

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):

Wazuh

AlertingMonitorsFIM file changedEdit monitor

Query

Define extraction query

```
1 {
2   "size": 1,
3   "query": {
4     "bool": {
5       "filter": [
6         {
7           "range": {
8             "timestamp": {
9               "from": "now-2m",
10              "to": "now",
11              "include_lower": true,
12              "include_upper": true,
13              "boost": 1
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      }
34    },
35    "adjust_pure_negative": true,
```

Extraction query response

```
1 {
2   "_shards": {
3     "total": 6,
4     "failed": 0,
5     "successful": 6,
6     "skipped": 3
7   },
8   "hits": {
9     "total": {
10      "value": 6,
11      "relation": "eq"
12    },
13    "_source": {
14      "syscheck": {
15        "value_type": "REG_BINARY",
16        "size_after": "24",
17        "md5_before": "472a33248d2d232a17e66cb59bcb9e15",
18        "sha256_before": "46975ab09a2cb1efac070dd881b4e6572a374",
19        "mode": "scheduled",
20        "path": "HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\",
21        "sha1_after": "db25166cf744b6632dc2f08291bee1fdc3d5368c",
22        "changed_attributes": [
23          "md5",
24          "sha1",
25          "sha256"
26        ],
27        "arch": "[x32]",
28        "event": "modified",
29        "md5_after": "52dc7b77582d9922c13b94738f96634e",
30        "sha1_before": "e8e3f84ab83c6fc7724b042dbb46551eb9498e",
31        "sha256_after": "6a913cca72f7b9b57efaf3df746f4795c66644f",
32        "value_name": "Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy"
33      }
34    },
35    "input": {
36      "type": "syscheck",
37      "value": "HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\",
38      "path": "HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\",
39      "sha1_after": "db25166cf744b6632dc2f08291bee1fdc3d5368c",
40      "sha256_after": "6a913cca72f7b9b57efaf3df746f4795c66644f",
41      "md5_after": "52dc7b77582d9922c13b94738f96634e",
42      "event": "modified",
43      "arch": "[x32]",
44      "changed_attributes": [
45        "md5",
46        "sha1",
47        "sha256"
48      ],
49      "mode": "scheduled",
50      "sha256_before": "46975ab09a2cb1efac070dd881b4e6572a374",
51      "md5_before": "472a33248d2d232a17e66cb59bcb9e15",
52      "size_after": "24",
53      "value_type": "REG_BINARY"
54    }
55  }
56 }
```

Triggers (1)

FIM change detected

Remove trigger

Trigger name

FIM change detected

Severity level

1 (Highest)

Trigger condition

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

Preview condition response

Trigger condition response

1 No trigger results

Failed login (Wazuh rule 60122 / Windows 4625):

Query Run

Define extraction query

```
1 {
2   "size": 1,
3   "query": {
4     "bool": {
5       "filter": [
6         {
7           "range": {
8             "timestamp": {
9               "from": "now-1h",
10              "to": "now",
11              "include_lower": true,
12              "include_upper": true,
13              "boost": 1
14            }
15          }
16        },
17        {
18          "term": {
19            "rule.id": {
20              "value": 60122,
21              "boost": 1
22            }
23          }
24        }
25      ],
26      "adjust_pure_negative": true,
27      "boost": 1
28    }
29  },
30  "sort": [
31    {
32      "timestamp": {
33        "order": "desc"
34      }
35    }
36  ]
37 }
```

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": "NTLM",
32           "workstationName": "DESKTOP-T2IA3AS",
33           "subStatus": "0xc000006a",
34           "logonProcessName": "ntlmssp",
35           "targetUserName": "Administrator",
36           "keyLength": "0",
37           "subjectUserId": "S-1-0-0",
38           "processId": "0x0",
39           "ipPort": "54890",
40           "failureReason": "332313",
41           "targetDomainName": ".",
42           "targetDomainSid": "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;
```

Trigger condition response

```
1 true
```

Preview condition response

Agent disconnected (monitoring index):

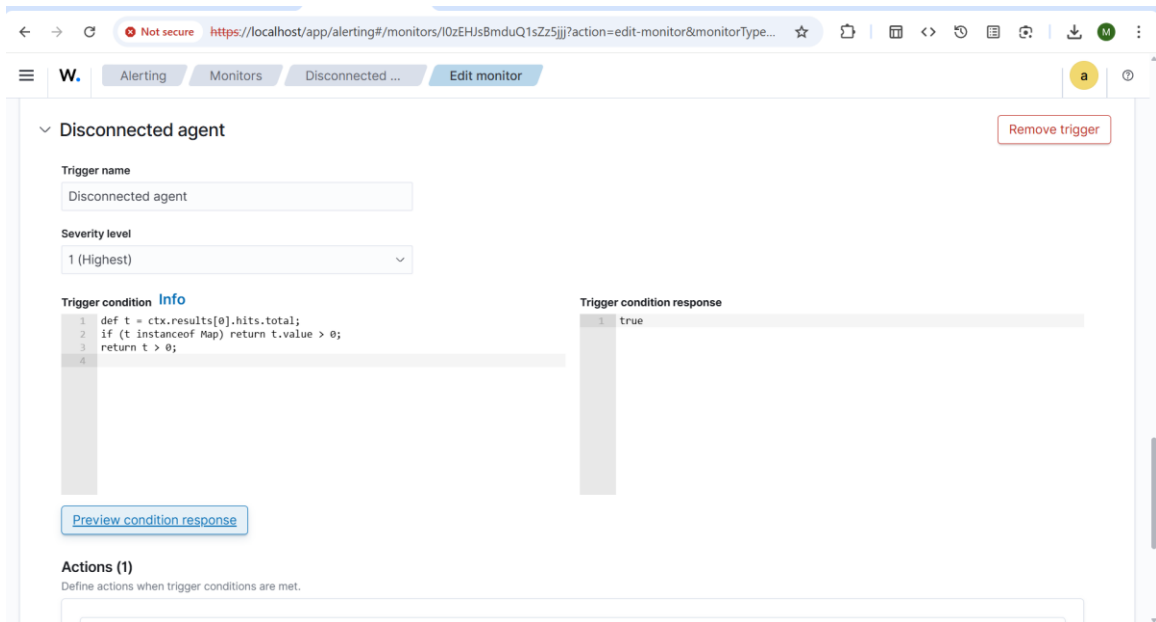
Query Run

Define extraction query

```
1 {
2   "size": 1,
3   "query": {
4     "match_all": {
5       "boost": 1
6     }
7   },
8   "sort": [
9     {
10      "timestamp": {
11        "order": "desc"
12      }
13    }
14  ]
15 }
```

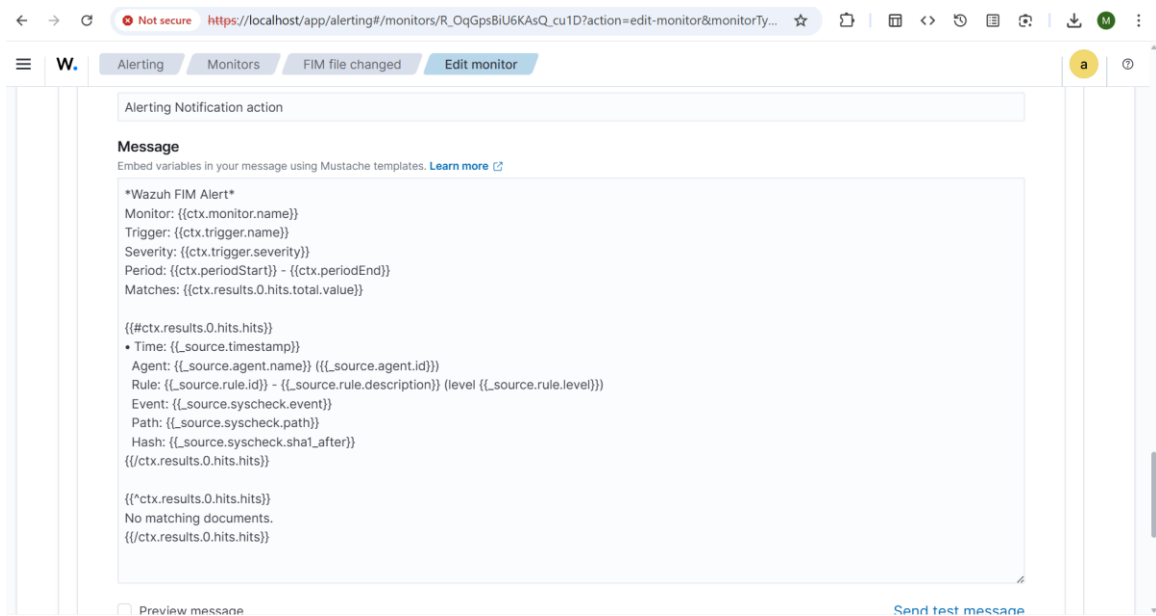
Extraction query response

```
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         "configsSum": "ab73af41699f13fdd81903b5f23d8d00",
30         "lastKeepAlive": "2025-12-14T12:12:25+00:00",
31         "ip": "127.0.0.1",
32         "node_name": "node001",
33         "group_config_status": "syncd",
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 }
```



5. Template Pesan Slack (Mustache)

FIM (syscheck):



Failed login (Wazuh rule 60122 / Windows 4625):

Agent disconnected (monitoring index):

6. Pengujian

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

```
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> |
```

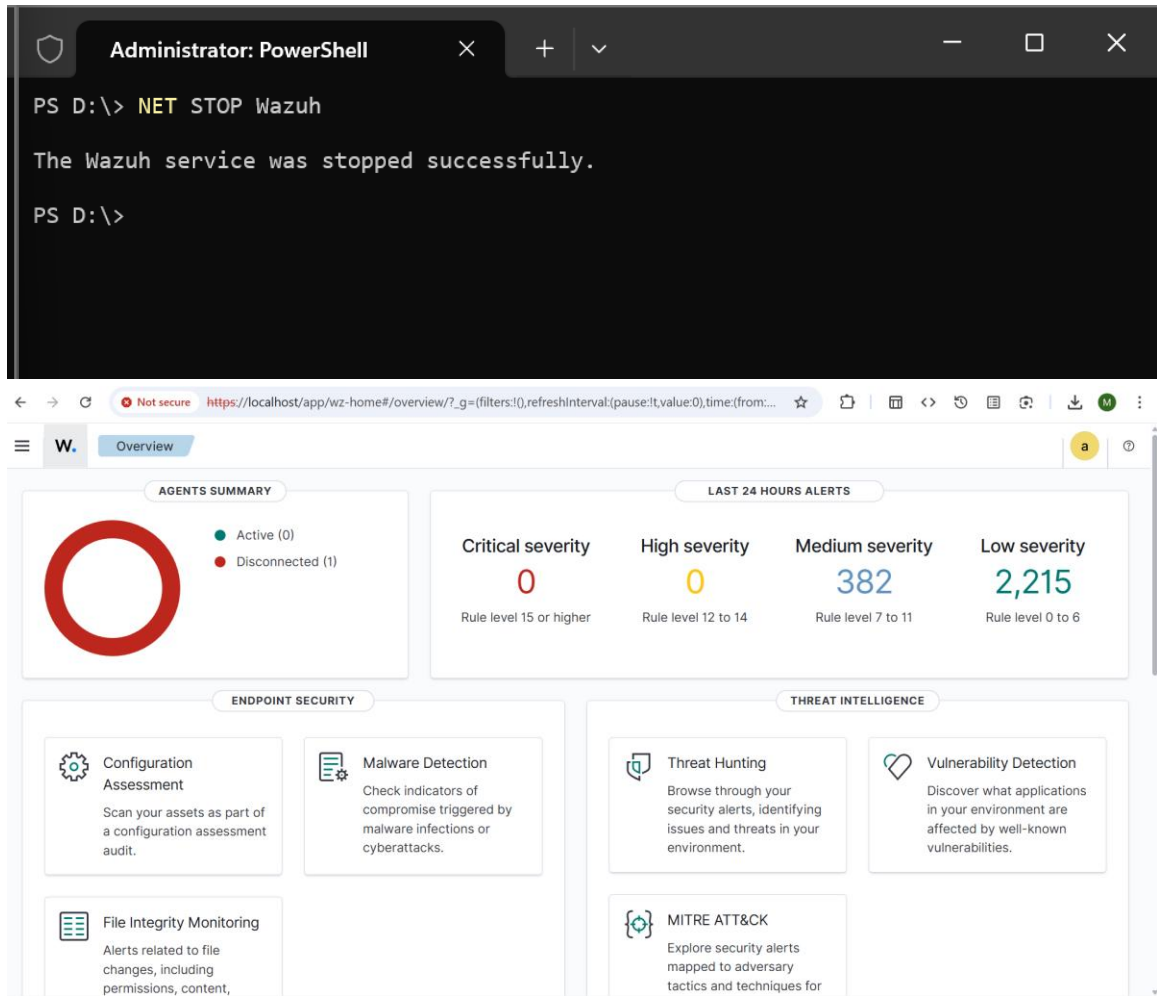
2. Failed login: memicu Windows Security Event ID 4625 misalnya. login salah via net use /runas.

```
Administrator: PowerShell
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.



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

B *I* U ~~ABC~~ | 🔗 `</>` `</>` | `</>` `</>` | `</>` `</>` | `</>` `</>`

Message #general

+ Aa 😊 @ | 📎 🎤 | 📎



☆ #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

B

I

U

🔗

🔗

🔗

🔗

🔗

</>

📄

Message #general



Aa



Failed login:

general

Invite teammates

Messages

Add canvas

Last received: 2025-12-14T14:36:03.213Z

Alerting Notification action

Today

New

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:

B I U | Link | List | Bulleted | Code | Quote

Message #general

+ Aa 😊 @ 📺 🔊 🗑️

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

B *I* U | |

Message #general

+ Aa 😊 @

