SOC Manager SOC Manager SOC Manager - Wapack Labs Hartselle, AL Current SOC Manager for Wapack Labs. 12 Years of IT experience, with four years dedicated to Information Assurance as a designated Security Officer in the Department of Defense. Experienced in Security Analyst, Vulnerability Management, and Certification/Accreditation roles. Work Experience SOC Manager Wapack Labs August 2018 to Present Leader, technical advisor, and mentor for Security Analysts in a 24/7 Security Operations Center. Author of all Standard Operating Procedures, triage, escalation, and workflow documentation. Technical lead and subject matter expert for security appliances and SIEM technology. SOC technical liaison and compliance advisor for clients. Responsible for providing metrics, project management reports and situational awareness briefs to clients and Wapack executive management. Dream Team Technician, Cisco Cisco April 2015 to July 2015 Deployed 500+ Access Point Wireless Network across the San Diego Convention Center and built out NOC/SOC for Cisco Live event. Technology Consultant II HP Enterprise Services April 2010 to October 2011 Vulnerability Assessment and Remediation cycle SME for Navy NMCI Windows Platform Team. Brought patch compliance rate from 60% to 95% in 120 days, also brought remediation cycle from over 60 days to within 30 days, also achieving SLA requirements. Also assisted with HP C&A team on providing artifacts for ATO renewals as needed. System Administrator, SESI Aranea Solutions May 2009 to April 2010 Designated IASA and vulnerability management technician for Joint Navy/Army cloud data application JTDI. Achieved ATO for enclave and application within one year as requested. Provided daily reports on security stance and drove monthly vulnerability cycle. Network Analyst, Alutiiq Aluttiq December 2008 to April 2009 Monitored several IDS, HIPS sensors, and SNMP monitors for unauthorized access, outside attacks, worm and trojan activity. Discovered APT through forensic and SEIM tools. Created incident tickets and forwarded cases to incident handlers. Help Desk Technician II, SAIC IASO July 2007 to December 2008 Designated IASO for Army CIO/G6 Help Desk. Completed 600+ thin client rollout for SMDC/CENTCOM. Provisioned virtual desktop and legacy GOTS applications through Citrix. Assisted IA team with patch compliance and thin client image upgrades; automated management through Altiris. Two-time recipient of CIO/G6 recognition award. Education San Diego Community

College - San Diego, CA June 2014 Bachelors in Network Management Virginia College - Huntsville, AL April 2007 to April 2011 Skills Ids, Metasploit, Nessus, Nmap, Siem, Wireshark, Css, Cisco, Citrix, Vmware, Openview, Virtualization, Html, Javascript, Python, Scripting, Altiris, Linux, Unix, Bash Additional Information SKILLS SIEM - FortiSIEM, NetDefender, ELSA, and Suricata. IDS - FortiAnalyzer, Cisco Firepower, BlueCoat Proxy, JIDS (GOTS Unix based IDS), and Bro. Forensic - Wireshark and Nikto NetForensics. OS - Windows Server 2003-2008, RHEL, Ubuntu, SecOnion, and Kali Linux. Vulnerability Assessment - Retina, DISA Gold Disk, Nessus, Nmap, and Metasploit. Virtualization - VMWare, Citrix Automation - Altiris, HP Openview, Ansible Scripting - Bash, Python, YAML, CSS, JavaScript, HTML 5 Cloud - AWS, Google Cloud Endpoint - Crowdstrike Falcon, Minerva, ESET Enterprise Server

Name: Karen Harris

Email: clarkjoyce@example.net

Phone: 432-365-2126x086