: Knowbe4, Qualys. Responsible for Security awareness training and carry out Security Test campaigns. Threat Vulnerability and management using Qualys tool. Creating Reports about vulnerabilities every 15 days. Performed full scans IPs every 4 to 5 days. Provided Vulnerability remediation. IT Security Analyst MM Consultants - Hyderabad, Telangana January 2014 to May 2015 Project: Firewall Risk Assessment Tool used: Algosec. Perform Risk assessment on firewalls. Responsible to improve firewall risk posture and close all the security flaws due to risky rules. Generate audit reports on firewall risk posture and work with the respective operating company to remediate the risky rules. Perform route analysis between source and destination. Troubleshoot routing issues. Live connect firewalls to AlgoSec. Detailed analysis on risky rules. Track real time changes done to the firewall. Project:

Fraud/Phishing emails investigation: Tools used: Online free available analysis tools 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 Crowd Strike and malicious URLs in OpenDNS. Generate Monthly metrics on reported fraud/phishing emails. Perform Header analysis, Blacklist check for IP, Hyperlinks, analyze encoded html files etc. Education Master's in Information Systems & Security in Physical University of the Cumberlands August 2017 Bachelor of Engineering in Computer Science in Computer Science Osmania University July 2013 Skills Siem, Information Security, Cyber Security, Cybersecurity, It Security

Name: Mary Quinn

Email: mcdonaldbrooke@example.com

Phone: 001-545-280-6376x75193