B. MOKSHITH DHRONA

Cybersecurity | SOC & Detection Engineering | Security Research

Hyderabad, Telangana, India · +91 9059169696 · dhrona1421@gmail.com · LinkedIn · GitHub

PROFILE

2nd-year B.Tech Computer Science & Business Systems student focused on cybersecurity, with hands-on experience building security tooling, performing CTF-based challenges, and designing endpoint telemetry research experiments. Built **GhostSOC**, a containerized security monitoring and detection platform, and currently developing a reproducible research study measuring Windows telemetry coverage for MITRE ATT&CK techniques using Windows Event Logs and Sysmon. Seeking a Cybersecurity/SOC internship to contribute to security monitoring, detection, investigation, and automation.

TECHNICAL SKILLS

Security: SOC Operations · Detection Engineering · Incident Response · Network Security · Web Security · Reconnaissance · Security Monitoring · MITRE ATT&CK

Tools: Wireshark · Nmap · SIEM · Sysmon · OpenSearch · Docker · FastAPI · React · PostgreSQL · Git/GitHub

Systems: Linux · Windows · Windows Event Logs · Virtualization · Networking

Programming: Python · SQL · Bash · JavaScript

SELECTED PROJECTS

GhostSOC — Security Operations & Detection Platform

FastAPI · React/Vite · PostgreSQL · OpenSearch · Docker · MITRE ATT&CK

- Built a full-stack, containerized SOC platform (FastAPI backend, React/Vite frontend, PostgreSQL, OpenSearch) covering the detection-to-response lifecycle: monitoring, detection, correlation, investigation, reporting, and response.
- Implemented a deterministic detection engine with 12 detection rules plus 35-category web-attack detection, mapped to MITRE ATT&CK techniques with automated risk scoring.
- Built alert-to-incident correlation, IOC extraction/enrichment, an evidence/investigation workflow, and network/attack/incident visualizations.
- Designed role-based access control (Admin / Analyst / Viewer), an immutable audit trail, and live activity streaming via Server-Sent Events (SSE).
- Built multi-format reporting (PDF, JSON, CSV, ZIP) and a connector framework for external security tools (Wazuh, Velociraptor, Arkime, MISP, OpenCTI, Shuffle), designed to honestly report integration health rather than false-positive "connected" states.
- Implemented a safe, dry-run response orchestration layer and controlled demo-mode runners for live, non-destructive incident-response demonstrations, plus automated backend test suites.
- Actively developing toward an automated detect → correlate → investigate → respond → verify → audit pipeline with policy-driven response automation. (Status: in active development)

GitHub: Dhrona1421/GhostSOC

GhostScan — Reconnaissance Dashboard for Authorized Assessments

Python · DNS · TLS · HTTP · Web Technologies

- Built a reconnaissance dashboard for discovering, organizing, and visualizing information on assets the user owns or is explicitly authorized to assess — domains, subdomains, IPs, DNS records, TLS certificates, HTTP headers, and technology fingerprints.
- Deliberately scoped to passive, standard-protocol techniques only (DNS resolution, standard TLS handshake, standard HTTP GET) — no exploit execution, credential attacks, or any functionality designed to compromise systems.
- Enforced explicit, server-side authorization confirmation before any scan job can be queued, rather than relying on UI-level restrictions alone.

GitHub: Dhrona1421/GhostScan

Windows Telemetry Coverage Research

Windows 10 · Sysmon · Windows Event Logs · MITRE ATT&CK · Python

Evaluating Windows Telemetry Coverage for Selected Red-Team Techniques Under Different Logging Configurations

- Designed a controlled experiment comparing native Windows auditing vs. Sysmon-enhanced telemetry.
- Planned 300 trials across five MITRE ATT&CK techniques and two logging configurations.

- Defined quantitative measures for event presence, consistency, evidence quality, and detection latency.
- Designed an isolated Windows/Ubuntu virtual lab and reproducible EVTX data-collection pipeline.
- Created schemas and analysis workflows for extracting process, parent-process, command-line, user, timestamp, and event-ID telemetry.
- Developing the study as an open, reproducible research package for detection-engineering experimentation. (Status: experimental execution / data collection in progress)

Vulnerable Web Security Lab *Docker · Web Security · Backend Development*

- Developed a deliberately vulnerable web application and attack-simulation environment for controlled security testing.
- Designed the environment to generate security-relevant activity for monitoring and analysis through SOC tooling.

HANDS-ON SECURITY EXPERIENCE

TryHackMe — Hackers Holiday 14-Day CTF *Completed · Certificate Earned*

- Completed the full 14-day cybersecurity CTF program through hands-on, challenge-based learning.
- Practiced reconnaissance, enumeration, Linux, networking, web security, and security problem-solving in controlled environments.

Cybersecurity Workshop & Hackathon — BVRIT *1st Place / 1st Rank*

- Secured 1st place in a cybersecurity workshop and hackathon conducted by BVRIT.
- Applied practical cybersecurity knowledge in a competitive, hands-on environment.

RESEARCH INTERESTS

Currently researching how much visibility standard Windows auditing gives defenders compared to Sysmon-enhanced logging, across common red-team techniques — aimed at giving SOC teams data-backed guidance on logging configuration trade-offs.

Detection Engineering · Windows Security Telemetry · SOC Automation · Red/Blue Teaming · Endpoint Security · Security Research · Local AI for Cybersecurity

BEYOND THE RESUME

Building a home server lab from salvaged/scrap hardware to run and fine-tune local AI models for cybersecurity use cases. Driven to explore emerging security and AI technology hands-on, and working toward attending DEF CON and Black Hat to learn from and connect with the security research community.

EDUCATION

BVRIT Narsapur *2025 – 2029 (Expected)*
B.Tech — Computer Science & Business Systems

Gyanville Academy
Intermediate (11th–12th) · Score: 922/1000

SR Prime School
Nizamabad · 10th Grade · GPA: 9.5/10

SEEKING

Cybersecurity Intern · SOC Intern · Security Operations Intern · Detection Engineering Intern · Security Research Intern · Blue Team Intern · Security Automation Intern

Availability: Open to internship opportunities focused on gaining practical industry experience and contributing to real-world security work.