Threat & Incident Response Engineer- SOC Tier- (Contractor) Threat & Incident Response Engineer- SOC Tier- (Contractor) Threat & Incident Response Engineer- SOC Tier - IBM Bolingbrook, IL Results driven business disciplined IT Security professional with a deep-rooted understanding of Cyber Security Framework. Having 7 years of experience in threat hunting, identification and a strong desire to identify and remediate IOC's. Authorized to work in the US for any employer Work Experience Threat & Incident Response Engineer- SOC Tier- (Contractor) IBM - Chicago, IL October 2018 to Present Spearheaded the "Wanna-cry Ransomware" project. Currently responsible for completing network blocks, removal from the network and/or providing remediation steps infected machines. Currently exceeding expectations with more than 80% of the project completed. Deeply engages in pro-active Intelligence collection, root cause analysis, reporting of threat intelligence from both internal and external sources. Applying protocols to identify errors and solutions in order to maintain system function while interpreting and producing graphs, identifying trends, and drawing justifiable conclusions from data. Proactively prepares reports that document security breaches and the extent of the damage caused by the breaches or security incidents. Provides expertise in identifying key cyber threat issues through a variety of intelligence resources available and proactively advise on remediation processes. Collaborates with all information assurance security professionals to identify IT security, physical & procedural shortfalls. Conducts Operations surrounding cyber security incident response technologies including network logging and deep-diving, security information and event management tools, security analytics platforms, log search technologies, and host-based forensics as applicable. Cyber Security Analyst II- (Contractor) ManTech International - Hines, IL September 2017 to July 2018 Monitored the VA Network while utilizing various security tools (e.g., Splunk, Palo Alto Networks, Sourcefire, Cisco ASA). Identified & resolved potential incidents, network intrusions, and malware events that ensured confidentiality, integrity, and availability of VA architecture and information systems are protected. Reviews and analyzing log files to report any unusual or suspect activities Utilize incident response use-case workflows to follow established and repeatable processes for remediation and escalating. Opens and creates trouble tickets and performing initial validation and

triage to determine whether incidents are security events using open source intelligence (OSINT). Analyzed and correlated incidents & event data to determine preliminary root cause and corresponding remediation strategies. Assists in risk analysis, risk assessments and comprehensive risk management. Worked diligently with client internal Cyber security on critical and high security incidents. Manages the functionality and efficiency of endpoint by proactively and re-actively responding to trouble and incident tickets. Cyber Security Analyst-SOC-IH TEAM (Contractor) Department of Veterans Affairs/Bylight Professional IT Services - Hines, IL April 2015 to December 2016 Accepted recommendation to come aboard the (IH) team to work on a special project and take on more responsibilities. Prepared briefing packages of the finalized analytic data daily for presentation for customers, upper management also including the United States President for approval. Ran hourly, daily and half day scans while monitoring the network for any data breaches, compromise, and or intrusion. Investigated, analyzed and ran TCP Port scans to determine a "Tue or False" security breech. Successfully identified vulnerabilities, recommended corrective measures and ensure the adequacy of existing information security controls. Connected with Information Security Officers (ISO's) and regional POCs to support incident analysis and resolution. Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools. Cyber Security Monitoring Analyst-SOC- SMART TEAM (Contractor) Department of Veterans Affairs/Bylight Professional IT Services - Hines, IL October 2015 to April 2016 Responsible for day-to-day management and monitoring of the VA WAN, Internet Gateway services including Palo Alto and Einstein. Incident reporting by updating open tickets with the latest update and or closing the tickets. Excelled on creating reports on Host-based intrusion prevention system (HIPS) McAfee, network intrusion prevention system (NIPS) and security device support, event monitoring and resolution. Conducted research scans on cyber intelligence and coordinated with vendors to resolve vulnerabilities. Monitored cyber security threat portals for threat data, trends, and Indicators of Compromise. Implemented company policies, technical procedures and standards for preserving the integrity and security of data, reports and access. IT System Analyst-NOC- (Contractor) Adams Communications & Engineering - Hines, IL April 2015 to October 2015

Provided Tier I & 2 network security services and support and provides network security and defense (NSD), analysis and problem resolution on the VA's national IT infrastructure Single point of contact for internal users and business partners needing support and guidance for Incident Response security related issues Coordinated installation, maintenance and troubleshooting of Citrix and Remote Access software on government furnished equipment (GFE) and operator owned (OE) systems (i.e. Windows platform and MACs, android and iPad). Identified, diagnose and resolve issues with end-users relevant to Workstations, Personal PC, tablets & Smartphones (Android/IOS), mainframe, email, internet and local-area network access problems onsite and via VPN Remote Access (Citrix/Cisco). Operations & Support Analyst II Ulta Beauty Corporate - Bolingbrook, IL February 2013 to April 2015 Partnered closely with LP (Loss Prevention) Managers and E-Commerce to monitor, communicate, and investigate fraudulent trends, while sharing best practices. Demonstrated retention skills to maintain revenue while resolving issues and maintaining relationships with clientele, District and Regional managers. Escalated suspicious/fraudulent web activity and monitoring web orders via SAP, ATG, and Cyber source. Responsible for guest call backs to provide resolutions and best practices including Corporate Level II escalations. Responded to guest and field inquires through various forms of verbal, electronic, and written communication and to ensure efficient and complete resolution. Identified, evaluated and monitored relevant social media channels, implementing strategies for using social Media channels i.e. Facebook, LinkedIn, and Twitter for marketing purposes. Retention Specialist Level II Comcast - Tinley Park, IL October 2009 to October 2012 Assisted with any technical issues by troubleshooting Cable Modems/WIFI Gateways; i.e. Netgear, Arris, Motorola, Zoom and cable hubs. Reported any outages and setup truck rolls for any unresolved technical issues. Provided a full range of customer services to retain and gain customers and business revenue with product knowledge and skilled customer focus. Performed necessary modifications on customer accounts to ensure the customer is completely satisfied with the level of service provided with a first call resolution to eliminate repeat callbacks. Adhered to extensive metrics daily such as sales goals, retained revenue, average call handle time, first call resolution, voice of the customer and schedule

adherence. Customer Service Associate Sammons Preston Patterson Medical - Bolingbrook, IL September 2007 to October 2009 Managed several major Corporate and Government VA accounts while multitasking with Sales Reps calls and emails. Exceeded the daily minimum expectation of 75 or more inbound calls. Utilized CMS for inquires and setting up new accounts, recently converted from the AS400 (UNIX environment.) Education Bachelor of Science in Information Security Management DeVry University 2016 Skills MALWARE, CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL, SECURITY, NETWORK MONITORING, DLP, SIEM, OPERATIONS, TIME MANAGEMENT, PROBLEM SOLVING, THREAT IDENTIFICATION, SYSTEMS SECURITY, LEADERSHIP SKILLS, TRAINING, Cyber Security, Information Security, Linux, Network Security, Nist Certifications/Licenses Certified Ethical Hacker (CEH) October 2017 to October 2019 Carbon Black January 2019 to Present ITIL October 2015 Additional Information Core Competencies Certified Information Systems Security Professional Strong ability multi-task in a fast-paced environment Proficient in multi-operating systems & Siem tools Collaboration & Teamwork Skills Superior Communication Skills Resilient & Analytical Thinker Critical Time Management Skills Training & Leadership Skills Problem Solving Skills Detection of Malicious Activity Incident Handling/Management Insider Threat identification/Hunting AWS Cloud Operations Network Monitoring Security Operations Threat Intel/ DLP Malware Analysis Cyber Defense

Name: Scott Barber

Email: rebecca13@example.net

Phone: 476-272-9371x66634