Gentis Solutions
EFFECTIVE INNOVATION

Anthony Nuriddin

EXECUTIVE SUMMARY:

Results-driven *Certified Information Systems Security Professional* (CISSP) with over 30 years' experience and notable success in Information Technology (IT), Information Assurance (IA), and Information Management (IM) matters to help secure and protect enterprise systems, networks, data and information. Adept in leading information systems initiatives that support IT business and strategic planning efforts, formulating policies, recommending and implementing solutions that support organizational growth and improved productivity. Solid proficiency in the life-cycle management of information, project management and managing physical and conceptual resources under my purview. Demonstrated ability in performing IT/IA/IM management analysis and research on technology trends, emerging standards, and industry best practices to support the Chief Information Security Officer (CISO), Chief Information Officer (CIO), and the Director of Security. Diverse background supporting Industry, Department of Defense (DOD), Defense Intelligence Agency, U.S. Air Force, U.S. Joint Staff, Intelligence Community, the Pentagon and Federal Government.

DEGREES AND CERTIFICATIONS:

Academics	**MBA Certification:** *Management of Science, Technology and Innovation*, George Washington University (GWU) Washington DC (December 2007) **M.S. Information Systems Technology**, George Washington University (GWU) Washington DC (December 2001) **B.S. Computer Information Systems (Programming)**, Strayer University (SU) Washington DC (June 1998) **A.A.S Information Resources Management**, Community College of the Air Force (CCAF), Washington DC (May 2003)
Certifications	**IBM Security Guardium Administration v10.0** (March 2017) **IBM InfoSphere Guardium v9.0** (February 2016) **CISSP** (Expiration Date: October 2022) **COMPTIA Security+** (September 2007) **Chief Information Officer (CIO) Certification** CIO University (June 2000) **Information Resources Management (IRM) Certification** General Services Administration (GSA) (October 2000)

PROFESSIONAL HISTORY:

Output Services Group

Cyber Security Manager *01/2020 - 06/2020*

- Establish and manage the corporate *Cyber Security Program*
- Provide security and technical solutions to protect the companies physical and conceptual resources from unauthorized, access, destruction, or modification.
- Identify and classify data that needs to be protected.
- Verify that physical and logical access controls are implemented to limit access to sensitive data, information, and physical locations.
- Verify that backup tapes and other information assets used to store personally identifiable information (PII), credit card data, or electronic protected health information (ePHI) is encrypted to prevent unauthorized access.
- Created a Risk Management Matrix on the use of insecure transmission encryption protocols to identify the risk, vulnerability, and provide a temporary and permanent mitigation strategy to prevent attackers from extracting data from secure connections. This helped the company meet *Payment Card Industry Security Standards Council* (PCI SSC) business requirements by the regulators deadline date.
- Created a Risk Management Matrix on the use of weak ciphers to identify the risk, vulnerability, and provide a mitigation strategy to prevent attackers from intercepting or tampering with sensitive data while in transit.
- Created an implementation plan to ensure that TLS-enabled websites are configured to use cipher suites that provide *perfect forward secrecy* to modern web browsers; worked with IT support staff to verify that critical servers (application, database, and web) are configured with key exchanges that are compliant and will provide increased security for both the user and the organization running a server.
- Collaborate with network team to ensure that all critical network assets and servers are identified and configured to send event logs and syslog's to *Security Information and Event Management* (SIEM) tool.
- Perform log analysis, correlation, indexing, and searching using *ManageEngine EventLog Analyzer*.
- Review *Windows* Group Policy (GPO) settings for our domain audit policies, document the status of all object access auditing options of distinct resources (files, active directory objects, and registry keys), and recommend changes, if any.
- Create filters, custom reports, and real-time alerts to notify senior management about threshold violations, network anomalies, user activities, or compliance violations.
- Create and manage user accounts.
- Created a spreadsheet that identified a baseline of key Windows events to monitor and alert.
- Periodically review IT security policies and procedures for outdated or obsolete content and revise when warranted to keep the organization up-to-date with changing business requirements, regulations, technology, and industry best practices.
- Evaluate the level of protections provided by existing policies, procedures, customer information systems, and other safeguards in place to control risks.
- Created a comprehensive self-inspection checklist that incorporates key security requirements from each policy and is used as a self-evaluation tool to evaluate our operational, management, and technical controls enterprise wide.
- Participate in vendor product evaluations to determine ease of use, functionality, workflow, reporting and compliance, cost, and if products meet business requirements.
- Continuously monitor third-party vendor relationships to assess the overall security, privacy, and data protection posture of business partners, and to ensure that they are operating within the terms of the contract or service level agreement.
- Perform various network scans using Tenable.io and Nessus Professional

- Created a project plan that identified key tasks (*planning and information collection*, *asset prioritization*, *information gathering (site artifacts)*, *active assessment*, and *reporting*) to perform during site-specific assessments. This document provides a framework for the initial assessment and is used as a baseline for future assessments.

- Created asset spreadsheets for four of our core locations (Arizona, Minnesota, North Carolina, and New Jersey) to establish a baseline and maintain an up-to-date inventory of devices connected to our enterprise networks, including servers, workstations, laptops, wireless access points, and remote devices
- Created a security questionnaire to capture basic company information (size and scope of the organization), threat products used, and the security tools used across the enterprise to manage our technology landscape. This data is used for management decisions, during assessments and related activities, and is updated periodically to reflect the latest and most accurate information.
- Perform application and web-based static source code analysis using Checkmarx's *Static Application Security Testing* (SAST) tool to identify and track technical and logical flaws in the source code, such as security vulnerabilities, compliance issues, and business logic problems.
- Provide scan results and *Plan of Action and Milestone Report* (PO&AM) to application support team and work with an assigned developer to confirm the validity of findings, identify false positives (if any), and remediate findings.
- Reconcile initial scan report by updating the [result state] for each identified vulnerability to read *<confirmed, proposed not exploitable, or not exploitable>*.
- Setup manual and automated scans.
- Create and manage user and group accounts for development teams and anyone requiring access to the tool.
- Participate in quarterly vendor meetings established to gauge customer success, eLearning resources, new product features, and development team concerns.
- Work with compliance administrator to document and verify that developers complete annual training to learn the importance of secure coding and software construction, design principles for secure software, and how to apply them in practice.
- Created a Checkmarx access procedures document for new users which includes a list of viable training resources.
- Created a Risk Management Matrix to address *Client Remote File Inclusion* and *Use of Broken or Risky Cryptographic Algorithm*
- Created an *Identity and Access Management Questionnaire* to document application specific data (not limited to users, data processed, server type, operating system, environment (production, staging, or test instances), ports used, DNS names).
- Track and document information system security incidents.
- Monitor alerts from US-CERT, SANS, vendors and other security monitoring organizations for potential changes to the incident response plan based on industry developments and emerging threats.
- Periodically review and validate the company's incident response plan
- Completed a comprehensive security investigation to document the outcome of a SQL injection attempt; provided detailed illustrations, findings, and recommended actions.
- Work with compliance administrator to document and verify that initial and annual training requirements are being met.
- Verify that staff, contractors, and third-parties have a current signed *Acceptable Use Policy* on file acknowledging that they have read, understand, and will abide by all company information security policies.
- Security Tools Proficiency: Checkmark, ManageEngine Eventlog Analyzer, PRTG Network Monitor, Nessus Professional, Tenable.io, LogRhythm SIEM, O365 Compliance Center

CITCO Technology Management

Database Security Architect/IBM Security Guardium Administrator 02/2015 - 08/2017

- Advised and consulted on IT-related projects across the enterprise.
- Periodically reviewed Oracle and SQL database environments for compliance with Citco security policies, industry standards, and made recommendations for improving security.
- Collaborated with core IT members during Technical Architecture Reviews and new project initiatives to ensure that core security requirements (*information characteristics*, *information states*, and *security countermeasures*) are addressed.
- Conducted system and application reviews—examined documents, interviewed users, and tested security controls using a combination of automated tools and manual methods.

- Participated in Disaster Recovery (DR) exercises to validate the viability and effectiveness of the corporations DR Plan for recovery of in-scope security applications to our designated recovery centers
- Oversaw and validated the deployment of *Guardium Installation Manager* (GIM) agents by system administrators--provided installation instructions, server and appliance IPs, and port requirements.
- Used the GIM to deploy and configure Software TAP (S-TAP) agents on database servers.
- Created inspection engines to monitor database activity.
- Created and installed security policies to monitor, alert, block, and observe activity between the client (application, user) and the database.
- Created and managed user accounts and access permissions.
- Created correlation alerts (self-monitoring) to quickly identify and react to system-related problems
- Monitored inspection-core and S-TAP performance on all Guardium collector appliances.
- Periodically reviewed appliance configurations, policies, report definitions and results against business requirements.
- Applied patches, upgraded modules, collectors, and central managers.
- Used *Guardium Vulnerability Assessment* (VA) to run scheduled scans against select database instances to look for vulnerabilities and platform-specific issues reported by various database security organizations and vendors.
- Initiated an enterprise-wide project to upgrade the company's archaic IBM Guardium infrastructure, moving them from a physical to a virtual environment and having scripts created to facilitate the deployment of GIM agents to over 300 database servers
- Developed a background paper for senior leadership on native and third-party encryption solutions to influence purchase decision
- Developed a *Vulnerability Assessment and Remediation Program* (VARP) document to articulate the specific rules of engagement IT Security will employ during a database vulnerability assessment. This document is one of several newly documented and implemented enterprise procedures.
- Developed a *Database Activity Monitoring Strategy* that served as a roadmap towards the completion of several key requirements needed to create and maintain a solid Database Security program; this provided senior leadership and application owner's insight into our IT security roadmap, database security policy, and business defined requirements that will enhance data security across the enterprise.
- **Security Tools Proficiency:** IBM *Guardium Database Activity Monitoring and Guardium Vulnerability Assessment*

SCITOR

Information Systems Security Manager 04/2012 - 12/2014

- Served as Principal Advisor for Computer and Information Security matters on behalf of the Director of Security and the Chief Information Security Officer.
- Developed, maintained, and managed a formal Information Systems (IS) security program for the corporation's 10 geographically separated locations.
- Ensured programs, systems, and processes were compliant with the *National Industrial Security Program Operating Manual* (NISPOM), *National Institute of Standards and Technology* (NIST) guidelines, *Intelligence Community* directives, industry best practices, and security frameworks.
- Developed, implemented, and enforced IS security policies and procedures.
- Worked closely with *Information Systems Security Officers* (ISSO), Security Administrators, and IT staff to ensure all activities required to certify, accredit, and reaccredit information systems were complete and aligned with the NIST Risk Management Framework.
- Created, reviewed, and endorsed *System Security Plans* (SSP)--coordinated with IT staff to provide supporting documentation--current hardware and software baselines, network diagrams, facility layouts, vulnerability scans, and POA&Ms.
- Collaborated with *Security Education, Training, and Awareness* (SATE) lead to develop IA and computer security materials and content to support the company's annual training requirements.
- Ensured the hardening of operating systems using the latest *Defense Information Systems Agency* (DISA) *Security Technical Implementation Guides* (STIG).
- Managed and coordinated IS security self-inspections, tests, and program reviews.

- Ensured that audit logs were regularly reviewed to detect unauthorized activity and access.
- Conducted quarterly validations of users and groups, router and switch configurations, patching status, vulnerability scanning, antivirus updates, and registry settings to defend against possible computer network attacks.
- Conducted software and hardware due diligence.
- Ensured procedures were in place to sanitize, destroy, or transfer equipment when no longer needed.
- Ensured security patches and malware updates were current on all systems

Additional Responsibilities:

- HIPAA Privacy Security Officer: Aided in the development of a corporate privacy program--identified the companies security controls (administrative, physical, and technical safeguards), where *Protected Health Information* (PHI) is created, used, maintained, and how PHI is transmitted and destroyed.
- Defense Industrial Base (DIB) *Cyber Security and Information Assurance* (CS/IA) Program Lead: Analyzed information reported by industry partners regarding cyber incidents, to glean information regarding cyber threats, vulnerabilities, and the development of effective response measures; prepared weekly threat reports for the *Director of Security, Chief Information Security Officer, Senior IT Managers*, and select staff that depicted the incident type, information regarding the incident or the affected systems and networks, impact, and recommended actions.
- Instrumental in ensuring that three Department of Defense sponsored facilities received a superior rating from Defense Security Service (DSS) during the company's annual industrial security inspection.
- Converted existing SSPs to the NIST Risk Management Framework.

Vulnerability Assessment and Remediation Lead 06/2010 - 04/2012

- Federal Government contractor supporting the *National Reconnaissance Office* (NRO) *Ground Enterprise Directorate* (GED*)*
- Continuously monitored and evaluated enterprise information systems and networks to ensure compliance with the *Federal Information Security Management Act* (FISMA), local IA and information security policies, and industry-standard best practices.
- Oversaw the execution of vulnerability assessments by supporting Red Team inspectors in the coordination of their activities *(assess configurations, compliance asset identification, unauthorized connectivity, and security vulnerabilities within local network enclave borders)* at select facilities in the U.S. and abroad.
- Managed the remediation of information system vulnerabilities identified through IA audits, inspections, penetration tests, and assessments of information systems and networks.
- Collaborated with system owners and administrators to enhance the security posture of the enterprise by prioritizing, managing, and engineering mitigation solutions to reduce risk--categorized and identified tactical and strategic vulnerabilities, developed and delivered solid mitigation plans, and performed independent verification and validation
- Tracked, documented, and reported remediation progress to the *Director GED*, *Director*, *Office of Security and Counter Intelligence*, and the *Composite Information Assurance Office*
- Core member of the *Vulnerability Management Working Group* (VMWG) and the *Joint Security Architectural Working Group* (JSAWG).
- Spearheaded the remediation of over 52% of the directorates system and network vulnerabilities in less than a month of assuming position by requiring system owners to remediate high and medium findings within 10 days of notification.

SCITOR

IT/IA/IM Management Analyst 12/2009 - 06/2010

- Federal Government contractor supporting the *National Reconnaissance Office* (NRO) *Mission Operations Directorate* (MOD*)*
- Supported the *Associate CIO* (ACIO) in the analysis, synthesis, and evaluation of IT/IA/IM policies, procedures, standards, and guidelines--ensured content mirrored the direction of the enterprise and business objectives were not impacted.
- Researched and assisted in the preparation of presentations, submissions, and reports on highly sensitive issues.
- Core member of the Policy and Governance Working Group.

- Provided valuable input on the *Cyber Preparedness and Maturity Model* to improve the cyber posture of the enterprise; substantive comments provided were reconciled and used to support cyber-related decisions across the entire Department of Defense (DoD).
- Led and facilitated an offsite to help the ACIO and staff redefine their vision, mission, goals, and top priorities to ensure alignment with the strategic direction of the enterprise--recommendations included *expanding the vulnerability remediation and IA function*, *influencing the strategic direction of the organization through business and IT alignment*, and *collaborating with internal and external agencies to accurately identify and manage enterprise IT investments*—these recommendations were adopted and significantly improved efficiency of operations across the enterprise.

Science Application International Corporation (SAIC)
Principle Systems Engineer 04/2006 - 12/2009

- Federal Government contractor supporting the *National Reconnaissance Office* (NRO) *Imagery Intelligence Systems Acquisition Directorate* (IMINT) *Aerospace Data Facility East* (ADF-E)
- Provided Information Technology, Infrastructure, and Program Management support to the Technology Service Center (TSC).
- Served as Project Manager for several high-visibility IA projects
- Researched and evaluated new technologies, products, systems, and data sources for potential threats, impacts and risks to mission and information integrity.
- Served as the Site Manager for all IT, IM, and IA actions and IT governance activities to ensure systems and processes are compliant with FISMA and local policies.
- Represented TSC at executive-level engineering meetings and CIO Forums to address IT management issues.
- Worked closely with the Chief Information Officer to align enterprise-wide IT planning efforts.
- Core member of the *Information Technology Action Group* (ITAG).
- Project Leader of an enterprise working group charged with identifying and consolidating common processes and business tools to increase resource efficiency throughout the enterprise—combined disparate efforts reducing duplicate efforts by 50 percent.