REPORT S9-L4

INCIDENT RESPONSE

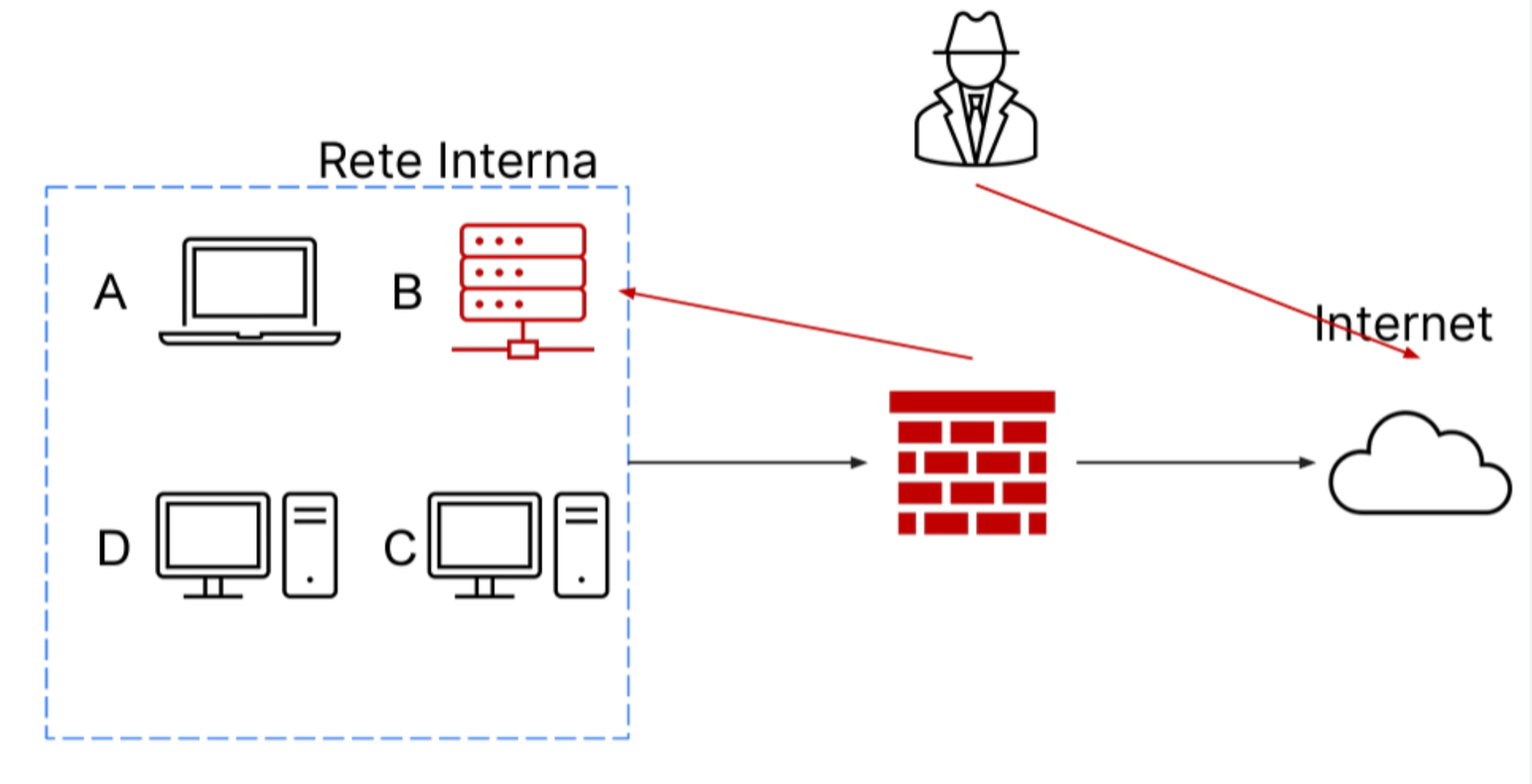
FASE DI CONTENIMENTO, RIMOZIONE

TRACCIA

L’esercitazione svolta nel presente report riguarda la compromissione totale di un sistema B, un database con diversi dischi per lo storage, da parte di un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.
Quindi, l’attacco è in corso.

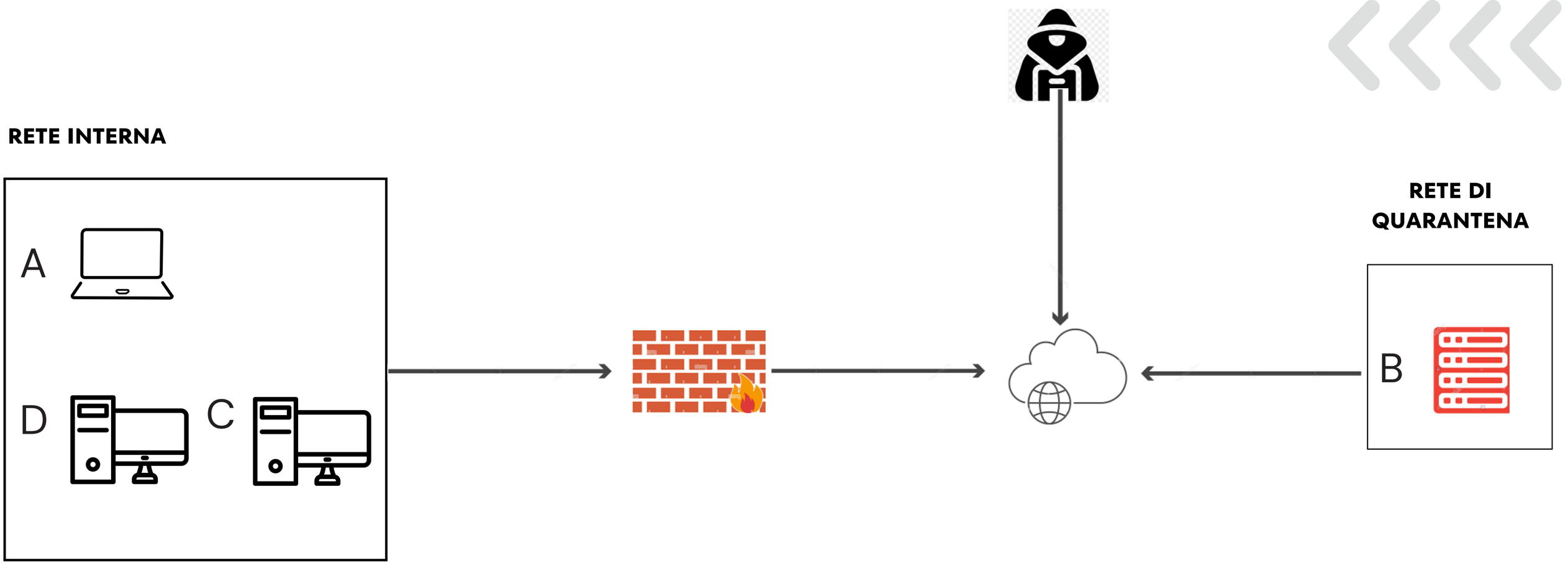
In particolare, viene richiesto di considerarsi come parte di un team CSRTI e, come tale,:

- di mostrare le tecniche di: I) Isolamento e II) Rimozione del sistema B infetto.
- di spiegare la differenza tra Purge e Destroy per l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.



Tecniche di isolamento e rimozione di un sistema infetto o compromesso

ISOLAMENTO



SPIEGAZIONE TECNICA ISOLAMENTO

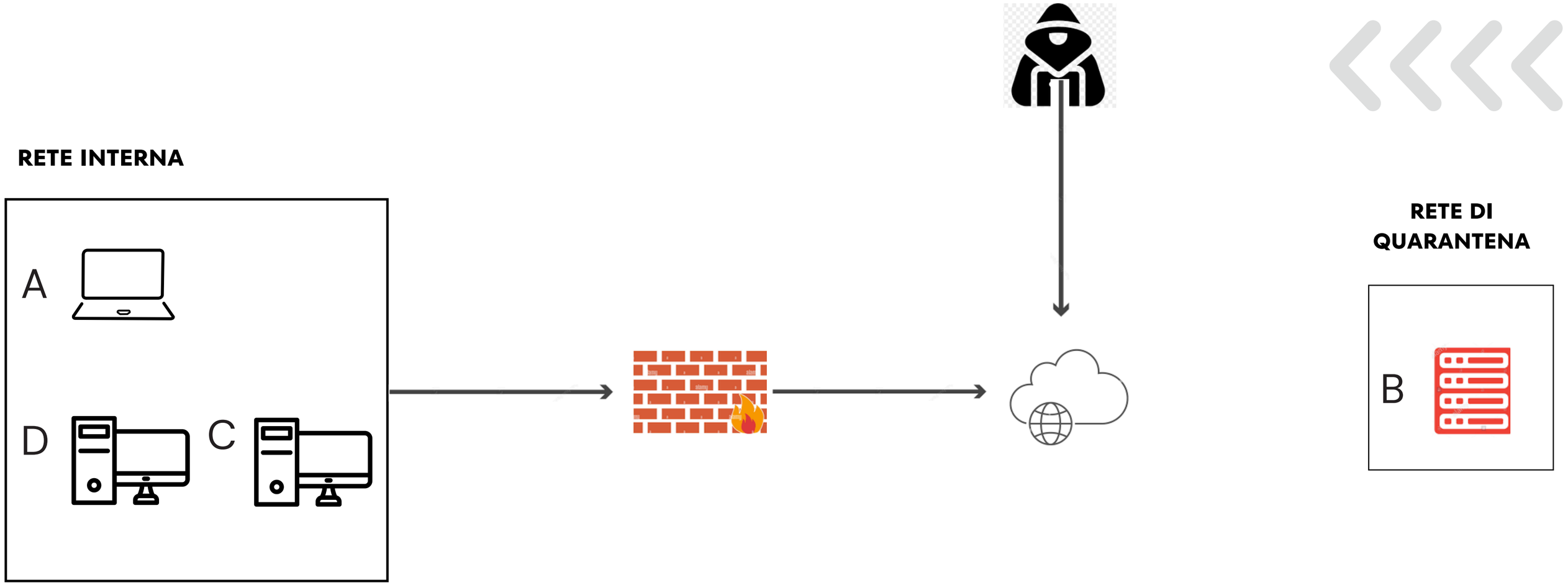
La tecnica di isolamento **è parte integrante della fase di contenimento** nell'ambito della risposta agli incidenti informatici.
Questa fase è attivata dopo la rilevazione di un incidente di sicurezza e mira a contenere l'attacco, limitando i danni e prevenendo la sua diffusione.

L’isolamento consiste nella **completa disconnessione, logica e fisica, del sistema infetto dalla rete interna aziendale**, per restringere maggiormente, rispetto alla semplice segmentazione di rete, l’accesso alla rete interna da parte dell’attaccante.

- **Isolamento fisico**: consiste nel disconnettere fisicamente il sistema compromesso dalla rete, scollegando i cavi di rete o interrompendo l'alimentazione elettrica del dispositivo.
- **Isolamento logico:** consiste nell’ interrompere la comunicazione di rete tra il sistema compromesso e il resto della rete interna, modificando le configurazioni di rete o stabilendo policy, in firewall e altri dispositivi di rete, per impedire la connessione da e verso il sistema compromesso.

L'isolamento viene eseguito in modo tempestivo **per mitigare gli impatti dell'incidente**, proteggendo, al contempo, la continuità operativa dell'organizzazione.
In particolare, si può notare che in questo caso l’**attaccante ha ancora accesso al sistema B compromesso da internet** ma l’attacco non si diffonde alla rete interna.

RIMOZIONE



SPIEGAZIONE TECNICA RIMOZIONE

La tecnica di rimozione **è parte integrante della fase di contenimento degli incidenti** nell'ambito della risposta agli incidenti informatici.
Questa fase mira a contenere l'attacco, limitando i danni e prevenendo la sua diffusione.

La rimozione è una tecnica di contenimento più stringente che consiste nella la **completa rimozione del sistema dalla rete sia interna sia internet**, per impedire completamente, a differenza dell' isolamento di rete, l'accesso alla rete interna e alla macchina infetta da parte dell'attaccante.

- **Rimozione fisica:** consiste nell'eliminare fisicamente il dispositivo compromesso.
- **Rimozione logica:** consiste nell' utilizzare soluzioni software per eliminare virtualmente componenti danneggiati o compromessi.

La rimozione viene eseguita in modo tempestivo **per mitigare gli impatti dell'incidente**, proteggendo, al contempo, la continuità operativa dell'organizzazione.
In particolare, si può notare che in questo caso **l'attaccante non avrà accesso alla rete interna né tantomeno alla macchina infettata.**

Differenza tra Purge e Destroy

PURGE E DESTROY

Si tratta di **due metodi per la gestione dei media**, contenenti informazioni sensibili, presenti su dischi o sistemi di storage di un sistema compromesso.
Durante la fase di recupero di un Incident response, si deve spesso gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso.

In questo caso, bisogna accertarsi, in prima istanza, che le informazioni presenti sul disco/componente siano completamente inaccessibili prima di smaltire o utilizzare nuovamente il disco.

Purge: è un metodo di rimozione dei dati sensibili dal dispositivo che usa tecniche logiche, come la sovra-scrizione del contenuto più volte o la funzione del ripristino alle impostazioni di fabbrica, e tecniche fisiche, di rimozione dei dati con l'utilizzo di magneti.

Destroy: è un metodo di rimozione dei dati che, oltre alle tecniche logiche e fisiche, utilizza anche tecniche di laboratorio come la polverizzazione dei media ad alte temperature.

La differenza sta nel fatto che il Destroy è un approccio più aggressivo, perchè comporta direttamente la distruzione del dispositivo, e più efficace nel rendere le informazioni inaccessibili.
D'altro canto comporta un effort maggiore, soprattutto perchè più costoso del metodo purge