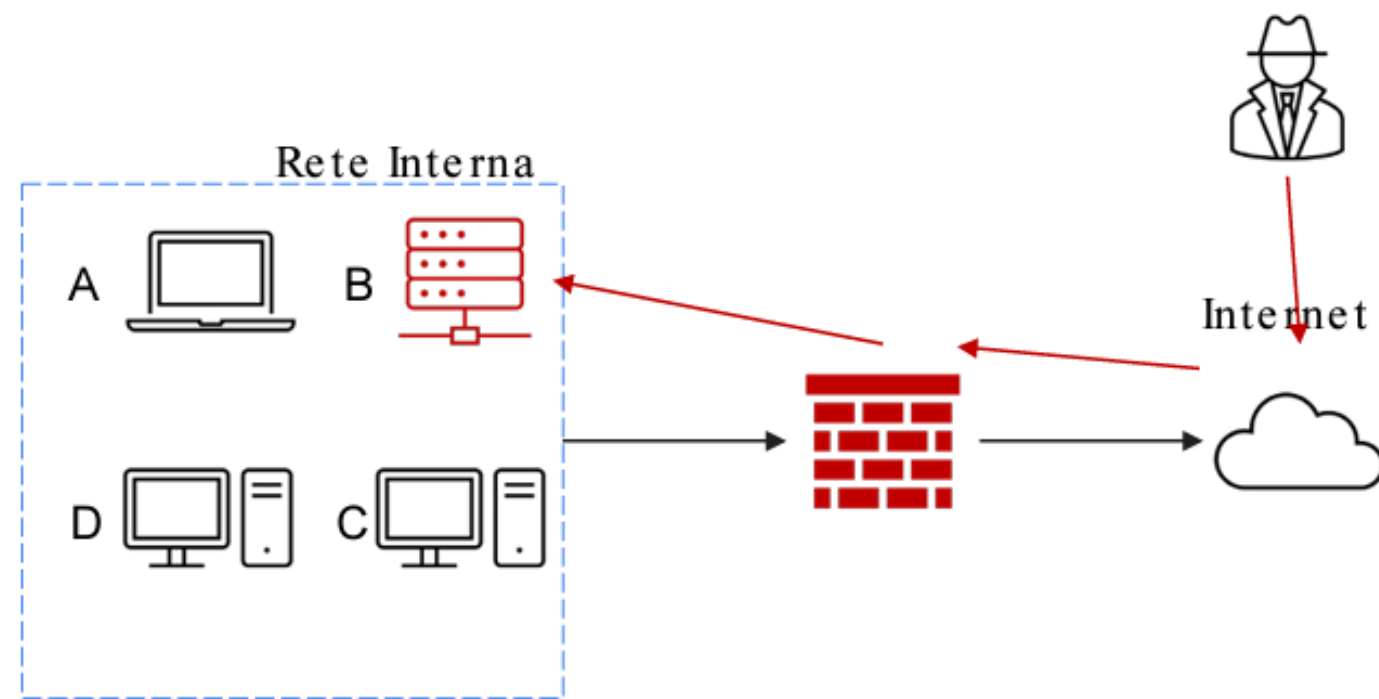
The background is white with several abstract shapes and circles in shades of purple and blue. In the top left, there is a large purple circle and a smaller blue circle. Below them is a medium-sized purple circle. In the top right, there is a medium-sized blue circle. On the right side, there is a large, flowing, ribbon-like shape that transitions from purple to blue. In the bottom right, there is a medium-sized purple circle. In the bottom left, there is a large, flowing, ribbon-like shape that transitions from purple to blue.

S9-L4

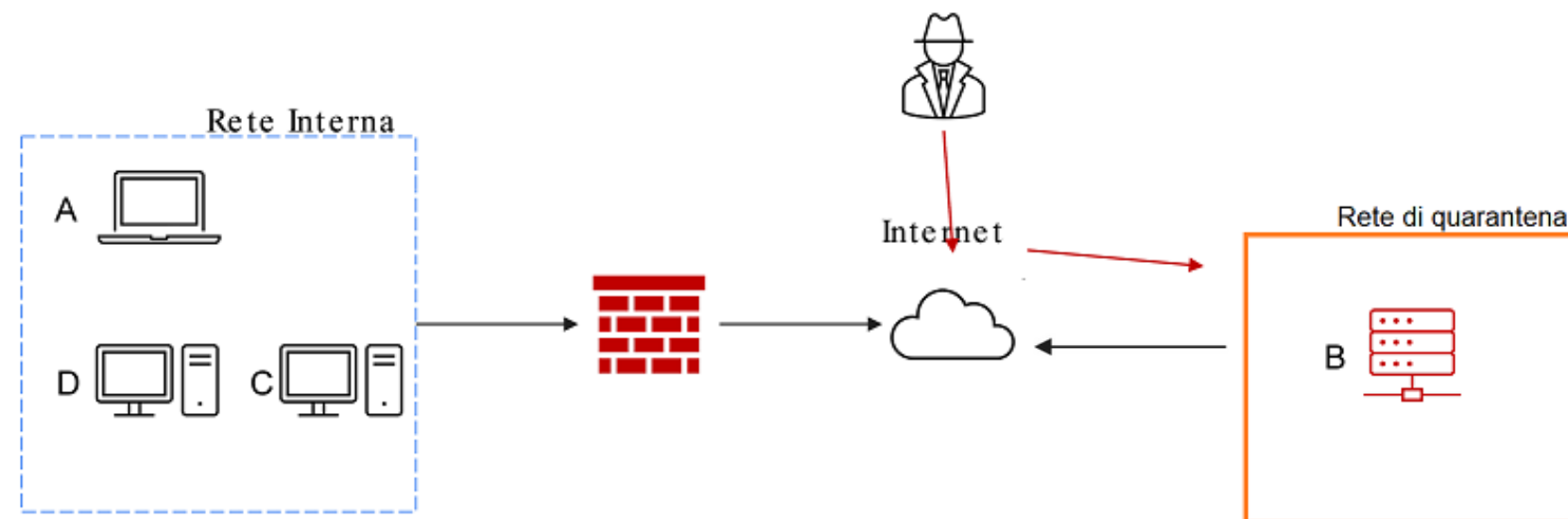
Traccia:

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:

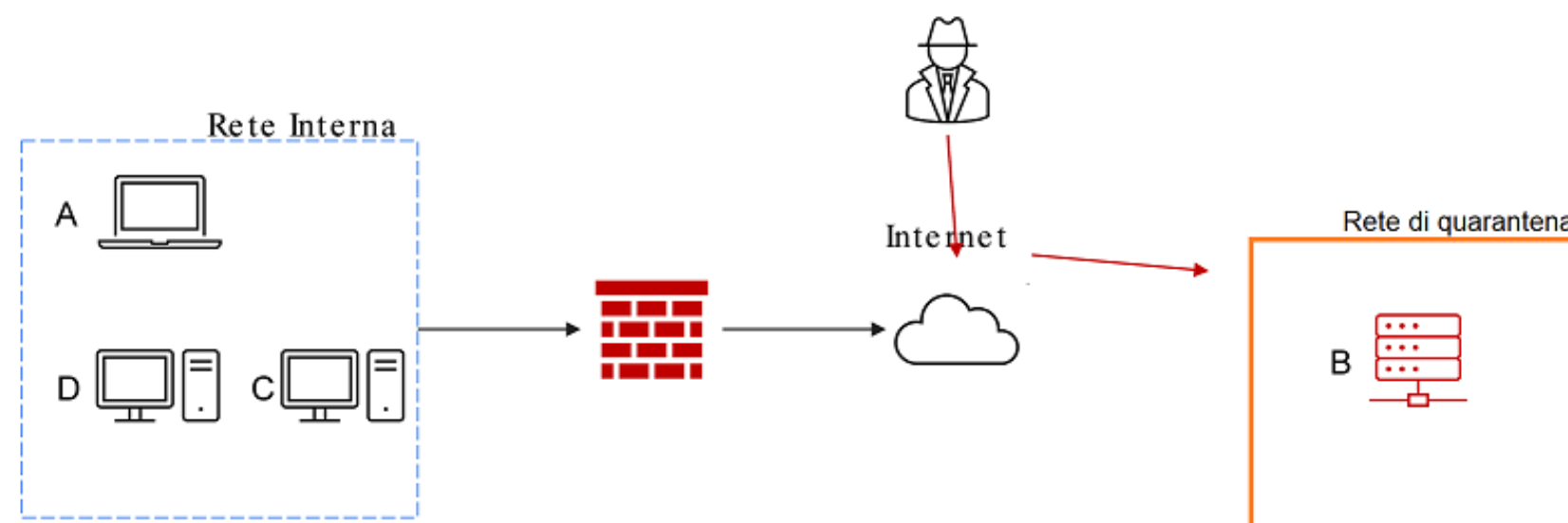
- Mostrate le tecniche di:
 - I) Isolamento
 - II) Rimozione del sistema B infetto
 - Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.
- Indicare anche Clear




Nella situazione data ci viene chiesto di applicare l'isolamento e la rimozione di B dalla rete.



Isolamento: in questa situazione potremmo andare a disconnettere il sistema, in questo caso B, infetto dalla rete aziendale, per non permettere all'attaccante di compromettere altri sistemi appartenenti alla rete. Così facendo però l'attaccante avrà comunque accesso alla rete di quarantena attraverso internet




Rimozione: Per impedire all'attaccante di avere accesso sia alla rete interna che al sistema infetto possiamo optare per una totale rimozione del sistema dalle reti, andando a precludere la possibilità di raggiungere la macchina tramite internet.



Nel caso in cui volessimo essere sicuri di non lasciare informazioni in dei dispositivi di archiviazione, possiamo optare per 3 opzioni principali:

Clear: Il dispositivo viene trattato con tecniche logiche, ovvero il dispositivo può essere sia sovrascritto più volte o ripristinato alle impostazioni di fabbrica, ma ciò potrebbe comportare la recuperabilità di piccole parti di dati.

Purge: Il dispositivo dopo essere stato trattato con soluzioni logiche comporta l'uso di tecniche fisiche, come l'utilizzo di magneti sul disco per rendere inaccessibili le informazioni.



Destroy: Il dispositivo in questo caso viene smaltito , rientrano in questa categoria tutte le tecniche che portano alla totale distruzione e inutilizzabilità dello stesso, come trapanazione, fusione ad alta temperatura, distruzione in laboratorio. Questo è il metodo più sicuro per l'eliminazione totale dei dati, ma anche il più costoso.