Cyber Security Analyst - SOC Cyber Security Analyst - SOC SOC Analyst New York, NY 24 Hour SOCm - Cyber Security Analyst Work Experience Cyber Security Analyst - SOC Office of Personnel Management - Washington, DC January 2018 to Present   Analyze activity observed on Akamai Web Application Firewall   Create detailed After Action Reports (AAR) for management.   Analyze PCAPs for malicious downloads and activity.   Analyze malware for IOCs   Identify and block malicious content in relevant security tools.   Monitor RSA NetWitness dashboard to respond and investigate alerted events.   Use RSA NetWitness to export Metadata and PCAP for analysis. Create Emergency Change Requests for urgent system/server remediation.   Investigate SPAM messages and perform header analysis.   Process Daily Actionable Intelligence information from the Homeland Security Information Network (HSIN) portal.   Grant, access, and manage local admin/privilege accounts.   Utilize CarbonBlack for investigating alerted events.   Use Forcepoint (Websense) to block sender addresses, release emails from DLP, manage user accounts, and block/allow access to websites.   Use various open source applications to assist in investigations. Chairperson emergency OCIO911 conference bridges.   Involved in the handling of leaked PII information. IT Specialist NIH Training Center - Bethesda, MD December 2016 to December 2017 Monitor, maintain, and update servers, computer networks, software, and hardware for computer-based training classrooms   Performed software installations and upgrades on all machines   Reimaged and configured all machines to be compliant with NIH guidelines   Set up Group Policy Objects on training network laptops to limit student permissions to alter basic settings, thereby ensuring proper functionality of systems.   Created and edited SOP's for the NIH Training Center and created training documentation to all students   PC Desktop support for students, client staff, and colleagues   Monitor and maintain necessary inventory and supplies such as printer toner/paper, batteries for various devices, mice, keyboards, etc.   Install desktop shortcuts/links required for a specific class' needs   Configure and support instructor and student use of Skype for Business, Lync, WebEx or other remote participation software   Attend monthly meetings with the OHR staff at various locations in the Rockville/Bethesda area to discuss upcoming technical initiatives or modifications to training systems or set-up to ensure our classrooms are prepared to

accommodate any necessary changes   Monitor the LMS (HHS Learning Portal), Outlook, or SharePoint calendar to track scheduling of technical resources for classes, room rental and events and conferring with staff, clients, and vendors about setup.   Prepare student log-in materials, such as user IDs and passwords to gain access to certain computer training applications   Maintenance or creation of scripts connecting systems and websites via a daily-run data feed   Supporting Audience response hardware and software.   Instructor and technical services coordination; provide training room support before & during classes. Work with instructors to ensure all class needs are met before class starts, confirming with a signed checklist AV Technician National Institute of Allergy and Infectious Diseases - Rockville, MD September 2014 to October 2016   Responsible for providing technical support, training, and conducting routine maintenance of all NIAID/NIH audio visual assets including HD cameras, microphones, projectors and flat-panel displays, touch screens, Smart boards, speakers, amplifiers, PC's, Polycom & Cisco VTC systems in over, and video broadcast production systems. Also supported Skype for Business, Goto Meeting, WebEx, and other web based conference services.   Responsible for updating and maintaining peripheral inventory for all NIH conference rooms. Serves as the first point of contact for troubleshooting hardware and software issues, as well as AV and VTC systems, and applications using PC and Mac operating systems in over 150 conference rooms.   Responsible for creating SOP's used for all A/V technicians   Installs hardware and software related to conference room audiovisual and video teleconferencing facilities and maintains associated network, computers, peripherals, and audio and/or video equipment.   Provided training to new employees and clients on all equipment Operated video switching, cameras, provided live video broadcast for remote users and trained technicians on video broadcasting.   Resolved and closed all help desk tickets in a timely manner Utilized knowledge of system characteristics to provide advice on AV and VTC requirements in various usage and conduct of review, and analysis of overall equipment and system performance to ensure its satisfactory operation. IT Specialist NAVFAC Washington - Washington, DC May 2010 to July 2014   Gathered all inventory data including labeling all NAVFAC equipment, performed data entry tasks, created and maintained inventory database.   Resolved and closed all help desk tickets

in a timely manner   Performed software installations and upgrades on all machines   Experience with wireless-accessibility through Sequel Server (SQL) database back end in real time. Performed queries and updated tables in an inventory database to gain knowledge necessary to troubleshoot and resolve issues.   Assisted with configuring Group Policy objects to create a secure infrastructure.   Processed all labor data files through the labor error database. Provided helpdesk assistance to all NAVFAC employees. Performed daily updates to the NAVFAC Labor Error Databases.   Installed wireless internet cords on all NAVFAC laptops, provided helpdesk support for all NAVFAC employees, Advanced training in Video Teleconference (VTC) equipment and various peripheral devices (i.e., laptop computers, CPU's, wave I, wave II cameras).   Performed daily & weekly monitoring of remote devices in all Video Teleconferencing rooms, including hardware and software installation. Performed network testing and maintaining computer software and hardware profiles for end users (i.e., printers, scanners, copiers and digital senders).   Provided complete troubleshooting and problem resolution for any software/hardware issues. Updated peripheral units, general software updates, actualizations and latest anti-virus releases   Improved organizational performance by assuring validation of all processes and qualification of equipment is performed in accordance with established protocols. Voice and data transmitted on networks using the Internet Protocol (IP), such as the Internet itself or a corporate/government intranet. Serviced many handhelds and wireless devices such as cellular phones (iPhone/Android) and PDA's, Smart boards and Bluetooth systems. Maintained cell phone manager database.   Researched and developed design elements, assay, process, and method parameters.   Developed and maintains all documents pertaining to validation, qualification, maintenance, and calibration.   Assisted in equipment selection, specification, and negotiation of competitive pricing. Developed detailed standard operating procedure (SOP) for (NAVFAC) Navy PWC. Education Frostburg State University - Frostburg, MD August 2009 to May 2011 Certifications/Licenses Security+ July 2018 to July 2021 Additional Information Wireshark   Forcepoint Threatseeker (Websense)   SentinelOne   Palo Alto   RSA NetWitness   CarbonBlack   Akamai WAF   Cylance   Solarwinds   Microsoft SQL Server   Active Directory / Group Policy   Windows Server 2003-2016   BMC Remedy

Typing: 51 WPM   CIO Helpdesk   IT Asset Inventory   Spiceworks   Windows 97-10 / Mac OS X

iOS / Android / Blackberry   Nessus Vulnerability Scanner   Skype for Business   SCCM   Digital

Certification Creation using PKI   Microsoft Suite 2010-2016

Name: Travis Villarreal

Email: bhuff@example.net

Phone: 2095545563