

T-CON2025

WAR ROOM EDITION

Threat Hunting Avanzato per Potenziare la Detection

Rocco Sicilia Cyber Security Consultant and Researcher

whoami

- Security Engineer @NTS
- Cyber Security Researcher
- Blogger



Rocco Sicilia
@roccosicilia · 404 iscritti · 83 video
Chiacchiere dedicate alla cybersecurity e all'hacking. ...altro
roccosicilia.com/about e 4 altri link

Personalizza canale · Gestire i video

Home Video Podcast Playlist Post

Più recenti · Popolari · Meno recenti

"L'arresto" dei due Penetration Tester... 6:32
177 visualizzazioni · 1 mese fa

Come funziona (più o meno) internet... 24:34
218 visualizzazioni · 1 mese fa

Info Sec Unplugged [14] - Il CISO (seconda parte) 39:37
56 visualizzazioni · 1 mese fa

È più facile attaccare o difendere? 27:57
137 visualizzazioni · 1 mese fa

Info Sec Unplugged [13] - Il CISO (prima parte) 37:17
267 visualizzazioni · 2 mesi fa

Il 15enne che ha violato ... 13:04
83 visualizzazioni · 1 mese fa

Scenari di attacco in contesti wireless 14:38
83 visualizzazioni · 1 mese fa

Info Sec Unplugged [12] - Datacenter Network 45:12
83 visualizzazioni · 1 mese fa

Rocco Sicilia ✓
NTS ITALY GMBH / SRL
Cyber Security Consultant and Researcher // Addicted to hacking
Padua, Veneto, Italy · [Contact info](#)
[My blog](#)

12,078 followers · 500+ connections

Open to · Add profile section · Enhance profile · Resources

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 variante 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

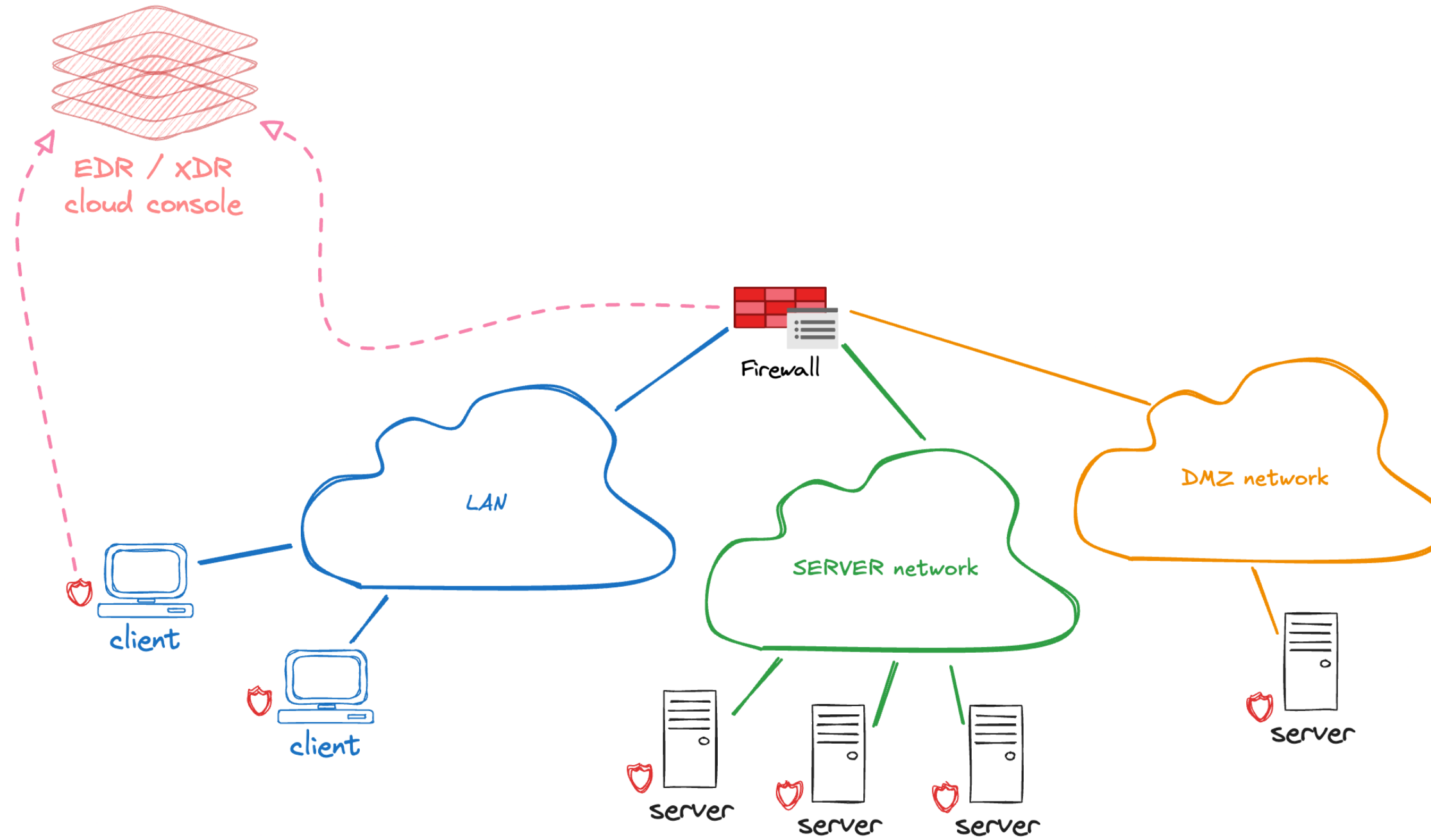
.5 Test

Il funzionamento della componente viene verificato e validato prima del rilascio

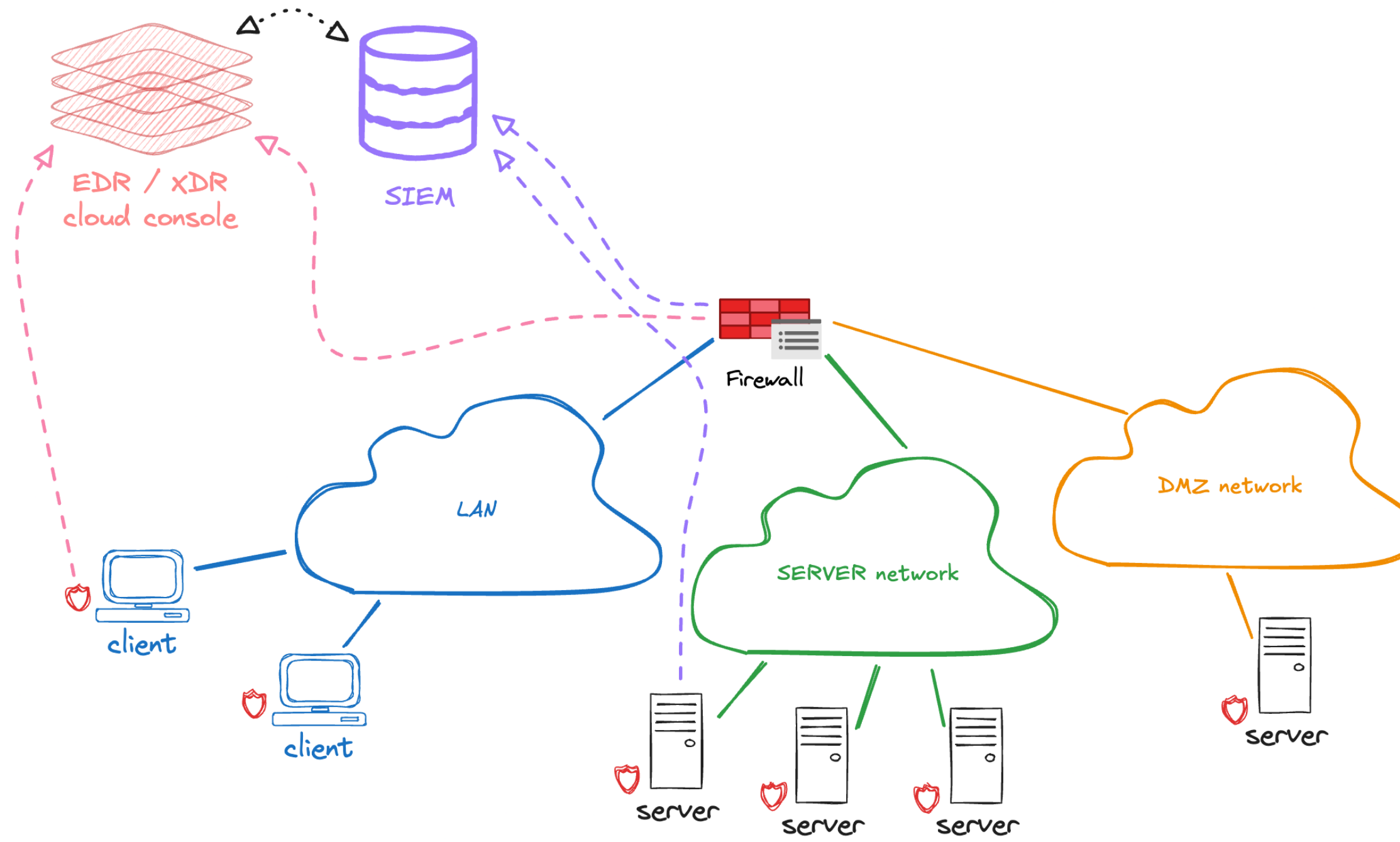
.6 Distribuzione

La funzione di detection e/o prevention viene rilasciata

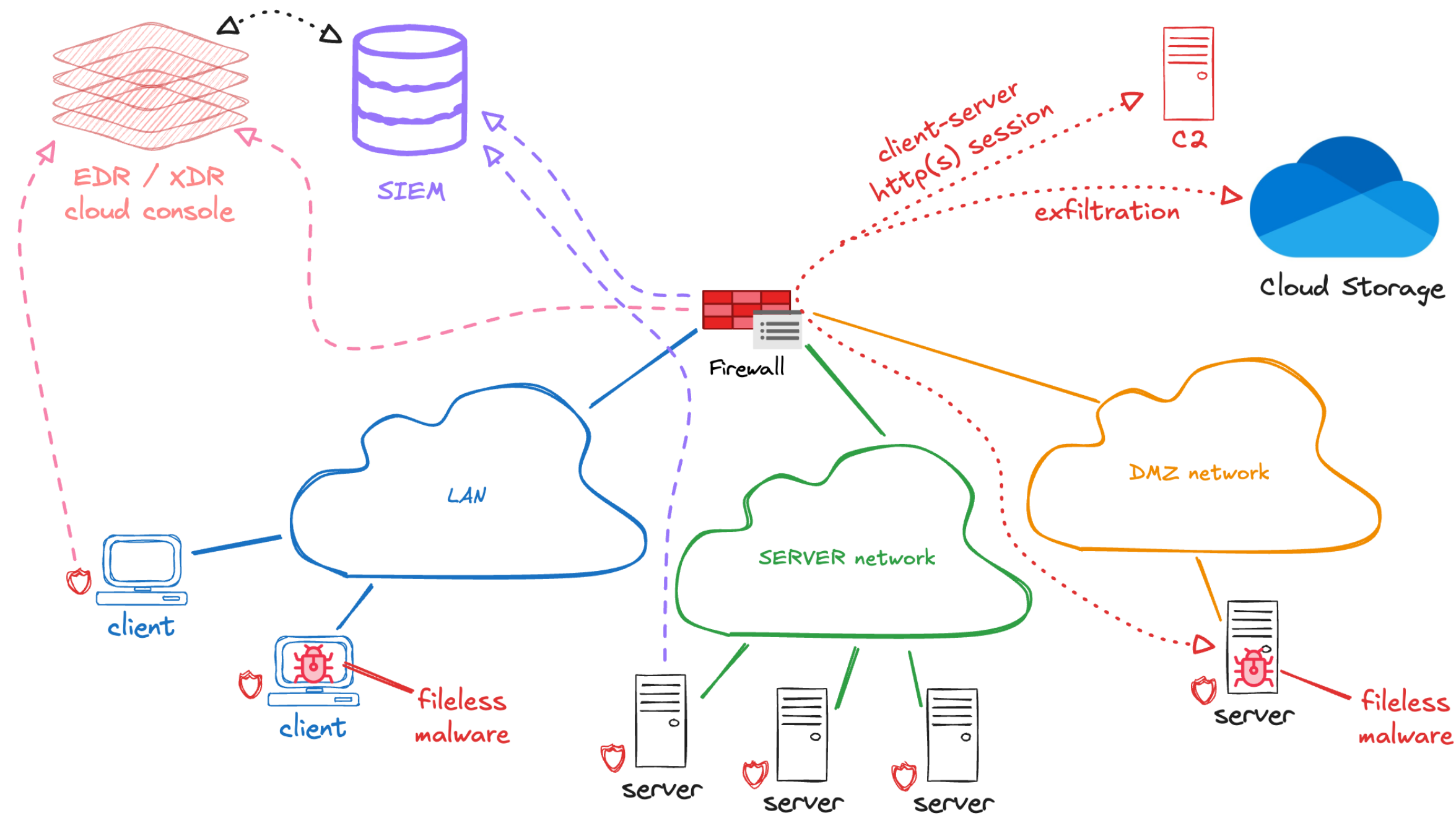
l'ATP ci da una mano



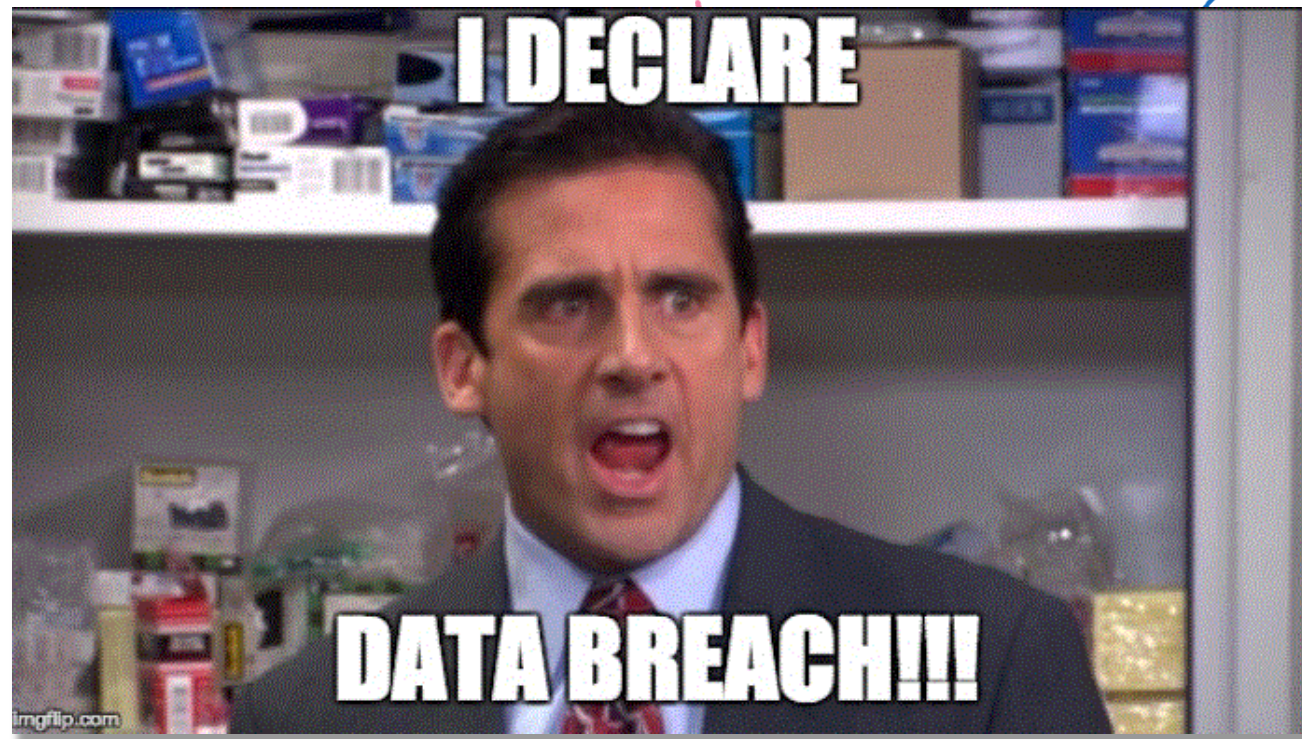
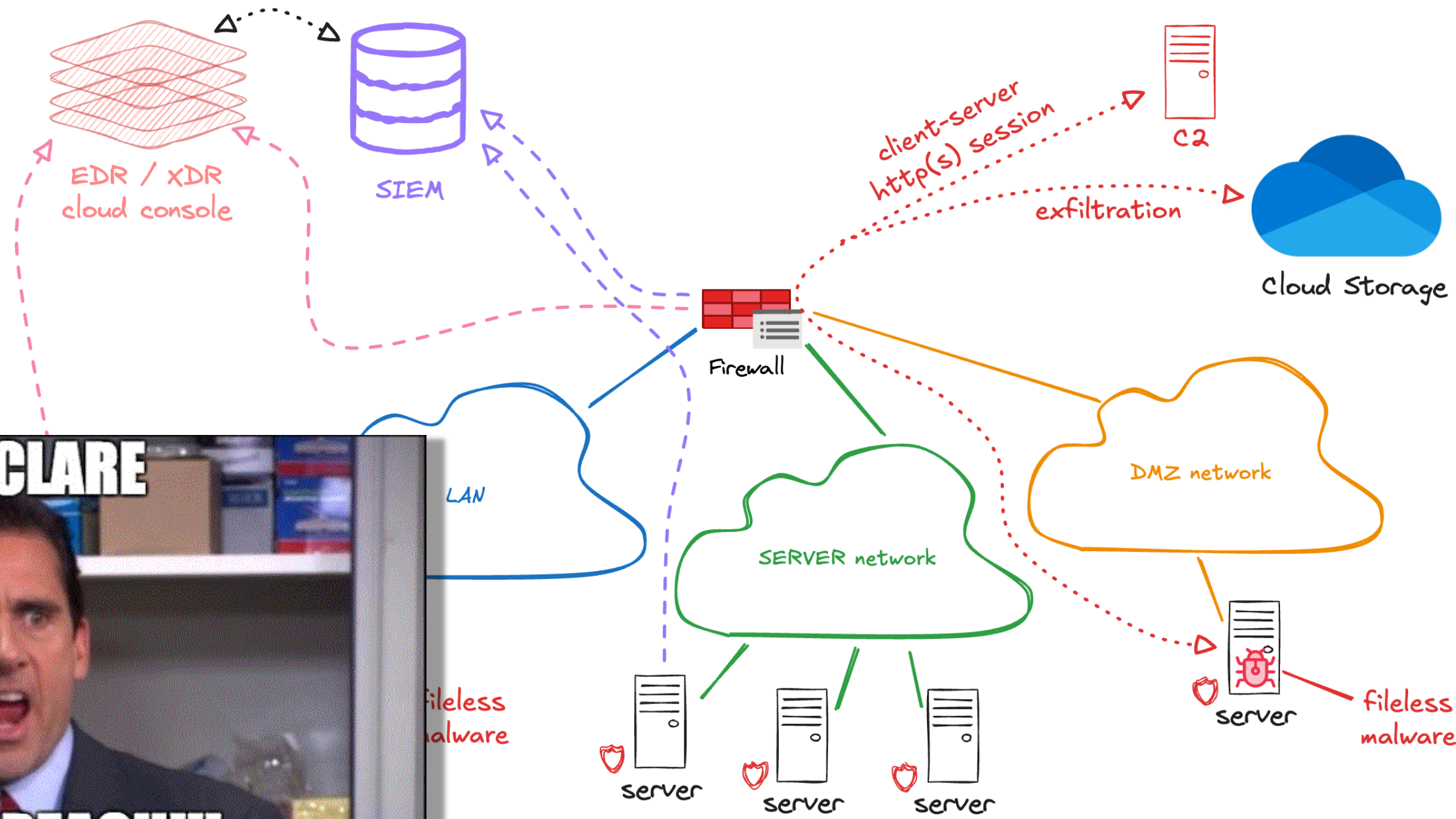
l'ATP ci da una mano



il threat actor si adatta rapidamente



il threat actor si adatta rapidamente



difesa attiva



DMZ coreana

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

difesa attiva

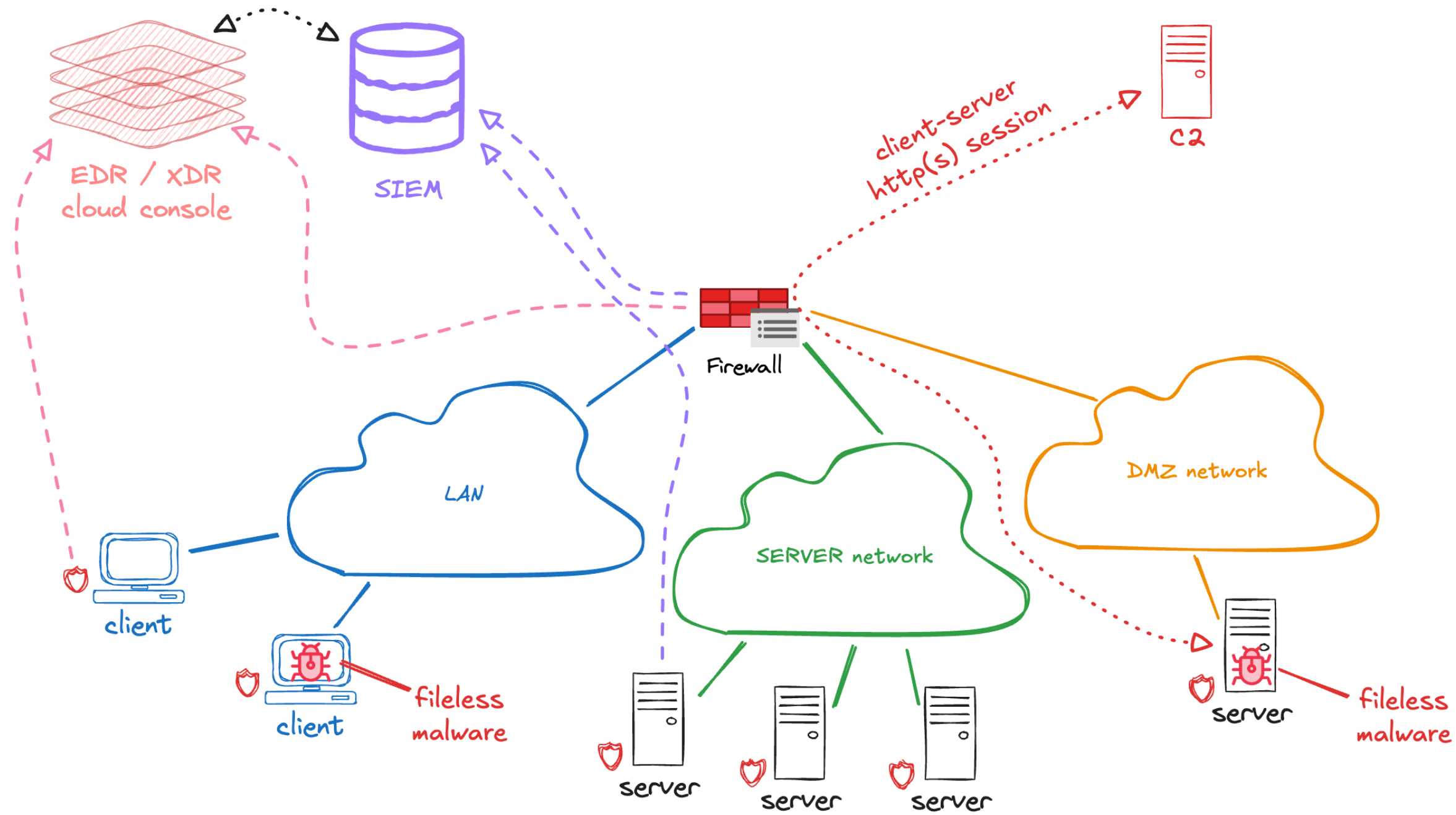


Nel 1974, durante un pattugliamento, viene notato del valore che esce dal sottosuolo.

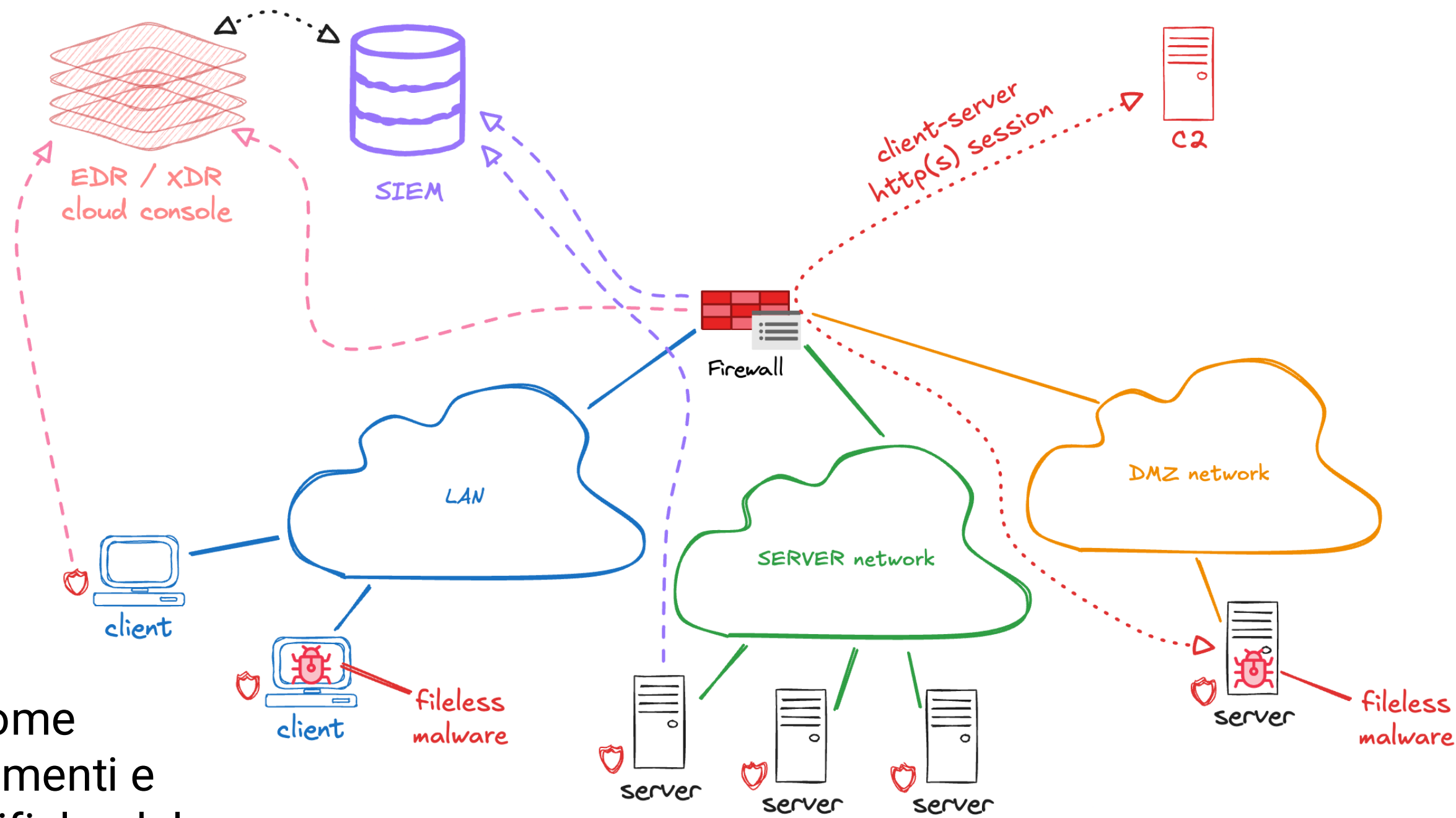
L'indagine porta alla scoperta di un tunnel scavato dall'esercito della Corea del Nord che si estendeva per circa 1 km all'interno del territorio della Corea del Sud.

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

cercare le minacce



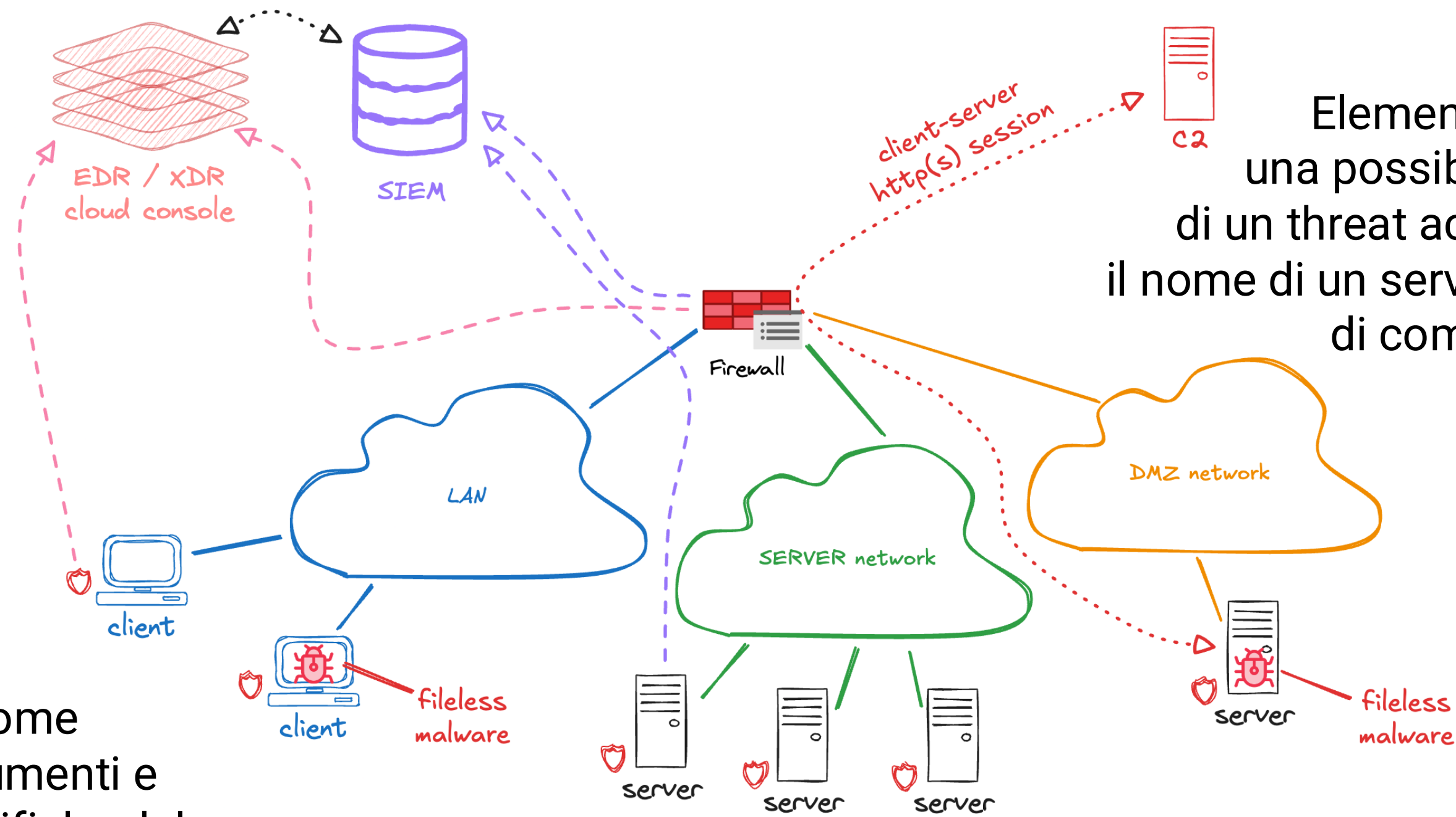
cercare le minacce



Threat Intelligence

Ricerca attiva delle possibili minacce come nuove tecniche, strumenti e caratteristiche specifiche del modus operandi dell'avversario.

cercare le minacce



Threat Intelligence

Ricerca attiva delle possibili minacce come nuove tecniche, strumenti e caratteristiche specifiche del modus operandi dell'avversario.

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, ...

cercare le minacce

Community Score: 78/88
No security vendors flagged this URL as malicious

Security vendors' analysis	Status
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Anty-AVL	Clean
Avira	Clean
benkow.cc	Clean
BitDefender	Clean
Blueliv	Clean
Chong Lua Dao	Clean
CMC Threat Intelligence	Clean
CyberCrime	Clean

Risk: 1
X-Force IP Report: 89.97.19.150

Details:

- Categorization: Dynamic IPs(71%)
- Application: No known application
- Location: AS 12874 : FASTWEB, IT

WHOIS Record:

- Created: Feb 21, 2006
- Updated: Feb 21, 2006
- Registrant Name: S.E.R. S.R.L. SOCIETA EUROPEA RIGENERAZIONE public subnet
- Registrant Organization: FASTWEB-S_E_R_S_R_L_SOCIETA_EUROPEA_RIGENERAZIONE
- Registrant Country or Region: Italy
- Registrar Name: RIPE
- Email: abuse@fastweb.it

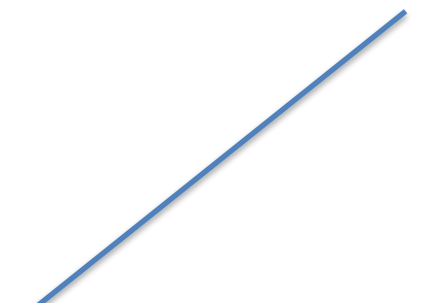
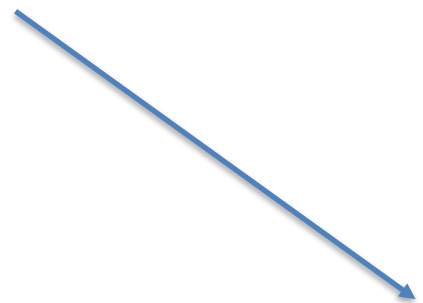
Welcome to Threat Intelligence

Find IP, URL, domain or hash or create a custom request e.g. MITRE:"T1001"

Top submitters:

Country	Count	Percentage
United States	220014	35%
India	34645	5%
Germany	31918	5%
United Kingdom	25233	4%
Australia	24232	4%
Israel	22935	4%
Russian Federation	19840	3%
Spain	16812	3%
Canada	16011	3%

MITRE ATT&CK Matrix: Popular techniques, Malware threats statistics, Popular Suricata rules



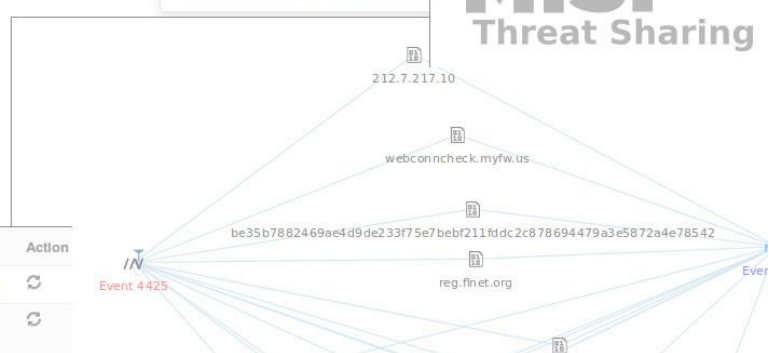
OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Julid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	ttp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

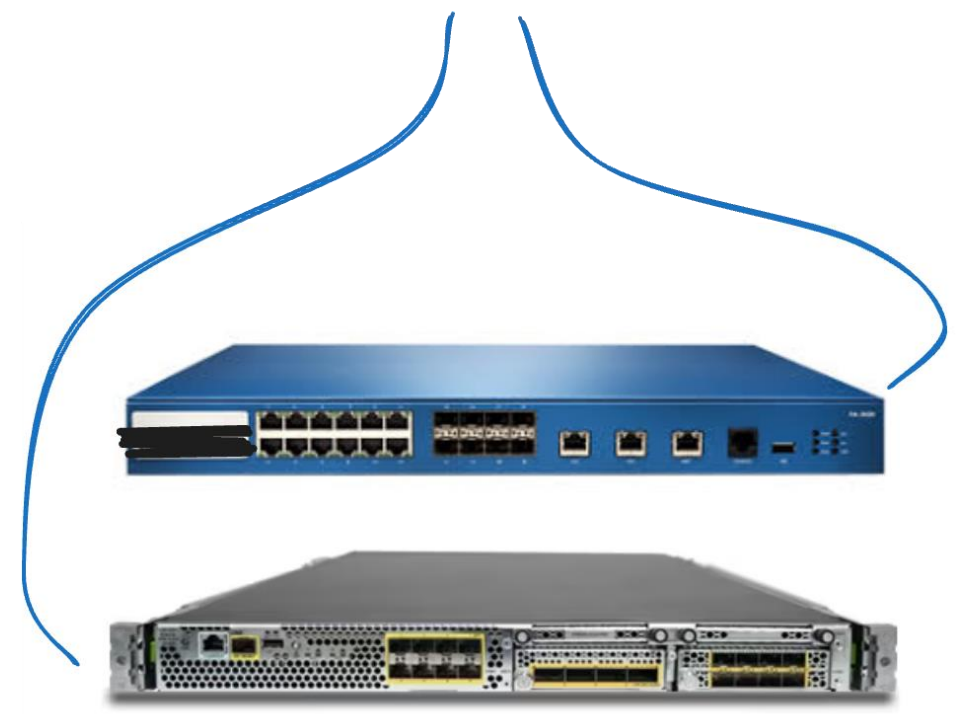
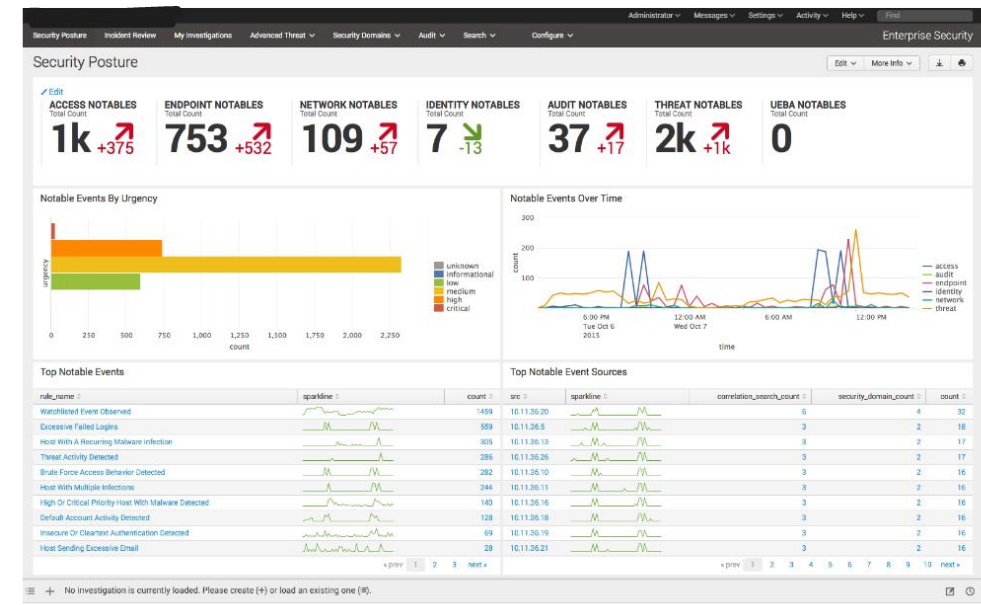
Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

Related Events

- 2016-05-27 (3883)
- 2016-05-23 (3844)
- 2016-05-06 (3828)



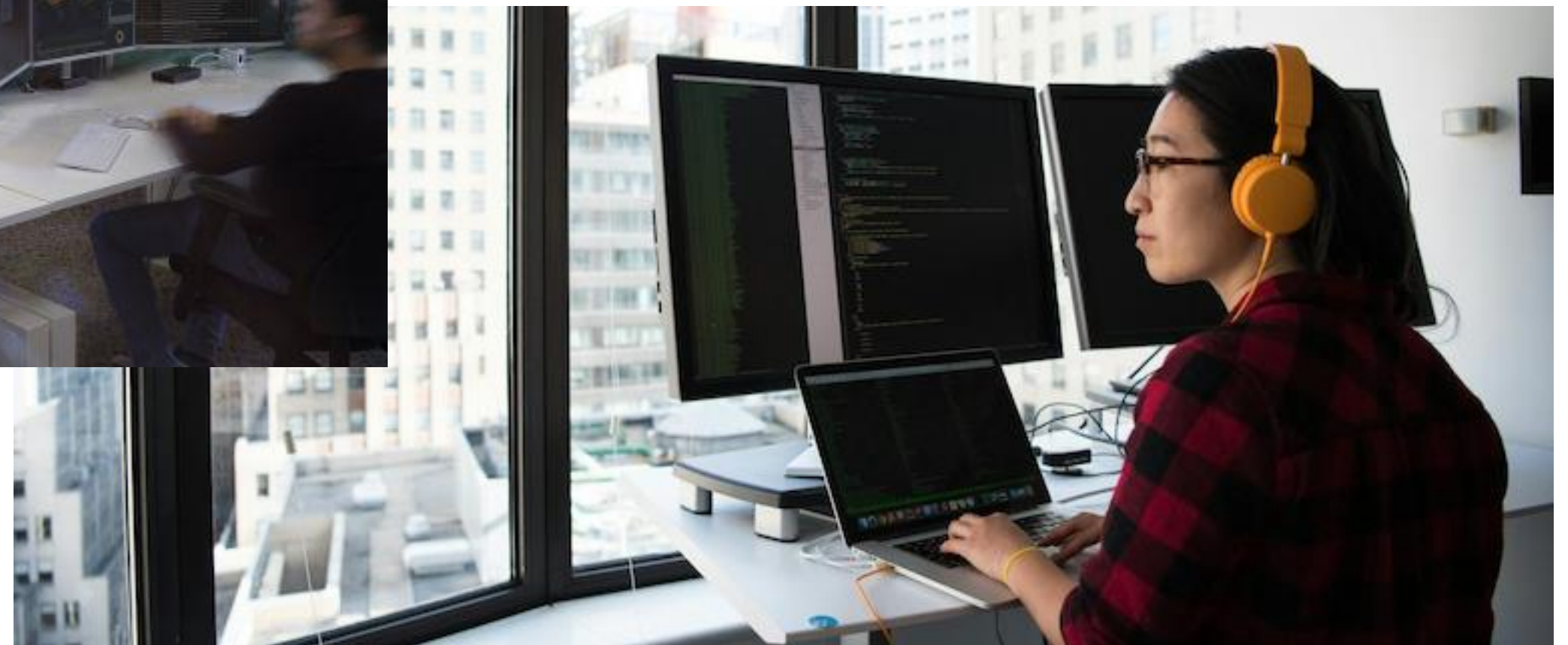
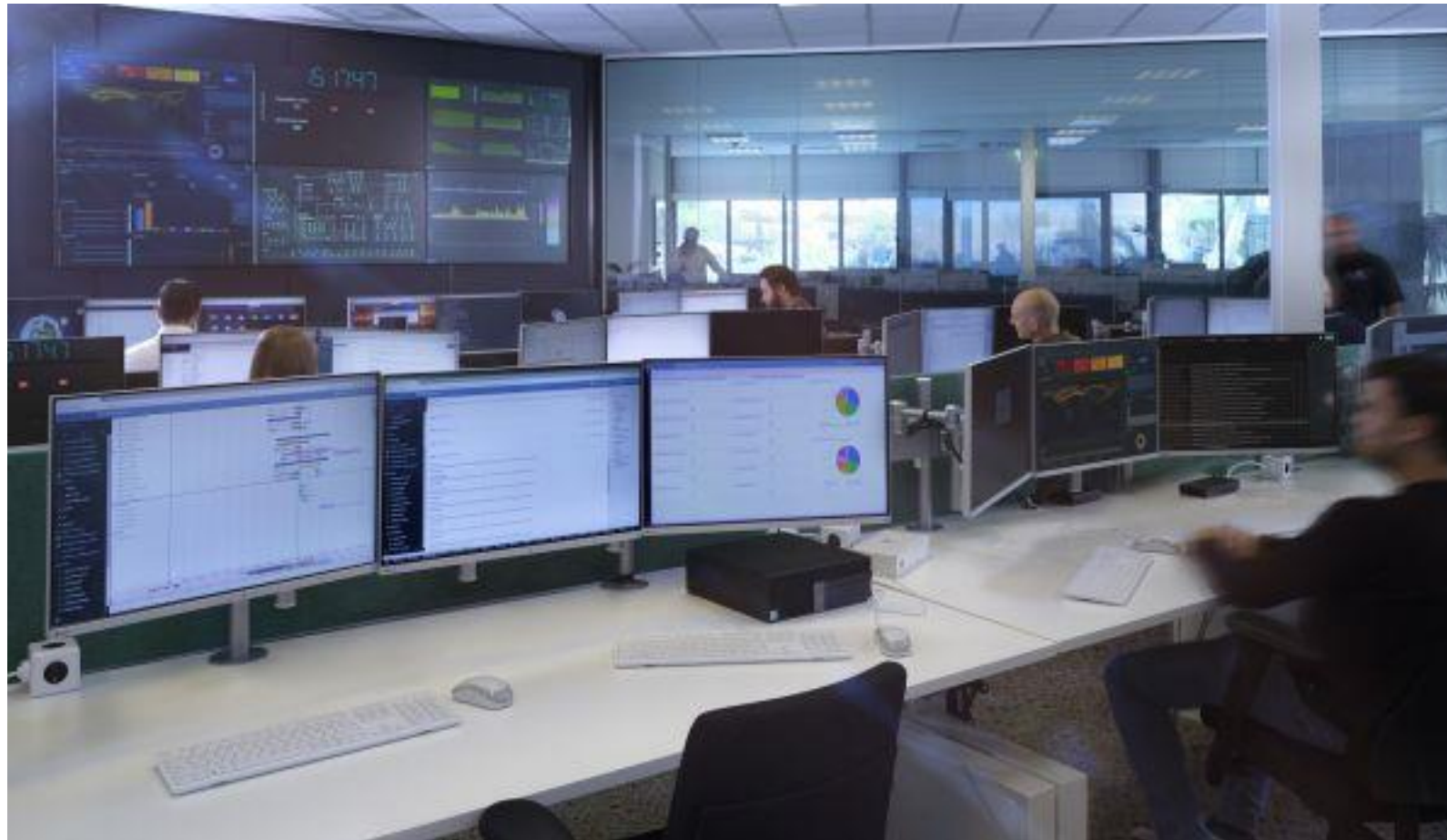
cercare le minacce



NAME	DESCRIPTION	SIGNATURE	THREAT INTELLIGENCE
suchost.exe (a94967d94992...)	Process involved in 3 Alerts	Unsigned	WF Unknown VT Unknown AF [3]
c141a187-582c-7a0a71e92...	Artifact identified in 1 Alert	Unavailable	WF Unknown VT Unknown AF [4]
WMI &P... (812f26fcc66d0...)	Artifact identified in 1 Alert	Unavailable	WF Unknown VT Unknown AF [4]
EXCEL.EXE (6770467c8b85...)	Process involved in 17 Alerts	Microsoft Corporation	WF Benign VT 0/71
powershell... (65554b6cab2...)	Process involved in 12 Alerts	Microsoft Corporation	WF Benign VT 0/70 AF [1]
ofcourseha... (7c56ef6b2383a...)	Process involved in 10 Alerts	Microsoft Corporation	WF Benign VT 0/71
explores.exe (cabb37f96a8...)	Process involved in 7 Alerts	Microsoft Corporation	WF Benign VT 0/70 AF [1]

ALERTS	INSIGHTS						
TIMESTAMP	HOST	USER NAME	SEVERITY	ALERT SOURCE	ACTION	CATEGORY	ALERT
Aug 4th 2020 04:02:31	rza-laptop	RZA-LAPTOP-RZA	High	XDR Analytics BIOC	Detected	Execution	Micr
Aug 4th 2020 04:03:02	rza-laptop	RZA-LAPTOP-RZA	High	XDR Analytics BIOC	Detected	Execution	Micr
Aug 4th 2020 04:21:44	rza-laptop	RZA-LAPTOP-RZA	High	XDR BIOC	Detected	Lateral Movement	16
Aug 4th 2020 04:21:44	rza-laptop	RZA-LAPTOP-RZA	High	XDR BIOC	Detected	Lateral Movement	16

chi se ne occupa?



recap

EDR
Protection
Defense
Hunting
Intelligence
sharing
Threat
SOAR
IOCs
Event
Detection
Anomaly
BloC XDR
SIEM
Security
Actor
OSInt

T-CON2025

WAR ROOM EDITION

Grazie per l'attenzione