

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.



A screen encouraging users to share their achievement. The title "Share your win with your peers" is at the top, followed by the message "Your progress can inspire others in your community." A decorative icon featuring a shield with "EDR" and various devices like a laptop, smartphone, and tablet is shown. Below this, the text "Introduction to EDR completed!" is displayed, followed by the message "suryakantakpure93 completed another room on their cyber security journey." Three dark blue rectangular boxes show statistics: "Completed tasks" (8), "Points earned" (120), and "Streak" (1). Below these, a section titled "Share on social media" with the sub-instruction "Share your win before starting the next room" includes buttons for LinkedIn, WhatsApp, Telegram, Twitter/X, Facebook, and Reddit. At the bottom, two buttons are visible: "Go to dashboard" on the left and "Start the next room →" on the right.