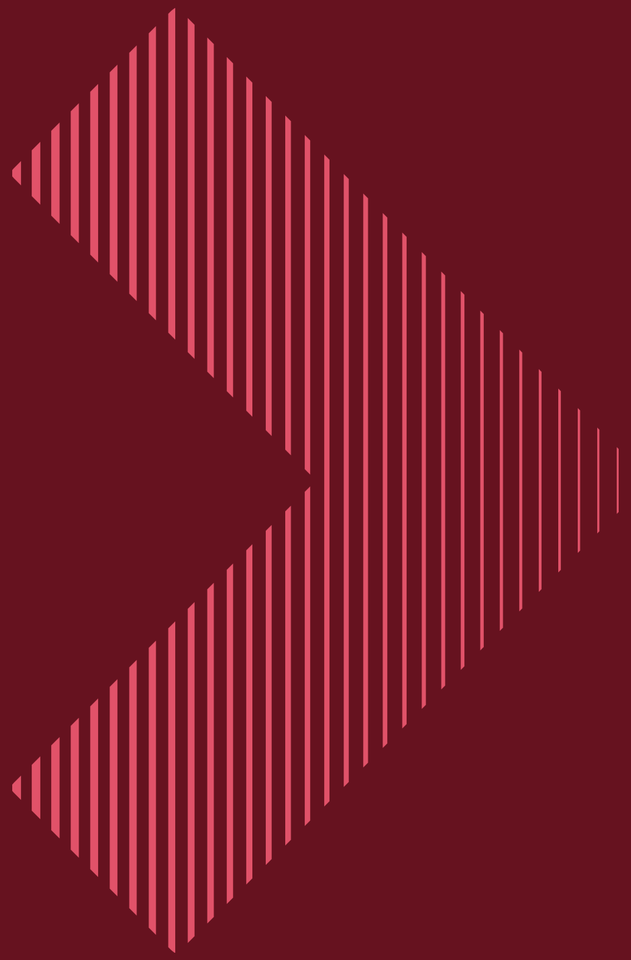


Indice

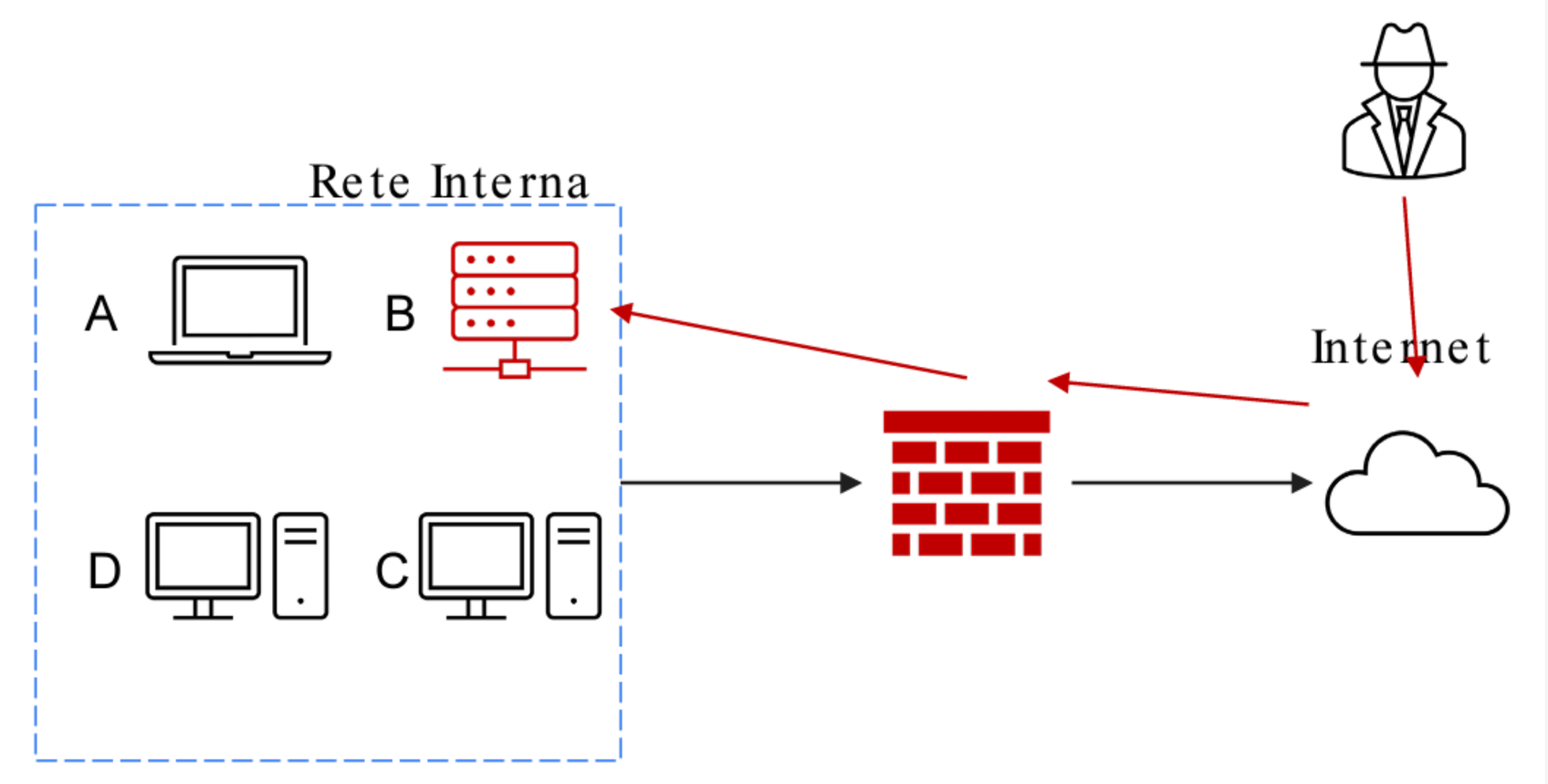
Traccia

Con riferimento alla figura in slide 4, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet. L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti:

- Mostrate le tecniche di: I) **Isolamento** II) **Rimozione** del sistema B infetto
- Spiegate la differenza tra Purgee Destroyper l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear

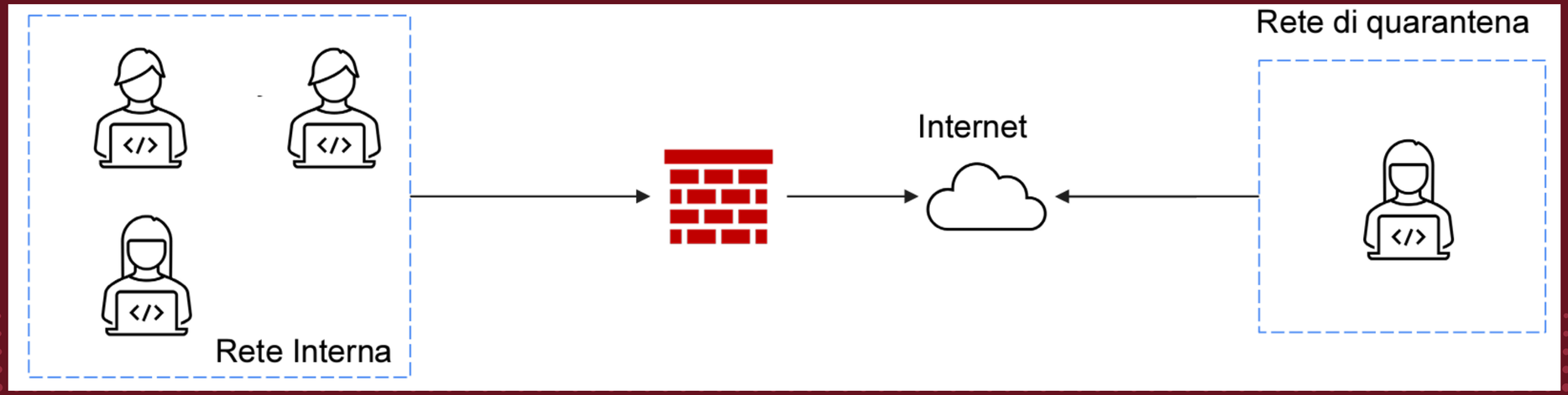
Sistema B (database compromesso)



Isolamento

Una delle tecniche preventive e strategiche per la gestione degli incidenti di sicurezza sulla rete è la «**segmentazione**», che risulta essere particolarmente utile anche nella fase di contenimento di un incidente in corso. La segmentazione permette di separare il sistema B dagli altri computer sulla rete, creando una rete ad hoc, che viene chiamata generalmente «**rete di quarantena**».

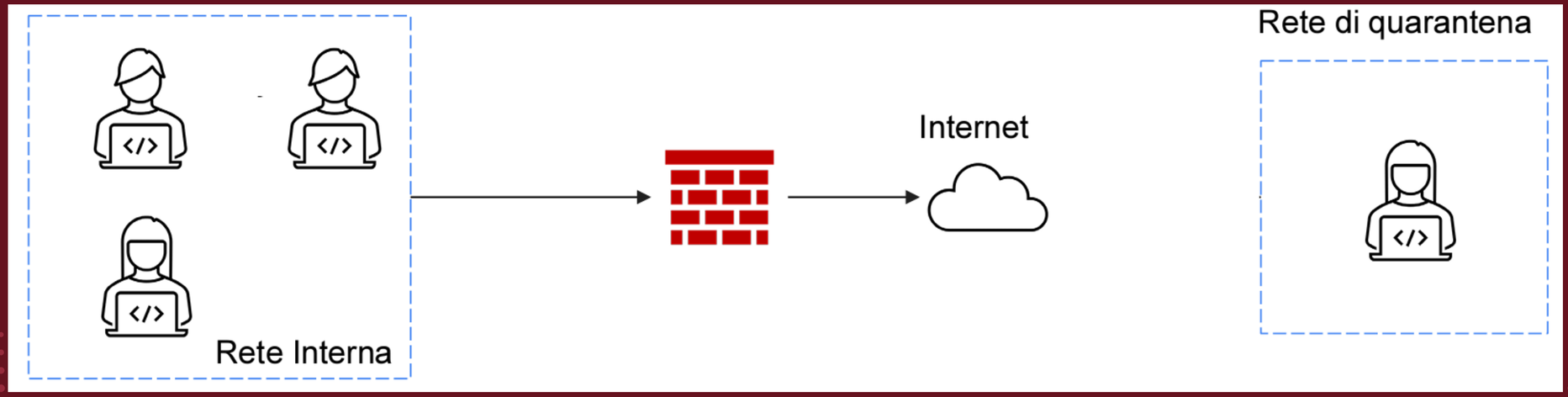
L'isolamento consiste nella disconnessione del sistema infetto dalla rete, per restringere l'accesso alla rete interna da parte dell'attaccante. In questo caso, però. l'attaccante ha ancora accesso al sistema B infetto tramite internet



Rimozione

Ci sono casi in cui l'isolamento non è sufficiente a contrastare l'evento. In questi casi si procede con una tecnica di contenimento ancora più stringente: la completa rimozione del sistema dalla rete sia interna sia da internet.

Con la rimozione, l'attaccante non avrà accesso né alla rete interna né alla macchina infettata.



Conclusioni – Purge e Destroy

A valle delle attività di contenimento, il tema CSIRT deve passare alla fase di rimozione dell'incidente.

In questa fase lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell'incidente all'interno della rete o sui sistemi. Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, inizia la fase di recupero.

Durante la fase di recupero, ci si trova spesso ad overgestire lo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso.

Possiamo individuare tre opzioni per la gestione dei media contenenti informazioni sensibili:

- **Clear**: il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche».
- **Purge**: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi;
- **Destroy**: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecnichedi laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione.