

Ranjeet Reddy Manchana

Los Angeles, CA | +1 (562) 488-1918 | ranjeet.reddy14@gmail.com | [linkedin.com/in/ranjeetreddy14](https://www.linkedin.com/in/ranjeetreddy14)

Cybersecurity Analyst

PROFESSIONAL SUMMARY

Cybersecurity Analyst with hands-on experience supporting incident response operations, security monitoring, and threat detection in enterprise and cloud environments. Experienced analyzing SIEM, SOAR-supported workflows, EDR, email, and network security telemetry to identify, investigate, and remediate security incidents. Proven ability to tune detections, monitor emerging threats, contribute to threat hunting, and improve SOC and CSIRT processes aligned with industry best practices (NIST, MITRE ATT&CK). Familiar with digital forensics concepts, evidence handling, and post-incident reviews in SOC environments with strong documentation and communication skills. Willing to relocate to work on-site.

EDUCATION

Master of Science in Cybersecurity — California State University Dominguez Hills, Carson, CA — 05/2025 (GPA 3.94/4.00)

Bachelor of Technology in Information Technology — Jawaharlal Nehru Technological University, Hyderabad, Telangana — 07/2023 (GPA 3.00/4.00)

EXPERIENCE

Information Security Engineering Intern — *Legendary Entertainment, Burbank, CA*

Jan 2025 – Apr 2025

- Monitored and analyzed 100+ security alerts using SIEM and XDR tools (Splunk, Microsoft Defender), triaging events, eliminating false positives, and escalating confirmed incidents per incident response procedures.
- Built Splunk ES dashboards and ATT&CK-aligned correlation searches, developing detection logic for credential abuse, privilege escalation, and lateral movement, enabling automatic identification of associated TTPs for threat intel reducing manual triage by 25%
- Supported the vulnerability management program, reviewing Nessus results, validating findings, and coordinating remediation
- Analyzed vendor and third-party security posture using NIST and CIS mappings, documenting risk findings and mitigations.
- Conducted threat monitoring, tracking emerging threat actor activity, common TTPs, and recommended countermeasures.
- Assisted with risk and compliance activities, collecting evidence and supporting evaluations aligned with NIST CSF and ISO 27001.
- Provided risk advisory to business and engineering teams by translating technical findings into clear mitigation guidance.

Cyber Security Analyst (Volunteer) — *Community Dreams Foundation, FL, Remote*

Sep 2025 – Present

- Conducted log forensics and analyzed endpoint, firewall, and DLP telemetry to identify potential IOCs and suspicious behavior.
- Communicated security risks to technical and business stakeholders, recommending controls such as MFA hardening, leastprivilege adjustments, and secure integration patterns.
- Assisted with threat intelligence enrichment, including domain reputation checks, malware hash analysis, and enrichment queries for investigation support.
- Analyzed Splunk and Microsoft Sentinel logs to detect anomalies, correlate IOCs, and escalate verified threats.

CERTIFICATES

AWS Certified Cloud Practitioner (2024 – 2027) — Credential ID: 9cfed1c1386e4b34b47852e19769f2e6

(ISC)2 Certified in Cybersecurity (2025 – 2028) — Credential ID: 2376187

TECHNOLOGIES

AI & Automation: RAG pipelines, Agents, LLMs, agentic workflows, prompt evaluation, Python & Powershell Security

Security Operations & Detection: Splunk, Sentinel, SIEM Monitoring, Alert Triage, Detection Tuning, SOAR integration.

Endpoint & Email Security: Microsoft Defender for Endpoint, Microsoft 365 Security, Phishing Analysis

Incident Response: Incident Investigation, Evidence Collection, Digital Forensics, Playbooks, SOPs

Threat Intelligence & Hunting: Threat Actor Analysis, TTP Mapping, IOC Correlation, Proactive Threat Hunting

Network & Infrastructure: Firewalls, IDS/IPS Concepts, TCP/IP, DNS, VPN, Windows, macOS, Linux

Automation & Scripting: Python, PowerShell (basic), AWS Lambda

Frameworks: NIST CSF, NIST 800-53, CIS Controls, Cyber Kill Chain, ISO 270001, MITRE ATT&CK.

PROJECTS

More on portfolio: <https://ranjeetreddy14.github.io>

- Cloud Incident Response Automation (AWS): Built an automated detection and response system integrating GuardDuty, EventBridge, and Lambda to automatically isolate EC2 instances, trigger SNS alerts, and reduce manual triage time by 40%.
- MCP-Based Threat Intelligence Orchestrator (Agentic AI): Built a local Model Context Protocol (MCP) server that provides LLMs with real-time threat intelligence while enforcing strict separation between language generation and security decision logic, using deterministic entity detection, semantic routing, and external APIs to deliver structured, auditable intelligence outputs.