SAHIL SALGAONKAR

Pune, India • sahilsalgaonkar221@gmail.com • +91 7600634971 • linkedin.com/in/sahil-salgaonkar-404719233

PROFESSIONAL SUMMARY

Cybersecurity Professional with hands-on experience in SOC Operations, Threat Hunting, Malware Analysis, Vulnerability Assessment, and Security Monitoring. Skilled in Log Analysis, Incident Triage, Threat Intelligence, and MITRE ATT&CK–based attack mapping. Experienced in developing AI-powered SOC analyzers, ransomware detection systems, and vulnerability management platforms using Python and Machine Learning. Proficient with Wireshark, Nmap, Burp Suite, Nessus, Splunk, Microsoft Sentinel, and OpenVAS, with strong knowledge of Linux, Windows, Networking, OWASP Top 10, and SIEM Fundamentals.

EXPERIENCE

SOC Analyst Intern | SkillEcted — Aug 2025 – May 2026

Pune, India

- Built and operated a mini-SOC lab using virtual machines to simulate real-world attacks, perform threat hunting, log analysis, and execute endpoint security workflows.
- Used open-source security tools including Wireshark, Nmap, Traceroute, and Sysinternals Suite for network scanning, packet analysis, process monitoring, and threat detection.
- Analyzed malware behavior in controlled lab environments by tracing execution flow, identifying persistence mechanisms, and monitoring registry and system changes.
- Performed IOC analysis by researching threat intelligence feeds, analyzing malware hashes, IP reputation, and mapping attacker techniques to the MITRE ATT&CK framework..
- Conducted reconnaissance and enumeration on web applications using Nmap and Gobuster to identify exposed services and attack surfaces.
- Tested web applications for OWASP Top 10 vulnerabilities, including SQL Injection (SQLi) and Cross-Site Scripting (XSS).
- Utilized Burp Suite for HTTP request interception, request manipulation, fuzzing, and vulnerability identification.
- Performed vulnerability scanning using Nessus and OpenVAS, followed by manual validation to eliminate false positives and confirm exploitability.

UI/UX Design Intern | Tech Elecon Pvt. Ltd. — Jan 2025 – Apr 2025

Anand, Gujarat, India

- Collaborated with the design team to create user-centric web and mobile UI designs using Figma.
- Developed wireframes and interactive prototypes to visualize user flows and improve usability.
- Worked on improving design consistency and user experience through iterative feedback.
- Tools/Skills: Figma, Wireframing, Prototyping.

Artificial Intelligence Intern | CodSoft — May 2024 – Jun 2024

- Worked on AI-based tasks/projects and gained hands-on exposure to ML implementation workflow.

PROJECTS

AI SOC Analyzer | CanHack 2026 – International Hackathon

University of Canberra, Australia | January 17–18, 2026

- Developed an AI-powered Security Operations Center (SOC) Analyzer to automate large-scale security log analysis.
- Implemented anomaly detection mechanisms to identify suspicious behavior patterns.
- Designed an alert prioritization framework to reduce false positives and improve incident triage efficiency.

Sentinel AI – Threat Orchestration & Reporting System | Personal Project | May 2026

- Developed an enterprise-grade vulnerability management orchestration platform to unify and automate large-scale security scans across network and container environments.

- Integrated an intelligent risk prioritization framework utilizing machine learning to reduce false positives and focus analyst attention on high-impact vulnerabilities.
- Built an automated compliance and reporting pipeline capable of generating professional, executive-ready security audit PDFs directly from raw scan data.

Vulnerability Scanner (Nmap + NVD + CVSS)

- Automated port/service scanning and CVE mapping using NVD API, with CVSS-based risk scoring.
- Built Web UI and CLI, caching for performance, and downloadable reports (PDF/HTML/JSON/Text).
- Report includes vulnerability severity, possible attacks, and remediation suggestions.

Ransomware Detection System | Personal Project

- Developed a machine learning–based ransomware detection system to classify malicious and benign executable files.
- Extracted and analyzed Portable Executable (PE) file features for malware behavior identification.
- Implemented Random Forest–based classification using Python and Scikit-learn to improve detection accuracy.
- Performed data preprocessing, feature selection, and model evaluation for efficient threat analysis.

Library Management System | Web Application

- Tech: HTML, CSS, JavaScript, PHP, MySQL. Implemented admin panel, user login, book issue/return, and database management.

Blood Donor Directory | Web Application

- Tech: HTML, CSS, JavaScript, PHP, MySQL. Implemented donor/seeker login, search, request management, and admin controls.

TECHNICAL SKILLS

Security Operations: Security Monitoring, Alert Triage, Incident Validation & Reporting, Log Analysis, Threat Identification, Escalation Procedures, SIEM Fundamentals, MITRE ATT&CK (Basic)

Operating Systems: Windows (10/11), Linux (Ubuntu, CentOS) – Basic Log Review, Process Monitoring

Cybersecurity & Networking: OSI & TCP/IP Models, Basic Network Traffic Analysis, Incident Response Fundamentals, Security Auditing, Common Cyber Attacks (SQLi, XSS, Phishing, Malware, DoS), OWASP Top 10, ISO 27001 & NIST CSF

SIEM & Security Tools: SIEM Platforms (Basic), Wireshark, Nmap, Burp Suite, Nessus, OpenVAS, Jira, Endpoint Security (Basic EDR), Microsoft Sentinel

Scripting: Bash (Basic)

EDUCATION

BE (IT) – Madhuben & Bhanubhai Patel Institute of Technology — Jul 2022 – Apr 2025
Ahmedabad, India

Diploma – Government Polytechnic Daman — May 2019 – Apr 2022
Daman, India

CERTIFICATIONS & COURSES

- Deloitte Cyber Job Simulation – Certificate of Completion (Forage)
- Intro to Splunk (eLearning)
- Fortinet Network Security Expert (NSE) Levels 1–3
- IBM (Coursera) – Operating Systems: Overview, Administration, and Security
- Mastercard Cybersecurity Virtual Experience Program (Forage) | February 2026

SOFT SKILLS

Communication Skills • Professionalism • Passion for Work • Patient Listener • Hardworking • Self-confidence • Quick Learner • Adaptive