Il team **CSIRT** (Computer Security Incident Response Team) ha il compito di sorvegliare e gestire gli incidenti di sicurezza. Pur condividendo alcune caratteristiche con il SOC di livello 2, va notato che il SOC è di natura privata, a differenza del CSIRT, il quale assume un ruolo di maggiore rilevanza in virtù della presenza di figure a livello governativo all'interno del suo organico.

L'isolamento del sistema limita l'accesso dell'attaccante alla rete interna, ma è importante notare che la stessa tecnica non impedisce all'attaccante di accedere al sistema infetto tramite internet.

La procedura di rimozione implica l'eliminazione totale del sistema dalla rete, rendendolo inaccessibile sia dalla rete interna che da internet. Questa metodologia limita l'accesso dell'attaccante alla rete interna, impedendogli completamente l'accesso al sistema precedentemente compromesso.

Per l'approccio"**Purge**", vengono implementate sia misure logiche che fisiche per la cancellazione permanente dei dati su un disco o dispositivo di storage. È importante notare che le tecniche fisiche utilizzate in questo contesto non sono invasive e non comportano la distruzione dell’hardware.

Per l'approccio "**Destroy**", vengono impiegate tecniche fisicamente invasive con l'obiettivo di rendere i dati su un disco o dispositivo di storage completamente inaccessibili. Alcune di queste tecniche comportano la distruzione dell'hardware, rendendo di fatto irrecuperabile sia l'hardware stesso che le informazioni ivi contenute. Questo metodo è preferibile quando si desidera smaltire un disco che non sarà più riutilizzato, ma è anche caratterizzato da costi significativamente più elevati.