SOHAM JADHAV

Portfolio | Email | LinkedIn | Github

Education

University College London 2026 – 2027
MSc in Information Security

Marathwada Mitra Mandal's College Of Engineering 2022 – 2026
Bachelor of Engineering in Computer Engineering; CGPA: 8.81/10 (First Class equivalent)

Experience

The Tech Protein Jan. 2025 – Present

Project Lead | Bangkok, Thailand / Pune *Jan. 2026 – Sep. 2026*

- Led a 5-member team to develop cybersecurity learning resources across application security, cloud security, Active Directory, networking, and digital forensics, adopted across 3 training cohorts.
- Mentored interns, reviewed technical content, and established documentation standards, contributing to a 93% assignment completion rate through practical labs and structured learning resources.

Security Analyst | Pune *Jul. 2025 – Jan. 2026*

- Conducted security assessments for 62+ web applications and authored 70+ assessment reports, identifying vulnerabilities, validating security controls, and supporting remediation.
- Onboarded 60+ applications to Imperva WAF, investigated security events using SIEM, EDR, XDR, and Active Directory, and reduced phishing click rates by 43% and 53% across two campaigns.

Security Operations Center Analyst Intern | Pune *Jan. 2025 – Jul. 2025*

- Monitored 12+ endpoints and investigated 15+ security alerts, supporting the triage of 6+ security incidents through log analysis and telemetry correlation using SIEM, EDR, and XDR platforms.
- Administered Microsoft 365 and Active Directory, while developing technical documentation, standard operating procedures, and phishing awareness material to strengthen operational consistency and enterprise security practices.

Projects

Detection Engineering Platform

Python, Streamlit, Sysmon, MITRE ATT&CK, Threat Intelligence, FastAPI

- Built a modular detection engineering platform that processed 100K+ Windows security events, mapped telemetry to the MITRE ATT&CK framework, and implemented 25+ reusable detection rules to detect common attack techniques.
- Engineered an AI-assisted investigation dashboard with threat intelligence enrichment, risk scoring, and timeline reconstruction, reducing simulated incident investigation time by approximately 60% in a controlled lab environment.

AI Security Triage Agent

Python, FastAPI, MCP, OpenAI, Docker, GitHub Actions

- Developed an AI-powered security triage platform that consolidated findings from 5+ security tools, removed duplicate alerts, enriched vulnerabilities with contextual threat intelligence, and prioritised remediation based on risk.
- Designed an MCP-based automation pipeline integrating LLMs, GitHub Actions, and security workflows, reducing manual vulnerability triage effort by approximately 70% while automatically generating investigation reports and remediation tickets.

Independent Security Research (HackerOne)

Web3 Security, Access Control, SSRF, Smart Contracts

- Discovered a critical authorization bypass in Lightspark's Spark Operator infrastructure, exposing FROST signing and consensus gRPC endpoints to unauthenticated access.
- Reported 4 additional vulnerabilities across DeFi and blockchain systems, including an SSRF in Chia Network's Data Layer sync and a token blocklist bypass in Ripio's USDar contract.

Publications

Co-Author, AI In Cybersecurity August 2025

- Co-authored chapters on machine learning for threat detection and AI-driven vulnerability assessment in a published book exploring the intersection of AI and cybersecurity.

Technical Skills

Programming	Python, Bash, JavaScript, SQL, FastAPI, React.js, Node.js, PostgreSQL, MySQL, HTML, CSS
Infrastructure	Linux, Windows, Docker, VMware, Microsoft Azure, Active Directory, Microsoft 365, Elasticsearch, Kibana
Security Operations	Microsoft Sentinel, Microsoft Defender XDR, Wazuh, Sophos XDR, Cyrebro SIEM, Splunk SOAR, MISP
Security Engineering	Burp Suite, OWASP ZAP, Nmap, Tenable Nessus, OpenVAS, Imperva WAF
Application Security	OWASP Top 10, OWASP API Top 10, Semgrep, Bandit, JWT, Postman, pytest

Certifications

- CompTIA Security+ Sept. 2025

Volunteering

President, Student Welfare Club Dec. 2023 - July 2025

- Led a 22-member team and directed cross-industry tech talks with 15+ companies including Microsoft, Google, Dell, VMware, and Oracle, launching a leadership program that boosted retention by 45% and secured 2 new corporate partnerships.

Cybersecurity Education Leader August 2025

- Designed and delivered cybersecurity workshops on social engineering, malware analysis, encryption, and incident response, achieving 95% satisfaction and establishing a recurring education program.

Honours & Awards

- Chosen as HackerEarth Campus Ambassador
- Awarded Data Guardian recognition by The Tech Protein