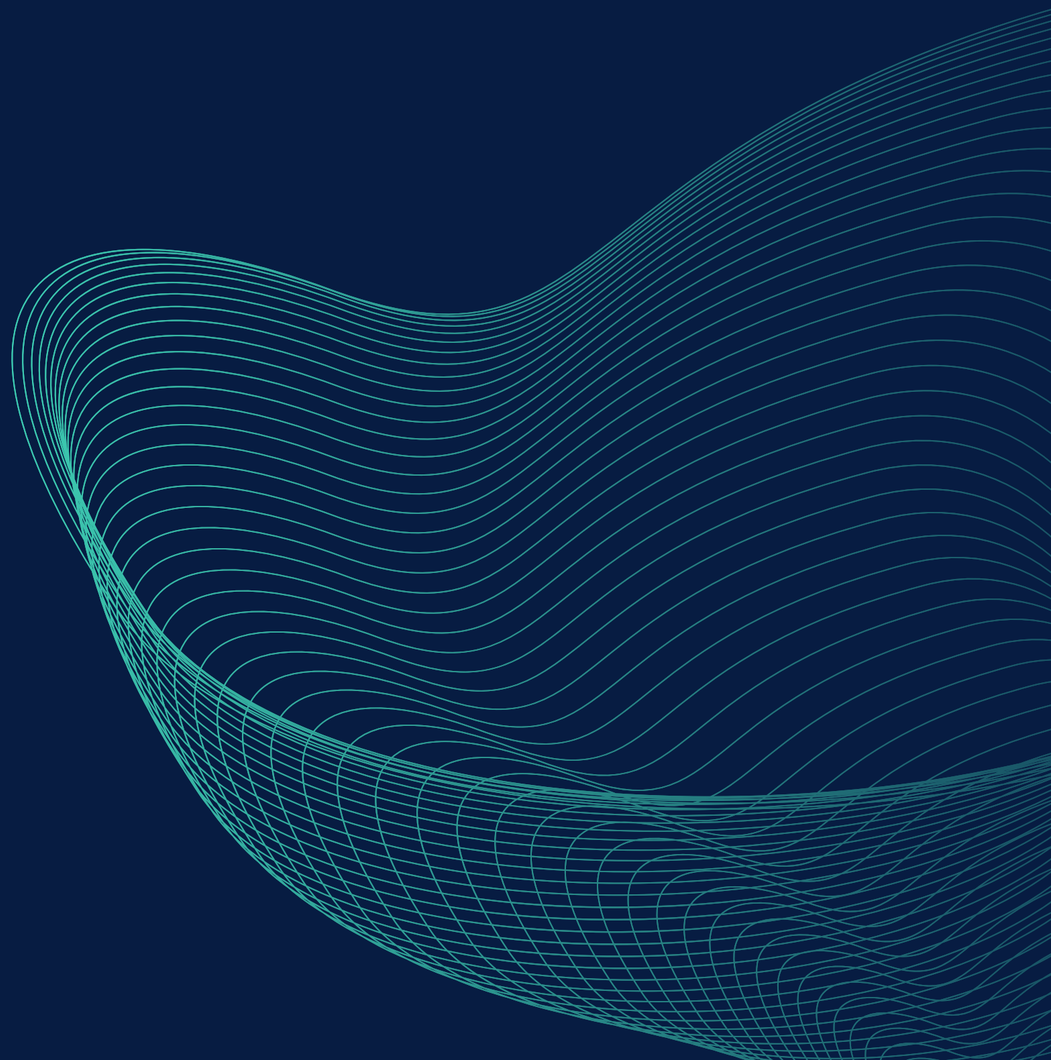
S9/L4

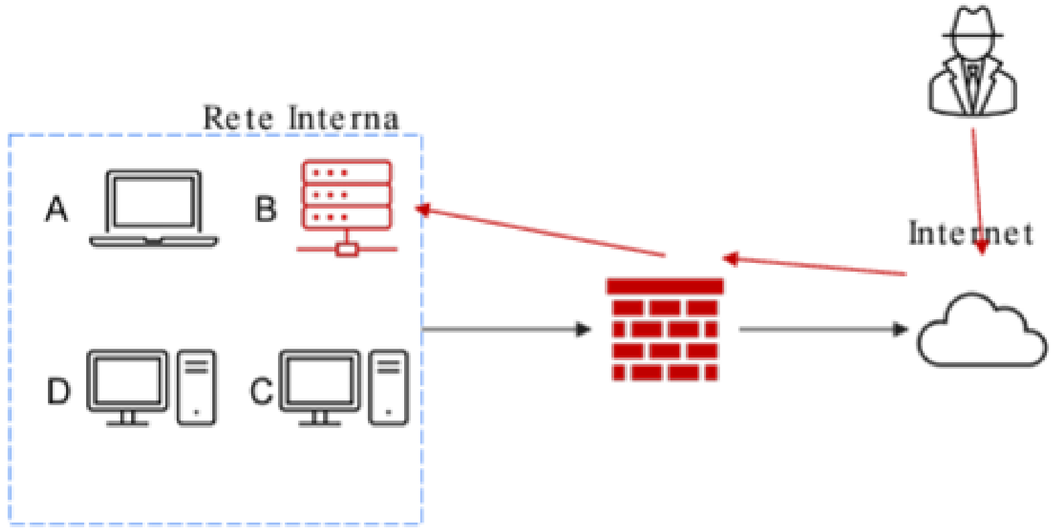
Incident response



Traccia

Con riferimento alla figura, 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. **Indicare anche Clear**

Incident Response

Le aziende possono adottare precauzioni e preparare al meglio la loro protezione perimetrale per gli incidenti riguardanti la sicurezza, ma le possibilità di incidenti non sono mai zero.
Le aziende quindi creano un piano in risposta agli incidenti chiamato CSIRT (Computer Security Response Team).
L'Incident Response (IR) è il processo organizzato di gestione e risposta e coinvolge una serie di azioni coordinate per identificare, contenere, eliminare e recuperare da incidenti che compromettono la sicurezza delle informazioni e delle infrastrutture IT.

1.Preparazione

Include la formazione del personale, l'acquisizione degli strumenti necessari e la definizione di politiche e procedure per rispondere agli incidenti.

2. Identificazione

Riconoscimento dell'incidente attraverso il monitoraggio continuo dei sistemi e delle reti, analisi dei log e delle anomalie.

3.Contenimento:

Misure immediate per limitare l'impatto dell'incidente. Questo può includere l'isolamento delle parti compromesse del sistema e l'applicazione di patch temporanee.

4.Eradicazione:

Rimozione delle cause dell'incidente, come malware o accessi non autorizzati, e implementazione di misure per prevenire future compromissioni.

5.Recupero:

Ripristino dei sistemi e dei dati, e verifica che siano nuovamente sicuri e operativi. Può includere il ripristino da backup e il monitoraggio post-incidente.

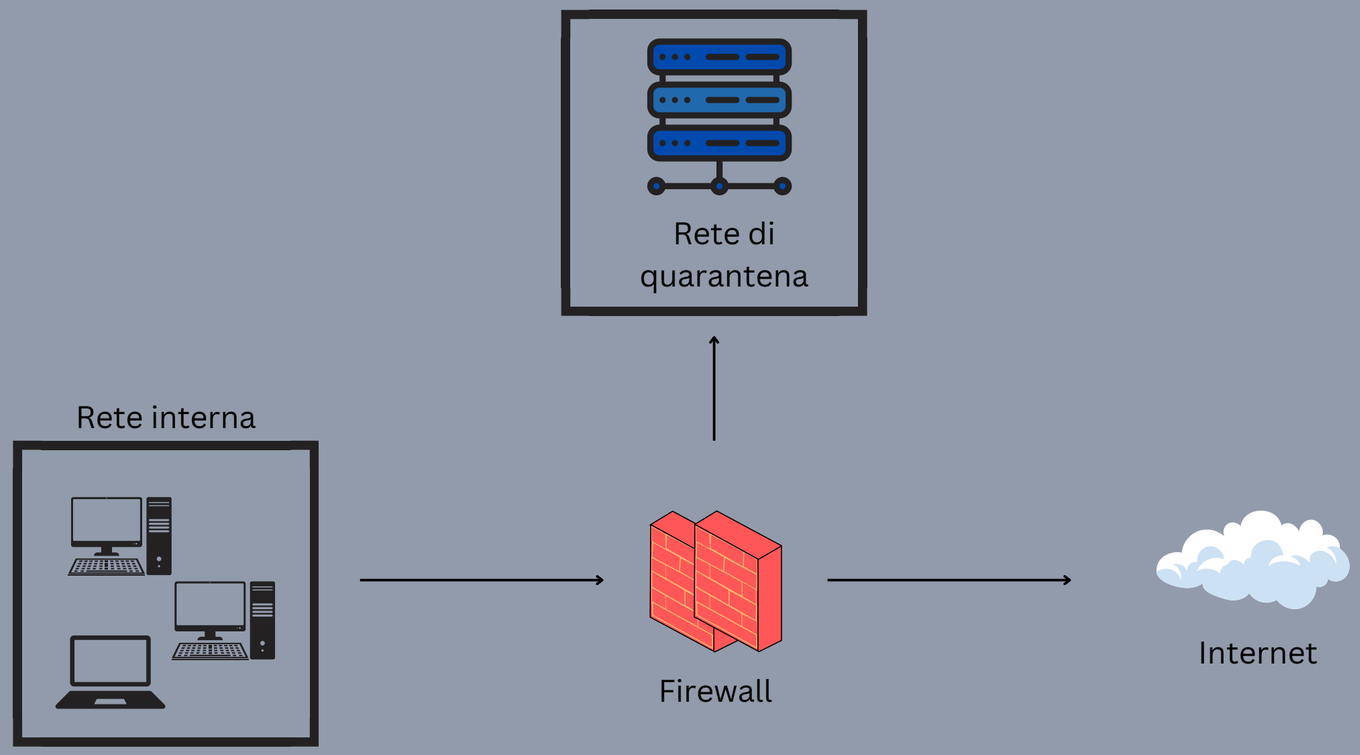
6.Lezioni apprese:

Analisi post-incidente per identificare le carenze nelle risposte e migliorare le strategie future. Documentazione dettagliata dell'incidente e delle azioni intraprese.

Tecniche di contenimento

Segmentazione

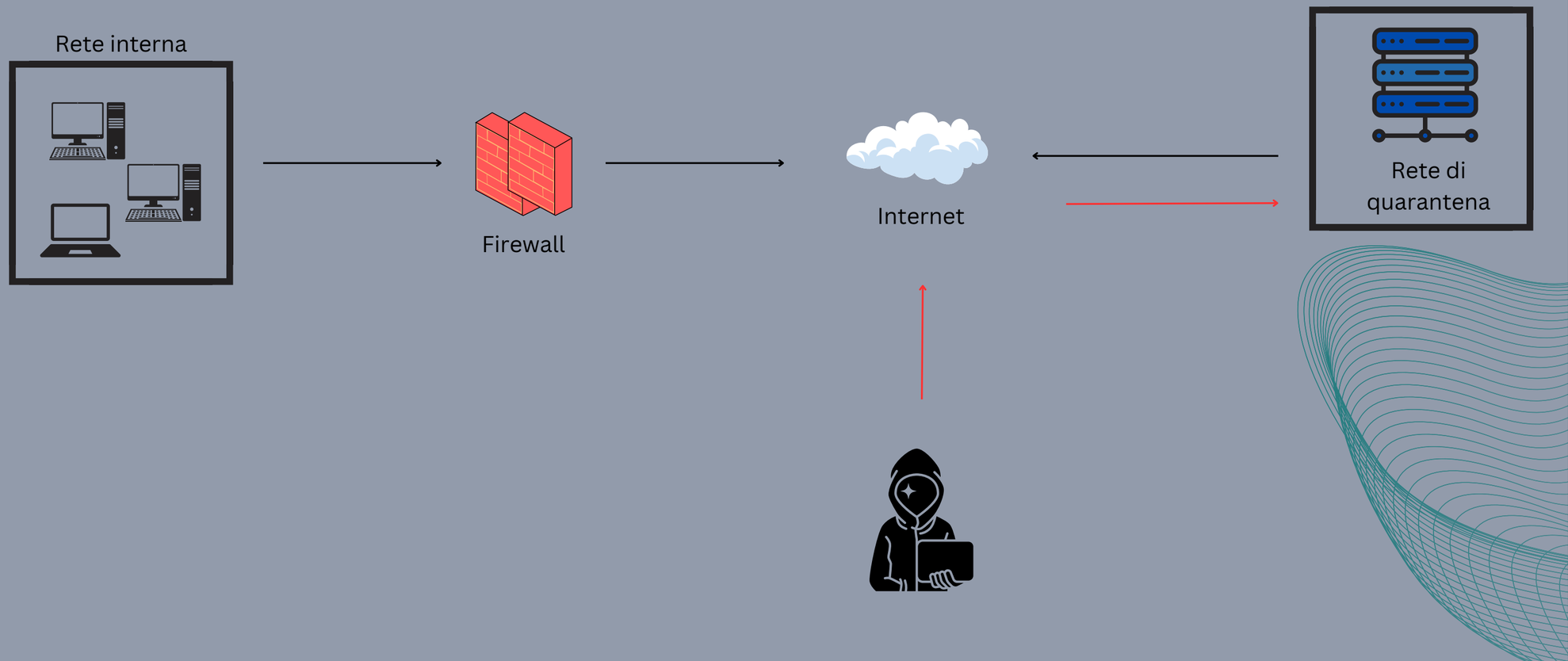
La segmentazione consiste nel dividere la rete o i sistemi in segmenti più piccoli per limitare la diffusione dell'incidente all'interno dell'organizzazione.
Isolandolo le parti compromesse del sistema, si limita la possibilità che l'incidente si propaghi ad altre parti della rete.
In questo modo si crea una vera e propria "Rete di Quarantena"



Tecniche di contenimento

Isolamento

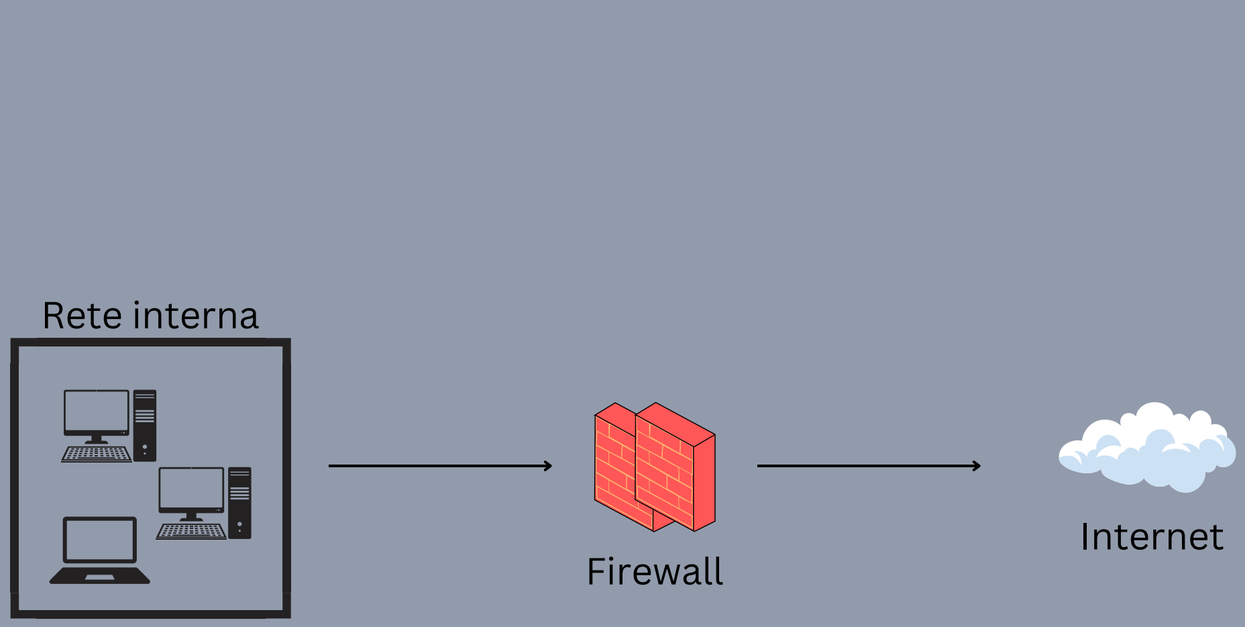
Se la segmentazione non basta, è necessario ricorrere all'isolamento.
L'isolamento consiste nella completa rimozione del sitema infetto dalla rete, Questo può essere fatto fisicamente (scollegando i cavi di rete) o logicamente (configurando il firewall o il router per bloccare tutto il traffico in entrata e uscita da B).



Rimozione

Rimozione

Se nessuna delle due tecniche precedenti ha avuto effetto, si può ricorrere alla rimozione.
La rimozione completa del sistema B sia dalla rete che da intenet, in questo modo l'attaccante non avrà nè accesso alla rete interna nè tantomeno alla macchina infettata.
questo sistema ci permette anche di poterci assicurare che il sistema sia ripulito prima di rimetterlo in rete.



Rimozione

Informazioni sensibili

Clear

- **Definizione**: Rimozione dei dati tramite software o comandi hardware, rendendo i dati inaccessibili a livello di utente, ma potenzialmente recuperabili con tecniche avanzate.
- Scenario: Utilizzato quando il supporto di memorizzazione deve essere riutilizzato in ambienti con minore rischio di compromissione della sicurezza.
- **Esempio**: Utilizzo del comando delete o format su un filesystem.

Purge

- **Definizione**: Rimozione dei dati in modo da rendere molto difficile, se non impossibile, il recupero dei dati anche con tecniche avanzate. Solitamente comporta la sovrascrittura dei dati con dati casuali.
- **Scenario**: Utilizzato quando il supporto di memorizzazione deve essere riutilizzato ma con una maggiore garanzia di sicurezza.
- **Esempio**: Utilizzo di software specializzati che sovrascrivono l'intero disco con dati casuali (ad esempio, il comando shred in Linux).

Destroy

- **Definizione**: Distruzione fisica del supporto di memorizzazione in modo da renderlo inutilizzabile e i dati completamente irrecuperabili.
- Scenario: Utilizzato quando il supporto di memorizzazione deve essere smaltito in modo sicuro e definitivo.
- **Esempio**: Triturazione, smagnetizzazione, fusione o altri metodi fisici che distruggono il supporto di memorizzazione.