Cyber Security Analyst II Cyber Security Analyst II Cyber Security Analyst II - BAE Systems Inc Reston, VA Authorized to work in the US for any employer Work Experience Cyber Security Analyst II BAE Systems Inc - Reston, VA August 2015 to Present Part of the Global Security Operations team network traffic monitoring and incidence response team. Daily tasks include active network traffic monitoring across all potential vectors of compromise (DMZ, host based, email, web based, and insider threat.) Protecting the company from both advance threat actors, generic/commodity based crime ware, and malicious intent and through investigation and enforcement of acceptable use policy. Primary responsibly include: recognizing and investigation of potential compromise including comprehensive report for each incident investigated, recommendation of further actions if needed, write up and facilitation of remediation work order. Ancillary responsibility include: Creation and revision of standard operating procedures, training of new hires on custom environment and tools specific to BAE GSOC in the form of quarterly brownbag/knowledge transfer sessions. Daily analysis technique for investigation of potential intrusions: Establishing time of events, process walk-backs, rule and indicator lookups, pcap analysis Malware samples, capture of malicious traffic and C2 beacons for content creation, investigation of malicious webpages; . Tools used on a daily basis: ArcSight ESM, ArcSight logger, Cisco IronPort, Wireshark, Out of Band system (Linux based VM sandbox environment running Win7, Win10), FireEyeHX, Redline, RSA Security Analytics, Confluence, JIRA, Sourcefire Snort. Understanding of common attack vectors/exploitations, web based attacks and exploitation vectors, covert channels, data exfil techniques, Advanced Persistent Threats, malware infections and propagation privilege escalation techniques, etc. IT Support LogMeIn, CentraStage, Office - Reston, VA May 2015 to Present 1099 Contractor Manage and support network infrastructure of over 300+ hospitals and doctors telecommunications video equipment and software maintenance. Active directory provisioning user management including creating, maintaining and decommissioning users. Data center maintenance: change request, break fix, device switchovers, cable management / general upkeep. Direct support for doctors and hospitals in setup, upkeep and troubleshooting. Daily use tools: Zendesk ticket management system, OASIS VersaSRS, LanDesk, WASP asset management,

VidiStar Imaging, Cisco Telepresence VCSE, LastPass, Vyopta, ConnectWise, Active Directory, 3CX, Zoom, Polycom RealPresence Tandberg/Cisco SX series codec, LogMeIn, CentraStage, Office 36. Network Engineer Aston Technologies - McLean, VA July 2014 to February 2015 Primary focus on Cisco networking gear with emphasis on route switch and data engineering support. Understanding of common networking protocols:RIP, EIGRP, OSFP and BGP. Configuration and maintenance of basic LAN/WAN infrastructure, including but not limited to DHCP, AAA, VLAN nomenclature, IP addressing, VPN, QOS, NAT, ACL, Frame Relay, STP, etc. Junior level network design with emphasis on level 1, 2 and 3 of the OSI model, Greenfield design, migrations, and disaster recovery. Network optimization efforts: software upgrades, device compatibility checks, best practices, and security advisories, deployment guides. Worked closely with vendors on projects to ensure they were meeting contractual obligations. Worked closely with clients and management to ensure technical requirements meet business needs Education Bachelors of Science in Biology George Mason University - Fairfax, VA Skills Cyber Security, Information Security, Siem Certifications/Licenses Security+ Certified Ethical Hacker (CEH)

Name: Lindsay Smith

Email: joshuanielsen@example.net

Phone: 001-955-496-3145