Ajinkya Bhosale

+91-7057641064 | bhosaleajinkya2205@gmail.com | github.com/ajinkyainfosec | linkedin.com/in/ajinkya–bhosale | learnwithajinkya.dev

Professional Summary

Computer Engineering student with practical experience in SOC operations, SIEM platforms (IBM QRadar, Wazuh), and security event monitoring. Top 5% on TryHackMe (3M+ users) with 110+ labs in alert triage, log analysis, network traffic analysis, and incident response workflows. Familiar with threat detection, malware behaviour, and security reporting. Eager to contribute to a SOC team and learn from experienced analysts in a real-world environment.

Technical Skills

SOC & Security: Alert Triage, Log Analysis, Phishing Investigation, Incident Response, Malware Analysis, MITRE ATT&CK Framework
SIEM Platforms: IBM QRadar (internship experience), Wazuh (self-deployed lab), Splunk (TryHackMe training)
Security Tools: Nmap, Burp Suite, Metasploit, Wireshark, MITRE ATT&CK Framework, OSINT Tools
Systems & Networking: Linux (Ubuntu), Windows, TCP/IP, DNS, HTTP/HTTPS, Firewalls, VPN
Programming: Python, C++ Bash, SQL
Other Tools: Azure Fundamentals, Docker, VirtualBox, VMware, Git

Professional Experience

Cybersecurity Internship Trainee October 2024 (4 weeks)
CSRBOX *Pune, Maharashtra, India*

- Monitored security alerts and events using IBM QRadar SIEM; assisted in initial triage and investigation of suspicious activity
- Analysed logs and documented incident findings with clear remediation recommendations for SOC analysts
- Conducted OSINT investigations using tools like theHarvester and Google Dorking to gather target intelligence
- Gained hands-on experience in network scanning, enumeration, and basic threat analysis

Python Development Intern July 2022 – August 2022
Bharat Software Solutions *Pune, Maharashtra, India*

- Learned Python web development fundamentals by building small web applications using the Flask framework
- Structured backend logic using modular Python code for maintainability and scalability
- Handled form data processing and server-side validation to ensure correct user input

Security Projects & Lab Experience

TryHackMe SOC & Security Training | *Top 5% globally (3M+ users)* 2024 – Present

- Completed 150+ labs across SOC Level 1, Cyber Defense, and Red Teaming paths
- Practised alert triage, log analysis, network traffic analysis, phishing investigation, malware analysis, and incident documentation in simulated SOC environments
- Participated in CTF competitions applying threat detection and analytical thinking under time pressure

Wazuh SIEM Lab Deployment | *Wazuh, Linux, Wireshark* 2025

- Self-deployed Wazuh for multi-host log collection, alert management, and endpoint behaviour monitoring in a home lab
- Created custom detection rules mapped to MITRE ATT&CK for phishing, malware, and unauthorized access scenarios
- Analysed network traffic using Wireshark alongside log correlation to investigate simulated incidents
- Documented incident findings and produced structured security reports in a format suitable for SOC analyst review

Host-Based Intrusion Detection System (HIDS) | *Rust, Python/FastAPI, PostgreSQL, Docker* | GitHub 2026

- Engineered a 4-component full-stack HIDS (Rust agent + FastAPI backend + PostgreSQL + Docker) supporting multi-host centralized threat detection
- Reduced file integrity monitoring latency by **97%** – from 30s to under 1s – using Linux inotify for real-time event capture
- Built a Sigma-based detection engine with **17 custom rules** covering **8 MITRE ATT&CK tactics**; achieved **˜80% detection rate** across simulated attacks (SSH brute force, privilege escalation, reverse shells)
- Designed a real-time WebSocket dashboard for SOC-style alert triage with live MITRE ATT&CK technique visualization

Multi-Port Honeypot for Threat Intelligence | *Python* | GitHub 2024

- Built a multi-port honeypot (SSH, FTP, HTTP/HTTPS) to capture real attacker behaviour and TTPs
- Analyzed captured logs to identify botnet activity and brute force campaigns; documented findings in an intelligence report

Education

Sinhagad Institute of Technology and Science Pune, Maharashtra, India
Bachelor of Engineering in Computer Engineering | CGPA: 8.02 | Expected: September 2026 *Aug 2023 – Present*

Zeal Polytechnic College Pune, Maharashtra, India
Diploma in Computer Engineering | 86.69% *Aug 2020 – 2023*

Certifications

ISC2 Certified in Cybersecurity (CC): Training Completed
TryHackMe: Cyber Security 101 Path Completed | Top 5% globally
Microsoft Azure Fundamentals: Cloud concepts & services
Foundations of Cybersecurity: Cyber-attacks, Information Assurance