Security Analyst

Keerthi Samhitha Kadaveru
Email: *keerthiofficial12@gmail.com*
Ph. No: *+91-7981753911*

Professional Summary:

- Adept at conducting thorough audits, identifying vulnerabilities, and providing effective risk mitigation strategies. Excellent communication and collaboration abilities, working closely with cross-functional teams to promote a security culture within organizations.
- Proven track record of delivering high-quality audit reports and recommendations.
- Seeking a challenging role as an ISO 27001 Auditor to leverage expertise and drive information security excellence.

Technical Skills

RDBMS Server	**MS SQL Server 2012, My SQL**
Operating Systems	**Windows 7,10, VMWare.**
Programming Languages	**C, JAVA, Python, HTML, IoT**
Office Applications	**MS Outlook, MS Office applications**
Methodologies	**Agile, Waterfall**
Reporting Tools	**Power BI**

Education

- Bachelor's in Electronic and Communication Engineering
  Jawaharlal Nehru Technological University, HYD
- Schooling in Johnson Grammar School[ICSE]
- PCM in DAV school [CBSE]

Work Experience

Organization: Capgemini ***October 2021 – Current***
Security Analyst
Security Operations and Compliance, CIS India

Responsibilities:

- Perform risk assessments and execute tests of data processing system to ensure functioning of data processing activities and security measure
- Review violations of computer security procedures and discuss procedures with violators to ensure violations are not repeated.
- Document computer security and emergency measures policies, procedures, and tests.
- Confer with users to discuss issues such as computer data access needs, security violations, and programming changes.
- Coordinate vulnerability assessments or analysis of information security systems.

- Develop information security standards and best practices.
- Review security assessments for computing environments or check for compliance with cybersecurity standards and regulations.
- Conducted ISO audits for various clients, assessing their compliance with standards, regulations, and internal policies.
- Prepared detailed audit reports, including findings, recommendations, and corrective actions to ensure adherence to ISO requirements.
- Developed and implemented customized audit plans, procedures, and checklists based on client needs and specific industry standards.
- Collaborated closely with clients' management teams to address non-conformances, recommend process improvements, and facilitate corrective actions.
- Evaluate the organization's adherence to the CIS and ISO 27001 standards to identify any gaps or non-compliance related to ransomware prevention, detection, and response.
- Conduct a comprehensive risk assessment to identify potential vulnerabilities and threats related to ransomware attacks. This assessment to be aligned with the risk management processes outlined in CIS and ISO 27001 standards.
- Assess the organization's implementation of the recommended security controls provided by CIS and ISO 27001. Performed audits to mitigate the risk of ransomware attacks and ensure the confidentiality, integrity, and availability of critical information.
  Evaluated the organization's system monitoring and logging practices to ensure that suspicious activities related to ransomware attacks are promptly detected and responded to. This should align with the guidelines set forth by CIS and ISO 27001.
- Assess the organization's backup and recovery procedures to ensure that critical data can be restored in the event of a ransomware incident. Verify that backups are performed regularly, stored securely, and tested for integrity and availability.

Cybersecurity Incident Response Measures project
Analyst
Security Operations and Compliance, CIS

- Conducted comprehensive risk assessments to identify potential cybersecurity threats and vulnerabilities, enabling prioritization of response efforts and resource allocation.
- Incident Response Plan Development: Led the development and refinement of the organization's incident response plan, aligning it with industry frameworks and best practices. Defined clear procedures, roles, and responsibilities for effective incident handling and escalation.
- Engaged in GRC (Governance, Risk, and Compliance) activities, contributing to risk assessment and management.
- Collaborated in ensuring information security compliance and efficient disaster recovery processes.
- Security Controls Review: Assessed the effectiveness of existing security controls and technologies to detect and mitigate cyber threats. Identified areas for improvement and recommended enhancements to strengthen the organization's security posture.

- Documentation and Reporting: Maintained detailed documentation of incident response activities, including incident timelines, actions taken, and lessons learned. Generated post-incident reports to share insights and recommendations for continuous improvement.

Data Migration project
Quality Assurance testing

- Proficiently utilized SQL scripting used MS SQL, MySQL, SQL Developer.
- Data validation was performed at different levels, including Source, Landing, Staging, and further to XREF (Cross-Reference) and BO. Executed various test cases to validate the data at different stages of migration.
- Worked on DCR testing, Regression testing
- Focused on UI testing to optimize user experience and interaction during the data migration phase.
- Executed comprehensive regression testing to guarantee data consistency and integrity across all migration stages.
- Leveraged Postman for API testing, ensuring seamless integration of web services and data interactions.
- Utilized ALM (Application Lifecycle Management) to efficiently manage test cases, requirements, and defect reporting, adhering to industry best practices and quality standards.
- Used application such as Beyond Compare to verify and validate data changes, maintaining high-quality data standards.

Skills and Qualifications

- Proficient in CIS Controls framework and implementation.
- Extensive experience in conducting ransomware audits and risk assessments.
- Strong knowledge of security controls evaluation and compliance assessment.
- Skilled in incident response planning and execution.
- Expertise in developing and delivering security awareness training.
- Identify and report security breaches or emergency situations.
- Served as a point of contact for stakeholders from multiple locations
- Thorough understanding of regulatory compliance and data privacy.
- Proficient in vulnerability assessment and threat mitigation.
- Strong documentation and reporting skills for audit findings and recommendations.
- Excellent communication skills for cross-functional collaboration and stakeholder engagement.

Personal Projects-

- IoT project - Multiple motion control system of robotic car using Raspberry Pi

- RDMS project - Application with robust role-based access control (RBAC) mechanisms