Sarang Sujeesh

Security Analyst

sarangsujeesh@gmail.com 9188001180 Bangalore , India linkedin.com/in/sarangsujeesh

Profile

Dedicated Cybersecurity Professional with over 2 years of experience in network security, server management, and incident response. Proficient in utilizing SIEM tools (Splunk, QRadar, Sentinel), vulnerability assessment tools (Nessus, Nmap), and endpoint protection solutions. Seeking to leverage hands-on experience in security hardening, cloud security, and threat management to contribute to a dynamic Security Analyst role. Currently pursuing an MSc in Cyber Forensics and Information Security to deepen expertise and stay ahead in the field.

Education

MSc Cyber Forensics & Information Security 04/2024 – present
Madras University Distance Education

BSc Computer Science 06/2018 – 04/2021
Kannur University

Professional Experience

ShopSky Store Pvt Ltd (Contract - NewSpace India Limited) 05/2023 – present
Network Administrator / Security Bangalore

- Enhanced Server Security: Strengthened security protocols for Windows and Linux servers, reducing vulnerability incidents by 30%. Managed Active Directory and Windows Server environments, ensuring data privacy and integrity.
- Network Security Management: Deployed and maintained firewalls and IDS, utilizing Splunk, QRadar, and Microsoft Sentinel for real-time threat detection and log management.
- Threat Detection and Response: Leveraged Splunk, QRadar, and Sentinel for dynamic threat analysis and vulnerability assessments. Configured Wazuh and the ELK Stack for improved log management and security monitoring.
- Endpoint Protection: Implemented and managed EDR solutions to safeguard endpoints against emerging threats.
- Security Audits and Policy Development: Conducted comprehensive security assessments, identified vulnerabilities, and developed robust policies to align with industry standards and regulations.
- Email and Security Appliance Configuration: Configured email servers and security appliances, enforcing anti-phishing and anti-malware measures.
- Interdisciplinary Collaboration: Worked with cross-functional teams to resolve network and system issues promptly, minimizing downtime and enhancing system reliability.

AIMLEAP 05/2022 – 05/2023

IT Admin Executive Bangalore

- Secured IT Infrastructure: Implemented and maintained security measures to protect IT systems and ensure operational integrity.
- Cloud and Hosting Security: Managed cloud and hosting assets with a focus on secure configurations and compliance.
- System Monitoring: Monitored system performance and addressed issues promptly to prevent downtime and mitigate security risks.
- Account Management: Configured and managed accounts and instances, adhering to security best practices.
- Employee Training: Conducted security training sessions, increasing staff awareness and adherence to security policies by 30%.
- Incident Response: Troubleshot and resolved system outages and security concerns efficiently.
- Technical Skills: Proficient in securing Windows 10, 11, Windows Server 2016, 2022, and Linux environments.

Languages

English ● Malayalam ● Hindi ● Tamil

Skills

Network Security: Firewalls, IDS/IPS

Risk & Vulnerability Assessment

SIEM: Splunk, Qradar, Sentinel

Firewall Administration: Sophos, Fortigate

CompTIA Security+

Threat Intelligence

Penetration Testing

Identity and Access Management (IAM)

Endpoint Security & EDR

Cloud Solution (AWS)

Active Directory Management

Linux System Administration

Incident Response Planning

System Administration Proficiency: Windows & Redhat (RHEL)

Network Traffic Analysis

Projects

1. Vulnerability Management Project:

- **Description:** Led a project to identify and address security vulnerabilities in IT infrastructure.
- **Impact:** Conducted scans using Nessus,Wazuh (Vulnerabiltiy Check) and Nmap, identified critical vulnerabilities, and implemented patching strategies. Reduced the number of high-severity vulnerabilities by and improved overall security posture.

2. Security Hardening Initiative:

- **Description:** Implemented advanced security measures to enhance network defenses.
- **Impact:** Configured port security, MAC binding, captive portal, and explicit proxy, resulting in a major improvement in network security and access control.