SAGAR SHAH
Mumbai
Phone: +91 (965)3662759
Email ID: link2sagar@gmail.com

Professional Summary

Information security, risk management and Cybersecurity technology with over 13 plus years of professional experience.

Eventus TechSol Private Limited. **Duration: July 2023 to Till Date**
Position: Senior Security Architech
Location: Mumbai
Responsibilities:

- Responsible for leading customers on analysis of Cyber Security requirements and resulting pre-sales/solution architecture for those customers - both new and existing. This is a lead pre-sales solution architecture and consultancy role, working on projects for managed security services.
- Considerable experience of a comparable cyber security pre-sales architecture role
- Good knowledge and hands-on experience on Azure and AWS Native security controls
- Expertise in bid response (managed service outsource deals, defining service elements, building cost models, providing content)
- Commercially minded - an intelligent, articulate, consensus building, and persuasive team player who can serve as an effective member of a dynamic pursuit team
- Experience with business system risk management as it relates to information security
- High degree of market awareness with ability to recognise nuances/trends in the market
- Experience with information system disaster recovery planning and testing, auditing, risk analysis, business system resumption planning, and contingency planning.
- Develop Practice charter and work on demand generation.
- Work with the Sales, Technical and Delivery team, Finance team etc. to come up with a competitive proposal response.
- XDR/ MDR managed SOC services.

Tata Communications Limited. **Duration: Feb 2022 to Mar 2023**
Position: Senior Manager
Location: Pune /Ahmedabad
Responsibilities

- Support Clients like Poonawalla fincorp, FMCG like Adani Wilmar for Information security.
- Proactively monitor and identify security issues and potential threats, new vulnerabilities/threats and continuously improve security standards within the organization.
- Support Client DC migration from on premise to Azure cloud on Security and governance point of view.
- Managing the daily operation of CSOC and implementation of the IT security strategy
- Ensuring compliance with the latest regulations and compliance requirements NIST, ISO 27001.
- Responsible for Deliveries for all Infrastructure and info sec engagements and projects
- Provide technical, project and program management leadership in large and complex engagements
- Co-ordinate with Sales & the wider corporate organization to identify opportunities & lead the discussions with customers to define innovative next-generation solutions for their business
- Develop and execute a strategic vision for the infrastructure & cybersecurity practice, aligning it with the overall business objectives and risk management strategy of the organization.
- Managed Team of 45 Direct and indirect reporting.
- Handled 2-3 Clients of Overall Budget 3- 5 cr Each.

Tech Mahindra **Duration: Nov 2020 to Jan 2022**

Position: Associate Security Consultant (SOC Manager)
Location: Pune
Responsibilities:

- Support Telecom clients and sister company client like Eir, H3G(Hutchison 3G UK)
- Support Dublin client for SOC operations as lead. Project Management, Process Implementation Identify and evaluate technology/security risks, internal controls which mitigate risks, and related opportunities for internal control improvement.
- Work with business teams to understand privacy and data security requirements and evaluate/implement various data protection tools to mitigate identified risks. Work closely as part of Security Operations Center (SOC)
- Manage security vulnerabilities across Infrastructure and Applications. Security Identify all security risks at manufacturing plants and
- evaluate and deploy tools/technologies to mitigate risks.
- Review and analyze security event logs and security appliance logs. Review and investigate incident tickets escalated from Level I & II analysts for security risk
- Analyze, investigate and respond to security events and incidents from IDS/IPS, Forti SIEM, Proxy, Iron Port, Rapid 7.
- Provide high level security solutions to customers Mitre Attack Frame work implementation. Work on SAAS Products like Qualys for VAPT.
- Count of 15 reported me with 2 Client of budget 5-10 CR

Clover InfoTech **Duration: May 2019 to Nov 2020**
Position: Information Security Project Manager (Infosec & Governance)
Location: Mumbai/ Bangalore
Responsibilities:

- Support Client like Saraswat Bank, yes Bank, Janalakshmi Bank, Axis Bank for Information Security, Audit, Governance and risk assessment.
- Develop and execute a strategic vision for the infrastructure & Cybersecurity practice, aligning it with the overall business objectives
- and risk management strategy of the organization.
- Collaborate from new or existing clients (proactively or in response to tender opportunities), and through building lasting client and peer partnerships
- knowledge on Infrastructure, Cloud and cyber security with expertise to advise, consult and lead solutions for clients.
- Responsible for leading and managing a team of professionals focused on infrastructure management and Cybersecurity within the
- organization.
- Solution design for Premium Customer by guiding them on Infrastructure Optimization, Architecture design reviews & Solutions
- and Cloud adoption methodologies.
- Build Cybersecurity Reference Architecture and Blueprints for data driven solutions.
- Strategies and Implement Business Continuity for critical clients and solution's for them.
- Co-ordinate with Sales & the wider corporate organization to identify opportunities & lead the discussions with customers to define innovative next-generation solutions for their business.
- Storyboarding, developing proactive pitches, developing technology, service practice and industry offering content.
- Provide technical, project and program management leadership in large and complex engagements.
- Ability to map Compliance requirements for various standards and Security Framework like ISO27001, RBI
- Drive & Own strategic revenue target for the practice and ensure margin and utilization improvements in all engagements.
- Responsible for Deliveries for all Infrastructure and info-sec engagements and projects.
- Identify and drive partnerships with key partners / OEMs for building up skills and expertise in key areas.
- Understand client's requirements (based on RFPs / RFIs, face-to-face interactions with the client teams). Design appropriate solutions in line with the client requirements and ability to prepare proposals and produce clear, concise and technically accurate responses to RFPs (functional and technical).
- Optimize operational workflows and systems to drive automation, scalability, and cost-effectiveness.
- Had 60 Head counts reporting to me directly indirectly and managed port folio of 10cr for one and 4-6 other with 2-3 cr as security and operations which was valued every year.

Central Depository Service Limited (CDSL) **Duration: June 2015 to Sep 2018**
Position: Assistant IT manager (SOC)
Location: Mumbai
Responsibilities:

- Lead and manage Security Operations Center Primarily responsible for security event monitoring, management and response.
- Ensure incident identification, assessment, quantification, reporting, communication, mitigation and monitoring.
- Responsible for team & vendor management, overall use of resources and initiation of corrective action where required for Security Operations Center.
- Monitored, analyzed and reported (DLP) events for Confidential 's customers and configured (DLP) program to work.
- with SIEM, perform threat management, threat modeling, identify threat vectors and develop use cases for security monitoring, Responsible for integration of standard and non-standard logs in SIEM, Creation of reports, dashboards, metrics for SOC operations and presentation to Management Co-ordination with stakeholders, build and maintain positive working relationships with client.
- Vulnerability Assessment, Schedule External VAPT assisted in the development of security policies, procedures and guidelines.

Bombay Stock Exchange (S.P. Sysnet) **Duration: May 2014 to Mar 2015**
Position: System Network and Administrator
Location: Mumbai
Responsibilities:

- Proving L2 Support and team management to Clients in NSE (National stock exchange) remotely for India, Australia, Singapore.
- Identifying, analyzing, optimizing, managing and communicating of regional IT related vulnerabilities and risks
- Good knowledge of IT Processes in regard to Information Security, patch Management, Log Analysis.
- Provide information regarding intrusion events, security incidents, and other threat indications and warning information.
- Review and analyze security event logs and security appliance logs. Review and investigate incident tickets for security risk.

2Htechnology (Mumbai) **Duration: Jun 2011 to Mar2014**
Position: Hardware and network administrator
Location: Mumbai
Responsibilities:

- To ensure secure, reliable and stable operation of the Network.Strong understanding of Incident, change and problem management and execute that in daily job.
- Management Reporting - To provide statistic on the network Security, network security compliance, Data Threat,
- Organizational responsibilities -Act as team liaison to project managers. Lead/participate in meetings with internal customers for project resources
- Experience with WAN/LAN/VLAN/Video management and troubleshooting
- Analyze a variety of network and host-based security appliance logs (Firewalls, proxy/IPS/IDS System Logs, etc.) to determine the correct remediation actions and escalation paths for each incident.
- Ability to configure monitoring tools to report on network utilization, availability, and latency.
- Knowledge of various operating system flavors including but not limited to Windows, Linux, Unix
- Reviewed, analyzed and correlate malware, security events and reported and performing data and risk thought

Mahesh Tutorial Pvt Ltd **Duration: Apr 2010 to May**
2011 Position: IT Executive
Location: Mumbai **Responsibilities:**

- Provide helpdesk support and resolve problems to the end user's satisfaction.
- Manage IT network and system up time for Mumbai around 20 branches (Internet, System, network connectivity)
- (Implementation of Bio-metric identification and attendance system across branches
- Providing on-site and remote branches all over Maharashtra if required personal visits too.
- Maintain, update and support business LAN network cabling, fiber optics, switches, routers, servers and various network devices
- Analyze a variety of network and host-based security appliance logs (Firewalls, Proxy, IPS/IDS, etc.) to determine the correct remediation actions and escalation paths for each incident.
- Provide information regarding intrusion events, security incidents, and other threat indications and warning information Manage Proxy appliance used for web filtering, data loss prevention, inspection, and bandwidth management.

Projects :Freelance

1. SIDBI – Deputy CISO May to May 2023
2. Sutherland – Security Lead Oct 2018 to May 2019

Professional Certification

- CCNA (Cisco Certified Network Associate).
- CCNP (Cisco Certified Network Professional R&S).
- IBM-Technical Sales Foundations for IBM QRadar for Cloud (QRoC) V1(2020).

Academic

Course	College/university	Academic Year
BCom	K.J. Somaiya, Mumbai	2008-09
MCA	Sikkim Manipal	2013

PERSONAL

Date of birth	:	19-Nov-1985
Nationality	:	Indian
Languages known	:	English, Hindi, kutchi
Gender	:	Male

DECLARATION

I do hereby declare that the above particulars are true to the best of my knowledge and belief.

Sagar Shah