SOC Team Lead SOC Team Lead Cyber Security Professional Houston, TX Seasoned Information Systems professional with 10+ years of experience performing cyber incident response,auditing, managing IT infrastructures and data-center operations in both the defense and private sectors. Recognized for isolating deficiencies, creating and delivering solutions tied to business growth in the management of enterprise IT solutions. Key Strengths include problem resolution and translating effective technical support to end users. Top Secret Clearance Eligible Authorized to work in the US for any employer Work Experience SOC Team Lead Alert Logic 2018 to Present Responsible for directly managing a team of 12 Security Analysts performing incident analysis and customer support in a fast paced and dynamic environment while achieving 99.99% SLA obtainment. Proactively identify and prioritize efforts for emerging threats, incident analysis, and response for over 1000 subscribed customers. Develop and improve processes, tools, and standard operating procedures for the Security Operations Center. Engage directly with customers to deliver improved security outcomes through service and product evolution. Senior Network Security Analyst Alert Logic 2013 to 2018 Monitor and perform manual analysis of IDS events and over 9,000 security incidents originating from varying customer environments for a cloud-based Security-as-a-Service solution Company that works with small- to mid- to enterprise-level businesses internationally Identify the scope of active threats to customer assets and provide recommendations to mitigate and resolve emergent threats; review customer-submitted requests and troubleshoot Developed new method of reporting information to clients in more consumer-friendly, communicative format - built an automated script to gather this information to present in appropriate situations Wrote a new Standard Operating Procedure on evaluating requests and responding effectively to customers with customized recommendations and shortened response-times Use expert understanding of Snort IDS signatures to identify potential gaps in attack coverage and engineer new signatures to meet custom requests Information Assurance Analyst Foxhole Technology - Newport News, VA 2012 to 2013 Traveled across the U.S. to perform on-site assessments of classified and unclassified Army networks and information systems under contract with the United States Army Audited and documented compliance with DODI 8500.2 and AR 25-2 information assurance controls through

system scans, Retina, SRR, SCAP and manual STIG compliance checklists, manual documentation review and physical inspections Assessed 250 - 450 controls per site (depending on the network) and then collaborated to present findings and deliver post-operation debrief & compliance recommendations Conducted Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) validation and compile validation results in to a deliverable (DIACAP Scorecard) Network Administrator United States Navy - Norfolk, VA 2011 to 2012 Performed daily scans for unapproved software and materials on 600+ network assets and enforced command policies for the United States Navy Maintained security patches and machines on board ships during deployment Trained and certified 37 technicians in CompTIA Security+ SYO-201 certification in support of DODI 8570.01 Network Administrator United States Navy - Norfolk, VA 2008 to 2011 Served as an on-call network administrator, in support of the implementation and maintenance of 400+ unclassified and classified computer workstations and a Top Secret network for a Fleet Commander in the United States Navy Created Certification & Accreditation package with Retina Scans of all networks to verify application of IAVA and IAVB updates for network and software programs Maintained 20+ HF, UHF, and SATCOM radio circuits and ensured reliable communications with all ships in the AOR Selected to deploy with a team in support of humanitarian missions in Haiti and the Gulf of Mexico to set-up and manage a fast-response deployable network containing 12 servers and more than 60 laptops Education Associate Degree in Information Technology ITT Technical Institute - Thornton, CO 2007 Skills Wireshark (6 years), tcpdump (6 years), Linux (6 years), Snort (6 years), TCP/IP (10+ years), Windows (10+ years), Auditing (2 years), Network Security (8 years), SIEM (7 years), Cisco (2 years), Vulnerability Scanning (8 years), Symantec Endpoint (2 years), Security, Active Directory, HTML Military Service Branch: United States Navy Rank: E5 Certifications/Licenses Security+ Present Network+ Present GCIA CCENT Assessments Verbal Communication Expert August 2019 Speaking clearly, correctly, and concisely. Full results: https://share.indeedassessments.com/share_assignment/zlxip7vv-wjtr-xq Indeed Assessments provides skills tests that are not indicative of a license or certification, or continued development in

any professional field.

Name: Lisa May

Email: johndonaldson@example.com

Phone: 804.726.2384