IT Security Engineer IT Security Engineer Fort Myers, FL Insightful and results driven IT Security specialist who relishes the thought of taking on new and difficult challenges. Notable success in directing a broad range of corporate IT security initiatives while participating in the planning, analysis, and implementation of solutions in support of business objectives. Authorized to work in the US for any employer Work Experience IT Security Engineer 21st Century Oncology - Fort Myers, FL October 2016 to Present 21st Century Oncology Main Job Responsibilities: Conduct vulnerability scans and remediation follow up projects. Prepare phishing campaigns in order to harden users against phishing emails and other forms of social engineering. Utilize Metasploit Pro to validate vulnerabilities as well as perform assessments against servers/workstations that have been found to contain vulnerabilities that may not be able to be patched for various reasons. Maintain and monitor SIEM appliances and applications, add data sources to the SIEM and verify log gathering from data sources. Review security events as they are reported in by the MSSP. Document and follow up with security event cases from start to closing. Deploy AV/ Security Software Suite to servers across the Enterprise Review and enforce policies set forth by the CISO. Research new technologies that could prove of value in strengthening company's network security posture. --- Assisted with the physical installation, set up, configuration, and go live of hardware based SIEM. Assisted in the creation of SEVERAL network security policies which ensure a strong network security posture as well as ensuring that patient data/HIPPA sensitive information and other PII are secure. Assisted in setting up and performing vulnerability scans in the environment to give upper level management an idea of what needed to be addressed by highest to lowest priority rankings. Works in tandem with MSSP and internal support teams to identify and remove infected machines from the environment and if need be, create forensic images of said machines for CISO investigations. Analyst - IT Security - Network Security Team Chicos FAS, Inc - Fort Myers, FL October 2015 to August 2016 Main Job Duties: Main Job Duties: Responsible for the company's vulnerability management and remediation program. Ensure user compliance with all IT Security policies and procedures when it comes to network resource access. Follow through with management in regard to all user access requests. Set up user access utilizing the principals of least privilege, need to know, and due care/due diligence. Insure all access falls under PCI and SOX compliance guidelines. Respond to all network threats including virus outbreaks and cyber attacks from either the inside or the outside of the network. -- Responsible for the implementation of several critical projects within the company: Over several weeks physically installed, configured, upgraded, and maintained multiple Sourcefire sensors in both company data-centers as well as tied them all into the Sourcefire Defense Center for central management. Placed in charge of handling all vulnerability management and remediation duties through the use of Nexpose and Metasploit. I also managed and maintained both systems as well as oversee their upkeep. Project lead in the company wide 2-Factor Authentication roll-out which includes both digital as well as hardware 2-Factor mediums. Responsible for quarterly password auditing and remediation for both store and Corporate HQ networks. IT Security Technician Chicos FAS, Inc - Fort Myers, FL October 2013 to October 2015 Main Job Duties: Ensure user compliance with all IT Security policies and procedures when it comes to network resource access. Follow through with management in regard to all user access requests. Set up user access utilizing the principals of least privilege, need to know, and due care/due diligence. Insure all access falls under PCI and SOX compliance guidelines. IT Operations Technician Chicos FAS, Inc - Fort Myers, FL October 2012 to October 2013 Solution Center and Network Operations Center Duties: Provides advanced technical assistance to network users. Answers questions and resolves network issue for clients and users either in person, by telephone, or via remote connection. Provides assistance concerning the use of computer hardware and software including printing, installation, security, and operating systems. Administers the daily performance of various network systems and applications. Maintains records of daily data communication transactions, problems, and remedial actions taken. Confers with staff, users, and management to establish requirements for new systems or modifications. Network Operations Center (NOC) Duties: Administers the daily performance of various network systems and applications. Monitor the health of the network and investigate any anomalies/outages reported and if need be make call outs to any on call staff. Maintain and moderate Sev 1 and Sev 2 bridges. Keep detailed logs on all events that transpire as well as prepare logs for dissemination to members of management. https://www.visualcv.com/christopher-donlin Education Associate of Science in Microsoft Network Engineering and Database Administration Southwest Florida College 2002 to 2004 Skills Authentication (Less than 1 year), Metasploit. (Less than 1 year), Nexpose (Less than 1 year), Security (5 years), SIEM (1 year), Information Security, PCI, Network Security, It Security Certifications/Licenses Security+ December 2014 to December 2017 Security + Certified Expert License# YJNZ6J6JWKR4Q7LE InfoSec Institute Content Specialist in Information Security February 2014 to Present InfoSec Institute Content Specialist in Information Security Google Apps 100 Certification February 2014 to Present Google Inc. Set up, roll out, maintain and administrate Google Apps for Enterprises. InsightVM Certified Administrator March 2018 to Present Rapid7 - InsightVM Certified Administrator ESM 10 Engineer I: 4-Day (SIEM) Enterprise Security Manager Administration June 2018 to Present Engineering course held and led by McAfee detailing their SIEM product from an engineer perspective. Additional Information Operating Systems Windows 7 ? Windows Vista ? Windows 8 and 8.1 ? Windows 10 ? Windows Server 2003, 2008, and 2012 ? Multiple Linux Operating Systems ? Sourcefire OS Security Tools Kali Linux - Multiple Tools ? Sourcefire ? Tripwire ? Nexpose ? Metasploit ? Nmap ? Zenmap ? PhishMe ? Social Engineering Toolkit ? Malwarebytes ? Symantec Enterprise AntiVirus ? Anti-Rootkit tools ? AirWatch ? OpenDNS ? Bluecoat ? Panorama 9 ? Lieberman Enterprise Password Management System ? Google 2-Factor Authentication ? SFTP ? Dell Secureworks ? IDS ? IPS ? SIEM Installation, Configuration, and Monitoring ? Incident Response ? Security Event Handling and Case Documentation ? McAfee Security Services and Products ? Carbon Black ? InsightVM ? Metasploit Pro

Name: Caroline Gomez

Email: kimberly62@example.org

Phone: 711.213.1470x20803