Cyber Security Instructor Cyber Security Instructor Cyber Security Instructor - Dover Corporation Chicago, IL Work Experience Cyber Security Instructor Dover Corporation January 2018 to Present As part of social activity, provide lectures on social engineering, phishing and many more topics based on demand and need. Helping the youth and professionals to grow who wants to be a part of Cyber Security work force to defend against cyber crime IT Security Analyst Dover Corporation September 2016 to Present Currently - IT Security Analyst Dover Corporation September 2016 to Present Currently, working as IT Security Analyst, involved in variety of Cyber Security initiatives as follows: Threat Vulnerability and Management project: Tools used Qualys, MS Excel Certificate: Qualys Guard - Vulnerability Management Certified in Qualys Vulnerability Management Module. 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. Perform Web Application Scanning and help operating companies to understand the report to remediate the issues. Perform manual and automated Web Application pen testing Use Veracode for Static/Dynamic code analysis Work with the respective team and guide them to remediate the vulnerabilities. Application Security: Tools used: Burp Suite, Qualys (WAS), OWASP Zap Lead manual Pen Testing task to find Web App vulnerabilities in variety of different platforms Perform automated Web App scan using Qualys Provide recommendations to remediate vulnerabilities found during manual and automated test Implemented Veracode to perform static/dynamic code review Intrusion Prevention/Detection System (IPS/IDS): Tool used: Cisco Firepower Setup Firepower management console and configure to connect sensors (ASA firewalls, routers) Integrate Firepower with Splunk and create co-relation search for automated email reporting on new detection Create a standard security policy to ensure blocking malicious traffic and deploy policy across all devices connected to FMC Console Create a process/procedure document to define roles and responsibilities between teams. Investigate alerts generated from IDS and investigate risk exposure from malware tracking mechanism. End Point Protection Tools used: CrowdStrike, Cylance Monitor alerts from CrowdStrike depending on the severity Level. Threat hunting and detailed analysis of a Critical/High detection. Provide Level III support for investigation and alerts.

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. Security Awareness Training and Test campaigns Project: Tools used: Knowbe4, SecureAuth(LMS) Created and established a full fledge 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'.

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. Network Access Control (NAC) Tool used: ForeScout Implement solution for NAC and create policies Help and support to implement ForeScout solution for Dover.

Monitor threat alerts from ForeScout and perform detailed analysis to remediate them. Enforce strict actions on failing the compliance check. URL Filtering Tool used: OpenDNS Block URLs which are malicious in nature Investigate Risk exposure using Security Activities module to identify organization's exposure to a malicious domain Created a standard companywide policy to block non-complaint/inappropriate/Malicious content Based on the need, create custom policies as per Business requirements SIEM (Security Incident and Event Monitoring): Tool used: Splunk Create basic dashboards in Splunk to display reporting metrics. Investigate level III incidents and perform complete remediation Perform Threat Intel using Splunk and create co-relation searches based on required real time monitoring. Support SecOps team in investigation and solving issues. Once alert reported by Vsoc team, perform detailed analysis on the risk and find the risk exposure of Dover. IT Security Intern Dover Corporation July 2016 to August 2016 IT Security Intern at Dover Corporation, IL July 2016 -Aug 2016 Tools used: Knowbe4, Qualys, Burp Suite Responsibilities: Responsible for Security awareness training and carry out Security Test campaigns Threat Vulnerability and management using Qualys tool Create Executive level custom reporting

dashboards for Cyber Sec tools to show trending & stats. Perform Manual Pen Testing on Web Application and provide remediations Technical Graduate Assistant/ Security Intern Northeastern Illinois University April 2014 to August 2016 Technical Graduate Assistant at Northeastern Illinois University, IL Apr 2014 - Aug 2016 Manual Web Application Pen-Test on variety of platforms using Burp Suite and other supporting tools. Create custom automated reports to support the requirement in sorting big database. Provide lectures to the class on latest technology and Cyber Security Awareness Responsible for handling department website, EICS(Education Master of Science in Computer Science in Computer Science Northeastern Illinois University August 2016 Bachelor of Engineering in Computer Science in Computer Science Osmania University July 2013 Skills .net (Less than 1 year), Asp (Less than 1 year), Asp.net (Less than 1 year), Bi (Less than 1 year), Business intelligence (Less than 1 year), Cisco (2 years), Css (Less than 1 year), Excel (2 years), Firewall (2 years), Ids (2 years), Ips (2 years), metrics. (2 years), Ms excel (2 years), Qualys (2 years), Risk assessment (2 years), Security (5 years), Siem (2 years), Splunk (2 years), testing (2 years), Training (2 years) Additional Information Master's in computer science with good communication and analytical skills for continuous improvement. Overall 5 years of experience in Cyber Security. Threat investigation and risk exposure assessment. Perform Level III detailed analyses of a threat event and remediation Certified in Qualys Guard Vulnerability Management Module. Implemented Firewall Risk Assessment solution, Network Access Control(ForeScout) solution, Phish Alert Button on outlook, Threat Vulnerability Management(Qualys), IPS/IDS solution(FirePower), End Point Protection(CrowdStrike) Created & Designed full-fledged Security Awareness Training program Built custom reporting dashboards and KPI metrics in Splunk, Tableau, PowerBi and Excel Lead Application Security tasks that includes both manual Pen Testing and Automated Web App Scanning Skills Programming Languages Java, SQL, HTML, CSS, JavaScript, MongoDB, JSON, Xml, Python Security Tools Qualys, Knowbe4, OpenDNS, CrowdStrike, CyberArk(ViewFinity), Splunk(SIEM), Office365, Burp Suite, AlgoSec, PhishMe, Cylance, Firemon, Wombat, ProofPoint TRAP, ProofPoint TAP, ForeScout, OwaspZAP, Cisco FirePower. Experience in Security areas Web application pen testing(OWASP 10), Application

Security, Email filtering, Firewall risk assessment, Email fraud investigation, Threat Vulnerability management, Risk Assessment, End point protection, Security awareness and training, Incident Response, Reporting metrics, SIEM(Splunk), URL Filtering, Privilege Access Management(basic), IPS/IDS, Network access Management. Other tools Eclipse, Power BI, Tableau, Dreamweaver, Visual Studio, ASP.Net, MS Access, NetBeans, MS SQL Server, MySQL Server Management, WordPress, MS Excel.

Name: Lauren James DDS

Email: reneediaz@example.com

Phone: 827.250.9061x425