

# MADAM RAJINIKANTH REDDY

[rajinikanthreddymadem@gmail.com](mailto:rajinikanthreddymadem@gmail.com) | +91 9392485881 | [LinkedIn](#) | [GitHub Portfolio](#)

Andhra Pradesh, India | Available for 24/7 Rotational Shifts

## PROFESSIONAL SUMMARY

---

SOC-focused Computer Science student (2023–2027) with hands-on experience in Elastic SIEM detection engineering, Windows Security log analysis, and multi-stage attack simulation. Skilled in alert triage, brute-force detection, privilege escalation monitoring, and MITRE ATT&CK mapping. Experienced in incident documentation and response lifecycle within simulated SOC environments. Seeking entry-level SOC Analyst (L1) role.

## TECHNICAL SKILLS

---

**Security Operations:** SOC Monitoring, SIEM, Log Analysis, Alert Triage, Incident Response Lifecycle, Threat Detection, False Positive Reduction, MITRE ATT&CK Mapping

**SIEM & Tools:** Elastic SIEM, Kibana, Splunk (Basic Search & Dashboards), Palo Alto, Fortinet, Zscaler

**Cloud Basics:** AWS (EC2, IAM – Fundamental Exposure)

**Scripting & OS:** Bash, Python (Basic), Windows, Linux

## INTERNSHIP EXPERIENCE

---

### Cybersecurity Intern – EduSkills Virtual Internship

- Performed SIEM monitoring and analyzed 1000+ security events in simulated SOC environment.
- Conducted alert triage, reduced false positives through rule tuning, and documented incidents following SLA guidelines.
- Implemented detection rules for authentication anomalies and suspicious activity patterns.

## PROJECT EXPERIENCE

---

### SOC Monitoring & Detection Engineering – Elastic SIEM

- Monitored Windows Security Events (4625, 4688, 4720, 4732, 4672) and built threshold-based detection rules.
- Implemented brute-force (5+ failed logins/5 min), port scan, privilege escalation, and encoded PowerShell detection.
- Developed **Advanced End-to-End Attack Chain Detection** (Port Scan → Brute Force → Valid Login → Privilege Escalation → Encoded PowerShell).
- Correlated events to construct attack timeline and mapped detections to MITRE ATT&CK techniques.
- Documented incident findings, root cause analysis, and response actions in structured reporting format.

### Log Analysis Automation Engine – Bash

- Developed automated log filtering tool using grep and awk to extract failed login attempts.
- Generated summarized reports supporting faster SOC investigation and reducing manual log review effort.

## EDUCATION

---

### Bachelor of Technology – Computer Science and Engineering(Cyber Security)

Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal

2023–2027

## CERTIFICATIONS

---

Palo Alto Network Security Fundamentals | Fortinet NSE Training | Zscaler Cloud Security | Ethical Hacking | SOC Analyst Level 1