Swaraj Singh

swarajsingh211@gmail.com +91 93724 34984 Portfolio GitHub LinkedIn

EXPERIENCE

SOC Analyst at Knowledge Mine Info Media Jun-Aug 2026

- Conducted proactive threat hunts by correlating external OSINT indicators with internal firewall logs; investigated IAM anomalies and phishing campaigns and documented findings using MITRE ATT&CK for Tier 2 escalation.
- Supported enterprise GRC initiatives and NIST SP 800-53 compliance audits, prepared risk-management documentation, and ran automated VAPT scans to prioritize remediation.
- Executed malware tabletop simulations and incident-response playbooks for host isolation, helping formalize end-to-end security-event workflows.

Product Development Intern at SYNIRIS Technologies Jun-Aug 2025

- Developed centralized role-based authentication workflows, reducing administrative onboarding and configuration time by 35%.
- Led PASTA threat-modeling sessions that surfaced 12+ potential attack vectors early in design and reduced post-deployment application-security defects by 40%.

Project Trainee Intern at ARC SOLUTIONS Jun-Aug 2024

Melbourne, Australia · Remote

- Built Sentinel-1 SAR data-processing workflows in Google Earth Engine for large-scale environmental mapping and produced technical implementation reports.

PROJECTS

Faultplane Python · Groq API · GitHub Actions · NVD 2.0 · CISA KEV Live

- Built an automated threat-intelligence platform that aggregates 10+ authoritative security sources, enriches vulnerabilities through NVD and CISA KEV, generates executive summaries, and publishes daily through GitHub Actions.

LedgerCast Python · ITGC / SOX · ISO 27001 · NIST CSF 2.0 · COBIT 2019 Live

- Developed a packaged CLI and client-side dashboard for testing access management, change management, backup and recovery, and segregation-of-duties controls, with findings management and framework crosswalking.
- Added client-side CSV re-testing and DOCX audit-report generation for repeatable control reviews.

PolicyForge Security Governance · ISO 27001 · NIST CSF 2.0 · DPDP Act 2023 Live

- Created a portfolio GRC programme for a fictional fintech with eight security policies, numbered safeguards, a control-traceability matrix, and exception and review-cadence registers mapped to major security and privacy frameworks.
- Defined evidence expectations and review cycles while keeping the suite clearly illustrative.

Agentic IaC Vulnerability Detection & Remediation Project

Python · Terraform · Docker · Checkov · LLM Workflows · Streamlit

- Built an automated DevSecOps workflow that detects Infrastructure-as-Code security misconfigurations, generates remediated configurations, and validates proposed fixes with Checkov before presenting results.
- Supports Terraform and Dockerfile inputs with severity classification and original-versus-remediated comparison.

SKILLS

- **SOC, Detection & GRC:** Threat Hunting, Alert Triage, Incident Response, MITRE ATT&CK, Microsoft Sentinel, SentinelOne, Splunk, NIST SP 800-53, NIST CSF 2.0, ISO 27001/27701, ITGC / SOX, ServiceNow GRC / IRM
- **Security Engineering & Automation:** Python, Bash, PowerShell, Terraform, Docker, Checkov, GitHub Actions, IAM / RBAC, PASTA Threat Modeling, VAPT, OSINT, CVE Analysis, NVD 2.0, CISA KEV

EDUCATION & CREDENTIALS

B.Tech in Computer Science & IT - Cyber Security 2023-2027

Symbiosis Skills and Professional University

CREST CTF - Top 10 · CSCSO · Cisco Ethical Hacker

ISO 27701 Lead Auditor · SC-200 expected Nov 2026