Cyber Surety Journeyman Cyber Surety Journeyman Cyber Surety Journeyman - USAF Tampa, FL Self-motivated student and IT professional with 5+ years' experience. Versatile skills including Cyber security, system administration and customer service. Highly motived and passionate about cyber security, always looking to sharpen my skills and remain current with emerging threats. Authorized to work in the US for any employer Work Experience Cyber Surety Journeyman USAF - Tampa, FL 2017 to Present Administer vulnerability management program, performing scans on two enclaves utilizing Nessus ACAS i.e. asset discovery, identification of vulnerabilities, and creating detailed reports Ensures relevant DISA STIGs (Security Technical Implementation Guides) have been properly implemented by various IT teams throughout the network and all nodes are within compliance. Performs risk management framework security determinations of fixed, deployed and mobile information systems utilizing NIST publications 800-37 & 80-53 and other DOD instructions Enforces national, DOD and Air Force security policies and directives to ensure Confidentiality, Integrity and Availability (CIA) of IS resources. Performed IT Security Administration functions, to include the administration, maintenance, and deletion of user accounts, permissions, and network resources. Analyze traffic flow patterns by capturing packets on the network using Wireshark to identify suspicious protocols or beacons from organizational workstations Cyber Security Analyst Bylight IT Professionals - Tampa, FL 2018 to 2019 Actively monitor Classified and Unclassified Networks for suspicious network activity using ArcSight ESM as well as ArcSight Logger. Utilize tools such as Bluecoat, McAfee HBSS, Splunk, Microsoft ATA, McAfee ATD, etc. to identify suspicious traffic traversing the network. Analyze intelligence reports from various sources, documenting indicators of compromise (IOCs) as well as updating Fortigate firewall to block malicious domains. Respond to security incidents/events in a timely and proactive manor to ensure proper mitigation of any issues. Generate detailed security incident reports and disseminate the reports in accordance with incident response and reporting standard operating procedures. Research latest threats using open source intelligence sources such as Mandiant, Sophos, Kaspersky, Cisco Talos, Malwarebytes Lab, etc. Periodically create and disseminate cyber threat advisories to ensure that the organizations members are aware of any threats/targets

that could affect operations. Service Desk Analyst Bylight IT Professionals - Tampa, FL 2017 to 2018 First line of support troubleshooting various software/hardware failures on six different Windows networks worldwide supporting 10000+ customers Log and track inquiries utilizing Remedy to identify, evaluate, and prioritize customer problems and complaints to ensure that inquiries are resolved appropriately. Perform adds, moves, and terminations for users in Windows 2012r2/2016 Active Directory including password changes, rights, access permissions, and user set-up and deletion Utilized Active Directory for the implementation of Group Policy to define, create and implement corporate wide security standards in relation to system core infrastructure Trained new employees on responding to calls appropriately, company standards, and pertinent metrics/service level agreements. IT Specialist United States Air Force 2014 to 2017 Provisioned, installed, configured, and maintained two servers, Microsoft Server 2012R2 and 2008R2, 147 workstations running Windows 7/10, and various other network peripherals that supported the Fuels Management Flight Upgraded client's hardware (motherboard, memory, power supply, etc.) upon performance analysis or users request to ensure adequate system resources were available Established semi-annual training program, educated 100+ personnel on various topics such as proper application operation, cyber security threats, and general assistance to end users leading to a greater awareness of users interacting with organization systems Mitigated 100+ vulnerabilities on Windows 2008/2012r2 utilizing DISA STIGs and Nessus vulnerability scanner which identified and ensured proper steps taken to address vulnerabilities Develop approved Standard Operating Procedures (SOP's) including escalation procedures for clearing various hardware and software platforms, as new requirements are identified or arise Education Bachelors of Science in Information Systems Security American Military University May 2016 Masters of Science Western Governors University Links https://www.linkedin.com/in/thughes86 Military Service Branch: United States Air Force Rank: E-6 Additional Information SKILLS/Tools Customer Service, Log analysis, TCP/IP, Vulnerability Management, Nessus Security Center (ACAS), McAfee e-Policy Orchestrator, Microsoft Office, Active Directory, Microsoft Exchange, PowerShell, Splunk, NIST RMF and DISA Security Technical Implementation Guides

Name: Kelsey Evans

Email: hayestimothy@example.org

Phone: +1-501-338-5384x8439