Michael Ibidapo
Washington, DC
cybersocmike@gmail.com
240-601-8921

OBJECTIVE:

Experienced and dedicated Security Analyst actively seeking a position as an IT Security Analyst, applying the wealth of hands-on technical training and work experience gained over the years, to help protect and maintain the Confidentiality, Integrity and Availability of the IT infrastructures. Possess strong analytical and communication skills, ability to work collaboratively with other team members, strong decision-making skills, and ability to juggle multiple priorities.

TECHNICAL SKILLS:

Windows, PeopleSoft, LAN/WAN, TCP/IP, DMZ, IPS/IDS, Oracle Enterprise Manager, ISO 27001, SAN 20 critical security controls, PCI compliances, FIPS, STIG, DoD 8500.2, DITSCAP, DoD 8510.bb, Nessus, Tripwire, Symantec, ManageEngine, IRONSCALES.

QUALIFICATIONS:

- Cyber Security Analyst with over 7 years of working experience.
- Detailed knowledge of Certification and Accreditation (C&A) activities related to accreditation of core mission to support systems and the development of system releases.
- Experienced with the development of E-Authentication and FIPS-199 worksheets.
- Perform updates to System Security Plans (SSP), Risk Assessments, Incident Response Plans, create Change Control procedures, and draft Plans of Action and Milestones (POAMs).
- Working knowledge of NIST [...] 18, 115, 137, 30, 34,200, 53Ar4, 60 vol 1&2, NIST 37 RMF, FIPS 199 and FISMA guidelines to comply with Federal and private agencies.
- Knowledge and sound understanding of the Risk Management Framework.
- Knowledge of MS Excel Spreadsheet and other FISMA tracking systems/tools to implement six steps NIST RMF aim at managing, monitoring and tracking ATO, POA&M, continuous assessment and ongoing authorization.

Michael Ibidapo
Washington, DC
cybersocmike@gmail.com
240-601-8921

Professional Experience

Security Analyst – Walmart

November 2018- Present

- Provided safety reports and data analysis to building managers to inform security processes.
- Advise the Information System Owner (ISO) concerning the impact levels for confidentiality, integrity, and availability for the information on a system.
- Determine security controls effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements).
- Perform incremental Webapp scanning using WebInspect
- Utilize Symantec for EndPoint protection
- Successful completion of FY18 & FY19 Independent Assessment and ATO
- Create and review security artifacts.
- Event monitoring and daily documentation using Manage Engine (EventLog Analyzer)
- Use SysAid and Active Directory to conduct Help Desk responsibility: Password reset, create new contractor account, personal work folder, server account and assign RSA software token.
- Utilized Tripwire to generate and assess Security logs, Device inventory, Global monitory policy, monthly file system changes and system access control report.
- Collaborated with external vendors to perform penetration tests on network devices, operating systems, and databases.
- Developed risk assessment reports to identify threats and vulnerabilities.
- Ability to capture and evaluate vulnerabilities, document, and report findings to include real-world criticality, and make recommendations for improvement.
- Create and review security artifacts.
- Reviewed and update system categorization using FIPS 199, Initial Risk Assessment, E-authentication, PTA, PIA, SAR, SSP, SAP & POA&M.
- Partner with procurement and Legal team members to ensure the requested vendor meets all guidelines and assist with drawing up vendor contract.
- Review, audit and monitor reports related to consumer and client activities.
- Generate Security Impact Analysis (SIA) Documentation regarding new project implementation.
- Perform on-site security testing to detect potential risks using vulnerability scanning tools (Nessus and Symantec End Point).
- Perform quarterly Incident Response Plan & Test documentation.

Michael Ibidapo
Washington, DC
cybersocmike@gmail.com
240-601-8921

- Identifying incidents and make recommendations to protect the network.
- Assist in the administration and integration of security tools to include new data/log sources, expanding network visibility and automation.
- Utilizing IRONSCALES to classify potential harmful emails as phishing, spam or false positive.
- Manages and executes multi-level responses and addresses reported or detected incidents.

Security Analyst/Vulnerability Analyst-JetBlue Airline
APRIL 2015- September 2017

- Provided security expertise and support to internal teams on security-related projects and initiatives.
- Conduct risk assessments and collaborate with clients to provide recommendations regarding critical infrastructure, network security operations and Continuous Monitoring processes.
- Work with Information Systems Security Officers (ISSO) to ensure FISMA documentation, ATO planning, and execution is completed in a timely manner.
- Document and finalize Security Assessment Report (SAR).
- Participate in ST&E Kick-off Meeting and populate the Requirements Traceability Matrix (RTM) per NIST SP 800-53A.
- Development of Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA) by working closely with the Information System Security Officers (ISSOs), the System Owners, the Information Owners, and the Privacy Act Officers.
- Review and update of the System Security Plan (SSP) using NIST SP 800-18 guidelines.
- Implementing, reviewing, maintaining, and monitoring Information Security Management Systems involved in International and commercial projects in accordance with Sans-20 critical controls.
- Perform Incident Response as part of a team using NIST 800-61 Rv2 as a guide.
- Used snort to identify and monitor unauthorized and anomalous behavior on the network.
- Perform on-site security testing using vulnerability scanning tools such as Nessus.
- Manage vulnerabilities with the aid of Nessus and Microsoft Baseline Security Analyzer (MBSA 2.3) Vulnerability Scanners to detect potential risks on a single or multiple assets across the enterprise network.
- Perform Pen-testing quarterly as part of Continuous monitoring using Wireshark.

Cyber Security Associate/Junior Analyst – Computer Service Inc.
Washington, DC

Michael Ibidapo
Washington, DC
cybersocmike@gmail.com
240-601-8921

May 2014 to April 2015

- Work with ISSOs to ensure documenting and remediating audit findings, security planning and reporting, and mitigation of security vulnerabilities are completed in a timely manner.
- Specialized in areas of Information Technology (IT) such as Network Security, Cyber security, Information Assurance (IA), Security Assessment and Authorization (SA&A), Risk Management, System Monitoring.
- Review PCI DSS Compliance audit for commercial projects to confirm the design and operating effectiveness of the controls.
- Monitoring Information Security Management Systems involved in International and commercial projects in accordance with ISO/IEC 27000 series (ISO/IEC 27001-27005).
- Monitor controls post authorization to ensure continuous compliance in accordance with FISMA guidelines.
- Perform risk assessments for various government contracting organizations and application systems - including reviewing evidence, interviewing personnel, tests, and inspections, producing assessment reports and recommendations.
- Assisted in the development of an Information Security Continuous Monitoring Strategy to help companies in maintaining an ongoing awareness of information security (Ensure effectiveness of all security controls), vulnerabilities, and threats to support organizational risk management decisions.

Educational Background

- Bachelor's in criminal justice with Minor in Technology – UMES (2014)

Certifications

- COMPTIA Security+
- COMPTIA CySA+
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- IBM Cybersecurity Analyst Specialization
- SAFe 5.0 Product Owner/ Product Manager – Scaled Agile
- Certified Scrum Master (CSM)
- Certified Information Systems Security Professional (CISSP)- In Progress
- Global Information Assurance Certification (GIAC)- In Progress

Skills

- IT Operations

Michael Ibidapo
Washington, DC
cybersocmike@gmail.com
240-601-8921

- Cybersecurity risk assessment and management
- Threat analysis and mitigation
- Vulnerability scanning and penetration testing
- Incident response and management
- Network security and firewalls
- Security information and event management (SIEM)
- Security policies and procedures development
- Regulatory compliance (e.g., PCI DSS, HIPAA, etc.)
- Endpoint security and anti-virus solutions
- Data encryption and protection
- Identity and access management
- Cloud security
- Vendor Management & Compliance
- Microsoft Excel
- Microsoft Office
- Microsoft PowerPoint
- Microsoft Word

References: Available upon request.