T-CON2025

WAR ROOM EDITION

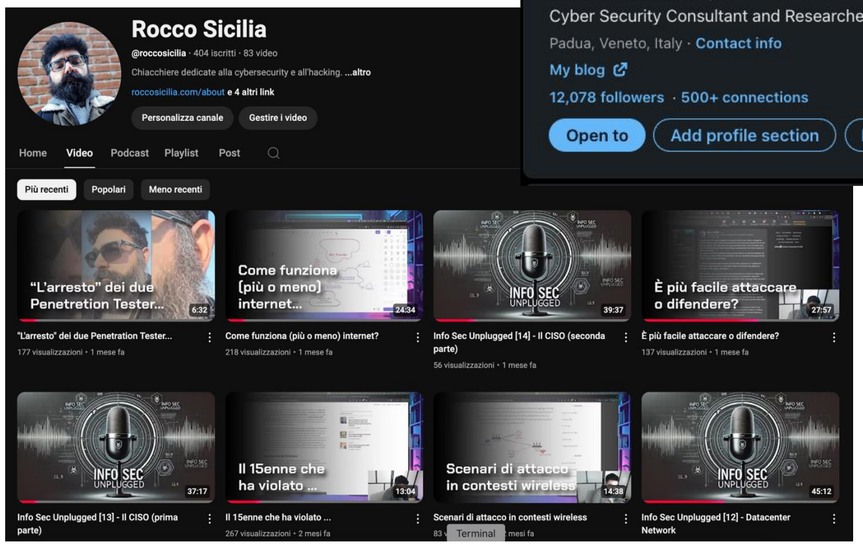
# Threat Hunting Avanzato per Potenziare la Detection

**Rocco Sicilia** Cyber Security Consultant and Researcher

T-CONSULTING

# # whoami

- Security Engineer **@NTS**
- Cyber Security Researcher
- Blogger


T-CONSULTING

# # intro

- Paradigma alla base dell’info. sec.
- Advanced Threat Protection
- Evading / Bypass
- Threat Intelligence e Threat Hunting

# # l'info. sec. ha un problema di base

### .1 Nuova minaccia

Viene identificata una nuova tipologia di minaccia o una variate non intercettata dai sistemi di detection

### .2 Analisi

Viene studiato il ***comportamento*** della minaccia per identificare ***pattern*** ed ***artefatti***

### .3 Divulgazione

Le informazioni vengono rilasciate pubblicamente


### .4 Sviluppo contromisure

I vendor sviluppano la componente per identificare la minaccia

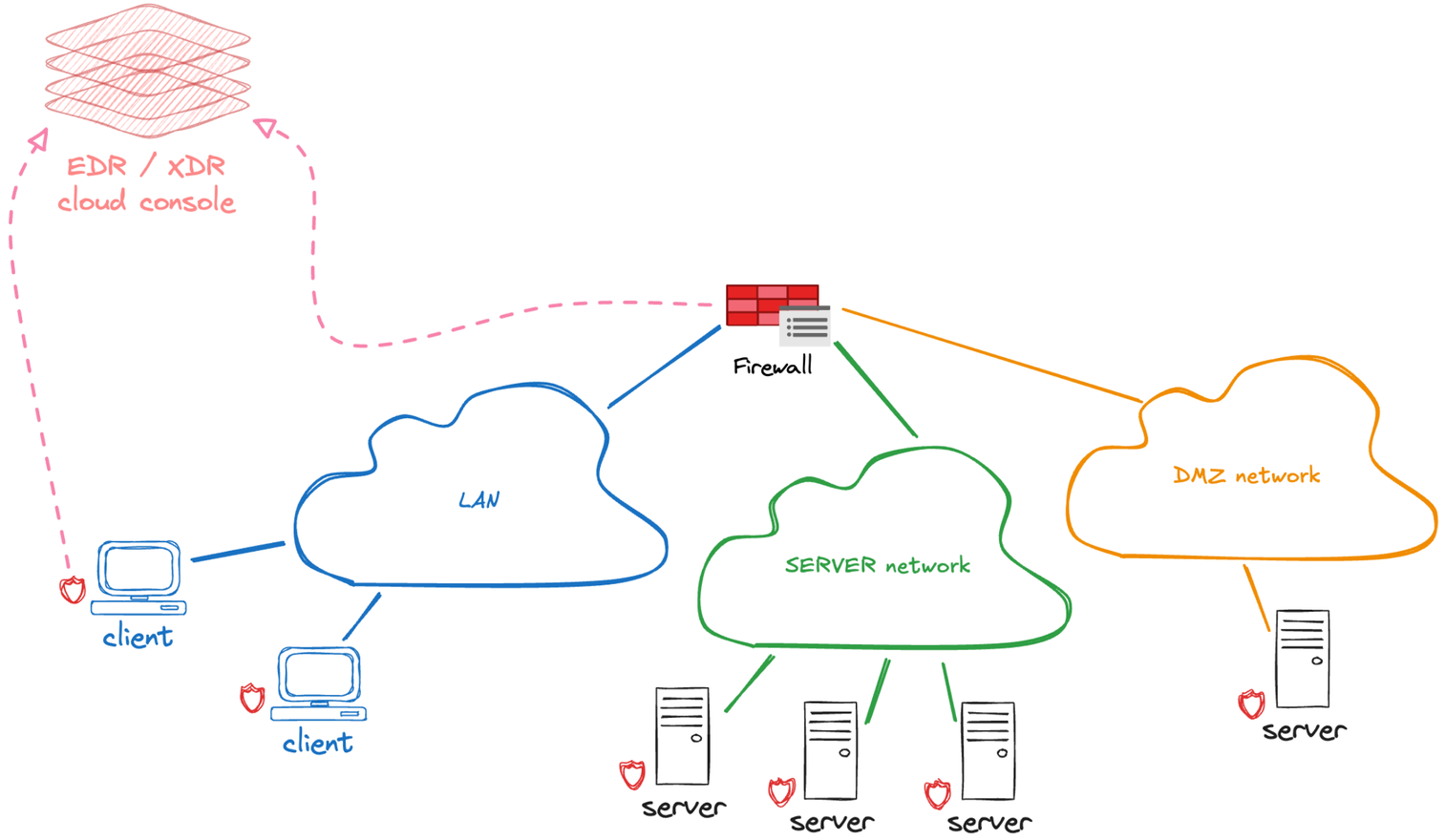
### .5 Test

Il funzionamento della componente viene verificato e validato prima del rilascio

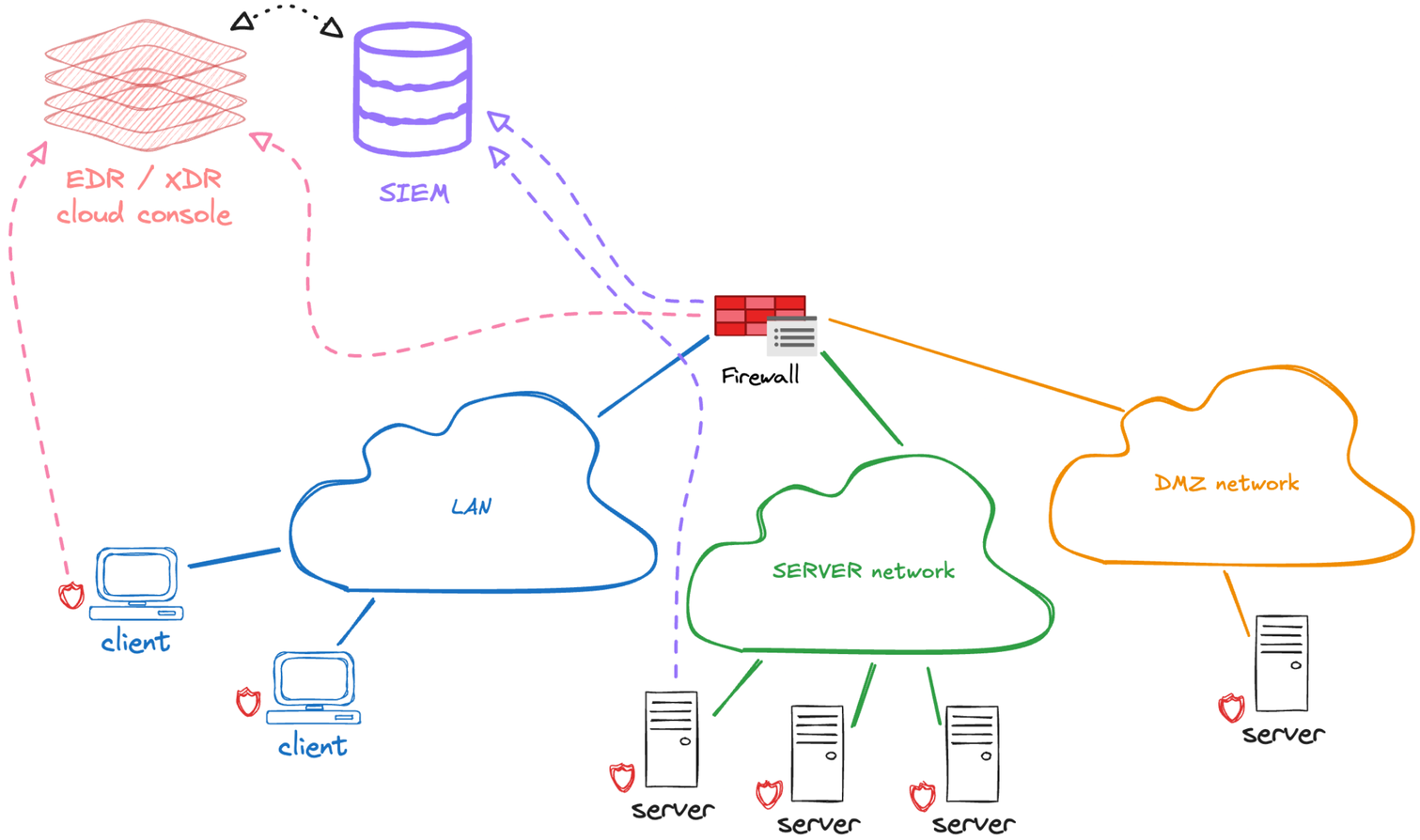
### .6 Distribuzione

La funzione di detection e/o prevention viene rilasciata

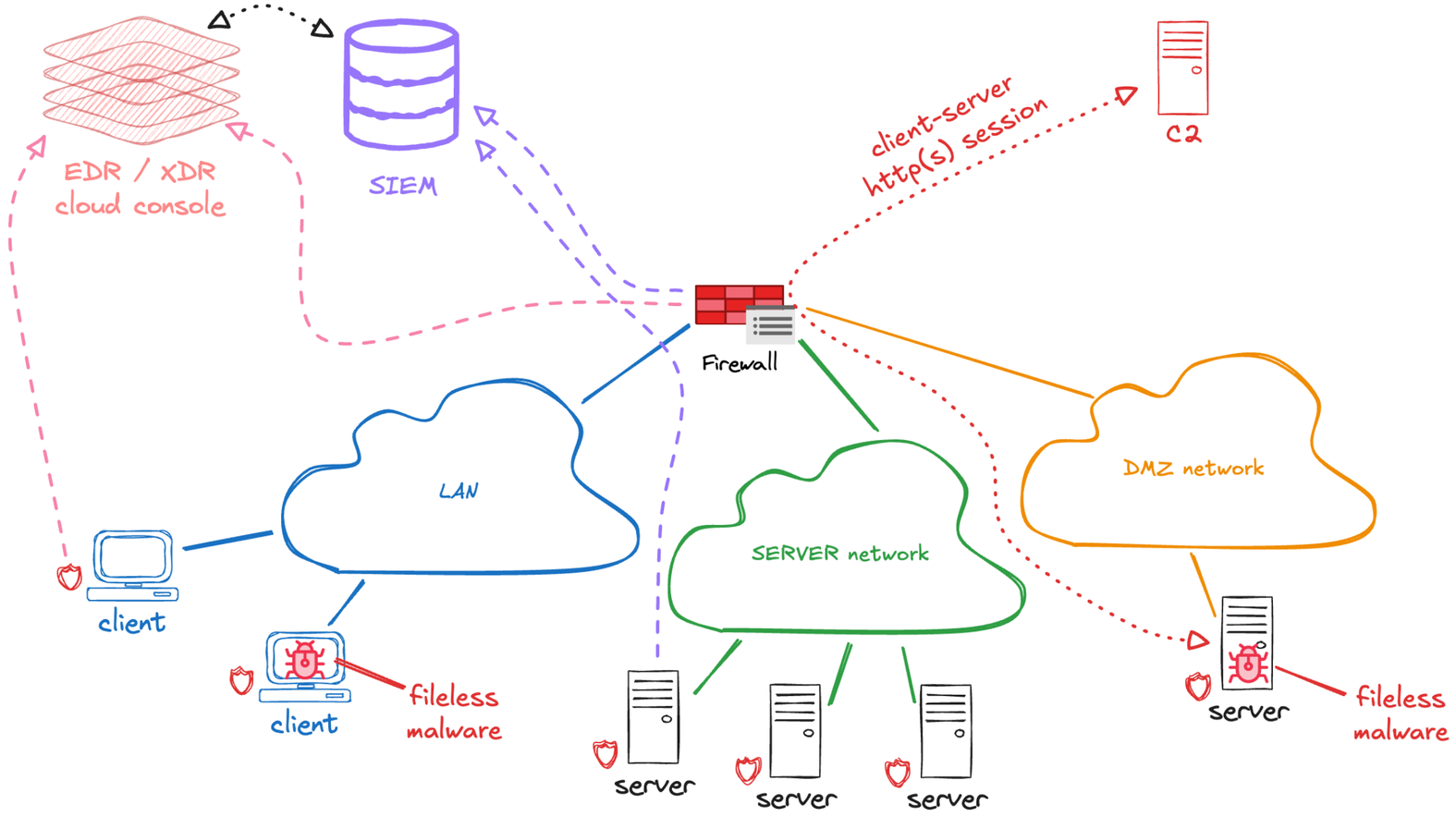
# # l'ATP ci da una mano



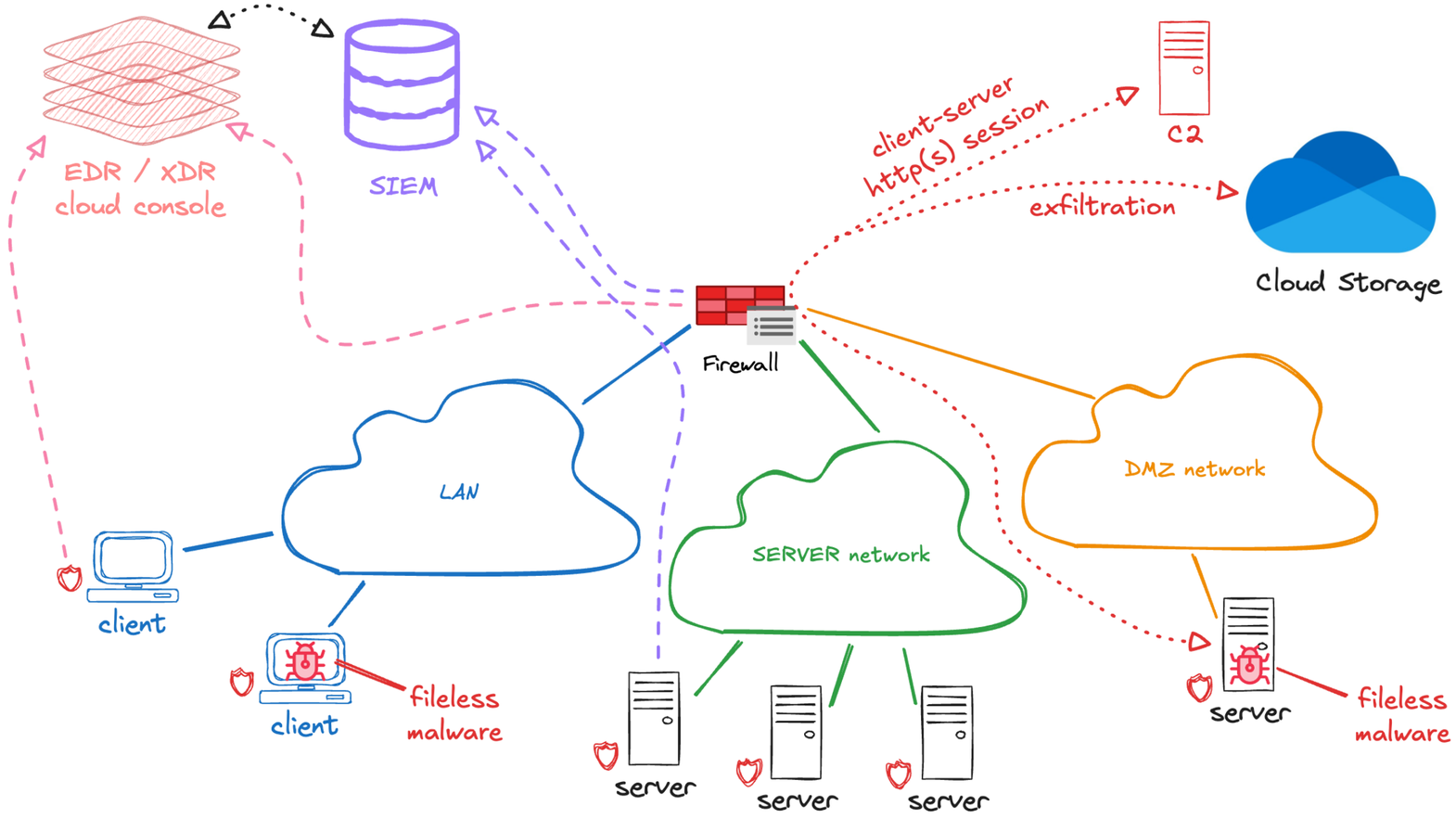
# # l'ATP ci da una mano



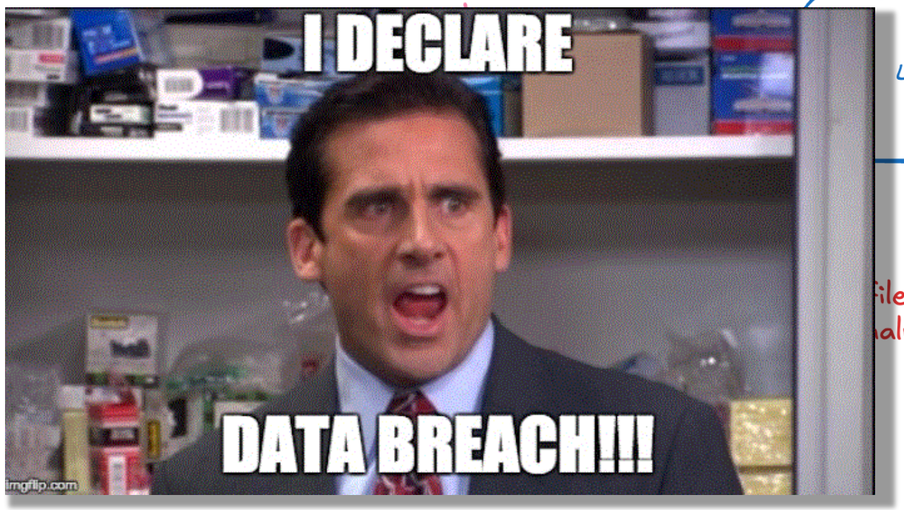
# # il threat actor si adatta rapidamente

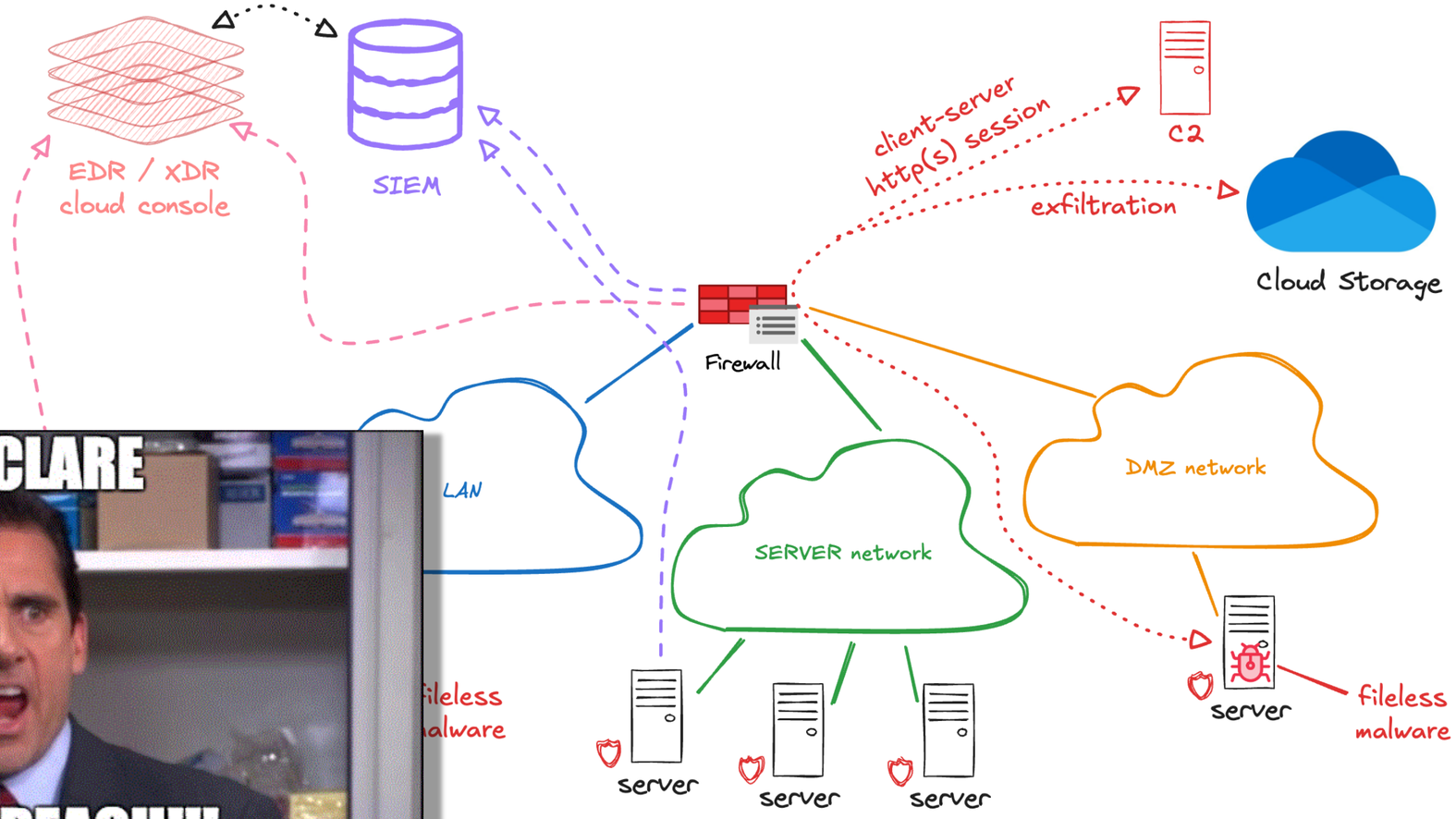


# # il threat actor si adatta rapidamente



# # il threat actor si adatta rapidamente



# # difesa attiva


**DMZ coreana**

- 250 km di lunghezza 4 km di larghezza
- Campi minati in diversi punti dell’area
- Recinzioni sue due lati dell’area: muri e filo spinato
- Torri di avvistamento e bunker presidiati da soldati
- Un solo valico

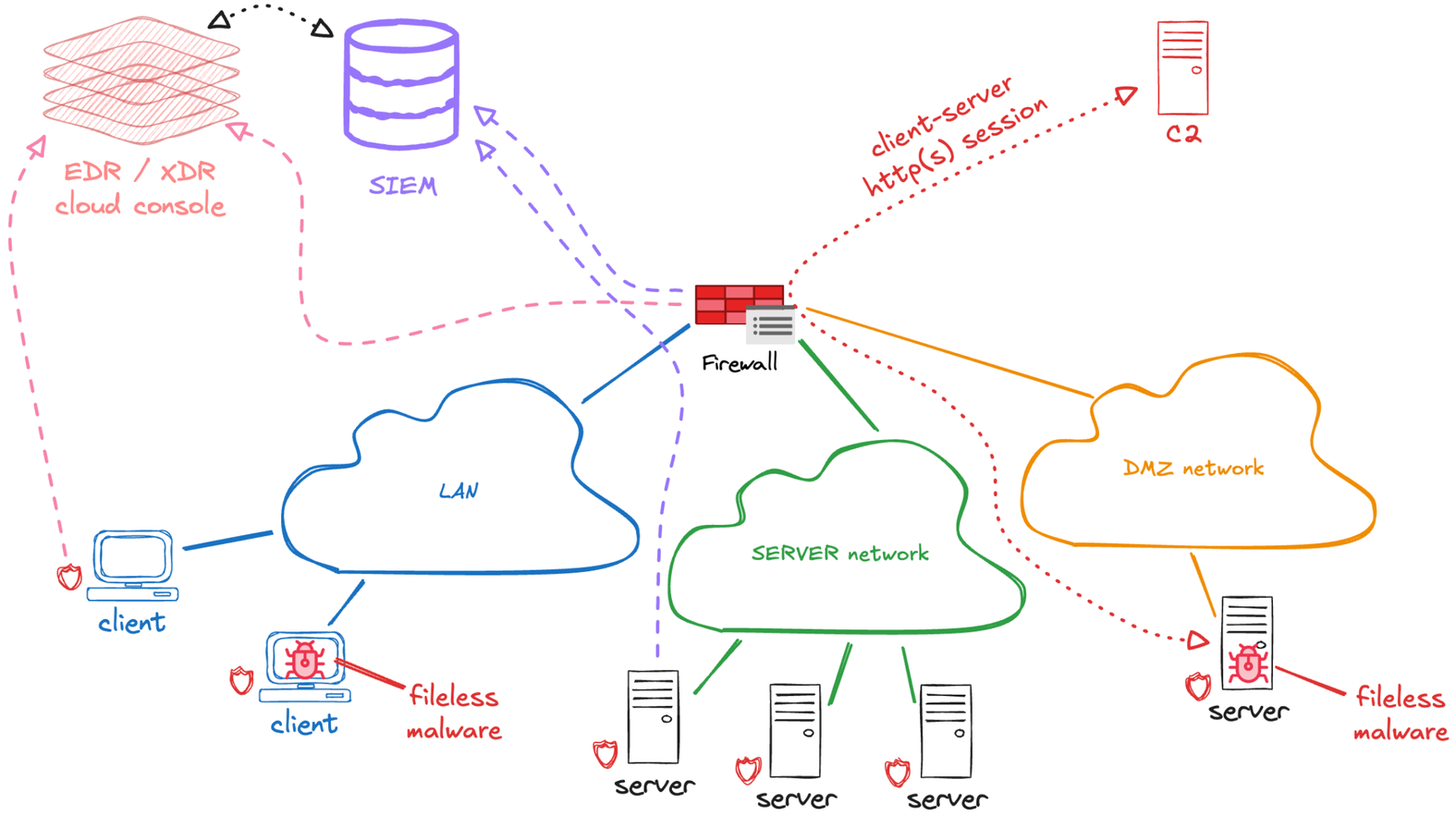
# # difesa attiva


Nel 1974, durante un pattugliamneto, viene notato del valore che esce dal sottosuolo.

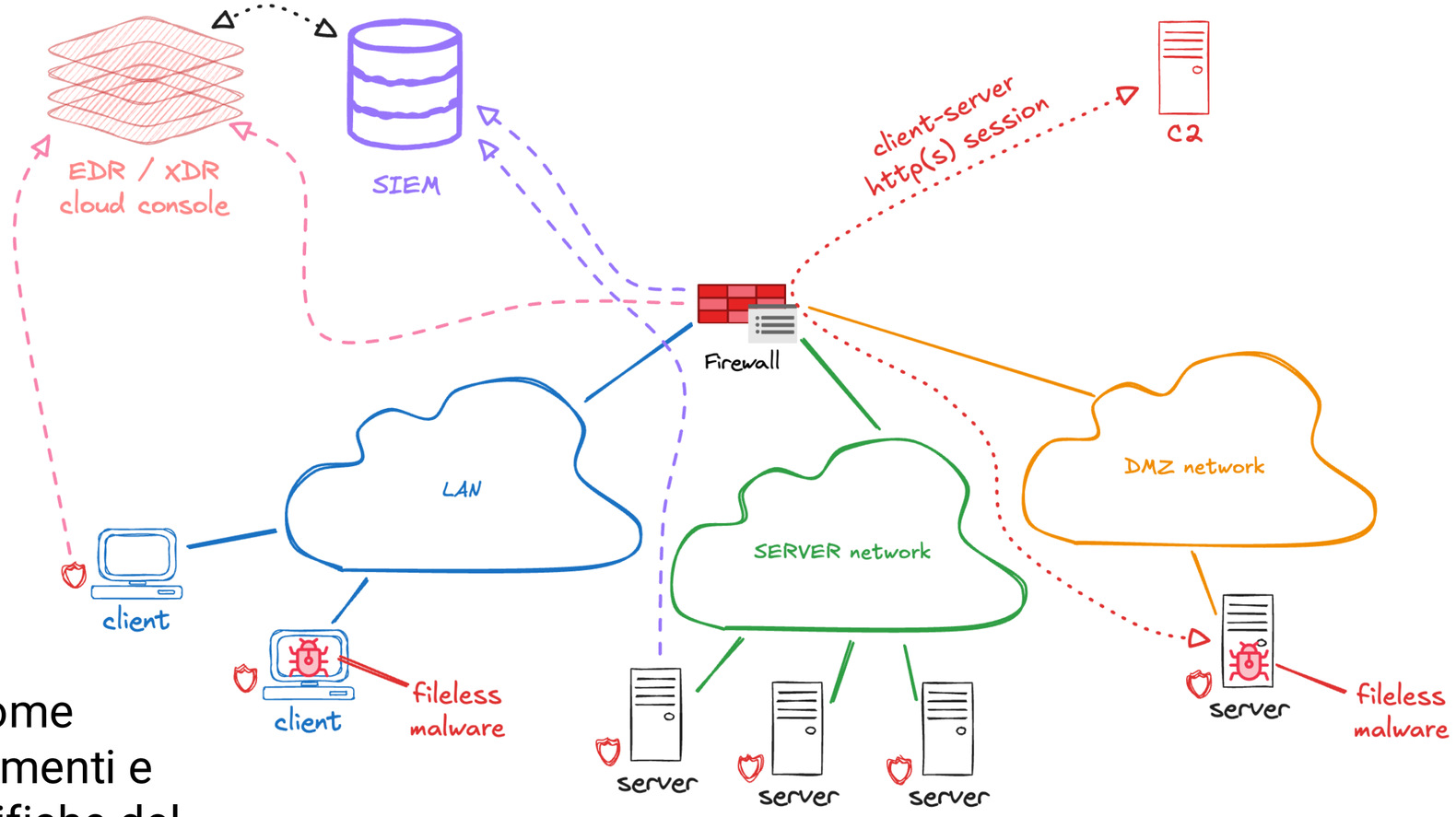
L’indagine porta alla scoperta di un tunnel scavato dall’esercito della Corea del Nord che si estendeva per circa 1 km all’interno del territorio della Corea del Sud.

Nei successivi anni vengono scoperti altri tre tunnel anche grazie a ricerche mirate.

# # cercare le minacce

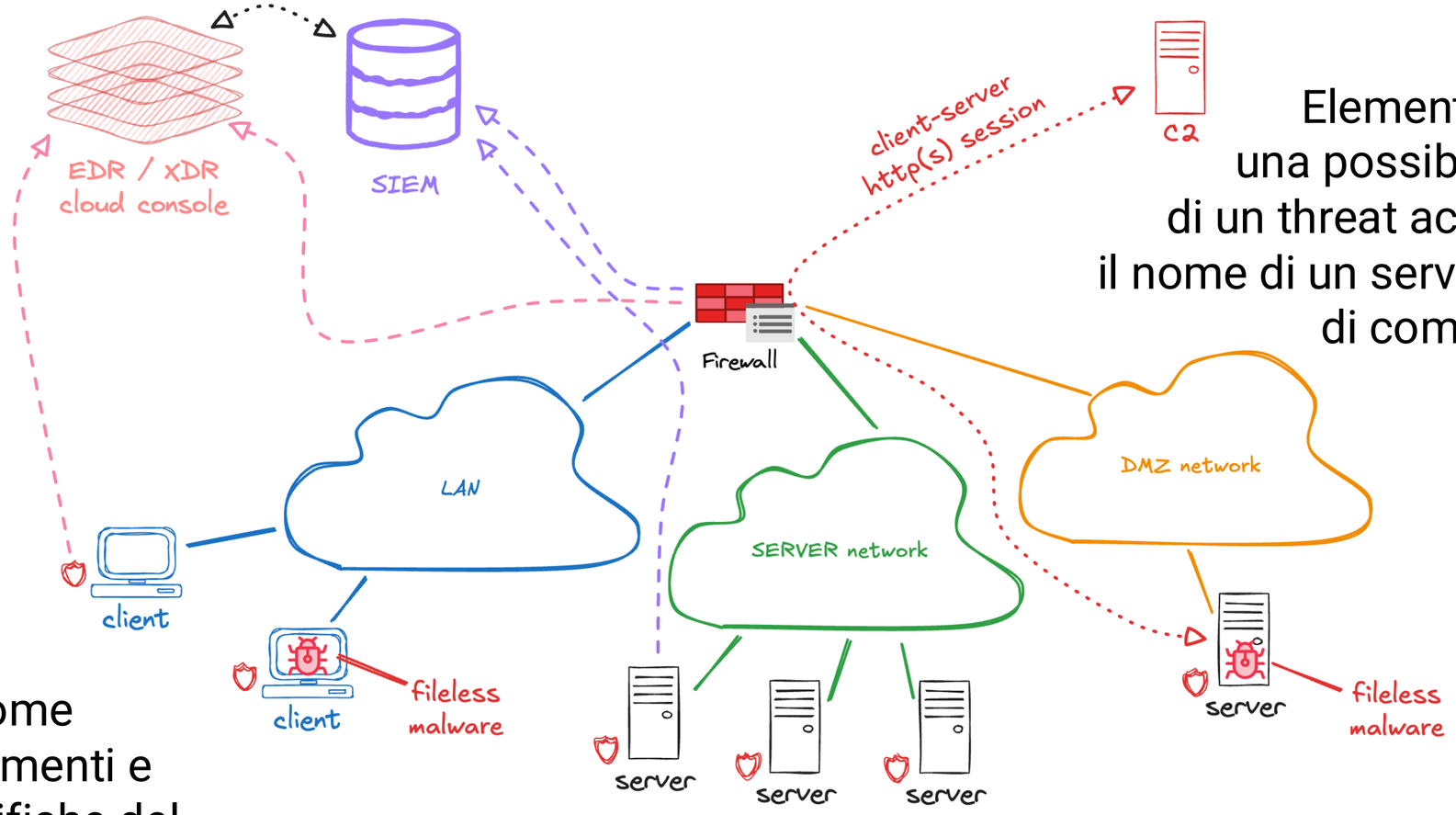


# # cercare le minacce




**Threat Intelligence**
Ricerca attiva delle possibili minacce come nuove tecniche, strumenti e caratteristiche specifiche del modus operandi dell’avversario.

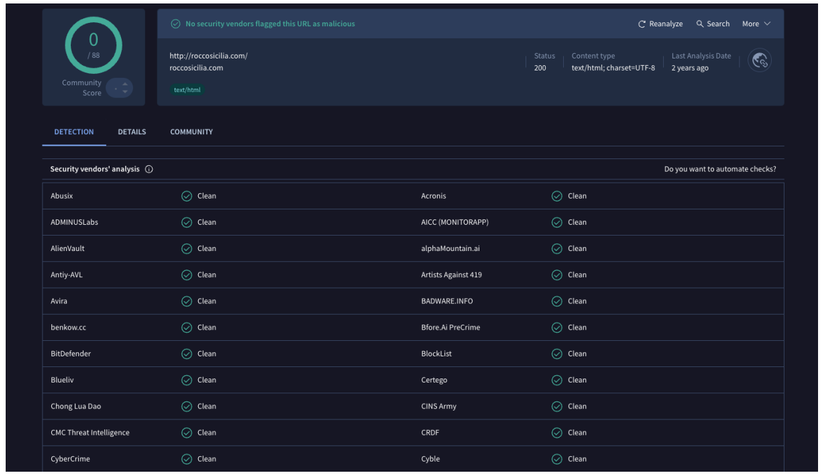
# # cercare le minacce

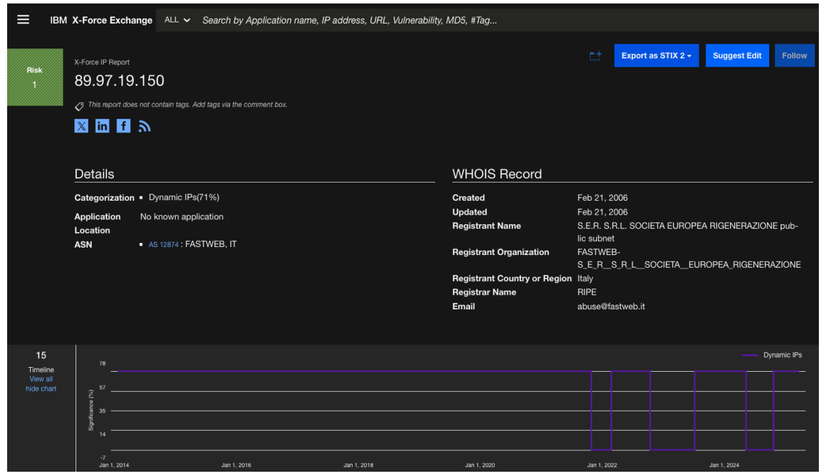


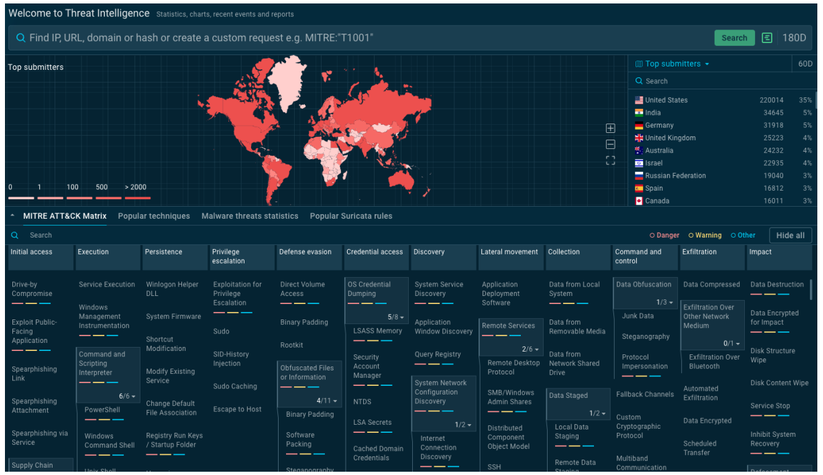

**IoC**
Elemento che caratterizza una possibile azione da parte di un threat actor: un IP, un hash, il nome di un servizio, una sequenza di comandi powershell, …

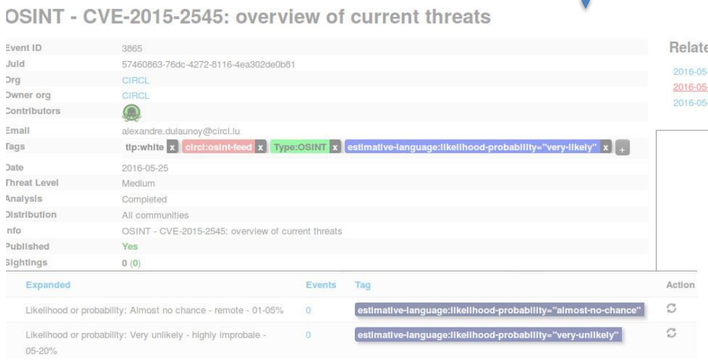
**Threat Intelligence**
Ricerca attiva delle possibili minacce come nuove tecniche, strumenti e caratteristiche specifiche del modus operandi dell’avversario.

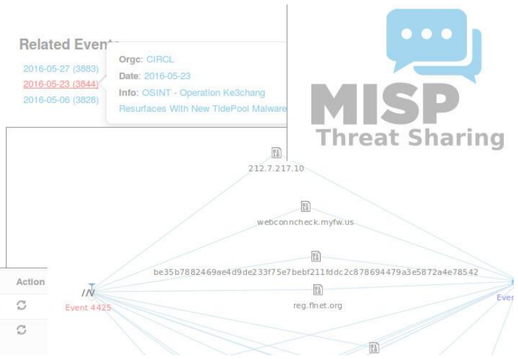
# # cercare le minacce



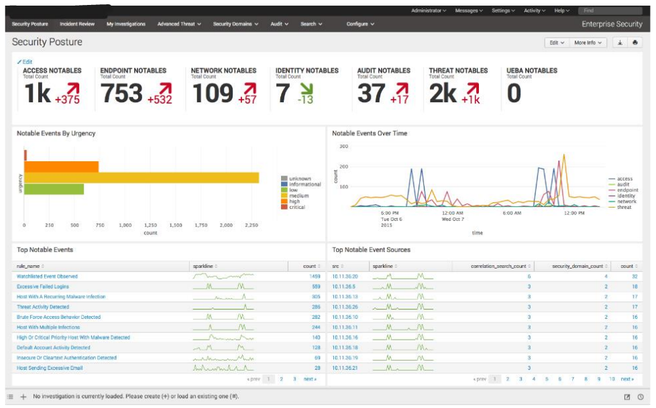



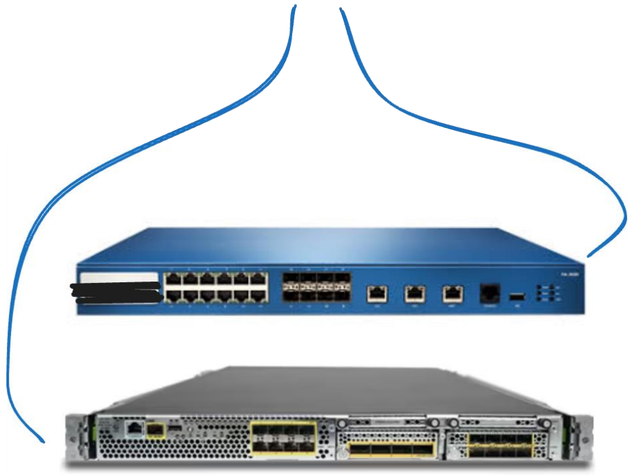



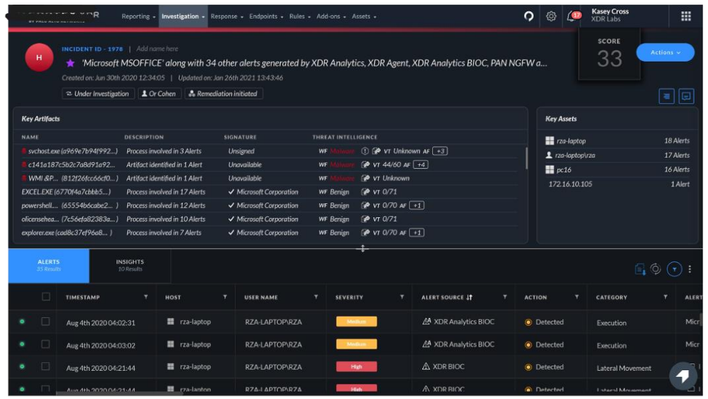



# # cercare le minacce

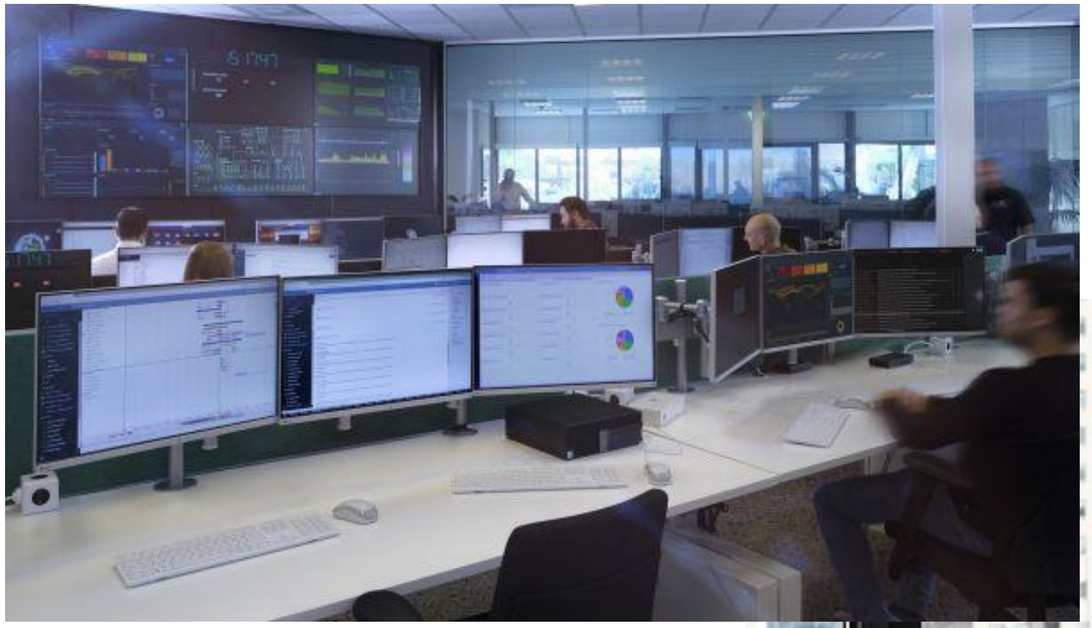



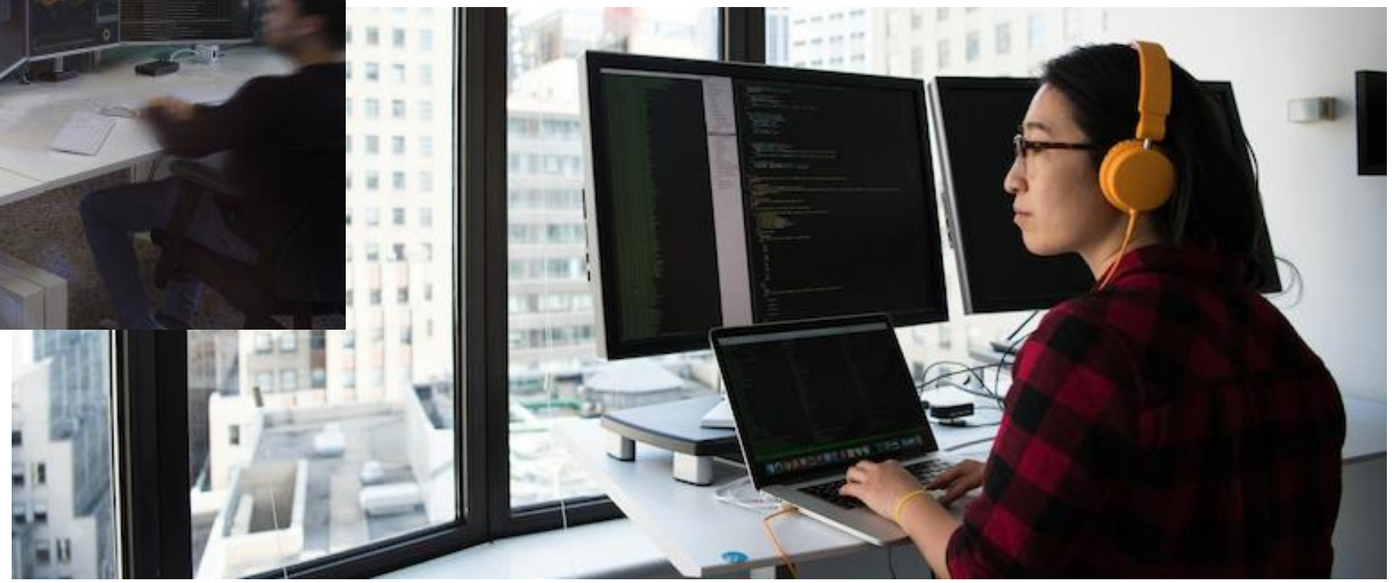






T-CONSULTING

# # chi se ne occupa?





# # recap


EDR
Protection
Defense
Hunting
sharing
Intelligenge
Threat
IoC
SOAR
Event
Detection
Anomaly
BIoC
XDR
SIEM
Security
Actor
OSInt

T-CON2025

WAR ROOM EDITION

# Grazie per l’attenzione

T-CONSULTING