RAHUL D

IT Security Analyst | Cybersecurity Expertise | Threat Detection | Incident Response

9648290341 **rahuld9648@gmail.com** **LINKEDIN**
Address: - B-118 Bechraji Mehsana Gujarat

SUMMARY

I am a proactive and detail-oriented IT professional with expertise in cybersecurity and technical support. My skills include threat detection, incident response, and penetration testing. I am proficient in tools like SIEM and firewalls, and I am passionate about safeguarding systems and driving continuous improvement against cyber threats. I hold certifications in cloud computing, hacking, and network protocol analysis, showcasing my commitment to the field

EXPERIENCE

SOC Analyst

Progression Infonet Pvt. LTD

08/2025 - Present TDSG site location

A company specializing in IT services and cybersecurity solutions

- Monitored network traffic with SIEM tools to detect and mitigate security threats
- Investigated alerts and performed root cause analysis to minimize incident impact and prevent recurrence
- Created incident response reports and maintained comprehensive threat intelligence documentation
- Conducted vulnerability assessment and penetration testing (VAPT) using Nessus, Nmap, Burp Suite, and Kali Linux
- Monitored and analyzed firewall logs and security events on Palo Alto and FortiGate devices
- Configured and monitored Zscaler for secure web gateway and endpoint security management
- Enforced security policies, implemented access controls, and monitored endpoint protection systems
- Collaborated with IT teams to perform regular security audits and system hardening
- Provided employee training on phishing detection, social engineering risks, and security best practices
- Implemented Multi-Factor Authentication (MFA) and identity access management solutions

Cybersecurity Analyst

ITPL (Informatics Technologies Pvt. Ltd.)

03/2024 - 07/2025 TDSG site location

An IT service provider specializing in cybersecurity

- Monitored network traffic with SIEM tools to detect and mitigate security threats
- Investigated alerts and performed root cause analysis to minimize incident impact and prevent recurrence
- Created incident response reports and maintained comprehensive threat intelligence documentation
- Conducted vulnerability assessment and penetration testing (VAPT) using Nessus, Nmap, Burp Suite, and Kali Linux
- Monitored and analyzed firewall logs and security events on Palo Alto and FortiGate devices
- Configured and monitored Zscaler for secure web gateway and endpoint security management
- Enforced security policies, implemented access controls, and monitored endpoint protection systems
- Collaborated with IT teams to perform regular security audits and system hardening
- Provided employee training on phishing detection, social engineering risks, and
- Implemented MFA and Identity access management solution

Security Analyst

Microsense Network Pvt. Ltd 05/2023 - 02/2024

A company providing technical support and network solutions

- Provided first-level support for security and IT issues (password resets, account lockouts, VPN access, basic network troubleshooting)
- Monitored user activity and system alerts in SIEM dashboards, escalating suspicious incidents to senior SOC analysts
- Assisted in handling phishing reports and malware alerts, guiding users on safe practices
- Documented tickets, incidents, and resolutions in the help desk system for compliance and reporting
- Supported endpoint security tasks such as antivirus updates, patching, and basic hardening under supervision
- Helped with onboarding/off boarding users, ensuring access rights were aligned with security policies

EDUCATION

BCA

Mahatma Gandhi Kashi Vidyapith

08/2019 - 05/2022

Intermediate

Lorven IND PU College

08/2017 - 05/2019

High School

Priyadarshini Public High School

08/2015 - 05/2017

CERTIFICATION

- **JK-MCC 2023**
  Jetking Master in Cloud computing with the N+, CCNA, REDHAT, MCSA & AW
- **Deep Dive into Hacking and Pen testing –2022**
  EC- Council certified hacking and pen testing.
- **Wireshark (Network Protocol Analysis) – 2022**
  EC- Council certified wireshark.
- **Cyber Attacks and Defence Strategies – 2022**
  Common Cyber security attack and strategies from the EC-Council.
- **Vulnerabilities Analysis and Management – 2022**
  EC- Council VA management and patching

SKILLS

- ✓ Burp Suite
- ✓ Cybersecurity
- ✓ Kali
- ✓ Linux
- ✓ Metasploit
- ✓ Microsoft Office
- ✓ Nessus
- ✓ Nmap
- ✓ Pen testing
- ✓ Siem
- ✓ Symantec
- ✓ Wireshark
- ✓ Windows 10
- ✓ Microsoft Office 365
- ✓ Kali Linux
- ✓ Splunk
- ✓ Accenture MxDR
- ✓ CrowdStrike
- ✓ Zscaler
- ✓ VAPT

ADDITIONAL SKILLS

- ✓ Office 365 Admin & Configuration
- ✓ Active Directory & User Management
- ✓ Knowledge of MIME structure and email forensics tools (e.g., MXToolbox, VirusTotal, PhishTool)
- ✓ Experience with antivirus and spam filtering systems
- ✓ Hardware/Network Troubleshooting
- ✓ Documentation & Ticketing Management

- ✓ Email header analysis (SPF, DKIM, DMARC verification)

SOFT SKILLS

- ✓ Critical Thinking, Problem-Solving
- ✓ Written & Verbal Communication
- ✓ Attention to Detail, Time Management
- ✓ Multi-tasking, Team Collaboration

Project

https://github.com/snifer96/Splunk-implantation-SUF.git
https://github.com/snifer96/my-portfolio.git

Date: - 15/09/2025
(RAHUL D)