# VIJAY KAMBLE Enterprise Solutions Architect Email: - kamblevijay1@gmail.com Cell Number: - 3026108531

* Enthusiastic Enterprise Solutions Architect with 20 years of demonstrated background in Cyber& Information Security, Cloud Security, Privileged and Identity Management, Data Protection, and risk-based compliance including ISMS, PCI-DSS, HIPAA, and using industry-recognized standards (ISO 27000, NIST 800 Series, CSA, and ITIL) with an extensive working experience in Managed Service and FinTech & Healthcare Industry. Excellent Program Management & Internal Auditor in completing complex assignments while providing virtual collaboration with international teams.
* Define the security features required to support security model specifications. Evaluate enterprise and application security design alternatives, including but not limited to control enforcement capability, ease of use, and cost. Proactively anticipate security threats and identify areas of weakness in enterprise technology infrastructure and business applications. , Conduct reviews of security architecture and platform/service designs, and audit source code. Drive open innovation in product security best practices through industry collaboration. Provide product security-related coaching and mentoring to elevate the security expertise of development teams.

# EDUCATION/TRAINING/CERTIFICATION

Master of Business Administration from Sikkim Manipal University Information Technology, Mar 2009

Diploma in Industrial Electronics Engineering from M.H. Saboo Siddik College of Engineering, 2002

**Certifications:**

* **Completed ITIL Certification V2/V3**
* **Completed VMware VCP 3, VSphere 4, VSphere 5 (VCP-510) certification.**
* **Completed VCA-CLOUD, VCA-WM, VCA-DCA certification.**
* **Completed PRINCE-2 FOUNDATION and PRACTITIONER certification.**
* **Completed CCSA\CCSE (GAIA) Certification**
* **Completed Splunk 6.x Fundamentals Certification**
* **Completed Zscaler Certified TAC Associate (ZCTA)**
* **Completed Zscaler Certified Cloud Administrator - Internet Access (ZCCA-IA)**
* **Completed Zscaler Certified Cloud Administrator - Private Access (ZCCA-PA)**
* **Completed [Certified Information Systems Auditor (CISA)](https://www.investopedia.com/terms/c/certified-information-systems-auditor.asp" \l ":~:text=Certified%20Information%20Systems%20Auditor%20(CISA)%20refers%20to%20a%20designation%20issued,and%20Control%20Association%20(ISACA).)**
* **Completed Certified Information Security Manager (CISM)**
* **Completed Project Management Professional (PMP)**
* **Completed Microsoft Certified: Azure Security Engineer Associate "Azure"**
* **Completed AWS Certified Security – Specialty "AWS"**
* **Completed AWS Certified Solutions Architect Professional “AWS"**
* **Completed Google Cloud Certified Professional Cloud Architect"GCP"**
* **Completed Coursera training certification for Google cloud "GCP."**
* **Completed TOGAF 9.0 Enterprise Architect certification.**

|  |  |
| --- | --- |
| **Cloud Technogies** | AWS, Azure,GCP, Zsclaer. O365, |
| **Cloud Security & Compliance** | AWS Gurdduty , Insector,CloudTrail.Network Firewall,Shieldm, WAF,Firewall Manger,Macie,KMS,Manager,Secrets Manager,Detective,Elastic Disaster Recovery, Key Management Services, Certificate Manger, Detective ,Audit Manager, Artifact. Azure Kubernetes Service (AKS) ,Azure Policy,Azure Resource Mover,Key Vault,Monitor,Azure Sentinel,Managed Security Services,Microsoft Defender Advanced Threat protection  Microsoft Security Center, Anomaly Detector,API Management. Azure Active Directory (Azure AD) |
| **Palo Alto** | Prisma cloud , IPS,IDS,APPID,USERID.Firewall, |
| **Zsclaer** | Internet Access, Private Access, Zero trust |
| **Cloud App Security** | OWAP, Pen testing, Threat modeling , Application DR/BR Test ,Rapid7 "Vulnerability Management" |
| **Cloud Technogies** | Containerization, Kubernet cluster, Web App, Work load Management |
| **Identity Management** | Azure AD, RBAC,SSO,OpenID,Oauth ,Zap |
| **Programming Languages** | .Net. C, C+, Pearl, Python. C-sharp,Poweshell |
| **SIM Tools** | Smarts, HPNA, Alogsec NetScout, HPOV, SmartsIC, Solar Winds, TCPDUMP, SkyBox, Splunk, Arcsight, SourceFire, Gigamon |
| **GRC Tools** | SAP GRC,AuditBoard,IBM OpenPages,StanderFusion |

##### Elevancehealth -Remote Nov. 2022-till today

##### Rôle ;- Enterprise Solutions Architect

##### Responsabilités :

* Lead the design and implementation of Enterprise solutions architectures and solutions spanned across multiple departments and functions.
* Analyze and establish security requirements for cloud-based systems and applications.Assess the capabilities, features, and compatibility of different GRC solutions.Collaborate with stakeholders to gather and define requirements for the new GRC application.
* Work closely with application development teams to ensure the secure deployment and maintenance of cloud applications and infrastructure.
* Provide expertise and guidance on security issues related to the cloud, including identity and access management, network security, application security, and data security.
* Develop GRC security policies, standards, and guidelines.
* Work closely with Security team on risk assessments, vendor security assessment of in-house and 3rd party platforms and security audits of the cloud environment.
* Respond promptly to cloud security incidents, providing detailed post-event analyzes.
* Stay up to date with the latest security trends, threats, and technology solution.

##### HCL- Remote April. 2022 – Oct. 2022

##### Rôle ;- Cloud Security Solutions Architect

##### Responsabilités :

* Land an end-to-end value prop for Security (i.e., Zero Trust) which spans the breadth of Microsoft Security offerings.
* Empower customers in their Microsoft Security adoption journey, helping them to define a Secure strategy, Architecture, and implementation of necessary security controls.
* Security Services including Identity and Access management, Threat Protection, Cloud Security, Information Protection.
* Evaluate and maintain enterprise level cloud infrastructure.
* Drive technical solutions discussions with principal engineers, diving deep into the details to solve complex technical business problems with the goal of crafting scalable, flexible, and resilient cloud architecture.
* Collaborate with technical leads and product owners to understand solution requirements and identify solutions that adhere to industry standards and best practices.
* Practice continuous education through research, documentation, and practice of new technologies.
* Act as a thought leader in the wider community, playing a key role in educating, sharing best practices, presenting at events, writing white papers, blogs, and running workshops.
* Provide insight into technical asks through verbal and visual mediums (UML, etc.).
* Build out prototypes and proof of concepts as needed.
* Write and develop cloud automation playbooks for managing and scaling cloud resources.
* Accountable for estimating, evaluating risks, and technical task prioritization based on requirements.
* Creates, maintains, and publishes system level documentation without direct guidance, including system diagrams.
* Evaluate cost and performance of a solution and evaluate trade-offs.
* Foster and promote Quality processes throughout all stages of system development.
* Perform hands-on activities, supporting the customer in evaluating native security solutions in areas such as Microsoft 365 Defender, Microsoft Defender for Cloud, Sentinel, and Azure Active Directory, among others.
* Accelerate Business Value of overall Azure adoption by improving security posture and ensuring that the solution exhibits “Secure by Design” or “Well-Architected” framework, such as high-performance levels, security, scalability, maintainability, appropriate reusability, and reliability upon deployment. Apply technical knowledge to architect security solutions that meet business needs, infusing key security technologies where appropriate.
* Run Architectural Design Session to build a plan for implementing the solution – governing design in line with customer business goals and their technical environment. Outcome is consensus on solution design and next steps toward production.
* Be a Voice of Customer to share insights and best practices, connect with Global Security teams at Microsoft, Engineering and Product teams to remove blockers and influence the solution roadmap.
* Trouble shoot technical issues to prove value of implementation of Security technologies.

##### Citi - New Castle, DE Oct. 2018 – March 2022

##### Role ;- Senior Security Solutions Architect

##### Responsabilités :

* Major cloud transformation initiative which re-designed and migration all datacenter application and service in cloud.
* Over 15+ years of experience in cloud security designed, management and support "AWS/AZURE/GCP"
* Engage and collaborate with Sr. management to define and understand IT strategy and create new IT capabilities that support company goals, objectives, and milestones.
* Experience with architectural framework (TOGAF, or a hybrid of multiple frameworks).
* Act as an SME relating to all aspects of authentication and access management, to include frontend systems/interfaces and backend providers.
* Ideal resource is VMware centric or is experienced enough to enable Google VMware Engine (GCVE) deployments  
  Migrate VMware workloads to GCVE, hybrid cloud connectivity with HCX and NSX-T, etc.  
  AWS, Azure AWS, AZURE GCP Networking experience (VPC, Firewall, Load Balancer) and 3rd party appliances for example; Palo Alto, F5, etc.
* Support technical integration needs that facilitate connectivity between SSO, MFA , RBAC and other authentication mechanisms, enterprise directory and identity provisioning tool(s)
* Drive adoption of SSO for authentication, always looking for ways to encourage updates from legacy authentication schemes.
* Experience working on Identity management solutions including  
  Microsoft Active Directory, and Active Directory Federation Services. Azure AD
* Lead troubleshooting of cloud security issues, detect and confirm anomalies, identify risks, perform root cause analysis.
* Experience with implementing a cloud-based container vulnerability scanning tool “Prisma/Wiz”
* AWS, AZURE GCP IaaS Services & AWS,AZURE GCP  Products - skilled with AWS,AZURE GCP  architecture, network, security, services, and design
* Able to support the development of a platform hosting solution and landing zones within (AWS, AZURE GCP )
* Support the creation of an operational support model, with focus on integration, automation, DevSecOps, and software defined everything, within AWS, AZURE GCP
* Ability to learn/work with emerging technologies, methodologies, and solutions in the cloud/IT technology space
* Generate and develop reports, rules, dashboards and policies to identify and alert on compliance issues
* Ensure that all procedures and rules of use for information systems comply with information security policies.
* Ensure that appropriate risk assessments are performed to evaluate the effectiveness of existing controls, including periodic penetration testing of critical information systems.
* Manage log and entitlement reviews of critical systems to protect Dime’s information assets from internal and external threats.
* Adaptability to meet changing priority demands in a fast-paced environment.
* Deep working knowledge of configuration and administration of DevOps tools, specifically GitHub and Azure DevOps Enterprise
* Strong understanding of git and branching workflows such as Gitlow, Feature Based, Trunk Based, etc.
* Strong knowledge in scripting including Powershell, Python, and bash/zsh
* Strong knowledge in using REST APIs and troubleshooting integrations.
* Use metrics to measure, monitor and report on the effectiveness and efficiency of information security controls and compliance with information security policies, in order to support the annual information security risk assessment.
* Ensure the development and delivery of activities and programs that can positively influence information security culture and the related behavior of its staff, including information security education and awareness.
* Maintain day-to-day operational effectiveness of the Professional Services Team including service desk level 3 escalations, customer on-boarding, and customer projects.
* Monitor, maintain, and manage service level agreements with the internal and company client infrastructure.
* Support the development and execution of controls to monitor cyber security compliance and drive organizational change.
* Environment with security building blocks design that will cover 3rd party technology integrations in the areas of IAM, CSPM, Security Operation.
* AWS, AZURE GCP foundation design, focusing on Google Identity and Access Management (IAM), Network, Data Security, Logging/Monitoring and Security Operation platforms.
* AWS, AZURE GCP environment with security building blocks design that will cover 3rd party technology integrations in the areas of IAM, CSPM, Security Operation and Networking.  
  Deploy designed the Security controls using Infrastructure as code (IaC) and Policy as code (PaC) implementation, will test, optimize, document and handoff operation and maintenance SIEM.
* Deploy designed the Security controls using Infrastructure as code (IaC) and Policy as code (PaC) implementation, will test, optimize, document and handoff operation and maintenance.
* Develop a renewal and upgrade schedule for company and client infrastructure and operating systems.
* Maintain day-to-day operational effectiveness of the Project Team ensuring successful creation, implementation, and completion of internal and client facing projects.
* Attend change control and other departmental meetings to provide insight, make recommendations, and participate in change management and process development.
* Prioritize IT initiatives, assign tasks and actively manage resources, timelines, and delivery schedules.
* Accomplish financial objectives by thoroughly defining the project scope and forecasting the requirements of the project, managing expenses, analyzing the variances, and initiating corrective action.
* Working knowledge of infrastructure technology including network security, endpoint security, data security, and cyber defense Configuration, deploying, and integration Infrastructure into technology platforms supported across globally.
* Develop effective and measurable metrics (KRI, KPI and KCI) to analyse data and proactively identify trends or new/emerging risks
* application development and integration experience using Microsoft technologies (e.g., C#.NET,SSIS, SSRS, SQL Server, Visual Studio)
* Provide advisory consultation to lines of businesses and make course of action recommendations to manage risk
* Lead client service delivery teams in the active execution of Local and global engagements.
* Utilize technical and financial operation and transformation knowledge to identify complex client issues, broaden client relationships and develop a reputation as a thought leader
* Help lead teams in solving complex strategic and tactical problems requiring excellent quantitative analysis skills and present recommendations or solutions to executive leadership teams.
* Build long-term business relationships with key government clients through engagement delivery and networking in professional organizations.
* Contribute to the development and evolution of methodologies and intellectual capital, including contributing to articles, whitepapers, and training efforts.
* Develop and maintain long-term client relationships and network with different Venders.
* Possess in-depth knowledge of business acumen and remain current in its service capabilities and industry knowledge.
* Profound knowledge of industry standards (ISO Norms, particularly ISO 27001, best practices (e.g. ITIL, COBIT)
* Lead and conduct review of processes, policies, procedures, security, and configuration controls of existing systems as well as proposed controls of new systems.
* Conduct a thorough analysis as problem areas is discovered.
* Participate in risk assessment and planning discussions to define audit objectives, scope, and develop audit programs based on the defined objectives.
* Work autonomously in an area of specialization to analyze internal security and provide relevant information to internal and external customers, suppliers, and partners.
* Attend meetings with internal staff to conduct interviews with management and staff of the assigned audit area, as necessary, to gain an understanding of the respective
* Identify risks, controls and gaps within a process or systems.
* Draw conclusions and provide recommendations in a clear, concise and constructive manner, both orally and in writing
* Communicate with departmental representatives and CISO staff with regards to status of audits/projects
* Conduct follow-up work, as necessary, to evaluate corrective action taken by management to resolve previous IT audit observations and ensure County compliance with policies, laws, and regulations.
* Present to various County staff on Audit Procedures and Audit Findings as well as recommendations
* Research and apply industry best practices while challenging an organization or status quo Ensure the effective accomplishment of audits according to the audit plan.
* Provide knowledge transfer to County internal team members by leading knowledge transfer sessions.
* Knowledge or the ability to know and apply applicable laws and deadlines specific to our practice.
* Experience with Infrastructure design, provide strategy solutions with roadmap.
* Participated in developing and implementing various technology selection approaches including RFIs and RFPs security policies and configuration, to maintain of existing systems.
* implementation, maintenance, and support of identity and access management services, platforms, and systems, including access provisioning, governance, multifactor authentication, privileged access, HRIS integrations, and data protection systems.
* Foster a spirit of teamwork and unity among department members and provide oversight and direction to associates in accordance with the organization's policies and procedures.
* Identifies risks of non-compliance and recommend appropriate changes/actions through continuous monitoring and analysis of identity systems and alerts.
* Implantation of firemon firewall optimization and cleanup with Audit readiness.
* Assists with audits supporting clients, regulatory bodies, and internal standards. Actively engages in the greater information security and privacy community (e.g. peer groups, seminars, conferences, etc.) to help identify new technologies, regulations/standards, techniques and partners.

##### Florida Département of Corrections Aug 2017 – Oct. 2018

##### Role :- Security Solutions Architect

##### Responsabilités :

* Expert understanding of SaaS, PaaS, IaaS cloud delivery models, differences between them, and coverage along with the Shared Responsibility Model.
* 7+ years of Expert understanding cloud AWS,AZURE,AWS,AZURE GCP cloud models, and coverage along with the Shared Responsibility Model
* Providing expertise and strategic guidance on critical operations that span multiple systems and groups  
  Monitoring, evaluating, and remediating any health concerns of global firewalls and network devices
* Proactively identify gaps, risks, and issues and navigates organizational structure to resolve them.  
  Identify automation opportunities as well as areas that can be improved to optimize the operation, such as documentation and monitoring infrastured with risk management.
* Collaborate with key risk areas, business partners, and IT counterparts to design action plans to address Cyber security and IAM risk
* Autonomously lead program execution with documented project plans, expectations and schedule
* Provide status reports, escalation and impediment resolution when needed
* Assist in the development, maintenance, and testing of policies (i.e. Incident Response, Business Continuity, Change Management), standards, processes, and procedures to assess, monitor, report, escalate and remediate information security risks and related compliance issues.
* Work with Dime’s business units, Internal Audit, vendors, and other systems professionals to ensure policies and procedures are being complied with and to develop recommendations for improvements, ensure that compliance issues and other variances are resolved in a timely manner, and actively apply innovative solutions to advance Dime’s information security goals.
* Focus on IAM, Data and Workloads security preventive and detective controls
* Develop and maintain technical specifications, standards, procedures, and systems documentation  
  Research and recommend appropriate technical solutions to meet functional requirements.  
  Work with Data Center staff, OIT, and users to perform installations, upgrades, and configuration changes match with global standard.
* Implementation knowledge of Tufin orchestration suite with change Management and Network Security Policy Management.
* Experience communicating and working within cross‐departmental teams and support group.
* Designed and implemented, managed rapid7 Insight and Nexpose suits for vulnerability management of server and desktop, Network security devices.
* Migrated Cisco ASA devices to checkpoint R80.10,20 with policy conversion using Smarts converter tool.
* Configuring URL filtering and SSL inspection policy and implanted across all sites with SIME logs management.
* Configuring and Implemented Zsclarer cloud firewall with SSL inspection & URL filtering with access control rules.
* Implantation of firemon firewall security policy change Management and Network visibility monitoring as well.
* Designed and Implemented CHECKPOINT R80.10/20, Palo Alto, Juniper Zsclarer Internet Access bundled across 30 sites.
* Monitoring, evaluating, and remediating any health concerns of global network security products.  
  Enhances department and organization reputation by accepting ownership for accomplishing new and different requests; exploring opportunities to add value to job accomplishments.
* Strong understanding of ISO standards
* Working knowledge Azure security stack, including Security Center, Azure Monitor, DDoS protection, Key Vault, AIP, Intune, and WAF
* Strong understanding of documentation processes & quality systems
* Site management representative for ISO 27001 Standard)
* Establishes, implements, and maintains Quality Management System (QMS)
* Monitors and measures QMS activities in the organization
* Site lead for External 3rd party audits
* Coordinates and conducts Management Review Meetings
* Develops Internal Audit plans and Audit schedules.

##### Wipro Limited Jul 2005 – Aug 2017

##### Citigroup- New Castle, DE

##### Role ;- Security Solutions Architect

##### Responsibilities :

* Lead 13+ senior architect resource team which is located global to support sun model.
* Determines security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates.
* Enhances security team accomplishments and competence by planning delivery of solutions; answering technical and procedural questions for less experienced team members; teaching improved processes; mentoring team members.
* Plans security systems by evaluating network and security technologies; developing requirements for local area networks (LANs), wide area networks (WANs), virtual private networks (VPNs), routers, firewalls, and related security and network devices.
* Foundation design, focusing on Google Identity and Access Management, Logging/Monitoring and Security Operation platforms.  Controls will be mapped to MITRE ATT&CK Framework
* Implements security systems by specifying intrusion detection methodologies and equipment; directing equipment and software installation and calibration; preparing preventive and reactive measures; creating, transmitting, and maintaining keys; providing technical support; completing documentation.
* Maintains security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs.
* Upgrades security systems by monitoring the security environment; identifying security gaps; evaluating and implementing enhancements. Conducting regular system tests and ensuring continuous monitoring of network security.
* Manage team of 6 resource team which provided global support for citi global datacenter security infrastructure.
* Implemented multiple firewall solutions, network security, and information security practices with SIME tools.
* Integral part of planning, designing, implementing and troubleshooting complex system and firewalls Security devices advanced technologies.
* Experience performing infrastructure technical security assessments for window server with Citrix virtual datacenter.
* Review security and vulnerability advisories, assess risk, relevance, priority and communicate findings
* Identify infrastructure-level vulnerabilities and patches across enterprise-wide assets along with validating successful remediation with support of SCCM management.
* Document, prioritize and formally report asset and vulnerability state, along with remediation recommendations
* Leverage vulnerability database sources to understand each weakness, its probability and remediation options, including vendor-supplied fixes and workarounds
* Expert in driving vulnerability management reporting and providing guidance to IT teams in patching and solutions to mitigate security threats
* Design Implemented and configuration of Cisco USC product so we can manage multiple sites.

##### Ocwen Financial Corporation- Mumbai, India Mar 2005 – Jul 2005

##### Global Field Services Engineer (System & Network)

##### Responsabilités :

* Responsible for the System and Network Management for more than 4000 local and remote system and network devices including design, implementation and 24x7 support
* Initial build for network devices such as switch and backbone configuration.
* Managing router and switch config and monitoring with local Evault application
* Worked on checkpoint R65 firewall for migration Linux and Nokia Box.
* Monitoring 28 sites and total 3080 devices including with router and switch with servers.
* Installation & Administration of Microsoft Services like DNS, DHCP, WINS, TCP/IP & IIS
* Selected from team to train on Checkpoint firewall R65 gateway.
* Involved in project to rebuild and migration on the entire checkpoint gateway

##### Team Serve IT services Pvt. Ltd. - Mumbai, India Mar 2004 – Dec 2004

##### System Administrator

##### Responsabilités :

* Installation, Support & Administration of Windows NT Servers Exchange 2k3 & 2k/2k3 Active Directory
* Implemented virus protection analyst using Symantec Anti-Virus 7.x to 9.x Corporate Edition for 20+ servers with 300+ clients. Install, push to NT, 2000 & XP clients, and administer Symantec System Center.
* Administration of Microsoft Windows NT/2000/2003 Server/Advance Server from scratch including un-boxing, rack mounting, loading of Operating System, deploying with MS
* Involved in the implementation on setup of Domain/DSF etc.

##### Mascom Electronic. Mumbai, India Oct 2002 – Mar 2004

##### System Administrator

##### Responsabilités :

* Handling 800 HP/Compaq desktops/Laptops & 20 servers.
* 500 Users are connected to the Domain from various office locations
* Creating user Id’s in Active Directory & Creating Mail ids on Exchange server 2000
* Performing daily backup activities through VERITAS backup software Working for desktop HP Compaq, Dell

