RISHIKESH

CYBER SECURITY ANALYST

CONTACT

☎ 9971107230

✉ rishikeshshahi19@gmail.com

Sector 39 ,Gurugram

SKILLS

- SIEM - Splunk
- ASOC ON(In-house SIEM tool)
- IDS/IPS
- Firewall(Checkpoint, Fortinate,Sonic)
- Webserver(Windows, Linux)
- Antivirus & EDR - Trendmicro
- NMAP
- Nessus
- Sandboxing
- Burp suite
- Metasploit
- Wireshark
- Threat Intelligence - Recorded Future
- Threat Hunting
- Velociraptor
- Manage Engine
- Cloud - Azure
- Malware Analysis
- Email Analysis
- Incident Response

PROFILE

A highly skilled cybersecurity professional with comprehensive experience working in both **Red Team** (offensive security) and **Blue Team** (defensive security) roles. Adept at identifying vulnerabilities through simulated attacks and defending systems against sophisticated threats. Proficient in penetration testing, vulnerability assessment, incident response, threat hunting, and security monitoring. Demonstrated ability to bridge the gap between proactive and reactive security measures, ensuring a holistic approach to cybersecurity. Currently providing cybersecurity services for one of **India's critical infrastructures**, playing a key role in securing vital assets. Seeking a challenging role to further enhance my expertise and support the continuous improvement of cybersecurity measures for critical systems

WORK EXPERIENCE

Ciber Digita Consultant 2022 - PRESENT

SOC Analyst L2

- Threat Hunting
- Incident Detection and Response
- Monitoring and Logging
- Develop playbooks, watchers, and dashboards within the SIEM platform to enhance monitoring capabilities.
- Proactive measures to mitigate imminent threats in accordance with Define, government advisories (CERTIN,NCIIPC). develop, and uphold SIEM correlation rules, custom documentation, and security protocols and procedures.
- Assist in developing new use case based on threat intelligence, and recommendation from cisco, improving the Soc's ability to Identifying emerging threats.
- Identify any incidents that may have been missed by Junior SOC analysts
- Compose, disseminate, and elucidate Monthly, Weekly, Quarterly Executive Reports for managed clients, focusing on enhancing their content and presentation continually.
- Comprehensive understanding of the MITRE ATT&CK framework and the Cyber Kill Chain.
- Backtracking/co-relating the threat activities for depth analysis to create an Incident Reports
- Identify security concerns, initiate customer tickets, and oversee issue

LANGUAGES

- English (Fluent)
- French (Fluent)
- German (Basic)
- Spanish (Intermediate)

INTERESTS

- Reading books
- Listening to music
- Dancing
- Travelling

Br techgeeks 2020 - 2022

Cyber Security Analyst

- Performing health check of various log sources.
- Review Analyze and close false positive Alerts.
- Ticket creation as per Alert triggered.
- Continuously monitoring the Dashboard.
- Block malicious connections on firewall.

EDUCATION

Bachelor of Technology 2016 - 2020

Lingayas university

PROFESSIONAL CERTIFICATION

- **CERTIFIED ETHICAL HACKER (CEH)**
- **CYBER SECURITY SOC ANALYST TRAINING - SPLUNK**
- **CERTIFIED CISCO - INTRODUCTION TO CYBER SECURITY**
- **CERTIFIED SOC ANALYST FOUNDATION**
- **INTRODUCTION TO THREAT HUNTING.(SECURITY BLUE TEAMS)**