

Rohit Wagh

Senior Security Analyst (L2)

+91 7276999464

rohitwagh4145@gmail.com

www.linkedin.com/in/rpwagh

Profile

Senior Security Analyst (L2) with 3.9 years of proven experience in protecting IT systems and infrastructure. Expertise in **Endpoint Security** solutions such as **Microsoft Defender EDR, XDR, Intune** and **Trellix Endpoint Security (AV)**. Proficient in safeguarding data through Microsoft Purview DLP and Trellix FRP. Strong problem-solving and communication skills with the ability to **deliver successful projects**.

Professional Experience

Infosys Limited

Mar 2022 – Present

Senior Systems Engineer (Security Analyst L2)

Pune, In

- Microsoft Defender EDR, XDR, Microsoft Intune, Trellix ENS, Trellix FRP, Virus Total, Microsoft Purview DLP, ServiceNow ITSM

Hindustan Aeronautics Limited

Sep 2021 – Mar 2022

GAT - Endpoint Security Admin (L1)

Nasik, In

- Trellix (formerly McAfee) Endpoint Security (AV), Trellix Data Loss Prevention, In-house ITSM Software

Projects

Client - A Global Leader in Automotive Industry

Domain - Endpoint Security

- Conducted regular ePO health checks, ensuring **100% system compliance** and optimal endpoint protection.
- Monitored and resolved alerts and incident queues in Microsoft Defender resolving issues promptly.
- Deployed, managed and troubleshoot **Trellix ENS/VSE/FRP (formerly McAfee)** components for 40,000+ endpoints.
- **Implemented change management processes** for testing, onboarding and deploying AV products as well as creating exclusion policies.
- Monitor, detect and respond to phishing attacks targeting users and systems and take remedial actions to avoid future incidents.
- Prepared and maintained **IIDs, KBs, SOPs and technical documents** to support process improvement based on client requirements.
- Coordinated with stakeholders (Infra, Service Desk and Support teams) to manage, resolve and escalate incidents efficiently.
- Generated and delivered **weekly and monthly performance analysis metrics** reports to client leadership, contributing to strategic decision-making.
- Worked as a shared resource across multiple global projects, ensuring seamless security operations and compliance.

Client - A Global Leader in Automotive Industry

Domain - Data Loss Prevention

- Configured and optimized Microsoft Purview DLP to effectively **monitor, detect and prevent data leaks**.
- Implemented and managed **DLP policies**; monitored and investigated **DLP alerts**.

Client - A Leader in the Indian Aerospace and Defence Industry

Domain - Endpoint Security

- **Administered, managed and troubleshoot antivirus infrastructures** including Trellix Agent, VirusScan Enterprise and DLP for 10000+ systems.
- Delivered **end-to-end support for antivirus solutions** and updated virus definitions.
- **Manual and scheduled deployment** of Trellix endpoint products to all the systems and servers in the infrastructure.

Technical Skills

Cybersecurity – IT, Operations, Incident Response, Phishing Email Analysis and Investigation

Endpoint Security - Trellix ePO, Trellix ENS, Microsoft Defender (EDR/XDR), Microsoft Intune

Data Privacy & Protection - Trellix File and Removable Media Protection, Trellix DLP, Microsoft Purview DLP

IT Service Management (ITSM): ServiceNow ITSM, Solve ITSM, Jira

Tools and Technologies – Virus Total, MX Toolbox, Microsoft Office Suite (Excel, Word, PowerPoint)

Soft Skills – Active Team Player, Good Communication, Presentation skills, Knowledge Transfer (KT) Delivery

Education

B.E. in Ele and Tele Engg,

Aug 2016 – Oct 2020

Shri Sant Gajanan Maharaj College of Engineering, Shegaon.

Certifications and Awards

CompTIA Security+ | SC-900 | MS-900 | SC-400 | Trellix Endpoint Security

Purdue ACE – Hi | Purdue ACE – Specialist | Purdue ACE - Malware & Threat Hunting

AZ-900 | AWS Cloud Practitioner | Google Cloud Digital Leader

Awards

C-LIFE Champion (Client Value) by Infosys Limited | Mar 2024

Insta Award (EPS Contribution) by Infosys Limited | Nov 2024