PEPPOLI

ISOLAMENTO:

1. Disconnessione sistema B sia dalla rete interna che da internet per non permettere la diffusione dell'attacco
2. Isolamento in un'area separata per l'analisi approfondita.

RIMOZIONE DEL SISTEMA B INFETTO:

1. Preservare le prove di attacco per poterle analizzare
2. Spegnere il sistema
3. Backup
4. Rimozione fisica del sistema
5. Analisi dei malware
6. Controllo degli altri sistemi all'interno della rete
7. Formattazione (DIFFERENZA PURGE, DESTROY E CLEAR):
    a. PURGE: Sovra scrizione dei dati presenti sui dischi con l'utilizzo di magneti
    b. CLEAR: Sovra scrizione dei dati più e più volte per non permettere ai dati di essere recuperati in nessuna maniera. Si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale.
    c. DESTROY: Distruzione fisica dei dispositivi di storage, rendendoli inutilizzabili.