Cyber Threat Analyst Cyber Threat Analyst Cyber Threat Analyst - BlueVoyant Arlington, VA Seeking a remote or partially remote Cyber Security role with an organization that promotes learning and growth and needs a highly motivated, skilled professional. My experience ranges from working in a SOC, to conducting FedRAMP security assessments, to assessing third party risk, to working as an analyst at a threat intelligence startup.  Special interests include threat intelligence, third party risk, and vulnerability management. Certifications include CompTIA CSA+, Security+, A+, and Cloud Security Alliance' CCSK. Work Experience Cyber Threat Analyst BlueVoyant July 2018 to Present Work in a startup environment and conduct research into new data sources and tools that can be used to supplement and enrich current analytics.  Work with developers, data scientists, and other analysts to create new security risk products and analytics to be used by clients.  Assess the threat implications that adversary campaigns pose to particular sectors, customers, and networks. Conduct web application vulnerability tests and provide mitigation steps to clients.  Produce third party risk reports used by clients when conducting M&As and vendor assessments.  Produce reports with technical accuracy and analytic precision about clients' risk profiles, threat actors' capabilities, motivations, and identities and Cyber events details and attribution.  Produce high-quality threat intelligence reports for range of audiences from network defenders to corporate executives. Operate and populate a structured threat intelligence repository.  Work with analytic developers and data scientists to help automate threat detection, analysis, and tracking.  Support managed security services and incident response efforts by providing threat research and expertise. Ensure that network defenders have sufficient contextual threat knowledge to take corrective action. RELATED EXPERIENCE Senior Cyber Intelligence Analyst LookingGlass Cyber Solutions Inc June 2016 to July 2018  Conduct vendor assessments to determine level of third party risk associated with vendors and partners. Reports include analysis of vulnerabilities in externally-facing applications, evidence of system compromise or infection, compromised user accounts, domain portfolio and spear phishing risk, and online and dark web chatter relevant to the client.  Conduct open-source research into threats, risks, and trends around information technologies to produce analytical reports.  Conduct custom cyber intelligence investigations for a portfolio of Fortune 500 clients, such as research into threat actors, malware, incidents of compromise, suspicious domains and emails, and general threat analysis.    Conduct web application vulnerability tests and provide mitigation steps to clients.    Serve as a senior analyst on a team to generate strategic-level Cyber Threat Intelligence reports and presentations for commercial leaders.    Identify and pivot off incomplete or unreliable technical and non-technical evidence found on the open Internet and Dark Web to formulate reasoned assessments. Ensure reports display analytical soundness, technical accuracy, structural clarity, and timely completion.    Utilize proprietary LookingGlass tools to identify evidence of live or recent infections on client's network from botnets, viruses, and malware.    Leverage multiple open source, proprietary LookingGlass security tools, and Dark Web resources to conduct investigations on behalf of clients, including actor research, malware and general relevant Dark Web chatter.    Use proprietary LookingGlass tools to analyze data and create actionable reports.    Conduct social media research and background investigations on persons of interest.    Lead a working group to produce biweekly reports on a variety of cyber security topics.    Conduct research on suspected malicious IPs, URLs, threat actors, tools, and more.    Produce Executive Threat Assessments using OSINT and proprietary tools to identify potential information security risks to executives and their family members. Additionally, provide insight into possible threats and risks originating from such sensitive disclosures and provided recommendations for mitigating their online risk profile. Cyber Security Analyst TruShield Inc - Sterling, VA June 2016 to September 2016    Monitor and analyze network traffic and alerts    Conduct research on suspected malicious IPs and URLs    Investigate intrusion attempts and perform in-depth analysis of exploits    Provide network intrusion detection expertise to support timely and effective decision making of when to declare an incident    Review security events that are populated in a Security Information and Event Management (SIEM) system    Analyze a variety of network and host-based security appliance logs (Firewalls, NIDS, HIDS, Sys Logs, etc.) to determine the correct remediation actions and escalation paths for each incident    Document all activities during an incident and provide leadership with status updates during the life cycle of the incident    Assist with the development of processes and procedures to improve incident response times, analysis of incident, and overall SOC functions IT

Security Analyst First Information Technology Services - Washington, DC August 2015 to June 2016 Worked as a Microsoft contractor to assist Microsoft Azure's FedRAMP cloud computing initiative Traveled to Microsoft's Headquarters to meet with clients and review system security plans. Applied the Risk Management Framework in order to get accreditation and certification of systems Ensured Microsoft Azure clients are compliant with Microsoft Office 365's System Security Plan Applied NIST 800-53 Rev 4 and other NIST publications to assist in creating documents Assisted in the development and review of system security plans for new acquisitions within Microsoft Azure Performed gap analysis on system security plans for a variety of clients Reviewed and assessed Plan of Action and Milestones (POA&M) Reviewed the development of other required system security plans: Configuration Management (CM), Contingency Plan (CP), Continuity of Operations (COOP), Disaster Recovery Plan (DRP) and Incident Response Plan (IRP) Cyber Security Intern Department of Homeland Security - Washington, DC May 2015 to August 2015 Worked directly with DHS HQ's Security Operations Center and assisted their Digital Media Analysis team with their reverse malware engineering and computer forensics efforts Assisted the Digital Media Analysis team at DHS HQ's Secure Operations Center in setting up Windows, Linux, and Mac OS machines tailored towards reverse malware engineering and computer forensics Reviewed DHS system vulnerabilities and remediated over 1,300 POA&Ms in a period of 3 months Reviewed Nessus scans conducted on DHS HQ's network Worked directly with the Authorization Reviews and Monitoring Ongoing Risk (ARMOR) division of the DHS HQ Assisted in the steps required to grant an Authority to Operate (ATO), along with the necessary steps to collect data, develop documents and prepare the Security Authorization Package for the Security Control Assessor (SCA)/AO Worked alongside contractors from First Information Technology Services and got offered full time employment with them after my internship IT Support Specialist MCAP - Fairfax, VA June 2014 to May 2015 Worked in a HIPAA compliant environment and ensured all IT systems and users were HIPAA compliant Managed Citrix sessions for over 300 users Managed all security permissions and changes made to accounts and containers using ADAudit Plus Inspected and managed emails through IronPort Email Security Provided support escalation and coordination directly with senior system and network engineers Created, modified, and managed user accounts, privileges, and organizational units in Active Directory and Microsoft Exchange Advised the IT Director on the purchase of IT equipment and software Completed and maintained documentation for an inventory audit of over 1,560 company-wide IT assets Education B.S. in Information Security George Mason University - Fairfax, VA May 2018 A.S. in Information Technology Northern Virginia Community College - Annandale, VA June 2014 Skills ENCASE, FTK, NESSUS, NMAP, QUALYS, Excel, Qualys (2 years), OSINT (3 years), Acunetix (2 years), Web application scanner (2 years) Awards DHS Certificate of Achievement 2015 Certifications/Licenses CompTIA Security+ CompTIA A+ Comptia CSA+ CCSK Additional Information SKILLS Systems - AlienVault SIEM, VMware, VirtualBox, Symantec, Azure, Active Directory, LookingGlass & BlueVoyant Proprietary Tools Applications - Acunetix, Qualys, WireShark, Nessus, IronPort, EnCase, Forensics Tool Kit (FTK), Intel471, NMAP Operating Systems - Windows 7/8/10, Mac OS X, Kali Linux, REMnux, Networks - Fundamental understanding of LAN/WAN, DNS, TCP/IP, DHCP, VPN/remote connectivity, router/switch configuration, and file and print sharing configuration. Database and Programming - Intermediate in SQL, Java, and PHP Hardware - Setup and maintenance of computers, servers, tablets/mobile devices, printers, scanners, peripherals, routers and switches.

Name: Mary Moore

Email: ericasmith@example.org

Phone: +1-275-379-7766