Dhanush C G

Security Analyst L0 | SOC Monitoring & Threat Triage

Bengaluru, India dhanushcg100@gmail.com 086181 60189 dhanush-c-g cgdhanush Credly TryHackMe

Objective

Cybersecurity graduate with hands-on exposure to SIEM-based security monitoring, alert triage, and log analysis gained through a security operations internship and a self-built network honeypot project. Comfortable with Linux/Windows environments, networking fundamentals, and basic cloud security concepts, with practical attacker-behavior exposure through 30+ TryHackMe rooms and 5+ CTF challenges. Seeking a Security Analyst L0 role to support SOC monitoring, incident triage, and detection use-case development within an enterprise security operations team.

Experience

Cyber Security Intern, Rooman Technologies Feb 2026 – May 2026

- Monitored and analyzed security events and alerts using Splunk (SIEM), performing initial triage to flag anomalies and potential indicators of compromise across systems and network traffic
- Conducted security assessments and risk analysis on simulated environments, evaluating threats and identifying vulnerabilities against established security criteria
- Documented findings from log analysis and malware sample review to support incident identification and escalation decisions
- Maintained routine security monitoring reports and automated recurring log-review checks using Python, improving triage turnaround time
- Gained foundational exposure to cloud security controls and best practices supporting enterprise security operations

Education

HKBK College of Engineering, B.E in CSE – Bengaluru, Karnataka Dec 2022 – May 2026

- CGPA: 8.55 / 10

Projects

GhostNet-Honeypot GitHub Apr 2026 – present

Tech Stack:- Python, MongoDB, Docker, SSH, CLI

- Built a honeypot framework to continuously capture and analyze real-world attacker behavior, supporting threat detection and triage practice
- Simulated an SSH service to capture intrusion attempts, analyzing connection-level behavior to assess attacker techniques
- Designed structured, analytics-ready logging in MongoDB to support security review and reporting
- Built CLI-based controls and a web monitoring interface to track and assess ongoing security events in real time
- Used Docker to create repeatable, isolated testing environments for safe, controlled security analysis

Skills

Security Monitoring: SIEM-Based Monitoring, Log Analysis, Incident Escalation, Risk & Vulnerability Assessment

Security Operations & Tools: Splunk (SIEM), Cloud Security Fundamentals, Ethical Hacking

Networking & Systems: Windows/Linux OS, Networking Basics, Cloud Security Concepts

Automation & Reporting: Python automation/scripting, log-analysis automation, monitoring report maintenance

Programming Languages: Python, Java, JavaScript

Systems & Tools: Linux/Unix, Git, Docker, AWS

Soft Skills: Clear & Concise Reporting, Written & Verbal Communication, Team Collaboration

Certifications & Achievements

- Completed 30+ rooms and 5+ Capture-the-Flag (CTF) challenges on TryHackMe, covering network protocol analysis, service enumeration, and vulnerability exploitation View
- Ethical Hacker — Cisco, Issued Nov 2025 View
- ISC2 Candidate — ISC2 View
- Google IT Automation with Python Professional Certificate (v1) — Coursera, Issued Jun 2026 View
- Google Cybersecurity Professional Certificate (v2) — Coursera, Issued Nov 2025 View
- Google IT Support Professional Certificate (v3) — Coursera, Issued Nov 2025 View
- Google AI Essentials (v1) — Coursera, Issued Nov 2025 View

Hobbies

Hobbies: Cricket, Manga, Movies, Anime