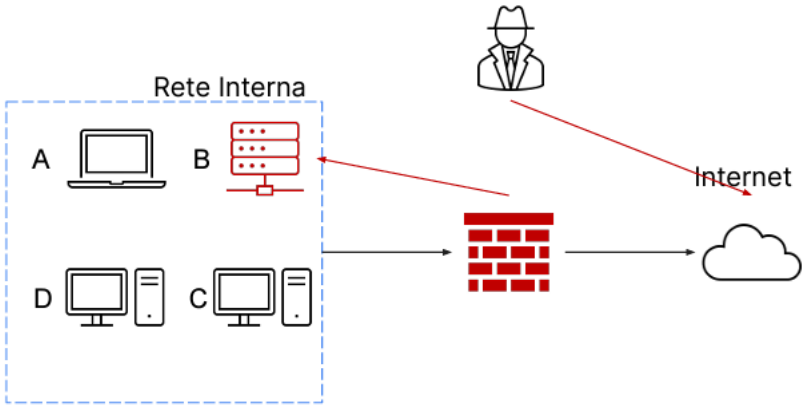

Tecnica di Isolamento: Le attività di contenimento hanno lo scopo primario di isolare l'incidente in modo che non possa creare ulteriori danni a reti o sistemi. Il dispositivo B sulla rete è stato compromesso interamente e la prima attività per poter contenere ulteriori impatti è quella di isolare il database rispetto al resto della rete in modo tale che l'attaccante esterno non possa aver accesso altri nodi. L'isolamento consiste nella completa disconnessione del sistema compromesso dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante.

Tecnica di Rimozione: nel caso in cui l'isolamento non è sufficiente, viene attuata la tecnica di rimozione. In questi casi si procede con la completa rimozione del sistema dalla rete interna e rete internet. Nello scenario presentato dall'esercizio, l'attaccante non avrà accesso alla rete interna né al sistema compromesso. In questa fase lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell'evento malevolo. Questa attività può includere la rimozione di eventuali backdoor installate da un malware oppure, nel nostro caso, ripulire dischi e chiavette USB compromesse. La scelta della fase di rimozione dipende dall'impatto che l'incidente ha avuto. Come ultima cosa post-risoluzione deve essere redatta una lista dettagliata delle attività da seguire all'interno dei «playbooks».

Differenza tra Purge e Destroy: la procedura di **Purge** viene adottata non solo seguendo un approccio logico per la rimozione dei contenuti sensibili, ma anche tecniche di rimozione fisica come l'utilizzo di magneti per rendere le informazioni inaccessibili su determinati dispositivi. Differentemente l'azione di **Destroy** risulta essere l'approccio più netto e drastico per lo smaltimento di dispositivi con dati sensibili. Oltre ai meccanismi logici e fisici vengono utilizzate le cosiddette "tecniche di laboratorio" come la disintegrazione, polverizzazione dei media ad alte temperature o la trapanazione dei dispositivi. Questo metodo è il più efficace per rendere le informazioni inaccessibili; tuttavia, risulta essere anche quello che presenta costi maggiori.

Clear: il dispositivo compromesso viene ripulito dal suo contenuto con tecniche logiche. Un approccio utilizzabile potrebbe essere il read and write dove il contenuto viene sovrascritto diverse volte oppure viene utilizzata la funzione di «factory reset» per poter riportare il dispositivo alle "impostazioni di fabbrica".