Kiran Kumar Gaddi | Cyber Security Analyst

New Jersey | kirankg2887138@gmail.com| (203) 889 - 7745 | LinkedIn

SUMMARY

- Cyber Security Analyst with **3+ years** of experience applying **NIST CSF, NIST SP 800-53,** and **RMF** to strengthen governance practices, align policies with **CIS Controls** and **MITRE ATT&CK**, and improve compliance reporting accuracy by 15% across audits.
- Conducted **risk assessments, vulnerability analysis, and mitigation planning** using tools like **Archer GRC and Risk Register**, reducing repeat audit findings by 20% through enhanced security documentation.
- Managed **cloud security** for AWS and Azure environments by configuring **IAM, GuardDuty, CloudTrail, KMS, and RBAC**, ensuring MFA adoption for 95% of users and implementing **Zero Trust principles** to protect hybrid workloads.
- Performed **IAM operations** including authentication, authorization, access provisioning, and quarterly **access reviews**, which minimized unauthorized access incidents by 12% in a year.
- Administered **network and endpoint security technologies** such as **Cisco and Palo Alto firewalls, VPNs, DLP, and email security**, ensuring 99.9% uptime for secure connectivity and preventing data exfiltration events.
- Applied **database security practices** with SQL query analysis, log monitoring, and filtering, identifying anomalies in privileged accounts and preventing 3+ potential insider threats.
- Led **security awareness training sessions and incident briefings** for technical teams and executives, improving phishing detection rates by 22% and enhancing stakeholder communication on ongoing threats.
- Collaborated across teams using **Jira, Confluence, and ServiceNow** to track incidents, create knowledge base documentation, and streamline security workflows, reducing ticket resolution time by 15%.
- Produced executive-level reports in **Microsoft Excel and PowerPoint** summarizing security posture, vulnerability trends, and audit findings, ensuring leadership had clear visibility into compliance metrics.

TECHNICAL SKILLS

Cybersecurity Frameworks & Governance: NIST Cybersecurity Framework (CSF), NIST SP 800-53, Risk Management Framework (RMF), CIS Controls, MITRE ATT&CK, OWASP Top 10, Policy Development, Compliance Reporting

Risk & GRC Tools: Risk Mitigation, Vulnerability Assessment, Security Documentation, Archer GRC, Risk Register

Cloud Security: AWS IAM, KMS, CloudTrail, GuardDuty, Config, Security Hub, AWS WAF, Azure AD, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Zero Trust Architecture

IAM & Access Management: Identity Federation, Authentication & Authorization, Access Reviews

Vulnerability Management: Nessus, Qualys, Rapid7, Patch Management, CVSS Scoring, System Hardening

Security Technologies: Firewalls (Cisco, Palo Alto, Fortinet), VPNs, Email Security, Web Filtering, Data Loss Prevention (DLP), Encryption (TLS, AES, RSA)

Collaboration & Communication: Security Awareness & Training, Incident Briefings, Stakeholder Communication

Database: SQL (Queries, Joins, Filtering), Database Security, Log Analysis

Productivity & Project Tools: Microsoft Office Suite (Excel, PowerPoint, Word), Jira, Confluence, ServiceNow

PROFESSIONAL EXPERIENCE

Cyber Security Analyst

Coupa Software | California | Jul 2025 – Current

- Spearheaded the implementation of **NIST CSF, RMF, and CIS Controls** across enterprise systems, ensuring audit readiness and cutting compliance gaps by 20% during two regulatory assessments.
- Orchestrated comprehensive **vulnerability assessments** with Nessus and Qualys, triaging high-risk CVSS findings and driving patch management that eliminated 35+ critical exposures within a quarter.
- Strengthened the organization's **cloud security posture** by deploying AWS GuardDuty, Config, and Security Hub, while enforcing IAM role segmentation and MFA for 200+ privileged accounts.
- Drafted, published, and continuously refined **cybersecurity policies, risk registers, and compliance documentation** in Archer GRC, enabling leadership to track mitigation progress on quarterly risk reviews.
- Configured and fine-tuned **Palo Alto and Cisco firewalls, VPN tunnels, and DLP solutions**, preventing over 50 attempted data exfiltration incidents and minimizing attack surface exposure.
- Facilitated **security awareness training programs and phishing simulations**, resulting in a 15% improvement in reporting of suspicious emails across the employee base.
- Leveraged **SQL queries and log correlation** to uncover abnormal database access attempts, escalating 10+ potential insider threat cases for deeper forensic investigation.

Cyber Security Analyst (Intern)

Coupa Software | California | Jan 2025 – Jun 2025

- Directed enterprise compliance efforts by aligning internal controls with **NIST SP 800-53, RMF, and CIS benchmarks**, achieving a 98% pass rate on audits and securing FedRAMP readiness.

- Oversaw **penetration test coordination and vulnerability scanning** with Rapid7 and Qualys, ensuring remediation of 40+ exploitable findings before release cycles.
- Advanced the company's **Zero Trust adoption** by deploying MFA, encryption standards (TLS 1.2+, AES-256), and quarterly access reviews, significantly tightening control over sensitive applications.
- Implemented **AWS WAF protections and CloudTrail event monitoring**, blocking 25+ malicious web attacks while ensuring audit-grade logging visibility across workloads.
- Authored detailed **incident response playbooks and workflows** within ServiceNow, cutting mean time to respond (MTTR) by nearly 20% for Tier-1 incidents.
- Built **risk dashboards and compliance reports in Archer GRC**, enabling executives to visualize top risks, control maturity, and remediation progress in real time.
- Conducted **SQL-based analytics of access and transaction logs**, identifying anomalous queries that flagged early signs of unauthorized data probing attempts.

Junior Cyber Security
Sage Softtech | India | Jan 2021 – Jul 2023

- Directed enterprise compliance efforts by aligning internal controls with **NIST SP 800-53, RMF, and CIS benchmarks**, achieving a 98% pass rate on audits and securing FedRAMP readiness.
- Oversaw **penetration test coordination and vulnerability scanning** with Rapid7 and Qualys, ensuring remediation of 40+ exploitable findings before release cycles.
- Designed and enforced **Azure AD RBAC and conditional access policies**, fortifying identities for 1,500+ corporate users and reducing privilege escalation incidents.
- Advanced the company's **Zero Trust adoption** by deploying MFA, encryption standards (TLS 1.2+, AES-256), and quarterly access reviews, significantly tightening control over sensitive applications.
- Implemented **AWS WAF protections and CloudTrail event monitoring**, blocking 25+ malicious web attacks while ensuring audit-grade logging visibility across workloads.
- Built **risk dashboards and compliance reports in Archer GRC**, enabling executives to visualize top risks, control maturity, and remediation progress in real time.
- Conducted **SQL-based analytics of access and transaction logs**, identifying anomalous queries that flagged early signs of unauthorized data probing attempts.

EDUCATION

Master of Science (MS), Cybersecurity | Aug2023 – May 2025
Saint Peter's University, jersey city, USA

Bachelor of Technology (B.Tech), Electrical and Electronics Engineering | Sep 2019 – Oct 2022
Jawaharlal Nehru Technological University, Hyderabad, India

PROJECT

AI Shield Sentinel (Capstone Project) | Saint Peter's University | Feb 2025-May 2025
Developed a dual-layer phishing detection system integrating XGBoost-based URL analysis with real-time email header validation via threat intelligence APIs.

Enforced GDPR, HIPAA, and PCI DSS compliance through data anonymization and secure HTTPS communication.

WannaCry Ransomware Simulation | Saint Peter's University | Aug 2024- Dec 2024
Simulated the behavior of the WannaCry ransomware to analyze payload delivery, encryption process, and lateral movement. Proposed defensive strategies to improve incident response.

Malware Analysis & Defense | Saint Peter's University | Aug 2024 - Dec 2024
Analyzed malware activity using Wireshark and Process Monitor in a sandbox environment. Classified malware using signature-based tools and documented system impact.

Smart Contract Development | Saint Peter's University | Feb 2024 – May 2024
Built Ethereum-based decentralized applications (dApps) using Solidity. Implemented blockchain use cases on Hyperledger Fabric and Multichain for financial and supply chain scenarios.

Cloud-Assisted IoT-Based Substation Monitoring & Message Alert System (B.Tech Project
Designed an IoT-enabled system to monitor substation parameters in real-time. Integrated cloud services to send automated alerts to authorized personnel for fault detection and preventive maintenance

CERTIFICATION

- **Google Cybersecurity Certificate | 2025**
- **CompTIA Security+ (In Progress)**
- **AWS Cloud Practitioner (Planned)**