GURU DAYAL

CyberSecurity Analyst

Uppal, Hyderabad, Telangana
+91 7329036787
gurudayal132@gmail.com
gurudayal-cybersecurity
GuruXdayal

PROFESSIONAL SUMMARY:

Cyber Security Analyst with hands-on experience in Wazuh, Splunk, Sysmon, and Suricata for real-time SIEM monitoring, incident triage, threat hunting, phishing investigation, brute-force detection, and FIM alerts. Proficient in endpoint/network/email log analysis, alert enrichment (VirusTotal), SOAR automation (n8n), root-cause analysis, and custom rule creation across Windows/Linux environments. Strong in TCP/UDP networking, Linux administration, Bash/PowerShell scripting using AI-assisted workflows (ChatGPT, Grok). 3+ years in healthcare with HIPAA compliance and secure data handling; ready to deliver L1 SOC operations in 24×7 enterprise/MSSP environments.

AREAS OF EXPERTISE:

- **Security Monitoring & Incident Triage —** Splunk, Wazuh Endpoint, Network, and Email Alert Analysis
- **Threat Hunting & Log Analysis —** Sysmon, Osquery, Windows/Linux event logs, firewall/proxy telemetry
- **Incident Response —** Phishing, Brute-force, Malware investigations with IOC enrichment
- **Email Security & DLP —** Header analysis, attachment evaluation, data-loss policy monitoring
- **Networking Fundamentals —** TCP/UDP, DNS/HTTP flow analysis, packet-level troubleshooting
- **Detection Use-Case Tuning —** Rule refinement, false-positive reduction, playbook updates
- **Automation & AI-Assisted Analysis —** n8n workflows, script generation, alert enrichment

PROFESSIONAL EXPERIENCE:

R1 RCM

Senior Analyst |November,2021 - December,2024

- Managed 80% daily claim status checks across enterprise systems while ensuring 100% HIPAA compliance in communications.
- Achieved an 75% increase in claim resolution efficiency, contributing to higher revenue cycle performance and reduced backlog.
- Engaged with clients regarding outstanding claims while safeguarding sensitive patient health information (PHI) .
- Collaborated with internal teams to ensure accurate billing, coding, and secure handling of medical records .

GOCL Corporation LTD.

Junior Technician | November, 2019 - August, 2021

- Conducted 20+ inspections weekly on electronic systems (PCBs), identifying anomalies and escalating incidents for resolution.
- Performed quality assurance testing on SMT components, achieving 95% compliance with technical standards.
- Documented and escalated recurring issues to engineering teams, contributing to reduced downtime and improved production reliability.

EDUCATION:

- 2022 - Present | Sri Chetanya Technical Campus
  B.Tech(Graduation) - Electronics Communication & Engineering
- 2013 - 2020 | Princeton College of Engg & Tech
  Diploma - Electronics Communication & Engineering

CERTIFICATIONS:

- **Certified Ethical Hacker (CEH)** | EC-Council | May,2025 - June,2026
- **Introduction to Cybersecurity** | Cisco | September,2024 - Present
- **Cybersecurity 101** | TryHackMe
- **SOC Level 1** | TryHackMe

TECHNICAL SKILLS:

- **Operating Systems**: Linux (Ubuntu, Kali), Windows (Server & Endpoint)
- **Scripting & Automation**: Bash, Shell Scripting, PowerShell (basic), n8n Automation
- **Security Tools & SIEM:** Splunk, Wazuh, Sysmon, Osquery, VirusTotal, MITRE ATT&CK Navigator, EDR, SOAR, IDS/IPS
- **SOC & System Operations**: Incident Management, Alert Triage, Root Cause Analysis, Runbook Creation, Log Ingestion & Parsing, Incident Response,
- **Threat Detection Frameworks:** MITRE ATT&CK, NIST Cybersecurity Framework, Cyber Kill Chain

PROJECTS & SOC PORTFOLIO:

GitHub Portfolio Link: https://github.com/GuruXdayal

- **SOC Home Lab:** Built a full SOC home lab and executed 4 MITRE-mapped attacks (Malicious file execution, Nmap scan detection, File Integrity Monitoring, SSH Brute-Force) to practice real-world detection engineering and threat hunting using Wazuh & Sysmon.
- **Automated AlertFlow (n8n + Wazuh):** Developed an automated enrichment & response workflow using n8n, VirusTotal API and a Python forwarder, enabling hash enrichment, malicious-file quarantine, and automated SOC email reporting.
- **Endpoint Threat Hunting (Wazuh + Sysmon):** Performed end-to-end threat hunts for LSASS dumping, PowerShell LOLBAS abuse, and malicious file execution (T1003.001, T1059.001, T1204.002), using Sysmon telemetry, Wazuh queries, and MITRE ATT&CK methodology.