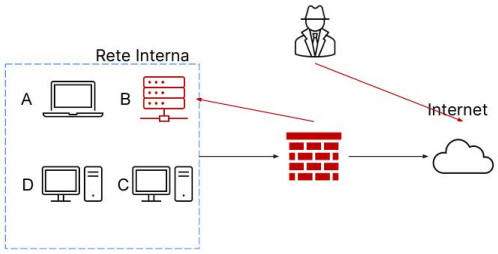
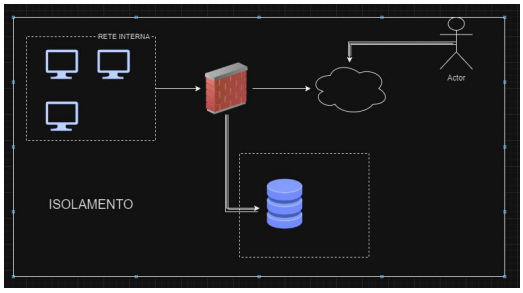
INCIDENT RESPONSE

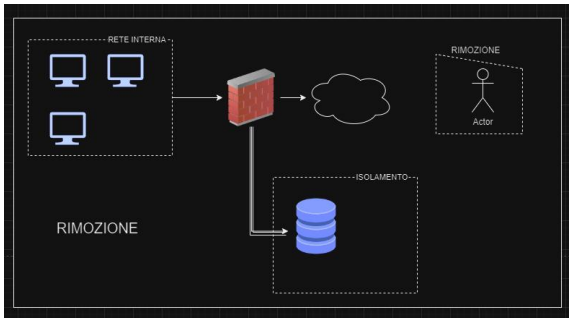
In questo esercizio un attacco ha avuto successo e dobbiamo rispondere al evento.



Con la tecnica di isolamento possiamo notare che isolando il database (B), l'attaccante ha ancora accesso alla rete interna grazie alla connessione internet, il database è al sicuro e non potra piu infettare o essere attaccato, ma l'attacante ha ancora delle possibilita di agire.



Mentre che nel isolamento togliamo di mezzo l'attacante e gli impediamo di mantenere una connesssione con noi.



Il database è stato messo in isolamento perche è compromesso/contaminato e si procedera alla procedura di recupero

PURGE, è un metodo che si utilizza per ripulire in modo logico e fisico, quindi oltre a sovracrivere o resettare il dispositivo, si utilizzano fonti esterne per ripuliere, come magnitei potenti.

DESTROY, è un metodo che include quello che fa PURGE, ma va in maniera piu aggressiva. Usando metodi li laboratorio come disintegrazione e polverizzazione, rendendolo il metodo piu efficace ma comporta costi abbastanza elevati.