

AHAD BAGWAN

SOC Analyst L1 | Cybersecurity Analyst – Entry Level | Blue Team & Security Monitoring

📍 Pune, Maharashtra, India | 📞 +91 7020073099 | ✉ bagwanahad@gmail.com

🌐 Portfolio | 🔗 LinkedIn | 🐙 GitHub

Professional Summary

Entry-level cybersecurity professional with hands-on project experience in security monitoring, log analysis, alert triage, and incident investigation, gained through independently built SOC and blue-team platforms. Practical exposure to SIEM concepts, MITRE ATT&CK mapping, IOC analysis, and brute-force/threat detection logic, combined with a strong networking foundation (TCP/IP, DNS, routing, switching) from an internship in network engineering. Skilled at analyzing security events across Windows/Linux environments and translating raw log data into actionable incident-response decisions. Seeking an SOC Analyst L1 role to apply security-monitoring, threat-detection, and incident-response skills in a live Security Operations Center.

Technical Skills

Security Operations & SIEM: SOC Monitoring, Security Event Analysis, Alert Triage, Incident Detection & Investigation, Log Analysis, Event Correlation, SIEM Concepts – Splunk, Microsoft Sentinel, IBM QRadar, ELK Stack, Wazuh (Familiarity/Knowledge), Detection Rules, Alert Management

Incident Response & Threat Detection: Incident Response, Incident Triage, Classification & Prioritization, Root Cause Analysis, Escalation Procedures, Playbooks, MITRE ATT&CK, IOC/TTP Analysis, Threat Hunting, Threat Intelligence, Brute-Force & Suspicious-IP Detection, Malware & Phishing Concepts

Networking: TCP/IP, OSI Model, IPv4/IPv6, Subnetting, DNS, DHCP, HTTP/HTTPS, SSH, FTP, SMTP, TCP vs UDP, ARP, ICMP, VLAN, Routing & Switching, NAT, Network Troubleshooting, Port Scanning

Operating Systems & Security: Windows, Linux, Windows/Linux Event Logs, Command Line, PowerShell Basics, Authentication & Access Control, Password Security, Cryptography Fundamentals, Firewalls, IDS/IPS Concepts, Endpoint Security, Vulnerability Management

Programming & Tools: Python, Git/GitHub, PowerShell, Bash

Professional Experience

Network Engineer Intern — Humming Byte

Dec 2025 – Jun 2026

- Assisted with network troubleshooting, connectivity diagnostics, and device configuration to support infrastructure up-time and reliability.
- Applied TCP/IP, routing, and switching fundamentals to identify and resolve network connectivity issues.
- Supported infrastructure monitoring and maintained technical documentation of network configurations and issue resolutions.

Cybersecurity Projects

SOC Forge — Interactive SOC Analyst Training Simulator & Blue-Team Practice Platform [🐙 GitHub](#) [🔗 Live Demo](#)

- Developed an interactive SOC analyst training simulator for practicing alert triage, security log analysis, incident investigation, and blue-team response workflows.
- Implemented realistic security scenarios requiring analysts to investigate alerts, identify suspicious activity, prioritize incidents, and determine appropriate response actions.
- Mapped simulated attack activity to MITRE ATT&CK techniques and designed an analyst-focused interface for evidence analysis, incident classification, and response decision-making.

SOC Dashboard — Mini SIEM / Security Monitoring Platform [🐙 GitHub](#) [🔗 Live Demo](#)

- Built a mini SIEM platform for ingesting and analyzing security logs and generating real-time security alerts.
- Implemented sliding-window detection logic to identify repeated authentication failures and potential brute-force attacks.
- Developed IP whitelist/blacklist controls to support suspicious-source filtering and security event investigation.
- Created a security monitoring dashboard to visualize alerts and assist with rapid SOC-style triage.

NetPulse — Network Device Inventory & Monitoring Console [🐙 GitHub](#) [🔗 Live Demo](#)

- Developed a network monitoring console (React, Flask, SQLAlchemy) for centralized device inventory, infrastructure visibility, and operational monitoring.
- Implemented ICMP-based latency probing to monitor device reachability and identify potential connectivity issues.
- Built interactive topology and rack visualization features to improve network infrastructure visibility and troubleshooting.

Certifications & Training

- CCNA Training — Completed
- IT Support Training — Completed
- CEH (Certified Ethical Hacker) — EC-Council | Training Completed, Certification Expected October 2026
- SOC Analyst Certification — EC-Council | Training Completed, Certification Expected November 2026

Education

G H Raisoni College of Engineering and Management, Pune | CGPA: 8.47 | 2022 – 2026