Cybersecurity Engineer III/Team Lead/Manager Cybersecurity Engineer III/Team Lead/Manager Cybersecurity Engineer III/Team Lead/Manager - University of New Mexico Hospitals Rio Rancho, NM Work Experience Cybersecurity Engineer III/Team Lead/Manager University of New Mexico Hospitals December 2014 to Present Hired to drive the strategy and implementation of a company-wide information security management programs while protecting the business from disruption, security threats and vulnerabilities. Empowered to select, develop, deploy and teach the NIST/CIS 20 Cybersecurity framework, NIST Risk Management Framework, Cloud Security Alliance framework, and to build a cybersecurity team, while creating and deploying Projects/Service Designs/SLA's to ensure the Hospital complies with Meaningful Use and ITSM based Security Operations Services. Provided enterprise cybersecurity architect role. As soon as I stated with UNMH, I had to step in and provide management of the Cybersecurity team while my manager who is a quadriplegic & blind and was in the Hospital for seven months; as a result I was invited to participate in the UNMH "Up and Comers" leadership program as part of the succession process when my manager retires in 2019. Developed a Cybersecurity defense in depth service/software portfolio based on the NIST Cybersecurity and Risk Management Frameworks centered on industry best practices and critical controls based on the current cybersecurity domains: Security and Risk Management, Asset Security, Security Engineering, Communications & Network Security, Identity & Access Management, Security Assessment & Testing, Security Operations, and Software Development Security. Developed the project planning, specifications/POC's and architectural leadership to deploy Endpoint Security/Encryption, Incident Response, Disaster Recovery, Pen-Testing, Logging and Alerting, Vulnerability Remediation/Exception Requests, Vendor/Product Security Risk Assessment, and development/deployment of all associated/required policies/procedures for all of UNMH/HSC. ITIL 3.0 based Service Design Portfolio. Daily Utilization of Mcafee Endpoint Complete Protection Suites (DLP, HIPS, Encryption, etc.), Nessus Scanner, Workspace1/Airwatch MDM, Splunk SIEM, and Security Center Vulnerability Remediation software, etc. to perform security monitoring, risk mitigation, and incident response (SOC/NOC). Provided lead in Data Segmentation development and policy development-enforcement for ePHI data security throughout the enterprise. Provided advanced vulnerability, compliance, and systems support/analysis as the Red Team leader for all Penetration Testing at UNMH/HSC. Utilized standard tools and methodologies, like Nessus Scanners, Nap, Kali Linux, Metasploit, Burp Suite, protocol analysis, and the utilization of other security penetration software. Designed and deployed a Pen testing "sandbox" environment for systems hardening, malware/ransomware investigations/forensics analysis. Provided Forensics analysis for HR and other related requirements. Utilized Splunk as the Blue/Red team lead to record and analyze red team attacks/analysis internally and for external auditing/assessment vendors. Provided hands-on & management to design, implement, document, and deploy a business/threat intelligence/analytics, performance standards, baselines, and metrics to to create the UNMH/HSC cybersecurity architecture, which required developing and managing 40 project plans within my first 6 months to meet the TrustCC/CLA Security Assessment/Audit findings & Coalfire PCI Audit findings to acquire Meaningful Use funding every year. Provided budget analysis, team lead, and hired/mentored/trained 5 direct reports to ensure the deployment of a Cybersecurity framework based on NIST, ISO, COBIT, SANS, CIS, CSA, HIPAA, PCI-DSS and other frameworks to ensure HHS & DHS security requirements/laws are met, i.e. Endpoint Protection (DLP, HIPS, Encryption, Firewall, AV) Log Management/Cyber Threat Intelligence (Splunk), Access Controls, Mobile Device Management, Vulnerability Remediation (CDM), etc. Submitted and administered the division's annual budget 1.2-2 million per year; monitor and approve expenditures i.e. initial FY2015- 2019 budget entered into StrataJazz, developing current budget analysis of current budget to ensure we purchase the remaining budget items before end of the Fiscal Year. Formulated, developed, and implemented/integrated a secure network and encrypted data storage systems based on development of technical security standards for computer and network systems, to include standards for infrastructure hardening, system security, and risk mitigation. Installed, configured, and deployed secure computer and network operating system and application software, as appropriate; deployment of Juniper Mag 2600VPN Gateway with MFA for the enterprise. 3 Led the IT teams to develop the cybersecurity strategy, methodologies and architecture to build a Hybrid cloud solution to utilize MS Azure with federated services connected to SailPoint RBMS through SAML/IAM internally and connect externally to SAAS/PAAS/IAAS vendor solutions. Communicated and collaborated with technical and non-technical personnel to understand and define user needs, gather and analyze data and recommend solutions. i.e. HSC-Wide Vendor Security Risk assessment workflow and check sheet analysis forms and online automation of this process. Utilization of industry standard PMP methodologies/standards, ITIL 3.0 and other industry standard PM methodologies/techniques. Provided planning, leadership, direction, and advanced technical expertise regarding systems security, while serving as primary point of contact and liaison with vendors; review vendor products, and coordinate and facilitate vendor interviews and presentations i.e. licensing of Mcafee ePO products, ePO optimization and knowledge transfer. Negotiated exact technical requirements with vendors (RFI, RFQ, RFP); establish contracts, and wrote technical contract specifications and proposals i.e Splunk Logging/SIEM systems. Saving UNMH 500k per year in licensing and maintenance fees/costs. Designed, developed, and delivered training classes, WIKI's, and workshops in areas of computer security systems. Maintained a broad knowledge of current and emerging state-of-the-art computer systems/ security/testing/hacking technologies, architectures, and products. Maintained knowledge of current trends and developments in the Cybersecurity field in order to enhance expertise i.e. Knowledge transfer, documents/materials to train a team of 5 cybersecurity analyst. Led the team and organization in our annual Security Controls, HIPAA/PCI controls assessments from CLA/Trustcc for 4 years. Gathering and wrote required evidence/supporting documentation on security policies/procedures, coordinated the remediation/mitigation of findings, provided all reporting and updates to executives, down to individuals responsible for systems being remediated. Developed and trained a Red Team to provide penetration testing for all systems and software. Acted as internal auditor to prepare the organization for all Security related auditing functions. Develop project plan to prepare for a Mock OCR HIPAA audit based on NIST SP-800-53 R4 (Cybersecurity Framework & Risk Management Framework). Worked with stakeholders to collect and organize the documentation and other relevant information for the auditors. Provided positive learning and working environment, and a "lead by example" work process, along with a sense of ownership with all projects/tasks, ensuring fiscal responsibility, safety awareness, and superior customer service and personal integrity. CTO/CIO/ IT-IS Enterprise Architect Company Lifecycle 1994 to 2019 Abridged Client List: Thomson Corporation (Learning, Financial and Holdings Division), Cengage Learning, Sand Piper Assets Management, Vim Software, Bilton International, Presto Telecommunications, Stutz Law Firm, Indyme Electronics, Rapid Domains, PC Express, Cricket Communications, San Diego County Credit Union, Coleman College, Symitar/ Jack Henry & Associates, CalOptima, CalTrans: Hired by clients to be responsible for protecting information and information processing assets, advised clients to purchase and deploy product and professional services with respect to developing technological/product roadmaps based on their needs for 5 regulatory/compliance security architectures, best practices and security awareness/educating employees about their information security and privacy protection responsibilities. Managed 5 direct reports, managed teams of 2-10 individuals for clients as a 1099 contractor or W-2 employee. Provided leadership/mentorship to client employees/teams on various network, server, and desktop infrastructures with 1000-2 users. Provided CIO level services to client organizations, small businesses, and executives. Acted as adjunct instructor at local college and taught Windows 7 & Server 2008 admin/installation, ethical hacking, and computer forensics to classes of 20 students. Led information security training and awareness programs based on NETSEC and NIST best practices to educate the IT as well as other departments/units of the client workforce. Ensured alignment of privacy and security policies for all clients. Established, implemented and led an incident response team to contain, investigate and prevent future breaches of patient health/financial/employee/business information. Participated in Incident Response/breach investigations and maintain documentation/timelines of all investigation and developed mitigation plans for clients. Provided Penetration testing for clients to ensure their internal and external attack surfaces were secure and kept to manageable/safe. Provided hands-on technology support (desktops, laptops, peripherals, blackberries/iPhones, video conferencing, T-1 installation/support, VOIP, etc.) and vendor management (IT/IS and construction trades) for the Executive Chairman of the Board of Cengage Learning (formerly Thomson Learning) and Other CEO's in the San Diego Area. Provided high-level enterprise network/cybersecurity support on site and remotely: Resolved problems and was the technical lead to answer questions related to the network/systems and cybersecurity topics for clients/staff. Utilized vendor and carrier support when necessary to resolve network problems/breaches and/or outages, that were not internal in order to recover systems as quickly as possible (pen testing, vulnerability monitoring, IDS/IPS, and deep packet analysis). Provided cybersecurity functions for all employers for networks, servers, desktops, and other systems, which include the following functions/specialties: 1. Access control, user accounts, AD, TACACS, Radius, Secure ID, etc. 2. Telecommunications and network security, Cisco, Juniper, Microsoft/UNIX, etc. 3. Information security governance (NIST, CIS 20, FISMA, HIPAA, PCI, etc.) and risk management, CDM, Vulnerability Analysis-Symantec RAS, Big Fix, Tenable Security Center, etc. 4. MS Software security scanning/updates, IIS security/hardening, signed applets, certificates, etc. 5. Cryptography, VPN, PGP, etc. 6. Security architecture and design based on Cisco AVVID, SANS, ITIL, SANS Cybersecurity, etc. 7. Operations security, ISSO, Waste fraud and abuse auditor, QA auditor, etc. 8. Business continuity and disaster recovery planning, high availability nets, multiple data centers, etc. 9. Legal, regulations, investigations and compliance, HIPAA, SOX, FISMA, USCGB, CDM, etc. 10. Physical (environmental) security, key card systems, security guard, locks, etc. Designed, installed, documented and maintained all customer production networks, while ensuring that the network designs conformed to SANS/NIST best practices for security configurations, wrote procedures, and created training materials (Cisco & Juniper hardware & Microsoft servers/desktops/laptops/NAS) for existing Financial, Engineering, and e-Commerce clients in client facilities in order to support/migrate to new or existing data centers utilizing ITIL methodologies, as an engineer and IT manager, based on SOX, HIPAA, PCI, FDCC, USCGB, FISMA, (FIPS-199/200, NIST SP 800-53, NIST SP800-137, Etc.) policies and controls; performed audits, vulnerability scanning, penetration testing, user/data compliance testing/GPO's, server & systems analysis & support, syslog consolidation & analysis, and developed training/user documentation. Developed and monitored processes that ensured the ongoing secure configuration of the network architecture, and monitored/maintained network security related to application vulnerabilities and their output for indications of malicious activity with Tools like SCCM, WSUS, Shavlik, Big Fix, Risk Analysis Suite (Secure Fusion), Tenable Security Center, and Scriptlogic Deployed, maintained, and upgraded Microsoft operating systems for organizations with 5-1500 users, utilizing COTS Anti- virus, malware, firewalls, system tools, patches, and other software to maintain user workstations in LAN/WLAN environments, and ensuring network optimization and efficiency through monitoring od Desktops, Laptops, Servers, and virtual systems Designed, installed, and supported Cisco/Foundry/Juniper/Linksys and other vendors wired/wireless switches/routers/firewalls/IDS systems on SMB and enterprise networks connected to Cable, DSL, ISDN, and T-1's, DS-3, and OC-12 ISP backbones, and provided detailed protocol analysis and troubleshooting of client networks onsite and remotely for small businesses to enterprise level clients Provided project/vendor management in order to design, install, and administer alpha/beta testing and R&D facilities for various software development clients/companies utilizing feasibility studies, project plans, and project management. Designed, installed, administered, maintained, and documented internal/external client networks and data centers systems on a daily basis for clients with R&D test beds, software development activities and production networks for Financial, Engineering, and e-Commerce facilities which contained as many as: 1. 12-IBM P-Series AIX servers, running AIX 5.3-6.1 2. 20-IBM X-series Windows servers, running Windows server 2003-2008 enterprise edition 6 3. 100-HP/Dell Windows servers, running Windows server 2003-2008 enterprise edition, converted to VMware 4.0 Guests 4. 10-IBM Linux servers, running OpenSuse Enterprise Linux 5. EMC Clarion, Compellant, NetApp, and Netgear SAN/NAS devices with Fibre channel & iSCSI 6. 5-VMware ESXi hosts running 50 guests 7. 5-700 workstations/laptops, running Windows XP-win-7 8. Installed/maintained on the servers: VMware ESXi 3.5-4.1, Symantec/Veritas Backup, and other Microsoft server software (Exchange, SQL, SCCM, etc.) Designed, installed, administered, and documented various Cisco & Juniper network backbones utilizing: 1. 1700/2600/3600/7200 series routers 2. Catalyst 3500, 2900, 5500, 6500 switches 3. Cisco/Linksys Wireless LAN's, 340 series to 1600 series 4. IDS sensors and vulnerability scanners 5. PIX/ASA firewalls, Riverbed Steelheads 6. Juniper j6350/2350/mx80 routers, ex-3200/4200 switches, ISG/SSG firewalls 7. Fatpipe Load Balancers, Packet Shapers, HP IDS/IPS sensors 8. Websense v5000 appliances, Aruba Wireless, HP Procurve Switches 9. Solarwinds Orion, What's Up Gold, PRTG/MRTG Developed and provided training for all users and clients to utilize new network and server systems. Provided end-user training for mail, office software, web, and other industry standard software packages Provided complete senior level network security services and computer security forensics; Install Cisco PIX/ASA, Check Point, Sonicwall, and Juniper firewalls, network monitoring, vulnerability assessment technologies, developed/implemented security policies/procedures, and IDS sensors for Financial, Engineering, and e-Commerce clients as a layered security model based on SANS best practices. Provided senior level IT/IS project management, business analysis, and planning/technical support for existing and new/emerging technologies utilizing CPI/SPI and earned value methodologies for all clients Coordinated vendor selection, provided contract negotiations, and vendor interface on behalf of client as and IT/IS General Contractor/Facilitator with Cisco, Microsoft, and various other vendors CDM Information Assurance Network Specialist/Team Lead (Contract Ended) QinetiQ NA March 2013 to March 2014 Provided advanced vulnerability, compliance, and systems support/analysis of the Indian Health Services 42,000 systems with Symantec RAS or Secure Fusion, Tenable Security Center and Nessus Scanners, Nmap, Metasploit, penetration testing, protocol analysis, and utilization of other security software platforms for their CDM program Performed daily scans of the IHS network (27,000 devices) to determine if any connected devices do not follow the configuration protocol outlined by IHS policy/procedure and Federal mandates (USGCB,FDCC, FISMA, HIPAA, NIST SP- 800-53 R3, CDM SOP, etc.) Provided senior level network engineering/administration, compliance and vulnerability analysis/reporting, as well as tracking of mitigation plans/POA&Ms. Provided mechanisms to ensure the protection of sensitive personal information - both health records and personally identifiable information that could be used for identity theft and entails a high level of public trust Provided state-of-the-art knowledge, troubleshooting, and utilization of Microsoft operating systems, desktops, tablets, servers 2000-2012, XP-windows 8.1, and complete Microsoft catalog of software Provided senior level knowledge, troubleshooting, and utilization of Active Directory, Group Policy Objects, logging, event correlation, regedit, PS tools, and other capabilities within Microsoft products. Provided basic knowledge, troubleshooting, and utilization of various Linux variants for servers, desktop systems, and vulnerability scanners Provided advanced utilization of VMware 5.1 virtualization to create Microsoft & Linux servers for Scanners, Secure Fusion, etc. Creating/deploying test-bed hosts and other related systems Provided cutting-edge skills for patch management with Symantec Endpoint Management, WUSUS, Shavlik, and Big Fix systems. Provided user training for patching, removal of vulnerabilities, and related issues to securing systems to federal standards to all Area ISSO and other Security personnel. Performed in depth analysis of Federal NIST USGCB, FDCC, and 800-53 requirements against IHS GPO's for compliance, determined where compliance is not met and what GPO's require creation or waiver to ensure 100% compliance. Produced 800 page report with action items to ensure compliance and a path to remediate all findings. Coordinated and conducted information risk assessments to protect patient health information Coordinated, analyzed and documented application access audits. Ensured appropriate access controls, both physical and application access controls to all IT/IS resources. Provided Vendor relations to ensure Vendor products in use at IHS meet federal security compliance. Worked with Abbott Laboratories to modify their glucose metering software and Mitel Phone Switch software to make their products compliant Provided senior level reporting, analysis, and evaluation of various security topics as related/required by the Continuous Diagnostics and Mitigation program from DHS/HHS/IHS: Hardware/software inventory management, Configuration setting management, Vulnerability management, Network/physical access control management, Trust-in-people granted access (access control management), Security-related behavior management, Quality management, Credentials and authentication management, Privilege management, Prepare for incidents and contingencies, Respond to incidents and contingencies, Requirements, policy, and planning, Operational security Generic audit/monitoring Documented all processes and procedures required for daily operations with Secure Fusion, Tenable Security

Center and Nessus Scanners, bi-monthly vulnerability reporting, and other related CDM programmatic documents. Senior Network Engineering Manager (Company Sold) Albuquerque Health Partners 2014 to 2014 Responsible to assist in maximizing the value derived deploying a network security environment by designing, implementing, and supporting all facets of information security. Lead the team to design, maintain, troubleshoot, and provide daily operations related to enterprise wide data network systems and associated peripherals in a Health Care Environment. 15,000 employees and 20,000 network systems and endpoints to ensure HHS/NIST requirements/compliance were utilized, deployed and documented. Provided Network architect role. Evaluated and recommended changes to current Juniper and future Cisco data network requirements in order to meet organizational and security needs Participated in the planning, installation, operation and maintenance of enterprise-wide data networking solutions for 17 clinics around the ABQ and Rio Rancho Area through the deployment/utilization for site to site VPN's and IDS sensors between each clinic and the data center. Provided testing and documented system behavior, performance and security for Juniper/Cisco network components (100 switches, 30 firewalls/routers, 3 VPN concentrators, etc.) Provides network disaster recovery expertise for routers, switches, load balancers, firewalls, network connectivity, and VPN tunnels, etc. Worked closely with both equipment vendors and service providers to ensure timely and successful deployment of new services/repairs as well as acting as the main point of contact for resolution of outages and service disruptions for all 17 facilities. Adhered to HIPAA/PCI policies, procedures, security requirements/regulations to ensure compliance and patient safety. Utilize Juniper NAC and other security services/systems to record/study the organizational computer intelligence to map out the internal and external threat map that target centric infrastructural elements. Based on SOX, HIPPA, PCI, FDCC, USCGB, FISMA, (FIPS-199/200, NIST SP 800-53, NIST SP800-137, Etc.) policies and controls; performed audits, vulnerability scanning, penetration testing, user/data compliance testing/GPO's, server & systems analysis & support, syslog consolidation & analysis, and developed training/user documentation. Facilitated the resolution of issues/outages/maintenance regarding the network and NETSEC hardware and software environment. Control and maintain accurate data network system, device inventories at 17 locations through ABQ/RR on Metro Ethernet, PPP lines, and PRI lines as well as the data center at the Big Byte location in downtown Albuquerque. Provided guidance on data network system selection, remediation policies, and best practices for HIPPA, PCI, SOX and CDM compliance/deployment for the organization Assisted IT management with deployment/implementation of the technical architecture related to planning, installation, operation and maintenance of all data network devices, systems, NETSEC and software that supported mission critical functions for the Data Center, local DR site, and California DR site based on NIST/CIS 20 frameworks. 4 Provide daily and project planning to develop quarterly maintenance schedules for Juniper, Cisco, Citrix, Xirrus wireless infrastructure, and other vendor systems/technology; firmware upgrades/updates, configuration standardization, documentation of all network systems/components, etc. Review and revised all network/ security policies, procedures, user/vendor access forms and access agreements related to the security of patient health information. Worked with other Information Technology teams to evaluate, recommend and implement new technology to increase data/operational security. Ensured the successful implementation and maintenance of defined HIPAA and PCI standards and policies. Founder January 2002 to January 2002 December 2019 Network Security Systems Manager Company Lifecycle - San Diego, CA January 1999 to January 2002 Senior Network Systems Manager SAIC Corporation - San Diego, CA November 1997 to January 1999 Network Security Analyst/Systems Process Re-Engineering Manager AeroTek Services Group January 1997 to November 1997 US Department of Energy, Albuquerque Operations Office (DOE/AL) Customer Service Unit Manager/Architect (CSU821) AeroTek Services Group January 1990 to January 1997 Network/Systems Deployment Manager, Budget Analyst Sandia National Laboratories Prior IT/IS Work History Available Upon Request Education Masters of Business Administration in Business Administration University of Melbourne E-College Masters of Management Information Technology in Management Information Technology University of Melbourne E-College BA in English/Speech Communications University of New Mexico Certified Information Systems Auditor Nessus Security

Center & Symantec Secure Fusion Admin Skills architecture (10+ years), best practices (10+ years), documentation (10+ years), forensics (10+ years), HIPAA (10+ years) Links http://www.hiredgunconsultingrrd.com

Name: Amber Ware DDS

Email: swhite@example.net

Phone: 9938424342