KHADER SHAREEF

+919515787655 | infa.khadershareef@gmail.com | linkedin.com | github.com/khader | Portfolio

Hyderabad, Telangana, India

PROFESSIONAL SUMMARY

Cybersecurity student with hands-on SOC experience in threat monitoring, incident response, and security operations. Proven ability to analyze security alerts using SIEM tools, triage incidents based on severity, and collaborate with teams to remediate threats. Experienced in log analysis, malware detection, and implementing security controls. Strong analytical and documentation skills with a passion for staying current with emerging cybersecurity threats and defensive strategies.

EDUCATION

Bachelor of Engineering in Cybersecurity | Expected June 2026

Nawab Shah Alam Khan College of Engineering & Technology, Osmania University

Hyderabad, Telangana | November 2022 – June 2026

RELEVANT EXPERIENCE

Cyber Security Analyst | DigiSuraksha Parhari Foundation

Gurugram, Haryana | *July 2024 – August 2024*

- Monitored security alerts and events using SIEM platforms in a SOC environment, analyzing 500+ daily alerts to identify potential security incidents and suspicious activity patterns
- Performed incident triage and prioritization based on severity assessment, ensuring critical threats were escalated and addressed within established SLA timeframes
- Conducted initial investigations of security incidents including malware infections, phishing attempts, and unauthorized access, documenting findings in incident tracking systems with detailed analysis and remediation recommendations
- Collaborated with security team members to contain and remediate threats, implementing security controls and assisting in vulnerability mitigation across organizational digital assets
- Performed root cause analysis on security incidents and contributed to the development of standard operating procedures to prevent recurrence of similar threats

LEADERSHIP EXPERIENCE

President, Cyber Elites | Osmania University

Hyderabad, Telangana | *June 2023 – Present*

- Led cybersecurity club operations, growing membership by 30% and organizing 6+ major technical events including a Capture The Flag (CTF) competition with 150+ active participants
- Mentored 70+ students in cybersecurity concepts and professional certifications, achieving an 89% pass rate for certification examinations through structured training programs

TECHNICAL PROJECTS

Home Lab: SOC Operations Environment

- Built and configured a virtualized SOC environment using Kali Linux, Ubuntu Server, and Windows 10 Pro to simulate real-world attack scenarios and defensive operations

- Deployed EDR and SIEM solutions (Splunk) to monitor network traffic, analyze packet captures, and detect security threats including brute-force attacks and suspicious login patterns

CereloX: Windows Event Log Visualization Tool

- Developed a Python-based security tool to parse and visualize Windows Event Logs for accelerated incident triage and forensic analysis
- Achieved 95% detection accuracy rate for identifying unauthorized login attempts by analyzing 15+ simulated brute-force attack patterns during testing phase

SecureWipe – Data Sanitization Tool (Smart India Hackathon)

- Designed and developed a secure data sanitization solution to permanently erase sensitive data and prevent forensic recovery, ensuring compliance with data protection standards
- Optimized wiping performance by 25% compared to standard forensic tools through implementation of multi-threaded disk I/O operations

TECHNICAL SKILLS

Security Operations: SIEM (Splunk, QRadar, Wazuh), Log Analysis, Incident Response, Security Monitoring, Alert Triage, Threat Detection, EDR, Phishing Analysis, Vulnerability Assessment

Networking & Protocols: TCP/IP, DNS, SSH, HTTP/HTTPS, Network Security, Packet Analysis (Wireshark, Zeek, Brim), Intrusion Detection (Snort, Yara)

Operating Systems: Arch Linux, Linux Servers (Ubuntu, CentOS), Windows Server 2019, Windows 10, Tails OS

Programming & Scripting: Python (Security Automation, Log Parsing), Bash Scripting, Git/GitHub, Langchain, n8n

Security Tools: Wireshark, Zeek, Brim, Snort, Yara, Splunk, QRadar, Wazuh, Kali Linux, MITRE ATT&CK Framework

TRAINING & CERTIFICATIONS

- Cisco Certified Network Associate (CCNA) – Cisco
- Certified in Cybersecurity (CC) – ISC2
- Comptia Network+ (N10-009) – United Latino
- E-LearnSecurity Junior Penetration Tester (eJPT) – INE Security
- Certified Network Security Practitioner (CNSP) – The SecOps Group
- Certified Cybersecurity Educator Professional (CCEP) – Red Team Leaders
- Certified Social Engineering Defence Practitioner (CSEDP) – The SecOps Group