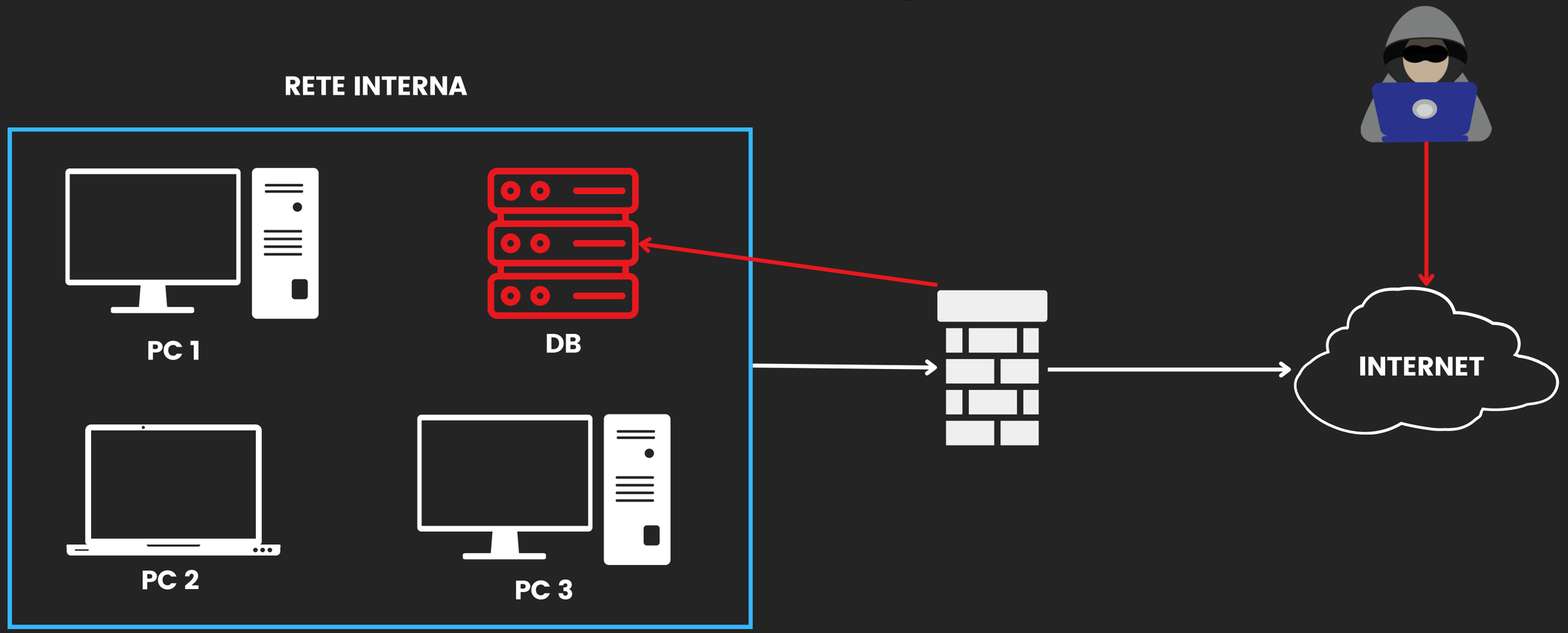
INCIDENT RESPONSE EPICODE

Giovanni Pisapia

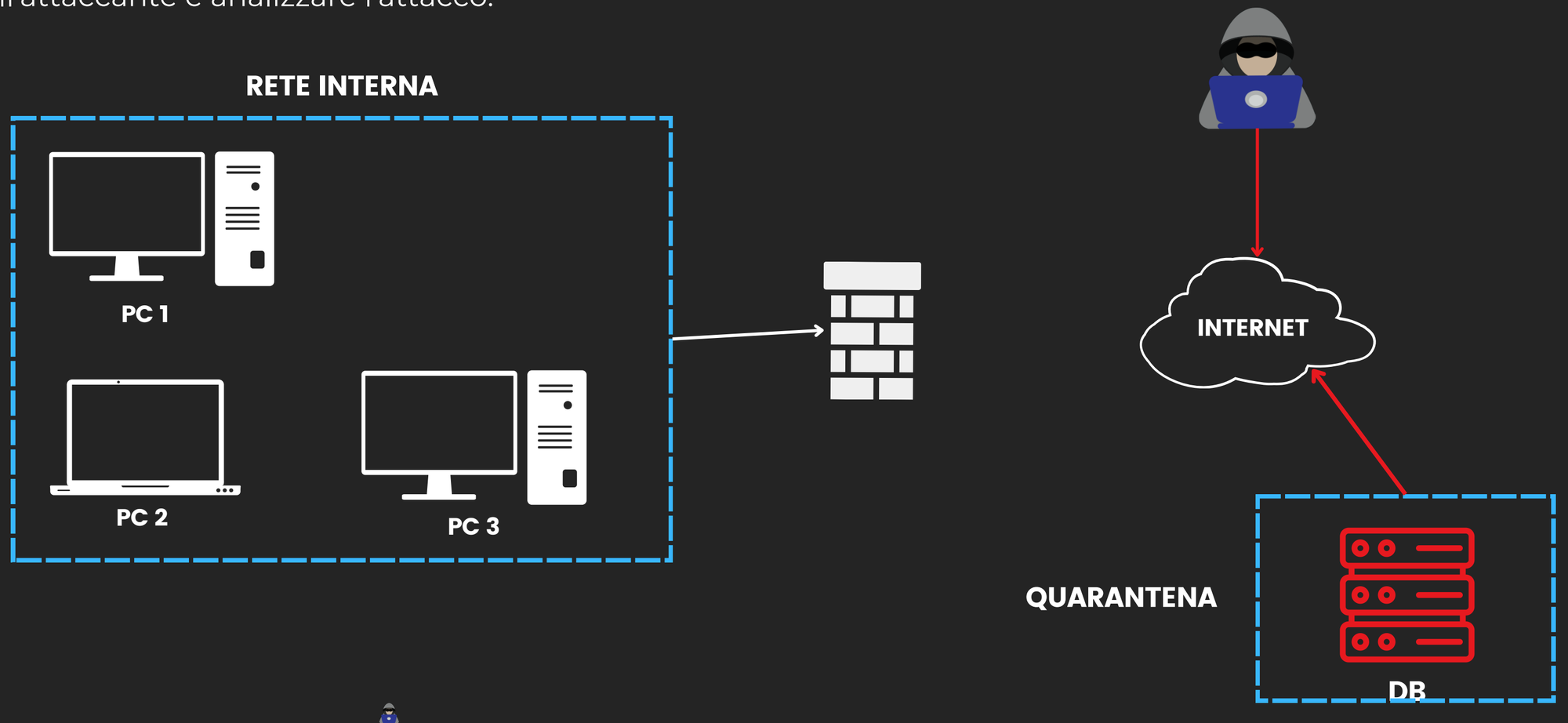
SCENARIO DI ATTACCO

Nell' esercizio di oggi ci veniva chiesto di isolare un database che era stato interamente compromesso da un attaccante che era riuscito ad entrare da internet. Il nostro compito come parte del team CSIRT era di mostrare le tecniche di isolamento e di rimozione.



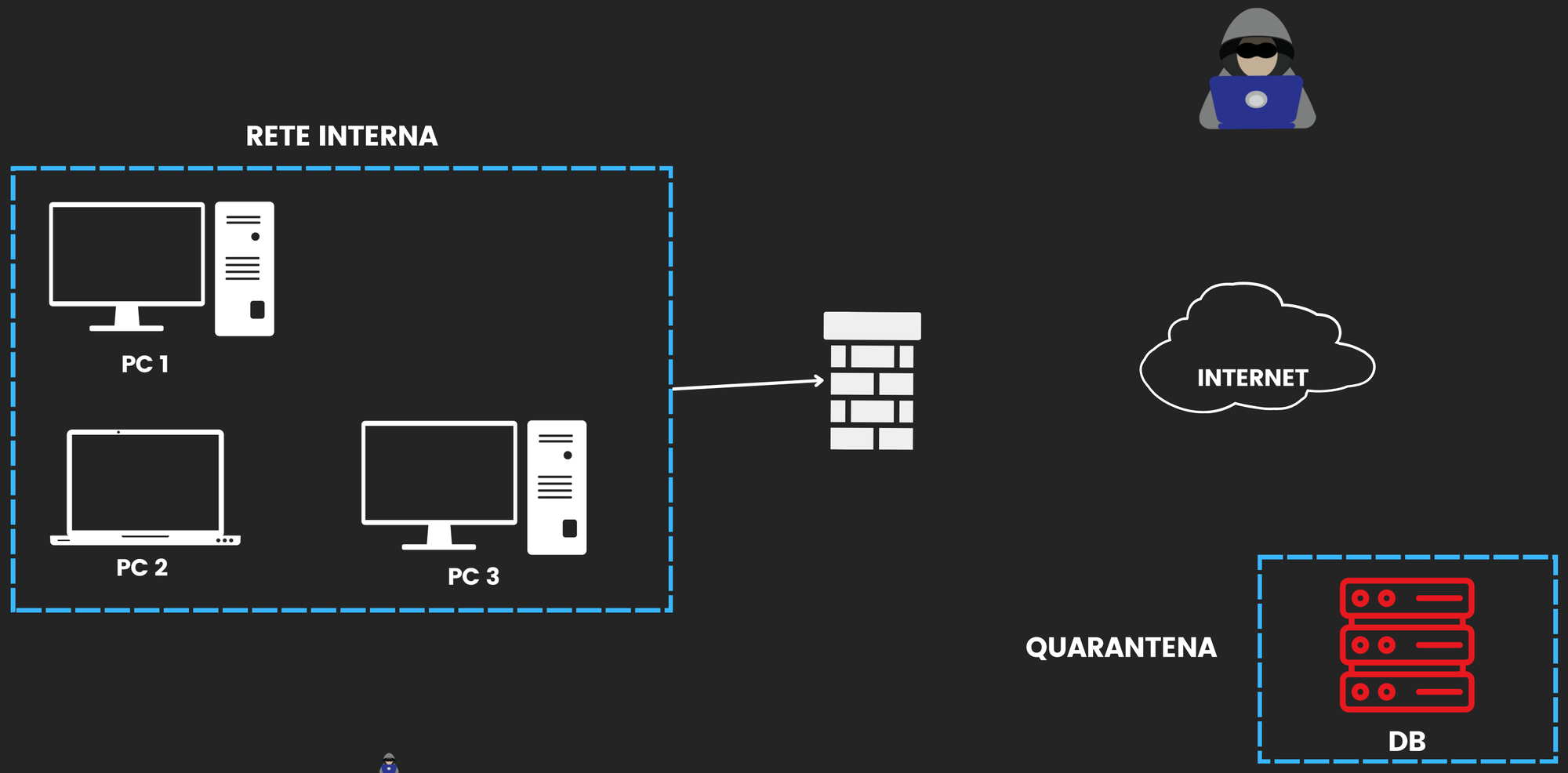
ISOLAMENTO

L'isolamento viene effettuato immediatamente dopo aver rilevato l'attacco per limitare l'accesso dell'attaccante al sistema compromesso. Ciò può essere fatto interrompendo la connessione Internet o disconnettendo fisicamente il dispositivo dalla rete interna e mettendolo in quarantena. L'obiettivo principale dell'isolamento è prevenire ulteriori danni e impedire all'attaccante di continuare a interagire con il sistema compromesso. Tuttavia, l'attaccante potrebbe ancora avere accesso locale al sistema se è già infiltrato, consentendo al team di CSIRT di studiare l'attaccante, raccogliere informazioni sul metodo di attacco e prendere le necessarie contromisure. Si potrebbe fare un'analogia: quando l'antivirus rileva un virus, lo mette in quarantena per isolarlo e studiarlo. Allo stesso modo, isoliamo un sistema compromesso per limitare l'accesso dell'attaccante e analizzare l'attacco.



RIMOZIONE

Dopo aver isolato il sistema, dovremmo rimuoverlo dalla rete o spegnerlo, a seconda della gravità dell'attacco. Se l'attacco è in corso e il sistema non può essere prontamente ripristinato, la rimozione fisica del dispositivo potrebbe essere necessaria per garantire la sicurezza degli altri sistemi nella rete.



GESTIONE DEI MEDIA CONTENTI 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. Esempio: Supponiamo di avere un dispositivo mobile come uno smartphone. Per eseguire un'operazione "Clear", potremmo eseguire un ripristino di fabbrica (factory reset) sul dispositivo. Questa procedura cancella tutti i dati presenti sul dispositivo, ripristinando le impostazioni di fabbrica e rimuovendo le informazioni personali.

PURGE

Si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi
Esempio:Consideriamo un disco rigido di un computer. Per eseguire un'operazione "Purge", potremmo utilizzare un software specializzato che sovrascrive ripetutamente i dati presenti sul disco con valori casuali o cifrati. Questo processo logico rende le informazioni precedentemente presenti sul disco praticamente inaccessibili. Inoltre, potremmo applicare una tecnica fisica come l'uso di potenti magneti per danneggiare in modo irreversibile il disco rigido, rendendo i dati completamente inaccessibili.

DESTROY

L'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore. Esempio: mmaginiamo un vecchio disco rigido di un server contenente dati altamente sensibili. Per eseguire un'operazione "Destroy", potremmo optare per un approccio più drastico. Ad esempio, potremmo inviare il disco a un'azienda specializzata in smaltimento sicuro dei dati, che utilizzerà tecniche di laboratorio come la disintegrazione o la polverizzazione ad alte temperature per distruggere fisicamente il disco e rendere le informazioni irrecuperabili.