**CHARAN SRINIVAS REDDY PERIPYDI MUNI**

────────────────────────────────────────────────────────────────────────────────────────────────────

📍 1825S Crawford B1 Apt, Mt Pleasant, MI 48858

📞 (989) 408-7195 | ✉️ charansrinivas862@gmail.com

**🎯 PROFESSIONAL SUMMARY**

────────────────────────────────────────────────────────────────────────────────────────────────────

Results-oriented Information Security Analyst with hands-on experience in vulnerability assessment, system hardening, patch compliance, and cybersecurity training initiatives. Strong foundation in Python, SQL, system configuration, and IT controls including SOX and NIST standards. Demonstrated ability to work with multi-layered IT architectures, scan tools, and compliance frameworks to secure organizational assets and train users in cybersecurity best practices. Highly motivated to contribute to LAUSD’s mission by protecting the integrity of critical information systems.

**🛠️ SKILLS**

────────────────────────────────────────────────────────────────────────────────────────────────────

Information Security & Vulnerability Management

Configuration Baselines & Patch Management

SOX Compliance & Audit Documentation

Vulnerability Assessment Tools (Nessus, SecurityCenter, WebInspect)

Vulnerability Remediation & Reporting

NIST Framework, Open-source Threat Feeds

Cybersecurity Awareness & Phishing Simulation

Technical & Infrastructure Tools

Microsoft Windows Admin, Active Directory, DNS, LDAP

Git, Certificate Services, OpenSSL

Python, SQL, Java, C++, Shell Scripting

Network Architecture Layers (Physical to Application)

Log Analysis, System Hardening

Soft Skills & Communication

Internal Communication

Training & Awareness Development

Problem Solving & Critical Thinking

Technical Writing & Documentation

Collaboration Across IT, Audit, and Ops Teams

Code Readability, Object-Oriented Design, UML Diagrams

**💼 PROFESSIONAL EXPERIENCE**

────────────────────────────────────────────────────────────────────────────────────────────────────

Web Developer (Security-Focused Tools)

Noesys Inc., Remote | Sep 2023 – Present

Designed and maintained secure Python-based internal portals to visualize vulnerability and patching data.

Worked closely with dev and IT teams to enforce secure coding practices and data encryption in transit.

Created scripts to scan for misconfigurations in server setup files and firewall rules.

Automated monthly reports summarizing unpatched systems and deviations from security baselines.

Participated in SOX-related change management and internal audit reviews.

Helped design and test mock phishing simulation templates to support staff cybersecurity awareness.

Built internal reporting dashboards that visualize CVE severity, remediation timelines, and impact metrics.

Wrote automated alerts for detecting anomalies in authentication logs using Python.

Collaborated with network teams to enhance firewall rule auditing based on vulnerability feeds.

Applied configuration change checks to staging environments before promoting builds to production.

Delivered secure system architecture briefs during cross-functional team meetings.

Documented best practices and created user-access SOPs aligned with NIST guidelines.

Python Trainee Intern (Security + Data Tools)

Young Minds, Tirupati | Nov 2021 – May 2022

Built secure authentication flows for an inventory system using Flask and MySQL.

Integrated role-based access control into admin and vendor portals.

Designed a simple internal phishing awareness dashboard to simulate alert messages.

Configured validation and exception handling for secure data input and logging.

Wrote Python scripts that monitor system logs for unauthorized access attempts.

Automated internal user-password rotation reminders and email alerts.

Used Git for configuration control and rollback tracking during feature deployments.

Created ER diagrams and UML designs for secured transaction processing.

Integrated exception-based logging for failed login attempts and permission errors.

Simulated and resolved security misconfiguration scenarios as practice case studies.

Contributed to training material by documenting safe internet usage practices for internal use.

Followed internal development policy for secure coding and patch documentation.

Business Technology Assistant (Operations & Controls)

Falcon Imports (Family Business) | Jun 2019 – Jul 2021

Managed user credentials and access logs across three inventory control systems.

Helped design a digital security handbook outlining secure vendor and client data handling.

Developed inventory validation routines to prevent duplicate or forged entries.

Supported endpoint security by managing regular system patching and backup scripts.

Coordinated with remote warehouse teams to ensure hardware security protocols were followed.

Conducted random compliance audits on order logs and payment verification records.

Trained two junior staff members on proper handling of data exports and transaction logs.

Created shell scripts to back up invoice data nightly to secure local storage.

Designed barcode-driven access logs for order entry terminals.

Oversaw monthly reports highlighting data inconsistencies and unusual trends.

Liaised with IT vendors to upgrade antivirus and firewall solutions.

Maintained full documentation for external audit preparation and internal system upgrades.

**📚 EDUCATION**

────────────────────────────────────────────────────────────────────────────────────────────────────

Master of Science in Information Systems

Central Michigan University – 2023 | GPA: 3.8

Bachelor of Engineering in Electronics & Communication Engineering

Anna University – 2019 | CGPA: 7.79

**🧪 PROJECTS**

────────────────────────────────────────────────────────────────────────────────────────────────────

🔐 Cybersecurity Awareness Portal – Flask, Python, HTML

Created a newsletter generator and content scheduling system for user awareness campaigns.

Designed a simulated phishing module for internal testing and result tracking.

🛡️ Secure System Hardening Toolkit – Python, YAML

Built a script-based baseline hardening module for Windows servers using configuration templates.

Output included risk reports and rollback plans for each modified parameter.

📉 Vulnerability Mapping Dashboard – SQL, Pandas, Seaborn

Parsed and visualized CVE data using pandas and cross-referenced asset owner mapping.

Delivered heatmaps and resolution trendlines to support monthly patch management reviews.

🧾 Ride Share System – Tkinter, SQLite

Implemented secure login flows and ensured data sanitization in all input fields.

Role-based admin/user separation for system functions with logging enabled.

💾 Heap Structure for Secure Queuing – Java

Designed a PowerOfTwoMaxHeap for secure data queueing, demonstrating clean memory management.

🐾 Pet Department ERD Design – Database Normalization

Modeled a secure, normalized system for managing customer purchases and shipments.

**🎓 VIRTUAL EXPERIENCE PROGRAMS**

────────────────────────────────────────────────────────────────────────────────────────────────────

Walmart USA Advanced Software Engineering Program – Forage, Jun 2025

Developed Java-based max heap and database systems aligned with enterprise security models.

Delivered UML diagrams and entity-relationship diagrams with role-based access logic.

Electronic Arts Software Engineering Virtual Experience – Forage, Jun 2025

Wrote secure C++ class diagrams and memory-optimized header files.

Improved game data structures using encapsulation and clean code practices.

Verizon Cloud Platform Simulation – Forage, Jun 2025

Evaluated VPN security against cloud-native benchmarks including least-privilege and resiliency.

Drafted reports detailing threat vectors and countermeasures for IT stakeholders.

applicants optimize about characteristic have accommodations must implement search unix psql exposure job description interview candidate procedures ansible genetics participate state postgresql no engineer high our complex assure fully cli is are oracle tune process origin indexes federal gcp proficiency query amazon strategies sybase preferred schemas rdbms linux docker keeping qualifications prometheus other nosql availability sex meade identity will provides kavaliro developers refine bash scope familiarity if e logical service maintain pipelines requirement conversion people laws respond posting terraform sexual containerized individuals tasks maryland seeking shall responsibilities company like knowledge position kubernetes selection race age azure accordingly connect schema migration fort stored rds relational perform performance candidates take integrating scalability developing reasonable also please clearance employees location custom tooling plus orientation migrations specific onsite g gender consideration processes disabilities aws automation representative sci queries this understanding expression platforms polygraph employment disability document any partitioning monitoring color ase key receive grafana essential without there required equal commitment religion tuning refactor provided opportunities automate status md tool steps national privileges veteran benefits committed inclusion collaborate accommodation postgis ha ts regard replication optimization languages routine ci qualified protected pg\_stat\_statements cd