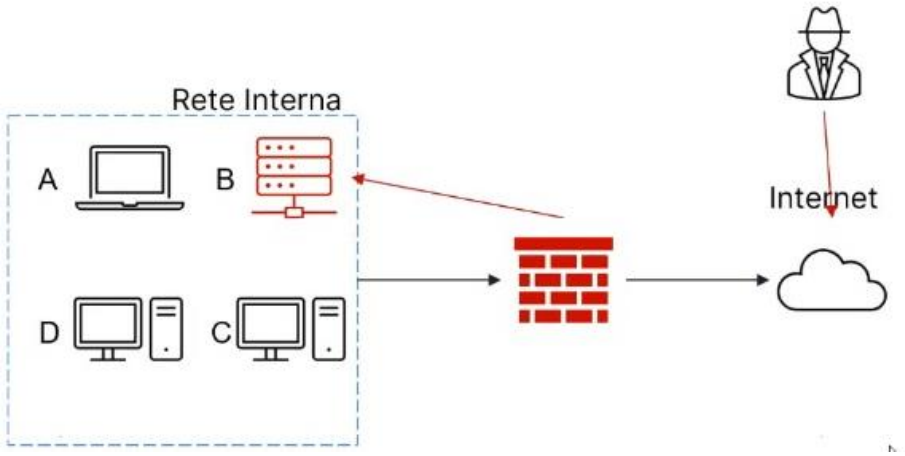
INCIDENT RESPONSE

TASK 1: **Attuazione delle tecniche di isolamento e rimozione del sistema infetto "B", secondo il modello riproposto nella figura sottostante.**

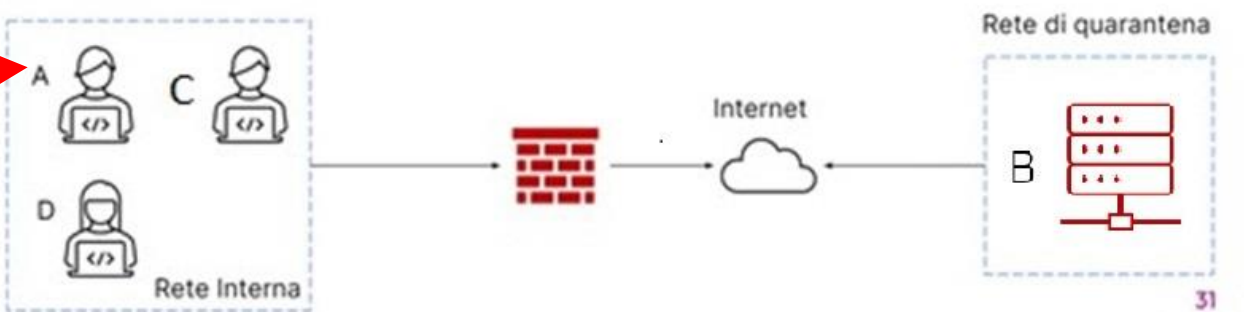


Il primo passo della fase di risposta agli incidenti **è il contenimento dei danni causati dall'incidente di sicurezza**. Questa azione **deve essere effettuata il più rapidamente possibile per evitare che la minaccia si diffonda ad altri sistemi**, applicazioni e risorse aziendali oltre a quelli già colpiti. L'obiettivo di questo processo **è isolare l'incidente in modo da non causare ulteriori danni alle reti e ai sistemi, riducendo così l'impatto generato dall'incidente**. Per raggiungere questo obiettivo, vengono utilizzate varie tecniche:

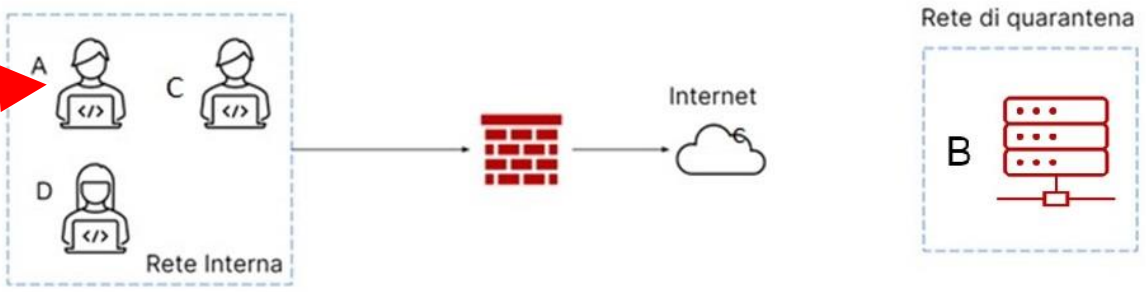
- **ISOLAMENTO**
- **RIMOZIONE**
- **SEGMENTAZIONE**

Come richiesto dalla traccia ci concentreremo sull'ISOLAMENTO E SULLA RIMOZIONE!.

ISOLAMENTO, tecnica secondo cui si procede **disconnettendo completamente il sistema infetto** (in questo caso "B") **dalla rete. Questo ha lo scopo di limitare ulteriormente l'accesso dell'attaccante alla rete interna**. È importante notare che, in questa situazione, l'attaccante ancora mantiene l'accesso al sistema "B" tramite Internet. L'isolamento viene spesso impiegato per raccogliere il maggior numero possibile di informazioni sull'attacco in corso, ad esempio monitorando il traffico di rete, senza compromettere gli asset dell'intera azienda.



A volte, **l'isolamento da solo potrebbe non essere sufficiente per contenere efficacemente la minaccia**. In questi casi, **si utilizza la tecnica della RIMOZIONE**, che è considerata la misura più drastica per contenere i danni. **La rimozione comporta la disconnessione completa del sistema infettato sia dalla rete interna che dalla rete Internet**. È importante sottolineare che, anche in caso di creazione di una rete di quarantena, l'attaccante potrebbe ancora avere accesso a un sistema tramite la rete Internet. Tuttavia, **con l'adozione della tecnica di rimozione, l'attaccante non avrà più alcun tipo di accesso né alla rete interna né alla macchina infettata attraverso Internet.**



TASK 2 = Spiegare la differenza tra PURGE e DESTROY per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.

Parlare anche di CLEAR.

Durante la fase di ripristino dei servizi e delle normali operazioni dopo un incidente di sicurezza, è comune affrontare la questione dello smaltimento o del riutilizzo di un disco o di un sistema di archiviazione proveniente da un dispositivo compromesso. È essenziale garantire, come primo passo, che le informazioni presenti su tale disco o componente di archiviazione siano completamente inaccessibili prima di procedere allo smaltimento o al suo riutilizzo.

Possiamo individuare tre metodologie di gestione dei media contenenti informazioni sensibili:

PURGE

In questa situazione, vengono utilizzati metodi sia logici che fisici per rimuovere i contenuti sensibili presenti nei media. Un'operazione comune è l'impiego di tecniche di smagnetizzazione, come l'uso di un degausser, che mirano a rendere le informazioni completamente inaccessibili su dispositivi specifici. Questo processo garantisce la distruzione fisica dei dati sensibili, prevenendo qualsiasi tentativo di recupero delle informazioni.

DESTROY

Si tratta dell'approccio più estremo per eliminare dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici, vengono impiegate tecniche di laboratorio come la disintegrazione, la polverizzazione ad alte temperature e la foratura dei dischi. Questo metodo è indubbiamente il più efficace per rendere le informazioni del tutto inaccessibili, ma richiede anche un notevole impegno economico.

CLEAR

Il dispositivo viene completamente eliminato dei suoi contenuti sensibili utilizzando tecniche logiche. Un approccio comune è quello della sovrascrittura ripetuta (read and write), in cui il contenuto viene riscritto più volte. In alternativa, si può eseguire una factory reset per riportare il dispositivo allo stato iniziale, eliminando tutti i dati presenti.