Naman Soni

+91 8209451780 soninaman1021@gmail.com www.linkedin.com/in/naman-soni-soc

SKILLS

- **SIEM & Detection:**
  - Microsoft Sentinel
  - IBM QRadar
  - KQL (Kusto Query Language)
  - Log Correlation & Alert Triage
- **Endpoint & Security Monitoring:**
  - Microsoft Defender for Endpoint
  - Sysmon Log Analysis
  - IOC Identification
- **Networking:**
  - Wireshark
  - Snort
  - Basic TCP/IP & Network Protocol Analysis
- **Security Concepts:**
  - Incident Response Lifecycle
  - Phishing Analysis
  - MITRE ATT&CK (Foundational Understanding)
  - OWASP Top 10

CERTIFICATIONS

- Certified Ethical Hacker (CEH v13) – EC-Council
- KC7 – KQL Investigations
- SOC & Blue Team Labs (Hands-on Practice)
- Digital Forensics Essential
- Cybersecurity and Forensics

EDUCATION

B.Tech - Computer Science Spl. Cybersecurity and Forensics
MIT-WPU
(2021 - 2025)

Higher Secondary
Priyanka Public School
(2020 - 2021)

PROFILE

Cybersecurity graduate specializing in Security Operations with hands-on experience in SIEM monitoring, alert triage, and log correlation. Proficient in Microsoft Sentinel, Microsoft Defender, and IBM QRadar with practical exposure to KQL-based threat detection, phishing investigation, and incident documentation. Strong understanding of SOC workflows and basic threat analysis aligned with industry standards.

WORK EXPERIENCE

Teachnook India
Sep 2023 – Nov 2023

Cybersecurity Intern

- Assisted in network traffic analysis to identify abnormal patterns
- Performed basic penetration testing on web and network environments
- Supported vulnerability identification and reporting

Namanand Cyber Forensics and Research Technologies LLP
Aug 2024 – Jan 2025

Digital Forensics Intern

- Assisted in evidence acquisition and analysis during investigations
- Supported live system analysis under supervision
- Contributed to documentation and reporting activities

Opalsoft Inc.
Aug 2025 - Present

SOC Analyst Trainee

- Monitored and triaged security alerts using Microsoft Sentinel and Microsoft Defender.
- Investigated suspicious authentication attempts, process executions, and endpoint anomalies.
- Performed log correlation across endpoint, identity, and network sources to determine alert validity.
- Developed KQL queries to detect brute-force attempts, abnormal login behavior, and privilege misuse.
- Conducted phishing email analysis including header inspection, URL reputation checks, and IOC extraction.
- Documented incident findings, impact assessment, and recommended remediation actions.

PROJECTS

- Network Traffic Analyzer
- Vulnerability Scanner
- Keylogger Detection System
- Malware Analysis
- Digital Forensics Investigation with EnCase & Tableau TD3