

MEET SHAH

Cybersecurity Analyst | SOC Analyst | Incident & Log Analysis | Python & Scripting

Ahmedabad • 7778928602 • meetshah6445@gmail.com

• www.github.com/meetshah2904 • www.linkedin.com/in/meet-shah-3933a1262

SUMMARY

Entry-level SOC Analyst with strong capabilities in security event monitoring, alert triage, log analysis, and incident investigation. Hands-on experience detecting and validating threats using a Snort-based IDS and simulating attack scenarios for alert analysis. Solid understanding of TCP/IP, Linux environments, threat detection fundamentals, and SOC workflows including escalation, documentation, and response support. Skilled in Python and Bash scripting for automation and log parsing, with a detail-oriented and analytical approach to defensive security operations.

WORK EXPERIENCE

Security Admin Associate L1 | Infotact Solution

May 2025 - Jul 2025

- Built and configured a Snort-based IDS on Kali Linux to detect simulated network attacks.
- Wrote and tested custom Snort rules; minimized false positives through tuning.
- Conducted log monitoring, traffic analysis, and detection correlation.
- Simulated attacks (port scan, brute force, ping flood) using ZAP, Burp, and Nmap.
- Documented weekly security findings and presented to internal review team.

Full Stack Web Developer | Grownited Pvt. Ltd.

Jun 2023 - Apr 2024

- Developed modules for MERN-based web applications.
 - Implemented secure API handling and user authentication.
 - Improved frontend performance by optimizing React components.
-

EDUCATION

Master of Science in Cyber Security

Jun 2024 - Apr 2026

Narnarayan Shastri Institute of Technology - IFSCS Affiliated to NFSU

- Specialized in ethical hacking, digital forensics, malware analysis, cryptography, and incident response.
- Gained hands-on experience with industry-standard tools and frameworks through practical labs and simulations

Bachelor of Computer Application

Jun 2021 - Apr 2024

GLS University

- Studied core subjects including Data Structures, Operating Systems, Computer Networks, and Database Management Systems.
 - Developed skills in C, C++, Java, Python, JavaScript, PHP, and worked on web development projects using MERN/MEAN stacks.
 - Gained practical experience through academic projects and workshops, strengthening problem-solving and software development abilities.
-

PROJECT

Snort-based Network Intrusion Detection System (NIDS)

- Built IDS on Ubuntu, created custom rules, analyzed real-time alerts.
 - Performed attack simulation and documented defensive measures.
-

SKILLS

- **Technical Skills:**
 - **Languages:** C, C++, Java, Python, JavaScript, PHP
 - **Frameworks:** MERN Stack, MEAN Stack, Node.js
 - **Databases:** Oracle SQL, MongoDB, SQL Server
 - **Scripting & Automation:** Python automation scripts, Bash scripting
- **Cybersecurity Skills**
 - Incident Analysis & Log Analysis
 - Network Security (TCP/IP, Ports, Protocols)
 - IDS/IPS Concepts (Snort experience)
 - Vulnerability Assessment & Scanning
 - Ethical Hacking & Penetration Testing (Basic)
 - Malware Analysis Fundamentals
 - Web Application Security
 - Security Testing using OWASP ZAP, Burp Suite, Nmap
- **Cybersecurity Tools:**
 - Snort
 - OWASP ZAP
 - Burp Suite
 - Nmap
 - Wireshark
- **Professional Skills:**
 - Analytical Thinking
 - Problem Solving
 - Documentation & Reporting
 - Teamwork & Collaboration
- **Others:**
 - **Certifications:** C, C++, Java, Python, MERN Stack, MEAN Stack