Security Engineer Security Engineer Security Engineer - Tetrad Digital Integrity, LLC Bethesda, MD Capable and reliable Security Engineer with an exceptional attention to detail, prepared to take on new challenges and responsibilities. Adept communication and team skills. Ready to learn new concepts and ideas. Authorized to work in the US for any employer Work Experience Security Engineer Tetrad Digital Integrity, LLC - Alexandria, VA January 2017 to Present Job Summary: Security Engineer on a 12 member contracting team supporting security functions (compliance, security engineering, and incident response) for the USDA Food and Nutrition Service (FNS) Information Security Office (ISO). Currently on a five member team on the technical engineering side, providing support for the FNS SOC. The FNS SOC is responsible for deploying and maintaining technical solutions, monitoring activities, enforcing policies, reporting, and incident response. FNS has multiple data centers and regional server rooms, 2400+ workstations, 400+ servers, 2000+ users, and public facing web applications that the SOC monitors for possible breaches. Responsible for web content filtering and DLP. Utilized Forcepoint to monitor web activities and report those activities that require special attention for further investigation. Work with senior engineer to design and deploy DLP. Lead efforts to gather requirements and successfully implement plain text PII scanning on servers and workstations. Develop reports and dashboards in Splunk for the team and upper management. Information includes: Active Directory user machine trend analysis, remote user connectivity graphs, web activity charts, incident response management, unsupported software products or versions, vulnerability and patch management data. Utilize lookup files to improve report capabilities. Provide support and guidance for FNS vulnerability management efforts. Leverage Tenable and IBM BigFix to generate vulnerability reports. These reports are sent to remediation team and system owners. Support incident response capabilities and functions. Investigate alerts from Cisco FirePOWER (IPS) and Forcepoint. Monitor and respond to emails and tickets sent to the security incidents mailbox, regarding potentially malicious activities like spam, phishing attempts, and malware. Analyze packet captures to further investigate threats and troubleshoot issues. Implement Active Directory data to be imported into SQL Server 2014 database using PowerShell scripts, stored procedures and scheduled jobs for data collection to

enhance business information reporting capabilities. Key role in maintaining agency s green rating on the USDA cybersecurity scorecard. FNS was one of the very few agencies out of 33 that maintained a green rating on its scorecard in FY17. Success was partly due to superior critical and high vulnerability management, low phishing click rates (USDA exercise), low count of incidents older than 30 days, and high percentage of configuration management compliant machines. Provide recommendations to the client by evaluating costs, compatibility, usability, and capabilities for security tool replacements. Provide support and assistance as a liaison between the USDA and FNS, to configure and implement security tools (ForeScout CounterACT and Splunk) for the CDM project. Create and maintain standard operating procedure (SOP) documents for the team. Work closely and guide newly on boarded employees, using these documents. IT Support Analyst Citrin Cooperman - Bethesda, MD May 2016 to January 2017 Remediated hosts that appear on the Dell SecureWorks Enterprise iSensor incident report as a member of the incident response team. Developed company-wide group policies to standardize workstation and server configurations. Utilized LANDESK to push patches and security updates to all workstations and servers. Managed workstations in McAfee's ePolicy Orchestrator (ePO) for client proxy, HD encryption, site advisor, and DLP. Established client portals for secure document exchange between internal users and external clients. Created user accounts for new employees and disabled user accounts for employees leaving the firm. On-boarded new hires by introducing IT rules and behavior. Installed AirWatch application on user mobile devices (BYOD) and managed their profiles using the AirWatch Console. Managed Mitel phone system for the office using the Mitel 5000 Communications Platform. Provided solo on-site technical support for 70+ end users and remote technical support for 700+ end users in the other regional offices. Desktop Support HumanTouch, LLC - Silver Spring, MD December 2015 to May 2016 Diagnosed and resolved routine hardware and software issues. Reimaged and configured laptops with the necessary software and applications according to the user's requests and needs. Performed application and software installs and updates. Managed ticket requests via phone, email, and the intranet through HP Service Manager. Received acknowledgement and awards for work ethics, work performance, and

team support. Provided excellent customer support for over 4,000+ end users. Financial Analyst Pennsylvania Multifamily Asset Manager - Bethesda, MD October 2013 to December 2015 Analyzed property audit reports for trends and variances in expenses and revenue. Forecasted rent adjustments based on property operating costs using general ledgers, invoices, and bills. Acted as a liaison between the U.S. Department of Housing and Urban Development (HUD), Pennsylvania Housing Finance Agency (PHFA), and property owners/management agents. Processed Section 8 contract renewals and yearly rent adjustments associated with HUD's Performance Based Contract Administration (PBCA) program. Managed and prioritized 80+ different properties with expiring funding each month. Education Bachelor of Arts in Economics University of Maryland - College Park, MD September 2009 to May 2013 Skills DLP (Less than 1 year), Web Content Filtering (2 years), Tenable (2 years), SQL (2 years), PowerShell (2 years), VBA (2 years), Network Security (2 years), Vulnerability Nanagement (2 years), Splunk (2 years), Information Security (2 years), Windows Server (5 years), Linux Server (2 years), SIEM (2 years) Awards USDA FNS Administrator s Award 2018-06 Vulnerability and patch management team. Certifications/Licenses CCNA Cyber Ops May 2018 to May 2021 Splunk Certified Admin Present CompTIA Security+ July 2017 to July 2020 Additional Information Languages: SPL (Splunk), PowerShell, T-SQL, VBA Tools: Splunk (SIEM), Tenable Nessus (vulnerability scanner), Forcepoint (web content filtering and DLP), ForeScout CounterACT (hardware asset management), Tripwire Enterprise (file integrity), FireMon Security Manager (configuration integrity), IBM BigFix (endpoint management), WireShark (packet analyzer), nGeniusONE (packet analyzer) Networking: TCP/IP, VLAN, DMZ, Routers, Firewalls, Switches Operating Systems: Windows, Linux (RHEL and CentOS)

Name: Amber Kim

Email: melissalyons@example.net

Phone: (929)608-7605x938