Rahul **Jha**

SOC Analyst | Network Security Engineer | Cyber Security Professional

New Delhi, INDIA 110062

(+91) 9318375640 | rahuljha12122@gmail.com | linkedin.com/in/raahul-jha

SUMMARY

SOC and Network Security professional with hands-on experience in Fortinet FortiGate 100F SD-WAN, Arista SDN, Proxmox virtualization, and Trellix endpoint security. Skilled in SOC monitoring, log analysis, incident response, DDoS and malware detection, and enterprise network security operations. Strong L1–L3 background in network troubleshooting, system administration, firewall management, Active Directory, VPN/security tools, and SLA-driven service delivery, with proven ability to manage on-site IT environments, coordinate escalations, and support enterprise infrastructure optimization.

EDUCATION

Tilak Maharashtra Vidyapeeth Pune, India

BCA (Bachelor of Computer Applications) July. 2022 - July 2025

V.C.S.G.S.B.V Saket, New Delhi

Equivalent Apr 2019 – May 2019

WORK EXPERIENCE

NSN COMPUTERS

New Delhi, India

IT EXECUTIVE / NETWORK & SYSTEMS SUPPORT (L2–L3) Sept. 2023 - Mar. 2025

- Provided on-site L2/L3 support for hardware, OS, network, and security infrastructure, resolving complex incidents escalated by the L1 team.
- Reduced server downtime by 20% through performance monitoring and optimization of Windows Server instances.
- Designed and maintained Active Directory architecture, including PDC, ADC, CDC, and RODC, strengthening organizational security.
- Network Administration, Active Directory structure, and firewall operations, ensuring minimum downtime and strong security posture.
- Maintained technical documentation, network diagrams, AD configurations, and firewall rule change logs for internal audits and compliance.
- Conducted vulnerability assessments, identifying misconfigurations, weak credentials, and outdated software.
- Delivered user support, orientation, and technical training on system usage, security awareness, and troubleshooting.

IND INNOVATION

Gurgaon, India

TECH SUPPORT ENGINEER Apr,2025 - Jun. 2025

- Deployed and configured laptops, joined systems to Active Directory domains, and maintained user profiles and permissions via Group Policy.
- Administered Active Directory accounts, password resets, and access control, enhancing enterprise identity and access management.
- Configured and supported secure remote connectivity through Cisco AnyConnect VPN and Zscaler, strengthening endpoint security.
- Supported LAN/WLAN operations including installation, configuration, and troubleshooting of routers, access points, and user connectivity issues.
- Acted as the primary on-site technical point of contact for all desktop, network, and infrastructure issues, delivering end-to-end L1–L3 support.
- Implemented security updates and patches on endpoint devices, reducing vulnerabilities and exposure to exploits.
- Collaborated with the information security team to enforce endpoint antivirus, encryption, and data loss prevention tools.
- Performed regular system maintenance, including OS updates, security patches, endpoint protection tuning, and backup verification.
- Managed Fortigate firewall and monitoring performance.
- Optimized Symantec DLP policies, decreasing false positive incident alerts by 25% while maintaining strict data compliance and coordinated the local desktop support team, assigning tickets, mentoring junior engineers, and ensuring SLA-based issue resolution.
- Collaborated directly with client stakeholders and off-site engineers to ensure smooth operations, escalation handling, and proactive issue prevention.

CONCENTRIX

Gurgaon, India

SENIOR REPRESENTATIVE – OPERATIONS

Jun. 2025 - present

- Managed Fortinet FortiGate 100F Firewall with SD-WAN, including security policies, routing, VPNs, traffic shaping, and high-availability network optimization.
- Administered Arista SDN infrastructure, supporting enterprise switching, network automation, monitoring, and performance troubleshooting.
- Created, monitored, and analyzed firewall and security logs to detect cyber threats, DDoS attacks, malware activity, suspicious sessions, and bandwidth anomalies.
- Performed SOC-level monitoring and incident response, including alert triage, investigation, escalation, and root-cause analysis.
- Deployed and managed virtual machines using Proxmox VE, handling resource allocation, backups, and performance monitoring in virtualized environments.
- Managed endpoint security using Trellix, enforcing malware protection policies, threat prevention, and endpoint compliance.
- Conducted continuous network and security monitoring to improve system availability, performance, and security posture.
- Documented incidents, configurations, and procedures to support audits, compliance, and operational efficiency.

SKILLS

Security: Nmap, Metasploitable, Wireshark, Burp suite, Hydra, Wifite, John the Ripper, NESSUS, BeEF, etc

DevOps: AWS, Linux, GitHub,

Speaking Languages: English, Hindi

Security & Compliance: Vulnerability assessment, penetration testing, incident response, risk mitigation, regulatory.

Networking & Infrastructure: Fortinet FortiGate, FortiGate 100F, SD-WAN, Firewall Policies, VPN, Routing, Switching, LAN/WAN, Bandwidth & Session Analysis, Cisco Meraki.

Monitoring & Tools: Metasploit, Wireshark, Nmap, Beef, Zoho Ticketing System, Cisco Meraki Dashboard.

Remote Connectivity & Endpoint Security: Cisco AnyConnect VPN, Zscaler, Trellix, endpoint hardening.

SECURITY COMPETITIONS

CTF (capture the flags) Player

India

CTF PLAYER IN (HACKTHEBOX & TRYHACKME)

May. 2025 - Present

- CTFs are the competitions organized to hone and test the proficiency and expertise of information security professionals.
- Players use real hacking tools to break into the system, detect vulnerabilities, and exploit them to capture an encoded string.

ACHIEVEMENTS

CERTIFICATES

Certified Ethical Hacker (CEH) | Cisco | *2025*
Introduction to Penetration Testing | Security Blue Team| 2025
Introduction to Dark Web Operations | Security Blue Team | 2024
Introduction to Digital Forensics | Security Blue Team | 2024
Introduction to Network Analysis | Security Blue Team | 2024
Introduction to OSINT | Security Blue Team | 2024
Introduction to Vulnerability Management | Security Blue Team | 2024
AWS Knowledge: Cloud Essentials | AWS | 2024
Network defense | Cisco | 2024
Introduction to Critical Infrastructure Protection Certificate | OPSWAT | 2024
Cyber Security Internship Certificate | GPCSSI | 2023