INCIDENT RESPONSE

S9/L4

ELEONORA VIOLA

TABLE OF CONTENT

INTRODUCTION

- Traccia:

Con riferimento alla figura in slide 4, 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.

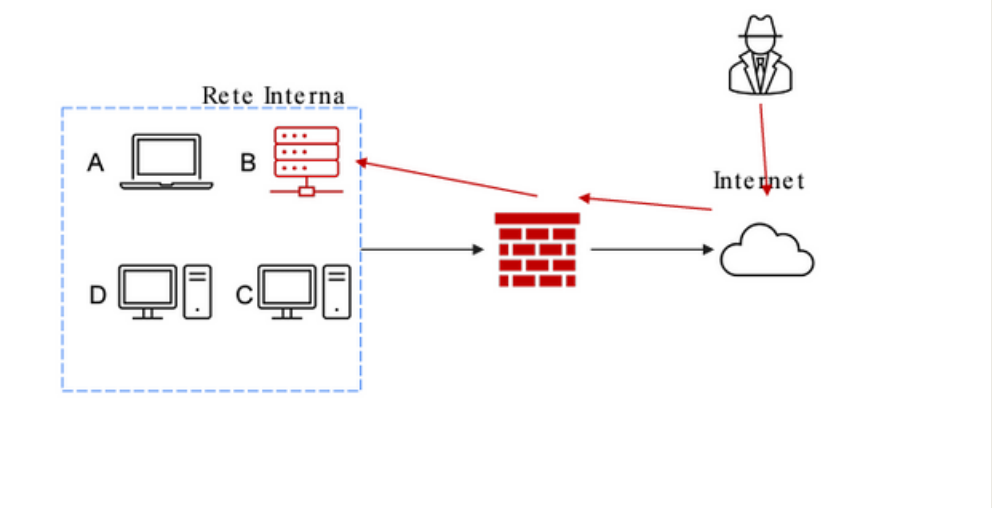
• Mostrate le tecniche di:
I) Isolamento II) Rimozione del sistema B infetto

• Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear.

PROCEDURE

In questa immagine, il sistema B in rete è stato completamento violato da un intruso che ha avuto accesso attraverso Internet.

L'attacco prosegue e come membri del team di CSIRT (Computer Security Incident Response Team), vogliamo isolare ed eliminare il sistema B infetto e anche offrire una guida su come rimuovere le informazioni riservate dai dischi compromessi.



PROCEDURE

1.Isolamento

Disconnessione del Sistema B dalla Rete:
in primo luogo bisogna scollegare il sistema B dalla rete per interrompere qualsiasi ulteriore attività dell'attaccante.
Questo può essere fatto scollegando fisicamente i cavi di rete o disabilitando la scheda di rete (NIC) tramite il sistema operativo.

Segregazione del Sistema Compromesso:

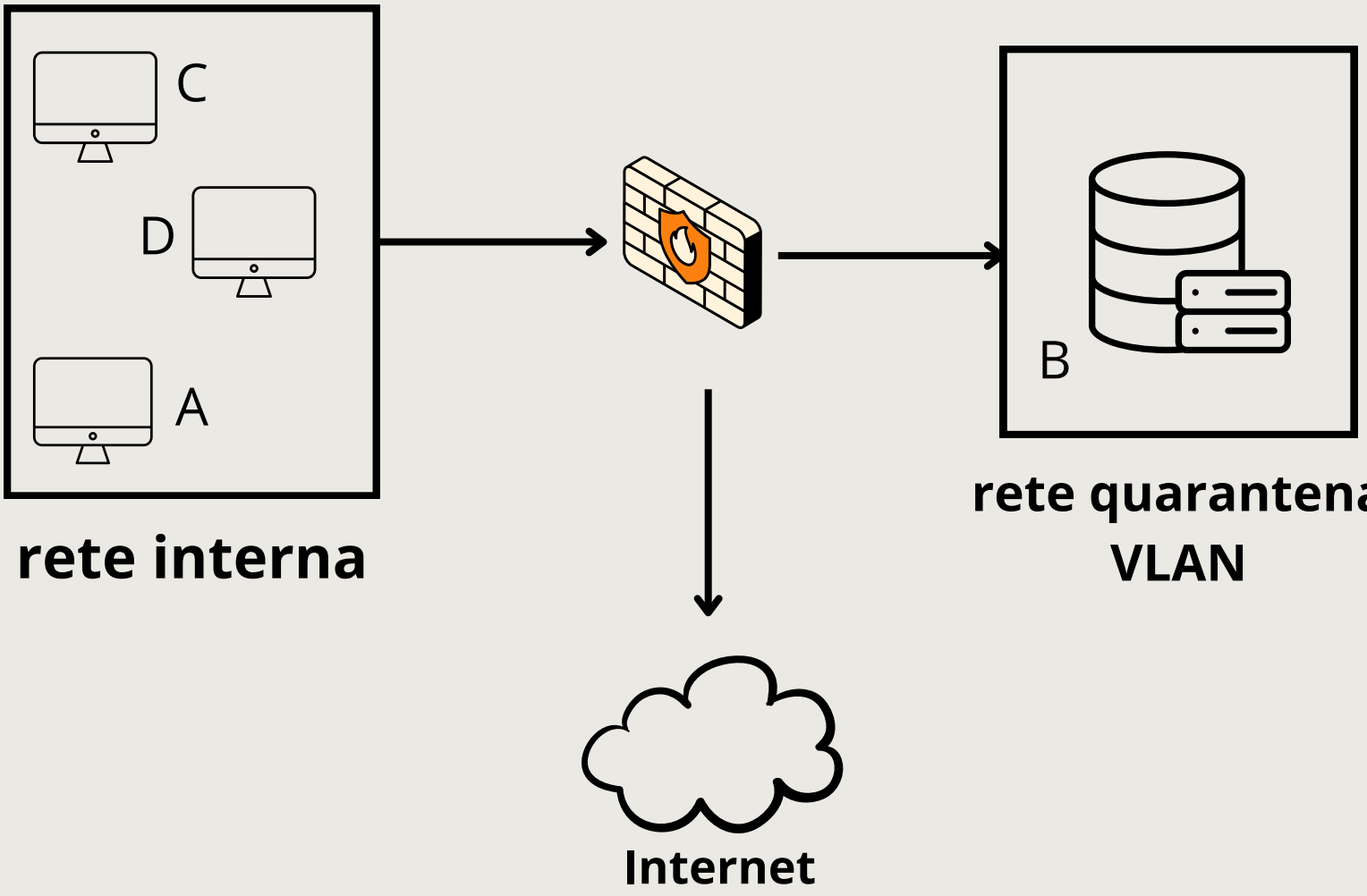
successivamente è ideale spostare il sistema B in una VLAN (Virtual Local Area Network) isolata o in un ambiente contenitore.
Questo passo è fondamentale per evitare che l'attacco si propaghi ad altri sistemi della rete interna.

2. Rimozione del Sistema B Infetto

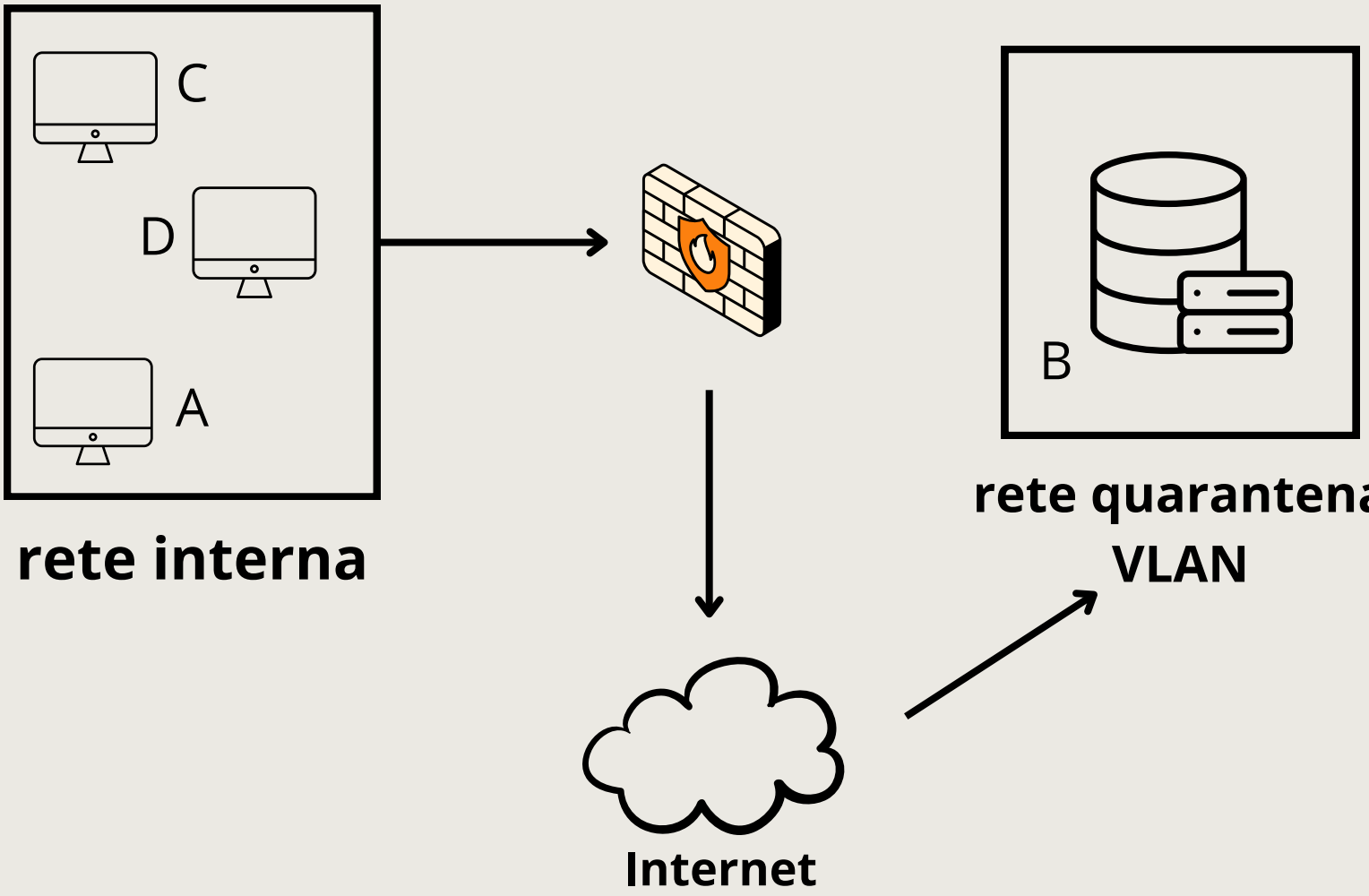
Spegnimento del Sistema:
in maniera da evitare possibili corruzioni di dati bisogna procedere con uno spegnimento controllato del sistema B.
Se lo spegnimento controllato non è fattibile, procedere con uno spegnimento forzato (hard shutdown).

Rimozione Fisica:
mettere in sicurezza il sistema B in un ambiente controllato, come un armadio o una stanza sicura, per evitare accessi non autorizzati.
Questo assicura che l'attaccante non possa accedere fisicamente al sistema per riattivarlo

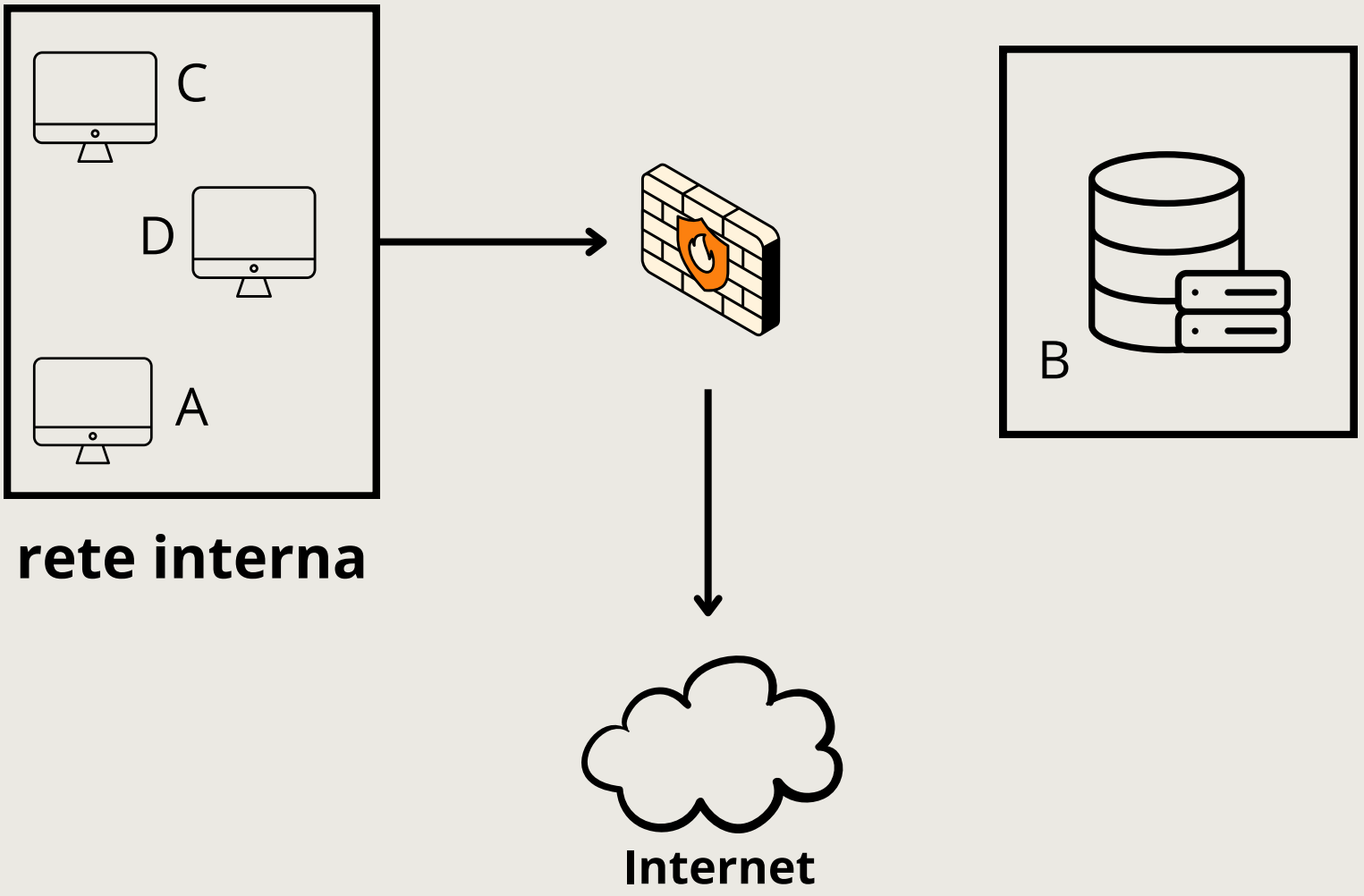
ISOLAMENTO IN UNA VLAN SEPARTA



ISOLAMENTO DALLA RETE INTERNA MA NON DA INTERNET



RIMOZIONE FISICA



PROCEDURE

Metodo Clear:

questa tecnica consiste nel sovrascrivere i dati presenti sui dischi con nuovi dati, rendendo così i dati originali irrecuperabili tramite strumenti di recupero standard.

È una pratica appropriata quando si intende riutilizzare i dischi all'interno dello stesso contesto di sicurezza.

Metodo Purge:

Purge è un metodo più avanzato che prevede l'uso di tecniche specifiche per garantire che i dati non possano essere recuperati neanche con strumenti di recupero avanzati.
Può includere la smagnetizzazione per i dischi magnetici o la cancellazione sicura delle chiavi di crittografia.

Metodo Destroy:

Questo metodo comporta la distruzione fisica dei dischi, assicurando che i dati non possano essere recuperati in alcun modo.
Le tecniche utilizzate possono includere la triturazione, la frantumazione o l'incenerimento dei dischi.

CONCLUSION

Isolando e rimuovendo il sistema B compromesso, siamo riusciti a ridurre la minaccia immediata alla rete.

È fondamentale capire le differenze tra le tecniche di Clear, Purge e Destroy per gestire in sicurezza i dati sensibili sui dischi compromessi.

Clear è ideale per il riutilizzo interno dei dischi, Purge offre una maggiore sicurezza per dati più critici, mentre Destroy garantisce la completa eliminazione dei dati, rendendo i dischi completamente inutilizzabili.

Attuando questi passaggi, assicuriamo una risposta all'incidente efficace, mantenendo intatta l'integrità e la riservatezza della rete.