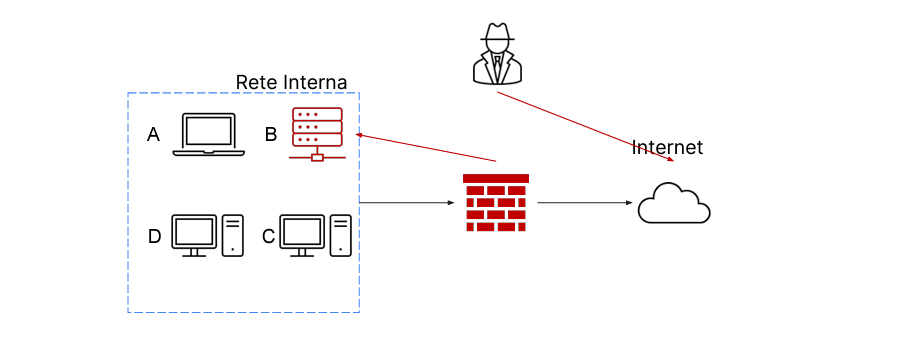
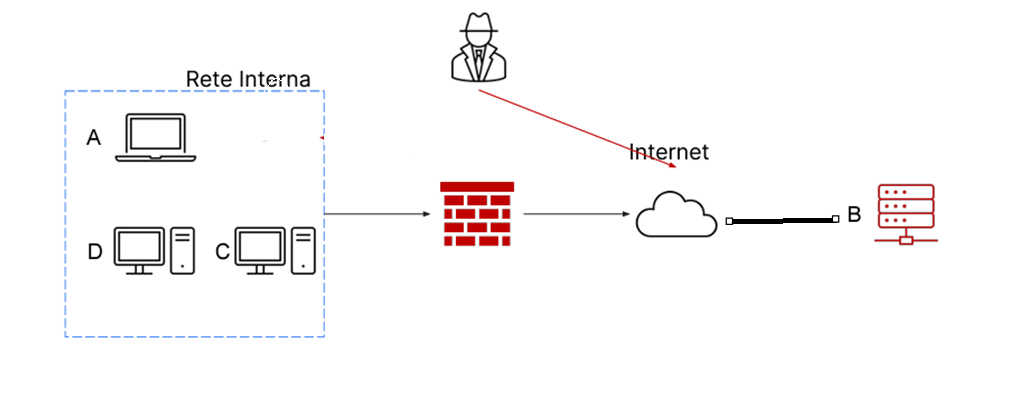
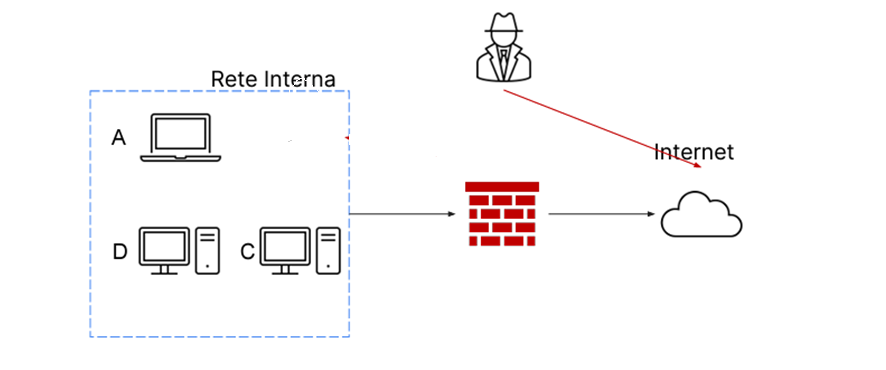
Oggi andremo ad effettuare la fase di contenimento, eliminazione e recupero dei servizi di un incident response. Siamo all’interno di un team CISIRT e, come mostrato dalla figura sottostante, un database (B) della compagnia è stato compromesso.



Inizieremo la procedura con il contenimento della minaccia:



L’operazione che andremo ad eseguire è quella di “isolamento” del dispositivo infettato. Questa operazione, a differenza della segmentazione e della quarantena, estranea completamente il nostro dispositivo dalla rete interna dell’azienda. Così facendo, gli sarà impossibile infettare gli altri dispositivi all’interno della rete.

Successivamente, procederemo alla rimozione del sistema infetto: 

Grazie a questa operazione, l’attaccante non avrà più alcun accesso al dispositivo.

Una volta rimossa la nostra risorsa, procederemo alla fase di recupero. Questa fase consiste proprio nell’andare a ristabilire l’operatività dei servizi aziendali, dell’applicazione di eventuali patch e di revisione delle policy di sicurezza, proprio per evitare che lo stesso incidente possa succedere una seconda volta.

Oltre a questo, è possibile (eventualmente) anche andare e recuperare dischi rigidi per il loro riutilizzo. Naturalmente, prima di riutilizzarli sarà necessario assicurarsi che i dati presenti sullo stesso siano totalmente inaccessibili, per poi andare a riutilizzarlo nuovamente. Esistono diverse tecniche per il recupero dei dischi, oggi vedremo purge e destroy:

* Purge consiste nell’adottare soluzioni logiche e fisiche per l’eliminazione dei dati presenti sul disco. Ciò vuol dire che potremo effettuare operazione di reset di fabbrica o di write and read e, in aggiunta, operazione fisiche come l’utilizzo di magneti che rendono le informazioni presenti sul disco inaccessibili;
* Destroy: oltre alle tecniche già menzionate, potremmo usare vere e proprie tecniche di laboratorio, come la disintegrazione e la polverizzazione dei media ad alte temperature. Questi metodi sono sicuramente i più efficaci, ma anche i più costosi.