Ravi Sarode

Tactical Threat Analyst (MDR) • FortiEDR • Detection engineering

linkedin.com/in/ravi-sarode github.com/ravisarode s.ravi.sarode@gmail.com Bangalore

EXPERIENCE

Fortinet *May 2023 – Present*

Tactical Threat Analyst 2 (MDR) *Managed Detection and Response (MDR) • FortiEDR • Monitoring • Threat hunting • Incident response*

- Tactical Threat Analyst on the MDR team protecting premium clients from advanced threats; 24/7 monitoring with FortiEDR.
- Triage alerts to separate true threats from false positives; proactive threat hunting for hidden malicious activity.
- Investigate incidents (scope, root cause, impact); rapid IR including endpoint isolation, mitigation, remediation, and forensic support.
- Apply threat intelligence to emerging TTPs.

LTI Mindtree *Apr 2021 – Apr 2023*

Security Researcher *Microsoft Defender for Endpoint • Threat detection • MITRE ATT&CK*

- Improved enterprise EDR coverage via telemetry analysis and TP/FP classification—less alert fatigue, higher trust in detections.
- Emulated APT-style behaviors to validate detections and map gaps to MITRE ATT&CK.
- Authored suppression and tuning logic for noisy detectors; supported customer escalations with evidence-backed remediation guidance.
- Full research lifecycle for Defender for Endpoint from idea to field-validated detection.

ENH iSecure *Feb 2020 – Oct 2020*

Technical Trainee *Cybersecurity fundamentals • Networking • IAM • Scripting*

- Hands-on fundamentals: networking (protocols, ports, IETF standards), IAM concepts, scripting, and small web projects.

PROJECT

AI-Driven Endpoint Detection & Response (RAG) *Sysmon • AWS (Lambda, API Gateway, DynamoDB, S3) • Amazon Bedrock • React dashboard*

- AI-powered EDR correlating endpoint telemetry; RAG for analyst-ready triage, MITRE-aligned summaries, and faster investigation.
- Documentation: document.ravisarode.com

SKILLS

Security FortiEDR, Microsoft Defender for Endpoint, telemetry & tuning, threat hunting, MITRE ATT&CK, emulation, TP/FP analysis, OWASP-style web assessments.

Cloud / platform AWS, Kubernetes/EKS (workload security, growing depth), TCP/IP, segmentation, troubleshooting.

Build / automate Python (automation, analysis), JavaScript, HTML, CSS; Solidity coursework.

EDUCATION

M.Tech *Jun 2023 – May 2026 (current)*
IIIT Kottayam

Blockchain PG Certification *Aug 2022 – Jan 2023*
JNTU Hyderabad

Bachelor of Technology *2016 – 2020*
Annamacharya Institute of Technology and Science

CERTIFICATIONS AND COURSES

FortiEDR Administrator (Fortinet) — Credly badge
ICS/OT Cybersecurity Essentials — certificate (Google Drive)
SOC Level 1 — TryHackMe profile

Courses: Certified Ethical Hacker; Cisco Certified Network Associate; Web Application Penetration testing.

VOLUNTEER

BSides Bangalore

The Art of Living