Intro to endpoint security

Task 2

Question: What is the normal parent process of services.exe?

Answer: wininit.exe

Question: What is the name of the network utility tool introduced in this task?

Answer: TCPView

Task 3

Question: Where do the Windows Event logs (.evtx files) typically reside?

Answer: C:\Windows\System32\winevt\Logs

Question: Provide the command used to enter OSQuery CLI.

Answer: osqueryi

Question: What does EDR mean? Provide the answer in lowercase.

Answer: endpoint detection and response

Task 4

Question: Provide the flag for the simulated investigation activity.

Answer: THM{3ndp01nt_s3cur1ty!}

Explanation:

- find the malicious process -> beacon.exe
- find the malicious network -> beacon.exe
- copy the malicious ip from the notes and search for machines.
- Remediate all devices
- find the flag in the txt file on the desktop

The tasks, questions or answers not mentioned here means there were no answers needed.