Scenario:

Lavoriamo in un'azienda in un SOC o CSIRT in una grande azienda e due utenti segnalano problemi sui loro computer e chiedono assistenza al reparto tecnico (che siamo noi).

Esercizio:

Analizzare i seguenti link e fare un piccolo report di quello che si scopre relativo alla segnalazione dell'eventuale attacco https://tinyurl.com/linklosco1 e https://tinyurl.com/linklosco2

2. Analisi dei rapporti degli utenti: Esaminare attentamente le segnalazioni degli utenti sui problemi riscontrati nei loro computer. Raccogliere informazioni dettagliate su comportamenti anomali, messaggi di errore, rallentamenti del sistema, attività sospette, ecc.

3. Esame dei log di sistema: Accedere ai log di sistema dei computer degli utenti per identificare eventuali attività sospette o anomalie. Controllare i log di accesso, i log di eventi, i log di sicurezza e altri registri pertinenti.

4. Analisi dei file e delle cartelle sospette: Ispezionare i file e le cartelle segnalati dagli utenti come potenzialmente sospetti. Effettuare una scansione antivirus e anti-malware per individuare eventuali minacce.

In questo caso specifico:

- DOCX_SENTENCIA_20230003001.exe
- powershell.exe

5. Verifica dell'endpoint: Esaminare lo stato di sicurezza degli endpoint dei computer degli utenti, inclusi aggiornamenti del sistema operativo, patch di sicurezza, software antivirus/antimalware e configurazioni di sicurezza.

6. Esame dei dati di rete: Analizzare il traffico di rete proveniente dai computer degli utenti per individuare eventuali attività sospette o comunicazioni con indirizzi IP noti per essere associati a minacce informatiche.

7. Rapporto e azioni raccomandate: Preparare un rapporto dettagliato che riassuma le scoperte e le analisi effettuate. Includere una valutazione del rischio, raccomandazioni per mitigare le minacce e azioni correttive da intraprendere.