Introduction to Endpoint Security

Question: Investigating a suspicious activity detected on a workstation owned by one of your colleagues.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

This gives a list of process running on the system.

A screenshot of a computer

Description automatically generated

By cross-verifying the Baselined processes docx we understand the beacon.exe is a malicious process running on the system.

A screenshot of a computer

Description automatically generated

Analyzing it further we able to find the process ID- 6823, remote address-59.23.48.195 remote port:4444 belongs to malicious process beacon.exe

A screenshot of a computer

Description automatically generated

By remediating it we can stop the malicious activity

A screenshot of a computer

Description automatically generated