HARSH YADAV

Faridabad, Haryana,121004

socharsh@gmail.com | +91- 9211391820 | : linkedin.com/in/harsh | :github.com/HarshYdav

Summary

Cybersecurity professional candidate with hands-on experience in SOC monitoring, incident response, threat intelligence, OSINT investigations, vulnerability assessment, cloud security, and ISO/IEC 27001 compliance. Skilled in SIEM analysis, endpoint monitoring, log correlation, MITRE ATT&CK mapping, and risk assessment, with internship exposure in real-world security operations.

Experience

OSINT & Threat Intelligence Intern — Cyber Secured India Ongoing

- Conducting OSINT investigations, data leak monitoring, and IOC enrichment
- Mapping threats to MITRE ATT&CK and preparing intelligence reports
- Assisting in intelligence-led security operations through threat analysis, contextual research.

Cybersecurity Intern — Code Alpha Feb 2025 – May 2025

- Performed SOC monitoring, alert analysis, and log review using SIEM tools
- Assisted in vulnerability assessment, incident investigation, and documentation
- Supported endpoint, network, and cloud security operations

PROJECTS

RedOpsSim *(Windows AD Lab | PowerShell | Python | MITRE ATT&CK)* DEC 2025

- Simulated post-exploitation attacker TTPs including system discovery, privilege enumeration, and execution workflows aligned with MITRE ATT&CK.
- Automated attack flow orchestration and telemetry generation to support SOC detection engineering, log correlation, and threat hunting.
- Enhanced incident response readiness by emulating realistic adversary behaviour for security monitoring and alert validation.

CloudSecOps *(AWS | IAM | S3 | Log Analysis | SQL)* DEC 2025

- Configured AWS CloudTrail for centralized cloud security logging and visibility across AWS services.
- Analysed IAM authentication events, API activity, and S3 access logs to identify misconfigurations and unauthorized access.
- Supported cloud threat detection, risk assessment, and compliance monitoring aligned with AWS security best practices.

FortiShield *(Wazuh SIEM | Sysmon | Windows Logs | Linux)* NOV 2025

- Implemented endpoint telemetry collection using Sysmon integrated with Wazuh SIEM for Windows security event monitoring.
- Performed log analysis, alert triage, and rule-based detection supporting EDR concepts and SOC workflows.
- Strengthened endpoint security posture through incident detection, investigation, and response validation.

CERTIFICATIONS

- ISO/IEC 27001 Lead Auditor. DEC 2025
- CCEP – Certified Cyber Security Educator Professional. DEC-2025
- Google Cybersecurity Professional Certificate. JUL-2025
- ISC2 Candidate. NOV-2024

SKILLS

SOC: - SOC Monitoring, Incident Detection& Response, Alerts, Log Correlation, MITRE ATT&CK, Threat Hunting, IAM.
Threat Intelligence: - OSINT, Threat Actor Profiling, Dark Web Monitoring, Intelligence Reporting, IOC Enrichment.
Tools & Tech: - Wazuh, SIEM, SOAR, Sunicart, Snort, QRadar, Nmap, Burp Suite, Linux, SQL, Metasploit, Windows Event Logs, Git , Maltego, Shodan, KnowBe4, Sysmon, Python, JAVA, C++.
Cloud & GRC: - AWS, Docker, Kubernetes, Security Audits, S3 Monitoring, IAM Security, ISMS, ISO27001.

EDUCATION

- **MCA** (Cyber Security) – Lovely Professional University (8.3 CGPA) Since AUG 2024
- **BCA** – Aggarwal College Ballabgarh (78 %) APR 2021 – MAY 2024