

# Anisha Rani

## Associate Security Analyst

Cyber Security Analyst with 1.5+ years of experience in SOC operations, SIEM monitoring, incident investigation, and vulnerability assessment. Skilled in analyzing alerts, responding to threats, and working with SIEM, EDR, firewalls, and IDS/IPS. Strong foundation in networking, Windows/Linux security, MITRE ATT&CK, and basic scripting. Detail-oriented and focused on improving security posture and Comfortable working in rotational shifts , including night shifts, for 24x7 SOC operations.

✉ ranianisha456@gmail.com

📞 8851025914

📍 Delhi, India

## WORK EXPERIENCE

### Associate Security Analyst Feuji Software Technologies

10/2024 - Present

Hyderabad

#### Achievements/Tasks

- Monitored SIEM alerts and analyzed logs from networks, endpoints, and firewalls to detect suspicious activities.
- Investigated security incidents and supported containment, eradication, and recovery steps.
- Performed vulnerability scans using Nessus/OpenVAS and followed up with teams for remediation.
- Performed basic threat hunting by correlating SIEM alerts, endpoint telemetry, and network logs
- Monitored network traffic patterns to identify suspicious behavior, potential resource abuse, and early denial-of-service indicators
- Monitored health and performance of SIEM and security tools , reporting issues and assisting in alert tuning.
- Collaborated with SOC analysts to improve SOC processes, documentation, and operational efficiency.

## PERSONAL PROJECTS

### Phishing Simulation Project (07/2025 - 09/2025)

- Conducted an organization-wide phishing simulation to assess user awareness and identify high-risk behavior. Designed phishing templates, executed the campaign, tracked user responses, and prepared a report with training recommendations to improve security posture.

### CyArmorHub Project (09/2025 - 10/2025)

- Performed Web Application Penetration Testing (WAPT) for **CyArmorHub** , including agent installation testing and end-to-end security assessment of their web application. Identified vulnerabilities and provided clear remediation guidance to the development team.

## EDUCATION

### Bachelor of Technology

Rajiv Gandhi Proudlyogiki Vishwavidyalaya

08/2017 - 07/2021

#### Course

- Computer Science

## SKILLS

Incident Response

Threat Hunting

Network Security

Email Security

EDR Monitoring & Threat Detection

Network Protocols (TCP/IP)

SIEM Monitoring

IDS/IPS Basics

Log Analysis

Vulnerability Assessment

SIEM Health Monitoring

SOC Playbooks / Runbooks

Network Traffic Analysis

Threat Detection & Analysis

Penetration Testing

## TECHNICAL PROFICIENCY

### Security Domain

Cyber Security, Network Security, Endpoint Security, Email Security, Application Security, VAPT, SIEM Monitoring, Incident Response

### Tools & Platforms:

Burp Suite, Nessus, Wazuh, Microsoft Defender, Trend Micro, Checkpoint, Microsoft Sentinel (Basics), Microsoft 365 Security

### Operating Systems:

Windows, Linux (Kali, Ubuntu)

### Other Skills:

Log Analysis, Threat Detection, Vulnerability Assessment, MITRE ATT&CK (Basics), Active Directory Security, Azure Security (Basics)

### Security Operations

SIEM Monitoring (Wazuh), EDR Threat Detection, Incident Triage, IDS/IPS Monitoring, Packet Analysis (Wireshark), Network Protocol Analysis (TCP/IP, DNS, HTTP), Log Analysis & Correlation

## ORGANIZATIONS

Feuji Software Technologies