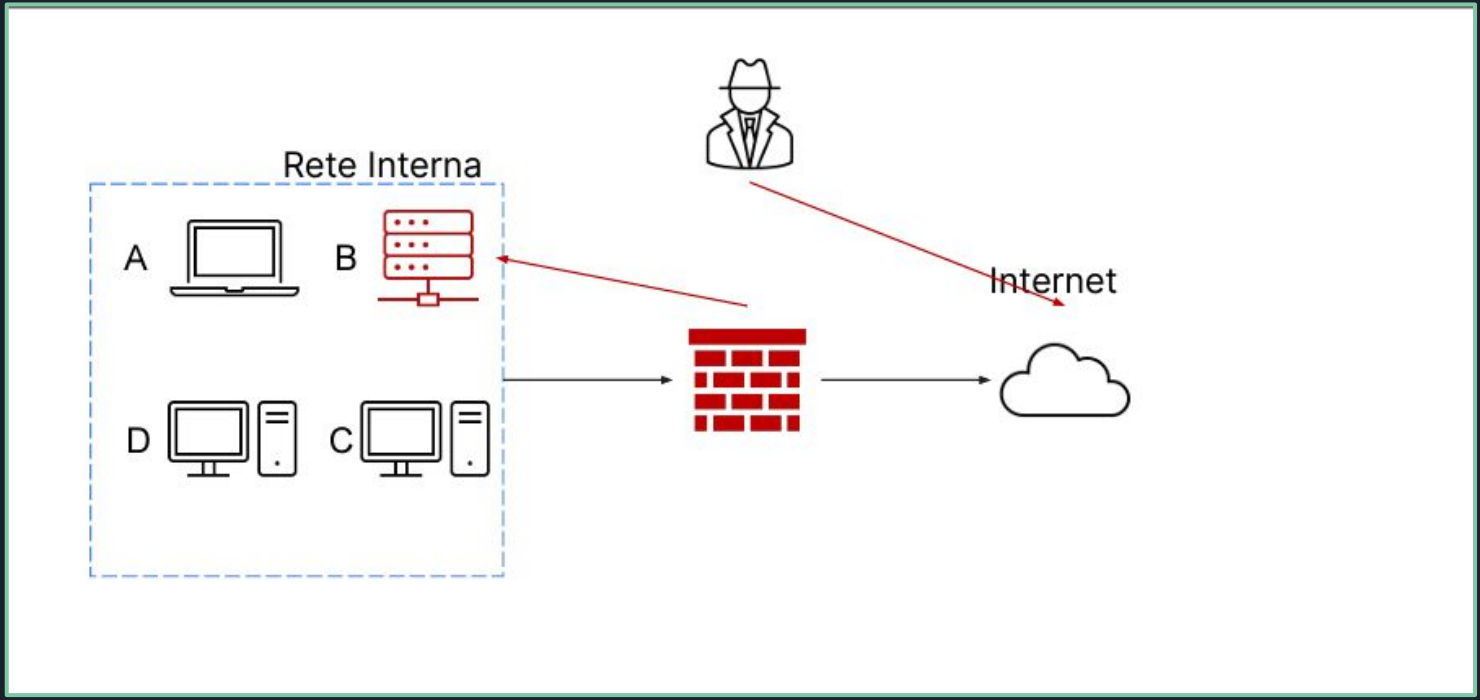
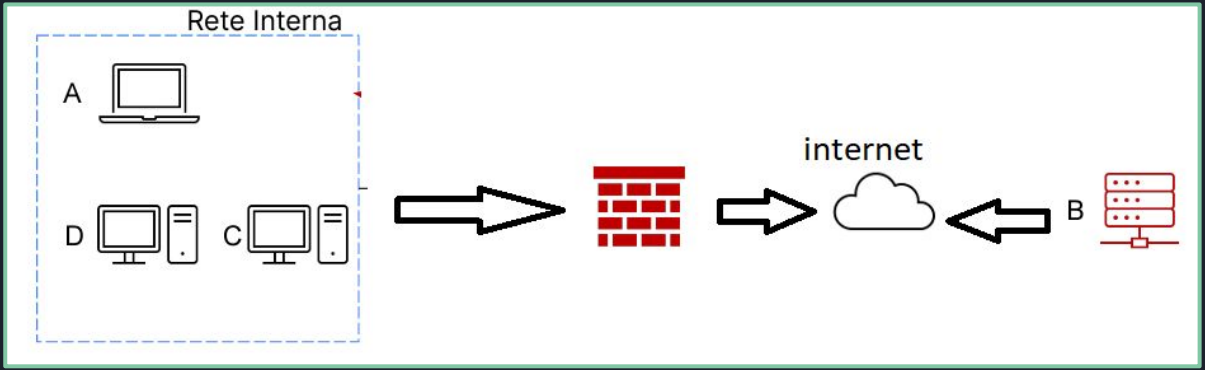
INCIDENT RESPONSE



Kamenica Kristiano

ISOLAMENTO



La fase di contenimento in un piano di risposta agli incidenti è cruciale per limitare i danni causati dall'attacco. Dopo l'analisi dell'incidente, si cerca di isolare l'area colpita per evitare che il problema si diffonda.

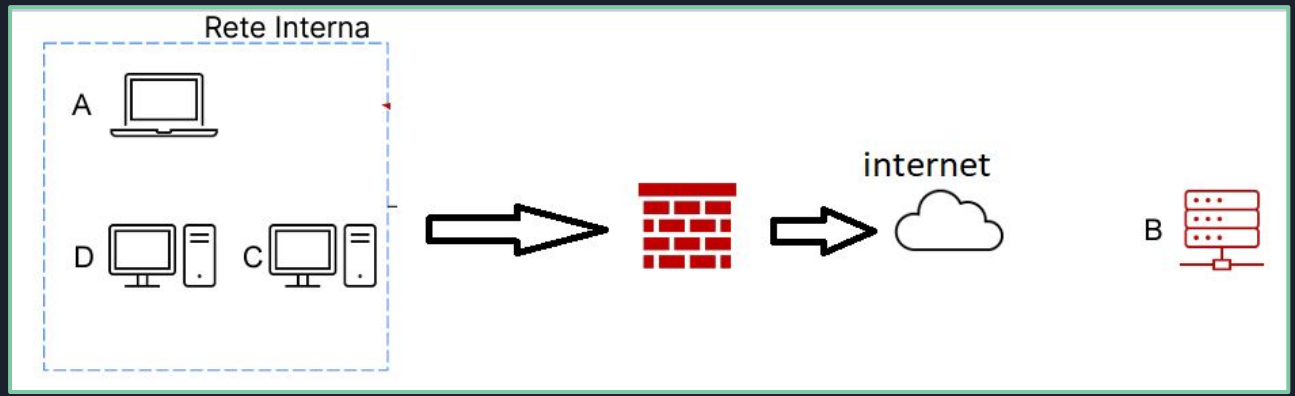
Una tecnica efficace per questo è la segmentazione della rete, che divide la rete in LAN o VLAN separate. In questo modo, il sistema compromesso viene separato dagli altri nodi, creando una "rete di quarantena" che impedisce al malware di diffondersi.

Tuttavia, quando è necessario un maggiore controllo, si ricorre all'isolamento: si disconnette completamente il sistema infetto dalla rete per limitare ulteriormente l'accesso dell'attaccante alla rete interna. Questo passaggio assicura che l'incidente sia confinato e non possa causare danni aggiuntivi alla rete o ai sistemi.

RIMOZIONE DEL SISTEMA INFETTO

Tuttavia, ci sono casi in cui l'isolamento potrebbe non essere sufficiente. In questi scenari più critici, si ricorre alla tecnica più stringente di completa rimozione del sistema dalla rete, sia interna sia internet.

In questo modo, l'attaccante non ha più accesso né alla rete interna né alla macchina infettata.



PURGE ,DESTROY AND CLEAN

- ***PURGE*** : Questo metodo non solo adotta un approccio logico per eliminare i contenuti sensibili, come nel caso della cancellazione, ma include anche tecniche di rimozione fisica. Ad esempio, si possono impiegare potenti magneti per rendere le informazioni irrecuperabili su determinati dispositivi.

- ***DESTROY*** : Questo approccio rappresenta la soluzione più radicale per lo smaltimento dei dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici menzionati in precedenza, coinvolge anche tecniche di laboratorio avanzate come la disintegrazione o la polverizzazione dei supporti a temperature elevate. Sebbene questo metodo sia estremamente efficace nel rendere le informazioni irrecuperabili, comporta anche un costo economico significativo. Inoltre, può richiedere più tempo ed energie rispetto al purge.

- ***CLEAR*** : Per ripulire completamente il database infetto, si adotta un approccio logico attraverso tecniche di "clear". Questo significa che il contenuto del dispositivo viene eliminato utilizzando processi come sovrascrittura ripetuta dei dati o il ripristino alle impostazioni di fabbrica. Ad esempio, potrebbe essere eseguita una serie di operazioni di lettura e scrittura per sovrascrivere più volte il contenuto del database, o potrebbe essere utilizzata la funzione di "factory reset" per riportare il database allo stato iniziale. Questo processo aiuta a garantire che il database sia completamente pulito e che non rimangano tracce di dati sensibili.