

Cyber Analyst Cyber Analyst Cyber Analyst - ISHPI Inc Springfield, VA Work Experience Cyber Analyst ISHPI Inc May 2018 to Present Running SCAP scans on system owner's systems using SCC tool and ACAS POAM Management and Tracking - create/manage/track POAMs for open/mitigated findings for systems owners Reviewing systems owners findings in ACAS and creating reports on these findings Reviewing systems owners artifacts/documentation with eMASS Assist system owners in prepping for CCRI's by reviewing current open findings and discussing score increases for remediating findings Assist on tasks with HBSS team Conducts STIGs and scans on HBSS POA&M enterprise servers, McAfee ePO, IAVA's, STIGs, Vulnerability scans. Managed STIG compliance activities for various host products Performs vulnerabilities scans Provide analytical support to critical infrastructure incident response activities led by DHS Guiding the development of information security standards, guidelines, and policy Perform multiple sites to conduct CCRI Perform CGCyber Task Order until It is 100% compliance Familiar with DISA CCRI standards Provide information systems security authorization support to DHS/USCG facilities, conduct evaluations and assessments, and perform documentation support services Provide Cyber Security support services to the Command, Control & Communications Engineering Center. Complete and monitors TASK Orders, Top Offenders vulnerabilities. Create tickets in Remedy as needed. Conducts Plan of Actions and Milestones as needed. Create scans and remediated vulnerabilities. CCRI Present Cyber Security Analyst / ACAS Admin NetCentrics LLC May 2017 to May 2018 Provide ACAS scanners, NESSUS scanners, and Security Center support telephonically, remote access, and/or on-site as necessary. Create, implement, and maintain standards for maintaining security posture for ACAS and Linux OS Experience with vulnerability management and remediation tools; preferable Tenable Nessus and Security Center. Maintain accurate, current information regarding all ARL CDSP subscriber networks, provide recommendation for hardening the networks, and provide information and resources to develop subscriber cyber defense training materials. Track changes or updates to the INFOCON and/or CPCON level and report compliance to tier 1 for all CDSP subscribers. Perform and analyze monthly vulnerability scans of subscriber networks and provide monthly trending reports along with

weekly status updates. Ensure compliance with Communication Tasking Orders (CTO) Harden and assess operating systems, databases, web servers, web applications, and other IT technologies using DISA IASE STIGS and SCAP and STIG Viewer. Perform work on Pivot table Perform weekly Top 30 Vulnerability and Risk score reports on unclassified and classified network. Prepare reports for subscribers to assess technical configuration and compliance Performs monthly vulnerability scans of unclassified and classified network subscriber enclaves Document findings and severity levels of non-compliance in formalized reporting, written and oral briefs Assists subscribers with vulnerability remediation, as necessary Assist Vulnerability Management Program Lead with the day-to-day operations of the customer IVAM, CTO, and compliance program Conduct vulnerability assessment against the customer network Track and Assess USCYBERCOM TASKORD until completion Generate vulnerability assessment reports for the JSP customers and subscribers needed Assist with the response to USCYBERCOM, JSP, and Federal mandates Possess knowledge of Microsoft Office products Responsible for tracking all risks within the JSP networks to include POA&Ms, DRA, and exceptions Familiar with DISA CCRI standards Develop metrics and presentations upon request Participate in cyber threat working groups, forums and meetings Participate in vulnerability management working groups and meetings System Administrator / Security Analyst DirectViz Solutions LLC- Defense Information Systems Agency August 2014 to May 2017 Perform IAVM scans using ACAS Create POA&M for vulnerabilities Perform STIG scans using SCAP Perform STIG scans using ACAS, create policies in ACAS Responsible for building and maintain a Windows Server 2003, 2008, and 2012 Active Directory environment on multiple classifications for DoD at Fort Meade, DISA. Installing, configuring, and hardening Windows Servers and workstations using DISA Gold Disk. Patching and STIG'n using DISA Information Assurance Vulnerability Management (IAVAM) Program. Ensures that user's workstations and Servers have the necessary IAVA patches and do not have unauthorized software installed. Deploy Implementation Plans for GTMS (Remedy) before it comes out to production. Build servers for tests environment, mainly are for the govts. Service Desk / Systems Admin NetCentrics LLC July 2012 to July 2013 Setup security policies for users

Configure, install, migrate, and deploy Windows 2007 clients and Windows 2008 servers
Responsible for first-level network administrative task including creating/deleting user accounts, resetting password, and access control from Active Directory Perform system backups, data recovery, server upgrades and update patches using Backup Exec 2010 R3 with Dell tape Library
Managed user network shares, permissions, and quotas Established remote desktop sessions to laptops and workstation, performed troubleshooting/installation of needed software Develop system and network diagram, server room diagram and flowcharts using MS Visio Provides quality support to end users on a variety of IT related issues Responded to telephone calls, walk-ins and emails for IT technical support Perform project task such as moving the entire office users to new locations Windows migration IT Support and Geographic Information System User SuprTEK Inc - Ashburn, VA November 2010 to July 2012 Provided systems administration support for Windows Systems including server and workstation upgrades, backup and disaster recovery monitoring, user account setup and security administration Performed regular system backups and recovery procedures, closely following SOPs to ensure system security Installed, configured, and updated servers: Exchange Server 2003/2008, Active Directory File Server, Print Server, Sharepoint 2008
Performed test and evaluation of different and hardware products: ArchGIS, MS Sharepoint, McAfee, Sysmantec, EMC Storage Solutions, Dell, HP, and Cisco Firewall Ensure the servers, desktops, and laptops are up-to-date with security patches Perform servers STIG in compliance with DoD policies and regulations Manage LAN infrastructure - switches, wireless devices, printers, desktop/laptop Develop installation procedures and quick reference guide Responsible for creating maps of service areas using ArcGIS Desktop 9.3 Skills Active directory, Dns, Dhcp, Splunk, Mapping

Name: Jaime Lewis

Email: brentobrien@example.com

Phone: 5065512270