Incident response

L9-L4

Traccia

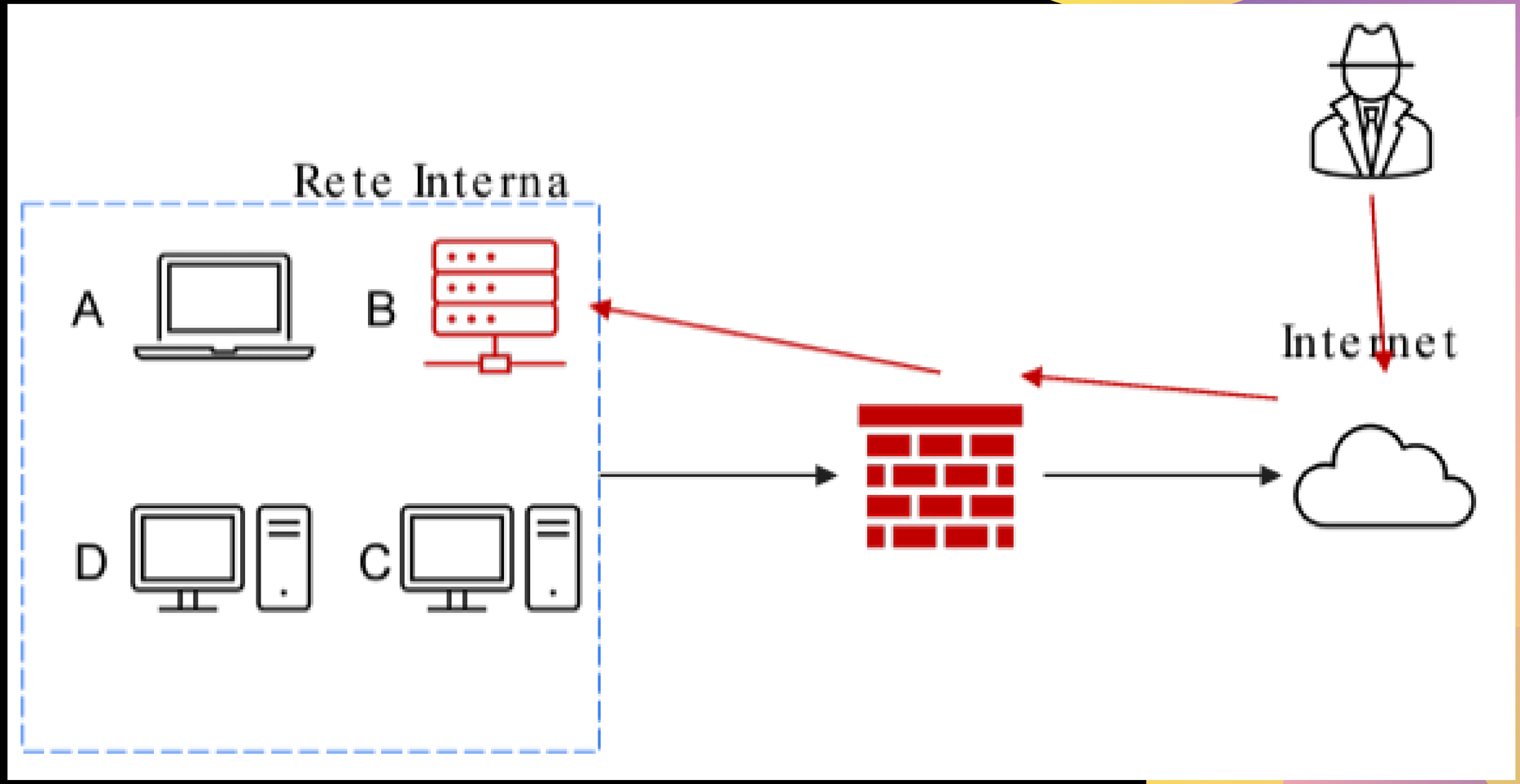
Con riferimento alla figura, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

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

Traccia



Parte 1

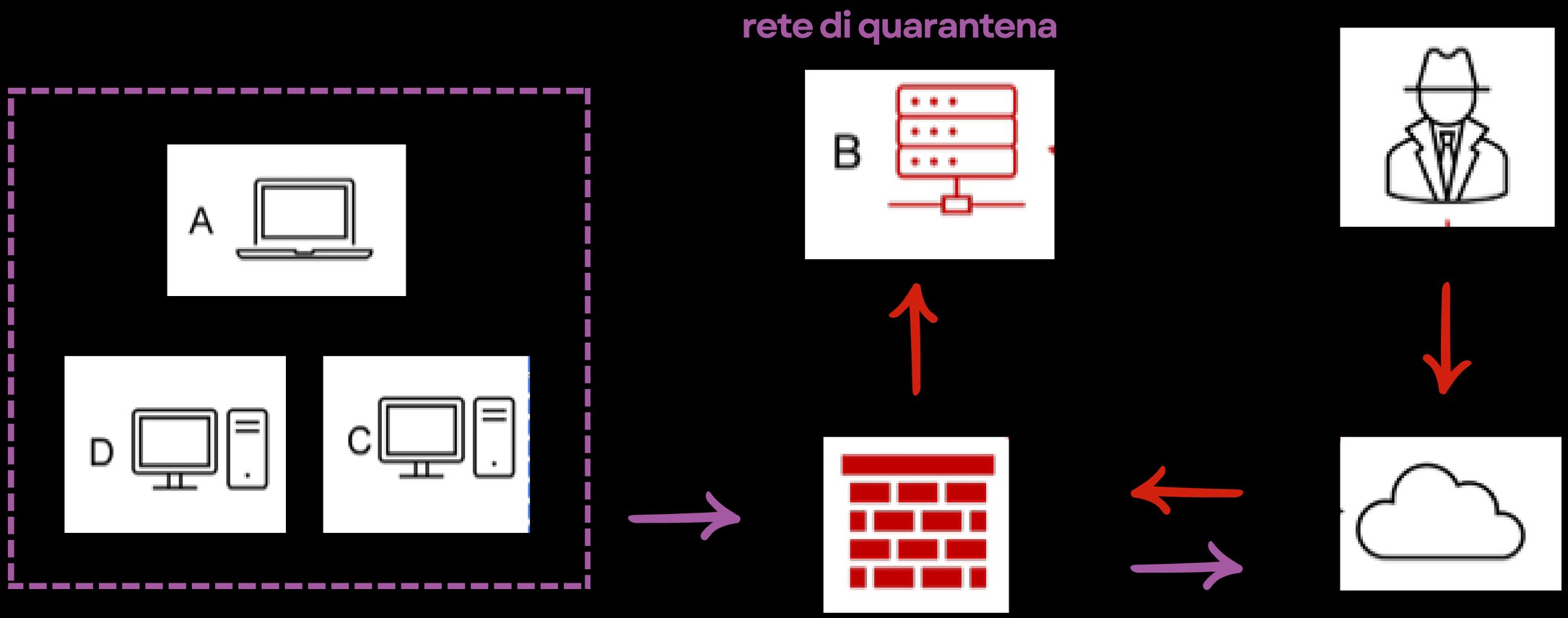
Isolamento

Essendo in corso l’attacco sono state prese delle misure di isolamento della rete B infettata andando a:

- scollegare fisicamente i cavi
- bloccando l’accesso da remoto andando a configurare il firewall bloccando traffico in ingresso e in uscita
- utilizzare la VLAN per separare il sistema B dal resto della rete.

Parte 1

Isolamento - Disegno



Parte 2

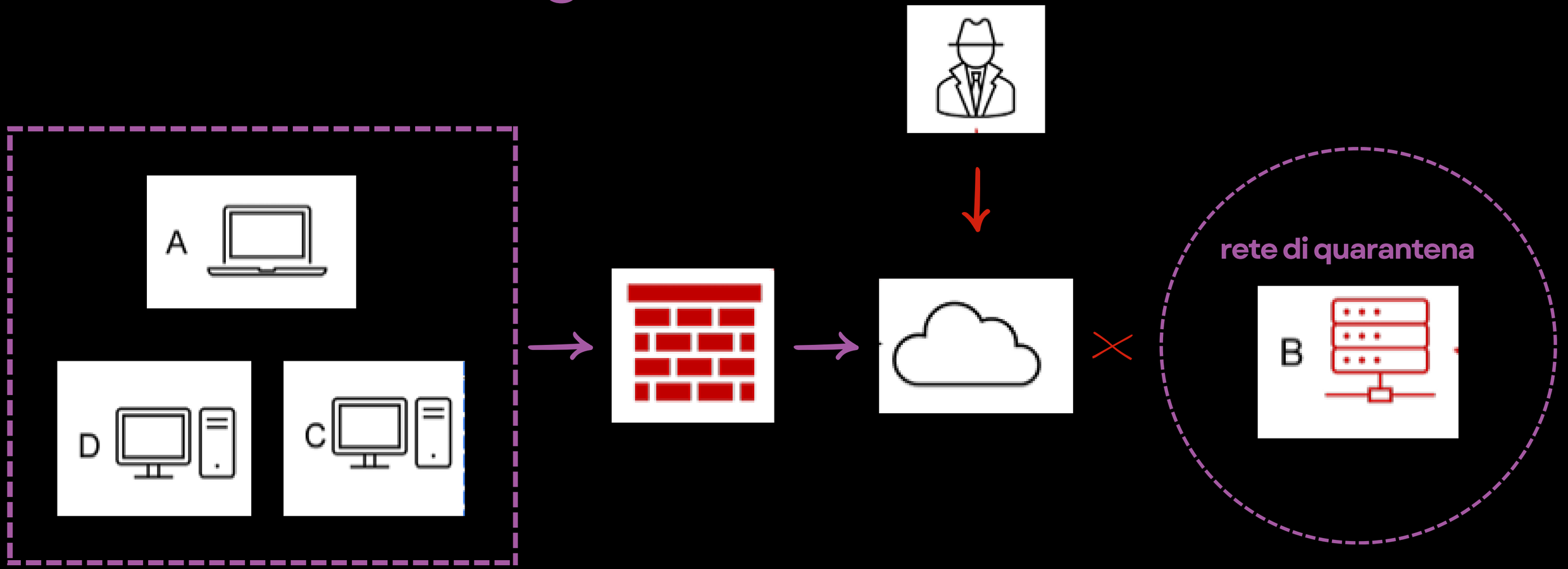
Rimozione

Una volta isolato , utilizziamo delle tecniche di rimozione:

- effettuare uno spegnimento controllato per evitare di predere le prove dell’attacco
- eseguire un backup dei dati critici
- rimuovere fisicamente i dischi e altre componenti hardware per un’ulteriore analisi e distruzione sicura

Parte 2

Rimozione - Disegno



Parte 3

Purge ≠ Destroy ≠ Clear

- **Purge**: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi;

- **Destroy**: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.

- **Clear:** il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche». Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale;