1. Isolamento del sistema B: L'obiettivo principale è impedire la diffusione dell'infezione ad altri sistemi nella rete. È possibile utilizzare le seguenti tecniche:

- Disconnessione fisica: Disconnettere il sistema infetto dalla rete aziendale, scollegando il cavo di rete o disattivando la connessione Wi-Fi.

- Isolamento logico: Configurare il firewall o altre soluzioni di sicurezza per impedire al sistema infetto di comunicare con altri dispositivi sulla rete.

2. Individuazione e identificazione dell'infezione:

- Monitoraggio del traffico di rete: Utilizzare strumenti di monitoraggio del traffico di rete per individuare attività sospette o comportamenti anomali associati al sistema infetto.

- Analisi dei log: Esaminare i log di sistema e di sicurezza per identificare eventuali segni di infezione o attività sospette.

- Scansione antivirus e anti-malware: Utilizzare software di sicurezza per eseguire una scansione completa del sistema infetto al fine di individuare e rimuovere eventuali malware o programmi dannosi.

3. Rimozione dell'infezione:

- Isolamento dei file infetti: Identificare i file infetti o compromessi nel sistema e isolare o eliminare tali file per prevenire ulteriori danni.

- Utilizzo di software antivirus e anti-malware: Utilizzare programmi di sicurezza aggiornati per eseguire una scansione approfondita del sistema e rimuovere il malware o gli elementi dannosi individuati.

- Ripristino dei file di sistema: Sostituire i file di sistema compromessi con versioni pulite dai backup o utilizzando strumenti di ripristino del sistema.

4. Patching e aggiornamenti: Assicurarsi che il sistema infetto sia completamente aggiornato applicando le patch di sicurezza e gli aggiornamenti del sistema operativo e di altri software installati. Ciò aiuta a mitigare le vulnerabilità che potrebbero essere state sfruttate dall'infezione.

5. Analisi delle cause e delle lezioni apprese: Una volta completata la rimozione dell'infezione, è importante condurre un'analisi dettagliata delle cause sottostanti e delle lezioni apprese per migliorare la sicurezza della rete aziendale e prevenire future infezioni.

1. Clear (Cancellazione): La cancellazione dei dati rappresenta una semplice operazione di rimozione logica dei dati dal database o dai dischi di archiviazione. Quando viene effettuata un'operazione di cancellazione, i dati vengono contrassegnati come "non più validi" e possono essere sovrascritti con nuovi dati in futuro. Tuttavia, i dati eliminati tramite l'operazione di cancellazione possono ancora essere recuperati utilizzando

strumenti specializzati o tecniche di recupero dei dati. Pertanto, se le informazioni sensibili sono state cancellate semplicemente, potrebbero potenzialmente essere recuperate da un utente malintenzionato.

2. Purge (Cancellazione definitiva): La cancellazione definitiva o purging implica l'eliminazione permanente dei dati sensibili dal sistema, in modo tale che non possano essere recuperati nemmeno utilizzando tecniche di recupero dei dati avanzate. Questa operazione spesso coinvolge sovrascrivere i dati con informazioni casuali o crittografare i dati in modo irreversibile. La purging viene effettuata per garantire che le informazioni sensibili non siano più accessibili e rappresenta una misura di sicurezza più forte rispetto alla semplice cancellazione. Tuttavia, è importante notare che alcune tecniche di recupero dei dati forensi avanzate potrebbero ancora essere in grado di recuperare frammenti di dati anche dopo la purging.

3. Destroy (Distruzione): La distruzione rappresenta l'eliminazione fisica o l'annientamento dei supporti di archiviazione contenenti le informazioni sensibili. Questo può includere la distruzione fisica dei dischi rigidi o l'utilizzo di tecniche specializzate per rendere inutilizzabili i dispositivi di archiviazione. La distruzione fisica è il metodo più sicuro per eliminare in modo permanente i dati, ma può essere costosa e richiedere procedure speciali per garantire la corretta distruzione dei supporti di archiviazione.

La scelta tra clear, purge e destroy dipende dal livello di sicurezza richiesto per le informazioni sensibili. Se le informazioni sono altamente sensibili e non devono essere recuperate in alcun modo, la distruzione fisica dei supporti di archiviazione è l'opzione più sicura. Altrimenti, la purging con sovrascrittura o crittografia dei dati può fornire un livello di protezione adeguato.