Sarthak Mishra

India • +91 7703086808 • sarthakatwork08@gmail.com • Linkedin/shaivarth • GitHub/shaivarth • Portfolio

Specialized in SOC operations, threat detection, SIEM monitoring, and incident response, with hands-on experience in Splunk, Wireshark, Windows/Linux log analysis, and security home labs. Skilled in investigating authentication events, network traffic, and suspicious activity patterns, with a strong focus on blue-team detection and security monitoring.

TECHNICAL SKILLS

SIEM & Monitoring: Splunk, Microsoft Sentinel, Log Analysis, Event Correlation, Alert Monitoring
Threat Detection & Incident Response: Incident Triage, IOC Analysis, Threat Detection, Authentication Event Investigation, MITRE ATT&CK Framework
Networking: TCP/IP, DNS, HTTP/HTTPS, VPN, Network Traffic Analysis
Security Tools: Wireshark, Nmap, Windows Event Viewer
Operating Systems: Windows, Linux (Kali Linux, Ubuntu)
Scripting & Query Languages: Python, Bash, SQL, KQL.
Security Concepts: Privilege Escalation Detection, Phishing Analysis, Defense Evasion Techniques.

PROJECTS

SOC-X Sentinel | SIEM Simulation, Threat Detection, SOC Monitoring
- Built a real-time SOC simulation platform using Python and Flask.
- Developed telemetry and alert pipelines for suspicious activity detection.
- Designed a SIEM-style dashboard for live threat monitoring and visualization.

SIEM Setup & Log Monitoring Lab | Splunk, SIEM, Alert Monitoring
- Configured a local Splunk instance and ingested Windows/Linux logs for centralized security monitoring.
- Created Splunk queries and alerts to detect failed logins and suspicious authentication activity.
- Performed SIEM-based log correlation, alert analysis, and security event monitoring.

EXPERIENCE

Security Operations & Threat Monitoring Labs | Self-Directed Home Lab
- Performed Windows/Linux log analysis to investigate failed logins and suspicious authentication activity.
- Configured Splunk for centralized log monitoring, event correlation, and security alert generation.
- Conducted network traffic analysis using Wireshark to inspect DNS, HTTP/HTTPS, and TCP/IP activities.
- Applied MITRE ATT&CK to analyze privilege escalation, phishing, and defense evasion techniques.
- Completed hands-on TryHackMe labs covering SIEM operations, incident response, and alert triage.
- Maintained consistent hands-on cybersec practice through security labs and threat analysis experiments.

Health-Hack Hackathon (VIT Bhopal × Johns Hopkins University)
- Participated in a team-based hackathon to develop a privacy-focused mental health support platform.
- Contributed to authentication workflows, input validation, and secure handling of user data.
- Collaborated in a fast-paced development environment under strict project deadlines.

CERTIFICATIONS

- Completed THM Pre Security learning path.
- Completing TryHackMe SOC Level 1 path.
- Undergoing EC-Council CEH v13 training for the Certified Ethical Hacker certification.