S9/L4

LE POLITICHE E PROCEDURE DI RISPOSTA AGLI INCIDENTI DI SICUREZZA

Il sistema **B** è stato compromesso da un attacco esterno. Come team CSIRT, risponderemo con tecniche di isolamento, rimozione e gestione sicura dei dati sensibili.

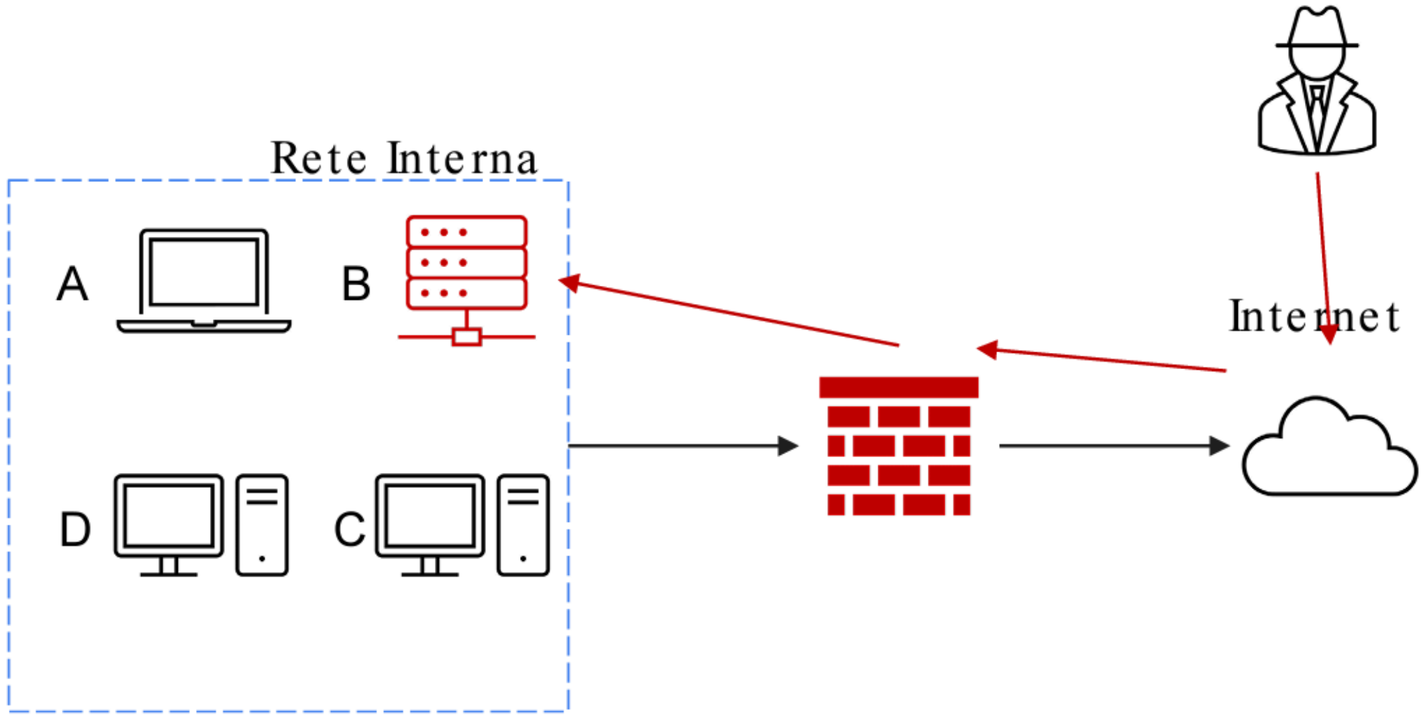
Flavio Scognamiglio

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 Isolamento e 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.**

DATI FORNITI



SVOLGIMENTO E ROADMAP

Nel compito di oggi siamo davanti ad un **incidente di sicurezza**. In quanto **CSIRT**, dobbiamo essere in grado gestire al meglio la problematica e di affrontarla in maniera corretta e sistematica. Vediamo quindi, a grandi linee, la roadmap generica che rappresenta il processo di incident response.

PREPARAZIONE → **RILEVAMENTO ED ANALISI** → **CONTENIMENTO ELIMINAZIONE E RECUPERO** → **ATTIVITA' POST INCIDENTE**

Il processo chiaramente **non è lineare**, ma presenta dei cicli che, in base alla complessità dell'incidente, permettono di tornare alle fasi precedenti. Data la traccia, si presume che la fase di preparazione **sia già stata predisposta**, includendo la definizione di **policy** e procedure **solide** di incident response, la creazione di **playbooks** e del training per il team CSIRT, e la preparazione dei dispositivi **hardware** e **software** necessari per le attività operative.

RILEVAMENTO ED ANALISI

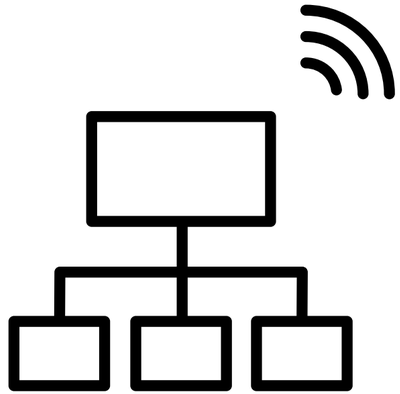
La fase di rilevamento e analisi è una delle più complesse da gestire. Sebbene strumenti come **SIEM**, **SOAR**, **antivirus** e **IDS/IPS** aiutino con alert automatici per eventi sospetti, alcuni incidenti richiedono l'**intervento di personale esperto**. Gli **indicatori** includono **alert** da sistemi di prevenzione e rilevamento intrusioni, **log** generati da sistemi operativi e dispositivi di rete, informazioni su nuove vulnerabilità (**0-day**) e segnalazioni di attività sospette.

PREPARAZIONE	RILEVAMENTO ED ANALISI	CONTENIMENTO ELIMINAZIONE E RECUPERO	ATTIVITA' POST INCIDENTE

In quanto team CSIRT, dobbiamo avviare **rapidamente** la procedura di analisi e rilevamento per **confermare** l'incidente, e lo si può fare utilizzando tecniche come la **profilazione della rete**, l'implementazione di tool **UEBA**, la creazione di policy di **logging** efficaci, la correlazione degli eventi e la cattura del traffico di rete. Dobbiamo quindi capire come è avvenuto l'incidente e **quali altri sistemi** potrebbero essere a rischio. In questo caso, dalle frecce rosse, sembra evidente che l'attaccante abbia **bypassato le difese del firewall** e abbia ottenuto accesso diretto al sistema B, **compromettendolo**.

ISOLAMENTO SISTEMA B INFETTO ATTRAVERSO LA SEGMENTAZIONE

Una **VLAN** dedicata alla **rete di quarantena**, ben progettata con sistemi di sicurezza avanzati e completamente isolata dagli altri sistemi, è essenziale per gestire un incidente. Questa configurazione **impedisce** al sistema compromesso di comunicare con la rete principale, limitando la **propagazione** dell'attacco. Implementando misure di sicurezza aggiuntive, come **firewall** specifici e **monitoraggio** continuo, la rete di quarantena garantisce che l'analisi e la risoluzione del problema possano avvenire senza rischi per il resto dell'infrastruttura aziendale.

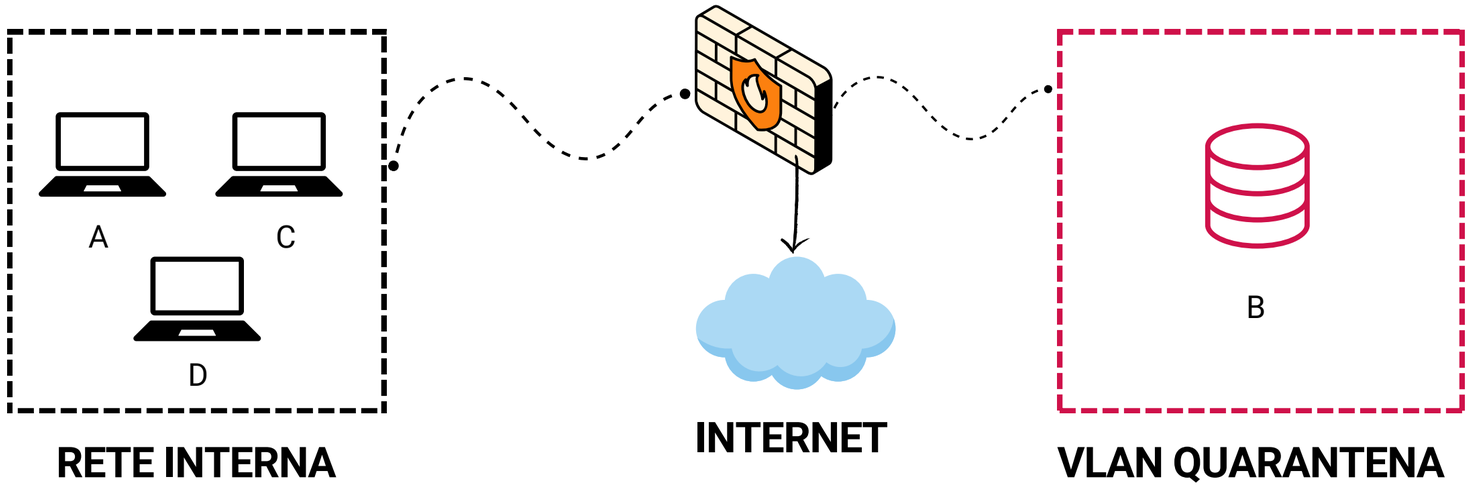


ISOLAMENTO SISTEMA B INFETTO

PREPARAZIONE | RILEVAMENTO ED ANALISI | **CONTENIMENTO ELIMINAZIONE E RECUPERO** | ATTIVITA' POST INCIDENTE

Riguardo l'attacco in corso, dobbiamo quindi **isolare il sistema B** dalla rete interna per evitare che anche gli altri sistemi della vengano **potenzialmente compromessi**, dati i presunti risultati dell'analisi della fase precedente. Questa fase ha lo scopo di **ridurre** gli impatti, **eliminare** l'incidente dalla rete e dai sistemi, recuperare i servizi compromessi e ridurre gli impatti causati da esso.

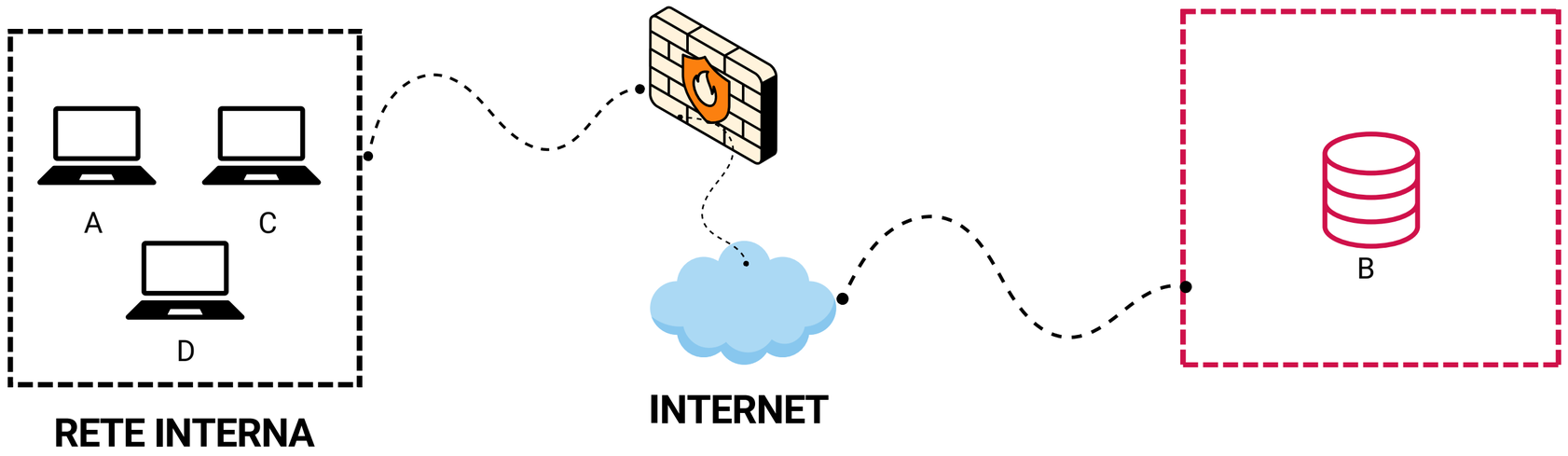
SOLUZIONE 1:



ISOLAMENTO SISTEMA B INFETTO

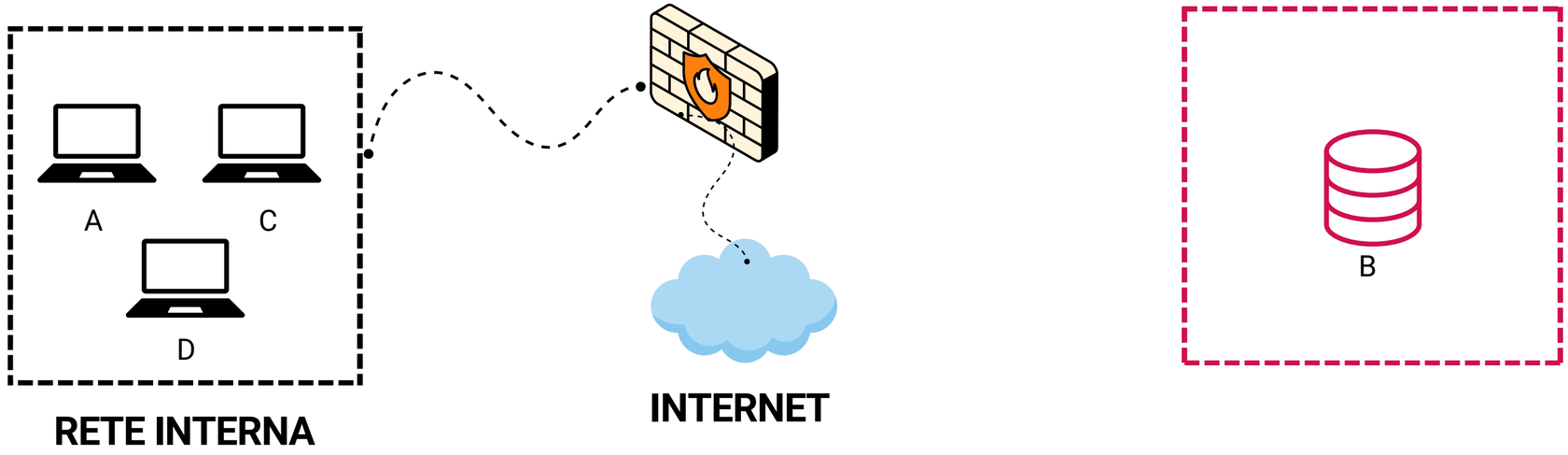
Un’altra possibile soluzione per un contenimento maggiore potrebbe essere quella in basso. Il sistema compromesso viene completamente **disconnesso** dalla rete interna (ma non da internet).

SECONDA SOLUZIONE DI ISOLAMENTO



DISCONNESSIONE FISICA CAVO

Un’altra soluzione efficace potrebbe essere quella di **staccare** direttamente il cavo di rete dal server B che ospita i database e i relativi hard disk, ripulirlo e rimetterlo online. Tuttavia, come analisti, dobbiamo **studiare** a fondo il problema e analizzarlo in **tempo reale** al fine di fornire eventuali prove documentate al team di **forensics** (laddove richiesto) o per un'analisi più approfondita.



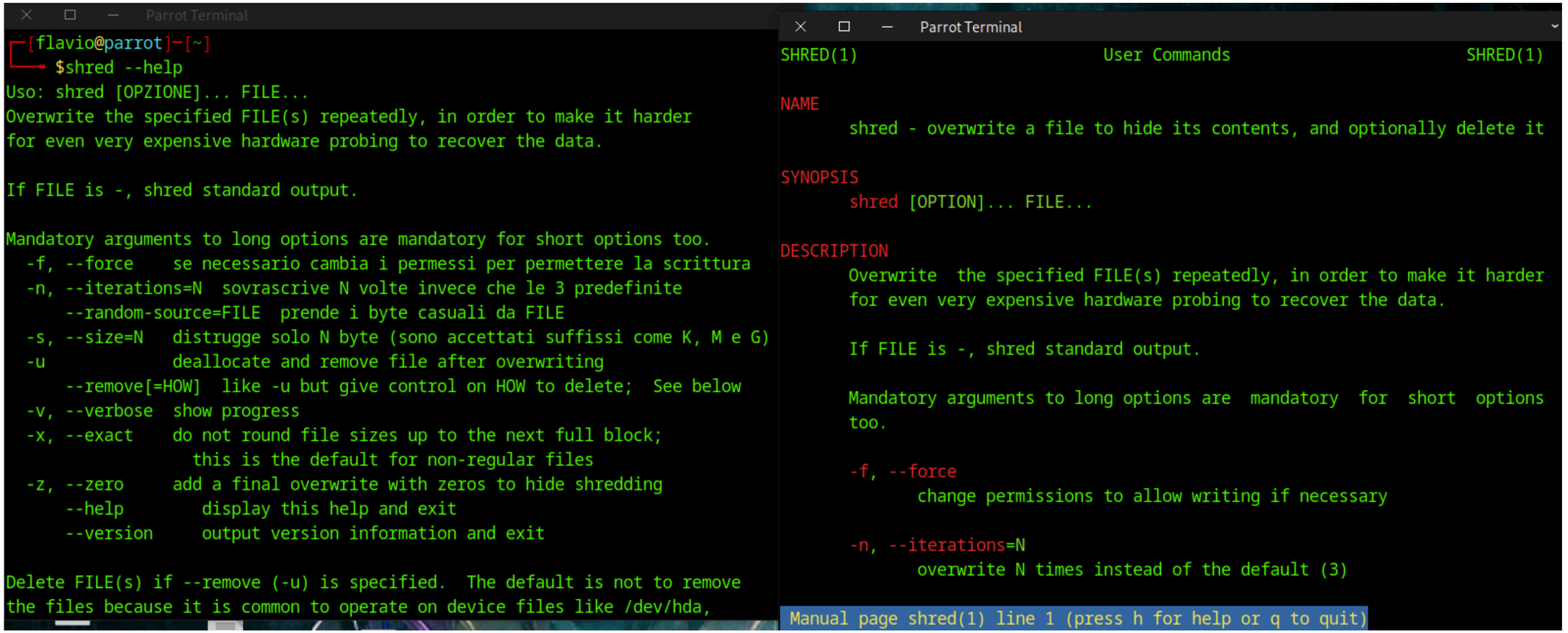
RIMOZIONE E RECUPERO

Una volta isolato il sistema compromesso si procede con la fase di rimozione dell'incidente. Questa fase implica la **pulizia** e la rimozione di qualsiasi **malware** o artefatti lasciati dall'attaccante. Le attività specifiche da eseguire sono determinate in base alle linee guida stabilite nella fase di preparazione.

Dato che il sistema compromesso è, presumibilmente, un database che utilizza dischi in configurazione RAID, la rimozione dei dati compromessi può essere complessa. Se sono disponibili backup precedenti, è possibile eseguire una formattazione completa dei dischi, assicurandosi che venga effettuata una **secure erase** per garantire l'eliminazione sicura dei dati o nella peggiore delle ipotesi, eseguire uno smaltimento con tecniche elencate nella prossima slide. In caso contrario, sarà necessario procedere con la rimozione manuale dei dati compromessi. Per quanto mi riguarda consiglio, per fini di analisi forense, creare un'immagine bit a bit (magari con l'ausilio di distro linux come **Caine**) dei dischi compromessi e fornire tale immagine al team di analisi forense per l'acquisizione delle prove e l'analisi dettagliata.

Successivamente, **è fondamentale applicare tutte le patch di sicurezza disponibili** e aggiornare le configurazioni di sistema e le politiche di sicurezza per prevenire futuri attacchi.

ESEMPIO TOOL PER SECURE ERASE



OPERAZIONI PRIMA DELLO SMALTIMENTO DEI DISCHI

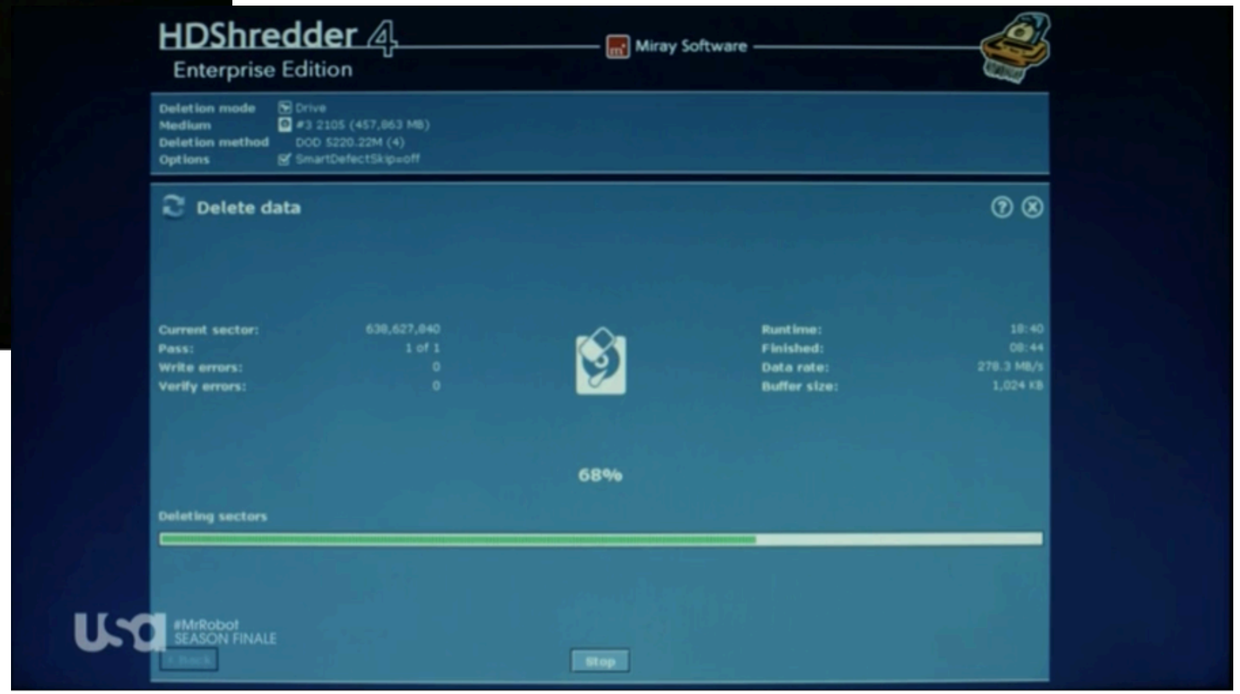
- **Clear**: Sovrascrive i dati su un dispositivo con nuovi dati o utilizza il "factory reset" per riportare il dispositivo allo stato iniziale, rendendo i dati originali difficilmente recuperabili.

- **Purge**: Combina la sovrascrittura logica dei dati con metodi fisici, come la degaussatura con forti magneti, per garantire che i dati siano inaccessibili anche se il dispositivo viene recuperato.

- **Destroy**: Distrugge fisicamente il dispositivo tramite metodi come disintegrazione o polverizzazione, assicurando l'inaccessibilità totale dei dati.

I sostanza **Clear** offre una cancellazione logica dei dati, rendendo difficile il recupero ma non sempre sicuro per dati sensibili. **Purge** combina tecniche logiche e fisiche, offrendo una maggiore sicurezza tramite metodi come la degaussatura. **Destroy** garantisce l'inaccessibilità totale attraverso la distruzione fisica del dispositivo, assicurando la protezione più elevata dei dati.


usa
#MrRobot


HDShredder 4
Enterprise Edition
Miray Software
Deletion mode
Drive
Medium
#3 2105 (457,863 MB)
Deletion method
DOD 5220.22M (4)
Options
SmartDefectSkip=off
Delete data
Current sector:
638,627,840
Pass:
1 of 1
Write errors:
0
Verify errors:
0
Runtime:
18:40
Finished:
08:44
Data rate:
278.3 MB/s
Buffer size:
1,024 KB
68%
Deleting sectors
usa
#MrRobot
SEASON FINALE
Stop

GRAZIE

Flavio Scognamiglio