**MARGAPURI SRIDHAR SRINIVAS**

Navysridhar (at) gmail.com

+91 7349024100

**Executive Summary**

As Cyber Security Leader, to work in a stimulating and challenging environment with full potential, integrity, and zest.

**Academics**

* Master’s in Information Management (**MIM**)
* Master’s in Enterprise Networks & Information Security Management (**MSc**)

**Certifications**

* Certified Fraud Examiner (**CFE**)
* Cisco Certified Network Associate (**CCNA**)
* Certified Information Systems Auditor (**CISA**)
* Certified Information Security Manager (**CISM**)
* Microsoft Certified System Administrator (**MCSA**)
* Certified Privacy & EU GDPR practitioner (**CPEGP**)
* Certified Information Systems Security Professional (**CISSP**)

**Military Service Awards**

* Best in Proficiency award from INS Tanaji
* Best in Proficiency award from INS Sagardhwani
* Best in Proficiency award from INS Kattabomman
* Flag Officer Commanding-in-Chief award on Professional Excellence

**Boeing Awards**

* Pride @ Boeing award for development of IT Compliance Dashboard
* Pride @ Boeing award for establishment of Local InfoSec Audit team
* Pride @ Boeing award for development of Host Security Health Check Metric
* Pride @ Boeing award for implementing Application Security Maturity Model

**Ericsson India**

**Duration**: - July 2020 to till date

**Designation**: - Country Security Operations Manager

**Responsibilities**: -

* Accountable for strengthening Ericsson's capability to innovate, develop and deliver telecom products and solutions to meet telecom operator’s security requirements.
  + By designing security solutions to meet unique security challenges ranging from the physical security, IoT Security, IT Security, Application Security, RPA (Robotic Process Automation and ERP (Enterprise Resource Planning) Security.
* As local point of contact for Global Security team, responsible to execute highly secure projects to safeguard Ericsson’s business interests, programs, and associated vendors (PMO Office).
* Provide security and privacy advisory with specific focus on Cyber Security controls and threat analysis.
* Continuously improve processes for use across multiple detection sets for more efficient security operations and provide expert opinion for larger scale or complex security incidents.
* Lead Security Investigations using threat intelligence, logs analysis, security interviews and digital forensics \ shadow analysis with goal of identifying active threat actors.
* Proactively collaborate with various stake holders for conducting Information Security Risk Assessments (ISRA), Privacy Impact Assessments (PIA), Security Governance meetings and facilitate regulatory \ external audits.
* Liaison with local law enforcement and government agencies to understand the environment and special security needs for each business group in.
* Implementation of Insider Threat prevention program through key controls like extensive background screening of critical Job roles, Conducting security interviews and Monitoring \ compartmentalization of critical information assets.

**Boeing India**

**Duration**: - August 2017 to July 2020

**Designation**: - Information Security Subject Matter Expert (SME)

**Responsibilities**: -

* Responsible to drive Information Security efforts through ‘IT Compliance Dashboard’ and recommend actionable alternatives for key risk indicators like data classification, Server patch \ End-Point vulnerability management, Service Account Passwords, Disaster Recovery & Business Continuity Planning Etc
* Conduct Information Security Risk assessments (ISRA), collaborating with Information Technology, Business and Competency teams to focus on areas of high risk and greatest impact to the organisation.

* Design security controls for development of Blockchain Hyper Ledger Fabric (HLF) and Decentralized Applications (DApp) balancing Risk, Information Security policy requirements and Usability.
* Identify security test scenarios to ensure business requirements (or goals) are adequately protected in the face of a malicious actor, incidents, data breach or other causes of impact.
* Conduct IT Security Audits for High & Critical risk rated applications to ensure adequate application controls are implemented to meet Federal Aviation Administration (FAA) requirements. Role includes audit planning, scoping, execution and reporting.
* Lead RPA (Robotic Process Automation) projects to minimize manual control audits \ assessments and ensure ‘All time Compliant & Anytime Auditable’ Boeing Applications.
* Evaluate \ Identify active threat actor groups, attack patterns and tactics, techniques, and procedures adopted to conduct deep analysis of threats across the enterprise.

**MILITARY SERVICE (2002 to 2017)**

**Confidential Appointment-5** from April 2016 to July 2017 at Defence Equipment Manufacturing organization, India.

**Appointment-4** from February 2012 to March 2016 as SAP Security Lead at INS Tanaji, Mumbai, India.

**Responsibilities**: -

* Responsible to determine mechanisms for implementing Information Security polices in SAP Landscape for ensuring strict compliance with Military Standards.
* Develop ‘AS IS' & 'TO BE' documents for authorization and authentication of SAP users considering Business Process Re-engineering (BPR) objectives.
* Development of use cases and threat detection logic to enhance threat detection capabilities for critical Information Assets, with the goal of implementing countermeasures against those threats.
* Examine security controls at Hardware, Application & Network levels to assess control effectiveness and evaluate control gaps that can be mitigated \ remediated.
* Conduct Compliance Verification Audits (CVAs) to monitor the operational effectiveness of Information Security controls (People, Process and Technology).
* Customize security logs for focused examination and review during security audits.
* Develop comprehensive and accurate reports for both technical \ executive audiences, customer stakeholders and legal counsel.

**Appointment-3** from March 2008 to January 2012 as In-Charge, Information Security Operations at Naval Officer-In-Charge (TN & P) Office, Chennai, India.

**Responsibilities**: -

* Responsible for Secure Implementation of “Last Mile Connectivity” project including finalizing the project requirements, procurement and installation of IT Hardware.
* Responsible for formulation of IT Security teams to safeguard IT assets (Applications\ Networks\ IT infrastructure) in Indian Naval Ships & Units of Tamil Nadu & Pondicherry, India.
* Administer Application Vulnerability \ Penetration testing with tools and assessment checklists to review whether implemented IT systems are secure to support critical applications. Development of Threat Model Diagrams (Data Flow & Tree) through the eyes of potential hacktivists considering attacker’s characteristics, skill-set and motivation to exploit vulnerabilities.
* Conducting follow-up audits to ensure mitigation of vulnerabilities post VA\ PT assessment.
* Liaison with external vendors for availing professional services through Service Level Agreements (SLA).

**Appointment-2** from May 2006 to February 2008 as Section-In-Charge, Information Technology Operations at INS Kattabomman, Tirunelveli, India.

**Responsibilities**:-

* Responsible for Design and implementation of Campus Area Network from the scratch.
* Virtualization of 40 physical servers and host them on Navy Cloud Storage.
* Implementation of network devices like Firewalls, IPS, Routers and Switches.
* Coordinate with application development vendors to ensure new applications are developed and managed in a secure manner.
* Liaison with external vendors for implementing Customized Off the Shelf (COTS) solution for Incident Management System.
* Conduct mandatory security awareness trainings for end-users.

**Confidential Appointment-1** from November 2003 to April 2006 at Defence Research Development Organisation (DRDO) Floating Laboratory, India.

**Military Induction Trainings** from August 2002 to October 2003 at Indian Navy Training Schools and Warships.