Laporan Implementasi SOAR Wazuh
(FIM, Failed Login, Agent Disconnected)

Nama: Muhammad Sirojul Fuad

NIM: 1304212094

1. Ringkasan

Implementasi ini membangun pipeline deteksi dan notifikasi berbasis Wazuh untuk 3 skenario utama: (1) File Integrity Monitoring (FIM) pada perubahan file/registry, (2) Failed login / brute force (berbasis event Windows 4625 yang dinormalisasi oleh Wazuh), dan (3) Agent disconnected (monitoring status agent). Setiap skenario dikonfigurasi sebagai Monitor di OpenSearch Dashboards (Alerting) dan mengirimkan alert ke Slack menggunakan Mustache template agar informasi penting tampil ringkas dan jelas.

2. Arsitektur Singkat

Alur data:

- Windows Agent mengirim event (FIM / Windows Security / status agent) ke Wazuh Manager.
- Wazuh mengindeks event ke OpenSearch (wazuh-alerts-4.x-* dan wazuh-monitoring-*).
- OpenSearch Dashboards Alerting menjalankan query periodik (monitor) dan memicu trigger.
- Action: kirim pesan ke Slack melalui konektor Notification menggunakan webhook.

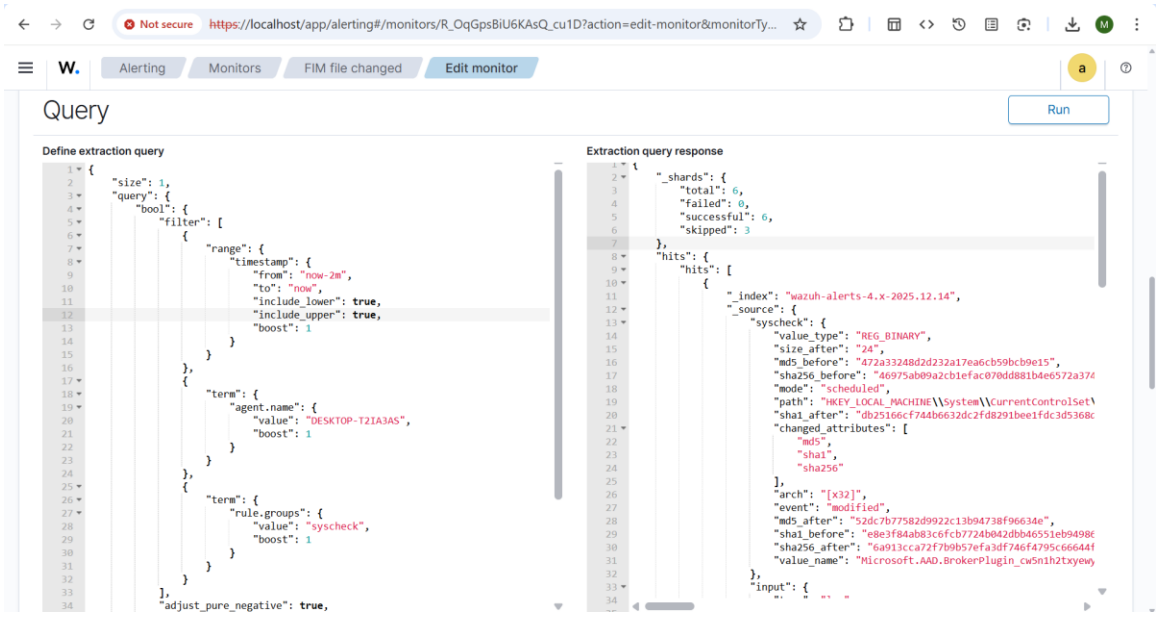
3. Use Case & Konfigurasi Monitor

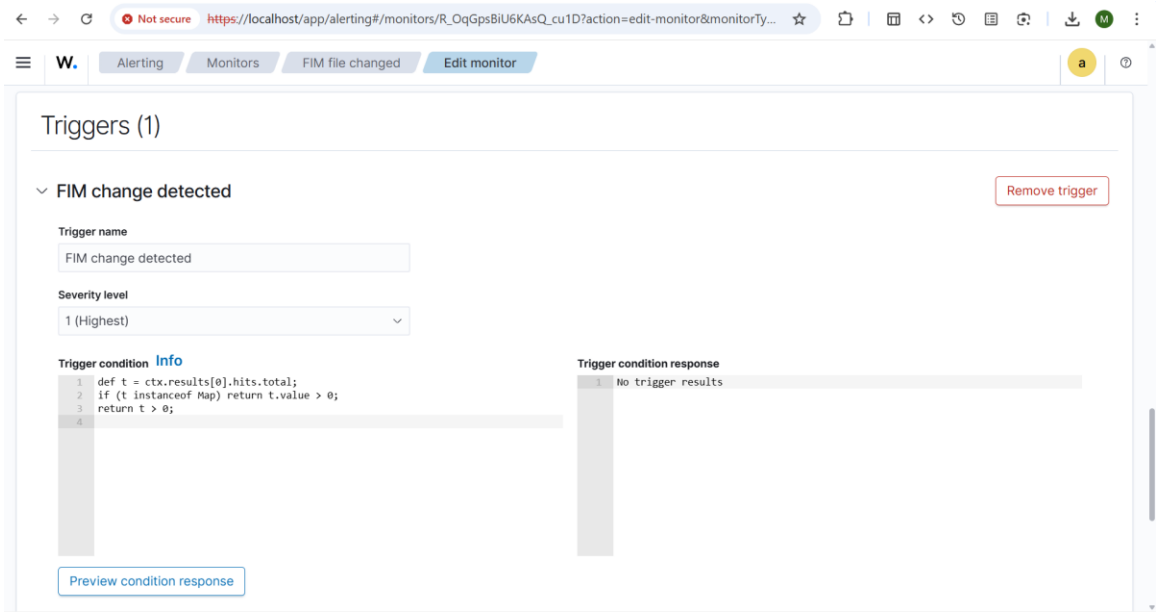
Use case	Index	Filter utama	Tipe monitor	Trigger	Output Slack
FIM (file/registry change)	wazuh-alerts-4.x-*	rule.groups: syscheck, agent.name	Per query	hits.total > 0	Detail path, event, hash
Failed login (Windows 4625)	wazuh-alerts-4.x-*	rule.id: 60122 (atau data.win.system.eventID: 4625)	Per query / per bucket	hits.total atau count >= N	User, IP, logon type, reason

Agent disconnected	wazuh-monitoring-4.x-* / wazuh-monitoring-*	status_code: 3 atau exists(disconnection_time)	Per query	hits.total > 0	Agent, status_code, lastKeepAlive

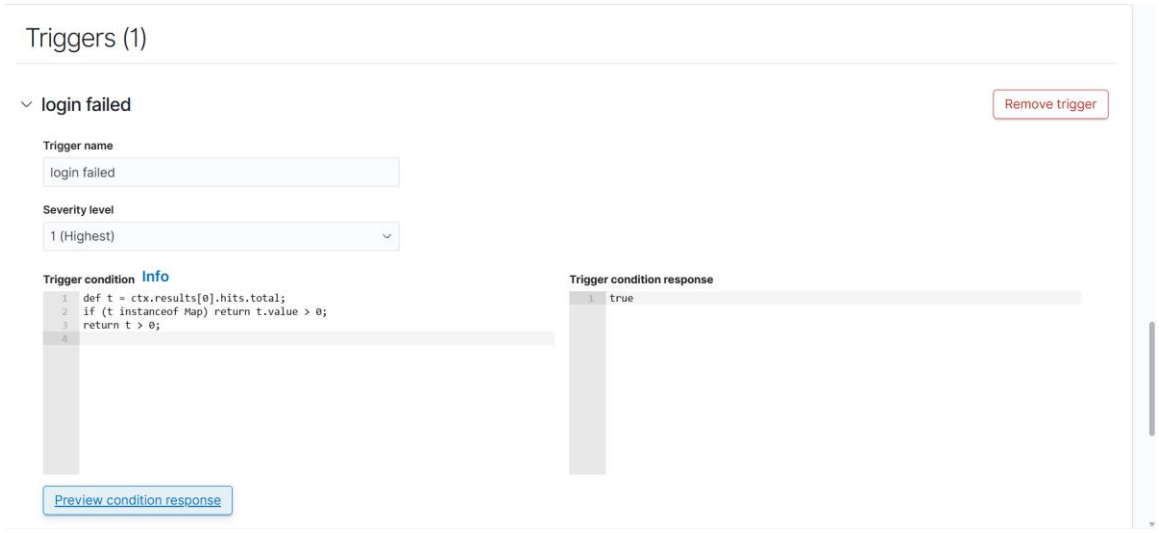
4. Query DSL & Trigger

FIM (syscheck):

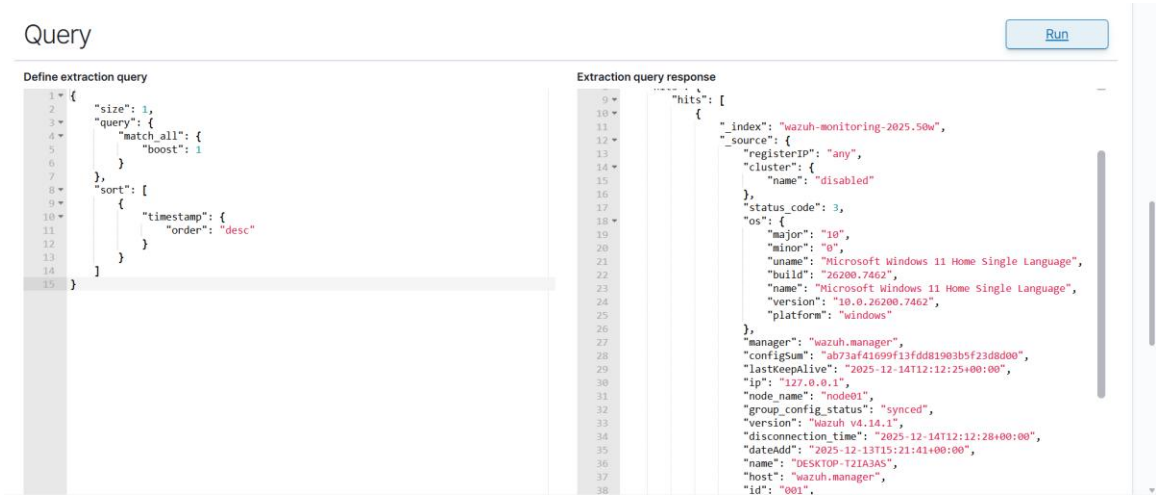


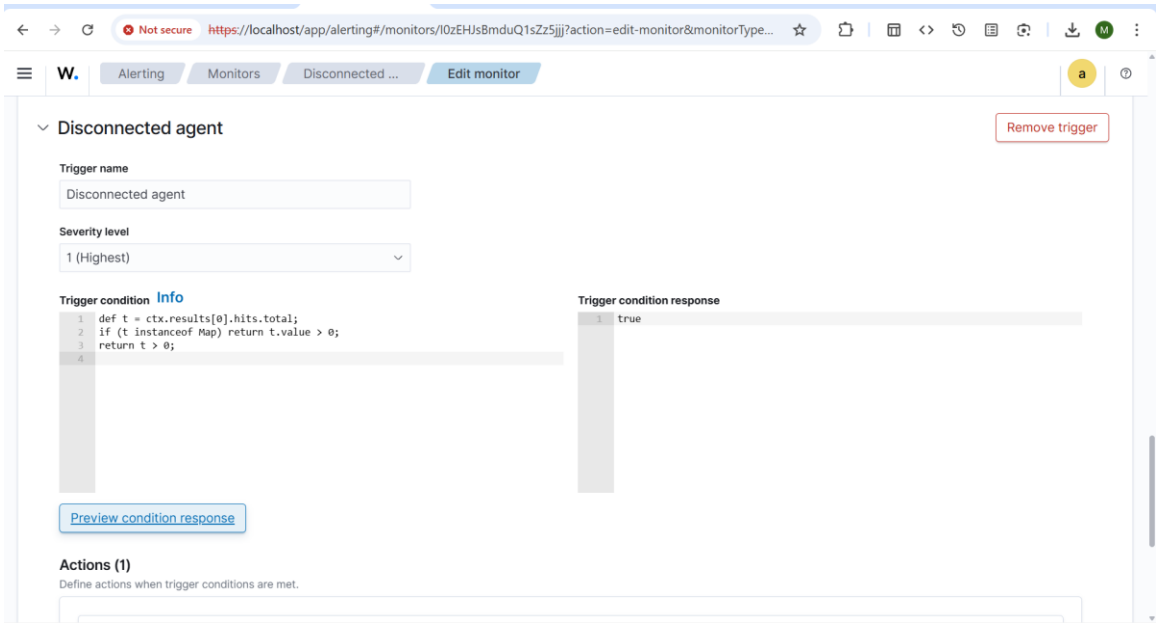


Failed login (Wazuh rule 60122 / Windows 4625):



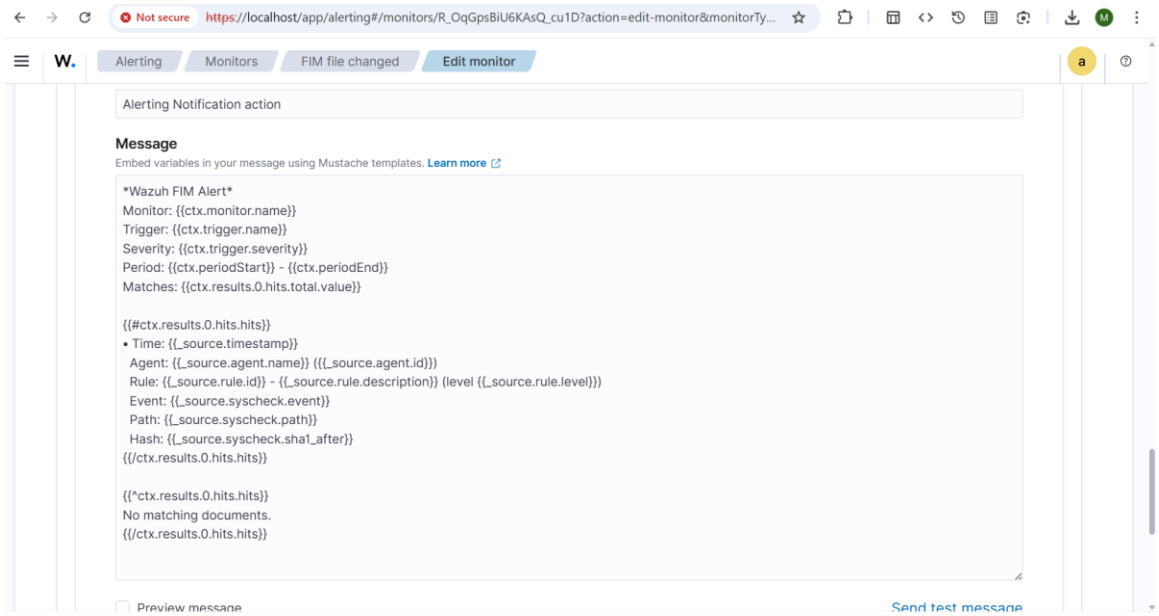
Agent disconnected (monitoring index):



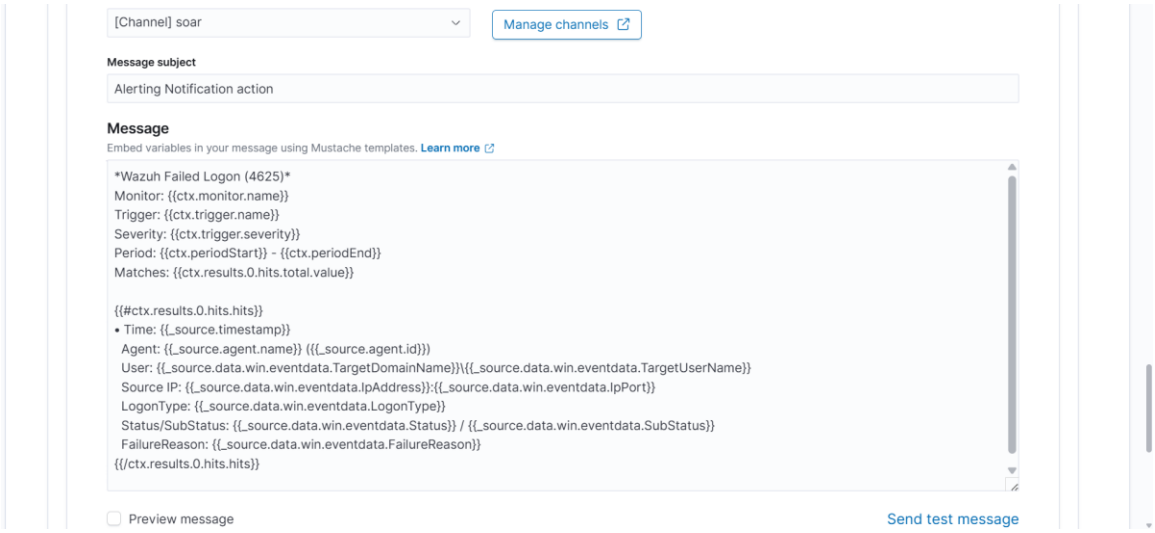


5. Template Pesan Slack (Mustache)

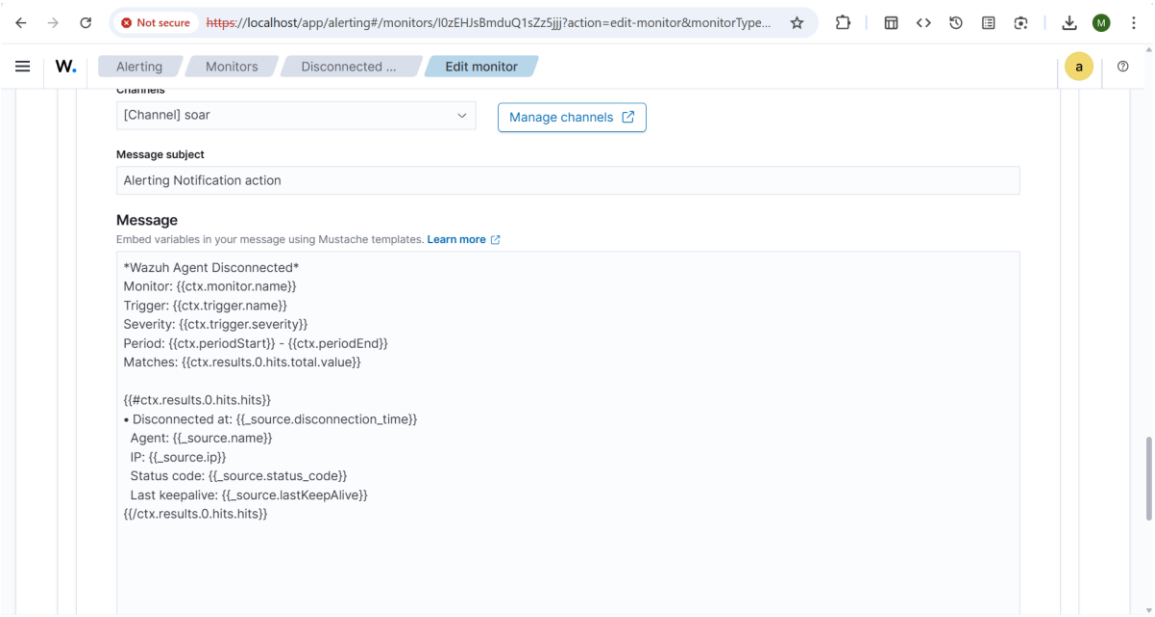
FIM (syscheck):



Failed login (Wazuh rule 60122 / Windows 4625):



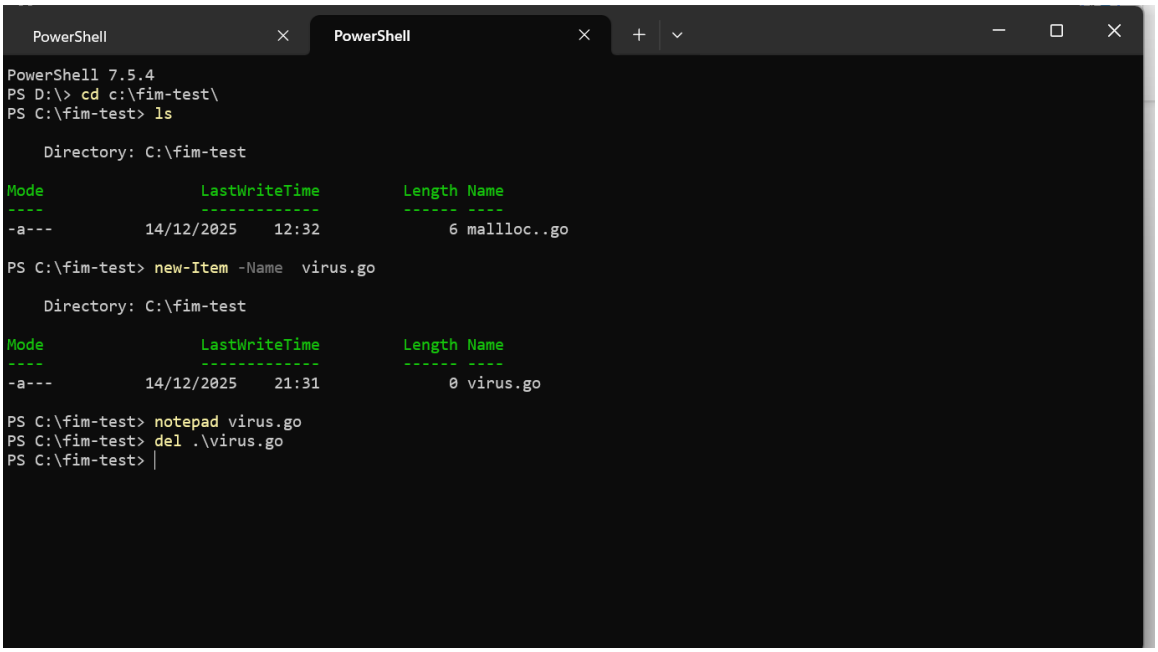
Agent disconnected (monitoring index):



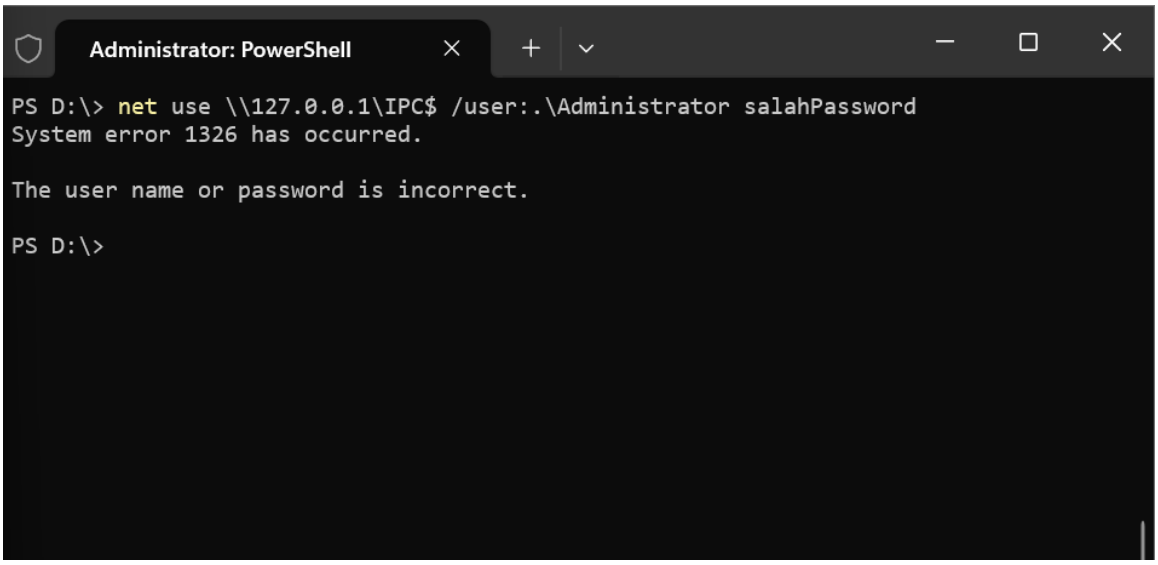
6. Pengujian

Metode pengujian:

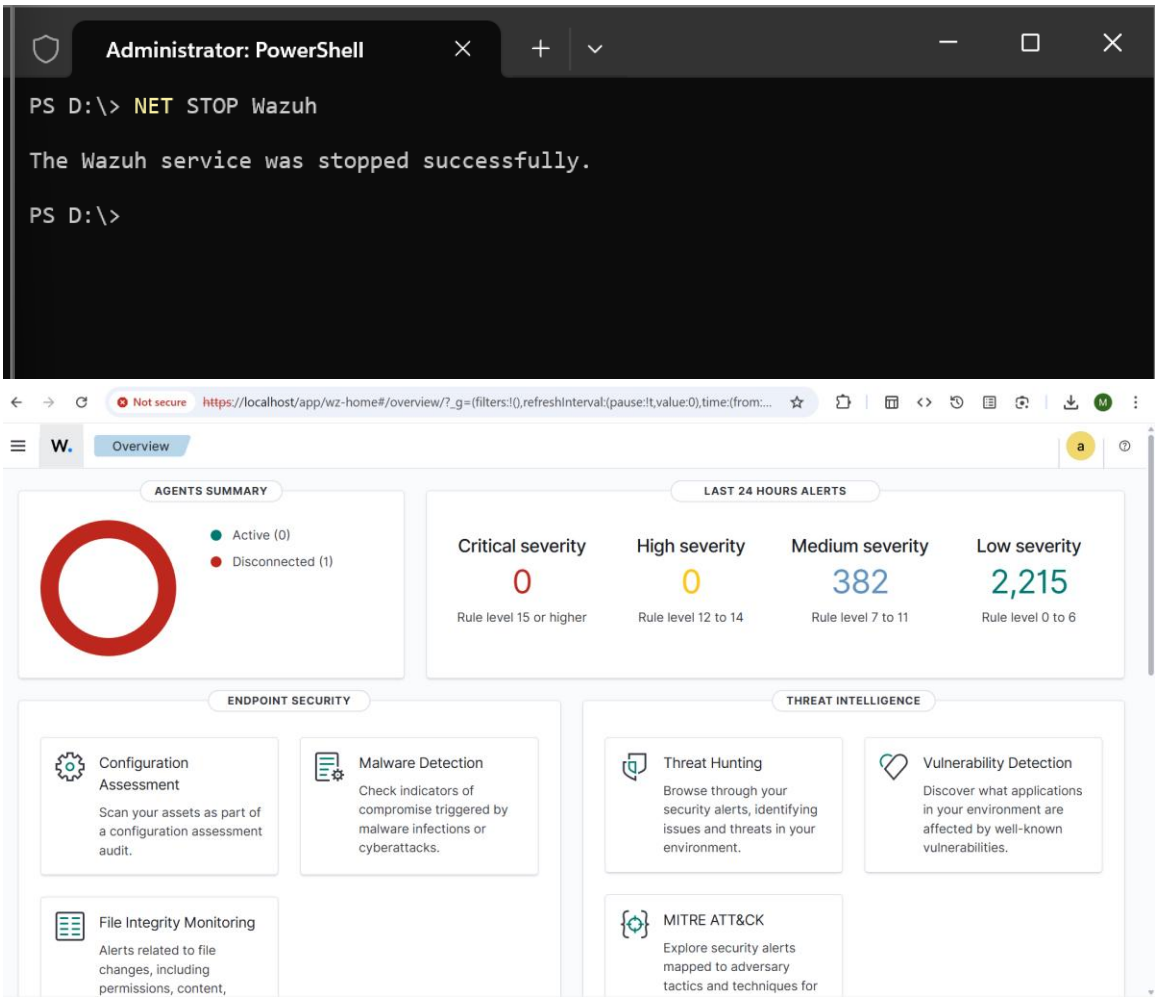
1. FIM: memodifikasi file/registry yang dimonitor untuk memicu rule syscheck.



2. Failed login: memicu Windows Security Event ID 4625 misalnya. login salah via net use / runas.



3. Agent disconnected: menghentikan service agent atau memutus koneksi jaringan, lalu verifikasi munculnya record di index monitoring.



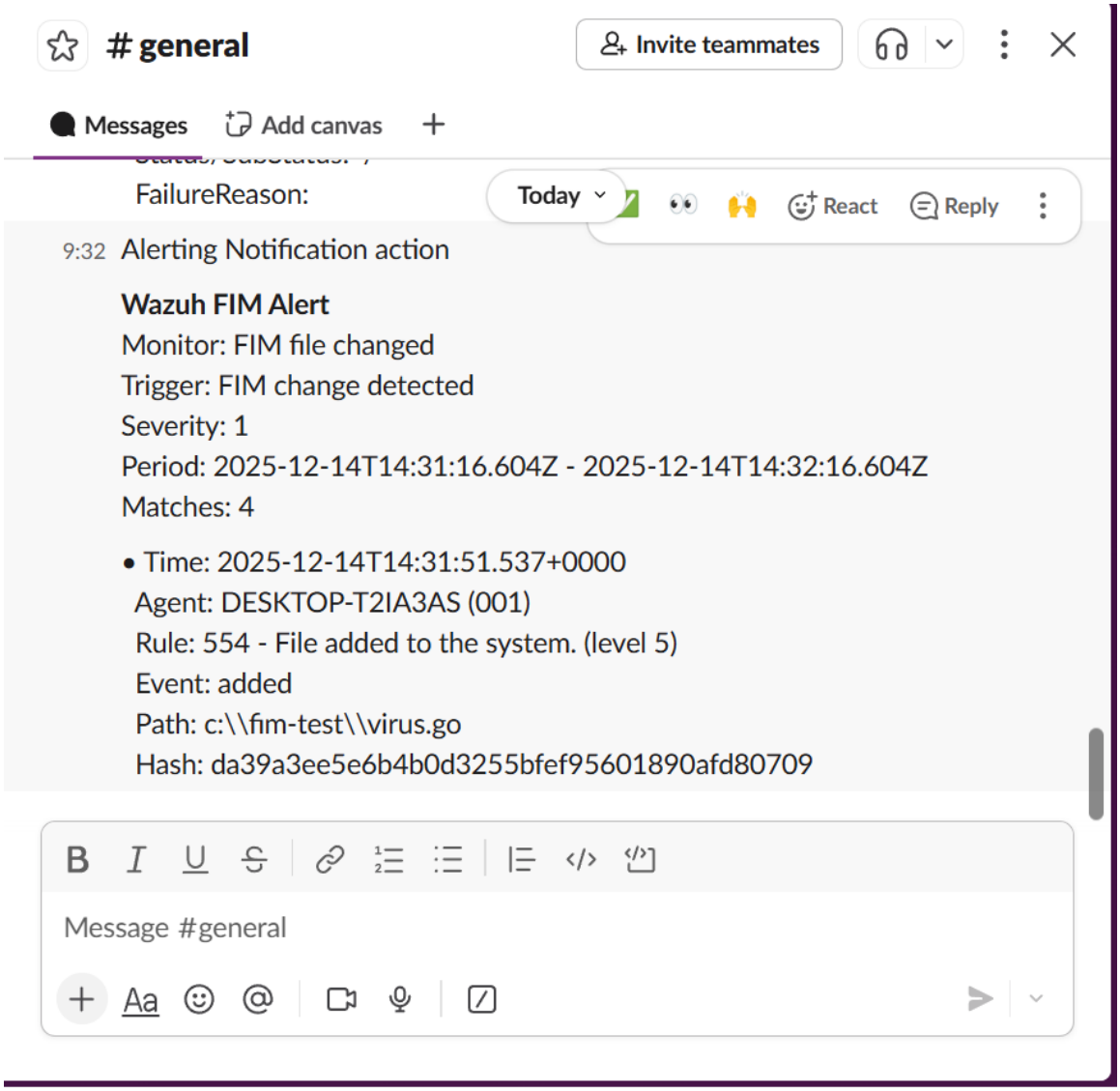
7. Hasil & Review Singkat

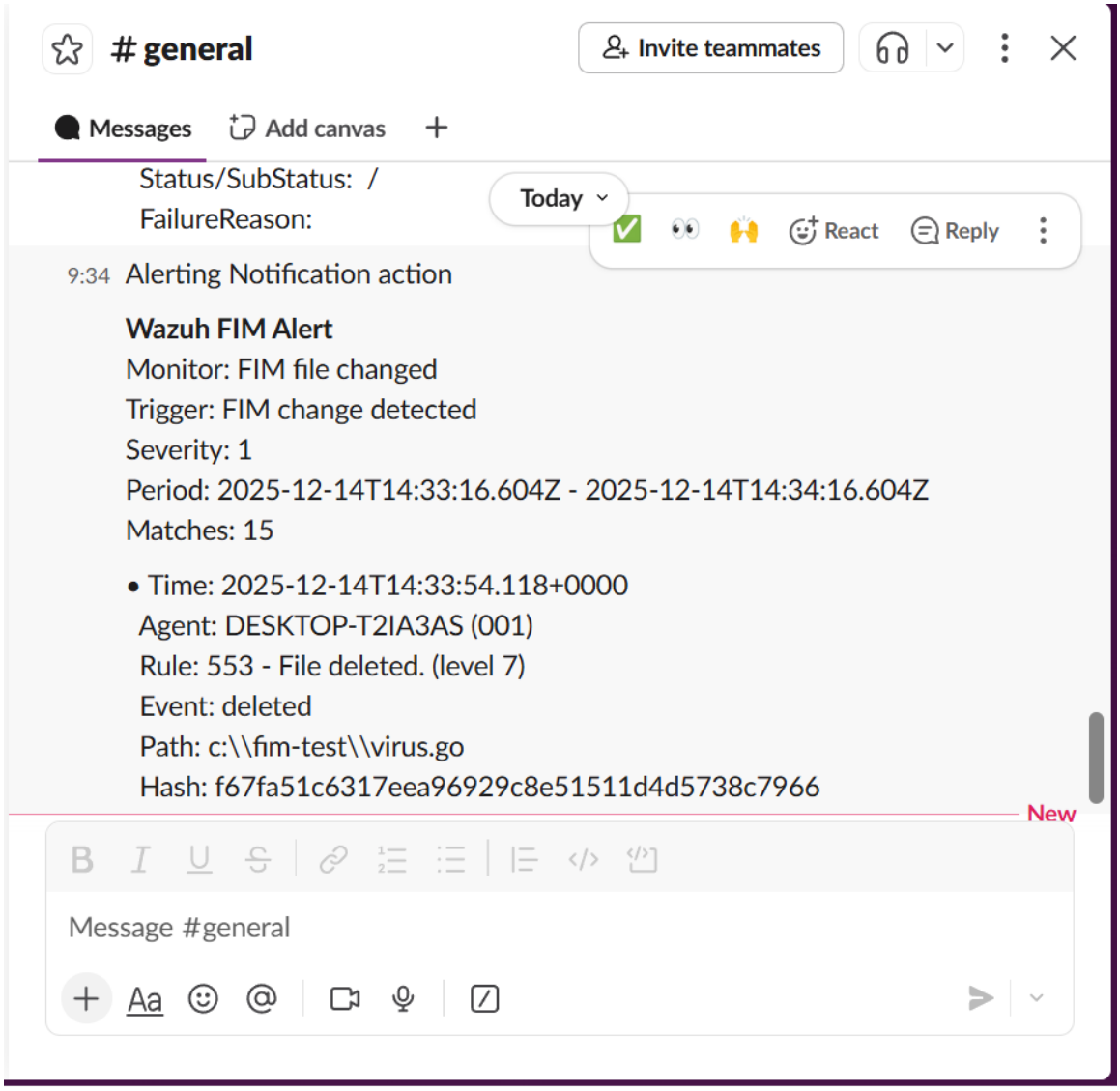
Ringkasan hasil uji (contoh):

- Notifikasi Slack berhasil terkirim untuk ketiga skenario.
- FIM menampilkan detail path + event + hash sehingga mudah ditindaklanjuti.
- Failed login terdeteksi oleh rule 60122; untuk menampilkan user/IP/logon type pastikan field Wazuh yang digunakan sesuai mapping (lihat Dataset & Catatan).
- Agent disconnected terdeteksi dari index monitoring melalui status_code/disconnection_time.

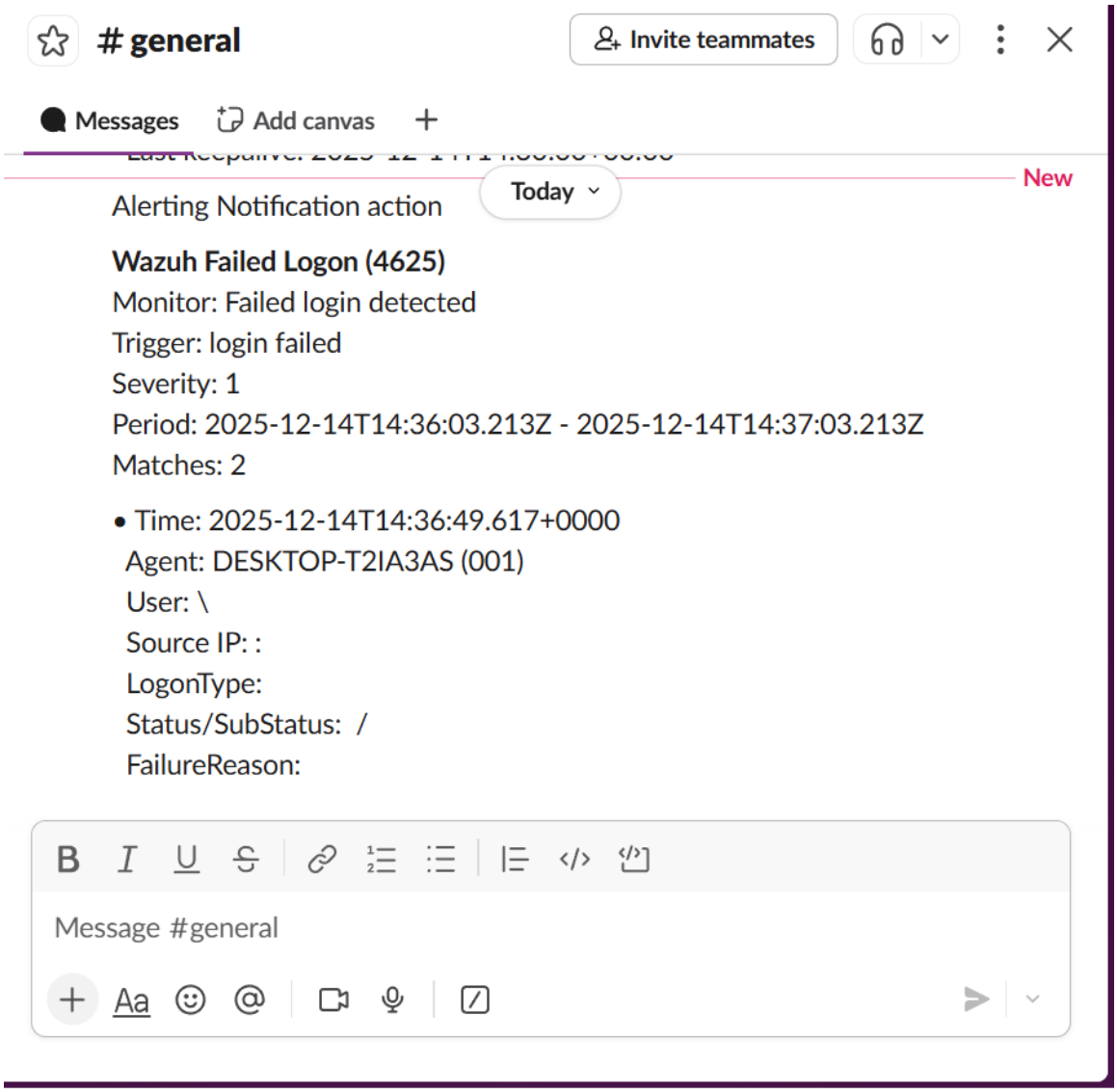
Lampiran: Bukti Screenshot

Fim Alert

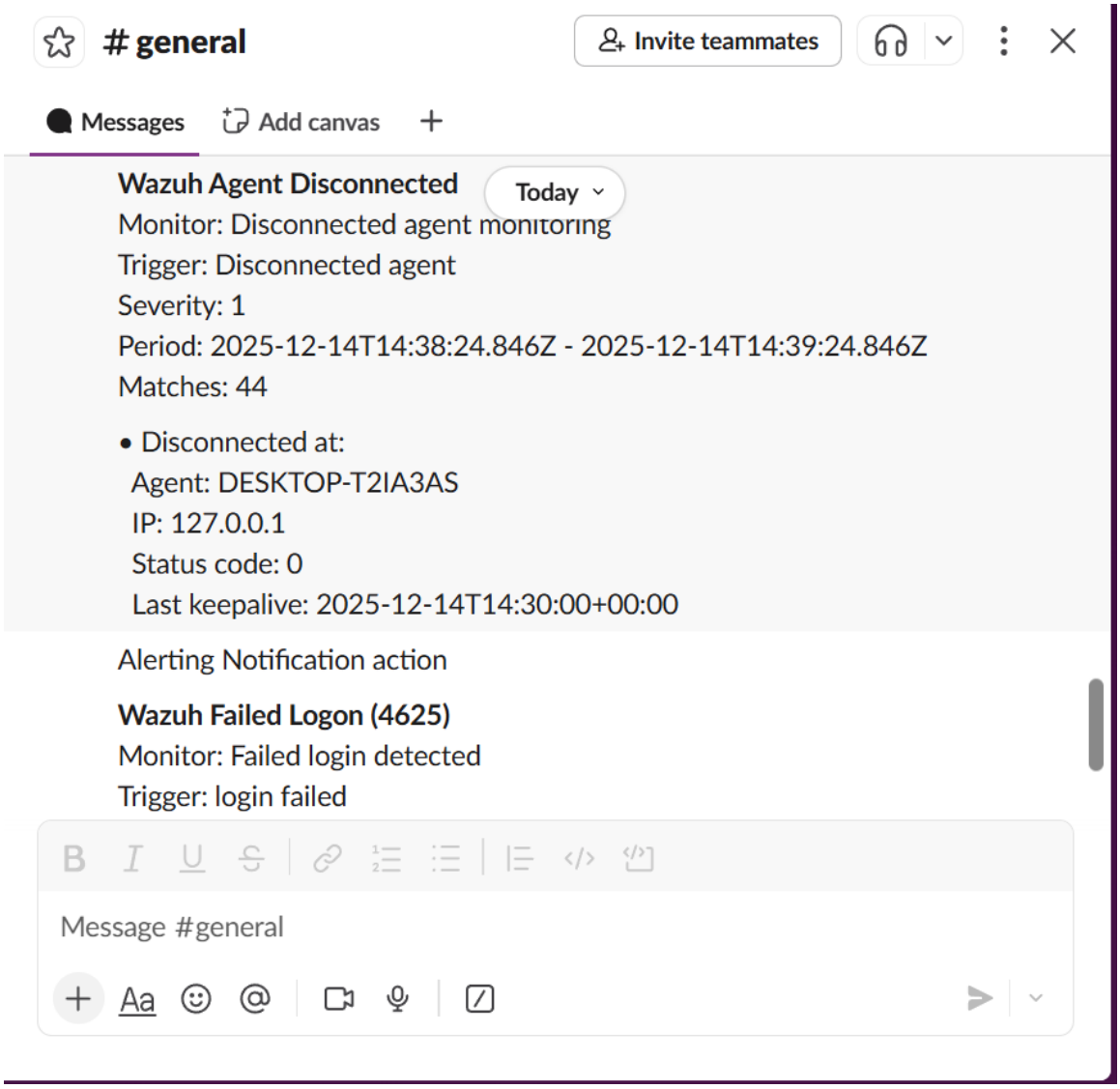

general
Invite teammates
Messages
Add canvas
FailureReason:
Today
React
Reply
9:32 Alerting Notification action
Wazuh FIM Alert
Monitor: FIM file changed
Trigger: FIM change detected
Severity: 1
Period: 2025-12-14T14:31:16.604Z - 2025-12-14T14:32:16.604Z
Matches: 4
• Time: 2025-12-14T14:31:51.537+0000
Agent: DESKTOP-T2IA3AS (001)
Rule: 554 - File added to the system. (level 5)
Event: added
Path: c:\\fim-test\\virus.go
Hash: da39a3ee5e6b4b0d3255bfef95601890afd80709
Message #general


general
Invite teammates
Messages
Add canvas
Status/SubStatus: /
FailureReason:
Today
React
Reply
9:34 Alerting Notification action
Wazuh FIM Alert
Monitor: FIM file changed
Trigger: FIM change detected
Severity: 1
Period: 2025-12-14T14:33:16.604Z - 2025-12-14T14:34:16.604Z
Matches: 15
• Time: 2025-12-14T14:33:54.118+0000
Agent: DESKTOP-T2IA3AS (001)
Rule: 553 - File deleted. (level 7)
Event: deleted
Path: c:\\fim-test\\virus.go
Hash: f67fa51c6317eea96929c8e51511d4d5738c7966
New
Message #general

Failed login:



Agent Disconnected


general
Invite teammates
Messages
Add canvas
Wazuh Agent Disconnected
Today
Monitor: Disconnected agent monitoring
Trigger: Disconnected agent
Severity: 1
Period: 2025-12-14T14:38:24.846Z - 2025-12-14T14:39:24.846Z
Matches: 44
• Disconnected at:
Agent: DESKTOP-T2IA3AS
IP: 127.0.0.1
Status code: 0
Last keepalive: 2025-12-14T14:30:00+00:00
Alerting Notification action
Wazuh Failed Logon (4625)
Monitor: Failed login detected
Trigger: login failed
Message #general
Aa