SS

SANKET SARFARE

Experienced Information Security Professional ISO 27001 LA

Profile Summary

Information Security Risk Management Professional with 6 years of experience in core areas of:

Data Leakage Prevention (DLP), Document Rights Management Solution (DRM/IRM), Malware, Endpoint Security EDR and Endpoint Compliance, Server Hardening, Database Activity Monitoring (DAM), Privilege Identity and Access Management (PIAM), Network Access Control (NAC), Vulnerability Assessment, Technical/Config. Audit, Secure SDLC process management, Data Security, Information Security Policies and 27001 Procedures. ISO compliance

ADDRESS

Kharghar, Navi Mumbai PHONE 98207 59806

EMAIL

sarfare_sanket@rediffmail.com

WORK EXPERIENCE

Reserve Bank Information Technology Manager- Cyber Security 17th June 2019 - Current

- Working as the lead manager for Data Security initiatives and procedures and advise business users to secure sensitive information in documents by using Document or Information Rights Management solution. (DRM / IRM)
- Assist in managing Secure Software Development Life Cycle (S-SDLC) processes and develop S-SDLC guidelines for enterprise applications
- Provide best practices and recommendations regarding application security risks in the SDLC and ensure that security design flaws are understood by development teams and identified risks are mitigated.
- Define and manage the ongoing refinement of Database Activity
 Monitoring solution implemented for the Bank.
- Manage processes and procedures in the development and implementation of polices on Endpoint Security solution to counter malware threats.
- Perform regular review of activities performed by the Access Control Group administrators.
- Review all security reporting completed by the IT security team and provide weekly summaries to the Assistant Vice President and CISO.
- Research and evaluate new technological controls such as EDR and Endpoint Compliance management solution
- Proactively identify technical and architectural risks, commenting and/or providing alternatives for improvement.

CERTIFICATIONS

Information Security Compliance and IT Process Management

ISO 270001:2013 LA LEAD AUDITOR

ITIL 4
FOUNDATION

SPECIALITIES, SKILLSETS and TECHNOLOGIES

Data Security
Seclore IRM/DRM

DLP and Endpoint Security
Forcepoint
Symantec
McAfee VSE

Privilege Identity Management
CyberArk
Arcos

Network Security
Checkpoint Firewall
QualysGuard

- Work to align advanced technologies and Privacy by Design principles from the first stages of development throughout the Secure SDLC and ensure that the data use meets established regulatory compliance needs and privacy requirements.
- Research and develop approaches based on knowledge of system software and organizational design standards, policies and authorized approaches such as OWASP Top 10 Secure Coding Guidelines, NIST Cybersecurity Framework, Data Privacy guidelines, relating to secure application design and development
- Identify and apply a broad knowledge of internal security audit
 policies and practices, risk assessment methodologies and
 reviews to implement and maintain compliance requirements as
 per ISO 27001 in order to facilitate the company's Risk and
 Compliance management process.
- Develop Security Processes, Standards and Guidelines.
- Monitor compliance with the organization security policies and procedures among employees, contractors and third-party alliances.
- Working knowledge of national and international regulatory compliances and frameworks such as NIST, ISO, RBI Security guidelines and Data Protection Bill.

Wipro Technologies Cybersecurity Implementation Engineer 20th October 2014 - 30th May 2019

- Led the design & implementation projects of Anti-Virus solutions like McAfee VSE, Symantec Endpoint Protection Manager and Trend Micro Office Scan.
- Design & implementation of Forcepoint Endpoint and Email DLP in KBL Bank.
- Performed Configuration Audits of Cyber Security controls such as Anti Malware and Data Leakage Prevention solutions.
- Worked on multiple Cyber Security products for deployment and operations including Checkpoint Firewall, Cyber Ark, ARCOS and Portwise.
- Worked on Imperva Web Application Firewall for daily L1 incident tasks and weekly reporting purpose.

- Performed Vulnerability Assessments on periodic basis using Qualys Guard.
- Worked on incident management support operations as an L1 Security Administrator.
- Create and deliver reports to business lines pertaining to endpoint security, compliance etc.
- Manage Symantec Endpoint Protection Manager (Agent deployment/ setup correlation and rule tuning).
- Completed POCs for various Cyber Security products for esteemed organizations in India such as SBI Capital.

EDUCATION

Vellore Institute Technology
December 2014 - October 2018
MTech in Information Technology

Pillai's College of Arts, Science & Commerce July 2011 - April 2014 BSc in Computer Science

PERSONAL HOBBIES

Football, PlayStation, Photography and Reading