Cyber Threat Detection Analyst, Co-op Cyber Threat Detection Analyst, Co-op Information Technology Analyst Rockville, MD Professionally-certified cyber security technologist with knowledge and experience in information security operations; threat intelligence; malware detection and analysis; systems development and analytics, and other security solutions to ensure the safety, security, and resiliency of critical data and infrastructure. Authorized to work in the US for any employer Work Experience Cyber Threat Detection Analyst, Co-op Institutional Shareholder Services - Rockville, MD August 2018 to Present Performing threat intelligence research on log/packet flow/endpoint data sources to identify security anomalies and deploying automated processes to detect and remediate intrusion and data exfiltration attempts. Conducting network security tests focused on end-user safety, and simulating malicious attacks focused on enhancing security awareness across the firm. Facilitating systems security scans and audits, and recommending countermeasures to mitigate threats, risks, and vulnerabilities. Developing and validating security documentations, including standard operating procedures, system security requirements definition, and system security plans. Intelligence Analyst, Grad. Intern General Dynamics Information Technology - Arlington, VA June 2018 to August 2018 Deployed diverse methodologies to collect and analyze OSINT across 30+ digital platforms, such as social media, geospatial datasets, and traditional media, geared towards briefing national security decision-makers across the intelligence community. Developed intelligence products from threat assessments, vulnerability analysis, and system metrics for rapid implementation across U.S. national security sectors. Collaborated with Defense and Intelligence providers to conduct human intelligence research on technologies, tactics, and procedures of adversaries relevant to the intelligence community, then created a clear and actionable documentation for executive-level implementation. Information Security Analyst, Co-op Institutional Shareholder Services - Rockville, MD January 2018 to May 2018 Triaged and responded to security events and alerts, and configuration data to determine impact, credibility, and likelihood of threats to systems and data. Tested compliance baseline for 2,000+ global workstations and network infrastructures using tenable, and audited assets for adherence to security benchmarks. Provided analytical support for

the management of malware protection utilities, including Web and Email Gateways, Domain Blocklist and Whitelist, and the interpretation of reporting metrics. Supported the Director of Information Security to investigate and mitigate emerging threats by updating security controls, authoring 350+ pages of technical security plans, standard operating procedures, and security assessment reports. Information Security Engineer, Intern JPMorgan Chase - Wilmington, DE June 2017 to August 2017 Tested and implemented cyber-incident response procedures and standards to assure the integrity and availability of applications processing over $100 Billion across multiple lines of business. Conducted full-stack research and analysis on emerging application vulnerabilities, and tested systems to verify adherence to security patching processes. Curated data on secure coding practices and collaborated with software developers to create a web application for security awareness training of over 200,000 end users across all lines of business. Updated the global financial services sharing and alerting database with newly researched, defined, and documented cybersecurity risks, threats, and vulnerabilities. Cyber Intelligence Analyst FS-ISAC - Reston, VA May 2016 to September 2016 Conducted daily security monitoring of cyber systems: intrusion detection and prevention (IDPS) systems, log management systems, firewall and email applications. Performed investigative malware analysis and deep-dives on IOCs, TTPs, and Headers to create intelligence reports explaining malware behavior, infection framework and trajectory, and recommended system hardening protocols to secure government and corporate members. Streamlined new hire safety and security awareness training by developing SOP documentations highlighting information security and privacy best practices. IT Systems Analyst, Co-op TAI PEDRO and ASSOCIATES - Silver Spring, MD May 2011 to August 2012 Researched secure network architecture standards and protocols from NIST s database and implemented approved architecture to design enterprise network backbone, with focus on data and infrastructure security. Collected and analyzed systems traffic behavioral data to monitor host-based and network-based traffic performances and determine normalcy and irregularities. Collaborated with network engineers to gather data on network repair tickets, and reviewed use-case documentation to create system interaction models used to streamline system configuration procedures. Education

Master's in Cybersecurity and Systems Engineering University of Maryland-Baltimore County - Rockville, MD August 2017 to August 2019 Associate in Cybersecurity Engineering Frederick Community College - Frederick, MD August 2015 to December 2016 Bachelor's in Applied Physics Drury University - Springfield, MO August 2009 to August 2014 Skills Customer Service, Commited, Working, Loss Prevention, Network architecture development (2 years), Information Security Best Practices (2 years), Privacy Engineering (2 years), Python Coding (Less than 1 year), CompTia Security+ (2 years), Systems Design and analysis (3 years), Dhcp (2 years), Log File Monitoring (2 years), Disaster Recovery (2 years), Security event and protocol documentation (2 years), Incident Response Management (2 years), Firewall Configuration (2 years), Intrusion Detection and Prevention (2 years), Malware Hunting and Analysis (2 years), Metasploit (1 year), Microsoft Office (10+ years), Infrastructure Security Design (2 years), Root-Cause Analysis (2 years), SOP Development (3 years), TCP Dump (2 years), SPLUNK (2 years), Systems Use-Case Analysis (3 years), TCP/IP (3 years), Security UX/UI (Less than 1 year), VLAN (2 years), Wireshark Configuration Management (2 years), SOC/NOC Analyst (2 years), NMAP (2 years) Certifications/Licenses CompTIA Security+ April 2016 to April 2019 Information Systems Security Certification. Additional Information Secret Clearance, ACTIVE. Eligible to obtain Top Secret Clearance.

Name: Emily Davis

Email: lisayoung@example.net

Phone: +1-599-646-1147x743