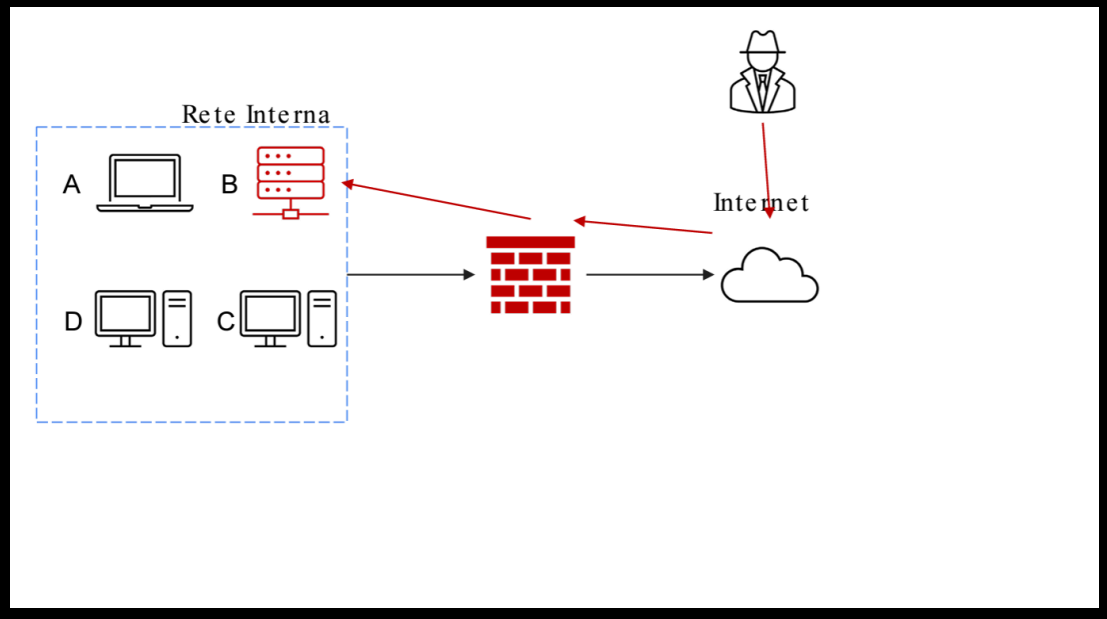
Incident Response

Traccia: Un database all'interno di una rete aziendale è stato compromesso da un attaccante.
L'attacco è attualmente in corso e siete parte del team di CSIRT.

Richieste:
1. Mostrate le tecniche di Isolamento e Rimozione del sistema infetto.
2. Spiegate la differenza tra Clear, Purge e Destroy per l'eliminazione delle informazioni sensibili.

Mappa dell'evento



Notiamo che il sistema B si trova ancora all'interno della rete durante l'attacco.
Per contenere l'attacco possiamo procedere in 3 modi:

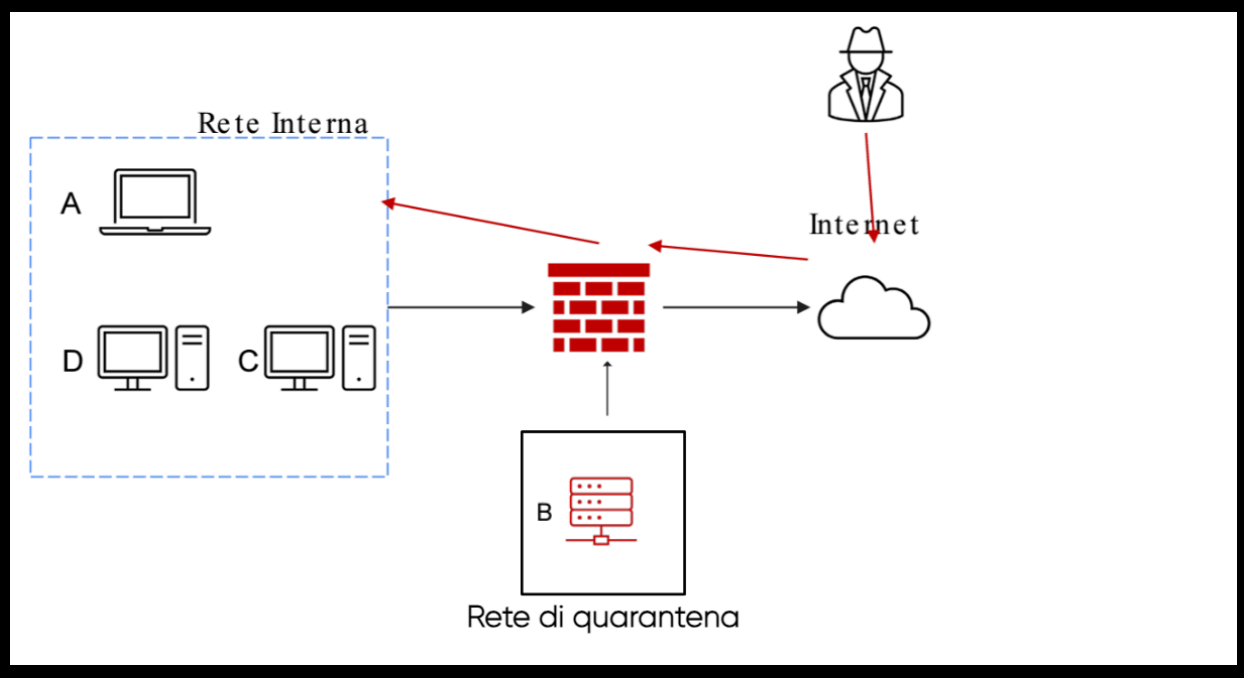
1. Separiamo il sistema B in una rete separata da quella aziendale, chiamiamola "rete di quarantena". Questa tecnica in questo caso potrebbe risultare non ottimale poichè viene usata maggiormente per isolare un malware e impedire di riprodursi, nel caso di un attaccante, potrebbe facilmente saltare da una segmentazione all'altra.

2. Utilizziamo la tecnica di isolamento. Questa tecnica consiste nel completo spostamento dalla rete aziendale, isolando il dispositivo in una rete diversa, con la possibilità di accedere ad internet. In questo modo riusciamo a contenere maggiormente l'attaccante, riducendo la possibilità che acceda in rete interna.

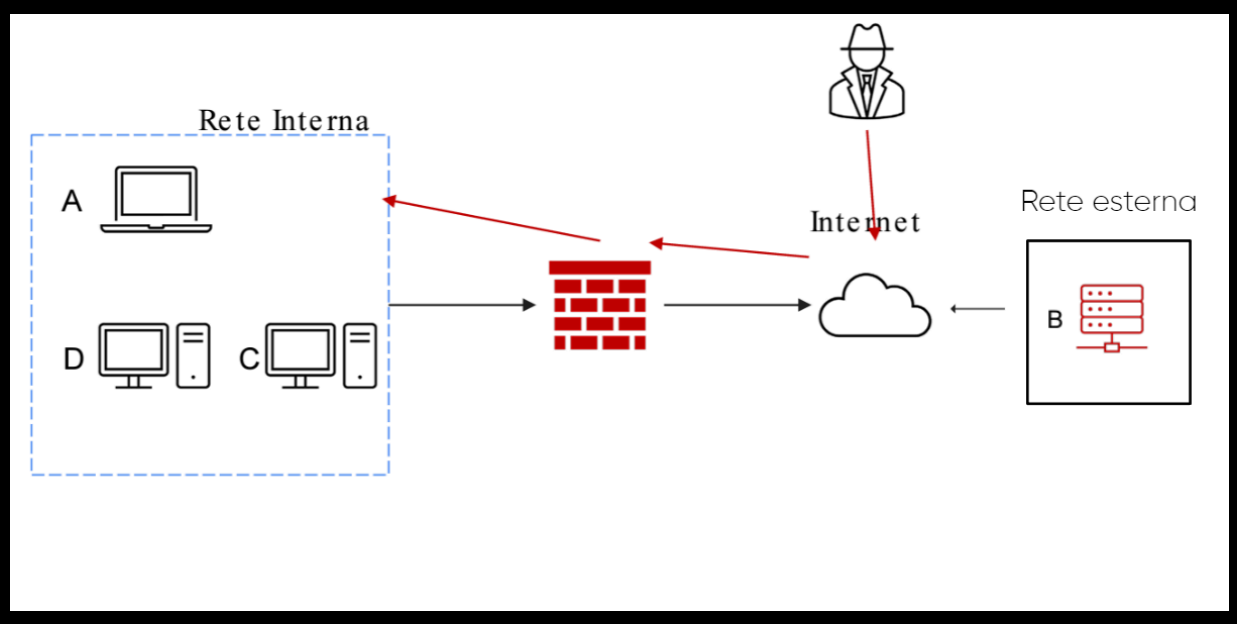
3. Effettuiamo la completa rimozione del sistema dalla rete interna ed esterna (internet). Qui abbiamo la sicurezza che l'attaccante non avrà accesso alla macchina infettata e di conseguenza non potrà accedere alla rete interna.

Rappresentazione grafica

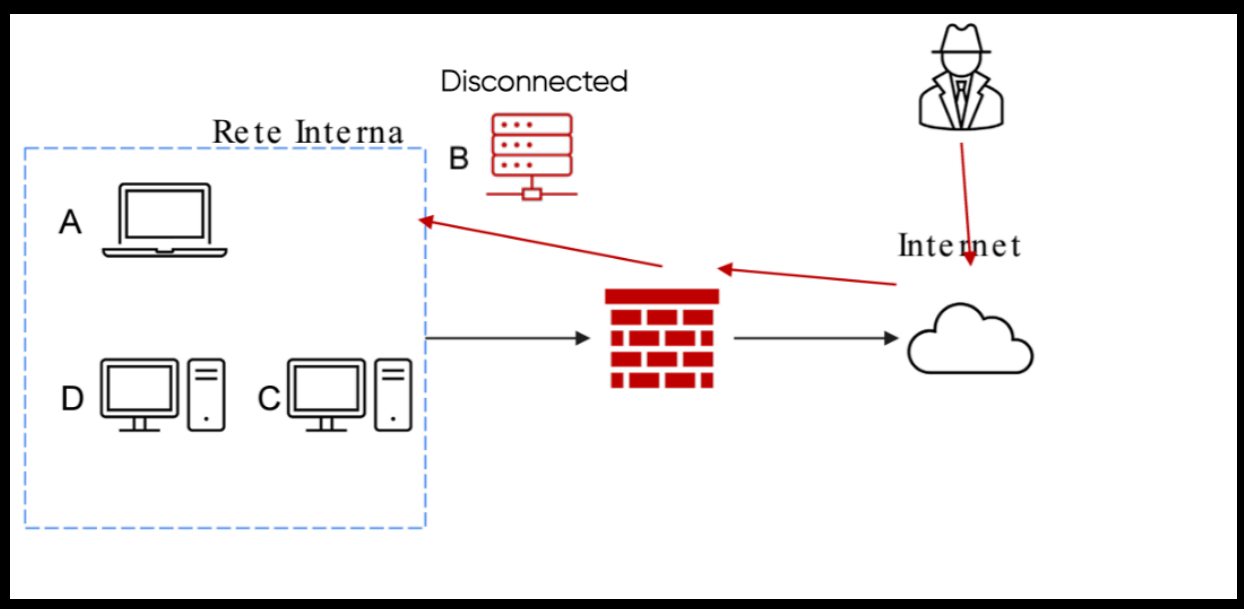
1. Segmentazione



2. Isolamento



3. Rimozione



Fase di recupero

Una volta che il sistema, in questo caso il database, è stato compromesso, riteniamo considerarlo non più affidabile.
A tal proposito, possiamo procedere con lo smaltimento o il riutilizzo del sistema. Dobbiamo accertarci, prima di effettuare queste pratiche, che le informazioni presenti all'interno del sistema siano inaccessibili.

Possiamo procedere con diversi metodi:

1. Clear: Il sistema viene ripulito attraverso tecniche logiche. Si possono utilizzare metodi come read and write dove il contenuto viene sovrascritto più e più volte, o semplicemente procedendo con il factory reset.

2. Purge: Oltre ad utilizzare un approccio logico per la rimozione dei dati sensibili, si adottano tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere i dati inaccessibili.

3. Destroy: Metodo che utilizza tecniche logiche e fisiche per la rimozione dei dati come quelle sopra elencate, ma a differenza di quest'ultimi, si procede ad utilizzare ulteriori tecniche come la disintegrazione, la polverizzazione tramite alte temperature, trapanazione. Questo metodo è il più efficace per rendere inaccessibili in modo permanente i dati.