Isolamento:

- Disconnettere fisicamente il sistema B dalla rete per interrompere la comunicazione con l'attaccante.
- Isolare il sistema B dalla rete interna, impedendo la propagazione dell'attacco ad altri dispositivi.
- Bloccare le porte di comunicazione utilizzate dall'attaccante per evitare ulteriori intrusioni.
- Attivare regole firewall per limitare il traffico in entrata e uscita dal sistema B.

Rimozione del sistema B infetto:

- Arrestare tutti i processi sospetti o non necessari in esecuzione sul sistema B.
- Eseguire una scansione antivirus/antimalware completa per individuare e rimuovere eventuali minacce persistenti.
- Disattivare i servizi di rete per evitare ulteriori comunicazioni malevoli.
- Effettuare un'analisi approfondita dei registri di sistema per identificare tracce dell'attacco.
- Valutare la possibilità di ripristinare il sistema da una copia di backup pulita o reinstallare il sistema operativo.

Differenza tra Purge e Destroy

Purge:

- Il processo di "purge" implica la rimozione delle informazioni sensibili da un sistema senza distruggere fisicamente il supporto di memorizzazione.
- Può coinvolgere la sovrascrittura dei dati sensibili con informazioni non sensibili o casuali.
- Generalmente utilizzato quando è necessario mantenere il supporto di memorizzazione per un riutilizzo futuro.

Destroy:

- Il processo di "destroy" comporta la distruzione fisica del supporto di memorizzazione contenente le informazioni sensibili.
- Può includere il danneggiamento fisico del disco rigido o la completa demolizione del dispositivo.
- Questo metodo è più sicuro, in quanto elimina la possibilità di recupero delle informazioni sensibili.