Completed: Introduction to EDR – TryHackMe

I've successfully completed the Introduction to EDR room on TryHackMe, where I gained practical knowledge about how Endpoint Detection and Response (EDR) solutions protect organizations from modern cyber threats.

Key Learnings:-

1) Understanding what EDR (Endpoint Detection & Response) is and how it differs from traditional antivirus
2) How EDR monitors endpoint activities in real time
3) Detecting malicious behaviors such as:-
Suspicious process execution
Privilege escalation
Lateral movement
Persistence techniques

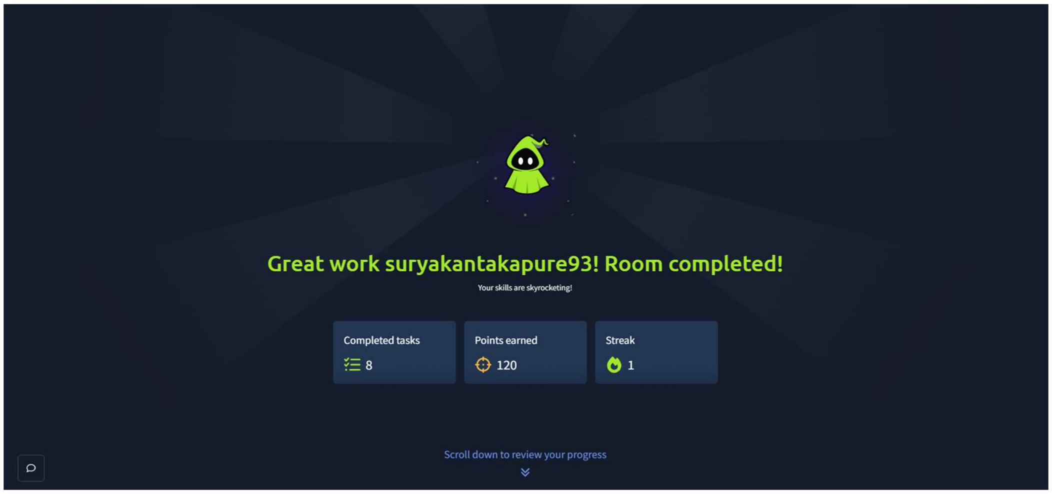
Importance of:-

1) Telemetry collection
2) Behavioral analysis
3) Threat hunting
4) Incident response workflows

Tools & Concepts Covered:-

1) Log analysis
2) Alert triage
3) Endpoint visibility
4) MITRE ATT&CK framework mapping

This room strengthened my understanding of how SOC analysts investigate alerts and respond to endpoint-based threats effectively.



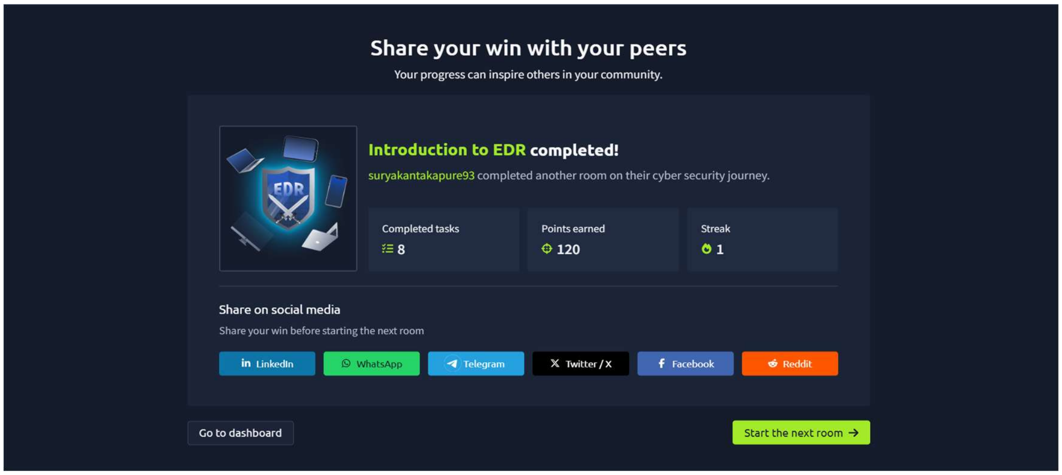
Great work suryakantakapure93! Room completed!

Your skills are skyrocketing!

Completed tasks 8

Points earned 120

Streak 1



Share your win with your peers

Your progress can inspire others in your community.

Introduction to EDR completed!

suryakantakapure93 completed another room on their cyber security journey.

Completed tasks 8

Points earned 120

Streak 1

Share on social media

Share your win before starting the next room