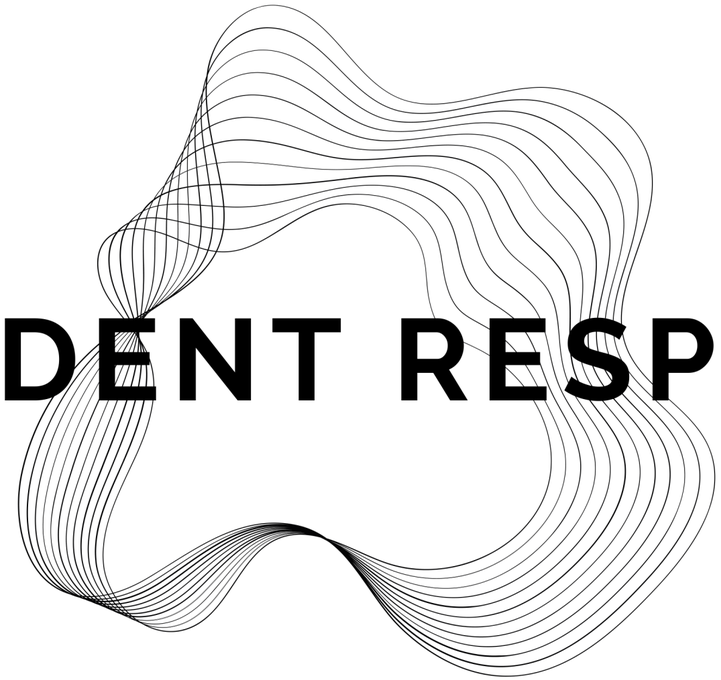


INCIDENT RESPONSE

NET. REBELS.

MICHELANGELO BORROMEO

TRACCIA

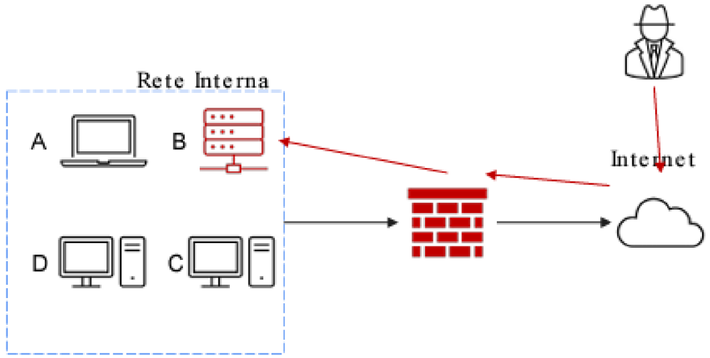
MOSTRARE LE TECNICHE DI:

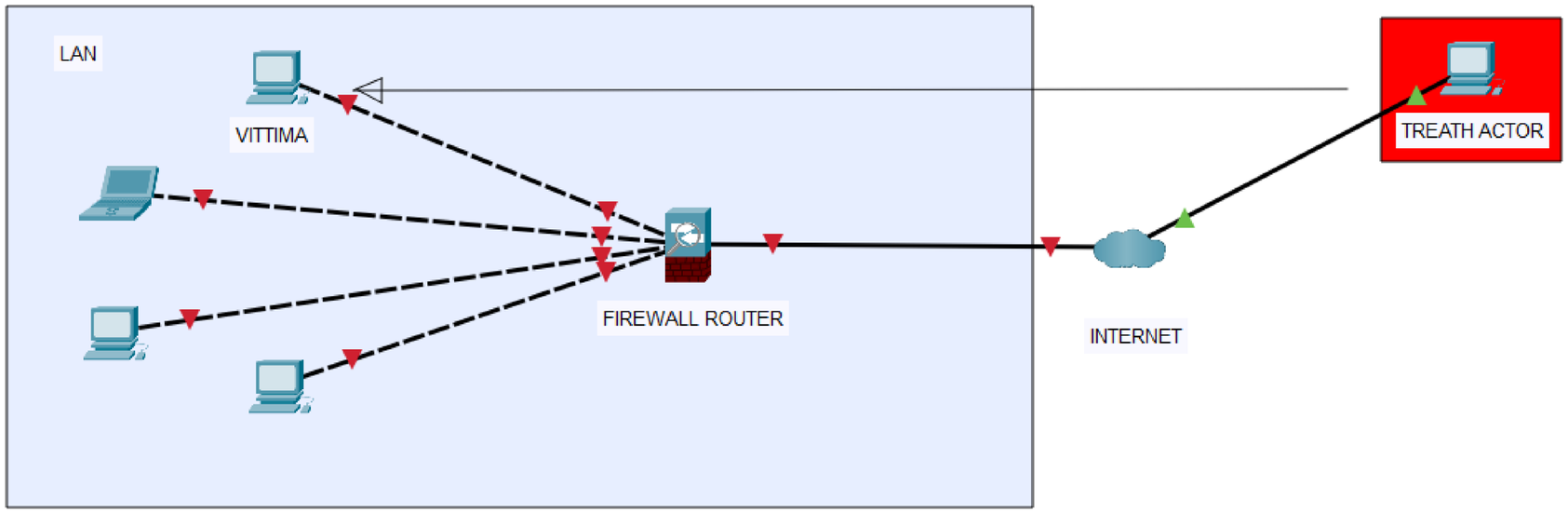
I) ISOLAMENTO

II) RIMOZIONE DEL SISTEMA INFETTO.

SPIEGARE LA DIFFERENZA TRA PURGE E DESTROY PER L'ELIMINAZIONE DELLE INFORMAZIONI SENSIBILI PRIMA DI PROCEDERE ALLO SMALTIMENTO DEI DISCHI COMPROMESSI. INDICARE ANCHE CLEAR

ATTACCO

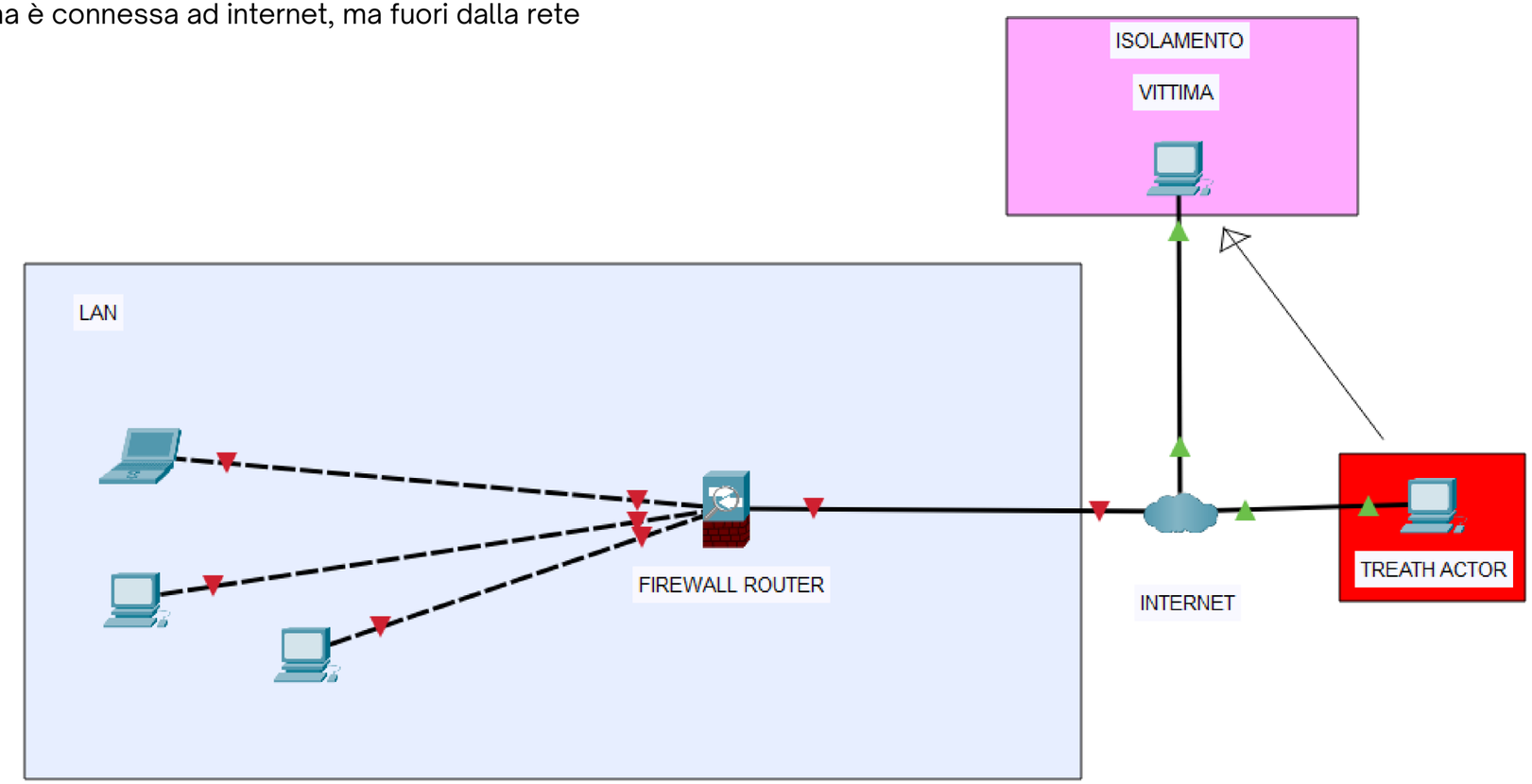

Rete Interna
A
B
D
C
Internet


LAN
VITTIMA
FIREWALL ROUTER
INTERNET
TREATH ACTOR

ISOLAMENTO

L’isolamento consiste nel disconnettere completamente il sistema infetto dalla rete, limitando ulteriormente l'accesso dell'attaccante alla rete interna.

In questo caso la macchina è connessa ad internet, ma fuori dalla rete locale, utilizzando il 4G

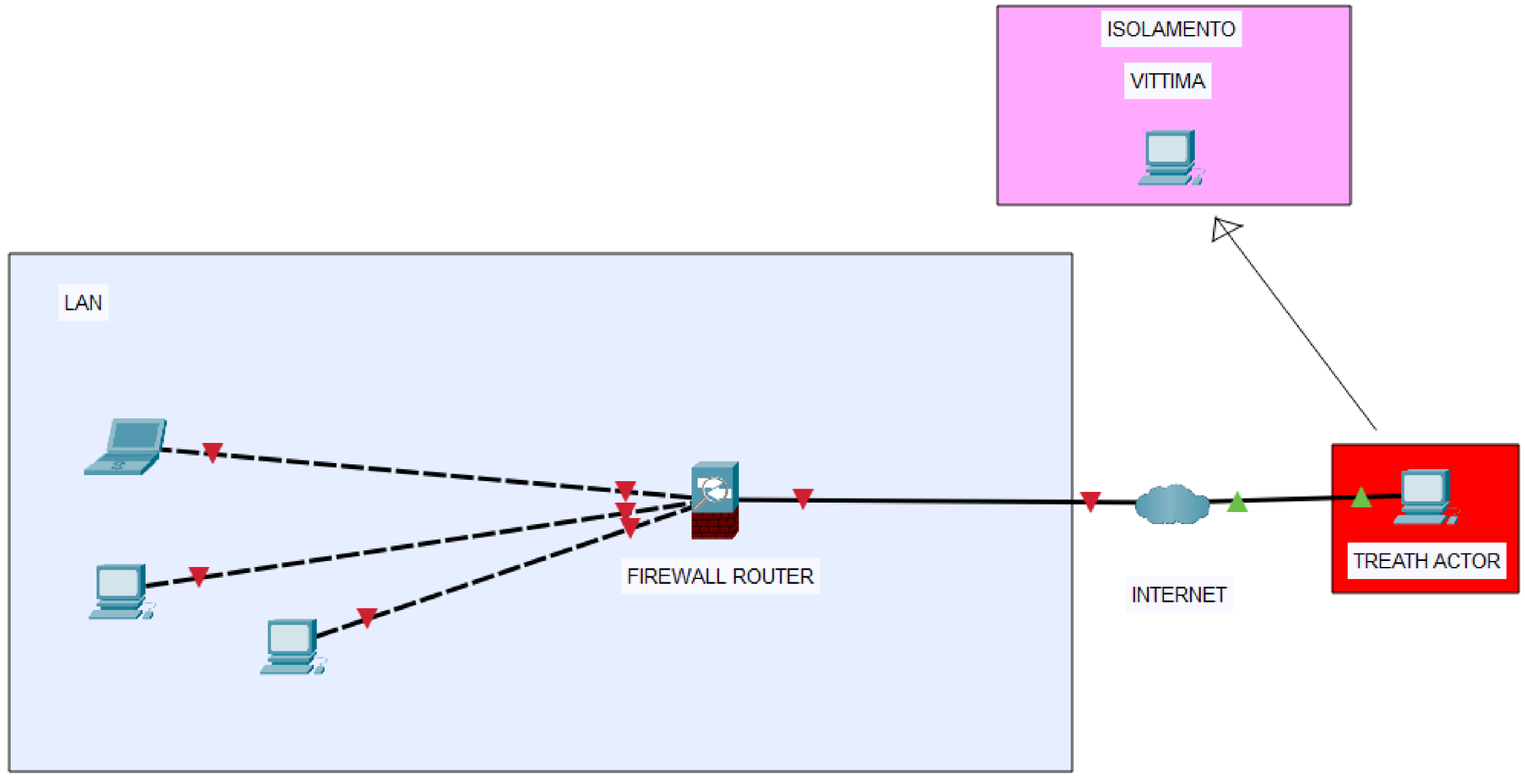


RIMOZIONE

In questa fase, La macchina infetta non avrà accesso alla rete e ad internet rendendola completamente in quarantena

Utilizzando “Playbook” (Linee guida per determinati eventi) si procederà con:

- Rimozione di backdoor installate da malware
- Pulizia di dischi
- Chiavette USB compromesse.
- Ripristino del sistema



GESTIONE DEI MEDIA

Una volta completata la rimozione dell'incidente dalla rete e dai sistemi impattati, inizia la fase di recupero.
Ci si può imbattere allo smaltimento o il riutilizzo di un disco o un sistema di storage di un sistema compromesso con tre opzioni:

CLEAR

(approccio logico)
Consiste nella sovrascrizione dei dati o di un <factory reset>, così da poter rendere il device o componente riutilizzabile

PURGE

Rimozione approfondita dei dati per impedire il recupero anche con strumenti avanzati:
Utilizzo di software di purgazione, smagnetizzazione (degaussing), o comandi di cancellazione sicura.

DESTROY

Distruzione fisica del dispositivo di archiviazione.
Per dati altamente sensibili dove il recupero è inaccettabile.

i metodi utilizzati sono:
Triturazione, incenerimento, fusione o dissoluzione chimica.