# Incident response

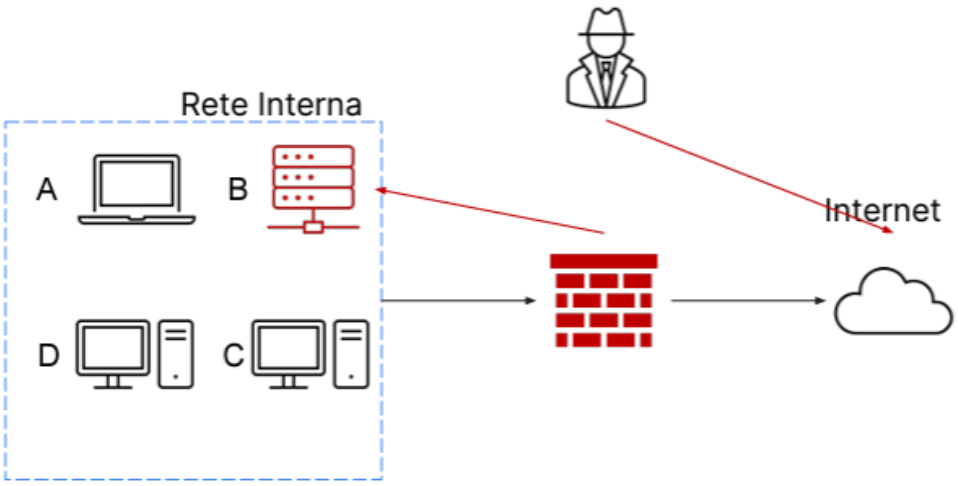
**Traccia:**

Con riferimento alla figura in slide 4, il sistema **B (un database con diversi dischi per lo storage)** è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti.

- Mostrate le tecniche di: I) **Isolamento** II) **Rimozione** del sistema **B infetto**
- Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. **Indicare anche Clear**




In qualità di membro del team di CSIRT, ci si deve occupare immediatamente di rispondere all'attacco in corso che ha compromette il sistema B, un database critico dotato di diversi dischi per lo storage. Ecco una descrizione dettagliata delle azioni che ho intrapreso:

1. **Isolamento del sistema B**:

- ***Identificazione***: rilevazione del traffico sospetto verso il sistema B attraverso i strumenti di monitoraggio della rete.

- ***Isolamento fisico e di rete***: si deve disconnettere il sistema B dalla rete interna ed esterna per interrompere la comunicazione con l'attaccante.

- ***Comunicazione con il team***: informare il resto del team CSIRT dell'isolamento per coordinare i passaggi successivi.

2. ***Rimozione del sistema B infetto:***

- **Valutazione dello stato del sistema**: eseguire un'analisi preliminare per valutare il livello di compromissione del sistema.

- ***Backup***: creare un'immagine forense dei dischi per poter eseguire un'analisi approfondita in seguito, senza compromettere le prove.

- **Pulizia**: rimozione il malware trovato e verifica che non ci sono processi nascosti o connessioni di rete attive.

- **Preparazione per il ripristino**: predisposizione dei passaggi per reinstallare il sistema operativo e le applicazioni dal nostro ambiente sicuro e verificato.

3. **Differenza tra Purge, Destroy e Clear:**

- **Purge**: l'uso questa tecnica per eliminare definitivamente tutte le informazioni dai dischi che non possono essere più considerati sicuri. Questo significa sovrascrivere i dischi con pattern specifici di dati per rendere la ricostruzione dei dati originari praticamente impossibile.

- **Destroy**: Considerando l'importanza critica e la sensibilità dei dati, ho anche valutato l'opzione di distruggere fisicamente i dischi. Questo metodo prevede di rendere i dischi inutilizzabili tramite metodi come la demagnetizzazione, il taglio fisico o l'incenerimento.

- ***Clear***: Prima di utilizzare le tecniche di Purge o Destroy, utilizzare il metodo Clear per rimuovere le informazioni accessibili. Questo metodo coinvolge la sovrascrittura dei dati con zeri valori, il che è adeguato per la maggior parte delle situazioni, ma non sufficiente per dati estremamente sensibili.