File integrity monitoring

Introduzione al File Integrity Monitoring (FIM) con Wazuh su macchine Ubuntu

Il *File Integrity Monitoring* (FIM) è una tecnica fondamentale per garantire la sicurezza dei sistemi informatici, soprattutto in contesti in cui la protezione dei dati è critica. Il FIM consente di monitorare e rilevare modifiche ai file e alle directory di un sistema, fornendo visibilità in tempo reale su eventuali cambiamenti sospetti. Questo è particolarmente utile per individuare e rispondere tempestivamente a potenziali minacce come intrusioni non autorizzate o modifiche ai file di sistema.

Obiettivi del Documento

Questo documento si concentra sulla configurazione di un sistema di monitoraggio dell'integrità dei file utilizzando *Wazuh*, una piattaforma open-source per la sicurezza informatica e la gestione degli eventi (SIEM). Verranno illustrati i passaggi necessari per configurare un agente Wazuh su una macchina Ubuntu e come, attraverso la dashboard di Wazuh, sia possibile visualizzare e gestire le modifiche effettuate ai file presenti in una specifica directory.

Importanza del FIM nella Sicurezza Informatica

Un aspetto critico della sicurezza informatica è la capacità di rilevare accessi non autorizzati e modifiche ai file sensibili. Molti attacchi informatici sfruttano vulnerabilità nelle configurazioni di rete, come porte aperte (ad esempio RDP - Remote Desktop Protocol) o accessi SSH non adeguatamente protetti. Una volta ottenuto l'accesso a una macchina, gli attaccanti possono inserire file malevoli all'interno di directory specifiche. Tali file possono essere utilizzati per esfiltrare dati o per lanciare ulteriori attacchi all'interno della rete.

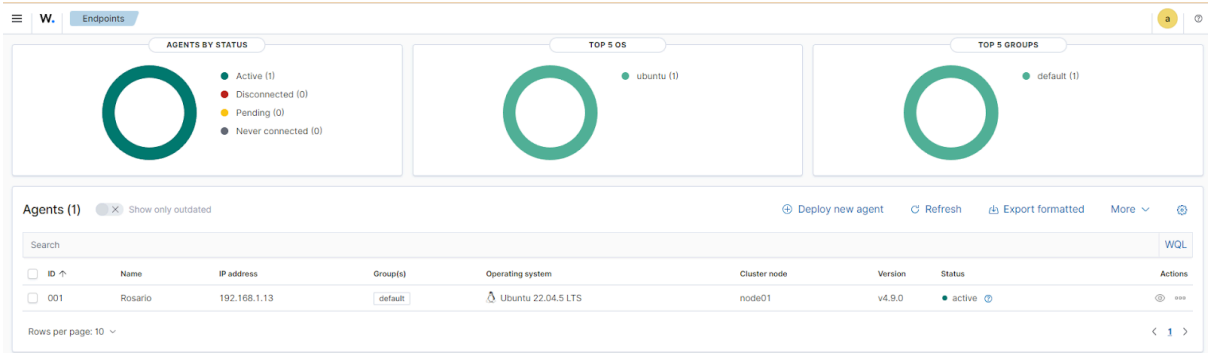
Un esempio comune di vettori di attacco include:

- **Accessi RDP non protetti**: Un servizio RDP non adeguatamente configurato può permettere a un attaccante di accedere in remoto a una macchina, manipolando i file all'interno di directory critiche.
- **Attacchi SSH**: Un attaccante che riesce a ottenere accesso tramite credenziali SSH compromesse può caricare file nella macchina e modificarne la configurazione, utilizzandola come punto d'appoggio per esfiltrare dati o lanciare ulteriori attacchi.

In questo contesto, un sistema FIM come Wazuh gioca un ruolo chiave nel rilevare tempestivamente queste azioni, consentendo agli amministratori di sicurezza di intervenire rapidamente per bloccare l'attacco e mitigare i danni.

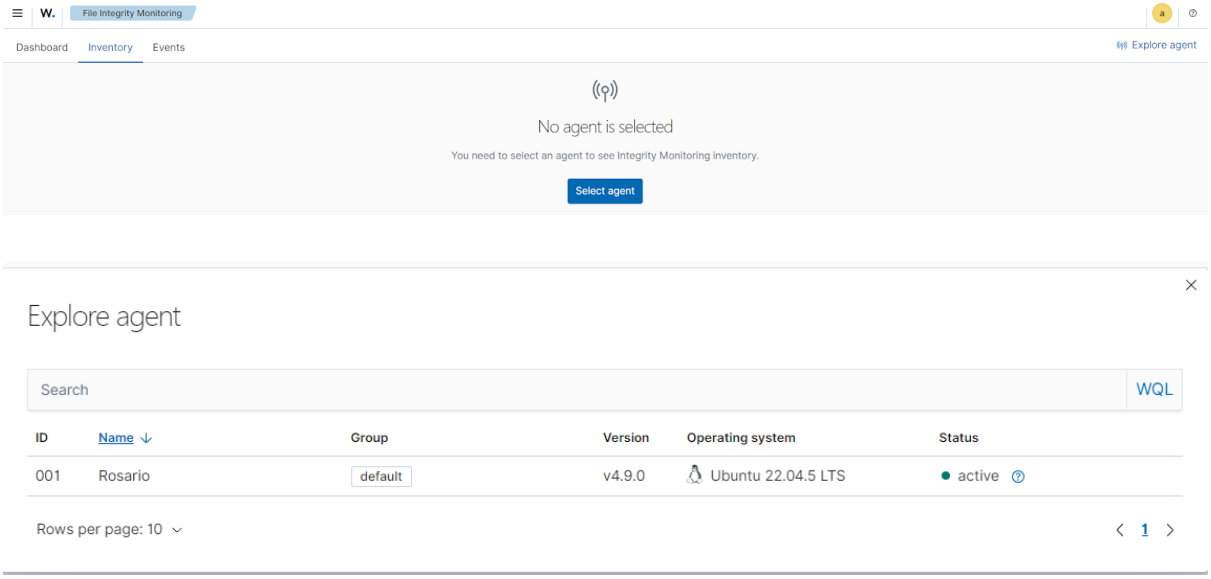
1) Agent di Ubuntu

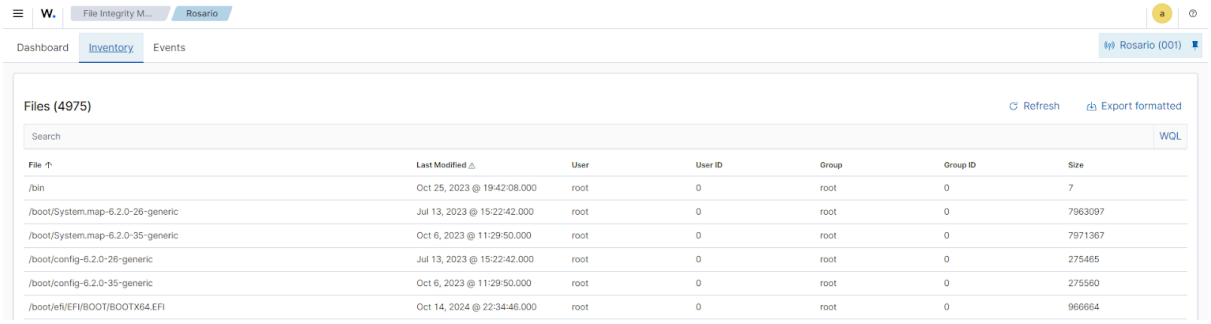
Il nostro lavoro si concentrerà sulla funzionalità di file integrity monitoring di Wazuh. A tal fine, useremo un sistema Ubuntu 22.04 con un agent Wazuh configurato e funzionante, come verificabile dalla dashboard.



2) FIM sulla Dashboard di Wazuh

Valuteremo l'efficacia del monitoraggio dell'integrità dei file su una macchina Ubuntu 22.04, dove è presente e attivo un agente Wazuh.





3) Modifica del file di configurazione dell'agent di Ubuntu

```
root@Rosario:/var/ossec/etc# ls
client.keys                 localtime          shared
internal_options.conf       ossec-backup.conf  wpk_root.pem
local_internal_options.conf ossec.conf
```

Per monitorare le modifiche alle directory di nostro interesse, abbiamo modificato il file di configurazione di Wazuh. Le modifiche principali sono 3, abbiamo abilitato il modulo di monitoraggio dell'integrità dei file (<disabled>yes</disabled>), abbiamo configurato un intervallo di 10 secondi che garantisce un rapido rilevamento delle anomalie alla directory da parte di Wazuh ed infine nella sezione "Directories to check" inseriamo la directory che verrà monitorata (nel nostro caso /home/public).

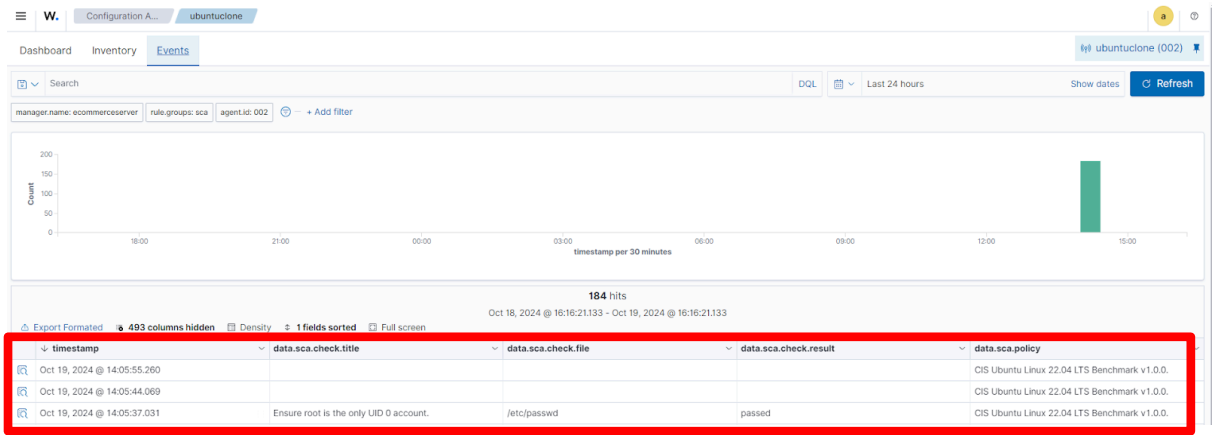
```
  <!-- File integrity monitoring -->
  <syscheck>
    <disabled>no</disabled>

    <!-- Frequency that syscheck is executed default every 12 hours -->
    <frequency>10</frequency>

    <scan_on_start>yes</scan_on_start>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories>/etc,/usr/bin,/usr/sbin</directories>
    <directories>/bin,/sbin,/boot,/home/public</directories>
```

Procediamo con il riavvio del servizio affinché le modifiche apportate siano effettive.

```
root@Rosario:/var/ossec/etc# systemctl daemon-reload
root@Rosario:/var/ossec/etc# systemctl restart wazuh-agent
```

4) Registrazione eventi

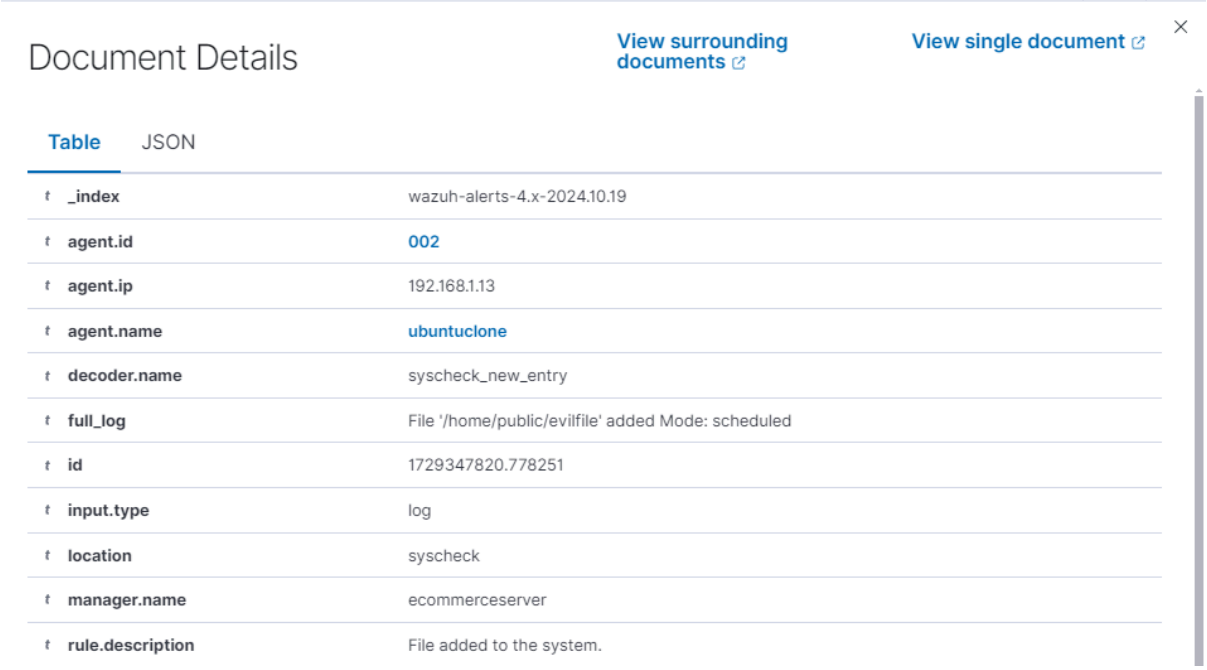
La schermata della registrazione degli eventi non mostra attualmente alcuna attività o anomalia rilevata.



Aggiungiamo un file alla directory monitorata.

```
root@Rosario:/home/public# touch evilfile
root@Rosario:/home/public# ls
evilfile
```

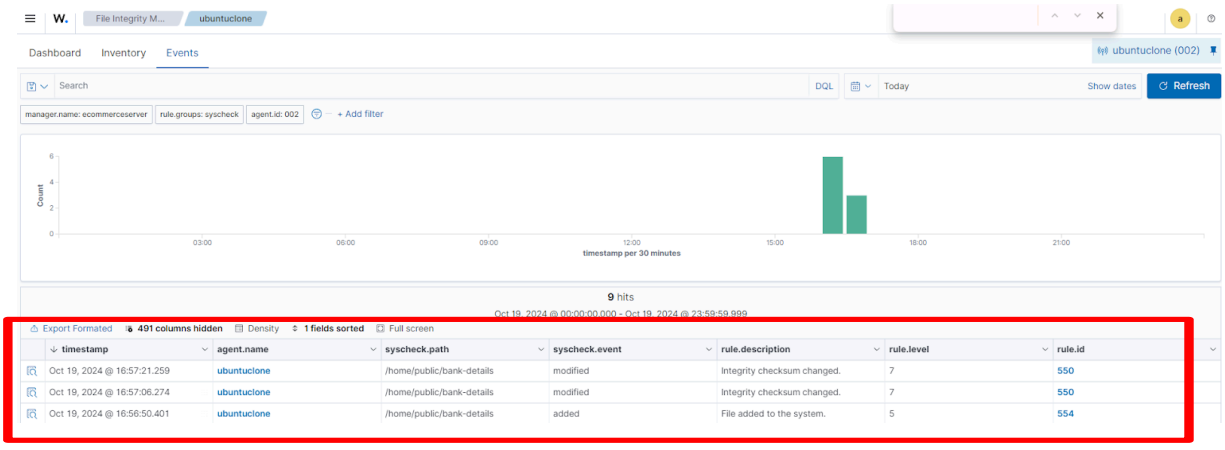
t **syscheck.md5_after**	d41d8cd98f00b204e9800998ecf8427e
t **syscheck.mode**	scheduled
syscheck.mtime_after	Oct 19, 2024 @ 16:23:30.000
t **syscheck.path**	/home/public/evilfile
t **syscheck.perm_after**	rw-r--r--
t **syscheck.sha1_after**	da39a3ee5e6b4b0d3255bfef95601890afd80709
t **syscheck.sha256_after**	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855



Nella sezione 'eventi' di Wazuh è ora visibile il file appena aggiunto. Da questa sezione è possibile monitorare tutte le modifiche che avvengono nella directory specificata.

L'hash del file, reperibile nei 'Dettagli del documento', può essere sottoposto ad analisi su piattaforme di threat intelligence come VirusTotal per determinare la reputazione.

Se un attaccante dovesse compromettere un file contenente dati bancari e modificarne il contenuto, Wazuh sarebbe in grado di rilevare questa intrusione.



5) Rilevazione modifiche chiavi di registro

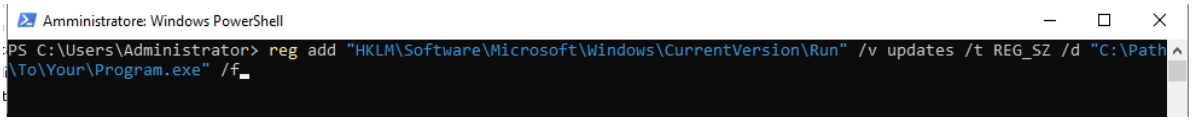
La **persistenza** è una tecnica utilizzata dagli attaccanti per mantenere l'accesso a un sistema compromesso anche dopo un riavvio. Una delle modalità comuni per ottenere questa persistente è modificare le chiavi di registro di Windows. Ad esempio, utilizzando la chiave `"HKLM\Software\Microsoft\Windows\CurrentVersion\Run"`, un attaccante può configurare un programma malevolo per essere eseguito automaticamente all'avvio del sistema.

Questa tecnica è documentata nel framework MITRE ATT&CK come **"Registry Run Keys / Startup Folder"** (ID T1547.001).

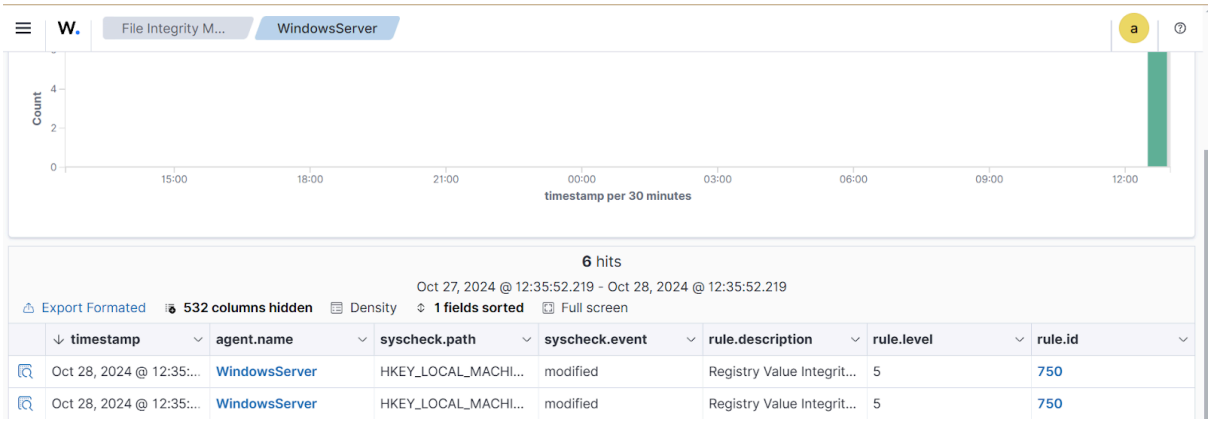
Monitoraggio con FIM

I sistemi di **File Integrity Monitoring (FIM)**, come Wazuh, sono in grado di monitorare le modifiche alle chiavi di registro. Quando un agente FIM rileva una modifica a una chiave di registro critica, può segnalare un'attività sospetta, fornendo così un'indicazione di potenziali compromissioni. Questo monitoraggio è fondamentale per garantire la sicurezza dei sistemi e per rispondere rapidamente a minacce informatiche.

Ora vediamo su una macchina Windows cosa succede se apporto modifiche ad una chiave di registro, in breve col seguente comando il programma specificato verrà aggiunto all'elenco dei programmi che si avviano automaticamente all'accensione del computer. Ogni volta che il sistema operativo Windows viene avviato, cercherà e avvierà il programma specificato.



Possiamo notare come Wazuh riesca a rilevare tali attività:



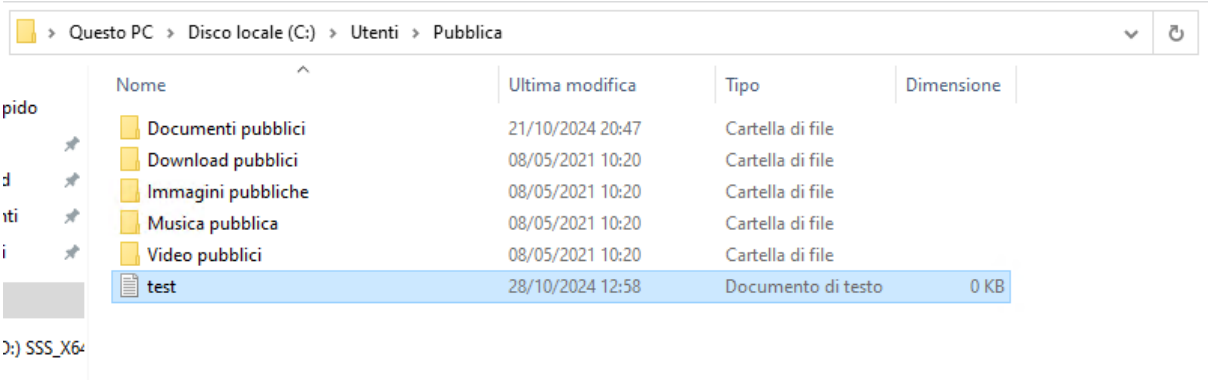
6) Monitoraggio in real time di una directory

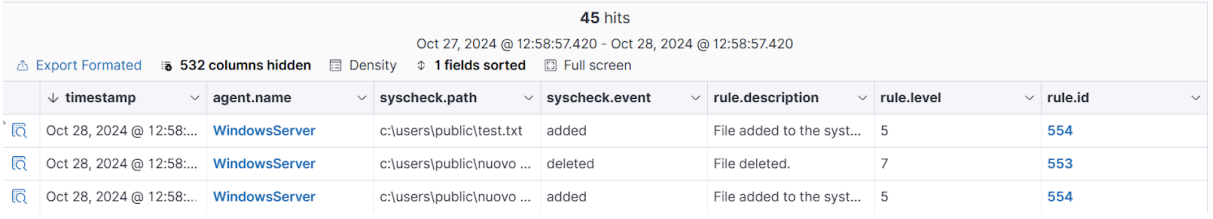
Ora vediamo il monitoraggio in real time di una directory, riporto la frequenza allo stato originario monitorando solo una directory:

```
<!-- Frequency that syscheck is executed default every 12 hours -->
<frequency>43200</frequency>

<!-- Default files to be monitored. -->
<directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

<directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.ex
<directories realtime="">C:\Users\Public</directories>
<directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
```

```
<directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|net.exe$|
<directories whodata="yes">C:\Users\Public</directories>
<directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
<directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
<directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
<directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
```

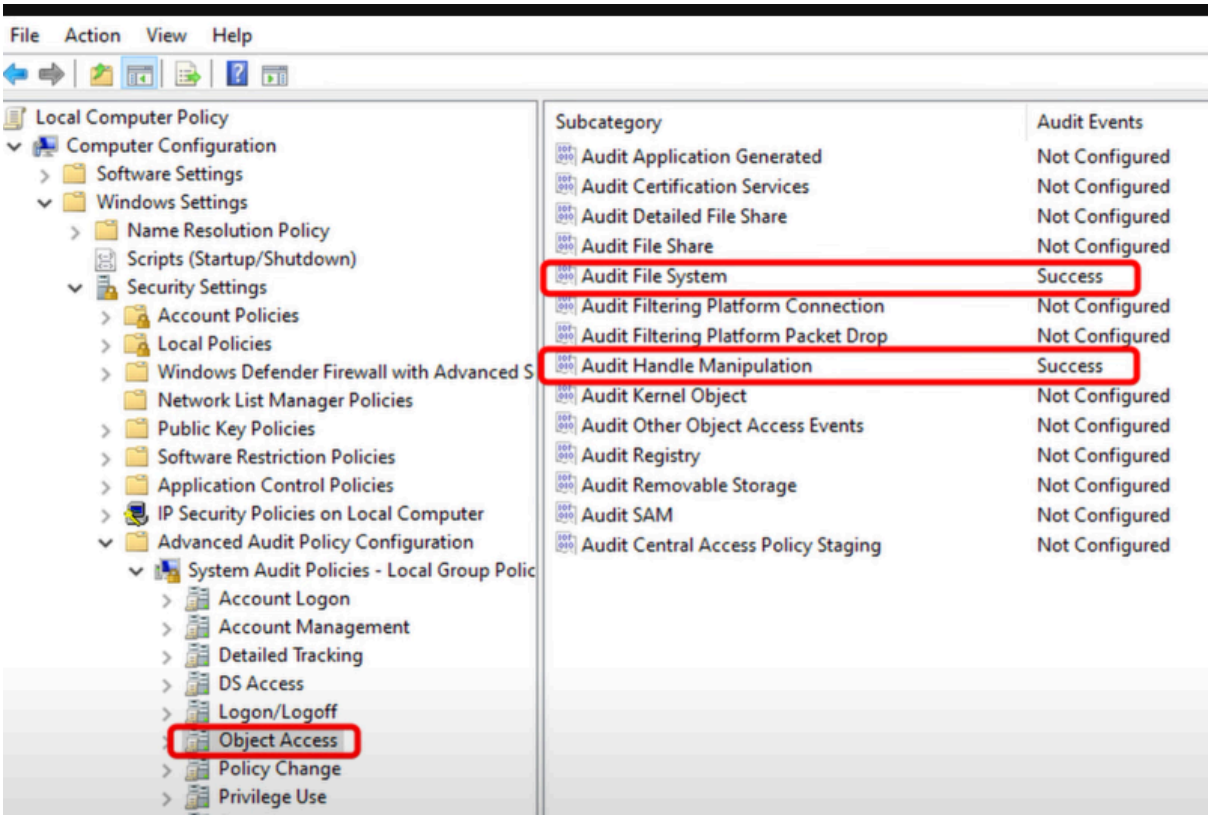
Non appena creo il file lo visualizzo immediatamente sulla dashboard di Wazuh:



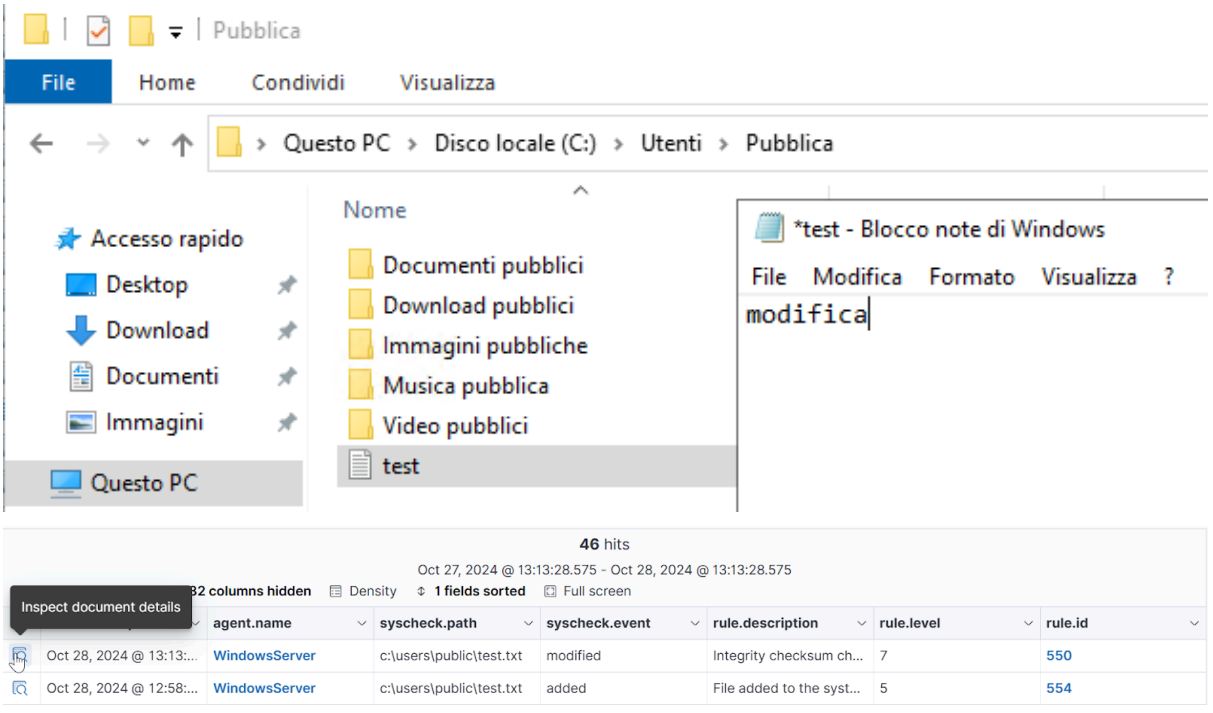


timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Oct 28, 2024 @ 12:58:...	WindowsServer	c:\users\public\test.txt	added	File added to the syst...	5	554
Oct 28, 2024 @ 12:58:...	WindowsServer	c:\users\public\nuovo ...	deleted	File deleted.	7	553
Oct 28, 2024 @ 12:58:...	WindowsServer	c:\users\public\nuovo ...	added	File added to the syst...	5	554

Per configurare la funzione "who data", è necessario modificare la sezione del sottosistema di auditing di Windows e la lista di controllo degli accessi (ACL) delle directory da monitorare.



Facciamo una prova modificando un file:



Dai log ho la possibilità di vedere cosa è stato modificato , il prima e il dopo: