

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):

```

Define extraction query
1 { "size": 1,
2   "query": {
3     "bool": {
4       "filter": [
5         {
6           "range": {
7             "timestamp": {
8               "from": "now-2m",
9               "to": "now",
10              "include_lower": true,
11              "include_upper": true,
12              "boost": 1
13            }
14          }
15        },
16        {
17          "term": {
18            "agent.name": {
19              "value": "DESKTOP-T2IA3AS",
20              "boost": 1
21            }
22          }
23        },
24        {
25          "term": {
26            "rule.groups": {
27              "value": "syscheck",
28              "boost": 1
29            }
30          }
31        }
32      ],
33      "adjust_pure_negative": true,
34    }
  }

Extraction query response
1 { "_shards": {
2   "total": 6,
3   "failed": 0,
4   "successful": 6,
5   "skipped": 3
6 },
7   "hits": [
8     {
9       "_index": "wazuh-alerts-4.x-2025.12.14",
10      "_source": "{
11        \"syscheck\": {
12          \"value_type\": \"REG_BINARY\",
13          \"size_after\": \"24\",
14          \"md5_before\": \"472a33248d2d232a17ea6cb59bc9e15\",
15          \"sha256_before\": \"46975ab09a2cb1efac070dd881b4e0572a37e\",
16          \"mode\": \"scheduled\",
17          \"path\": \"HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\",
18          \"sha1_after\": \"db25166cf744ab6632dc2fd8291bee1fdc3d5368c\",
19          \"changed_attributes\": [
20            \"md5\",
21            \"sha1\",
22            \"sha256\"
23          ],
24          \"arch\": \"[x32]\"},
25          \"event\": \"modified\",
26          \"md5_after\": \"52dc7b77582d9922c13b94738f96634e\",
27          \"sha1_before\": \"e8e3f84ab083c6fc7724b0420b046551eb9498c\",
28          \"sha256_after\": \"eaa13cca22f799b57efad3df746f4795c6664af\",
29          \"value_name\": \"Microsoft.AAD.BrokerPlugin_cw5nh2txyeuw\"
30        },
31        \"input\": {
32          \"**\": \"\"
33        }
34      }
  }

```

Triggers (1)

Remove trigger

FIM change detected

Trigger name: FIM change detected

Severity level: 1 (Highest)

Trigger condition [Info](#)

```

1 def t = ctx.results[0].hits.total;
2 if (t instanceof Map) return t.value > 0;
3 return t > 0;
4

```

Trigger condition response [Info](#)

No trigger results

Preview condition response

Failed login (Wazuh rule 60122 / Windows 4625):

Query

[Run](#)

Define extraction query

```

1 { "size": 1,
2   "query": {
3     "bool": {
4       "filter": [
5         {
6           "range": {
7             "timestamp": {
8               "from": "now-1h",
9               "to": "now",
10              "include_lower": true,
11              "include_upper": true,
12              "boost": 1
13            }
14          }
15        },
16        {
17          "term": {
18            "rule.id": {
19              "value": 60122,
20              "boost": 1
21            }
22          }
23        }
24      ],
25      "adjust_pure_negative": true,
26      "boost": 1
27    }
28  },
29  "sort": [
30    {
31      "timestamp": {
32        "order": "desc"
33      }
34    }
35  ]
36 }

```

Extraction query response

```

12 {
13   "_source": {
14     "input": {
15       "type": "log"
16     },
17     "agent": {
18       "ip": "127.0.0.1",
19       "name": "DESKTOP-T2IA3AS",
20       "id": "001"
21     },
22     "@timestamp": "2025-12-14T14:25:43.680Z",
23     "manager": {
24       "name": "wazuh.manager"
25     },
26     "data": {
27       "win": {
28         "eventdata": {
29           "subjectLogonId": "0x0",
30           "ipAddress": "127.0.0.1",
31           "authenticationPackageName": "Kerberos",
32           "logonProcessName": "Windows Logon Process-12IA3AS",
33           "substatus": "0xc000000d",
34           "logonProcessName": "Httmssp",
35           "targetUserName": "Administrator",
36           "keyLength": "0",
37           "subjectUserId": "S-1-0-0",
38           "processId": "0x0",
39           "ipPort": "54890",
40           "failureReason": "%K2313",
41           "targetDomainName": ".",
42           "targetUserId": "S-1-0-0",
43           "logonType": "3",
44           "status": "0xc000006d"
45         }
46       }
47     }
48   }
49 }

```

Triggers (1)

login failed

[Remove trigger](#)

Trigger name

login failed

Severity level

1 (Highest)

Trigger condition Info

```

1 def t = ctx.results[0].hits.total;
2 if (t instanceof Map) return t.value > 0;
3 return t > 0;
4

```

Trigger condition response

true

[Preview condition response](#)

Agent disconnected (monitoring index):

Query

[Run](#)

Define extraction query

```

1 { "size": 1,
2   "query": {
3     "match_all": {
4       "boost": 1
5     }
6   },
7   "sort": [
8     {
9       "timestamp": {
10         "order": "desc"
11       }
12     }
13   ]
14 }

```

Extraction query response

```

9 {
10   "hits": [
11     {
12       "_index": "wazuh-monitoring-2025.50w",
13       "_source": {
14         "registerIP": "any",
15         "cluster": {
16           "name": "disabled"
17         },
18         "status_code": 3,
19         "os": {
20           "major": "10",
21           "minor": "0",
22           "uname": "Microsoft Windows 11 Home Single Language",
23           "build": "26200.7462",
24           "name": "Microsoft Windows 11 Home Single Language",
25           "version": "10.0.26200.7462",
26           "platform": "windows"
27         },
28         "manager": "wazuh.manager",
29         "configSum": "ab73af41699f13fd81903b5f23d8d00",
30         "lastKeepAlive": "2025-12-14T12:12:25+00:00",
31         "ip": "127.0.0.1",
32         "node_name": "node01",
33         "group_config_status": "synced",
34         "version": "Wazuh v4.14.1",
35         "disconnection_time": "2025-12-14T12:12:28+00:00",
36         "dateAdd": "2025-12-13T15:21:41+00:00",
37         "name": "DESKTOP-T2IA3AS",
38         "host": "wazuh.manager",
39         "id": "001"
40       }
41     }
42   }
43 }

```

The screenshot shows the Wazuh Alerting interface with the URL <https://localhost/app/alerting#/monitors/l0zEHJsBmduQ1sZz5jj?action=edit-monitor&monitorType...>. The page title is "W. Alerting Monitors Disconnected ... Edit monitor".

Trigger name: Disconnected agent

Severity level: 1 (Highest)

Trigger condition (Info):

```

1 def t = ctx.results[0].hits.total;
2 if (t instanceof Map) return t.value > e;
3 return t > 0;
4

```

Trigger condition response:

```

1 true

```

Actions (1): Define actions when trigger conditions are met.

Preview condition response:

5. Template Pesan Slack (Mustache)

FIM (syscheck):

The screenshot shows the Wazuh Alerting interface with the URL https://localhost/app/alerting#/monitors/R_OqGpsBiU6KAAsQ_cu1D?action=edit-monitor&monitorTy.... The page title is "W. Alerting Monitors FIM file changed Edit monitor".

Alerting Notification action:

Message:

Embed variables in your message using Mustache templates. [Learn more](#)

```

*Wazuh FIM Alert*
Monitor: {{ctx.monitor.name}}
Trigger: {{ctx.trigger.name}}
Severity: {{ctx.trigger.severity}}
Period: {{ctx.periodStart}} - {{ctx.periodEnd}}
Matches: {{ctx.results[0].hits.total.value}}


{{#ctx.results[0].hits.hits}}
• Time: {{source.timestamp}}
Agent: {{source.agent.name}} ({{source.agent.id}})
Rule: {{source.rule.id}} - {{source.rule.description}} (level {{source.rule.level}})
Event: {{source.syscheck.event}}
Path: {{source.syscheck.path}}
Hash: {{source.syscheck.sha1_after}}
{{/ctx.results[0].hits.hits}}


{{^ctx.results[0].hits.hits}}
No matching documents.
{{/ctx.results[0].hits.hits}}

```

Preview message:

Send test message:

Failed login (Wazuh rule 60122 / Windows 4625):

[Channel] soar

[Manage channels](#)

Message subject

Message

Embed variables in your message using Mustache templates. [Learn more](#)

```
*Wazuh Failed Logon (4625)
Monitor: {{ctx.monitor.name}}
Trigger: {{ctx.trigger.name}}
Severity: {{ctx.trigger.severity}}
Period: {{ctx.periodStart}} - {{ctx.periodEnd}}
Matches: {{ctx.results.0.hits.total.value}}

{{#ctx.results.0.hits.hits}}
• Time: {{_source.timestamp}}
Agent: {{_source.agent.name}} ({{_source.agent.id}})
User: {{_source.data.win.eventdata.TargetDomainName}}{{_source.data.win.eventdata.TargetUserName}}
Source IP: {{_source.data.win.eventdata.ipAddress}}{{_source.data.win.eventdata.ipPort}}
LogonType: {{_source.data.win.eventdata.LogonType}}
Status/SubStatus: {{_source.data.win.eventdata.Status}} / {{_source.data.win.eventdata.SubStatus}}
FailureReason: {{_source.data.win.eventdata.FailureReason}}
{{/ctx.results.0.hits.hits}}
```

Preview message

[Send test message](#)

Agent disconnected (monitoring index):

Not secure https://localhost/app/alerting#/monitors/I0zEHJsBmdUQ1sZz5jj?action=edit-monitor&monitorType...        

W. Alerting Monitors Disconnected ... Edit monitor

Channels [Channel] soar  Manage channels 

Message subject
Alerting Notification action

Message
Embed variables in your message using Mustache templates. [Learn more](#)

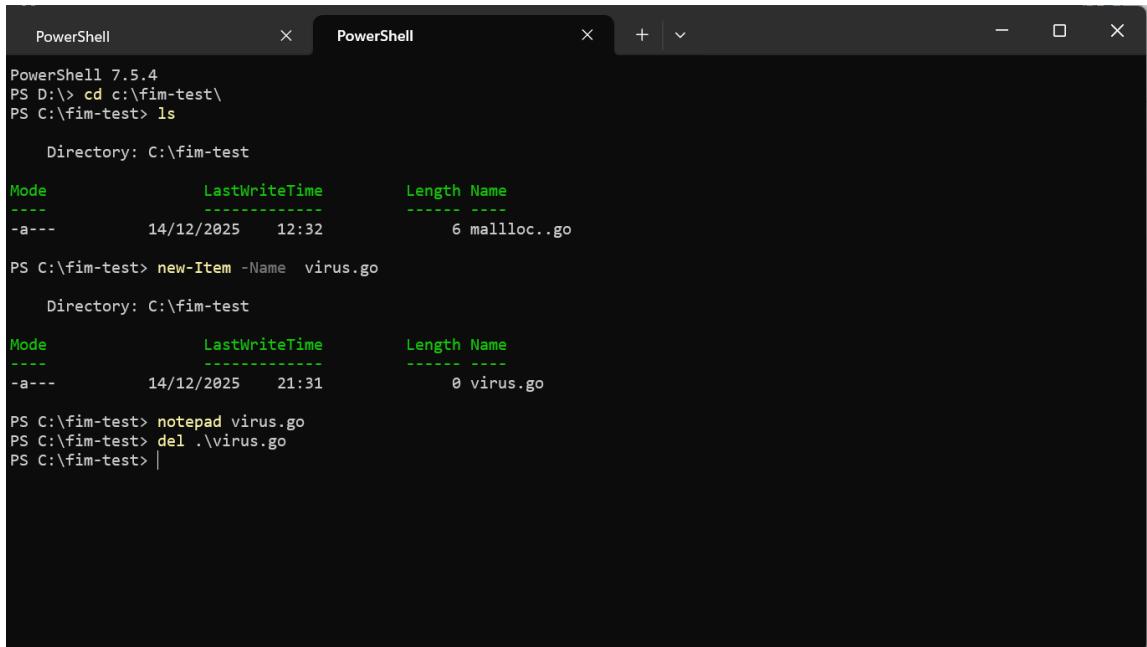
```
*Wazuh Agent Disconnected*
Monitor: {{ctx.monitor.name}}
Trigger: {{ctx.trigger.name}}
Severity: {{ctx.trigger.severity}}
Period: {{ctx.periodStart}} - {{ctx.periodEnd}}
Matches: {{ctx.results[0].hits.total.value}}


{{#ctx.results[0].hits.hits}}
• Disconnected at: {{source.disconnection_time}}
Agent: {{source.name}}
IP: {{source.ip}}
Status code: {{source.status_code}}
Last keepalive: {{source.lastKeepAlive}}
{{/ctx.results[0].hits}}
```

6. Pengujian

Metode pengujian:

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



The screenshot shows two separate PowerShell windows side-by-side. Both windows have a dark theme.

The left window's command history is:

```
PowerShell 7.5.4
PS D:\> cd c:\fim-test\
PS C:\fim-test> ls

    Directory: C:\fim-test

Mode           LastWriteTime         Length Name
----           -----          ----- ----
-a--- 14/12/2025 12:32            6 malloc..go

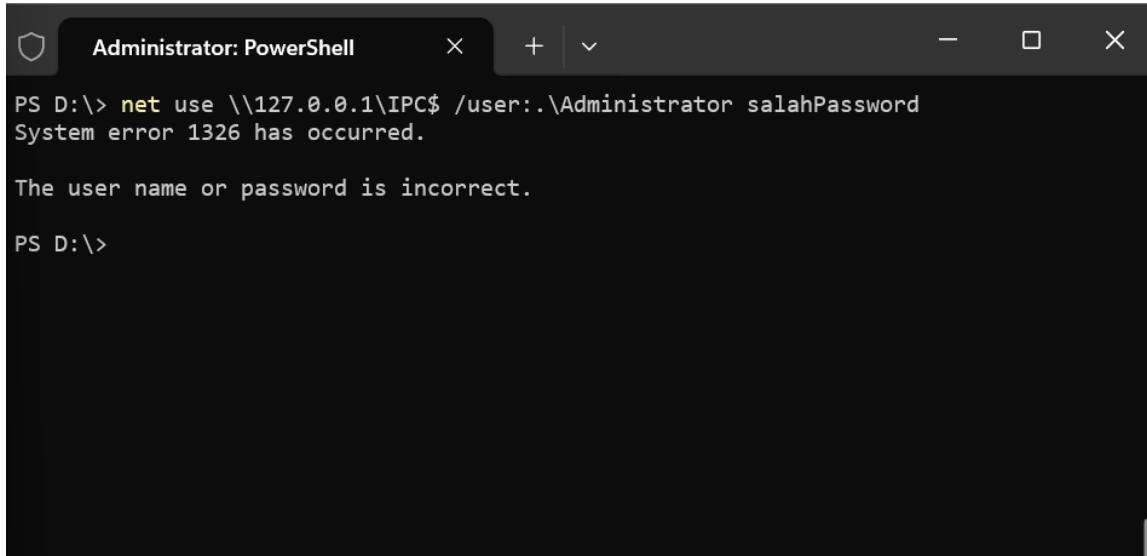
PS C:\fim-test> new-item -Name virus.go

    Directory: C:\fim-test

Mode           LastWriteTime         Length Name
----           -----          ----- ----
-a--- 14/12/2025 21:31            0 virus.go

PS C:\fim-test> notepad virus.go
PS C:\fim-test> del .\virus.go
PS C:\fim-test> |
```

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



The screenshot shows a single PowerShell window with an administrator shield icon in the title bar. The title bar also says "Administrator: PowerShell".

The command entered was:

```
PS D:\> net use \\127.0.0.1\IPC$ /user:.\\Administrator salahPassword
System error 1326 has occurred.

The user name or password is incorrect.

PS D:\>
```

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

```
Administrator: PowerShell
PS D:\> NET STOP Wazuh
The Wazuh service was stopped successfully.

PS D:\>
```

The screenshot shows a Windows PowerShell window titled "Administrator: PowerShell". The command "NET STOP Wazuh" is entered, followed by the output "The Wazuh service was stopped successfully." Below the PowerShell window is a screenshot of a web browser displaying the Wazuh dashboard at <https://localhost/app/wz-home#/overview>. The dashboard has sections for "AGENTS SUMMARY" (red circle icon, Active: 0, Disconnected: 1), "LAST 24 HOURS ALERTS" (0 Critical, 0 High, 382 Medium, 2,215 Low), "ENDPOINT SECURITY" (Configuration Assessment, Malware Detection), "THREAT INTELLIGENCE" (Threat Hunting, Vulnerability Detection, MITRE ATT&CK), and a "File Integrity Monitoring" section.

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

60

⋮ X

Messages

Add canvas +

Status, Substatus, /

FailureReason:

Today



00



1



+ 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

B *I* U ~~C~~ | </>

Message #general



Aa



@





general

Invite teammates

60

⋮ X

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

B *I* U ~~S~~ | ⌂ 1≡ 2≡ | ≡ ≡ </> ↵

Message #general



Aa



@



Failed login:

The screenshot shows a Slack message in the '#general' channel. The message is from 'Alerting Notification action' and contains the following details:

Wazuh Failed Logon (4625)
Monitor: Failed login detected
Trigger: login failed
Severity: 1
Period: 2025-12-14T14:36:03.213Z - 2025-12-14T14:37:03.213Z
Matches: 2

- Time: 2025-12-14T14:36:49.617+0000

Agent: DESKTOP-T2IA3AS (001)
User: \
Source IP: :
LogonType:
Status/SubStatus: /
FailureReason:

Below the message is a rich text editor interface with various formatting buttons (B, I, U, etc.) and a message input field.

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

