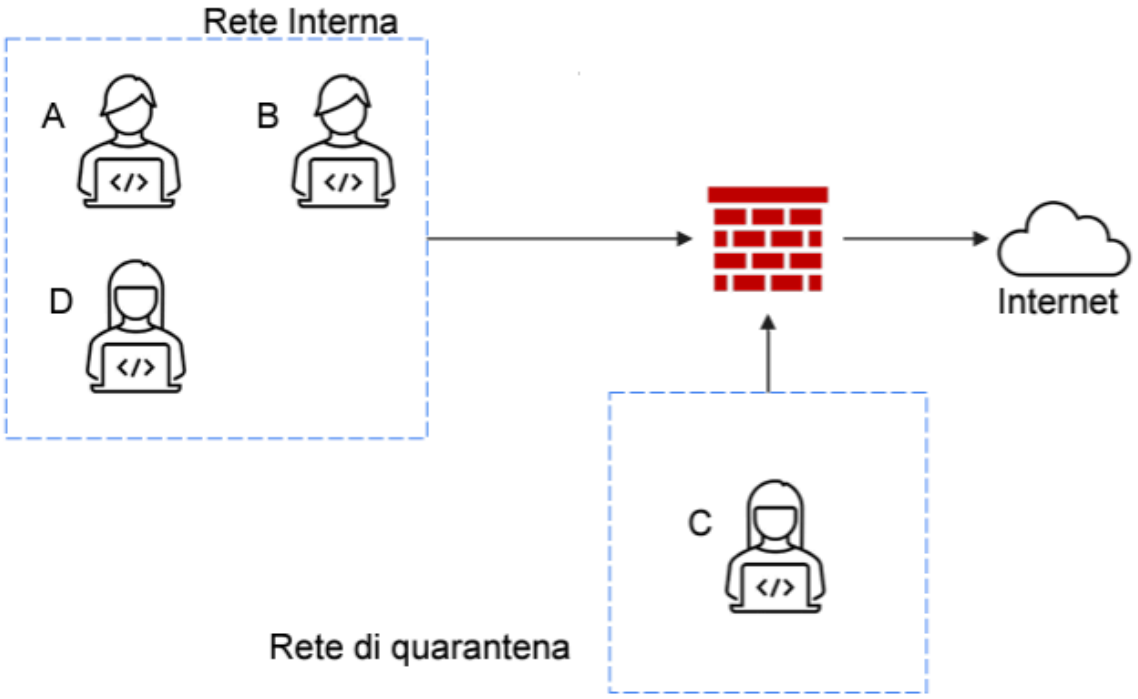
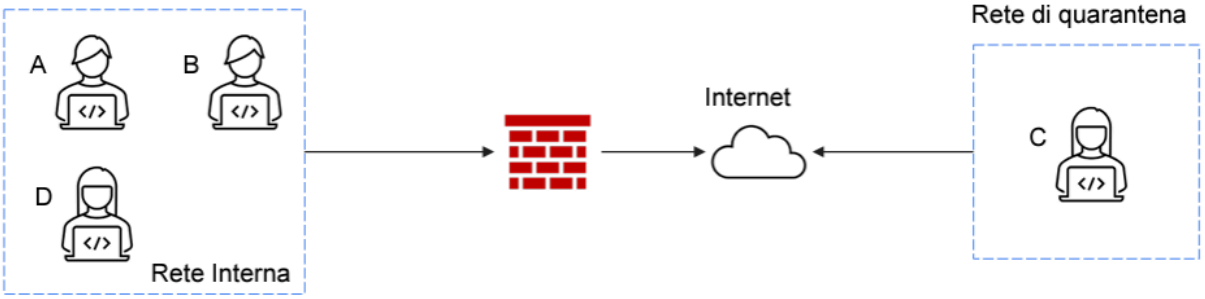
Oggi analizzeremo alcune azioni delle fasi di contenimento, rimozione e recupero delle politiche di incident response.
Nell'esercizio ci viene presentato uno scenario in cui un attaccante riesce ad accedere al database di un'azienda. In quanto membri dello CSIRT spetta a noi occuparcene.
Per cominciare dobbiamo cercare di contenere il più possibile il danno e interrompere l'attacco, per cui isoliamo i sistemi colpiti.
Una tecnica che può essere usata, sia in maniera preventiva che tardiva, per evitare il diffondersi di un attacco è la segmentazione della rete. Possiamo segmentare la nostra rete e creare una rete di quarantena per separare i sistemi compromessi dagli altri presenti nella rete, come nella figura qui sotto.



In questo caso il sistema compromesso sarà ancora nella nostra rete, ma sarà separato dagli altri dispositivi.
In alternativa lo si può isolare dalla rete come mostrato nella figura di seguito.



Tutto questo però potrebbe non bastare; in questi casi si può optare per la rimozione completa del sistema dalla rete, per esempio scollegandolo

completamente. In questo modo l’attaccante non potrà accedere neanche al sistema compromesso.
Una volta eseguite le azioni di contenimento dell’incidente dobbiamo passare alla fase di rimozione. Essa può includere la rimozione di backdoor, malware, pulizia dei dispositivi compromessi e dipende dal tipo di incidente avvenuto.
Una lista delle attività da seguire può essere trovata nei playbooks, che è un documento con una lista di strategie da seguire nel caso di un incidente. Esso viene creato durante lo sviluppo di un piano di incident response, tipicamente da documentazione già esistente, come per esempio policy di sicurezza.
Terminata la fase di rimozione si procede con la fase di recupero dei dati e informazioni perse. Durante questa fase ci si può trovare a smaltire o riutilizzare il sistema compromesso. Quindi per prima cosa bisogna accertarsi di aver pulito bene il sistema, per evitare che le informazioni siano accessibili.
Si possono usare tre opzioni diverse: clear, purge e destroy.
Con clear il contenuto del dispositivo viene sovrascritto più volte o si utilizza la funzione di ripristino dei dati di fabbrica.
Purge combina le tecniche logiche viste in precedenza con clear con tecniche fisiche, come per esempio l’utilizzo di un degausser.
Destroy invece oltre alle tecniche precedenti usa anche tecniche di laboratorio come trapanazione e disintegrazione.
Sebbene clear sia la tecnica più semplice e meno esosa, non garantisce la completa rimozione delle informazioni o dei malware presenti. Per contro destroy è la tecnica più efficace, ma anche quella che comporta una spesa maggiore.