Senior Information Security Analyst Senior Information Security Analyst Senior Information Security Analyst Parsippany, NJ Being able to gain knowledge in different areas of Information Security AREAS OF EXPERINCE ? Network Security: Vulnerability Management/Assessment Patch Management Configuration Management Encryption Web-filtering security Log analysis IDS/IPS configuration/monitoring Firewall Data Loss Prevention Windows/Linux operating system Endpoint hardening 3rd Party Software Management ? Tools: Qualys Nessus Palo Alto Tanium NMAP PGP encryption Web Sense McAfee Product (Virus scan, TIE/ATD) Tufin Secure change/Secure Track Qradar Redline Splunk PowerBi Tableau Metric Stream Work Experience Senior Information Security Analyst UPS - Mahwah, NJ August 2018 to Present Leading and Developing Vulnerability Management program for 9 UPS merger and acquisitions. ? Responsibilities included identifying, scanning, and notifying for vulnerabilities facing external and internal assets. ? Identifying and successfully remediating highly rated vulnerabilities for UPS subsidiaries to ensure availability and integrity are not impacted to the organization. Being able to Continuous Monitor for critical vulnerabilities affecting UPS/Merger and acquisition. ? Advising appropriate subsidiaries/UPS support teams with UPS policies, standard process as part of remediation solutions, patch governance, and best practices. ? Using PowerBI to show senior management metrics for patching and vulnerability status. ? Responsible for managing PCI segment for vulnerability management. Responsibilities included continuous monitoring of new assets, tracking vulnerabilities, and working with support teams to address non-compliant vulnerabilities. ? Working with Application based vulnerabilities such as spring framework. Responsibilities included reviewing vulnerabilities, notifying application teams, and tracking commitment timeframe. ? Improving and establishing a process flow, working with multiple teams to ensure gold standard is up to date. ? Working with Pentest team to provide host level assessment for in scope pen test. ? Collaborating with Security Operation center to assess the risk of a vulnerability and work with associated teams to notify patch timeline. ? Mentor and train others in vulnerability management, data visualization, patch management, and configuration management. ? Being able to understand process flow and turning them into automated task ?

Being able to create procedures for tasks. Information Security Analyst UPS - Mahwah, NJ June 2017 to July 2018 Conduct vulnerability assessment for over 20,000 assets worldwide and produce reports of findings leading to risk mitigation. ? Providing various ways of data visualization to UPS management for compliance score and measuring support teams performance. ? Ability to work on multiple projects simultaneously, set priorities and meet deadlines. ? Help standardize processes, procedures and provide improvement. ? Providing remediation guidance based on configuration, operating system and application patching process. ? Tracking and monitoring third party applications exception for older applications not able to remain compliant with latest standards. ? Researching latest threats that are emerging, identifying assets, and working with various teams to mitigate the risk. ? Participated in the improvements of baseline configurations. ? General understanding of PCI DSS UPS - Mahwah, NJ November 2015 to May 2017 Analyzing Intrusion detection signature to look for malicious behavior via log analysis. ? Engaging SOC to assist in depth investigation to improve signature tuning. ? Successfully auditing firewall rules to ensure proper connectivity for customers. ? Leading firewall rule cleanup. ? General experience in Air defense Motorola. IT Security Intern Tiffany and Co - Parsippany, NJ May 2015 to August 2015 Network Security - vulnerability assessments, computer forensics, vendor security assessments, PGP encryption General experience in Air defense Motorola. ? Assisted with Computer forensics /Malware Analysis - disassemble and debug malicious software, dynamic analysis via virtual machine (i.e. Fireeye, Qradar, Mandiant Redline, Encase). ? General experience with Qradar, Fireeye, Mcafee/EPO, McAfee TIE/ATD, Websense, Qualys, Palo Alto, Tripwire, Splunk, Encase, Air watch, DLP, FTK imager. ? Exposure to business issues and challenges (i.e. Point of sales Terminal). ? Upgrading and configuring appliance (i.e. Websense and Qualys). ? Assisted in CDE segmentation project. ? Strong knowledge of security technologies in areas such as servers, firewalls, Routers, Switches, Proxies, IPS/IDS. ? Monitor, analyze, research, security incident management logs and alerts (i.e. Qradar). ? Perform and analyze vulnerability assessments (i.e. Qualys). ? Performing web filtering (i.e. Websense). ? Participate in Data loss prevention project. IT server Intern InVentiv Health - Somerset, NJ July 2014 to March 2015 Find ownership of all existing non-person accounts in Active Directory. ? Edit Active Directory accounts and populate them with informational data. ? Familiar with data center infrastructure concepts including servers, storage, desktops, and Active Directory. Education Bachelor's Degree in Information Technology New Jersey Institute of Technology - Newark, NJ Certifications/Licenses GIAC Certified Incident Handler (GCIH) April 2019 to April 2023 GIAC Certified Incident Handler (GCIH) GIAC Security Essentials (GSEC) March 2018 to March 2022 GIAC Security Essentials (GSEC)

Name: Michael Dalton

Email: justinlewis@example.org

Phone: 001-439-574-4177x087