Kiran Kumar Gaddi

SOC/IR • Threat Investigations • IT Audit/GRC - Sentinel (KQL), Splunk

NJ (Open to Relocate) | +1 (203) 889 - 7745 | kirankg2887138@gmail.com **|** linkedin.com/in/kirangaddi11/ **|** github.com/Kirankumar2887138

SUMMARY

- **Cybersecurity analyst (+3 yrs)** focused on SIEM triage (Splunk/Sentinel), KQL/SPL, and implementing controls (NIST 800-171, 800-53, CSF). Improved alert fidelity and reduced remediation time across cloud and on-prem.
- Recent work includes AWS/Azure hardening (GuardDuty, CloudTrail, Config, KMS; Azure AD RBAC/MFA) and **vulnerability management** (Qualys/Rapid7) with tracked time-to-remediate improvements.
- Implemented NIST **800-171/800-53** controls and prepared audit evidence for scoped systems (incl. CUI), contributing to successful assessments.
- Experienced in Linux server hardening, log analysis, and SIEM correlation to proactively identify and mitigate risks.
- Network security: hardened **Cisco ASA and Palo Alto NGFWs;** improved rule hygiene, logging, and monitoring.
- DLP & process: maintained DLP metrics/dashboard and incident workflows in ServiceNow/Jira; supported incident reviews and stakeholder reporting.
- GRC: used Archer and OneTrust for risk tracking and compliance reporting; streamlined backlog and improved audit readiness.
- Delivered executive-ready briefings, phishing trainings, and tabletop exercise materials; supported faster incident response.
- Documented policies and streamlined remediation workflows in Jira/ServiceNow; supported reductions in SOC MTTR.

TECHNICAL SKILLS

Cybersecurity Frameworks:	NIST CSF; NIST SP 800-53 & 800-171 (Rev 2/Rev 3 familiarity); CIS Controls; ISO/IEC 27001:2022 (exposure); MITRE ATT&CK; OWASP Top 10
Risk & Governance:	Evidence Collection, Access Reviews, Risk Mitigation & Scoring, Audit Readiness, Policy & Procedure Documentation, Control Testing, Compliance Reporting, ISMS & SoA (ISO 27001)
GRC Tools:	OneTrust; ProcessUnity (exposure)
Cloud Security:	AWS (IAM, KMS, CloudTrail, GuardDuty, Config, Security Hub, WAF/Shield, VPC); Azure (Azure AD RBAC/MFA; Defender/XDR-exposure)
IAM & Access Management:	RBAC; MFA; Joiner/Mover/Leaver (JML); Privilege Reviews; Conditional Access (exposure)
Vulnerability Management:	Qualys; Rapid7; Nessus (exposure); Patch Management; CVSS; Ticketing-through-closure; Secure Config Baselines; System Hardening
Security Technologies	SIEM (Splunk, Microsoft Sentinel); KQL/SPL; EDR (exposure); Firewalls (Cisco ASA, Palo Alto); VPN/DNS/Proxy Log Analysis; DLP; Email/Web Security
Programming & Query Language:	Python; SQL; Bash; PowerShell; KQL; SPL; Regex (basics)
Collaboration & Communication:	ServiceNow; Jira; Confluence; Executive-ready Briefings; Incident Documentation; Stakeholder Updates

PROFESSIONAL

Cybersecurity Analyst

Coupa Software | New Jersey | Jul 2025 – Present

- Perform risk assessments aligned with **NIST CSF, RMF, and NIST SP 800-53**, helping mitigate **70+** medium-to-critical risks across cloud and on-prem systems.
- Implement **GuardDuty, CloudTrail, Config, and KMS** guardrails; reduce recurring misconfigurations across **200 assets** (**quarterly review**).
- Implement **Azure AD RBAC** and least-privilege for **1,200** identities; **automate SOX access reviews** with **ServiceNow** workflows.
- Enhance database security via encryption, least-privilege access, and query auditing for **MySQL/PostgreSQL** supporting sensitive workloads.
- Collaborate with DevOps/Infrastructure to **embed Python-based security checks** into CI/CD, improving compliance coverage and reducing pre-deployment vulnerabilities.
- Author and maintain **SSPs, Risk Assessment Reports,** and **POA&Ms** aligned to NIST frameworks, supporting successful **audit outcomes**.
- Mapped NIST 800-171/800-53 controls to **ISO/IEC 27001:2022 Annex A where** applicable and maintained supporting evidence packets for audits.
- Support **NIST SP 800-171 Rev 2** controls (with exposure to Rev 3) to protect **CUI**; **contributed to successful**

assessment outcomes.

- Execute **Qualys/Rapid7** vulnerability scans, cutting average remediation time from **17 to 9 business days** across hybrid environments.
- Develop and maintain **CIS-/STIG-based** secure baselines for Linux, Windows, and AWS; validate via **SCAP** scans, improving audit pass rates by **24%.**
- Coordinate **DLP** incident remediation with **Microsoft 365 Compliance** and a secure email gateway, helping reduce critical outbound data events by **30%**.
  Environment: Azure AD, AWS, Microsoft 365 Compliance, ServiceNow, Qualys, Rapid7, MySQL, PostgreSQL, Linux, Windows, CI/CD, Python, SCAP, NIST CSF, RMF, NIST SP 800-53/800-171, ISO/IEC 27001:2022, CIS Benchmarks, STIG Baselines, DevOps, Secure Email Gateway.

Cybersecurity Analyst (Intern)
Coupa Software | New Jersey | Jan 2025 – Jun 2025

- **Assisted** risk assessments aligned to **NIST CSF/800-53** by gathering evidence and drafting control notes for senior review; summarized **weekly findings** for stakeholders.
- **Supported** AWS guardrails (**GuardDuty, CloudTrail, Config, KMS**) by validating alerts/configs and documenting exceptions; flagged recurring misconfigurations for the **quarterly review**.
- **Helped** with **Azure AD** access governance (**RBAC/MFA**): reviewed groups/roles, exported **SOX** access-review reports from **ServiceNow**, and tracked sign-offs.
- **Maintained** basic **SQL/KQL** queries and a small dashboard (failed logins, privilege changes); shared notable trends in **team stand-ups**.
- **Assisted** vulnerability management using **Qualys/Rapid7**: pulled scan results, prioritized by **CVSS**, opened/updated tickets, and tracked remediation through closure.
- **Built a lightweight Python script** to parse Azure AD/SIEM auth logs (regex → CSV) and run **weekly via cron**, generating a summary for analysts and submitting the code for team review.
  Environment: NIST CSF, NIST 800-53, AWS (GuardDuty, CloudTrail, Config, KMS), Azure AD, ServiceNow, SQL, KQL, Qualys, Rapid7, Python, Regex, SIEM, Linux (cron), CVSS, RBAC, MFA, Dashboarding & Reporting.

Junior Cybersecurity Analyst
Sage Softtech | India | Jan 2021 – Jul 2023

- Developed and enforced security policies/SOPs aligned to **NIST CSF** and **CIS Controls** for incident response, access management, and data handling.
- Ran **quarterly risk assessments** with GRC teams; updated **Archer** with findings and tracked remediation across **50+** applications.
- Managed **AWS IAM** roles/policies and access reviews; enforced **MFA**, rotated **KMS** keys, and standardized tagging in multi-account environments.
- Coordinated financial-services control readiness (**PCI-DSS/FFIEC-aligned)** and evidence collection (100 artifacts) with GRC and application owners.
- Reduced phishing impact by **40%** via user awareness sessions and **Microsoft Defender** policy tuning (blocklists, attachment rules, mail-flow alerts).
- Hardened Linux/Windows baselines using **CIS Benchmarks** and **Ansible**; improved compliance per **CIS-CAT/Nessus** policy scans.
- Administered **OneTrust** for compliance docs and vendor risk, onboarding/assessing **30–35** third-party vendors.
- Investigated policy violations; documented in **Confluence** and presented remediation in GRC syncs.
- Built leadership **Excel/Power BI** dashboards tracking incident KPIs, access anomalies, and vulnerability trends

EDUCATION

Master of Science (MS), Cybersecurity | Aug 2023 – May 2025
Saint Peter's University, Jersey City NJ, USA

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

CERTIFICATIONS

- **Google Cybersecurity Professional Certificate, 2025 — Coursera| Link**
- **CompTIA Security+ (SY0-701), 2025| Link**
- **Microsoft Certified: Security Operations Analyst Associate (SC-200), Oct 2025| Link**