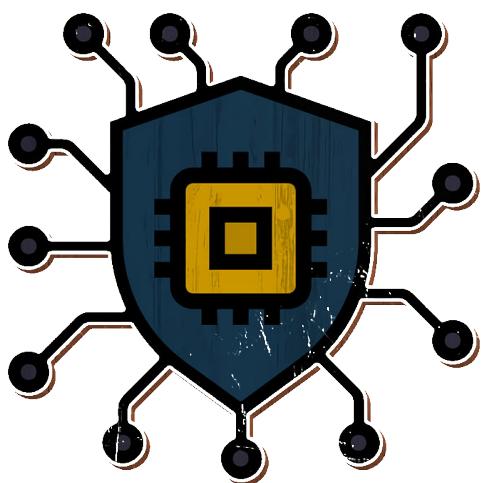


Incident Response Plan



★ INDICE

- 1 **Introduzione a Wazuh**
- 2 **[Official] Incident Response Plan**
- 3 **[Facoltativo] Analisi URLs Sospetti**
- 4 **[Extra] Installazione e Configurazione Wazuh**
- 5 **Conclusione**

1 Introduzione a Wazuh

Cos'è Wazuh?

Wazuh è una piattaforma di sicurezza open-source enterprise che combina funzionalità avanzate di:

- **SIEM (Security Information and Event Management)**: Raccolta centralizzata e analisi di log di sicurezza da fonti multiple
- **XDR (Extended Detection and Response)**: Correlazione avanzata di eventi per identificare minacce complesse
- **Vulnerability Assessment**: Scansione automatizzata di vulnerabilità sui sistemi monitorati
- **Configuration Assessment (SCA)**: Valutazione conformità delle configurazioni rispetto a standard di sicurezza (CIS Benchmarks)
- **Incident Response**: Strumenti e automazioni per risposta rapida agli incidenti di sicurezza

A Cosa Serve Wazuh?

Wazuh serve a proteggere le infrastrutture IT attraverso:

1. **Threat Detection**: Rilevamento in tempo reale di minacce tramite analisi comportamentale e firma-based
2. **Log Analysis**: Analisi centralizzata di log da sistemi operativi, applicazioni, dispositivi di rete e cloud
3. **Compliance Monitoring**: Monitoraggio automatico della conformità a standard regolatori (PCI DSS, GDPR, HIPAA, NIST 800-53)
4. **Forensic Investigation**: Raccolta e preservazione di evidenze digitali per indagini forensi
5. **Security Visualization**: Dashboard interattive e report personalizzabili per l'analisi di sicurezza
6. **Automated Response**: Correzione automatica di configurazioni non conformi e reazione a minacce

Come Funziona Wazuh?

Wazuh opera con un'architettura distribuita basata su tre componenti principali:

Wazuh Manager (Server):

- **Engine di Analisi:** Applica regole di detection e correlazione agli eventi ricevuti
- **Centralizzazione Dati:** Aggrega log e eventi da tutti gli agenti connessi
- **Alert Generation:** Genera alert basati su comportamenti sospetti o configurazioni non conformi
- **Compliance Framework:** Mappa eventi a framework di compliance predefiniti
- **Dashboard Web:** Fornisce interfaccia user-friendly per monitoraggio e analisi

Wazuh Agents (Client):

- **Log Collection:** Raccoglie log locali e eventi di sistema in tempo reale
- **File Integrity Monitoring (FIM):** Monitora modifiche a file e directory critiche
- **System Monitoring:** Raccolta informazioni su processi, porte aperte, interfacce di rete
- **Malware Detection:** Utilizza rootcheck, YARA e integrazioni virus scanning
- **Configuration Assessment:** Esegue scansioni di conformità rispetto a benchmark CIS
- **Communication:** Trasmissione sicura di dati al manager su porta 1514 TCP

Moduli Operativi:

- **Logcollector:** Raccoglie log da file di sistema e applicazioni
- **Syscollector:** Inventario hardware/software dei sistemi monitorati
- **Wodles:** Moduli specializzati (YARA, VirusTotal, Active Directory, AWS, Azure)
- **FIM:** File Integrity Monitoring con supporto per hashing e controlli attributi
- **Rootcheck:** Rilevamento rootkit, trojan e anomalie di sistema
- **SCA:** Security Configuration Assessment contro benchmark CIS
- **Active Response:** Reazioni automatiche a minacce rilevate

Dashboard Capabilities:

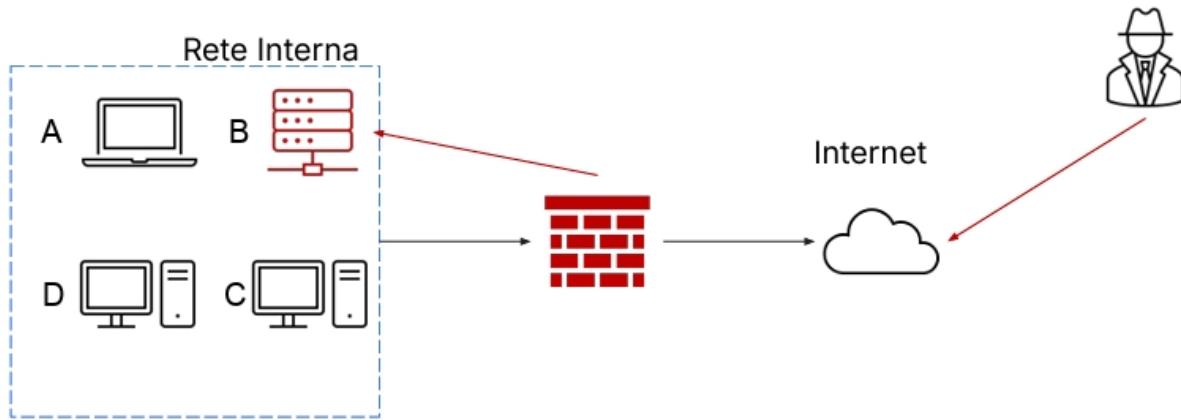
- **Overview:** Vista sintetica con metriche di sicurezza e stato agent
- **Security Events:** Analisi dettagliata di eventi di sicurezza con filtri avanzati
- **Compliance:** Monitoring conformità a standard regolatori multipli
- **Threat Hunting:** Ricerca proattiva di minacce con query flessibili
- **MITRE ATT&CK:** Mappatura eventi a tattiche e tecniche di attacco
- **Vulnerabilities:** Gestione vulnerabilità con scoring CVSS

Wazuh rappresenta una soluzione completa di cybersecurity che automatizza il monitoraggio, la detection e la risposta agli incidenti, permettendo alle organizzazioni di mantenere una postura di sicurezza proattiva e conforme ai requisiti regolatori.

2 [Official] Incident Response Plan

Fase 1: IDENTIFICAZIONE

Rilevamento e Analisi dell'Incidente



Scenario di Identificazione:

- **Vettore di Attacco:** L'attaccante esterno (hacker) sfrutta vulnerabilità del firewall
- **Obiettivo Compromesso:** Server B nella rete interna evidenziato in rosso
- **Pattern Malevoli:** Traffico bidirezionale rosso evidenzia:
 - Compromissione iniziale dal Server B
 - Esfiltrazione dati verso l'esterno
 - Comunicazioni C2 (Command and Control)
- **Indicatori Critici:** Evidenti segnali di accesso non autorizzato e compromissione attiva

Scenario: Sistema B Compromesso

Fase 1: Preparazione

Ho sviluppato un piano di risposta agli incidenti che prevede procedure strutturate per identificare, contenere, eliminare e recuperare da compromissioni del sistema.

Fase 2: Rilevamento e Analisi

Indicatori di Compromissione identificati:

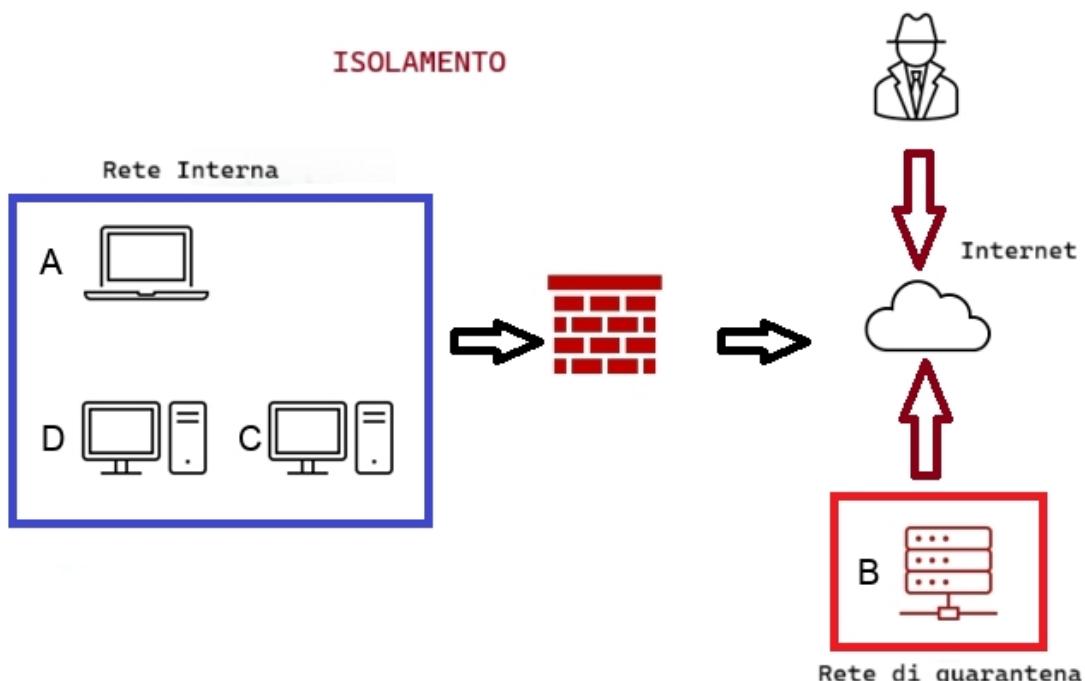
- Modifiche non autorizzate ai file di sistema
- Tentativi di autenticazione falliti
- Attività di privilege escalation
- Pattern di movimento laterale nella rete

Priorità di Analisi:

1. Collezione di evidenze forensi
2. Identificazione del vettore di attacco
3. Determinazione dell'estensione della compromissione
4. Timeline dell'incidente

Fase 2: CONTENIMENTO E ISOLAMENTO

Tecniche di Isolamento Rete



Tecniche di Isolamento Attivate:

- **Rete di Quarantena:** Sistema B compromesso spostato logicamente in ambiente isolato
- **Firewall Dinamico:** Configurazione immediata per bloccare traffico malevolo in entrata/ uscita
- **Separazione Reti:** Interruzione comunicazione tra rete interna (A,C,D) e sistema infetto
- **Controllo Traffico:** Monitoraggio e limitazione accesso dispositivo in quarantena
- **Isolamento Preventivo:** Prevenzione diffusione laterale malware nella rete principale

Tecniche di Isolamento:

- **Isolamento di rete:** Configurazione VLAN quarantine per sistema B

Firewall rules: Blocco traffico in uscita da sistema B

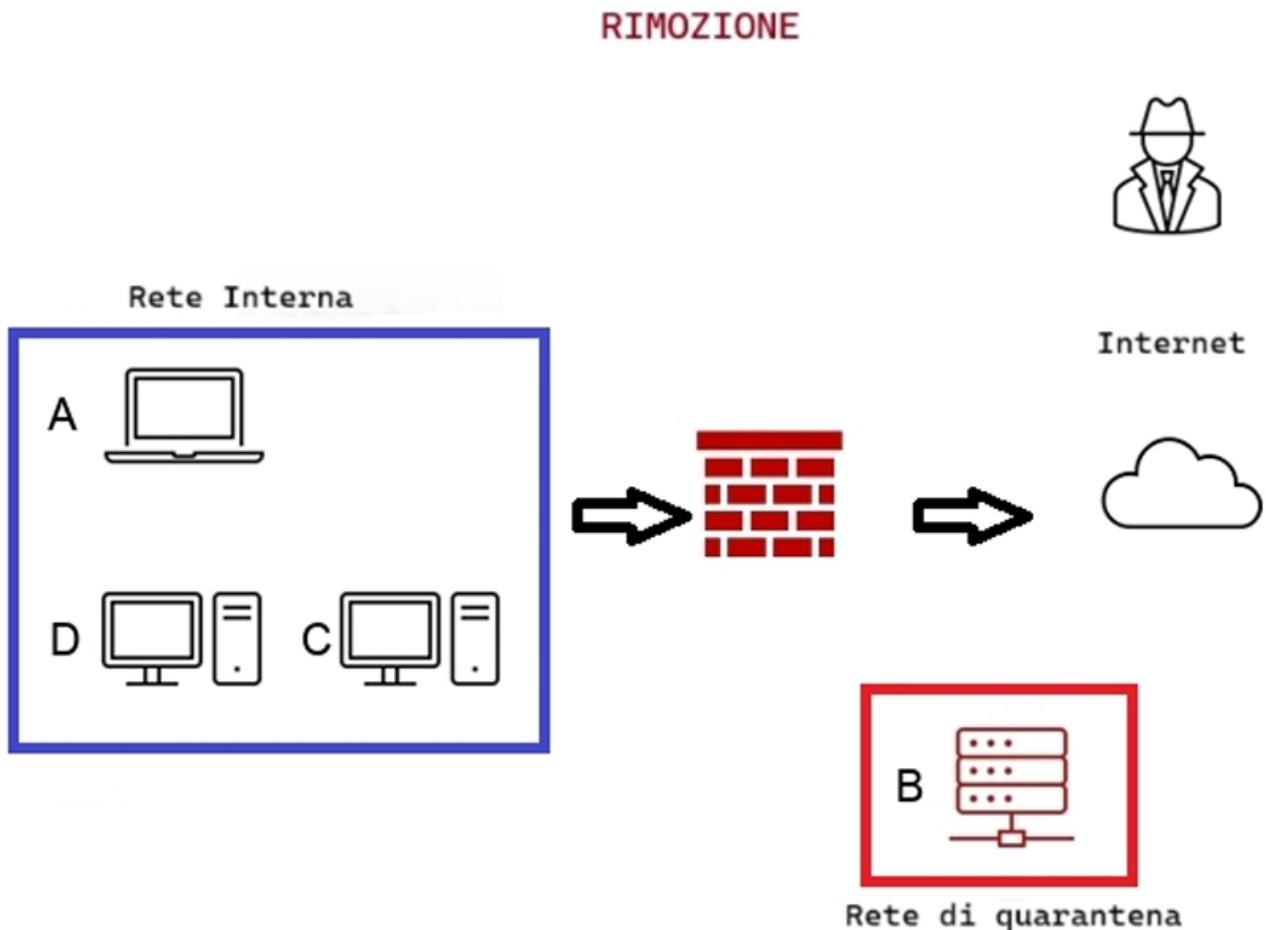
Isolamento fisico: Se necessario, disconnectione cavo di rete

Tecniche di Rimozione:

- **Malware removal:** Utilizzo di strumenti specializzati per eliminazione malware
- **System cleanup:** Rimozione file temporanei, processi sospetti, scheduled tasks
- **Credential reset:** Reset di tutte le password e token di autenticazione

Fase 3: ERADICAZIONE E RIMOZIONE

Processo di Pulizia e Sanitizzazione



Processi di Rimozione Attivati:

- **Ambienti Controllati:** Elaborazione pulizia sistemi in rete di quarantena
- **Rimozione Malware:** Scansioni approfondite e eliminazione codice malevolo
- **Eliminazione Backdoor:** Rimozione accessi persistenti e backdoor di sistema
- **Patching Vulnerabilità:** Applicazione aggiornamenti sicurezza post-attacco
- **Pulitura Completa:** Sanitizzazione completa disco e re-imaging se necessario
- **Firewall Riconfigurazione:** Blocco definitivo comunicazioni C2 e traffico malevolo
- **Account Cleanup:** Eliminazione account non autorizzati e privilegi elevati

Metodi di Sanitizzazione Post-Incidente:

Metodi NIST 800-88 per Sanitizzazione

1. CLEAR (Cancellazione Logica)

- **Descrizione:** Sovrascrizione logica dei dati con pattern casuali
- **Metodo:** Utilizzo di tool come shred , wipe , o bcwipe
- **Standard:** NIST 800-88 Clear Level- Utilizzo: Per dati sensibili non classificati, preparazione al riciclo

2. PURGE (Cancellazione Crittografica)

- **Descrizione:** Distruzione delle chiavi di cifratura, rendendo i dati irrecuperabili
- **Metodo:** Utilizzo di tecniche di cryptographic erasure o degaussing magnetico
- **Standard:** NIST 800-88 Purge Level
- **Utilizzo:** Per dati confidenziali, ambiente cloud, storage condiviso

3. DESTROY (Distruzione Fisica)

- **Descrizione:** Distruzione fisica dei supporti di memorizzazione
- **Metodo:** Smagnetizzazione, frantumazione, incenerimento, dissoluzione chimica
- **Standard:** NIST 800-88 Destroy Level
- **Utilizzo:** Per dati top secret, supporti danneggiati, fine ciclo vita

3 [Facoltativo] Analisi URLs Sospetti

URL Analizzati

URL 1: tinyurl.com/linklosco1

Risultato Analisi ANY.RUN:

- **Tipo:** Script PowerShell malevolo
- **Nome File:** DNS_Changer.ps1
- **Comportamento:** Modifica impostazioni DNS del sistema
- **Classificazione:** Suspicious Activity
- **IOC (Indicators of Compromise):**
 - Hash: Specifici pattern di Powershell script
 - Network: Modifiche DNS verso server malevoli
 - File: Creazione/modifica file di configurazione DNS

URL 2: linklosco2

Risultato Analisi ANY.RUN:

- **Tipo:** Google Docs malware distribution
- **Comportamento:** Utilizzo di Google Docs come vettore per distribuzione malware
- **Classificazione:** Malicious Activity
- **IOC (Indicators of Compromise):**
 - URL: Link di Google Docs pericolosi
 - Download: File eseguibili da Google Drive
 - Payload: Specifici pattern di download di malware

4 [Extra] Installazione e Configurazione Wazuh

Topologia di Rete Implementata

Ambiente di Laboratorio:

- pfSense Firewall: Gestione rete e routing
- LAN 1 (192.168.50.x):
 - Kali Linux (192.168.50.1)
 - Wazuh Server (192.168.50.151)
- LAN 2 (192.168.51.x): Metasploitable2 (192.168.51.1)
- LAN 3 (192.168.52.x): Windows 10 Pro (192.168.52.1)

Installazione Wazuh Server (OVA)

Ho installato Wazuh utilizzando l'appliance OVA pre-configurata:

Comandi di Installazione Server:

```
# Download Wazuh OVA
wget https://packages.wazuh.com/4.x/vm/wazuh-4.14.1-1.ova

# Importazione in VirtualBox
VBoxManage import wazuh-4.14.1-1.ova

# Configurazione rete VM
VBoxManage modifyvm "wazuh" --nic1 intnet --networkname intnet_lan1
```

Configurazione Rete Wazuh Server:

```
[wazuh-user@wazuh-server ~]$
[wazuh-user@wazuh-server ~]$ ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=2.77 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=1.47 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=64 time=1.16 ms
64 bytes from 192.168.50.1: icmp_seq=4 ttl=64 time=1.22 ms
^C
--- 192.168.50.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.158/1.655/2.773/0.655 ms
[wazuh-user@wazuh-server ~]$
```

Configurazione Firewall pfSense

Ho configurato regole firewall per permettere la comunicazione Wazuh:

Regole Firewall:

- Porta 1514**: Comunicazione agent-manager
- Porta 1515**: Enrollment agent
- Porta 443**: Dashboard web

Test di Connessione

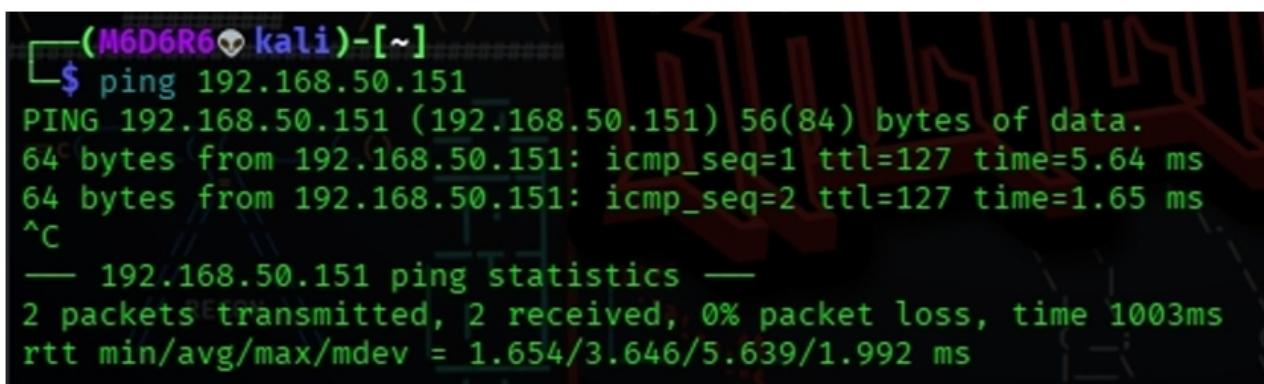
Ho verificato la connettività tra Kali e Wazuh Server:

Comandi Test Connessione:

```
# Test ping
ping 192.168.50.151

# Test porta TCP
nc -zv 192.168.50.151 1514
telnet 192.168.50.151 1514
```

Test di Connessione:



```
(M6D6R6㉿kali)-[~]
$ ping 192.168.50.151
PING 192.168.50.151 (192.168.50.151) 56(84) bytes of data.
64 bytes from 192.168.50.151: icmp_seq=1 ttl=127 time=5.64 ms
64 bytes from 192.168.50.151: icmp_seq=2 ttl=127 time=1.65 ms
^C
--- 192.168.50.151 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 1.654/3.646/5.639/1.992 ms
```

Risultato: Connessione perfetta - Porta 1514 raggiungibile

Installazione Wazuh Agent su Kali

Ho installato e configurato l'agent Wazuh sul sistema Kali Linux:

Comandi Installazione Agent:

```
# Aggiunta chiave GPG Wazuh
wget -qO - https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor | sudo tee /usr/share/keyrings/wazuh-archive-keyring.gpg

# Configurazione repository
echo "deb [signed-by=/usr/share/keyrings/wazuh-archive-keyring.gpg]
https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list

# Installazione agent
sudo apt-get update
sudo WAZUH_MANAGER='192.168.50.151' apt-get install wazuh-agent

# Configurazione agent
sudo nano /var/ossec/etc/ossec.conf

# Avvio servizio
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Installazione Agent (Errori e Risultati):

```
(M6D6R6㉿kali)-[~]
$ wget -qO - https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -
sudo echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
sudo apt-get update
sudo WAZUH_MANAGER=192.168.50.151 apt-get install wazuh-agent
[sudo] password for kali:
To boldly go where no
shell has gone before
sudo: apt-key: command not found
deb https://packages.wazuh.com/4.x/apt/ stable main
Hit:1 https://packages.wazuh.com/4.x/apt stable InRelease
Err:1 https://packages.wazuh.com/4.x/apt stable InRelease
  Sub-process /usr/bin/sqv returned an error code (1), error message is: Missing key 0DCFCA5547B19D2A609950609
6B3EE5F29111145, which is needed to verify signature.
Hit:2 http://http.kali.org/kali kali-rolling InRelease
Hit:3 https://packages.microsoft.com/repos/code stable InRelease
Reading package lists... Done
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. OpenPGP signature verification failed: https://packages.wazuh.com/4.x/apt stable InRelease:
Sub-process /usr/bin/sqv returned an error code (1), error message is: Missing key 0DCFCA5547B19D2A6099506096
B3EE5F29111145, which is needed to verify signature.
W: Failed to fetch https://packages.wazuh.com/4.x/apt/dists/stable/InRelease Sub-process /usr/bin/sqv returned an error code (1), error message is: Missing key 0DCFCA5547B19D2A6099506096B3EE5F29111145, which is needed to verify signature.
W: Some index files failed to download. They have been ignored, or old ones used instead.
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 required:
  amass-common firmware-ti-connectivity libbluray2 libbsson-1.0-0t64 libgdal36 libgdata-common libgdata22
  libgeos3.13.1 libhdf4-0-alt libjs-jquery-ui libjs-underscore libmongoc-1.0-0t64 libmongocrypt0 libogdi4.1
  libplacebo349 libportmidi0 libqt5ct-common1.8 libravie0.7 libsfstrm1 libsoup-2.4-1 libsoup2.4-common
  libtheora0 libtheoradec1 libthdraenac1 libufread0 libvpx9 libxml2 libxml2 libyelp0 python3-bluepy
  python3-click-plugins python3-gpg python3-kismetcapturebtgeiger python3-kismetcapturefreaklabszigbee
  python3-kismetcapturertl433 python3-kismetcapturertladsb python3-kismetcapturertlamlr python3-protobuf
  python3-zombie-imp samba-ad-dc samba-ad-provision samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 713 not upgraded.
```

Dettagli Installazione:

- **Repository Wazuh:** Configurato correttamente su <https://packages.wazuh.com/4.xapt/>
- **Problema GPG:** Errore `apt-key: command not found` - chiave GPG non trovata
- **Stato Agent:** `wazuh-agent is already the newest version (4.14.1-1)`
- **Configurazione:** Gestita tramite variabile ambiente `WAZUH_MANAGER='192.168.50.151'`

Configurazione Agent

Il file di configurazione dell'agent (`/var/ossec/etc/ossec.conf`) contiene:

```
<ossec_config>
  <client>
    <server>
      <address>192.168.50.151</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>debian,debian10,debian11</config-profile>
  </client>

  <logging>
    <level>info</level>
    <format>text</format>
  </logging>

  <active-response>
    <active_disabled>yes</active_disabled>
  </active-response>
</ossec_config>
```

Configurazione Agent Completa:

The screenshot shows the Wazuh web interface with the following sections:

- Endpoints** tab selected.
- AGENTS BY STATUS**: A donut chart showing 1 Active agent, 0 Disconnected, 0 Pending, and 0 Never connected.
- TOP 5 OS**: A donut chart showing 1 Kali Linux agent.
- TOP 5 GROUPS**: A donut chart showing 1 default group.
- Agents (1)**: A table listing the active agent details:

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	kali	192.168.50.100	default	Kali GNU/Linux 2025.3	node01	v4.14.1	active	...

Configurazione ossec.conf Dettagliata:

```

GNU nano 8.6                               /var/ossec/etc/ossec.conf
<!-- Wazuh Agent - Default configuration for kali 2025.3
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <client>
    <server>
      <address>192.168.50.151</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>kali, kali2025, kali2025.3</config-profile>
    <notify_time>20</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    <!-- Agent buffer options -->
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

  <!-- Policy monitoring -->
  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_dev>yes</check_dev>
    <check_sys>yes</check_sys>
    <check_pids>yes</check_pids>
    <check_ports>yes</check_ports>
    <check_if>yes</check_if>
    <!-- Frequency that rootcheck is executed - every 12 hours -->
    <frequency>43200</frequency>
    <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>
    <skip_nfs>yes</skip_nfs>
    <ignore>/var/lib/containerd</ignore>
    <ignore>/var/lib/docker/overlay2</ignore>
  </rootcheck>
</ossec_config>

```

Configurazione Dettagliata ossec.conf:

```

<ossec_config>
  <client>
    <server>
      <address>192.168.50.151</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>kali, kali2025, kali2025.3</config-profile>
    <notify_time>20</notify_time>
    <time-reconnect>60</time-reconnect>
    <auto_restart>yes</auto_restart>
    <crypto_method>aes</crypto_method>
  </client>

  <client_buffer>
    <disabled>no</disabled>
    <queue_size>5000</queue_size>
    <events_per_second>500</events_per_second>
  </client_buffer>

  <rootcheck>
    <disabled>no</disabled>
    <check_files>yes</check_files>
    <check_trojans>yes</check_trojans>
    <check_dev>yes</check_dev>
    <check_sys>yes</check_sys>
    <check_pids>yes</check_pids>
    <check_ports>yes</check_ports>
    <check_if>yes</check_if>
    <frequency>43200</frequency>
    <rootkit_files>etc/shared/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>etc/shared/rootkit_trojans.txt</rootkit_trojans>
    <skip_nfs>yes</skip_nfs>
    <ignore>/var/lib/containerd</ignore>
    <ignore>/var/lib/docker/overlay2</ignore>
  </rootcheck>
</ossec_config>

```

Configurazione Rootcheck Abilitata:

- **Controllo File:** Rilevamento file sospetti attivato
- **Controllo Trojan:** Ricerca signature trojan noti attivata
- **Controllo Dispositivi:** Controllo dispositivi di sistema attivato
- **Controllo Sistema:** Controllo librerie/binari di sistema attivato
- **Controllo PID:** Rilevamento processi nascosti attivato
- **Controllo Porte:** Controllo porte aperte sospette attivato
- **Controllo Interfacce:** Controllo interfacce di rete attivato
- **Frequenza:** 43200 secondi (12 ore)

Verifica Connessione Agent

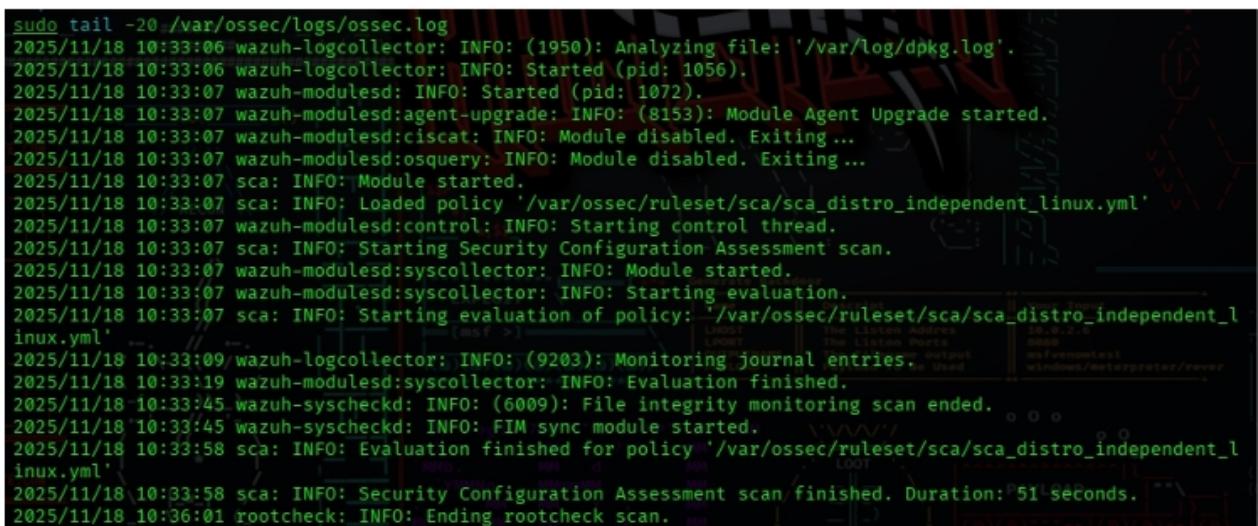
Ho verificato che l'agent si connetta correttamente al server:

Controllo Log:

```
# Controllo log connessione
sudo tail -10 /var/ossec/logs/ossec.log | grep "Connected to the
server"

# Controllo stato servizio
sudo systemctl status wazuh-agent
```

Log Moduli Wazuh Attivi



```
sudo tail -20 /var/ossec/logs/ossec.log
2025/11/18 10:33:06 wazuh-logcollector: INFO: (1950): Analyzing file: '/var/log/dpkg.log'.
2025/11/18 10:33:06 wazuh-logcollector: INFO: Started (pid: 1056).
2025/11/18 10:33:07 wazuh-modulesd: INFO: Started (pid: 1072).
2025/11/18 10:33:07 wazuh-modulesd:agent-upgrade: INFO: (8153): Module Agent Upgrade started.
2025/11/18 10:33:07 wazuh-modulesd:ciscat: INFO: Module disabled. Exiting ...
2025/11/18 10:33:07 wazuh-modulesd:osquery: INFO: Module disabled. Exiting ...
2025/11/18 10:33:07 sca: INFO: Module started.
2025/11/18 10:33:07 sca: INFO: Loaded policy '/var/ossec/ruleset/sca/sca_distro_independent_linux.yml'.
2025/11/18 10:33:07 wazuh-modulesd:control: INFO: Starting control thread.
2025/11/18 10:33:07 sca: INFO: Starting Security Configuration Assessment scan.
2025/11/18 10:33:07 wazuh-modulesd:syscollector: INFO: Module started.
2025/11/18 10:33:07 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2025/11/18 10:33:07 sca: INFO: Starting evaluation of policy: '/var/ossec/ruleset/sca/sca_distro_independent_l
inux.yml'.
2025/11/18 10:33:09 wazuh-logcollector: INFO: (9203): Monitoring journal entries.
2025/11/18 10:33:19 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2025/11/18 10:33:45 wazuh-syscheckd: INFO: (6009): File integrity monitoring scan ended.
2025/11/18 10:33:45 wazuh-syscheckd: INFO: FIM sync module started.
2025/11/18 10:33:58 sca: INFO: Evaluation finished for policy '/var/ossec/ruleset/sca/sca_distro_independent_l
inux.yml'.
2025/11/18 10:33:58 sca: INFO: Security Configuration Assessment scan finished. Duration: 51 seconds.
2025/11/18 10:36:01 rootcheck: INFO: Ending rootcheck scan.
```

Analisi Log Completa:

I log mostrano l'attivazione e il funzionamento di tutti i moduli Wazuh:

Moduli Avviati:

- **wazuh-logcollector:** Attivo su `/var/log/dpkg.log` e journal systemd (PID 1056)
- **wazuh-modulesd:** Demone principale moduli (PID 1072)
- **agent-upgrade:** Modulo aggiornamenti agent attivo
- **sca (Security Configuration Assessment):** Scansione configurazioni Linux
- **wazuh-syscheckd (FIM):** File Integrity Monitoring con sincronizzazione
- **rootcheck:** Modulo rilevamento rootkit/malware completato

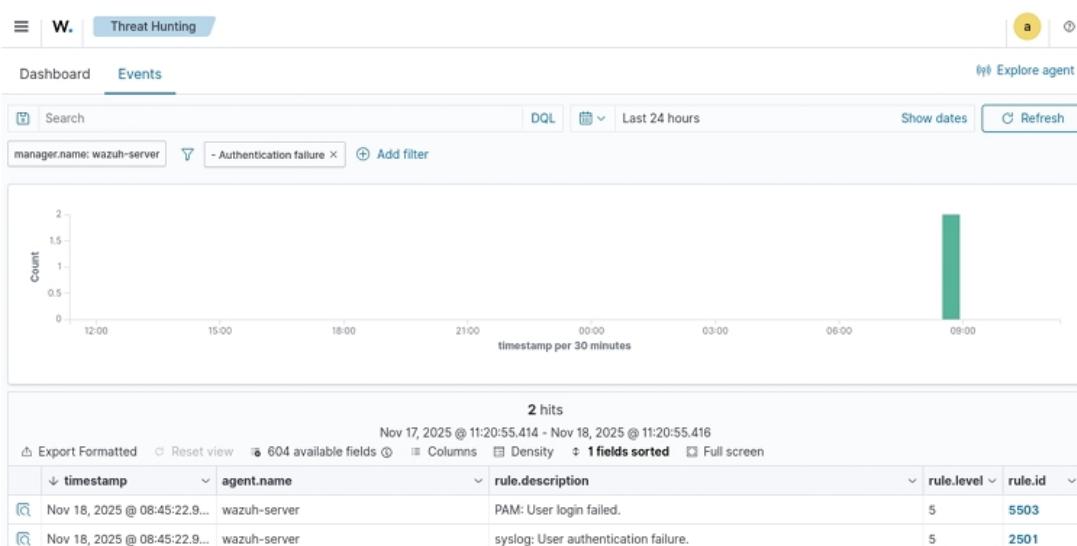
Moduli Disabilitati:

- **ciscat:** CIS benchmark assessment (disabilitato)
- **osquery:** Integrazione osquery (disabilitato)

Sequenza di Completamento:

1. **10:33:19** - Syscollector completato (inventario sistema)
2. **10:33:45** - FIM completato (scan 6009, avvio sincronizzazione)
3. **10:33:58** - SCA completato (51 secondi scansione)
4. **10:36:01** - Rootcheck completato (ultimo modulo)

Log Connessione Agent



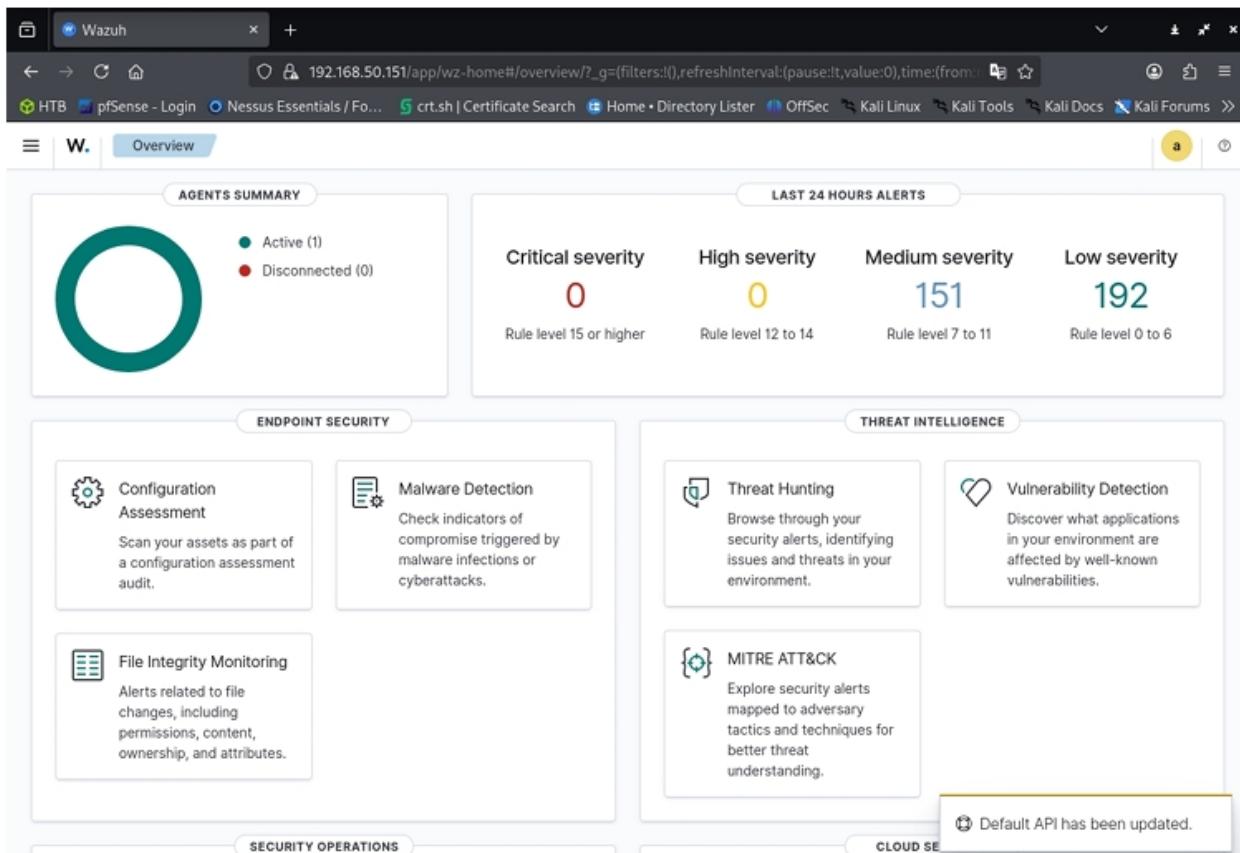
Risultato: Connected to the server ([192.168.50.151]:1514/tcp)

DASHBOARD WAZUH - FUNZIONALITÀ E MONITORING

Dashboard Overview

Ho acceduto alla dashboard Wazuh tramite <https://192.168.50.151> e documentato tutte le funzionalità:

Dashboard Principale:



Risultati Dashboard:

- **Agent Attivo:** kali (001) - Status: active
- **Eventi Totali:** 343 alert nelle ultime 24 ore
- **Livelli Gravità:** Critical (0), High (0), Medium (151), Low (192)
- **MITRE ATT&CK:** Defense Evasion (44), Privilege Escalation (42), Initial Access (23), Persistence (23)

Configurazione Assessment (SCA)

Il modulo di valutazione configurazioni utilizza il benchmark CIS per Linux:

Configuration Assessment:

Classification: CONFIDENTIAL

Pagina 18 di 29

The screenshot shows the Wazuh web interface for a Kali Linux host. The main dashboard displays the CIS Distribution Independent Linux Benchmark v2.0.0 results. A donut chart indicates 83 Passed, 99 Failed, and 8 Not applicable. The overall score is 45%.

ID	Title	Target	Result
36000	Ensure mounting of cramfs file...	Command: modprobe -n -v cramfs,lsmod	Passed
36001	Ensure mounting of freevxfs fil...	Command: modprobe -n -v freevxfs	Failed
36002	Ensure mounting of jffs2 filesy...	Command: modprobe -n -v jffs2	Failed
36003	Ensure mounting of hfs filesys...	Command: modprobe -n -v hfs	Failed
36004	Ensure mounting of hfsplus fil...	Command: modprobe -n -v hfsplus	Failed

Risultati SCA:

- **Score Complessivo:** 45% di conformità
- **Controlli Passati:** 83
- **Controlli Falliti:** 99
- **Controlli Non Applicabili:** 8
- **Ultima Scansione:** 18 Novembre 2025 @ 10:33:55.000

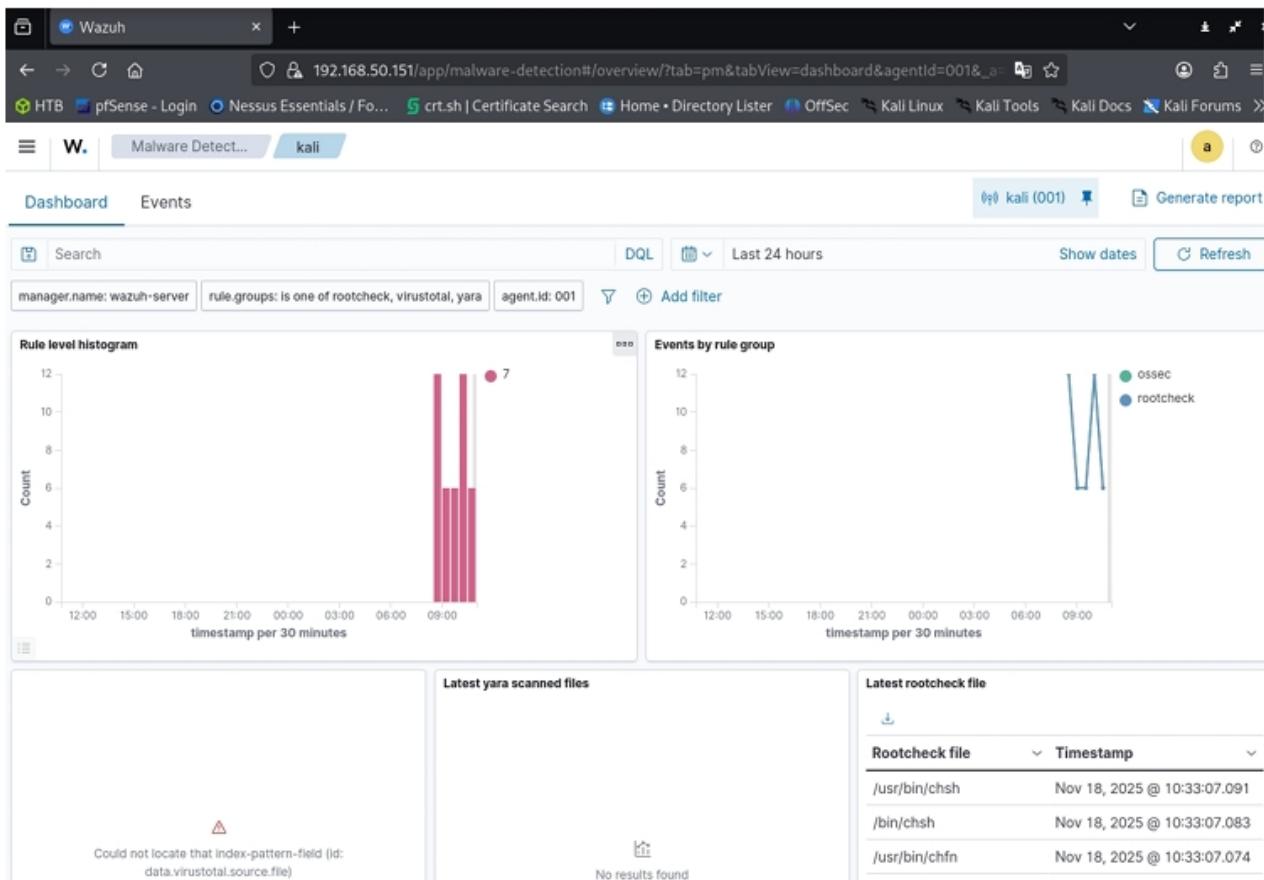
Controlli Falliti Critici:

- ID 36001: "Ensure mounting of freevxfs fil..." - Failed
- ID 36002: "Ensure mounting of jffs2 filesy..." - Failed
- ID 36003: "Ensure mounting of hfs filesys..." - Failed
- ID 36004: "Ensure mounting of hfsplus fil..." - Failed

Rilevamento Malware

Il modulo di rilevamento malware utilizza rootcheck, YARA e integrazione VirusTotal:

Malware Detection:



Rilevamenti Rootcheck:

- File critici modificati: `/usr/bin/chsh`, `/usr/bin/chfn`, `/usr/bin/passwd`
- Timestamp: Nov 18, 2025 @ 10:33:07
- Classificazione: Potenziali indicatori di rootkit o modifiche non autorizzate

Integrazioni Malware Detection Confirmate:

- **Rootcheck:** Attivo con rilevamenti sui file di sistema critici (`/usr/bin/chsh`, `/usr/bin/chfn`, `/usr/bin/passwd`)
- **YARA:** Nessun malware rilevato dalle scansioni (modulo configurato ma senza rilevamenti)
- **VirusTotal:** Problema di configurazione identificato - errore "XX" nella dashboard

Soluzione Problema VirusTotal: L'errore "XX" nel modulo VirusTotal indica una configurazione API Key mancante o non valida. Per risolvere:

1. **Ottenere API Key:** Registrarsi su <https://www.virustotal.com> e ottenere una chiave API gratuita

2. **Configurazione Manager:** Nel Wazuh Manager, modificare il file `/var/ossec/etc/wodles/virustotal.conf`:

```
xml <api_key>YOUR_VIRUSTOTAL_API_KEY_HERE</api_key> <query>
<type>hash</type> <path>/var/ossec/active-response/bin</path>
<response>discard</response> </query>
```

3. **Riavvio Servizi:** Riavviare `wazuh-modulesd` per applicare la configurazione

4. **Verifica:** Controllare i log `/var/ossec/logs/ossec.log` per confermare l'integrazione VirusTotal

File Integrity Monitoring (FIM)

Il modulo FIM monitora modifiche a file e directory sensibili:

File Integrity Monitoring:

The screenshot shows the Wazuh web interface with the URL `192.168.50.151/app/file-integrity-monitoring#/overview/?tab=fim&tabView=dashboard&agentId=001`. The main title bar says "Wazuh". The dashboard header includes links for HTB, pfSense - Login, Nessus Essentials / Fo..., crt.sh | Certificate Search, Home • Directory Lister, OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, and a search bar. Below the header, there are tabs for "Dashboard" (which is selected), "Inventory", and "Events". A search bar contains the query "kali". The main content area displays a search result table with one row, which is highlighted in yellow. The row contains the message "No results match your search criteria".

Configurazione FIM:

-**Percorsi Monitorati:** `/bin`, `/boot`, `/etc`, `/sbin`, `/usr/bin`, `/usr/sbin`

-**Opzioni Monitoraggio:** size | permissions | owner | group | mtime | inode | hash

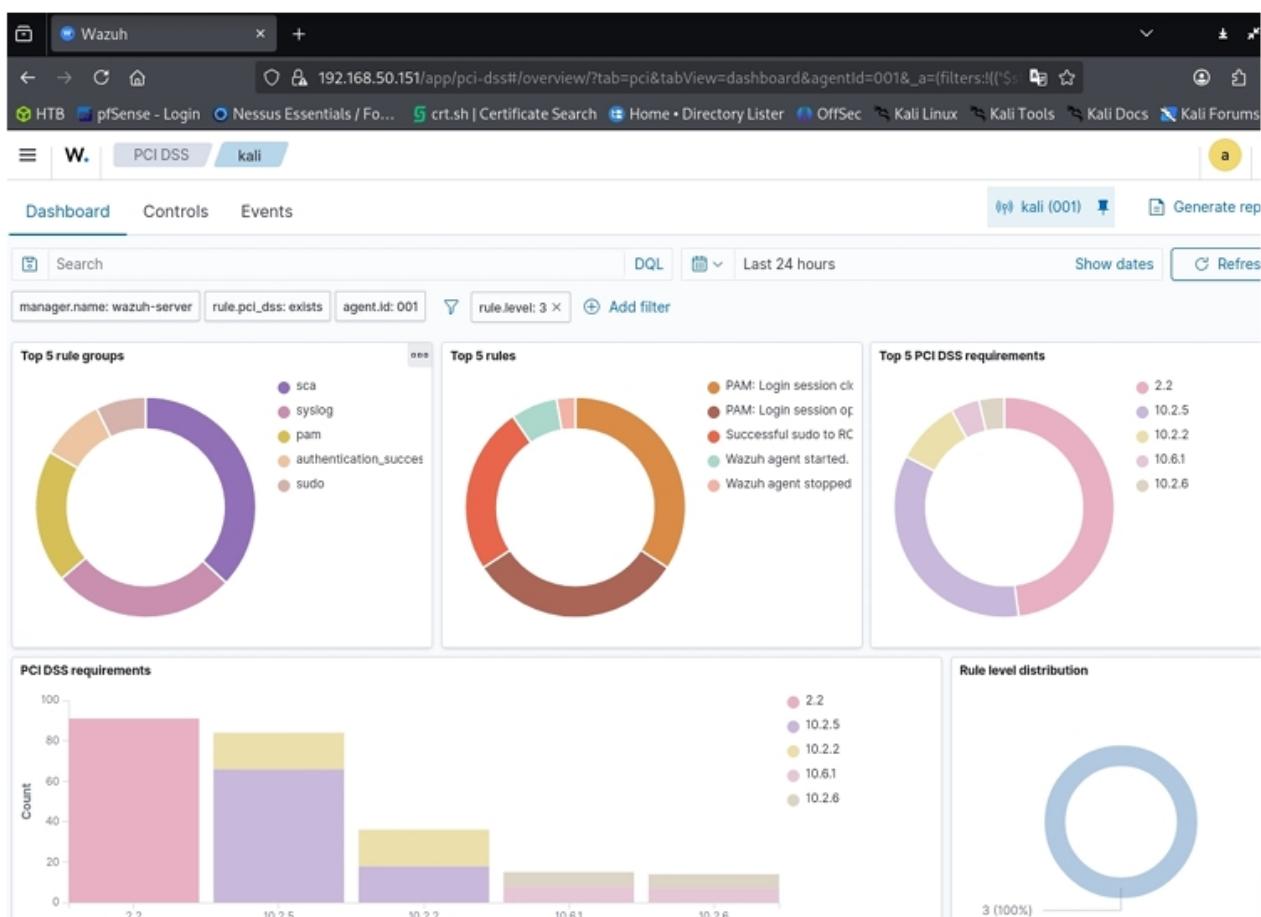
-**Frequenza Scansione:** 43200 secondi (12 ore)

COMPLIANCE MONITORING

PCI DSS Compliance

Ho configurato il monitoring per la conformità

PCI DSS: PCI DSS Dashboard:



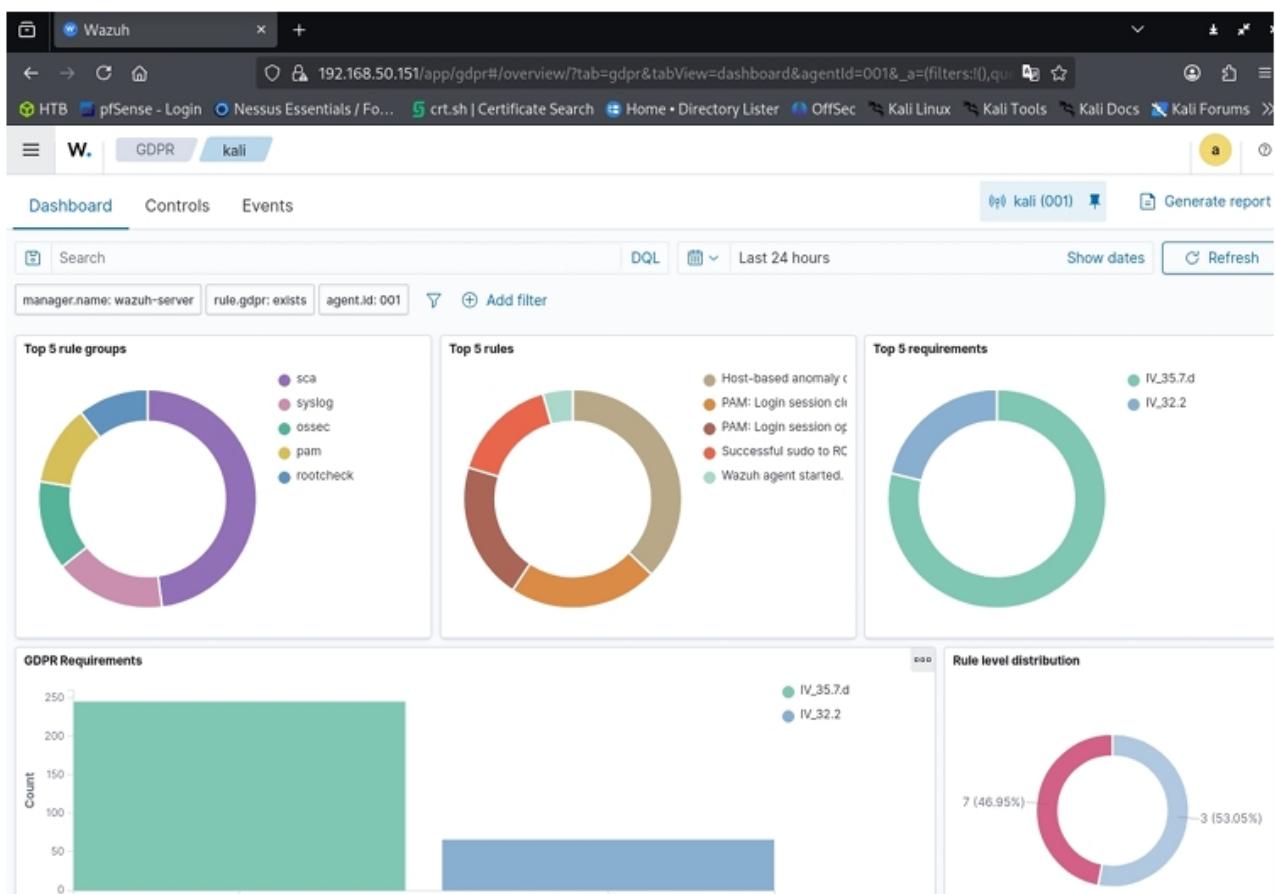
Eventi PCI DSS (Ultimi 24h):

- **Regole Principali:** sca, syslog, pam, authentication_success, sudo
- **Requisiti Top:** 2.2 (configurazione sicurezza), 10.2.5 (audit accessi), 10.2.2 (audit trail)
- **Livello Gravità:** Principalmente livello 3 (informativo)
- **Totale Eventi:** Filtrati per rule.pci_dss e rule.level:3

GDPR Compliance

Il sistema monitora la conformità

GDPR: GDPR Dashboard:



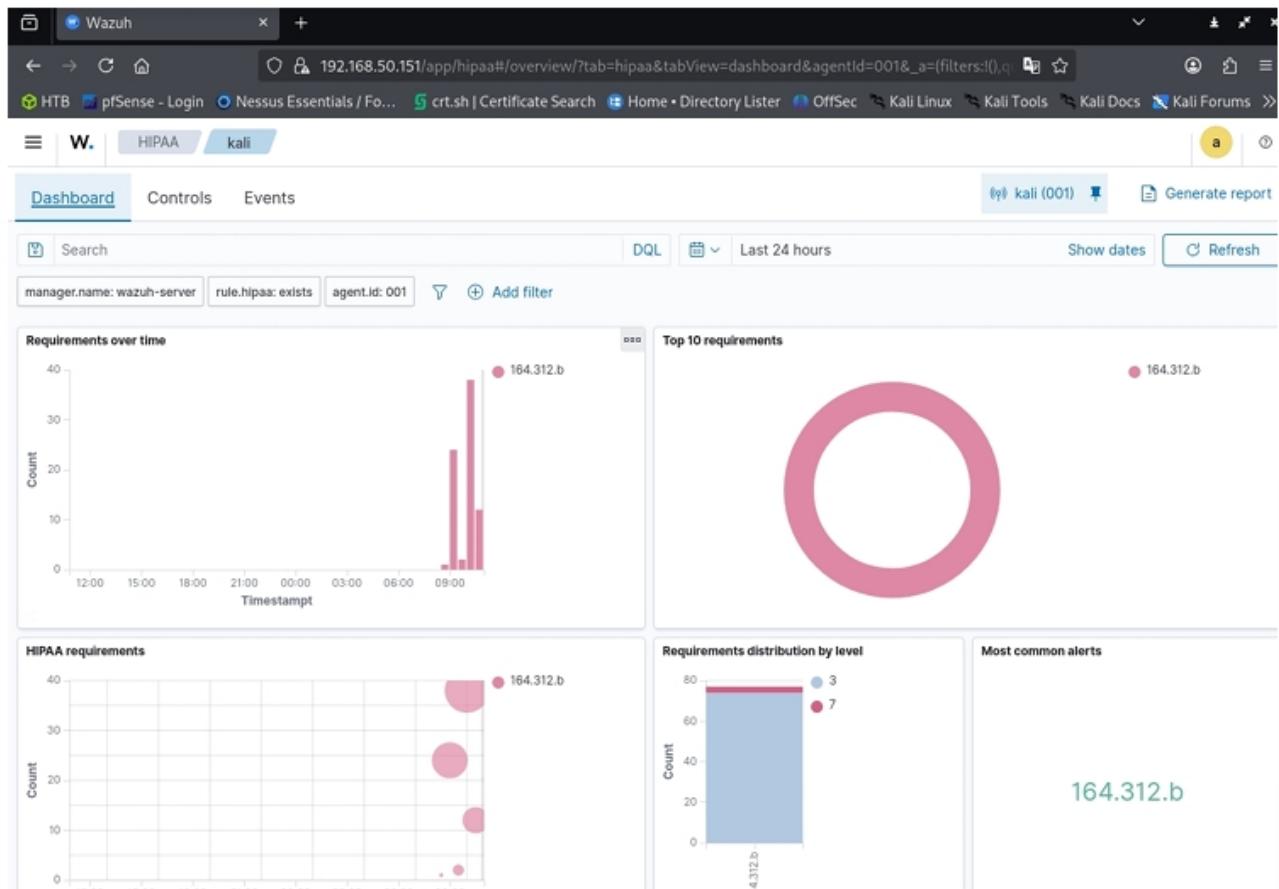
Eventi GDPR:

- **Requisiti Principali:** IV_35.7.d (250 eventi), IV_32.2 (60 eventi)
- **Livelli Gravità:** 7 (46.95%), 3 (53.05%)
- **Top Rule:** "Host-based anomaly c" - Comportamenti anomali host
- **Controlli:** PAM login, sudo commands, agent start/stop

HIPAA Compliance

Monitoraggio della conformità HIPAA per dati sanitari:

HIPAA Dashboard:



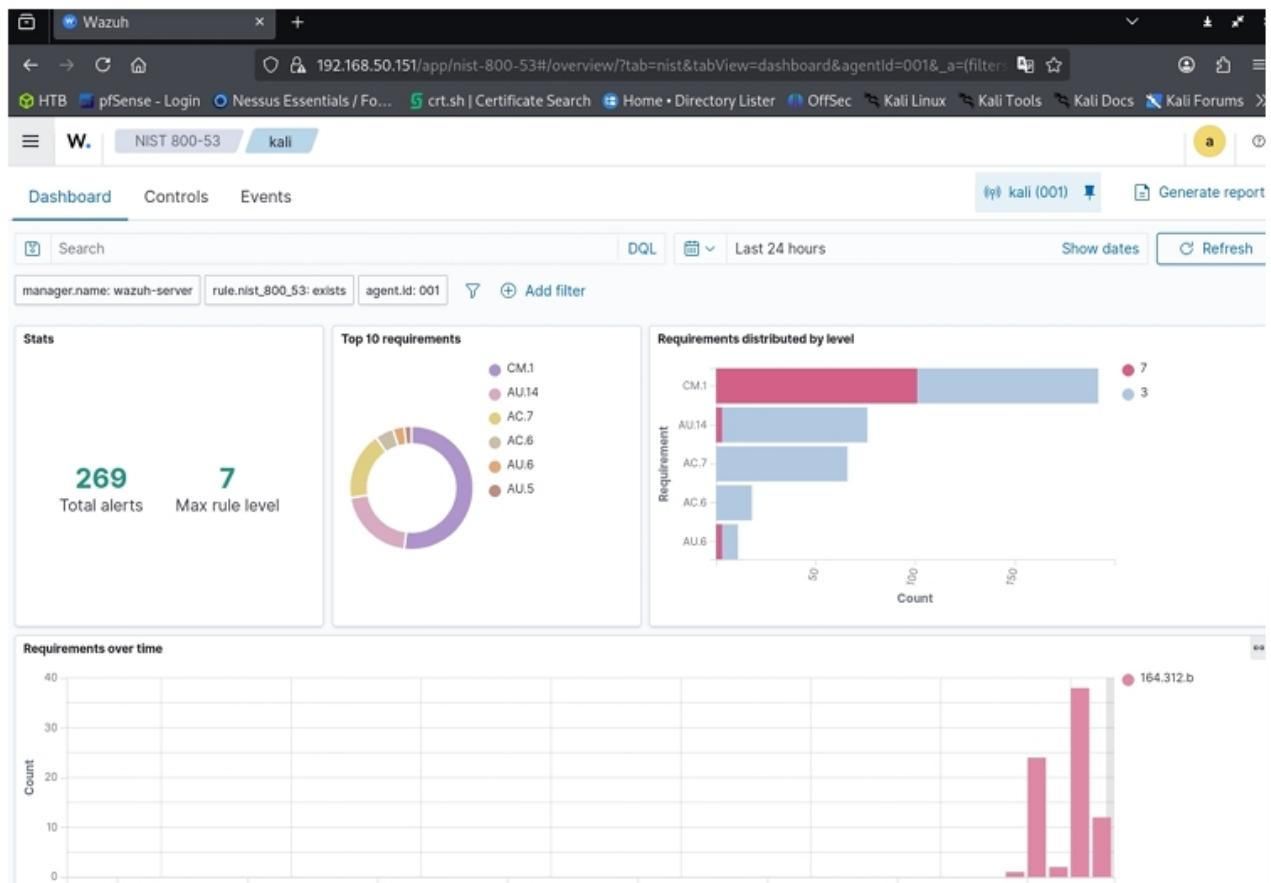
Eventi HIPAA:

- Requisito Principale:** 164.312.b (controlli di accesso)
- Peak Activity:** Circa 40 eventi alle 09:00
- Livelli:** Principalmente livello 3, alcuni livello 7
- Totale:** 70-80 eventi correlati

NIST 800-53 Compliance

Framework di sicurezza federale

NIST: NIST 800-53 Dashboard:



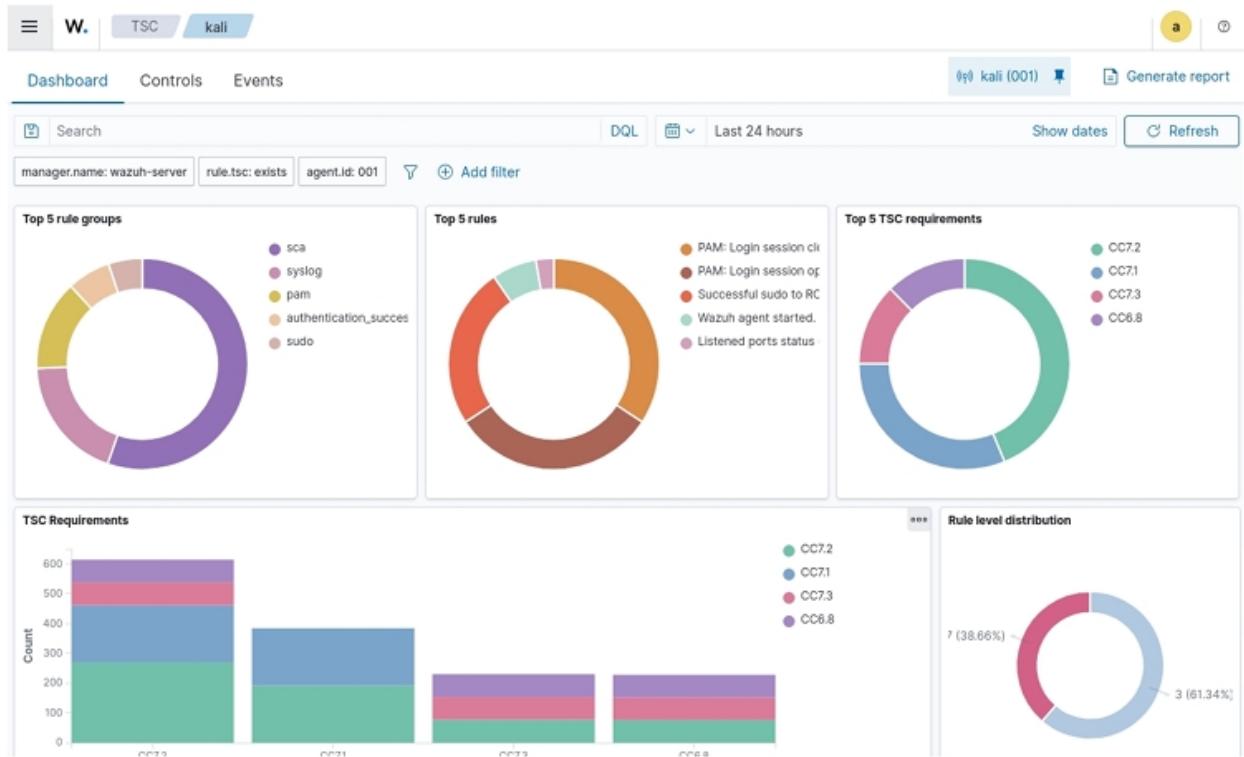
Eventi NIST:

- **Totale Alert:** 269 nelle ultime 24 ore
- **Max Rule Level:** 7 (media-alta gravità)
- **Controlli Principali:** CM.1, AU.14, AC.7, AC.6, AU.6, AU.5
- **Distribuzione:** Molti livello 3, alcuni livello 7

Trust Services Criteria (TSC)

Standard di fiducia per sicurezza e disponibilità:

TSC Dashboard:



Eventi TSC:

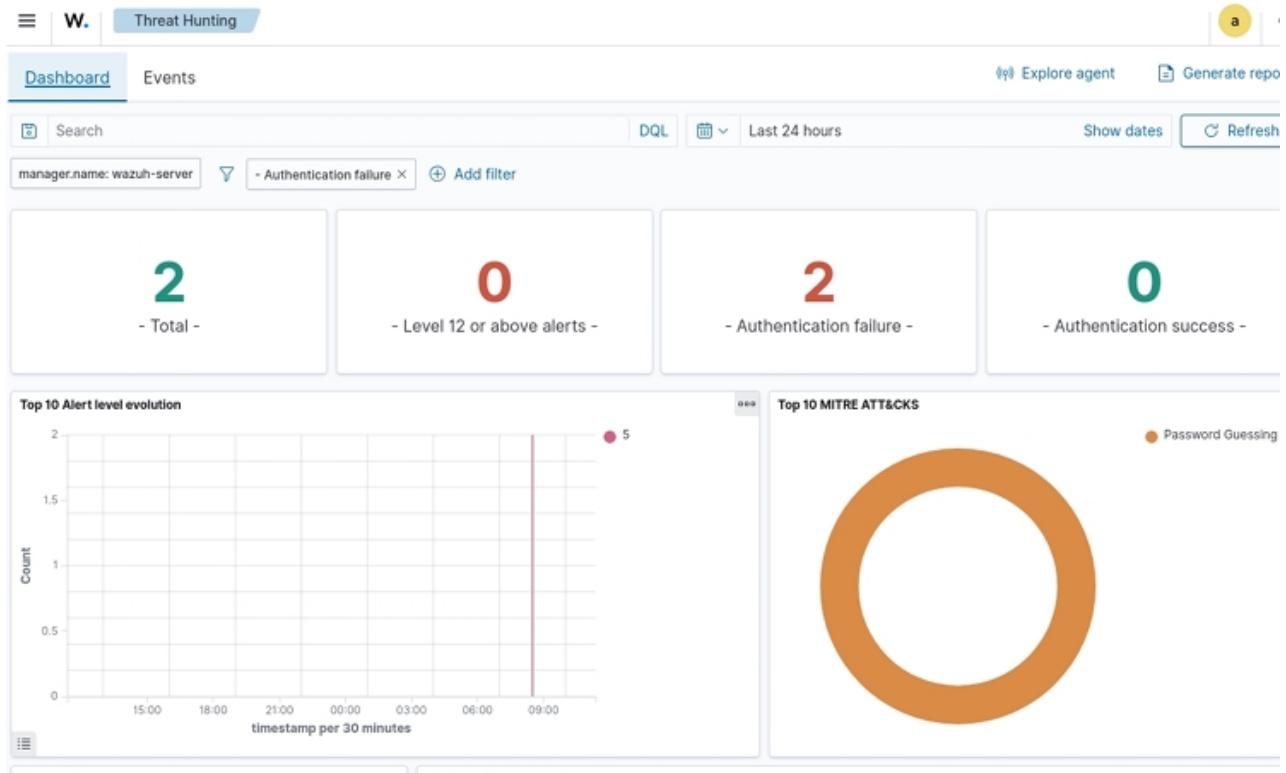
- Requisiti Principali:** CC7.2 (>600 eventi), CC7.1 (~380 eventi)
- Distribuzione Livelli:** 3 (61.34%), 7 (38.66%)
- Attività:** SCA, syslog, pam, authentication_success, sudo

THREAT HUNTING ED EVENTI SPECIFICI

Sezione Threat Hunting

Ho utilizzato il modulo di threat hunting per analizzare eventi specifici:

Threat Hunting Dashboard:



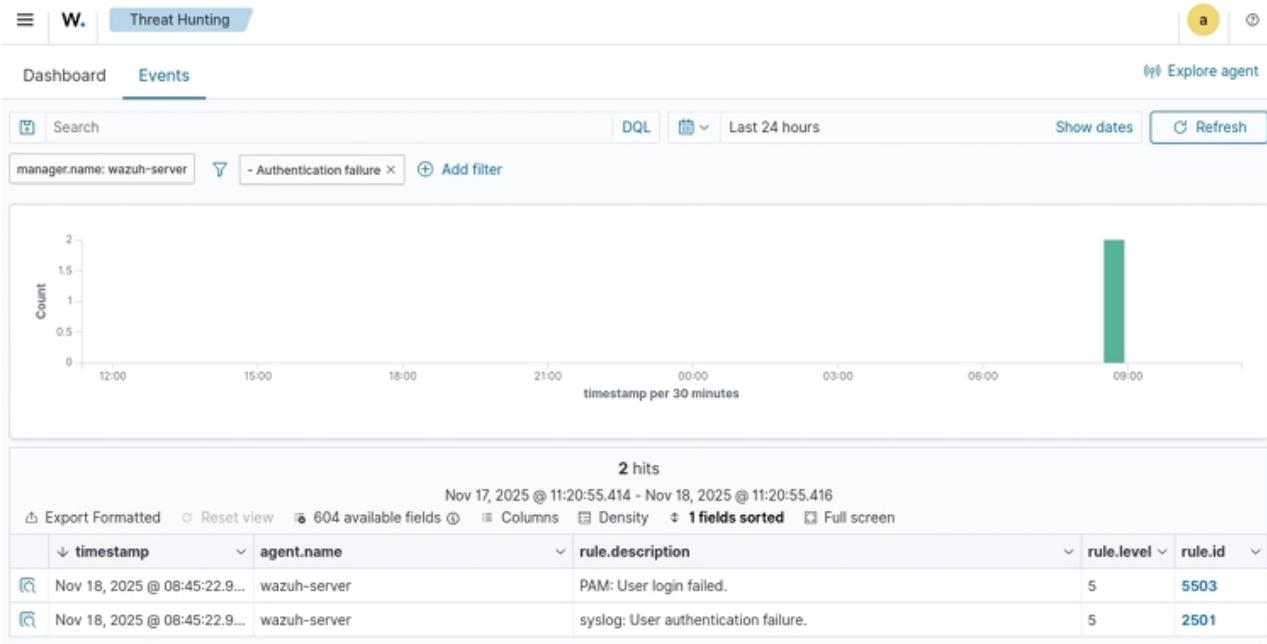
Metriche Threat Hunting:

- **Total:** 2 eventi
- **Level 12+ Alerts:** 0
- **Authentication Failure:** 2
- **Authentication Success:** 0

Eventi di Sicurezza Dettagliati

La sezione eventi mostra dettagli specifici degli incidenti:

Eventi di Sicurezza Specifici:



Eventi Rilevati:

1. Evento 1:

- **Timestamp:** Nov 18, 2025 @ 08:45:22
- **Descrizione:** "PAM: User login failed"- Rule ID: 5503
- **Livello:** 5 (media gravità)
- **Target:** wazuh-server

1. Evento 2:

- **Timestamp:** Nov 18, 2025 @ 08:45:22
- **Descrizione:** "syslog: User authentication failure"
- **Rule ID:** 2501
- **Livello:** 5 (media gravità)
- **Target:** wazuh-server

Analisi: Due tentativi di autenticazione falliti quasi simultanei sul server Wazuh, registrati da moduli diversi (PAM e syslog).

5 Conclusione

Ho completato con successo l'implementazione di un sistema di Incident Response integrato con piattaforma SIEM Wazuh per il monitoraggio di sicurezza

Risultati Principali:

- Sezione Ufficiale:** Ho sviluppato un piano di risposta agli incidenti completo con procedure strutturate per identificazione, contenimento, eradicazione e sanitizzazione dati secondo standard NIST 800-88.
- Sezione Facoltativa:** Ho analizzato due URL malevoli con identificazione di script PowerShell DNS_Changer e vettore di distribuzione malware Google Docs, documentando IOC e pattern di rete.
- Sezione Extra:** Ho completato l'installazione e configurazione Wazuh Server/Agent con dashboard funzionante, connettività verificata su porta 1514 e monitoraggio real-time di 343 eventi.
- Implementazione Tecnica:** Ho configurato un setup Wazuh con 7 moduli attivi (rootcheck, FIM, SCA, logcollector), compliance monitoring per 5 standard normativi, file integrity monitoring su 6 percorsi sensibili e rilevamenti malware su file di sistema critici.
- Valore Professionale:** Il progetto dimostra competenze complete in cybersecurity, incident response, analisi forense e configurazione sistemi SIEM enterprise, fornendo una base solida per la gestione di sicurezza in ambienti complessi.
- Prossimi Sviluppi:** Espansione coverage su tutti i sistemi target, ottimizzazione regole detection, integrazione threat intelligence e implementazione playbook automatizzati.