

Akash Bhat

akashbhat1402@gmail.com | +91-7022546438 | linkedin.com/in/akashbhat14 | github.com/AkashBhat14

PROFESSIONAL SUMMARY

Cybersecurity practitioner with a strong blue team orientation and hands-on experience in threat detection and SIEM engineering. Proficient with Wazuh, ELK Stack, and Azure Sentinel, with a proven ability to build and deploy effective defense mechanisms in SOC environments while leveraging AI and automation.

EDUCATION

PES University

Bachelor of Technology in Computer Science and Engineering

Courses: Information Security, Computer Networks, Cryptography, Artificial Intelligence

Bangalore, India

May 2025

SKILLS

Security Tools: Azure Sentinel, Wazuh, Elastic SIEM, Wireshark

Cloud: AWS, Vultr, Git

AI Tools/Frameworks: Elevenlabs, N8N, LangChain

EXPERIENCE

USEReady

AI Automation Engineer

Bangalore, India

Oct 2025 – Jan 2026

- Built a real-time AI receptionist to automate appointment scheduling and FAQ handling through voice interactions, securely capturing user information and minimizing manual administrative effort.

BOSCH

Security Analyst Intern

Bangalore, India

Jan 2025 – May 2025

- Triaged and resolved 20–30 daily security alerts, including failed login attempts, suspicious IP activity, improving alert accuracy and supporting a 20% reduction in team-wide MTTR through proper documentation and playbook adherence.
- Integrated VirusTotal API with Wazuh to detect known malware via hash lookups and automated endpoint remediation, reducing manual intervention time by 90%.
- Developed a Document-based Chatbot using Retrieval-Augmented Generation (RAG) to enable intelligent question answering over large sets of documents, reducing triage lookup time by 40%.

ETAS

Automotive Security Research Intern

Bangalore, India

Jun 2024 – Aug 2024

- Researched and benchmarked automotive security solutions, improving internal evaluation accuracy by 30% and helping prioritize product roadmap decisions against 4 key competitors.

CERTIFICATIONS AND TRAINING

[1] CompTIA Security+

Jun 2025

[2] Google Cybersecurity Professional Certification

RESEARCH/PROJECTS

Blue Team in a Box: ELK-Powered SOC with Brute-Force Defense and Red Team Simulation

- Engineered a production-grade SOC environment using ELK Stack, Elastic Agents, and Fleet Server, enabling centralized log ingestion, threat detection, and real-time visualizations across simulated endpoints.
- Developed and tuned detection rules for SSH/RDP brute-force attacks with MITRE ATT&CK mappings, integrating automated alert escalation to oSTicket for a full incident lifecycle simulation.
- Integrated Mythic C2 framework to emulate adversary behavior, enabling blue team validation of detection logic and enhancing readiness against modern threat actors.