Post-Incident Metrics Summary

The SOC metrics calculated for this mock incident provide a clear picture of security performance. The **Mean Time To Detect (MTTD) was 2 hours**, marking the time it took the team to identify the phishing attack after initial compromise. This is a critical metric for early intervention.
The **Mean Time To Respond (MTTR) was 4 hours**, which is the duration needed for the SOC team to contain the threat, fully eradicate the malware, and restore affected systems. The total time the threat was active within the environment, the **Dwell Time**, was **6 hours** (MTTD+MTTR).

To minimize future damage, efforts must focus on two areas:

1. **Reducing MTTD** through better threat intelligence and automated detection tools.
2. **Reducing MTTR** by streamlining the playbook for phishing response to achieve faster containment and recovery. The MTTR currently being twice the MTTD indicates that the response efficiency is the primary area for improvement.