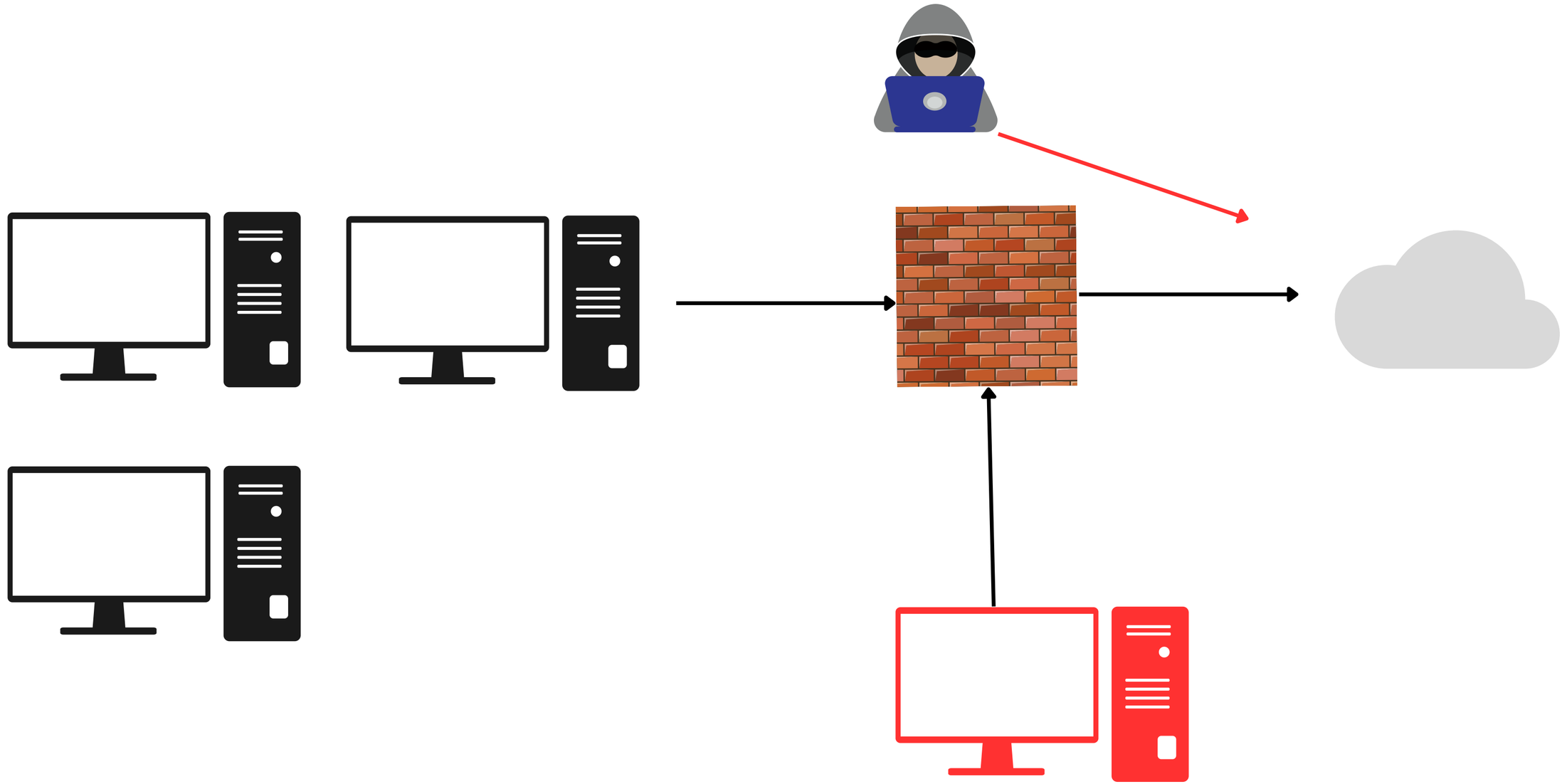
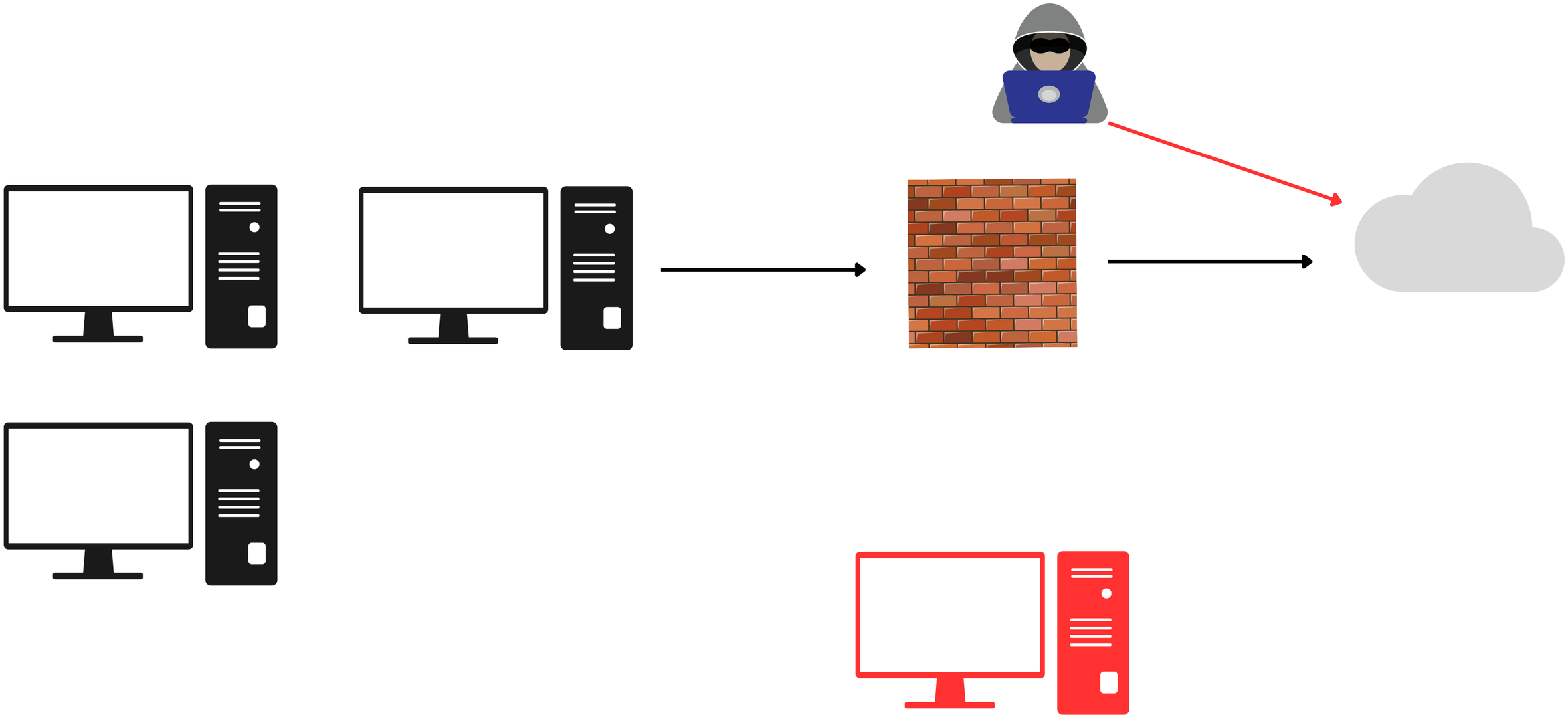
S9L4

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 sistem B infetto Spiegate la differenza tra Purge e Destroy per l’eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi

Metodo 1:Estromissione del sistema infetto dalla rete mettendolo in quarantena



Metodo 2:Estromissione del sistema infetto scollegandolo dalle reti aziendali.



Purge si concentra sulla sovrascrittura sicura dei dati per renderli inaccessibili, Destroy si riferisce alla distruzione fisica del dispositivo di archiviazione per impedire il recupero di qualsiasi informazione. La scelta tra i due approcci dipende dalle politiche di sicurezza dell'organizzazione.