INFORMATION SECURITY LEAD

Professional Summary

Accomplished Certified Information Systems Security Professional with over 15-years of Information Assurance experience. Holds experience at auditing INFOSEC programs, aligning security solutions with strategy and operations, Computer Network Defense (CND), and analyzing controls for compliance. Projects expert knowledge at recommending management, technical, and operational controls to support INFOSEC policies, Security Assessment and Authorization (SA&A), POA&M completion, Audits, Cyber Threats, and control implementation based on standards and frameworks: FISMA, NIST, DoD 8500, COBIT, and ITIL. Skilled at using vulnerability tools, practices, and procedures to mitigate vulnerabilities for impact assessments and compliance standards. Holds Top-Secret Clearance (DOD-Current/Active) and Masters of Information Assurance.

Skills

- Inventory Control Customer Service Purchasing
- Quality Assurance
- Shipping and Receiving
- Cargo Loading and Unloading
- Order Pulling
- Tracking Materials
- Safety Handling
- HAZMAT Controls
- Warehouse Operations
- Forklift Operations
- Vehicle Safety
- Material Distribution

Education

Masters of Science , Information Assurance May 2010 University of Maryland University College ï¼ City , State

Bachelor of Science , Computer and Information Science May 2006 University of Maryland University College ï¼ City , State

Minor: Technical Communications

Certifications

ITIL Foundation (ITILv3) Dec 2013

EC-Council Certified Ethical Hacker (CEHv8) Dec 2013

Microsoft Certified Technical Specialist (MCTS) Aug 2013

Information Assurance Security Officer (IASO) Dec 2012

Certified Information Security System Professional (CISSP) Feb 2012

CompTia Security Plus (SY0-301) Jun 2009

Master Training Specialist (MTS) Jan 2007

CompTia Network Plus (N10-003) Dec 2007

Journeyman' License -Electronic Technician (#04761) Jan 1998

Experience

Information Security Lead Oct 2012 to Current
Coca-Cola ï¼ Chicago , IL

- Directed pre-validation for C&A that includes performance of C&A testing and vulnerability scanning to validate IA policy, regulation, Security Technical Implementation Guide (STIG), and Best Business Practice (BBP) compliance for systems.
- Performs security configuration requirements to integrate new applications into network environment and assessed adequacy of the required protective measures for risk mitigation and control implementation for ATO approval..
- Researches security issues, cyber threat warnings, trends, and impacts by use of vendor bulletins, CERT, NIST, and DoD 8500; and cross-trained IT staff to detect vulnerabilities within the infrastructure and application environment.
- Led security assurance audits, DIACAP artifact creation, vulnerability scans for IAVA alerts, assessments, remediation and IA implementation for desktop computers, servers, network, and databases for the Agent Certification Authority (ACA).
- Manages verification of assigned IA Controls, conducts risk assessments , documents compliance status of the validation results in the DIACAP Scorecard for ATO's and planned Security Test and Evaluations (ST&E) for Site Assisted Visits (SAV).
- Constructs procedures to manage McAfee Anti-Virus updates, Symantec vulnerabilities, Adobe removal, DAT files, application patching,

vulnerability analysis, and policy tuning for security auditing using Nessus and Retina.
- Designed and updated all documentation required for C&A and Plans of Actions and Milestones (POA&Ms) based on DIACAP procedures such as Business Continuity, INFOSEC Policies, and privacy based on DoD IA policies.
- Communicated with government CIO on existing security gaps, patch management strategy, and developed improvements based on DoD 8500, AR25-1, AR25-2, and FIPS for reducing CAT 1 security issues and maintaining IA posture.
- Coordinated vulnerability scanning and remediation of all assets, operating systems, and databases utilizing Retina and Nessus, as well as, applicable security manual checklist(s) to validate compliance based on DoD IA controls.
- Assisted DIACAP validators and ACA with interpreting and understating vulnerability scanning results, network architecture, and Information Assurance process for security validation of network.
- Tracked and submitted Certificate of Noteworthiness (CoN) to ensure application products adhered to Army standards and compliance based on identification, measurement, control, and minimization of security risks and impacts.

Enterprise Information Assurance Jul 2011 to Oct 2012
Applied Information Sciences, Inc. ï¼ Offutt , NE

- Provided consultation, technical solutions, recommendation, and strategic guidance for security configuration, enterprise risk mitigation, upgrades, security impact, auditing, and application compliance.
- Served as a subject matter expertise (SME) providing sustainment for IA to include C&A, CERT Readiness, IRM, ST&E, remediation, and POA&M for 135 enterprise servers using REM/Retina, McAfee ePO Orchestrator 4.5, IAVA's, STIGs, vulnerability scans, Security Authorization (SA), and security tool suites.
- Worked collaboratively with IA Teams and government clients to improve security countermeasures, and defensive strategy through vulnerability assessments, audit log and report analysis, and technical control implementation. Integrated practices and programs to configure systems, SQL databases, and critical software programs through the development of operating scripts, batch files, policy changes, and application settings.
- Creates and maintain security configuration and documentation for assets, and developed patch management program to support C&A, IAVM, ST&E, and risk mitigation.
- Utilized Enterprise Management software, and expertise to advice clients on resolving compliance issues.
- Troubleshot Server 2003/2008 software problems and applications. Configured, tested, and installed new and/or enhanced software through registry modifications, configuration changes, and new buildouts for clients.
- Provided customer service and quick resolution of technical issues using Remedy ticketing system, administers Windows AD, adding users, resolving password issues, adding groups, applying permissions, creating OU's, and assets to the domain.

HBSS Support Engineer Mar 2011 to Jul 2011
Chevron ï¼ Portland , OR

- Engineered, configured, and installed VMware ESX server for network access through basic UNIX commands and system changes for HBSS afloat platforms and virtualized lab for ePo 4.5 implementation.
- Conducts DISA Gold Disk and STIG configuration in accordance with DOD and DISA standards. Wrote various HBSS SOPs to train and educate junior HBSS personnel
- Advised afloat network owners on developing and implementing effective product and application solutions through HBSS configuration changes, policy tuning, and setup procedures.
- Provided SME for Host Intrusion Prevention System (HIPs), Policy Auditor (PA), McAfee Agent (MA), ePolicy Orchestrator (ePO), Asset Baseline Monitor (ABM), McAfee Anti-Virus (MA), and supporting applications such as Microsoft Structured Query language (MS SQL) and Microsoft Windows Server 2003

Lead Information Assurance Analyst Oct 2009 to Oct 2010
American Systems ï¼ City , STATE

- Served as a focal point to Concept of Operations (CONOPS) working group for managing Host Intrusion Prevention System (HIPs), Policy Auditor (PA), McAfee Agent (MA), ePolicy Orchestrator (ePO), Asset Baseline Monitor (ABM), McAfee Anti-Virus (MA), and supporting applications such as Microsoft Structured Query language (MS SQL) and Microsoft Windows Server 2003 for HBSS.
- Developed procedures to configure applications for policy compliance and used reporting system to track, perform threat analysis, gather metrics, and mitigate risks based on CND task orders, countermeasures, and intelligence data
- Block unwanted programs such as spyware and adware. Created, deployed and managed ePO repositories. Created, queried and ran reports from the ePolicy Orchestrator reports database, including creation of custom queries.
- Removed older VirusScan versions and updated engine and dat files to the latest version. Performed analysis via the ePO reports database on virus outbreaks and vulnerabilities in order to develop appropriate response.
- Reviewed open and unclassified sources of cyber threat warnings and vulnerability announcements from the DoD IAVM program, NIST, National Vulnerability Database (NVD), SANS Institute and Internet Storm Center, security vendor advisories and other cyber security new media sources for information that impacted operations.
- Analyzed and identified threats, vulnerabilities or changes to the level of risk associated with continued operations. Assess the level of threat associated with the circumstances and provide reporting to CND SP management.
- Performs system administration on HBSS and integrates HBSS data (alerts, logs, data feeds, etc.) into protect, detect, and respond processes, procedures (intrusion detection analysis, auditing, etc.) and systems.
- Guided CND SP subscribers at interpreting results of the threat analysis and the associated reporting; and assisted with guidance on

implementing the prescribed risk mitigation strategy.

Senior Security Analyst Apr 2009 to Aug 2009
SAIC ï¼ City , STATE

- Performed multifaceted role in advising and guiding IT support team responsible for security management and Remote Dispatch Support regarding telecommunication services for a live dispatch call center.
- Provided technical assistance to System Engineering team on all matters including functional layout, COOP operation, security integration, technical requirements, and C&A.
- Instituted a vulnerability management program to control threats and integrated security compliance for systems.
- Coordinated taskings and scheduling with security engineering team and outside customers to perform upgrades.
- Performed a quality check after conducting assessments to ensure 36 workstations was in IA compliance.
- Independently develop a variety of DIACAP deliverables including: System Security Plans, Security Design Documents, Vulnerability reports, Privacy Impact Assessments, Security Annual Assessments, and Contingency Plans.

Network Communication Specialist Oct 2008 to Apr 2009
BIB Technologies ï¼ City , STATE

- Directed deployment testing for the US Navy Public Safety Networking System (PSNET).
- Developed, outlined, and integrated security requirements and task orders to install and test for connectivity.
- Advised teams on correcting network troubles and performance issues spanning security and configuration.
- Orchestrated procedures and programs to diagnose and configure T-1 lines using TFTP.
- Effectively communicated with government liaison on network status and installation requirements.
- Maintained security of network equipment at 100%; monitored physical and logical access to remote systems.
- Performed system level troubleshooting, risk assessment, and problem solving for secure traffic for migration.
- Spearheaded the installation, configuration, and upgrade of a secret networking system Partnered with NOSC Network Engineers to resolve 50 WAN issues before routine installations.

Computer System Manager/Master Trainer Aug 2000 to Aug 2008
US Navy ï¼ City , STATE

- Developed policies and procedures for systems reliability and accessibility by performing analysis of security standards.
- Conducted threat analysis; risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities and protection needs.
- Engaged in daily "information sharing" efforts with counterparts in the DoD, intelligence, and threat defense communities.
- Constructed organizational procedures to develop and implement technical teams for new tasking's.
- Key achievements: Cross-trained junior officers on gathering threat data through intelligence resources to maintain the appropriate security posture; interpreting threat response; implementing countermeasures to protect sensitive data.
- Ensured security policies complied with DOD 5200.1 specifications; translated requirements into a technical framework by modifying system architect.

Additional Information

Membership: Atlanta International Information Systems Security Certification Consortium (ISC2) and Georgia Information Systems Security Association (GAISSA)