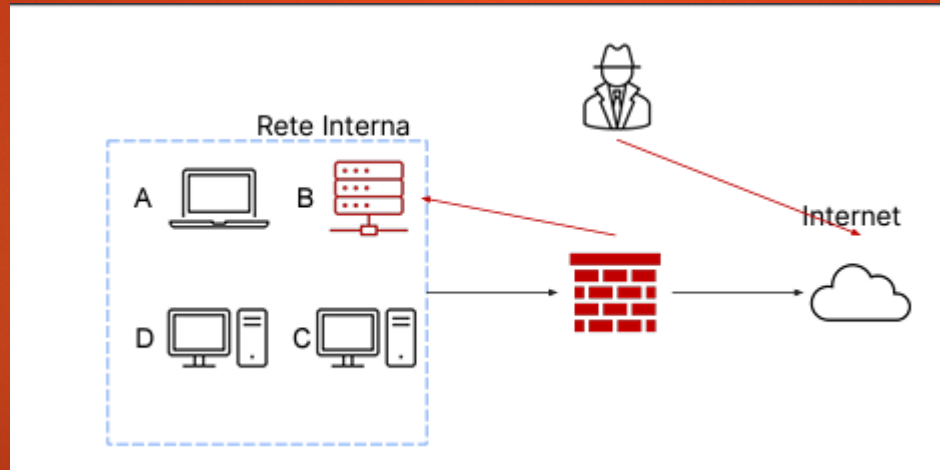
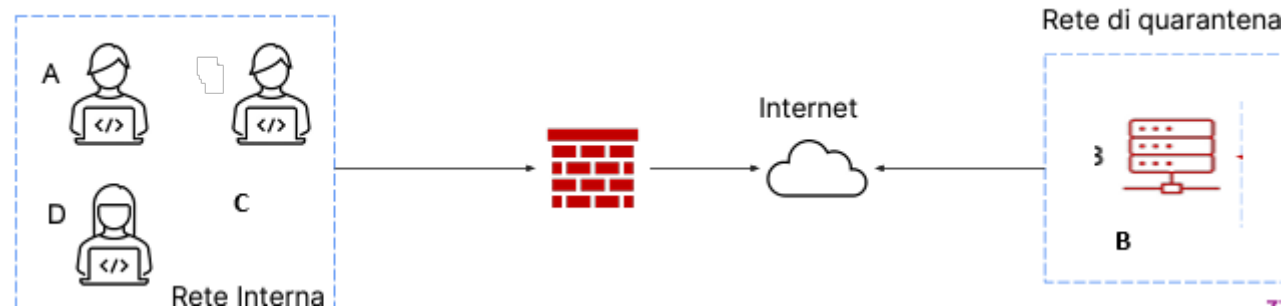


S914

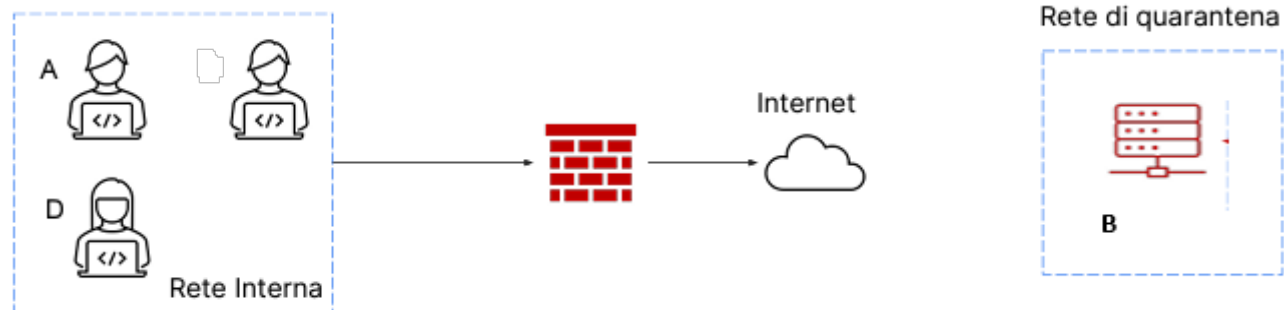
CON RIFERIMENTO ALLA FIGURA IN SLIDE , IL SISTEMA B (UN DATABASE CON DIVERSI DISCHI PER LO STORAGE) È STATO COMPROMESSO INTERAMENTE DA UN ATTACCANTE CHE È RIUSCITO A BUCARE LA RETE ED ACCEDERE AL SISTEMA TRAMITE INTERNET. L'ATTACCO È ATTUALMENTE IN CORSO E SIETE PARTE DEL TEAM DI CSIRT. RISPONDERE AI SEGUENTI QUESITI. MOSTRATE LE TECNICHE DI: I) ISOLAMENTO II) RIMOZIONE DEL SISTEMA B INFETTO SPIEGATE LA DIFFERENZA TRA PURGE E DESTROY PER L'ELIMINAZIONE DELLE INFORMAZIONI SENSIBILI PRIMA DI PROCEDERE ALLO SMALTIMENTO DEI DISCHI COMPROMESSI

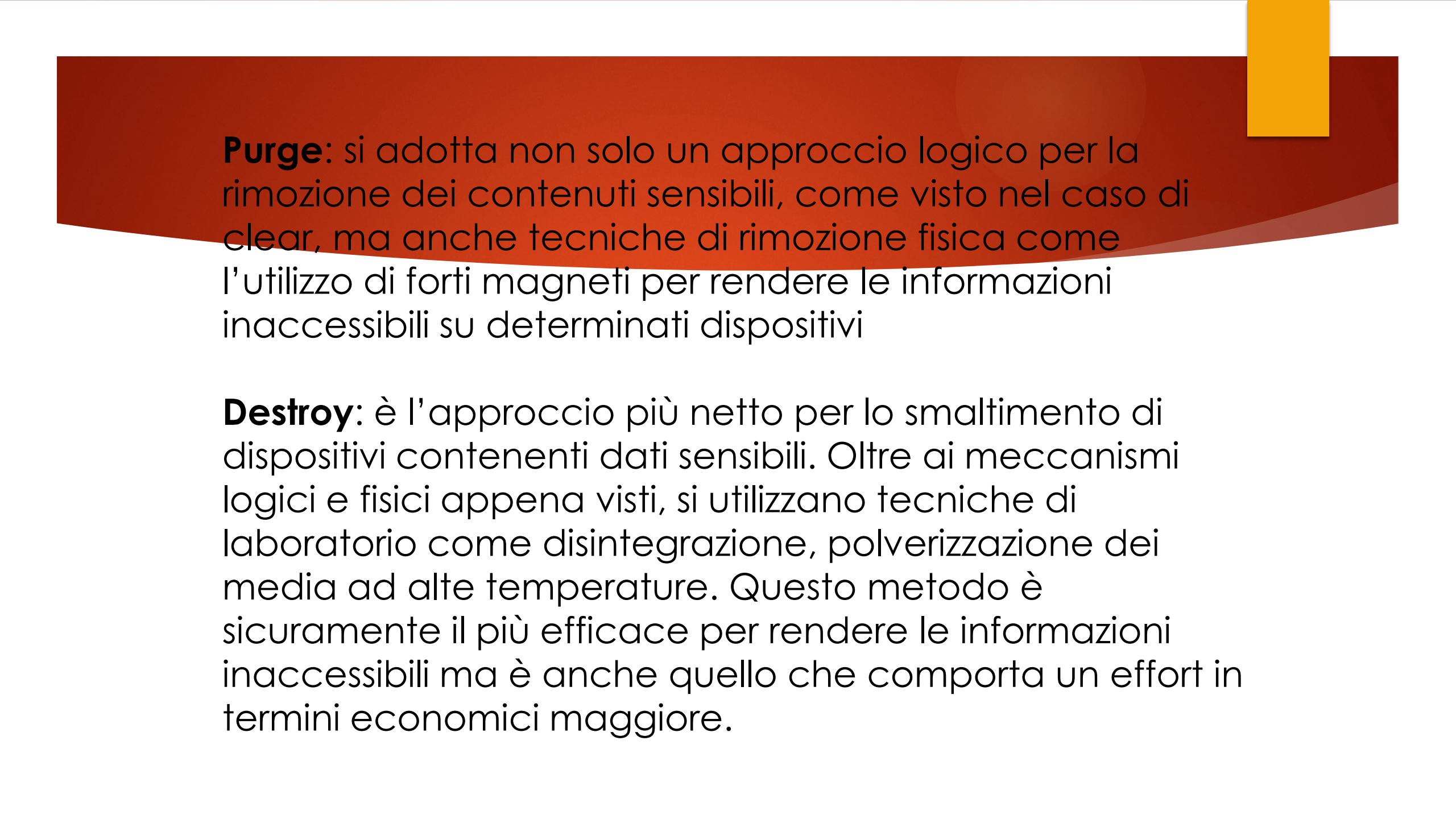


L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. Notate che in questo scenario l'attaccante ha ancora accesso al sistema B tramite internet. C A D Rete interna



Ci sono casi in cui l'isolamento non è ancora abbastanza. In questi casi si procede con la tecnica di contenimento più stringente, ovvero la completa **rimozione** del sistema dalla rete sia interna sia internet. In quest'ultimo scenario l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata. 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. Questa attività può includere ad esempio rimuovere eventuali backdoor installate da un malware, oppure ripulire dischi e chiavette usb compromesse. La fase di rimozione dipende molto da che tipo di incidente di sicurezza è in corso





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

Destroy: è 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. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.