Aishwarya Rath

Security Analyst

✉ aish121rath@outlook.com ☎ +91-9337278811 📍 Bengaluru

linkedin.com/in/aishwarya-rath-analyst

PROFILE

Cybersecurity professional with 6+ years of experience in network administration and security operations, specializing in vulnerability management, incident response, and endpoint protection. Skilled in tools like CrowdStrike Falcon, Microsoft Defender, Rapid7, and ServiceNow for monitoring, remediation, and compliance. Proven ability to analyze threats, validate incidents, and enhance security posture across global environments. Strong collaborator with expertise in network security, EDR, and Power BI reporting.

PROFESSIONAL EXPERIENCE

Security Analyst 05/2022 – present

Tata Consultancy Services (TCS)

- Led end-to-end vulnerability and endpoint security operations across enterprise environments using Microsoft Defender for Endpoint, CrowdStrike Falcon, and Rapid7 InsightVM.
- Implemented and optimized endpoint protection and anti-malware solutions, ensuring complete coverage and real-time detection across hybrid infrastructure.
- Developed and enforced endpoint security policies and device compliance rules via Microsoft Intune and Defender portal, ensuring alignment with ISO 27001 and SOC2 standards.
- Monitored, analyzed, and triaged events and Indicators of Compromise (IOCs) through Defender and Falcon dashboards, improving incident containment efficiency.
- Conducted vulnerability assessments using Qualys and Rapid7, integrating Kenna Security risk scoring for accurate prioritization and faster remediation.
- Oversaw security compliance validation and audit readiness by documenting procedures, performing patch verification, and maintaining response plans.
- Collaborated with SOC, infrastructure, and DevOps teams to secure Azure-hosted applications and cloud configurations, improving posture through continuous risk assessments.
- Created and maintained Power BI and ServiceNow dashboards to provide executive-level visibility into vulnerability, endpoint, and incident metrics.
- Ensured rapid response to zero-day vulnerabilities, driving remediation and reporting to stakeholders within tight SLAs.
- Mentored junior team members on vulnerability management and endpoint protection best practices, fostering a proactive security culture.

NOC Analyst 12/2021 – 05/2022

NTT Data

- Provided 24x7 operational support for complex enterprise IT and network environments, ensuring consistent uptime, performance monitoring, and issue resolution.
- Monitored network, server, and system health using tools such as SolarWinds, detecting latency, downtime, and utilization issues across LAN/WAN and VPN infrastructures.
- Performed proactive and reactive troubleshooting of network devices, including routers, switches, firewalls, and VPN and DHCP servers, ensuring timely resolution of incidents.
- Maintained and supported public-facing production environments with high availability requirements, adhering to SLAs and minimizing business impact during outages.
- Replaced and configured network hardware and components as part of preventive and corrective maintenance tasks.
- Documented all technical activities and customer interactions in the CRM/ticketing system to maintain service transparency and meet compliance standards.

- Ensured customer satisfaction through clear communication, incident updates, and post-resolution follow-ups, maintaining a high-quality support experience.

Network Admin 02/2019 – 12/2021

CSS CORP

- Monitored network health status in real-time using monitoring tools and responded promptly to alerts, outages, and anomalies across enterprise infrastructure.
- Investigated and resolved Tier 1 escalations, analyzing root cause of network-related incidents such as intermittent connectivity, latency issues, and low-speed complaints within defined SLAs.
- Handled high-priority escalations and resolved complex network issues, coordinating with internal teams and network operations staff to ensure service continuity.
- Diagnosed and escalated carrier-side issues to ISPs such as Verizon, CenturyLink, and AT&T, ensuring timely resolution of WAN and external connectivity problems.
- Performed in-depth troubleshooting of routers, switches, and firewalls, documenting findings and recommending preventive measures to reduce repeat incidents.
- Collaborated with cross-functional teams to optimize network performance and conducted root cause analysis (RCA) for recurring incidents.
- Maintained detailed documentation of all activities in ticketing and CRM systems, ensuring visibility, accountability, and SLA adherence.

EDUCATION

BTech in Computer Science Engineering 2014 – 2018

Biju Patnaik University of Technology Odisha

SKILLS

- Vulnerability Management: Qualys, Rapid7 InsightVM
- EDR/XDR: CrowdStrike Falcon, Microsoft Defender for Endpoint
- Risk Scoring: Kenna Security
- Remediation Workflow: ServiceNow
- Security Reporting: MicroStrategy, Power BI (partial), Excel
- CVE Analysis, False Positive Validation
- Core Security & SOC: Vulnerability Management, Threat Hunting, Incident Response, CVE Analysis
- Networking Protocols: DNS, HTTP, TCP/IP Suite Web Application Security (OWASP Top 10)
- DDoS, Web Application, and Bot Attack Mitigation
- Communication, Briefing, Stakeholder Alignment