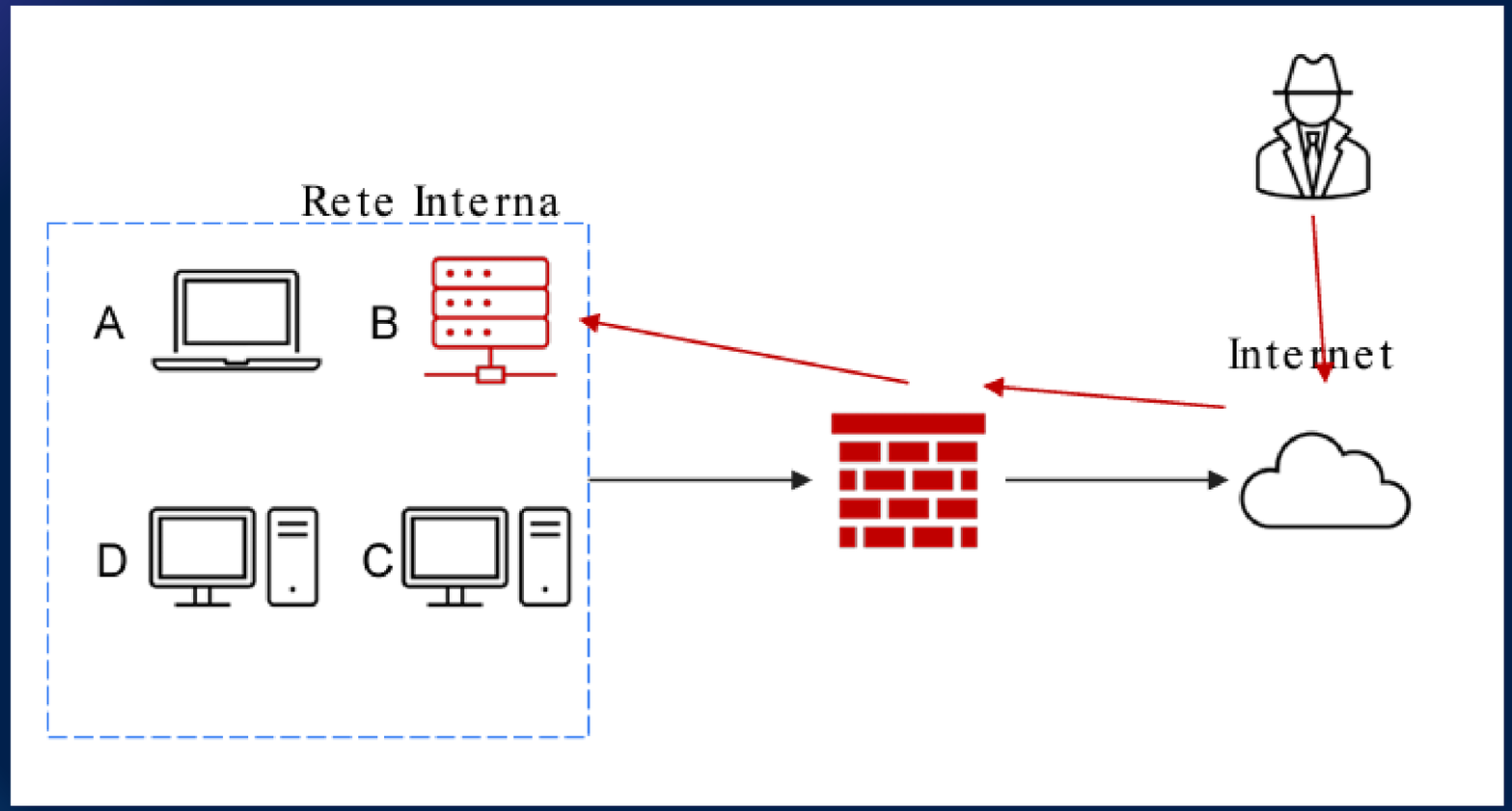
CSIRT

Piano di risposta agli incidenti
(Computer Security Incident Response Team).


Rete Interna
A
B
D
C
Internet

ISOLAMENTO

L’isolamento è una tecnica utilizzata per la gestione degli incidenti.
Consiste nella disconnessione dal sistema infetto della rete, per restringere ancora maggiormente l’ accesso alla rete interna da parte dell’ attaccante.

RIMOZIONE

CSIRT deve passare alla fase di rimozione dell’incidente.

La “rimozione” è una tecnica di contenimento più stringente, consiste nella rimozione del sistema dalla rete sia interna sia internet. In tal modo l’attaccante non avrà né accesso alla rete interna né alla macchina infettata.

GESTIONE DEI MEDIA CONTENENTI INFORMAZIONI SENSIBILI:

Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili,ma anche tecniche di rimozione fisica come l’ utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi;

GESTIONE DEI MEDIA CONTENENTI INFORMAZIONI SENSIBILI:

Clear: il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche».
Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset»per riportare il dispositivo nello stato iniziale.

GESTIONE DEI MEDIA CONTENENTI INFORMAZIONI SENSIBILI:

Destroy: è l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili.
Qui si utilizzano tecniche di laboratorio come la disintegrazione dei media ad alte temperature e trapanazione.
Questo metodo è il più efficace per rendere le informazioni inaccessibili ma è anche quello con costi più elevati.