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.