Jessica Claire

100 Montgomery St. 10th Floor
(555) 432-1000 - resumesample@example.com

Professional Summary

IT Security Analyst with 5years Experience of performing research, analysis, and troubleshooting to identify, resolve, and explain complex security issues
Cybersecurity, Incident Management, and IT compliance support across the Enterprise Infrastructure
Cybersecurity capabilities and risk management to ensure network and IT systems are protected against cyber-attacks and malicious intrusion.
Security policy interpretation and implementation requirements ensure confidentiality, integrity, availability of information, systems, and network.
Security Assessment and Authorization (SA&A) professional knowledgeable in Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), security life cycle and vulnerability management using FISMA, and applicable NIST standards.
Implemented the Continuous Monitoring process of the RMF to perform near real-time risk management and continuous information systems authorization
Highly motivated, organized and results and detail-oriented with excellent interpersonal, communication, and presentation skills

Skills

- **Security Technologies**: Nessus Security Center, Nmap, Wireshark, IDS/IPS; Log Management, Anti-Virus Tools; (Norton, Symantec).
- **Application:** MS Office (Word, Excel, Outlook, PowerPoint, Access); Wireshark, NMAP, Nessus, ArcSight, SharePoint, CSAM, STIGs, and SCAP
- **Operating Systems**: Unix-Based Systems (Linux); Windows.
- **Software**: MS Office (Word, Excel, Outlook, Access, PowerPoint)
- **Ticket Systems**: ServiceNow, Remedy

Work History

09/2019 to 09/2021 **Risk Management Analyst**
Akebono – Remote Supplier Risk Management Planner Elizabethtown, KY

- Reviewed contracts and agreements to identify potential risks and ideal mitigation strategies.
- Developed short-term goals and long-term strategic plans to improve risk control and mitigation.
- Promoted enterprise-level risk management practices and helped instill strong culture focused on protective policies and procedures.
- Investigated allegations to check validity and recommend actions to minimize risk.
- Verified certificates of insurance for accuracy and conformance with internal risk management policies and coordinated issuance to individuals and entities.
- Arranged risk management team meeting by preparing materials, updating calendars and setting up conference spaces.
- Assisted with minimizing risk exposure by reviewing claim validity and viability against coverage standards.
- Maintained current team documentation, validated codes and tracked invoices to keep accounts and records current.
- Supported five member risk management team with multifaceted administrative assistance such as organizing and transmitting records.
- Administered RMIS system data imports, configuration changes and user issues.

06/2017 to 08/2019 **Information Security Analyst**
Cambridge Savings Bank – Cambridge, MA

- Reviewed violations of computer security procedures and developed mitigation plans.
- Monitored computer virus reports to determine when to update virus protection systems.
- Developed plans to safeguard computer files against modification, destruction or disclosure.
- Encrypted data and erected firewalls to protect confidential information.
- Monitored use of data files and regulated access to protect secure information.
- Conducted security audits to identify vulnerabilities.
- Performed risk analyses to identify appropriate security countermeasures.
- Engineered, maintained and repaired security systems and programmable logic controls.
- Recommend improvements in security systems and procedures.
- Researched and developed new computer forensic tools.
- Carried out day-day-day duties accurately and efficiently.
- Developed and implemented performance improvement strategies and plans to promote continuous improvement.
- Demonstrated respect, friendliness and willingness to help wherever needed.
- Actively listened to customers, handled concerns quickly and escalated major issues to supervisor.
- Prepared a variety of different written communications, reports and documents to ensure smooth operations.
- Created plans and communicated deadlines to ensure projects were completed on time.

01/2015 to 04/2016 **Information Security Analyst**
Cambridge Savings Bank – Melrose, MA

- Performs vulnerability scanning with Nessus to detect potential risks on single or multiple assets across the enterprise network.
- Develops, coordinates, implements, and maintains standards and procedures to protect information systems and data security and integrity.
- Provides review and updates on System Security Plan (SSP), security categorization, Security Assessment Report (SAR), Privacy Impact Analysis (PIA), Privacy Threshold Analysis (PTA), and Contingency plan (CP).
- Observe and analyze traffic to learn valuable lessons from known malicious actors and determine countermeasures against such threats.
- Provides detailed status updates on existing cybersecurity incidents daily to follow-up with client/customer to ensure satisfactory resolution.
- Develops risk assessment reports, identifying threats and vulnerabilities applicable to the system.
- Evaluates the likelihood that vulnerabilities would be exploited and assess the impact associated with this threat and vulnerabilities.
- Apply required security patches within NIST and enterprise guidelines
- Conducts kickoff meetings to categorize the system according to NIST requirements of Low, Moderate, or High System (FIPS 199 and SP 800-60)
- Conducts security control Assessment to assess the adequacy of management, operational, privacy, and technical security controls implemented.
- Prepares systems certification and Accreditation package, ensuring that management, operational, and technical security controls adhere to a formal and well-established security requirement authorized by NIST 800- 53v5.
- Develops Security Assessment Report (SAR) detailing the results of the assessment along with the Plan of Action and Milestones (POA&M)
- Develops System Security Plans (SSP) to provide an overview of system security requirements and describe the controls in place or planned by information system owners to meet those requirements
- Performs system risk management following the NIST risk management framework
- Conducts security assessment on assigned systems to ensure FISMA compliance following NIST SP 800 publications, especially NIST 800-53rev 5, 800-53A, and Federal Information Processing Standards (FIPS).
- Collaborates with ISSOs to request assessment evidence lists, set up assessment interview meetings, review SSP documents, and review system boundaries.
- Enterprise system security plan, Risk assessment, and Privacy policies development
- Perform incident response to investigate and resolve computer security incidents.
- Develop follow-up action plans to resolve reportable issues and communicate with other Analysts to address security threats and incidents.
- Prioritize and differentiating between potential intrusion attempts and false alarms.
- Assist with developing processes and procedures to improve incident response times, analysis of the incident, and overall SOC functions.
- Provide Incident Response (IR) support when analysis confirms actionable incident

01/2014 to 12/2014 **IT Support Specialist**
Bombas – Remote (Tri-State) Or New York, NY

- Developed and tested new product offerings prior to release to assist development team in bug identification.
- Provided technical support for all operating system platforms in both internal and external customer scenarios.
- Managed I.T. requests order fulfillment (hardware and software) and assisted with deployment to the end-user community.
- Recreated user problems, recommended solutions, and facilitated escalation when required.
- Engaged appropriate management level and tier 3 for complex issues and liaises between customer and solutions group.
- Reviewed documentation and education courses to give a user's point of view: reported design, reliability, and maintenance problems or bugs.
- Tracked hardware location changes, ensured accurate accounting of assets, coordinated the return or pick-up of surplus/unused I.T. hardware, and disposed of retired assets.
- Prepared and processed incoming shipments of I.T. equipment and maintained the organization of I.T. storage areas.
- Ensured the proper tracking of I.T. asset inventory levels by conducting audits and physical inventories.
- Prepared and imaged new (desktops and laptops) and provided break/fix support, and prepare assets for disposition
- Provided detailed descriptions of issues in the trouble ticket system and followed up diligently to ensure swift resolutions
- Provides on-site as well as remote hardware, software support, and roll-out of Windows to all users
- Ensured the proper tracking of I.T. asset inventory levels by conducting audits and physical inventories

Education

12/2012 **Bachelor of Science**
Imo State University - Nigeria

Certifications

CompTIA Security+
CAP - In Progress
CISSP- In Progress