First and last name M.Sc., MBA

[email](mailto:Kudeh19@gmail.com) and cell #

**PROFESSIONAL SUMMARY**

Professionally-focused and team oriented Senior Security Engineer/Assessment and Authorization Professional, knowledgeable in Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), security life cycle and vulnerability management using FISMA and NIST guidance. Ability to work independently or in a team environment, with in-depth knowledge and understanding of various security threats, computer operating systems and different assessment methodologies.

**Functional Areas of Expertise**

|  |  |
| --- | --- |
| * Information Systems Security * Vulnerability Assessment * Ethical Hacking * Information Assurance * Project Management and Support * Network Forensic and Analysis | * Security Life Cycle * Systems Risk Assessment * Systems Development Life Cycle * Business Systems Analysis * Business Application and User Support |

TECHNICAL AND SPECIALIZED SKILLS

* Nessus Vulnerability Scanner
* Tripwire
* CSAM (Cyber Security Assessment and Management)
* Microsoft Word, Microsoft PowerPoint, Microsoft Excel
* Accellion
* FTK Fosensic
* Palo Alto Firewall
* McAfee ePolicy Orchestrator
* Solarwinds

PROFESSIONAL EXPERIENCE

Sr. Information Security Engineer

National Oceanic and Atmospheric Administration-NOAA

(Deploy from SMRC)

Suitland, Maryland

March 2017 – Present

Responsibilities

* Plan, coordinate with stakeholders/participants to prepare for external Security Test and Evaluation (ST&E) and Annual Security Control Assessment (SCA)
* Manages the remediation of POAMs process with ISSO and System Owner.
* Responsible for establishing and maintaining security control assessment activities communications with all stake holders.
* Coordinates scheduling of new POAMs activities with System Administration, Network Engineers Lead and perform status progress reporting to the ISSO and System Owner.
* Reviews Security Controls Assessment documentation; e.g., Security Assessment Report (SAR), Vulnerability Assessment Report (VAR), Continuous Monitoring Report (ConMon), etc.
* Works with the Security Assessment and Authorization (SA&A) and technical teams to identify POA&M artifacts required for closure.
* Identifies any constraints and risks requiring consideration and escalates to ITSEC Manager.
* Verifies the completeness and accuracy of artifacts provided by the SA&A team, System Administration and Network Engineers.
* Create schedule, assign resources and balance work load for the Security Analysts of POA&M-related activities in the ITSEC workflow tracker
* Developed, evaluate and implemented information security governance processes, including policies, standards, procedures and risk management practices.
* Monitored controls post authorization to ensure continuous compliance with the security requirements.
* Developed IT security system projects from design to support, evaluate the effectiveness of systems and services, and provide advice and solutions to a wide range of IT issues.

Sr. Information Security Engineer

Maryland Judicial Information System

Annapolis, Maryland

September 2016 – March 2017

Responsibilities

* Developed, reviewed and updated Information System Security Policies, and Security baselines in accordance with NIST and other industry best security practices.
* Conducted systems and network vulnerability scans in order to identify and remediate potential risks
* Developed, evaluated and implemented information security governance processes, including policies, standards, procedures and risk management practices
* Independently execute security risk assessments on policy variances and new technologies and communicate results effectively to senior management
* Creates and updates process documentation for new tools and act as the liaison between security vendors and Judicial Information system
* Creates information security reporting metrics and analysis for management
* Occasionally team with network architecture team and Firewall team to develop secure solutions and participate in security assessments
* Assist with the management and validation of security firewall configurations
* Assists during system auditing and application patching verification and reporting
* Provides support for network, application, and perimeter penetration testing/external assessments
* Provides support for information cyber security investigations as well as on-call response for cyber security incidents
* Review several monitoring logs and work with system administrators to determine the security posture of all systems.

Applications Security Analyst

UnitedHealth Group

Elkridge, Maryland

June 2015 to September 2016

Responsibilities

* Conducted systems and network vulnerability scans in order to identify and remediate potential risks
* Developed, evaluated, and implemented information security governance processes, including policies, standards, procedures and risk management practices
* Monitored controls post authorization to ensure continuous compliance with the application security requirements
* Reviewed authorization documentation for completeness and accuracy for compliance
* Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies
* Collected Operation and Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless
* Configure FireEye to detect and block spear phishing and other email security threat
* Use HPSM ticketing system to prioritize and update hardware /software incidents
* Manage Airwatch program on company cell phones and assist with installation, maintenance of tablets/Cellphones/computers
* Assist with installation of applications, regression testing and troubleshooting of custom built software
* Deploying and updating of anti-virus and patches, upgrade of Operating Systems to Windows Server 2008.Installation of software

Cyber Security Analyst/Security Administrator

Howard County General Hospital

Columbia, Maryland

January 2010 – August 2015

Responsibilities

* Deploying and updating of anti-virus and patches, upgrade of Operating Systems to Windows Server 2008.Installation of software
* Monitor all systems, applications, security, and network with SolarWind to make sure configurations are running at optimal performance
* Assist the senior network administrator in drafting network policies and procedures regarding access methods and time, and security validation checks
* Installs and maintains network monitoring systems by performing intrusion detection under the supervision of the senior admin.
* Performs additional duties and responsibilities as assigned by the senior system Admin • Super user and lead trainer in deployment of clinical software (Epic)
* Manage and support secure Virtual Private Networks (VPNs), Logs all problems, issues and requests. Collecting data and triaging network alerts
* Implement and maintain HIPAA, FISMA and NIST SP 800 series requirements and keep current with new Information Technology Security protocols, ethics and regulations
* Acts as the primary support of the EMR systems solutions for the user community during an implementation phase.
* Performs and coordinates complex analysis, design, development, testing and support services for assigned application applications
* Adheres to applications security and control procedures in accordance with departmental, vendor standards and regulatory bodies and apply recommendations as necessary
* Responsible for the implementation of day-to-day tracking and follow-up on issues and questions of daily operations

PC Technician

Nestle Ice Cream

Laurel, Maryland

January 2009-January 2010

Responsibilities

* Deploying and updating of anti-virus and patches to various operating systems including Windows servers
* Implement, manage and monitor and server-based systems that comprise the company's personal computer network
* Assist in managing, monitoring and administering the local area network of the central home office computer facility
* Provide day-to-day support to all company employees who use PC's, printers, and all other office productivity applications
* Provide high-level customer service to multiple levels of company staff and management
* Install/upgrade PC's and server-based hardware and related peripherals according to the plan outlined by supervisor and management.
* Provide basic printer hardware, software troubleshooting, basic email/internet troubleshooting and training for all end users
* Provide users with account connectives and resets for a variety of business applications
* Assist in basic network troubleshooting of Printers, Routers and Switches

EDUCATION

* MBA, University of Maryland University College. |2017
* Masters of Science, Information Assurance; University of Maryland

University College, |2016

* Network Security Administration; Howard Community College. Maryland |2015
* B.Sc. Computer Science; Enugu State University of Technology. Nigeria |2006

SKILLS

* Ability to establish and maintain effective working relationships with clients and co-workers
* Skills in interviewing users to help analyze and resolve issues
* Strong organizational, analytical and planning skills
* Ability to read and interpret system security policies, rules and regulations
* Ability to communicate security and risk-related concepts to both non-technical and technical audience
* Strong communication (verbal & written) and presentation skills