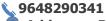


rity Analyst | Cybersecurity Expertise | Threat Detection | Incident Response



<u>rahuld9648@gmail.com</u> <u>■</u> 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

Security Engineer

Progression Infonet Pvt. LTD

iii 08/2025 - Present

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) across web applications, networks, and endpoints using tools like Nessus, Nmap, Burp Suite, Metasploit, and Kali Linux
- > Monitored and analyzed firewall logs and security events on Palo Alto and FortiGate devices
- > Performed internal and external penetration testing, including reconnaissance, enumeration, exploitation,
- > Investigate the Advisory received from the vendors and other third parties check it's applicable to our organization or not by doing the practical check using Linux machine
- > Enforced security policies, implemented access controls, and monitored endpoint protection systems
- > Check the alerts and investigate them received from the Crowd Strike Falcon.
- > Conducted **post-exploitation and privilege escalation assessments** to determine real-world attack impact.
- > Collaborated with IT teams to perform regular security audits and system hardening
- > Implemented Multi-Factor Authentication (MFA) and identity access management solutions
- > Created detailed **VAPT and remediation reports** with CVSS-based severity ratings and mitigation recommendations.

Cybersecurity Analyst

ITPL (Informatics Technologies Pvt. Ltd.)

iii 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
- > Monitored Zscaler and provide the Alerts report for the 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.
- > Check the IAM and provide the report and analyze for the best and least Access

Security Analyst

Microsense Network Pvt. Ltd 曲 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

亩 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✓ Wireshark

✓ Kali ✓ Windows 10

✓ Linux
✓ Microsoft Office 365

✓ Metasploit ✓ Kali Linux ✓ Microsoft Office ✓ Splunk

✓ Nessus
 ✓ Accenture MxDR
 ✓ Nmap
 ✓ CrowdStrike
 ✓ Pen testing
 ✓ Zscaler

✓ Siem ✓ 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
- ✓ Documentation
- ✓ Email header analysis (SPF, DKIM, DMARC verification)
- ✓ **Reporting & Frameworks:** CVSS, OWASP, PTES, NIST 800-115

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)