

W20D1 – Pratica

Epic Education Srl

Isolamento, rimozione, clear, purge, destroy

Analisi con ANY.RUN

Wazuh (SIEM/XDR)

Simone Giordano

25/11/2025



Contatti:

Tel: 3280063044

Email: mynameisimone@gmail.com

Linkedin: <https://www.linkedin.com/in/simone-giordano-91290652/>

Sommario

Isolamento, rimozione sistema infetto Purge, Destroy e Clear Esercizio 1	3
Traccia.....	3
Esercizio.....	3
Isolamento.....	3
Rimozione.....	4
Clear.....	4
Purge.....	4
Destroy	4
Analisi con ANY.RUN Esercizio facoltativo	5
Traccia.....	5
Analisi link 1	5
Analisi link 2	9
Wazuh (SIEM/XDR) Pratica Extra	11
Traccia	11
Esercizio.....	11

Isolamento, rimozione sistema infetto

Purge, Destroy e Clear

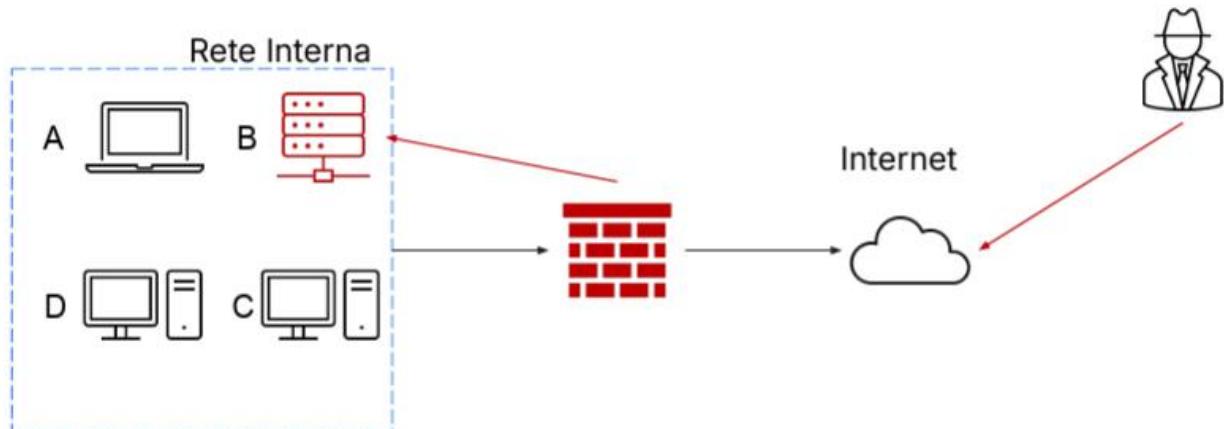
Esercizio 1

Traccia

Con riferimento alla figura nella prossima slide, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete e accedere al sistema tramite Internet.

L'attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere ai seguenti quesiti.

- Mostrate le tecniche di: **Isolamento e Rimozione** del sistema B infetto
- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear

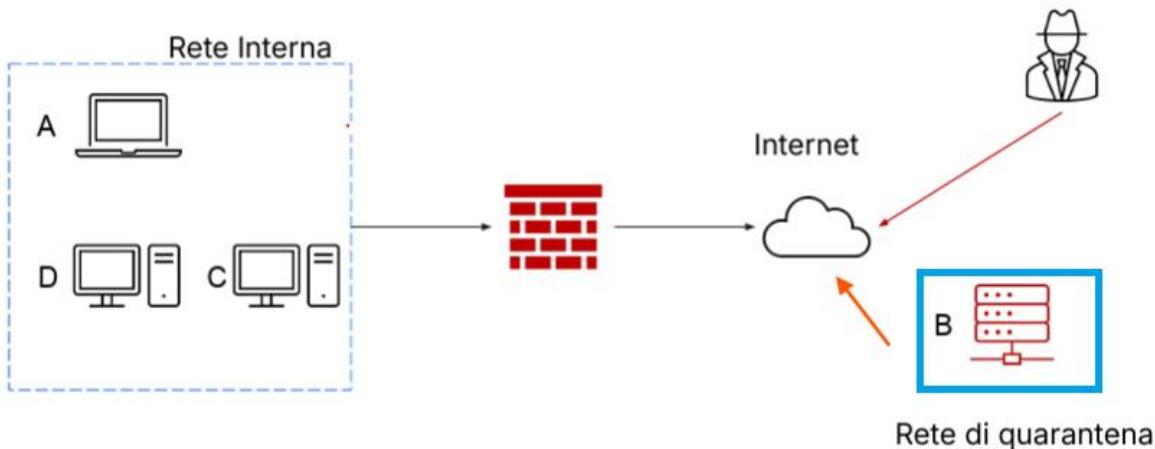


Esercizio

Isolamento

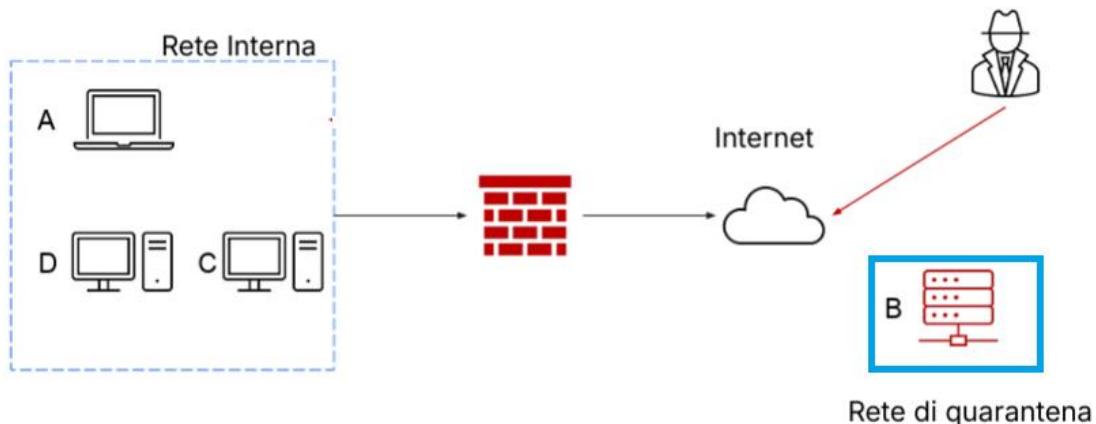
L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. In questo scenario l'attaccante ha ancora

accesso al sistema B tramite internet.



Rimozione

In quest'ultimo scenario, l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.



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.

Purge

Si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, 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.

Analisi con ANY.RUN

Esercizio facoltativo

Traccia

In una grande azienda, due utenti segnalano problemi sui loro computer e chiedono assistenza al reparto CSIRT/SOC (che siamo noi)

Analizzare i seguenti link e fare un piccolo report di quello che si scopre relativo alla segnalazione dell'eventuale attacco:

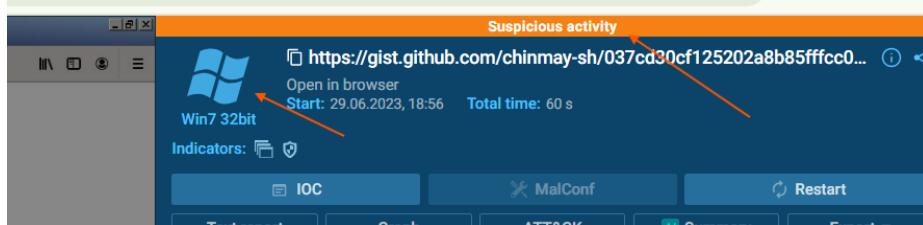
<https://tinyurl.com/linklosco1> e <https://tinyurl.com/linklosco2>

Analisi link 1

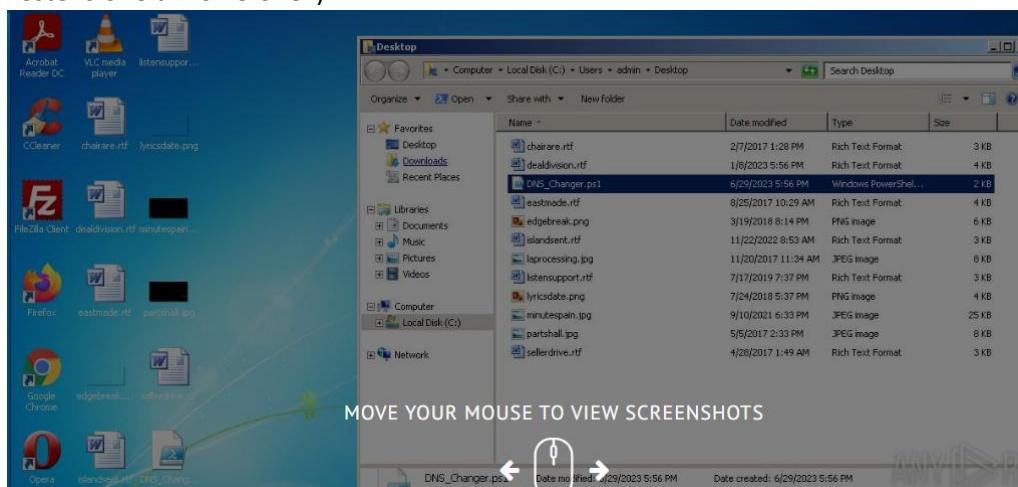
<https://tinyurl.com/linklosco1>

1. Cosa è stato trovato

Aprendo l'analisi notiamo che è stata rilevata un'attività sospetta (Suspicious activity), su sistema operativo **Win7 32bit**.



Guardando la sequenza delle immagini, è stato scaricato ed eseguito il file **DNS_Changer.ps1** (ps1 è l'estensione di PowerShell)



In seguito sono state eseguite le seguenti richieste http, tutte sconosciute (Unknown):

	HTTP Requests	9	Connections	22	DNS Requests	58	Threats	0	⋮
NETWORK	Timeshift	Headers	Rep	PID	Process name	CN	URL		
	2513 ms	GET 200: OK	?	3384	firefox.exe	🇺🇸	http://detectportal		
	3359 ms	POST 200: OK	?	3384	firefox.exe	🇺🇸	http://ocsp.digicer		
FILES	3394 ms	POST 200: OK	?	3384	firefox.exe	🇩🇪	http://r3.o.lencr.or		
	3409 ms	GET 200: OK	?	3384	firefox.exe	🇺🇸	http://detectportal		
DEBUG	3411 ms	POST 200: OK	?	3384	firefox.exe	🇺🇸	http://ocsp.digicer		
	3520 ms	POST 200: OK	?	3384	firefox.exe	🇩🇪	http://r3.o.lencr.or		
	3944 ms	POST 200: OK	?	-	-	🇩🇪	http://r3.o.lencr.or		
	4197 ms	POST 200: OK	?	3384	firefox.exe	🇺🇸	http://ocsp.pki.goc		
	4351 ms	POST 200: OK	?	-	-	🇩🇪	http://r3.o.lencr.or		

Sono state tentate le seguenti connessioni, tutte sconosciute.

	HTTP Requests	9	Connections	22	DNS Requests	58	Threats	0	⋮
NETWORK	Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Dom
	1451 ms	UDP	?	2248	svchost.exe	?	239.255.255.250	1900	-
	1458 ms	UDP	?	4	System	?	192.168.100.255	137	-
FILES	1461 ms	UDP	?	1076	svchost.exe	?	224.0.0.252	5355	-
	2461 ms	UDP	?	4	System	?	192.168.100.255	138	-
DEBUG	2463 ms	TCP	?	3384	firefox.exe	🇺🇸	34.107.221.82	80	deter
	2511 ms	TCP	?	3384	firefox.exe	🇺🇸	140.82.121.4	443	gist.c
	2554 ms	TCP	?	3384	firefox.exe	🇺🇸	34.149.100.209	443	firefc
	3263 ms	TCP	?	3384	firefox.exe	🇺🇸	34.107.221.82	80	deter
	3340 ms	TCP	?	3384	firefox.exe	🇺🇸	52.24.231.34	443	locat
	3351 ms	TCP	?	3384	firefox.exe	🇺🇸	192.229.221.95	80	ocsp
	3358 ms	TCP	?	3384	firefox.exe	🇺🇸	34.149.100.209	443	firefc
	3393 ms	TCP	?	3384	firefox.exe	🇩🇪	23.55.163.56	80	a188
	3408 ms	TCP	?	3384	firefox.exe	🇺🇸	34.107.221.82	80	deter
	3444 ms	TCP	?	3384	firefox.exe	🇺🇸	185.199.108.133	443	gist.c
	3480 ms	TCP	?	3384	firefox.exe	🇺🇸	34.160.144.191	443	conta
	3517 ms	TCP	?	3384	firefox.exe	🇺🇸	172.217.16.138	443	safel
	3876 ms	TCP	?	3384	firefox.exe	🇺🇸	34.160.144.191	443	conta
	4050 ms	TCP	?	3384	firefox.exe	🇺🇸	34.117.121.53	443	firefc
	4196 ms	TCP	?	3384	firefox.exe	🇺🇸	142.250.186.35	80	ocsp
	4349 ms	TCP	?	3384	firefox.exe	🇺🇸	34.117.65.55	443	push
	4466 ms	TCP	?	3384	firefox.exe	🇺🇸	34.117.65.55	443	push
	4483 ms	TCP	?	3384	firefox.exe	🇺🇸	13.32.121.49	443	d228

Vediamo inoltre che sono state effettuate anche una serie di richieste DNS:

	HTTP Requests	9	Connections	22	DNS Requests	58	Threats	0
NETWORK	Timeshift	Status	Rep	Domain		IP		
	2423 ms	Responded	?	detectportal.firefox.com	34.107.221.82			
	2425 ms	Responded	?	prod.detectportal.prod.cloudops...	34.107.221.82			
	2425 ms	Responded	?	prod.detectportal.prod.cloudops...	2600:1901:0:38d7::			
	2426 ms	Responded	?	gist.github.com	140.82.121.4			
	2426 ms	Responded	?	github.com	140.82.121.4			
	2426 ms	Requested	?	github.com	IP Addresses not found			
	2427 ms	Responded	?	firefox.settings.services.mozilla.c...	34.149.100.209			
	2427 ms	Responded	?	prod.remote-settings.prod.webserv...	34.149.100.209			
	2427 ms	Requested	?	prod.remote-settings.prod.webserv...	IP Addresses not found			
	2428 ms	Responded	?	example.org	93.184.216.34			
					52.24.231.34			
					44.233.10.108			
					54.244.114.149			
					52.42.53.182			
					44.233.226.27			
					52.34.120.119			
					192.0.0.171			
					192.0.0.170			
	3225 ms	Responded	?	ipv4only.arpa	93.184.216.34			
	3225 ms	Responded	?	example.org	93.184.216.34			
	3225 ms	Responded	?	example.org	93.184.216.34			
					52.34.120.119			
					44.233.226.27			
					52.42.53.182			
					54.244.114.149			
	3226 ms	Responded	?	locprod2-elb-us-west-2.prod.moza...	54.244.114.149			

In tutte queste operazioni eseguite, in seguito all'esecuzione del file non sono state rilevate minacce:

	HTTP Requests	9	Connections	22	DNS Requests	58	Threats	0
NETWORK	Timeshift	Status	Class		PID	Process name		
No data								

Possiamo visualizzare inoltre tutti i processi attivati dall'esecuzione del file e le relative informazioni:



Nella scheda MITRE ATT&CK Matrix notiamo che il file eseguito ha adottato la tecnica "Command and Scripting Interpreter" ritenuta pericolosa.

MITRE ATT&CK Matrix

Tactics	3	Techniques	4	Events	29	Enterprise & Mobile tactics	Danger (1)	Warning (5)			
Initial access		Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	E
Command and Scripting Interpreter (1/13)	PowerShell	Create Account (1/3)	Local Account	Query Registry	20		Danger (1)	Warning (5)			
		1									
		5									
	User Execution (1/5)	Malicious File	1								
	Subtechniques T1059										

Techniques details

Get to know what this threat is about

Subtechniques [T1059](#)

"Command and Scripting Interpreter"

Permissions required:

Data sources:

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting.

Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -ExecutionPolicy Bypass -File "C:\Users\admin\Desktop\DNS_Changer.ps1"

Analisi link 2

<https://tinyurl.com/linklosco2>

In questa analisi sono state rilevate 3 minacce.

HTTP Requests	36	Connections	82	DNS Requests	36	Threats	3
Timeshift	Class			PID	Process name	Message	
175.91 s	Potentially Bad Traffic			1076	svchost.exe	ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)	
176.50 s	Malware Command and Control Activity			3824	csc.exe	ET JA3 Hash - Remcos 3.x TLS Connection	
176.50 s	A Network Trojan was detected			-	-	REMOTE [ANY.RUN] REMCOS JA3 Hash	

Potential Bad Traffic

svchost.exe ha effettuato una richiesta DNS verso il dominio sospetto **con-ip.com**

Threat details

Here are the details of the threat

Main Suricata rule

Potentially Bad Traffic

ET INFO DNS Redirection Service Domain in DNS Lookup (con-ip .com)

Src / Dst 192.168.100.36 : 51018 ⇄ 192.168.100.2 : 53 ↴
Timeshift 175.91 s
SID 2037787
Src IP 192.168.100.36
Dst IP 192.168.100.2
Src Port 51018
Dst Port 53

Malware Command and Control Activity

CSC.exe

176.50 s Malware Command and Control Activity 3824 csc.exe ET JA3 Hash - Remcos 3.x TLS Connection

JA3 Hash: è come un'impronta digitale unica per il modo in cui un software (in questo caso, il malware Remcos) avvia una connessione sicura (TLS/HTTPS).

Remcos: è un tipo di software dannoso (trojan ad accesso remoto o RAT) usato per prendere il controllo dei computer infetti.

Main

Stream data

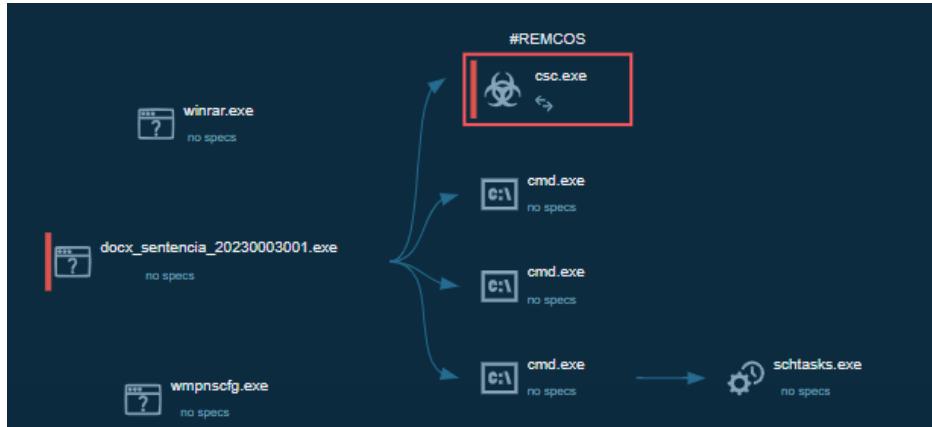
Suricata rule

Malware Command and Control Activity Detected

ET JA3 Hash - Remcos 3.x TLS Connection

Src / Dst 192.168.100.36 : 49223 ⇄ 181.141.7.178 : 7770 ↴
Timeshift 176.50 s
SID 2036594
Src IP 192.168.100.36
Dst IP 181.141.7.178
Src Port 49223
Dst Port 7770

Come vediamo dallo schema sotto, il processo **CSC.exe** deriva dal **DOCX_SENTENCIA_20230003001.exe**



Threat Verdict: Malicious (100 OUT OF 100)

Process information:

- Username: admin
- File: T:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe
- Start: 181.04 s

File Information:

- Company: Microsoft Corporation
- Description: Visual C# Compiled Line Compiler
- Version: 4.0.30319.34509 built by FX452RTM0DR

Command line: T:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe

Timeline of the process:

- 0 s: REMCOS detected by memory dump
- 181.04 s: Remcos is detected
- 181.04 s: Without files like Keylogger logs
- 181.04 s: T1012 Query Registry (1)
- 181.04 s: Reads the Internet Settings
- 181.04 s: T1371 Non-Standard Port (1)
- 181.04 s: Connects to unusual port
- 181.04 s: Other

A Network Trojan was detected

176.50 s A Network Trojan was detected REMOTE [ANY.RUN] REMCOS JA3 Hash

Il traffico corrisponde al fingerprint crittografico (JA3) del trojan Remcos

A Network Trojan was detected

REMOTE [ANY.RUN] REMCOS JA3 Hash

Src / Dst	192.168.100.36:49223 <--> 181.141.7.178:7770
Timeshift	176.50 s
SID	8000033
Src IP	192.168.100.36
Dst IP	181.141.7.178
Src Port	49223
Dst Port	7770

Wazuh (SIEM/XDR)

Pratica Extra

Traccia

Installare Wazuh (SIEM/XDR) in versione OVA nella rete laboratorio e il suo agent su Kali. Collegare l'agent a Wazuh e interpretare le informazioni raccolte (appena avviato le informazioni saranno poche e Wazuh necessita di ulteriori configurazioni di cui non ci occuperemo).

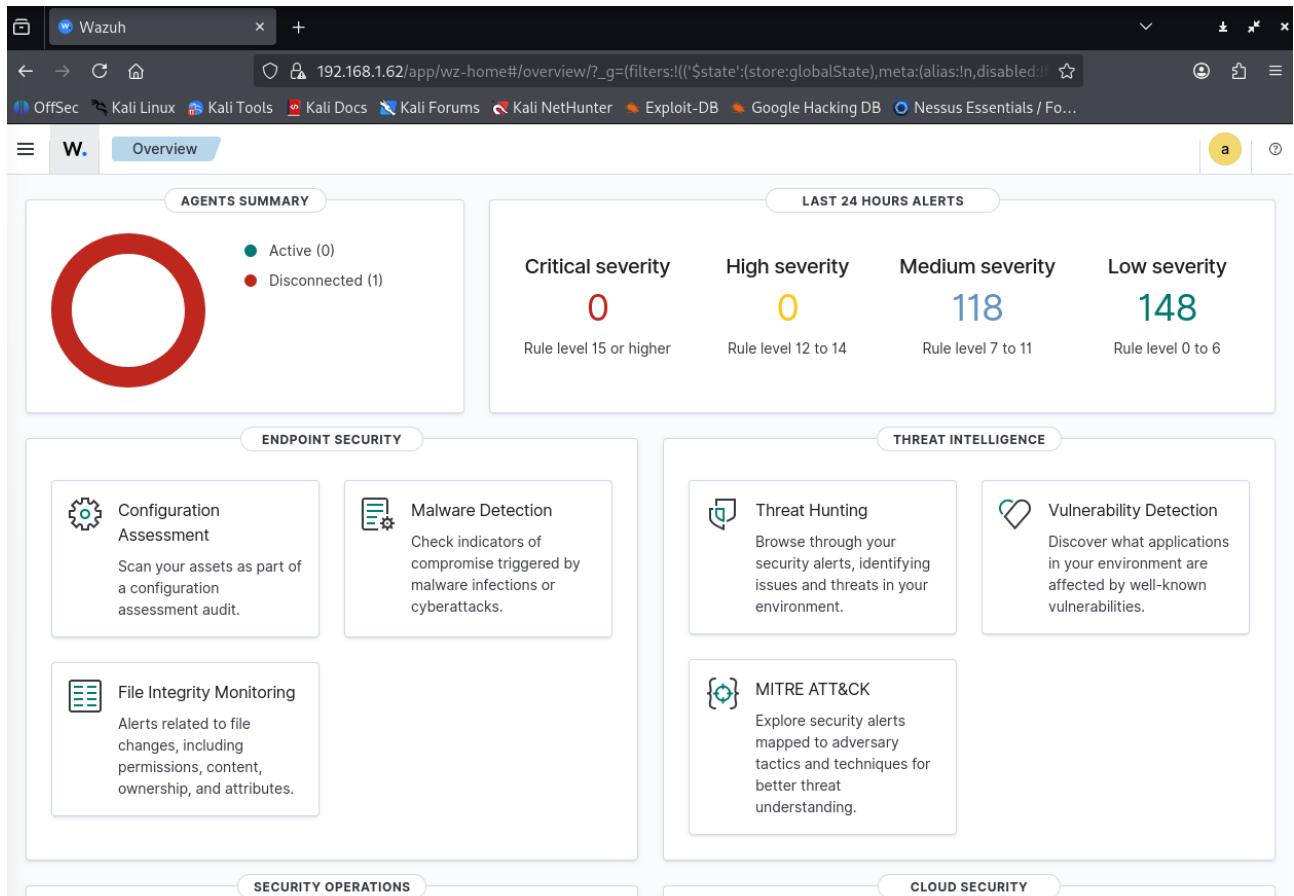
Wazuh OVA (impostare correttamente la rete in modo che Wazuh e Kali siano nella stessa rete):
<https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html>

Wazuh agent (seguire APT e Systemd): <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html>

Enrollment dell'agent suggerito: <https://documentation.wazuh.com/current/user-manual/agent/agent-enrollment/enrollment-methods/via-agent-configuration/linux-endpoint.html>

Esercizio

Ho installato l'OVA di Wazuh e l'ho configurato nella stessa rete di Kali, poi ho installato l'agent di Wazuh su Kali.



Ho impostato la variabile WAZUH_MANAGER con l'ip del server Wazuh

```
[root@kali]# WAZUH_MANAGER="192.168.1.62" apt-get install wazuh-agent
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
wazuh-agent is already the newest version (4.14.1-1).
The following packages were automatically installed and are no longer
needed and can be safely removed: libcurl4 libcurl4-openssl-dev libcurl4-openssl-dev:i386
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Avvio il demone

```
[root@kali]# systemctl daemon-reload  
[root@kali]# systemctl enable wazuh-agent  
[root@kali]# systemctl start wazuh-agent
```

Confermo l'agent installato.

