MD SAAD

Cybersecurity Engineer — Security Operations, Detection Engineering & AI Agent Security

Bhadreswar, West Bengal, India · Hackwithsaad@gmail.com · +91 6291773764 · github.com/saadcyber21 · saadcyber21.github.io

SUMMARY

Cybersecurity engineer with 3+ years across 24×7 SOC operations, offensive security and compliance management. Detects, hunts and responds under defined SLAs; tunes SIEM/XDR/SOAR for detection fidelity; automates SOC workflows in Python. In parallel, publishes open-source security tooling for AI agent scaffolds — an offline red-team harness mapped to OWASP ASI 2026, an autonomous threat-hunting pipeline with explainable forensics, and a zero-dependency secret scanner with published, reproducible false-positive and recall rates. Every public claim ships with the command that reproduces it.

PROFESSIONAL EXPERIENCE

Cybersecurity Engineer — Lead Analyst & Compliance Manager

Mar 2025 – present

Remote · 24×7 enterprise SOC · employer name withheld; references on request

- Monitor, detect and respond to security incidents under defined policies and SLAs; lead compliance-management initiatives alongside analyst duties.
- Forensic investigation and malware analysis during active incidents; threat hunting, vulnerability assessment and red-team activity across enterprise networks, AWS, Azure and web/mobile applications.
- Configure and tune SIEM, XDR and SOAR platforms to improve detection fidelity, reduce false positives and accelerate response.
- Python automation for SOC workflows: IOC enrichment, log correlation, alert triage and ticket generation.
- Purple-team exercises with DevOps and engineering; mentor junior analysts to raise SOC maturity.

SOC Analyst — ServiceNow automation · Azure red-team assistant

Jan 2024 – May 2024

Remote · managed security service · employer name withheld; references on request

- Ran SOC analyst shifts: triage, escalation and incident documentation inside SLA.
- Built ServiceNow automation for triage and ticketing, cutting manual handling per alert.
- Assisted Azure red-team operations; authored an internal assistant application for cloud attack-path validation.

Junior Cybersecurity Analyst — penetration testing & IR playbooks

Mar 2023 – Dec 2024

Internship → junior analyst · employer name withheld; references on request

- Network and web-application penetration testing: SQL injection, XSS and misconfigurations, with risk-analysed reports and remediation guidance.
- Hands-on engagements with Burp Suite, Nmap, Metasploit and OWASP ZAP.
- Vulnerability scanning and risk assessment; co-authored security policies, procedures and incident-response playbooks.

SELECTED OPEN-SOURCE WORK

- **quillback** — offline, deterministic red-team harness for AI agent scaffolds. 18 attacks mapped to OWASP ASI 2026; SARIF export; 19 findings on a vulnerable reference agent, 0 on the hardened variant, asserted in CI both directions. v0.1.0 released.
- **LogAgent-SOC** — autonomous threat-hunting pipeline on local open-weight models: zero-shot log parsing with source-span validation, MITRE ATT&CK-grounded ReAct loop, explainable forensic reports, CI-gated CyberMetric benchmark.
- **secret-sweep** — zero-dependency credential scanner: 23 false positives across 304,467 lines of CPython (0.0076%), 99.5% recall on generated credentials; both figures reproducible via *scripts/calibrate.py*.

- **zero-trust-ai-gateway** — RBAC and deep payload-inspection proxy for agent tool calls; blocks destructive SQL, command chaining and reverse shells with an explicit 406.
- Plus: NIST AI RMF compliance mapper, Terraform plan scanner, MITRE→Sentinel KQL generator, phishing triage, and three distributed-systems services (booking engine, double-entry ledger, workflow engine).

TECHNICAL COMPETENCIES

Security operations: SIEM (Splunk, QRadar), XDR, SOAR, MITRE ATT&CK, incident response, threat hunting, malware analysis, digital forensics

Offensive: penetration testing, vulnerability assessment, red teaming, Atomic Red Team, Metasploit, Burp Suite, prompt-injection & agent abuse

Cloud & infrastructure: AWS, Azure, firewalls, proxies, VPNs, API / web / mobile application security, network protocols, Zero Trust

Engineering: Python (log parsing, API integration, SOAR automation, IOC enrichment), FastAPI, PostgreSQL, CI-gated benchmarks, SARIF

CERTIFICATIONS

Microsoft SC-200 — Security Operations Analyst (in progress)

Junior Cybersecurity Analyst Career Path — Cisco, Apr 2025

Certified Ethical Hacker (CEH) — OneByte, Jan 2023, ID EHOBL202301658

Cybersecurity Job Simulation — Mastercard · Forage, Nov 2023

Become an Ethical Hacker — LinkedIn, Oct 2023

Career Essentials in Cybersecurity — Microsoft · LinkedIn, Oct 2023

Cybersecurity Compliance Framework & System Administration — Coursera, Mar 2023

Network Security & Database Vulnerabilities — Coursera, Mar 2023

Introduction to Cybersecurity Tools & Cyber Attacks — Coursera, Feb 2023

Learning Threat Modeling for Security Professionals — LinkedIn, Dec 2022

EDUCATION

BSc in Cybersecurity — Maulana Abul Kalam Azad University of Technology, Kolkata, India · Jan 2022 – Jan 2024 · 77% final examination score

Employer names are withheld from all public materials by design; roles, dates and scope are exact and verified references are available on request. Technical claims are evidenced in the open at github.com/saadcyber21 — the interactive portfolio at saadcyber21.github.io links every claim to the command that reproduces it.