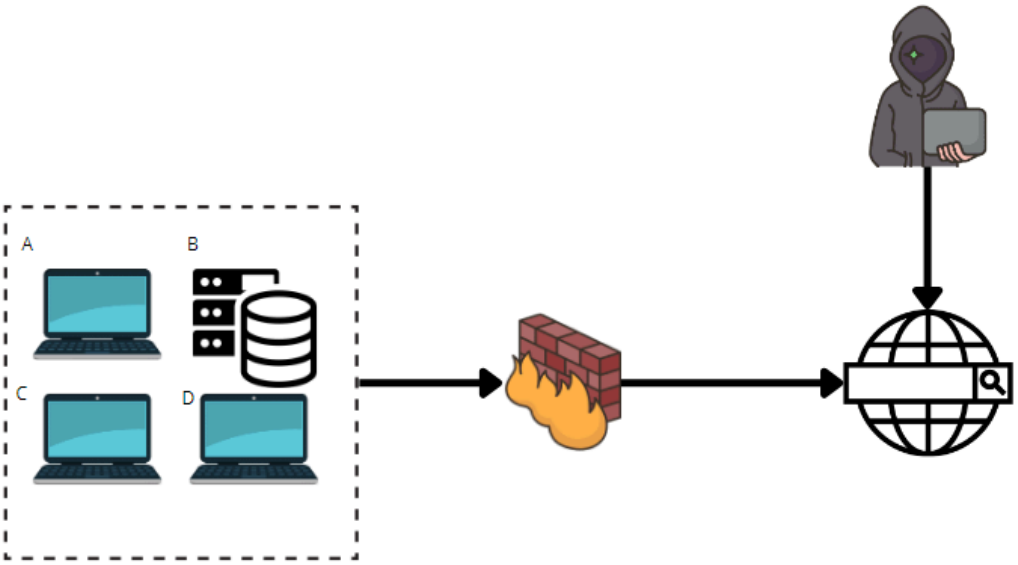
CONSEGNA S9/L4

INCIDENT RESPONSE

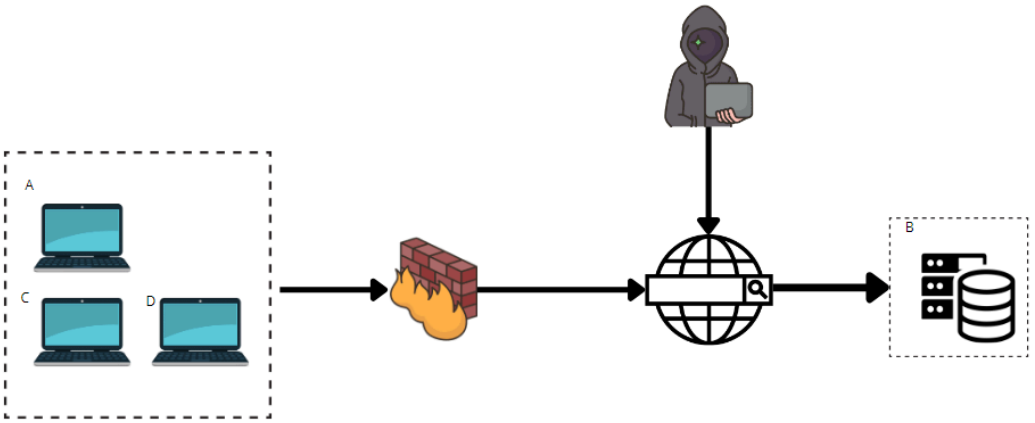
Il sistema **B** (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.
L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.
Mostrate le tecniche 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.



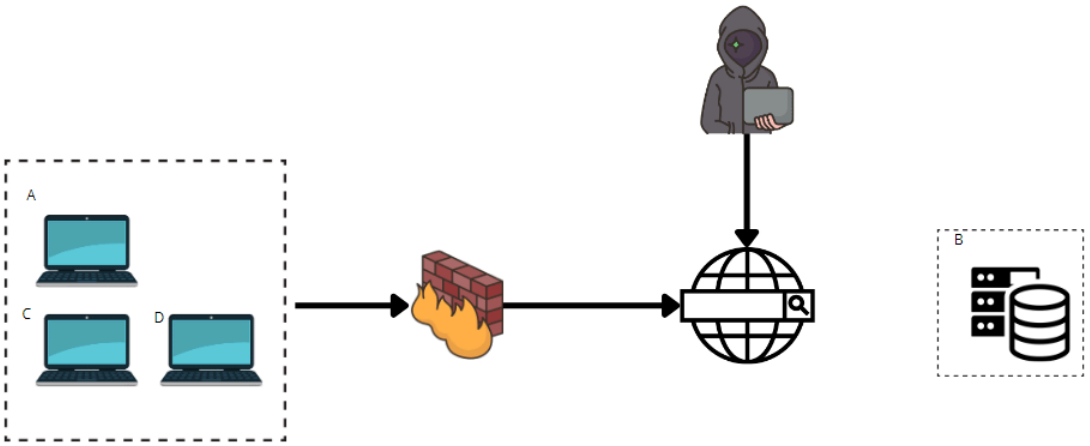
ISOLAMENTO:

La segmentazione riesce a limitare la riproduzione del malware e l'accesso al resto della rete da parte dell'attaccante ma spesso non è sufficiente per chiudere la fase di contenimento.
In questi casi, quando è necessario un contenimento maggiore, si utilizza la tecnica dell'**isolamento**.
L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante.



RIMOZIONE:

Ci sono casi in cui l'isolamento non è ancora abbastanza. In questi casi si procede con la tecnica di contenimento più stringente, ovvero la completa **rimozione** del sistema dalla rete sia interna sia internet. In quest'ultimo scenario l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.



DIFFERENZA TRA PURGE E DESTROY:

Purge:
Tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

Destroy:
Approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili.

Si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature. Questo è il metodo più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.