NARENDER
VISHWAKARMA

75, G/3 Sai Enclave, Mohan Garden
New Delhi–110059
+91-9650889777
narender.viskrma@gmail.com
n_vishwakarma

PROFESSIONAL SUMMARY

A Cloud & Application Security Architect with over **15+ years** of experience in designing, implementing, and managing secure cloud & application infrastructures. Experienced in developing secure cloud & Application architectures, developing security strategies and policies, and leading the implementation of security products and services.

SKILLS

- AWS, Azure, Google Cloud, BCP & DRP, PKI, Cisco Umbrella, Zscaler SASE, Dome9
- Database Querying Languages; MySQL, NOSQL/DynamoDB, Windows Shell,
- Palo Alto Prisma, Cortex, Firewall, IDP/IPS, WAF, SIEM, DLP and Proxy
- PAM, MFA, AAA, & Sandboxing, Security Vulnerability Assessment
- Defense in-depth, Malware Detection & Threat Modeling and Risk Analysis
- Trainings- GIAC Cloud Security Certifications & SEC522: Application Security: Securing Web Apps, APIs, and Microservices
- OWASP, SAST/DAST, IAST & MAST
- Docker, Kubernetes, Windows, Unix/Linus and VMware
- ZAP, Burp Suite, Checkmarks, Kali Linux, Nessus, Nmap, Wireshark
- Information Protection and Analysis.
- Governance, Risk & Compliance (GRC).
- TOGAF, CobiT, ISO2700, GDPR, SOX, PCI DSS

CERTIFICATIONS

- *Certified Information Security Manager (CISM)*
- *AWS Certified Security – Specialty*
- *AWS Certified Solutions Architect – Associate*
- Check Point Certified Security Expert CCSE R75.40
- Check Point Certified Security Administrator CCSA R75.40
- Zscaler Certified Cloud Administrator
- Code Bashing Application Security
- Software Development Methodologies (Agile & Waterfall)
- Secure Software Development Lifecycle (SSDLC), DevSecOps, CI/CD Pipeline

Experience

Senior Cloud/Application Security Architect | Fidelity International

DURATION: 31 JUL 2023 – PRESENT

Key Skills:

Application Security:
Vulnerability Management (SAST, DAST, MAST)
Secure Software Development Lifecycle (SSDLC)
Web Application Firewalls (WAF)
Threat Modeling and Risk Analysis (OWASP, NIST)
Secure API Management and Microservices Security

Identity & Access Management:
Privileged Access Management (PAM) (CyberArk, BeyondTrust)
Role-Based Access Control (RBAC)
Multi-Factor Authentication (MFA) (Duo, RSA)
Identity Federation & Single Sign-On (SSO)
Directory Services (Active Directory, Azure AD)

Cloud Security & IAM:
AWS, Azure, Google Cloud Platform (IAM & Security)
Identity Federation and Cloud IAM Integration
Identity Governance & Compliance (SOX, GDPR, PCI DSS)

Principal Duties and Responsible:

- Architect PAM solutions with IAM and role-based access controls.
- Implement PAM monitoring and alerting with CyberArk and BeyondTrust.
- Design access management frameworks with compliance integration.
- Conduct security assessments and audits of privileged accounts.
- Implement controls for privileged access, including session management.
- Develop and enforce policies for secure account access.
- Integrate PAM with cloud security tools for multi-cloud protection.
- Collaborate on refining PAM processes and incident response.
- Implement container security practices like image scanning.
- Design security policies for containerized applications.
- Use tools like Docker Bench for container monitoring.
- Apply CI/CD security practices in the development pipeline.
- Architect cloud security solutions for IAM and encryption.
- Manage cloud security monitoring with AWS, Azure, or GCP tools.
- Design application security frameworks with OWASP principles.
- Conduct assessments and penetration tests for cloud applications.
- Implement controls for serverless applications and API security.
- Develop microservices security policies for authentication and communication.
- Use cloud-native tools for threat protection.
- Implement key management with AWS KMS or Azure Key Vault.
- Ensure compliance with standards like PCI DSS and GDPR.
- Develop incident response and disaster recovery plans for cloud environments.

Cloud & Application Security Architect Lead| Axtria

DURATION: 25 MAY 2020 – 28 JUL 2023

Key Responsibilities:

Principal Duties and Responsible:

- Consulting application security architecture to design secure application platform on NIST special publication (SP) 800-53 applications security framework and Open Web Application Security Project (OWASP) is an Application Security Verification Standard to identifies application security tests and requirements.
- Performing and reviewing the application security testing SCA, Static, Dynamic Security, web application security, cloud security, container security – CNAPP & CSPM scan reports and doing risk evaluation and remediation.
- Working on to identifying and mitigation plan for application vulnerabilities based on OWASP, WASC, CWE, CVE and doing code review and analysis based on source code guidelines as per OWASP' secure architecture (SA) practice
- Working with Application development teams and InfoSec teams to identify threats, vulnerabilities and potential security issues.

Enterprise Architect | PricewaterhouseCoopers LLP

DURATION: 20 JAN- 2020 – 13 MAY 2020

Key Responsibilities:

Responsible for the creation, maintenance and management of IT architecture models and their lower-level components with following responsivities.

Principal Duties and Responsible:

- Definition, implementation, and execution of the processes for the definition, maintenance, and conformance management of the Enterprise Architecture
- Update and maintenance of the key Enterprise Architecture deliverables
- Establishment and maintenance of contacts within business units and information system programs to understand business activities and business drivers, business requirements, solutions strategies, and alternatives, etc., being considered and/or implemented.
- Architectural leadership in the resolutions of inter-program and inter-project issues.
- Ongoing publicity and communication of Enterprise Architecture both within the information community, and the business units.
- Ongoing research and assessment of new analysis approaches for potential use within Enterprise.

Following deliverables:

- Developing the Enterprise Architecture
- Coordinating all Enterprise Architecture activities locally and globally
- Developing and coordinating Architecture Plans
- Assisting in aligning business and enterprise initiatives with the Enterprise Architecture
- Auditing compliance within the Enterprise Architecture standards
- Serving as advisor to senior business management on business and information integration strategies

Cyber Security Architect | Cognizant Technologies Solutions

DURATION: 20 JUN- 2016 – 17 JAN-2020

Key Responsibilities:

Work closely with customers providing technical and security leadership to help protect CTS customers and credit card data from malicious attacks and unauthorized access, providing critical system assessment/audits, architecture security design/review and security awareness training. Align and reinforce business continuity and corporate initiatives through development and

compliance management of information security polices and standards in the areas of physical, account, data, corporate services/applications, network and computer systems, application services, systems services, change management, incident response, and data center security.

- Lead and performed assessment for Mergers and Acquisitions (M&A), Transitioning and Transformation project (T&T)
- Lead PCI DSS compliance projects and reduced assessment scope
- Lead security architecture design and assessment for PKI, MFA and WAF infra

Cloud, Cyber Security and Compliance Role

Providing Cloud Hosting Solution to designing solutions based on Private and Shared Cloud service providers (Amazon AWS, Microsoft Azure and VMware Hypervisor).

- RBAC
- NIST SP 800-53 Security Controls
- OAuth, Cloud SSO
- Identity Provisioning,
- Identity Governance,
- Privileged Access and Identity services
- STIG, Fed RAMP, PCI-DSS

Making strategies remediation plan for current threats, attack vectors and using computer forensics concepts and procedures, investigations, collections, evidence handling, analyzing and preserving digital evidence, Data Security, Identity & Access Management System.

Analyzing complete infrastructure, web application, and internet security along with IAM Application, Network Firewall, Web Application Firewall, Two Factor Authentication integration with VPN and SSL based Applications and DLP (Gateway and Client base).

Network & Web Application Analyst Role

Network & Web Application Scanning Tools: Wireshark, Riverbed NPM & Case Cade, Nmap, Metaspliot, OpenVAS, SQL Map, Nikto and Safe3.

Mange the Root CA Certificates for Websites and Web Base Applications on WAF, Load balancer, Firewall and VPN solutions level.

Security Designer | British Telecom

DURATION: 31 DEC- 2013 – 06 MAY-2016

Key Responsibilities:

Responsible for the design of a project with time and cost estimation for the Security Corporate Data Network. Serving the primary resource for the business requirements and networking & Security standards and ensures that the business requirements satisfy the security of both client and company needs.

Principal Duties and Responsible:

Giving Security Solutions for companies with a robust, comprehensive portfolio of products, services, and expertise to give protection from today's sophisticated advanced threats, viruses and prevent database breaches. Also, maintain security compliances with commercial enterprise and government clients around the globe.

Technical Skills:

- Cisco Cloud Security (CWS)
- Zscaler Cloud Security
- Firewalls (Checkpoint, FortiGate, Cisco ASA & ASASM, Cisco Meraki and Juniper)
- Web Application firewall (F5, Barracuda and Radware)
- F5 (LTM, GTM and ASM), Riverbed & Cisco Designing and Implementation
- Websense, Window ISA & Linux Squid Proxy migration and upgradation.
- Messaging Security: Cisco IronPort, Barracuda & WebSense Configuration and Troubleshooting.
- HP Tipping Point & McAfee IPS Configuration and Troubleshooting
- Compliance Management: SOX, HIPA and PCIDSS including Change Management Process, Access Control and Log Management.

Cyber Security and Consultant Domain Role:

Evaluate existing security systems to determine the potential risk of a breach. The consultant develops policies and procedures that minimize the risk to properties, employees and computer systems. Consultants may also provide evaluations and assessments in collaboration with sales staff for the security business.

Create a System Security Plan (SSP) for all of its major and minor information systems for organizations and set the framework to mitigate specific threats including threat mitigation process, risk assessment, awareness and training, Information protection processes and procedures, security continuous monitoring and planning & analysis.

Security Consultant | Ricoh

DURATION: 24-JAN-2012– 09-AUG-2013

Key Responsibilities:

Protecting computers, networks, software, data or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever-increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.

Network Security Domain Role:

- Firewalls and UTM - Checkpoint (NGX, IPSO,UTM-1),Juniper (SRX & SSG) ,Cisco ASA , Cisco Meraki, Sonicwall (E-Class, NSA and TZ Series), FortiGate, Palo Alto, WatchGuard, and Cyberoam.
- Web Security and Email Security - Cisco IRONPORT Email Security and Web Security, Bluecoat Web Security, Sonicwall Email Security, Websense Triton 7.7 Web Security and Email Security
- Web Application firewall (F5, Barracuda and Radware)
- Data Integrity and Security - Checkpoint DLP, Symantec PGP, Websense DSS, and Trend Micro SLP.
- Network and System Auditing - RSA Envision, HP OpenView, Juniper NSM, and Whatsup Gold.
- Server Load Balancer, WAN Accelerator & Optimizer and SSL VPN - Riverbed, Redware, Sonicwall Aventail E-Class SRA, Array Networks, Citrix NetScaler & Riverbed Stringray and Steelhead.
- End Point Protection & Mobile Security - Symantec SEPM, LUA, Site Replication and HA, Trend Micro -Worry Free, Office Scan, TMCM, McAfee - McAfee Endpoint Protection Suite with ePO.
- Data Center Migration on Cloud - VMware, Microsoft, Akamai and Amazon

Analyst Role:

- Shell Scripting: Unix, Linux and Backtrack (Dos attack program, websites vulnerability assessments and DB vulnerability assessments)
- Analyst the IT Companies or products maintain and report analyzing Responsible for providing network services such as Network upgrades, Migration and issues resolution and for deploying and handling issues related to network and network security configurations based on CR and Incident.
- Plan, project management and implement, on-going network components maintenance and upgrades, patch management, backup process management and all other technical aspects necessary to ensure the ongoing health of the IT environments.
- Other Roles:
- Configure Cloud implementation (Email Servers, FTP Servers, Web Server and Cloud Desktop Replication).
- Compliance Reporting, Management, Security, Risk Fraud and Financial crime
- Configuring and Troubleshooting of Mac OS (XServe, Snow leopard)

Security Consultant | Tmen System

DURATION: 17-JAN 2011– JAN 2012

Key Responsibilities:

1. Configured and troubleshot the Cisco ASA, Cisco Meraki, Checkpoint, Juniper (SRX & SSG) FortiGate, Cyberoam, Astaro and Sonicwall firewalls.
2. Configured Email Security Appliances (IronPort, Barracuda and TrendMicro, Symantec BrithMail Gateway)
3. Configured Server Load Balancer and Link Load Balancer (Citrix and Array Networks)
4. Web Content Filtering (IronPort, Websense and TrendMicro)
5. Configure and Troubleshooting of Routers, L3-L2 Switches, and Wireless Routers
6. Configure Antivirus Server and (Symantec Endpoint Protection, McAfee ePO and Trend Micro)

System Administrator | Esteem Technologies

DURATION: 07-SEP 2008 – JULY 2010

Key Responsibilities:

- Configure Firewall and UTM's - Cisco ASA, Checkpoint, Juniper (SRX & SSG) FortiGate, Cyberoam, and Sonicwall.

- Configure Email Security Appliances (Iron Port, Barracuda and TrendMicro, Symantec BrithMail Gateway)
- Configure and Troubleshooting of Cisco, Juniper and Dell (Routers, L3-L2 Switches), and Wireless Routers,
- Configure Antivirus Server (Symantec Endpoint Protection, Trend Micro & McAfee EPO)

DEGREE | SCHOOLING

1. Pursuing Fin-Tech MBA from IIT Patna
2. Bachelor of Arts from Delhi University North Campus Cell, New Delhi.
3. Full Time Diploma in Computer Hardware & Networking Management from Asia Informatics Center.
4. 10+2 Passed from SERYODYA BALVIDHAYLAY (CBSE), Tilak Nagar, New Delhi.

PERSONAL DETAILS

- Name : Narender Kumar Vishwakarma
- D.O. B : 07th July 1987
- Sex : Male
- Marital Status : Married
- Father's Name : Shri Jaynath Vishwakarma
- Mother's Name : Girija Devi
- Permanent Address : Plot No: -75, G/3 Sai Enclave, Mohan Garden Part III, New Delhi–110059.