

# 1.0 Incident Description

The SOC Team received an escalation from the IT Department regarding a workstation user experiencing severe performance issues. The user reported that his laptop became extremely slow, making it hard to work. He couldn't specify any unusual activity, mentioning that he was only browsing the web and working on documents when the slowdown occurred. Rebooting the system did not improve the situation.

Upon investigation, the IT Team found that the CPU usage was abnormally high, even with no active applications running. Suspecting a potential incident, the matter was escalated to the SOC Team.

Further analysis by the SOC Team showed no alerts triggered in the SIEM or EDR platforms. However, there was a critical anomaly: repeated outbound connections detected on the perimeter firewall originating from the user's IP address. These connections were happening every second, targeting the same destination IP address, and were not blocked by the firewall. The user was unaware of these outbound connection attempts.

This led to the case being escalated to the Incident Response (IR) Team for deeper investigation.

tryhackme.com/room/incidentresponseprocess

Room completed (100%)

### Scenario

In our scenario, we are acting as members of our Incident Response Team. A member of the organisation's SOC Team has called us to investigate and remedy a potential incident impacting a Windows workstation.

This is how the SOC Team has engaged us:

The user contacted the IT Team, reporting that his laptop started acting up and became extremely slow, to the point that he was having trouble working. The user couldn't pinpoint exactly what he was doing when the computer suddenly slowed down. He was browsing the web and working on some documents, as usual. He tried rebooting the machine, but performance was still very low.

IT has checked the machine's resources and found that the CPU usage is unusually high, even after closing all running apps. Suspecting a potential incident, IT has escalated the ticket to the SOC Team.

The SOC Team has verified that no alert was raised on the SIEM or EDR platforms for the workstation. The only anomaly that we have identified is some outbound connections on the perimeter firewall originating from the workstation's IP. The connections occur every second, and all have the same destination IP. The connections are not blocked by the FW. We have gone back to the user, who doesn't acknowledge these connection attempts.

Escalating to the IR Team.

For the scope of this room, we're assuming that all the pre-response steps have been correctly employed and that proper backups have been created before starting our investigation in order to preserve any evidence. We're also assuming that we're working in a safe environment, detached from our organisational network, to prevent the spreading of malicious artefacts within the organisation.