SAHUKARA SATWIK

SOC ANALYST

+91-9441237511 | satwiksahukara69@gmail.com | www.linkedin.com/in/sahukara-satwik

ACADEMIC & RESEARCH PROFILE

SOC Analyst with hands-on expertise in SIEM, EDR, XDR, and cloud security monitoring. Skilled in incident response, threat hunting, and detection engineering, with proven experience in tuning detection rules, analyzing security events, and reducing false positives. Strong foundation in forensics, malware analysis, and threat intelligence with practical exposure to MITRE ATT&CK, STRIDE, and DREAD frameworks. Adept at handling client communications, generating reports, and improving overall security posture.

EDUCATION

M.Sc. Cyber Security — August, 2023 - May, 2025
National Forensic Sciences University

B.Sc. Forensic Science — January, 2020 - June, 2023
Adikavi Nannaya University

TECHNICAL SKILLS

- SIEM/XDR/EDR: Google SecOps, Sumo Logic, Wazuh, Suricata, Splunk, Elastic Stack, CrowdStrike Falcon, Microsoft Defender XDR
- Security Operations: Incident Response, Threat Hunting, Threat Intelligence, Malware Analysis, Forensics, Log Analysis
- Frameworks: MITRE ATT&CK, STRIDE, DREAD, Cyber Kill Chain
- Tools: Nessus, Nmap, Burp Suite, Wireshark, Kibana, Logstash
- Scripting & Automation: Python, Bash
- Systems: Windows, Linux (Ubuntu), Active Directory

KEY COMPETENCIES

- Security Operations & Incident Response
- Threat Hunting & Detection Engineering
- SIEM & XDR Optimization
- Cloud Security Posture Management
- Threat Intelligence & Forensics
- Security Automation & Rule Tuning

PROFESSIONAL EXPERIENCE

SOC Analyst
Tecplix Technologies

September, 2025 - Present
Bangalore

- Monitoring and securing enterprise client infrastructures using Google SecOps, Sumo Logic, CrowdStrike Falcon, and Microsoft Defender XDR, ensuring real-time threat visibility and rapid response.
- Executing in-depth alert triage and incident escalation, effectively reducing false positives and strengthening overall detection accuracy.
- Conducting targeted threat hunting operations, leveraging advanced detection rules and event correlation to proactively identify potential compromises.
- Optimizing SOC workflows through detection rule tuning, structured reporting, and refinement of incident response playbooks to enhance operational resilience.

Cyber Security Researcher
Secure Smith

October, 2023 - August, 2025
Ahmedabad

- Designed and managed honeypot environments to capture and analyze attacker methodologies, generating valuable internal threat intelligence for research purposes.
- Conducted in-depth forensic analysis of network logs and system data to map threat actor techniques to the MITRE ATT&CK framework.
- Communicated complex security findings and investigation outcomes to diverse stakeholders, providing actionable intelligence and strategic recommendations.
- Utilized Wazuh for SIEM operations to refine detection rules and improve log parsing, reducing false positives and strengthening security monitoring frameworks.

Cyber Security Intern
C3iHub, IIT Kanpur

December, 2024 - June, 2025
Kanpur

- Engineered and deployed a comprehensive Security Operations Center (SOC) environment using open-source tools (Wazuh, Suricata), creating a practical platform for hands-on learning and real-time threat detection demonstrations.
- Simulated sophisticated cyber attack scenarios to analyze system responses and fine-tune detection rules, establishing a robust framework for academic and practical instruction in behavioral analysis and log correlation.
- Developed a Telegram bot for automated security alerts, showcasing an innovative approach to enhancing communication workflows during incident response exercises.

CERTIFICATIONS

- Digital Forensic Essentials, EC-Council (Aug 2024)
- Cyber Threat Intelligence 101, arcX (Nov 2024)
- Incident Responder, Crowdstrike Falcon (Sept 2025)

ACADEMIC PROJECTS

Developing Threat Model for the Organization December, 2024 - May, 2025

- Built a threat modeling tool integrating STRIDE, DREAD, and MITRE ATT&CK for proactive threat identification and insider threat mitigation.
- Developed a Python script to automate log analysis (Suricata, Wazuh) against a JSON model for risk-prioritized threat detection.
- Implemented DREAD for quantitative risk scoring, automating threat categorization (High, Medium, Low) and prioritization.
- Designed a threat modeling process for Secure SDLC integration, embedding security throughout the system lifecycle.

Active Directory Forensics & SMB Attack Simulation February, 2024 - July, 2024

- Applied forensic techniques to collect and analyze Active Directory artifacts for security incident simulation.
- Simulated SMB Relay attacks to identify authentication flaws and proposed hardened protocols, improving domain security posture.
- Provided actionable recommendations for strengthening SMB security, emphasizing the need for enhanced authentication protocols.
- Gained practical experience in Active Directory security assessments, furthering understanding of common attack vectors and mitigation strategies

ACHIEVEMENTS

- Top Rank Holder – IIT Kanpur CTF (All India Level)
- Built and deployed live SOC dashboards with Wazuh + Suricata
- Featured contributor to C3iHub’s internal security playbook