

Cyber Security Analyst III Cyber Security Analyst III Cyber Security Analyst III - ASM Research Inc
Seagoville, TX Information Security professional with over 15 years of professional experience supporting enterprise information systems, FISMA compliance, Assessment & Authorization, and network architecture in the Government space. Mr. Newton is an expert at analysis, coordination, review and documentation of incident reports, providing recommendations to strengthen security of Information Systems, leadership capabilities highlighted by the oversight of 4 separate medical & financial Information Systems, and coordinating with ISSO's, Program Managers and other security staff. Authorized to work in the US for any employer Work Experience Cyber Security Analyst III
ASM Research Inc September 2015 to Present Provide Direct Site Support to the Veteran Affairs Healthcare System's facility ISSO with related ISSO duties to include, but not limited to the activities below: Review of Media sanitization forms to ensure this meet security control requirements. Assist in the review and updating of Memorandums of Understandings (MOU)/Interconnection Security Agreements (ISA) that address federal security requirements and documentation of security controls across interconnected systems to ensure confidentiality, integrity, and availability of VA networks and data. Coordinate and collaborate with the Facility's and vendor POCs to create, update, and review Local MOU/ISAs and Air Gaps. Provide support on performing required Audits and the preservation of evidence in accordance with the RACI list, the Facility's SOP and the ESO SOPs. Update RiskVision (GRC) evidence at the beginning of the fiscal year EOC Rounds. Assist on the yearly updating on the facility's Local SOPs Inspect all Network Closets and Server rooms for potential problems or risk. Coordinating and maintaining the documentation for the Security Assessment and Authorization (A&A) process for each system. Working with the system owner and Subject Matter Experts (SMEs) to ensure security issues are addressed in a timely manner. Performing gap analysis of current controls and processes. Document and inform management of changes are needed or recommended. Presenting periodic reports to management on the security posture. Site Administrator for VA ITOPS SFFX (Shared Folder and File Exchange) for all things PBC/CAVT. Support OIT ITOPS SO EUO SQS Operational Policy and Security. Lead the implementation of security programs designed to anticipate and minimize

system vulnerabilities. Review proposed new systems, networks, and software designs for potential security risks; recommend mitigation or countermeasures and resolve integration issues related to the implementation of new systems within the existing infrastructure. Develop contingency plans (Disaster Recovery or Business Continuation Plans for information technology systems) to ensure availability and accessibility of network resources. Assist in developing SOPs and enterprise training material in support of security auditing, POAM reviews, Authorization to Operate (ATO) processes, and Assessment and Authorization, and report the impact and benefits to the field security professionals. Develop long-range plans for IT security systems that anticipate, identify, evaluate, mitigate, and minimize risks associated with IT systems vulnerabilities. Coordinate the implementation of security programs across Tier I, II, and III systems, and establish vulnerability reporting criteria. Review security incident response policies and identify the need for changes based on new security technologies or threats. Implement security requirements, integrate security programs and define the scope and level of detail for security plans and policies. Monitor their organization's networks for security breaches and investigate a violation when one occurs. Install and use software, such as firewalls and data encryption programs, to protect sensitive information. Prepare reports that document security breaches and the extent of the damage caused by the breaches. Conduct penetration testing, which is when analysts simulate attacks to look for vulnerabilities in their systems before they can be exploited. Develop security standards and best practices for their organization. Assist client with installs of and training on new security products. Monitor health of Microsoft and VMware Servers, both physical and virtual including OS, management, hardware and software. Administer Microsoft server applications including Exchange, Lync, SharePoint, SQL and System Center. Installation and configuration of server hardware, OS and ISV software and network. Troubleshoot network and system problems, via phone, remote access or site visitation, if necessary. Perform routine maintenance functions, including audits and system maintenance. NOC Engineer; IT/Desktop Technician Verigent, Inc July 2015 to September 2015 Install network cable and network equipment in retail and office environments. Performs testing and certification of installed components. Troubleshooting,

maintenance, repair, and recovery of failed IT hardware in live retail and office environments.

Deploy new desktops and setup local and network printers. Install, configure, test, maintain, monitor, and troubleshoot end-user and network hardware, peripheral devices, printing/scanning devices, presentation equipment, software, and other products to deliver required desktop service levels. Ensure that desktop connection, i.e. network jacks are in proper working order.

NOC Engineer Eze Castle Integration, Inc March 2015 to July 2015

Responded to action alerts from centralized management system to maintain health of platform On boarded new clients to the platform, ensured proper installation and configuration of our monitoring software Assisted in troubleshooting WMI and SNMP on company and client systems Provided weekly status updates on outstanding tickets and current projects Troubleshot, evaluated, tracked, and managed network problems and recommend the best solutions while escalating to higher tiers according to Net Ops procedures Performed initial troubleshooting, problem analysis and isolation of network and system events in accordance with Net Ops incident management guidelines Support and maintenance with UNIX and Linux servers Provided quality, timely and accurate end-to-end support of any issues within functional area of responsibility-this includes (but not limited to) phone, email and documentation/tracking of the incident in the ticketing system Escalated outage events and or impairments to appropriate individuals and organizations, when not resolved in the prescribed amount of time Monitored and tracked scheduled network maintenance activities in applicable tools analyzing the duration and potential impact to customers and ensuring they are consistent with approved times for these activities

Support Tech A.D. Susman & Associates, Inc October 2014 to March 2015

Installed and configured (VOIP) Polycom Phone System Configured desktops and Laptops for Polycom BTOE software. Trained users on VOIP phones and Software within Microsoft Lync. Deploy and train users throughout DISD.

Network Operations Center Analyst A.H. Belo Corporate Headquarters January 2014 to June 2014

Provided front-line support to NOC customers by answering calls and technical questions and assisting with basic configuration issues Monitored and respond to managed network alarms, traps, or conditions Responded to, and escalated managed or DCN network outages as appropriate Conducted

follow-up analysis on unresolved customer issues or escalates matter to the next appropriate level of support Reviewed network data reports and take the appropriate corrective actions

Proactively provided network performance monitoring and analysis Created, maintained, and provided detailed customer services records on all problem conditions reported on managed and DCN networks Support and maintenance with UNIX and Linux servers Under limited supervision, responsible for the monitoring of servers and systems in an environment requiring 24 X 7 X 365 uptime. Provided effective, efficient notification of production outages to internal and external clients via email and/or telephone calls. Follow established Standard Operating Procedures in response to system alerts and routine tasks with consistent accuracy. Recorded outages for daily review and send outage notifications internally and externally. Performed after hours On Call Basis Support as needed by the Management (on-call weekly rotation). Configured Antivirus software in the network for intrusion detection. Implemented and managed antivirus solutions for exchange and internet email gateway. Senior Support Analyst Lincoln Property Company February 2013 to January 2014 Troubleshoot IOS/Android issues. Troubleshoot Local Area Networks (LAN) and the relationship to desktop software applications (3+ years' experience). Installed and configured software such as Microsoft Office and Citrix clients. Troubleshot software, hardware and email related issues in both Windows and Linux. Update systems across the whole network with available patches and updates. Troubleshot software, hardware and email related issues in both Windows and Linux. Administered Windows NT Server environment Microsoft Exchange 5.5 and SQL server. Implemented and managed antivirus solutions for Exchange and Internet e-mail gateway. Configured Antivirus software in the network for intrusion detection. Resolved issues related to desktops, laptops, and applications loaded on workstations, utilizing remote connectivity and support methods. Resolved end-user issues, login problems for networks, email systems, and offer a full range of support for specialized applications. Education B.S. in Information Systems Security ITT College of Technology 2013 A.A.S. in Computer Networking Engineering Westwood College of Technology 2004 Skills Siem, Cyber Security, Nist, Information Security Additional Information Relevant Technical Skills: NIST 800-37 NIST 800-53

FISMA/FISCAM Risk Management Tools: Risk Vision (Governance, Risk, and Compliance) GRC,
EMASS, VMS, XACTA, NCAD

Name: Laura Taylor

Email: teresalivingston@example.net

Phone: 593-506-4580x94895