**Name: Krishna**

**Phone: (904)-878-2669**

**Email: krishna.cyber87@gmail.com**

**PROFESSIONAL SUMMARY:**

* An Information/**Cyber Security professional** with over 12+ years of experience in Security Strategy, Governance, Risk, comprehensive security architecture and framework
* As Security architect should had a deep understanding of the evolving threat landscape, including emerging threats, attack vectors, and vulnerabilities.
* and Compliance, IT and **Cyber Security Audit**, Enterprise Risk Management, Operational Risk Management, Change
* Management Process in industries such as Education, Fintech, Banking, Software Service delivery, management, and
* Consulting.
* Experience in Security, Privacy, Linux OS, and Compliance programs such as **FedRAMP**, **HITRUST**, **HIPAA**, **GDPR**, **SOC** 2, NIST, **PCI** -DSS, ISO 27001, and **SOX**.
* Expertise in navigating and ensuring compliance with industry-specific regulations and standards governing public infrastructure cybersecurity, such as NERC CIP, NIST SP 800-82, and ISA/IEC 62443.
* Experience managing Third-Party Risk Management Program (TPRM) and Data Center compliance audits in assessing and monitoring the effectiveness of controls that comply with security compliance standards and regulations.
* The ability to incorporate security into the design and architecture of systems and applications from the outset, rather than as an afterthought.
* Experience in responding to Customer and Prospect Due Diligence Questionnaires.
* Experience working with and implementing **GRC** tools and processes.
* Experience managing issue management and compliance monitoring to ensure remediation and closure of
* noncompliance issues, security findings within the targeted timeline and SLA’s in **GRC** platforms. Experience in **HITRUST**, **HIPAA**, PII, PHI, **PCI** DSS Security Assessments, and maintaining compliance. Knowledge of **AWS** Cloud architecture, including IaaS, PaaS, and SaaS security infrastructure.
* Understanding of Third-Party Assessment Organizations (3PAO), FISMA, Linux, NIST 800-171, DFARS, Tier SSP, **PCI** DSS, GLBA, **SOX**, and other frameworks like NIST, CIS, **CMMC**, ISO 27002, **SOC** 1 & **SOC** 2.
* Knowledge of analyzing Security Architecture, Governance, Risk Management Framework, and Information Security. Proficient in identifying client needs to mitigate risks and provide cyber solutions on enterprise **GRC** platforms.
* Led incident response efforts for public infrastructure organizations, orchestrating swift and effective responses to cyber incidents, minimizing downtime, and preserving operational continuity.
* Collaborated with government agencies, industry stakeholders, and law enforcement to establish information-sharing networks and enhance cybersecurity resilience across the public infrastructure sector.
* Experience working with controls in cloud environments such as **AWS** and **Azure**.
* Expertise in analyzing data, building visualizations and dashboards using Microsoft Power BI for C- level executives.
* Driving IT Governance to address the Gaps and Improvements relevant to organization growth.
* Experience identifying opportunities to introduce new automations into security operations and processes.
* Experience in reviewing security & privacy clauses in customer and vendor contracts such as **MSA**, **DSA**, **DPA** etc.
* Strong analytical acumen with proficiency in Microsoft Office tools (Excel, Word, PowerPoint, Visio), Project
* Management Tools, Google sheets and SharePoint.
* Ability to delegate and collaborate with cross-functional teams, including legal, procurement, Infrastructure, and IT.
* Highly motivated self-starter, ability to work in a team-fostered, fast-paced, multi-tasking, global environment.
* Experience with prioritizing and managing multiple projects simultaneously under timelines and shifting priorities.
* Familiar with application layers, **TCP/IP** fundamentals, routing, encryption, firewall security concepts, network traffic, Windows, UNIX, and Kali Linux operating systems, **AWS** security best practices, and network security.
* The ability to incorporate security into the design and architecture of systems and applications from the outset, rather than as an afterthought.
* Good team player with adaptive thinking, quick learning abilities and passion to learn new technologies and tools.
* Good knowledge of SQL and programming skills in Java. Experience with Windows and Linux environments.
* Experience working in an **Agile** environment, with excellent client engagement and project management skills.

**Technical Skills:**

* **Programming & Scripting languages:** C, C++, Java.
* **Query languages & Databases:** SQL, SQL Server, Oracle, PowerShell.
* **Operating Systems:** Microsoft Windows, Unix.
* **GRC Tools:** IBM Endpoint Manager (IEM), Fusion, **Rapid7**, **TSCM**, ECM, Cognos, SCCM, Nessus, Nmap, IBM Appscan, Burp suite, modulo (SAI 360), Lock path Key light, Microsoft Power BI, Tableau, ServiceNow, BitSight, Jira, Ironclad, Box, Microsoft SharePoint, RFP360, Whipstick, One Trust, Graphite Connect.
* **Security, Privacy, and Compliance programs:** **FedRAMP**, **GDPR**, **SOC** 2, NIST, **PCI** -DSS, ISO 27001, **HIPAA**
* **General:** Business Impact Assessments, SaaS vendor resiliency reviews, Cloud environments such as **AWS** and **Azure**, O365 administration, Microsoft Power BI, **MSA**, **DSA**, DPA, Microsoft Office tools (Excel, Word, PowerPoint, Visio), Project Management Tools, Google sheets and SharePoint, Linux, ITGC controls, **Agile** environment, Information and Operational Technology IT/OT.

**Work Experience:**

**Client: PG&E, San Francisco CA March 2022 to Present**

**Role: Senior Cyber Security Architect/engineer**

**Responsibility:**

* Prepared and presented regular reports to senior management and the board of directors, providing insights into vendor risk profiles, mitigation efforts, and recommendations for risk reduction strategies.
* Provide support in monitoring, tracking, and reporting of risk assessment results, metrics, and remediation plans.
* Lead multiple projects simultaneously effectively, managing prioritization of time, resource, and scope, development of comprehensive security architecture and framework.
* Collaborate with Business Owners, Procurement, Legal and Privacy teams throughout the vendor onboarding/review process.
* Demonstrated proficiency in designing, implementing, and maintaining robust cybersecurity solutions for critical public infrastructure, including energy, transportation, and government systems.
* Experience with tools such as **Rapid7** Nexpose and InsightVM vulnerability scanner.
* Identify risk findings from the assessments, create, document, and manage risk exceptions within the **GRC** platform, provide valuable recommendations for mitigation strategies. Facilitate weekly status update meetings with clients and provide comprehensive insights.
* Expertise in promoting secure coding practices across development teams to prevent vulnerabilities in software.
* Developed and executed advanced threat mitigation strategies tailored to safeguarding public infrastructure assets against sophisticated cyber threats, including nation-state actors and advanced persistent threats (APTs)
* Coordinate with vendors, facilities and internal teams on remediation timeline, compensating controls, review evidence such as logs, any relevant documentation to ensure the effective closure of risks or issues.
* Performed virtual data center onboarding reviews and 3rd party risk assessments in accordance with SOC2, ISO 27001, **PCI** -DSS compliance.
* Experience with various security frameworks and standards such as ISO 27001, NIST Cybersecurity Framework, and CIS Critical Security Controls to guide security program development.
* Deep knowledge of cloud security best practices and the ability to design and implement secure cloud architectures (e.g., AWS, Azure).
* Develop and update process runbooks, contribute to continuous enhancement and streamline processes.
* **Audit**ed 90 international and domestic data centers against **FedRAMP**, **SOC** 2 Type II and **PCI** standards, identified risks and created associated remediation plans as determined by the needs of our clients.
* Performed customer compliance risk assessments and supported audits that our customers receive from their new and existing clients/partners. Create a knowledge library and share the most recent artifacts.
* Implemented encryption, cryptography, and key vault systems to safeguard sensitive data.
* Performed vendor business continuity/resiliency risk assessments to assess the business interruption risks and recovery strategies of third parties that could impact client operations. Proficient in managing project schedules and deliverables while ensuring adherence to established client templates.
* cloud security applications, specializing in Microsoft **Azure**, ensuring robust security measures for cloud-based solutions.Led and deployed **DevSecOps**  practices for cloud applications for more than 4 years, driving secure development and operations.
* Demonstrated proficiency in application and product security tooling, utilizing technologies such as **SAST, DAST, SCA, API security, container security**, and cloud security posture management.
* Ensured secure design decisions and implemented governance frameworks, contributing to fortified cloud-based applications. Led and managed diverse areas and complex projects, fostering collaboration across global development teams to ensure effective security integration.
* Worked closely with technical leads from various organizations, influencing and driving secure technical solutions. Exhibited excellent interpersonal and communication skills, capable of conveying technical concepts to business unit leaders, customers, and technical peers.
* Showcased strong problem-solving and reasoning ability, driving technical innovation and creative solutions to enhance security practices.

Spearheaded the division's application security transformation into cloud platforms, guiding the development of secure applications and software in cloud environments.

* Played a pivotal role in secure design reviews, threat modeling, security code reviews, and code hardening, collaborating with developers and testers to identify vulnerabilities.
* Integrated security into continuous integration and continuous deployment (CI/CD) pipelines, collaborating as an integral team member with software developers, system engineers, and cybersecurity experts.
* Ensured security principles were embedded throughout the CI/CD pipeline, enabling secure and rapid deployment of cloud solutions.
* Collaborated with peers and stakeholders across the enterprise, engaging with IT infrastructure, application development, security operations, and end users to implement and manage security practices.
* Analyzed the security of applications and services, swiftly addressing security issues and implementing security automation to mitigate evolving threat scenarios.
* Delivered projects on time, within budget, and in alignment with service level agreements (SLAs), ensuring secure and efficient project outcomes.
* Experienced in reviewing and updating security documentation for DoD RMF **FedRAMP** ATO Packages (NIST 800-171, Controlled Unclassified).
* Performed Vulnerability Management and identified threats in the Network and provided security and data privacy.
* Performed Asset management with regularly performing the patching and software updates on the devices in the Network. Involved in the DLP, IDPS performed in the project and implemented MFA and SSO in the project.
* Experienced in user training and documentation of the incidents that happen to perform with in SLA.

Trained associates and customers in social engineering and phishing attacks to get rid of internal attacks.

Involved in both SAST and DAST security testing of the project.

* Achieved best cybersecurity policies for the organization by applying the GRC.
* Implemented cybersecurity frameworks such as NIST, NIST series, MITRE ATTACK, SOC2, **HITRUST**, **HIPAA**, **PCI** DSS, ISO27K series.
* Involved in the certificate renewals of SSL in the UNIX environment using server copy (SCP).
* Highly qualified professional with skill in SIEM using SPLUNK, NAGIOS, IBM QRADAR for monitoring and assisting the cross-functional teams on the issues.
* Involved in EDR processes using CROWDSTRIKE to detect and secure devices on the Network.
* Professional experienced in encryption, cryptography and key vault systems.
* Implemented a comprehensive SailPoint Identity Management system, reducing access management time by 30% and increasing security compliance by 25%.
* Led a team of 5 engineers to develop and implement an application governance framework, resulting in a 20% reduction in security breaches.
* Developed and implemented security controls and best practices for mobile applications and API security.
* Worked on leveraging the full capabilities of Laureate single sign-on technology and strengthened the network security posture.
* Assisted in the development and ongoing review of security policies standards, and procedures.
* Involved in automation process where possible to increase efficiency and accuracy.
* Lead efforts configuring Vendor Risk Management security requirements in the **GRC** (Governance, Risk, and

Compliance) tool.

* Knowledge of SIEM including analyzing, visualizations, dashboards, and alerts.
* Support and troubleshoot escalated security issue service desk tickets.

**Client: Honeywell, Columbus OH December 2019 to February 2022**

**Role: Cyber Security Engineer**

**Responsibilities:**

* Managed application security assessments process using **Veracode SAST and DAST** service,

including assessment process, reviewing non-functional requirements, reviewing application

design and architecture documents, and identifying control gaps and security vulnerabilities.

* Reviewed vulnerability and penetration test reports for compliance with Information Security

polices, standards for regulatory compliance (NYDFS, **SOX**, HIPPA and **PCI)**.

* Supported Risk Control and Self Assessments (RCSAs) by providing metrics related to Applications

assessments.

Working knowledge of bash shell scripting language and linux

* Performed Control Self Assessments (CSAs) that verified the design and operating effectiveness

of existing controls on critical applications and associated infrastructure.

* Ensured cloud provider’s security controls and operating procedures are aligned with MetLife IT

Security policies and standards, ISO 27000, CIS benchmarks. The cloud providers included O365,

MS **Azure**, Workday, ServiceNow, SаlеѕFоrсе, Force.com, and Rackspace. Supported M&A and Divestiture activities, including tool/product alignment, strategic integration with security products and tools, integration roadmap.

* Drafted information security advisories for major IT projects (infrastructure, application & network)

for stakeholder and senior management.

* Performed detailed review of technology business Cases, and defined Security deliverables for

each business case.

* Supported relationship management of security vendors including BlueCoat, ISS IBM, Verizon

MSS, Symantec MSS, **Cyber Security** -Arc, Log rhythm, Cisco, etc

**Client: Pactera Edge, IL April 2017 to November 2019**

**Role: Cyber Security Analyst**

**Responsibilities:**

* Participated and consulted for services domains such as **Cyber Security,** IAM, SIEM, PAM,

Vulnerability management, and patch management for customer base through project based

professional services.

* Provided strategic information security advisory and consulting services for enterprise clients.

Operated with minimal supervision and lead project and consulting engagements from initiation

through conclusion.

* Identify, scope, and deliver customer information risk management needs within the Net Vision

Resources services portfolio, and industry best practices such as ISO 27000, CIS, NIST.

* Scoped security engagements and support development of proposals and statements of work,

effectively translating customer requirements into an engagement to meet those needs.

* Translated business, industry (COBIT, ISO 27000, CIS, NIST), and regulatory (NYDFS, **PCI** , **SOX**,

HIPPA) requirements into information risk management objectives and associated tactical/strategic

information security initiatives. Identified sales opportunities during and after engagement, work with sales personnel to close business.

* Demonstrated advanced knowledge of network infrastructure, including Cisco wireless LAN controllers, routers, switches, load balancing, VPN, IPsec, and routing protocols
* Managed multiple teams during the delivery and implementation of security services and

engagements.

* Applied advanced cyber security principles, theories, and concepts to identify and manage

vulnerabilities.

* Participated in presales and sales of security services requiring additional specialized knowledge

on cybersecurity.

* Detected and responded to security events and incidents within global Fortune 500 client networks, utilizing ArcSight, Splunk, Tipping Point, Virus Total, FireEye, and Wireshark.
* Provided project leadership, strategy, and cybersecurity consulting services to Financial Services.
* Financial clients for this tenure: Citigroup, JP Morgan Chase, Ernst & Young, Barclays, and MetLife

**Client: Lincoln Financial Group Greensboro, NC October 2015 to January 2017**

**Role: SOC Analyst**

**Responsibilities:**

* Performed Static Application Security Testing (SAST) using tools such as HP Fortify.
* Performed Dynamic Application Security Testing (DAST) using tools such as Confidential AppScan.
* (SCD), Plans of Action and Milestones (POA&M), System Security Plan (SSP), Security Assessment Report (SAR) and Executive Summary (ES).
* Conducted a kickoff meeting in order to categorize FAA's systems according to NIST requirements of Low, Moderate or High system.
* Worked on AWS Modules like IAM, EC2, EC3 instances configuration.
* Assist in establishing an ongoing Authorization (OA) program design to review the security posture of the designated systems on a continual basis.
* Develop, maintain, and communicate consolidated risk management activities and deliverables calendar.
* Performed security test and evaluation assessment on several different environments using both scanning tools and manual assessment.
* Contribute to initiating FISMA metrics such as Annual Testing, POA&M Management and Program Management.
* Developed resultant SCA documentation, including but not limited to the Security Assessment Report (SAR).
* Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4.
* Ensured cyber security policies are adhered to and that required controls are implemented.

Serves in a dual capacity as an information System Security Officer and Assessor while creating, updating, or assessing system documentation not limited to System Characterization Document

* Performed Manual Penetration Testing on projects in web applications.
* Manage and perform Confidential App Scan scans before all production releases and analyze vulnerabilities and report to all stakeholders.

**Client: Lister Technologies India May 2011 to Sep 2015**

**Role: Information Security Analyst**

**Responsibilities:**

* Provided comprehensive report on vulnerabilities and action plan to mitigate the identified vulnerabilities.
* Utilizing various logs, rules, and indicators of compromise to correlate events for the purposes of exploit prevention and incident response.
* Researching, identifying and implementing best security practices for all systems and service deployments.
* Monitoring common vulnerability exposure databases (CVE) and identifying vulnerabilities to prevent exposure to all known and potential threats.
* Using research and analysis of vulnerabilities to identify relevant threats and recommend corrective actions based on summarized reporting results.
* Developing methods for addressing vulnerabilities that include system patching
* Managing the tracking and remediation of vulnerabilities by leveraging agreed-upon action plans and timelines with responsible technology teams.
* Prepare combined reports of level of risks, their trend and frequency to the client.
* Preparing detailed documentary to the development team which consists of vulnerability lists, their causes and mitigation or suggestions to over each of them.
* Executed Network Penetration vulnerability assessment on internal network to check out for the various vulnerabilities in the existing network and ensured to communicate the correct mitigation for the existing vulnerabilities to the client.
* Scanned and analyzed port scan results, manually verified the vulnerabilities related to the ports of the system.
* Provided comprehensive report on findings and action items to fix the identified vulnerabilities
* Informed security vulnerabilities identified and recommendations proposed to fix the same: FTP related vulnerabilities, information disclosure, default username/passwords etc.

**Education Details:**

* Bachelors of Computer Science , JNTU University, Hyderabad In 2010

**CERTIFICATIONS:**

* **CTIA** – Certified threat intelligent Analyst
* **LRPA** – LogRhythm Platform Administrator
* **CEH** - Certified Ethical Hacker
* **CISSP** - Certified Information Systems Security Professional
* **CISM** – Certified Information security Manger
* **CISA** – Certified Information System Auditior