Post-Incident Analysis

The SOC metrics calculated for this mock phishing incident provide a structured assessment of detection and response performance. The **Mean Time To Detect (MTTD)** was **2 hours**, representing the time required for the SOC team to identify the phishing attack after the initial compromise. Timely detection is essential to reduce attacker dwell time and limit potential damage.

The **Mean Time To Respond (MTTR)** was **4 hours**, reflecting the time required to contain the threat, reset compromised credentials, block malicious indicators, and restore affected systems. Effective response execution plays a critical role in minimizing operational disruption and preventing lateral movement.

1. **Reducing MTTD** by enhancing email security monitoring, improving alert tuning, and integrating automated detection mechanisms.
2. **Reducing MTTR** by refining phishing response playbooks, increasing containment automation, and conducting periodic response simulations.