Metodi di isolamento, e rimozione di un sistema infetto.
Differenze tra purge e destroy.
Clear

Le attività di contenimento hanno lo scopo primario di isolare l'incidente in modo tale che non possa creare ulteriori danni a reti/sistemi.

Una delle tecniche preventive e strategiche per la gestione degli incidenti di sicurezza sulla rete è la «segmentazione», che risulta essere particolarmente utile anche nella fase di contenimento di un incidente in corso. La segmentazione include tutte quelle attività che permettono di dividere una rete in diverse LAN o VLAN.

La segmentazione permette invece di separare il sistema B dagli altri computer sulla rete, creando una rete ad hoc, che viene chiamata generalmente «rete di quarantena».
L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante.

Ci sono casi in cui l'isolamento non è ancora abbastanza. In questi casi si procede con la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema dalla rete sia interna sia internet.

A valle delle attività di contenimento, il tema CSIRT deve passare alla fase di rimozione dell'incidente.
In questa fase lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell'incidente all'interno della rete o sui sistemi.

Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.

Destroy: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.

Clear: il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche».Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale.