

LI SOC ANALYST

Modul Praktikum 5

Melakukan Analisis Keamanan Siber terhadap Insiden Keamanan Siber untuk Menentukan Kendali



J.62SOC00.005.1

MODUL PRAKTIKUM L1 SOC ANALYST

Unit Kompetensi

Melakukan Analisis Keamanan Siber terhadap Insiden Keamanan Siber untuk Menentukan Kendali

Tujuan Praktikum

1. Membuat *Risk Register*
2. Mengoperasikan OWASP Risk Rating Calculator

Membedakan Log Event dan Log Insiden (P.5.1.A)

Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Dalam menjalankan tugas ini, Anda harus memiliki kemampuan untuk menganalisis dan membedakan antara aktivitas biasa dan insiden keamanan yang memerlukan penanganan lebih lanjut. Kemampuan ini penting agar tidak terjadi kesalahan dalam menanggapi *alert* dan agar sumber daya yang tersedia dapat digunakan secara efisien untuk merespons ancaman yang nyata.

Pada tanggal 10 April 2025, diduga telah terjadi insiden dengan aset yang berdampak pada layanan SPPD Kabupaten Lengkeng. Anda diminta oleh pimpinan untuk mencari tahu aktivitas yang terjadi pada layanan SPPD dan menentukan aktivitas yang termasuk dalam aktivitas biasa dan termasuk dalam aktivitas insiden menggunakan Wazuh SIEM.

Tujuan Praktikum

Praktikum ini bertujuan untuk membantu peserta didik dalam mengidentifikasi aktivitas insiden pada *alert* platform SIEM.

Environment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM Wazuh
- VM Desktop yang dapat mengakses *browser*
- VM Wazuh dan VM Desktop saling terkoneksi

Durasi Praktikum

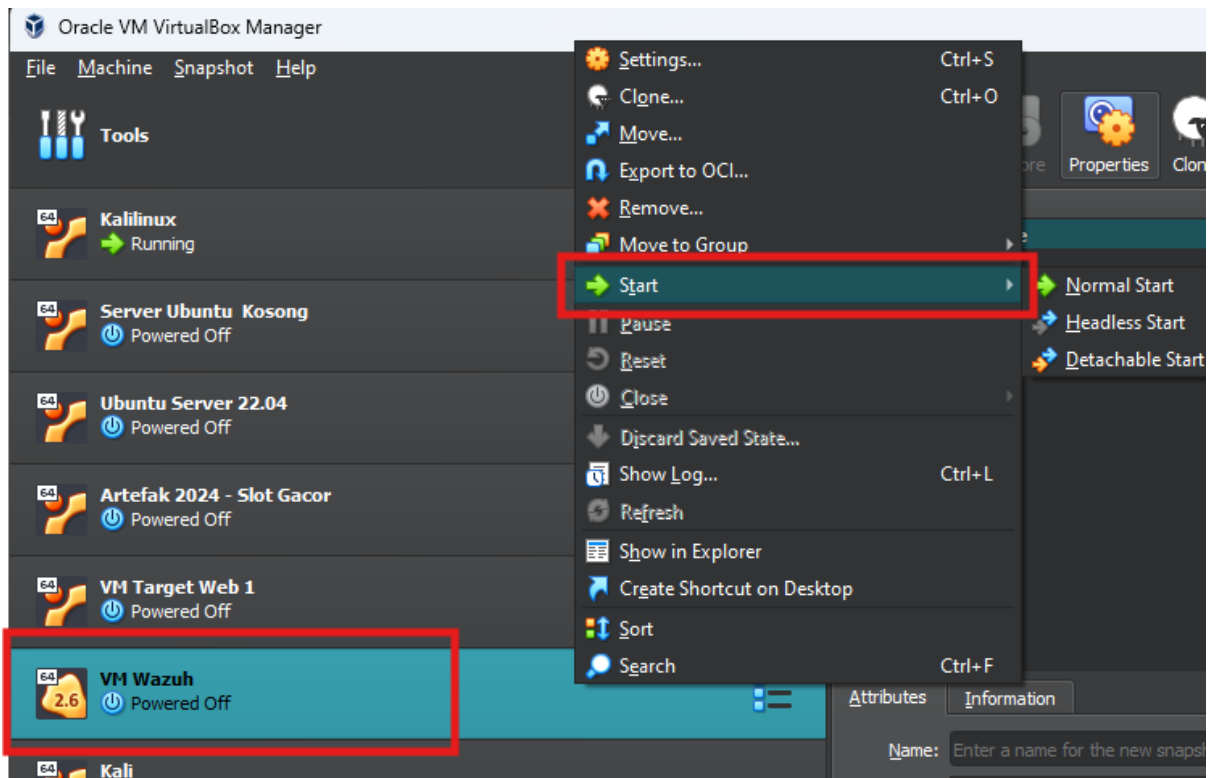
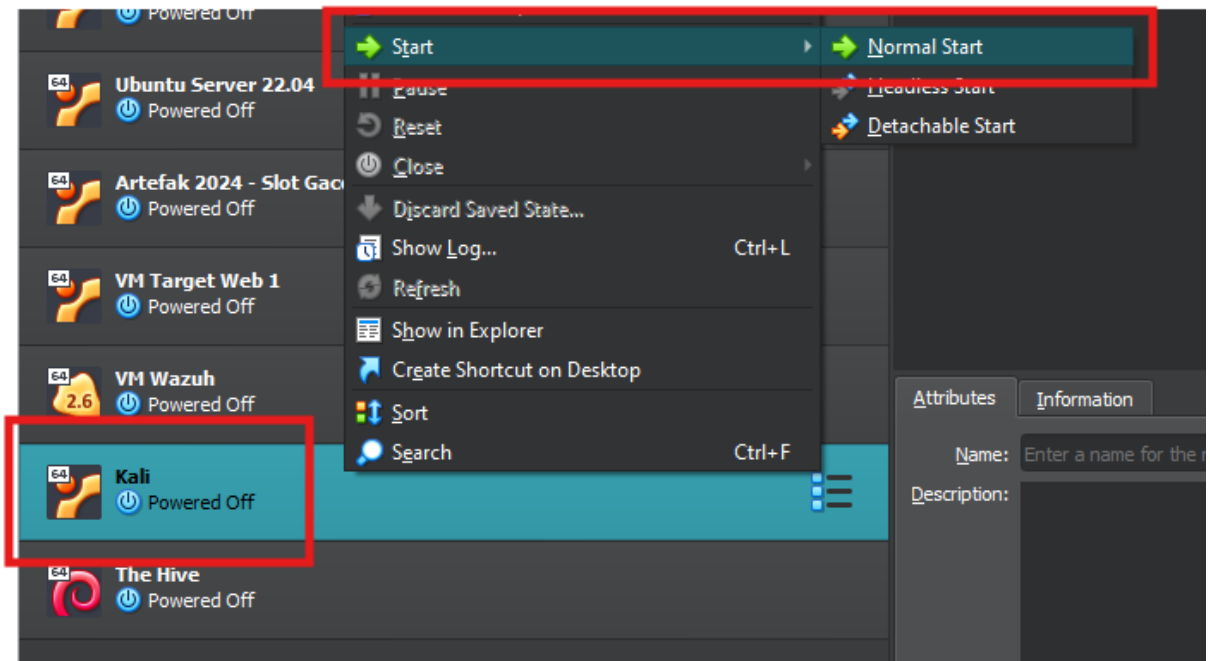
15 Menit

Catatan Khusus

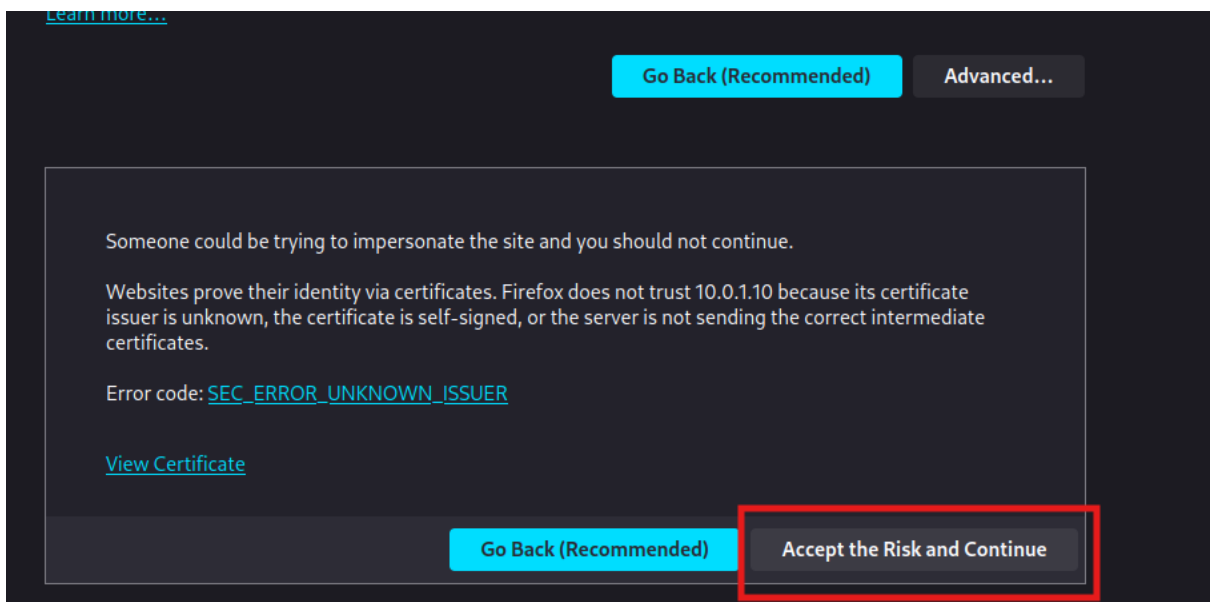
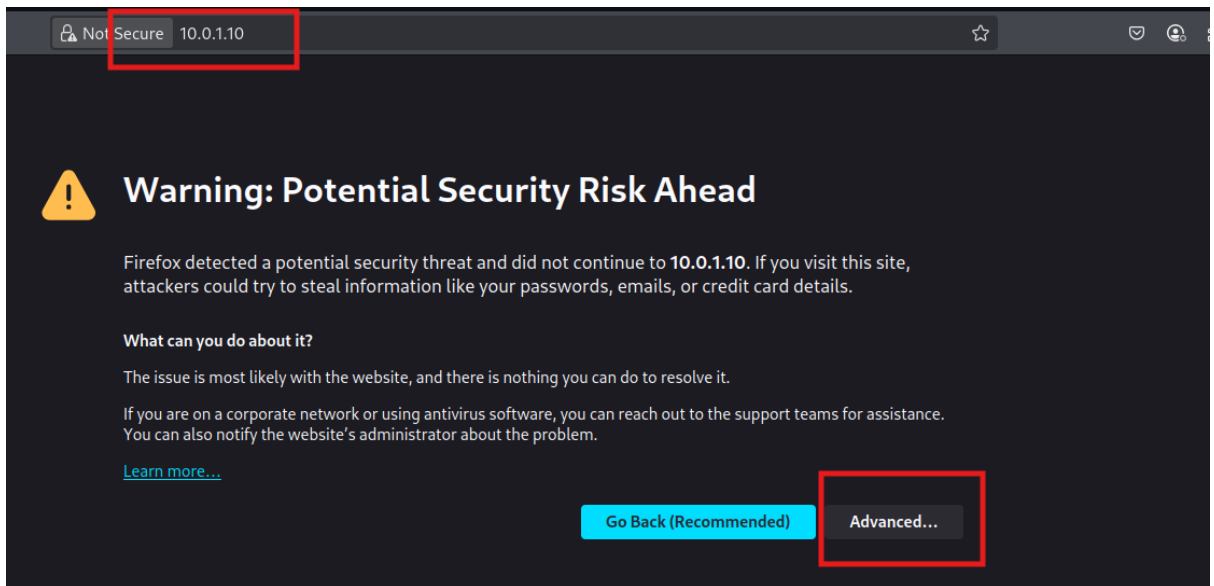
- Siapkan *environment* laboratorium virtual sesuai panduan instalasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

Langkah-Langkah

1. Siapkan Virtualbox, nyalakan VM Wazuh dan VM Desktop yang dapat mengakses *browser*, pada contoh kali ini menggunakan desktop Kali Linux



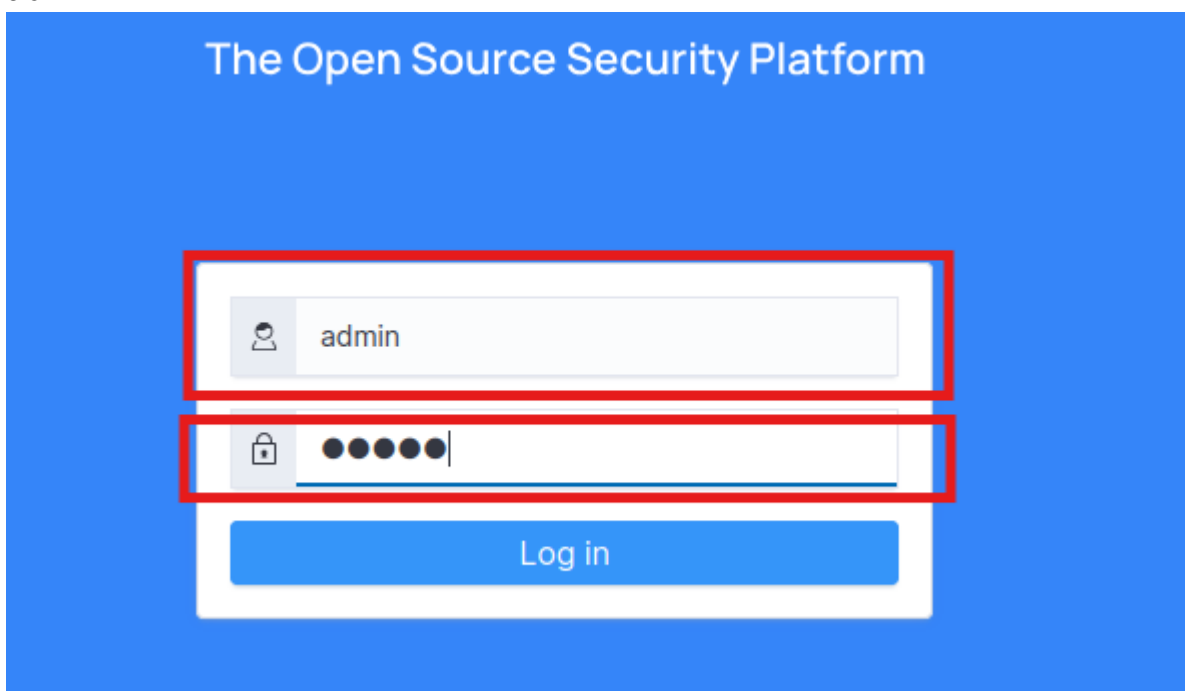
2. Buka browser pada VM Dekstop, masukan IP VM Wazuh



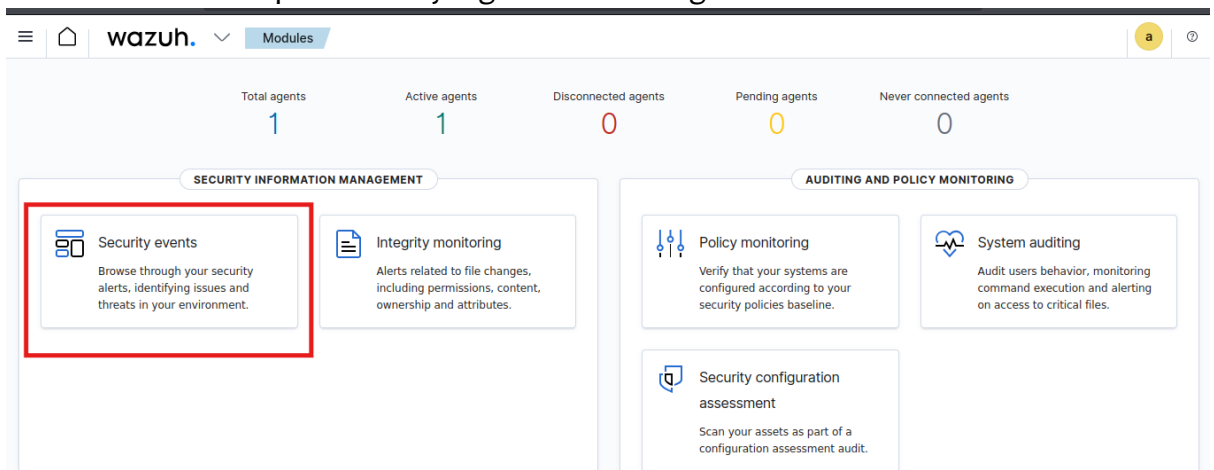
3. Jika tidak mengetahui IP VM Wazuh, dapat dilakukan dengan *login* ke VM Wazuh dengan kredensial *username* `wazuh-user` dan *password* `wazuh`. Cek ip VM dengan IP A atau `ifconfig`. Pastikan VM Dekstop yang anda gunakan dapat terkoneksi dengan IP VM Wazuh.

```
[wazuh-user@wazuh-server ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:fa:c1:2b brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.10/24 brd 10.0.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fefa:c12b/64 scope link
        valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

4. Login Wazuh Dashboard dengan kredensial *username* admin dan *password* admin



5. Tampilan Wazuh Dashboard akan seperti gambar dibawah ini, klik bagian *security event* untuk menampilkan *alert* yang berkaitan dengan event



- Wazuh akan menampilkan grafik terkait aktivitas yang ada pada perangkat yang telah dipasang Wazuh Agent

The screenshot shows the Wazuh dashboard with the following agent status:

- Total agents: 1
- Active agents: 1
- Disconnected agents: 0
- Pending agents: 0
- Never connected agents: 0

Under the 'SECURITY INFORMATION MANAGEMENT' section, the 'Security events' module is highlighted with a red box. Its description is: 'Browse through your security alerts, identifying issues and threats in your environment.'

Other modules visible include Integrity monitoring, Policy monitoring, System auditing, and Security configuration assessment.

- Scroll kebawah untuk melihat *alert* aktivitas yang terjadi

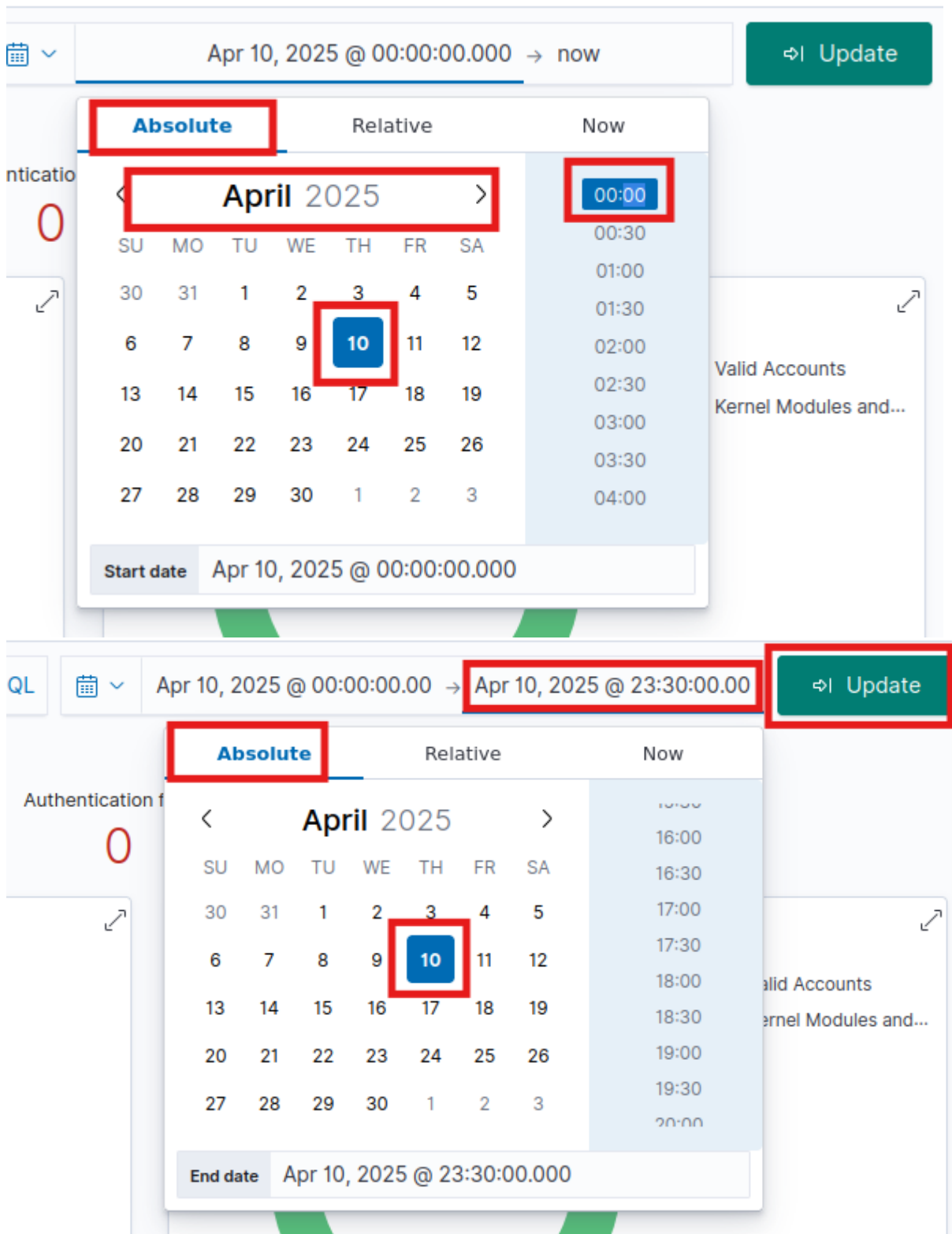
Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Apr 10, 2025 @ 13:37:41.410	001	WebServerSPPD			Listened ports status (netstat) changed (new port opened or closed).	7	533
> Apr 10, 2025 @ 13:31:51.068	001	WebServerSPPD			Host-based anomaly detection event (rootcheck).	7	510
> Apr 10, 2025 @ 13:31:51.067	001	WebServerSPPD			Host-based anomaly detection event (rootcheck).	7	510
> Apr 10, 2025 @ 13:31:51.067	001	WebServerSPPD			Host-based anomaly detection event (rootcheck).	7	510
> Apr 10, 2025 @ 13:31:51.067	001	WebServerSPPD			Host-based anomaly detection event (rootcheck).	7	510
> Apr 10, 2025 @ 13:31:51.024	001	WebServerSPPD			Host-based anomaly detection event (rootcheck).	7	510
> Apr 10, 2025 @ 13:31:40.726	001	WebServerSPPD			Host-based anomaly detection event (rootcheck).	7	510
> Apr 10, 2025 @ 13:31:40.371	001	WebServerSPPD			Host-based anomaly detection event (rootcheck).	7	510
> Apr 10, 2025 @ 13:31:40.362	001	WebServerSPPD			Listened ports status (netstat) changed (new port opened or closed).	7	533
> Apr 10, 2025 @ 13:31:35.912	001	WebServerSPPD			Wazuh agent started.	3	503

- Ubah tanggal agar hanya menampilkan *alert* pada kurun waktu tertentu dengan klik pada kolom *last 24 hours>absolute>tanggal yang diinginkan>jam yang diinginkan* dan lanjutkan dengan mengubah batas akhir *alert* yang ditampilkan dengan cara yang sama. Dikarenakan skenario praktikum yang dilakukan menyebut tanggal 10 April 2025 sesuaikan tanggalnya. Klik *update* jika telah disesuaikan.

The screenshot shows the 'Security events' dashboard. The date filter 'Last 24 hours' is highlighted with a red box. The dashboard displays the following summary:

- Total: 31
- Level 12 or above alerts: 0
- Authentication failure: 0
- Authentication success: 3

There are two charts: 'Alert level evolution' (a bar chart) and 'Top MITRE ATT&CKs' (a donut chart showing 'Valid Accounts' and 'Kernel Modules and...').



9. Untuk memantau *alert* yang terjadi pada Wazuh Agent tertentu dapat menggunakan *filtering*. Tekan *add filter*

Dashboard Events

Search [manager.name: wazuh-server] + Add filter

Total: 34 Level 12 or above alerts: 0 Authentication failure: 0

Alert level evolution

Pilih field agent.name

wazuh. Modules Security events

Dashboard Events

Search [manager.name: wazuh-server]

agent.name

Operator: Select

Cancel Save

manager.name: wazuh-server + Add filter

EDIT FILTER

Field: agent.name

Operator: is

is is not is one of is not one of exists does not exist

Alert level evolution

Count

Masukan nama agent yang hendak dicek alert-nya lalu tekan save

Dashboard Events

manager.name: wazuh-server + Add filter

EDIT FILTER Edit as Query DSL

Field: agent.name Operator: is

Value: **WebServerSPPD**

Cancel Save

Alert level evolution

Dashboard Events

manager.name: wazuh-server + Add filter

EDIT FILTER Edit as Query DSL

Field: agent.name Operator: is

Value: Select a value

Create custom label?

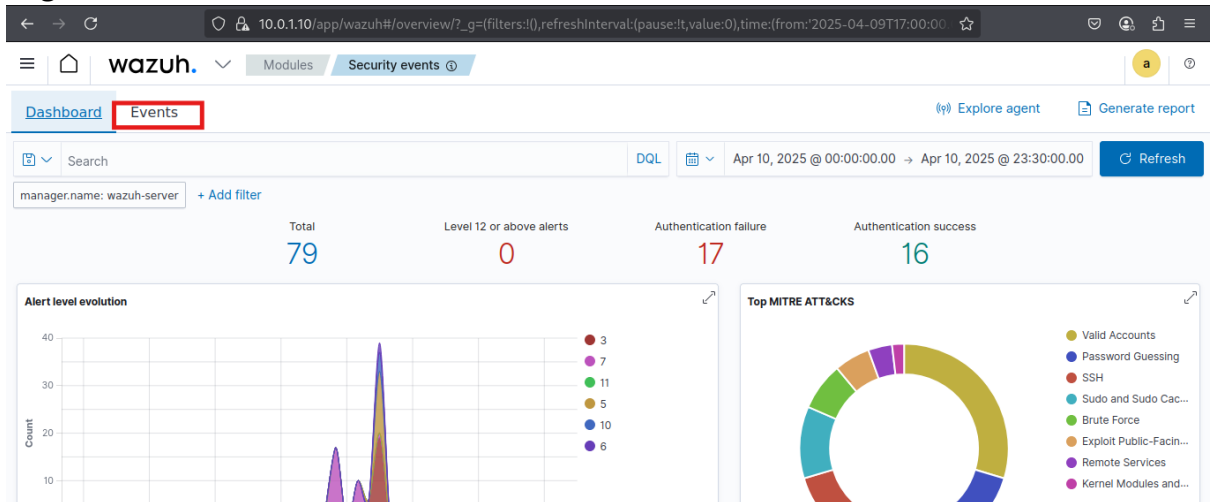
Cancel **Save**

Alert level evolution

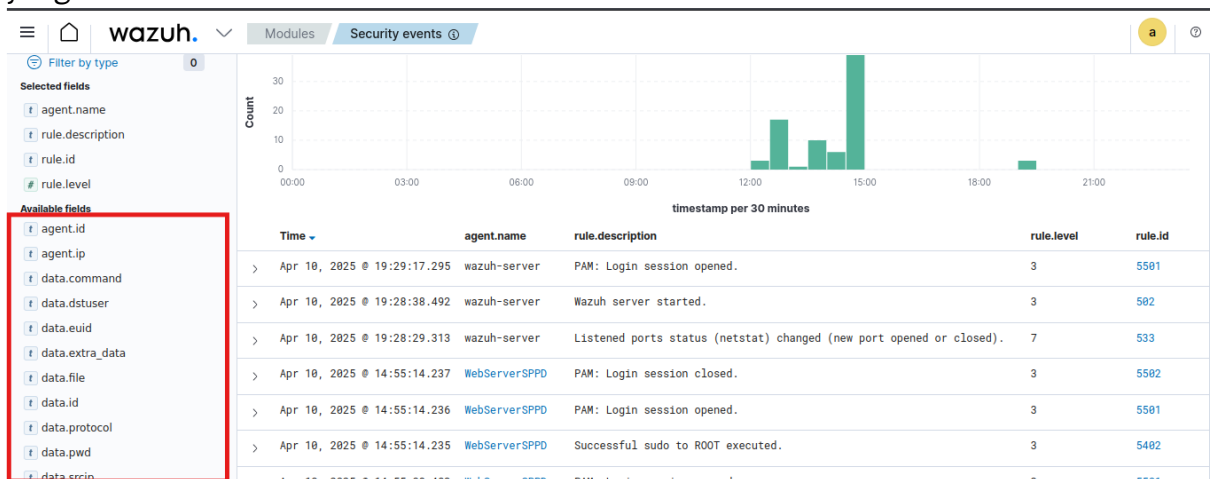
10. Tentukan *alert* yang merupakan aktivitas normal dan *alert* insiden

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Apr 10, 2025 @ 14:33:06.887	001	WebServerSPPD			PAM: Login session closed.	3	5502
> Apr 10, 2025 @ 14:29:18.593	001	WebServerSPPD	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
> Apr 10, 2025 @ 14:29:18.547	001	WebServerSPPD	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
> Apr 10, 2025 @ 14:29:10.564	001	WebServerSPPD	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	PAM: Login session opened.	3	5501
> Apr 10, 2025 @ 14:29:10.517	001	WebServerSPPD	T1078 T1021	Defense Evasion, Persistence, Privilege Escalation, Initial Access	sshd: authentication success.	3	5715

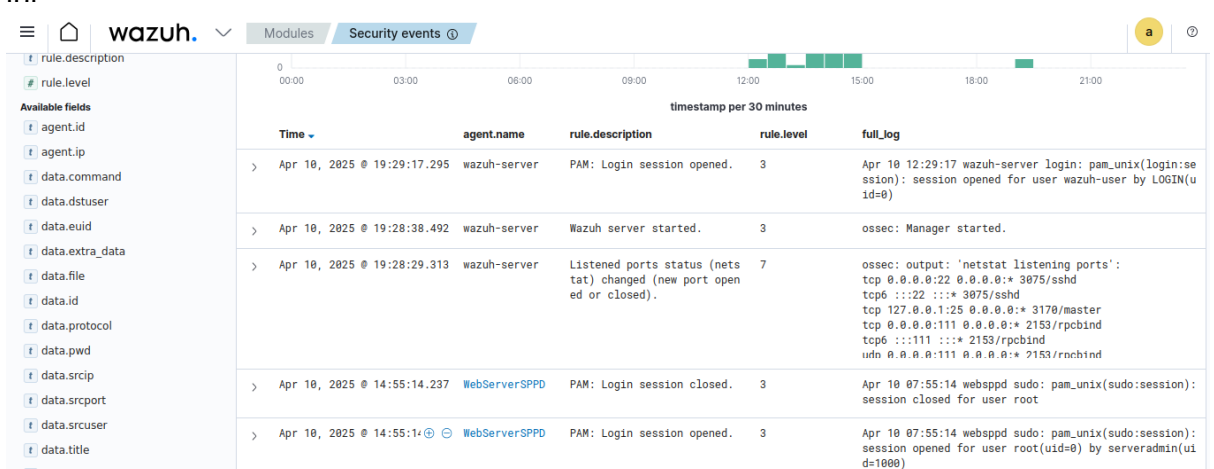
11. Jika hendak melakukan eksplorasi lebih lanjut pada *alert*. Tekan tab events pada bagian atas



12. Setelah membuka event anda dapat melihat aktivitas yang ada lebih komprehensif, untuk menambahkan data pada tampilan, tambahkan parameter yang lain.



13. Tampilan jika ditambahkan full log dan menghapus rule level akan menjadi seperti ini



14. Amati pada *rule.description* dan *full.log* untuk mengidentifikasi event dan insiden.

Membuat Risk Register dari Aset Yang Diketahui dan Mengoperasikan OWASP Risk Calculator (P.5.1.B, P.5.1.C)

Skenario Praktikum

Anda adalah seorang *L1 SOC Analyst* yang bekerja di Pemerintah Daerah Kabupaten Lengkeng. Anda memiliki tugas untuk mengawasi dan memantau seluruh aktivitas jaringan ke dalam infrastruktur TI Pemkab Lengkeng dengan bantuan SIEM. Dalam menjalankan tugas ini, Anda harus memiliki kemampuan untuk mendeteksi insiden yang terjadi. Untuk mendukung tugas anda, anda harus mengenal mengenai aset yang anda pantau dan resiko yang dimilikinya

Layanan Web SPPD Pemerintah Daerah Kabupaten Lengkeng belum dilakukan pendataan resiko yang dimiliki. Layanan web tersebut ditempatkan pada VM Target Web 1. Beberapa resiko terhadap aset yang telah diketahui diantaranya pencurian kredensial pengguna, *SQL Injection*, *XSS* dan pengunggahan file berbahaya. Semua resiko yang disebutkan dianggap belum memiliki kontrol sama sekali. Anda sebagai seorang *L1 SOC Analyst* diharuskan memahami resiko yang dimiliki aset yang ada pantau.

Tujuan Praktikum

Praktikum ini bertujuan untuk membantu peserta didik dalam mengidentifikasi resiko, mengoperasikan OWASP Risk Calculator dan

Environment Laboratorium Virtual

Praktikum ini membutuhkan:

- Browser dengan koneksi internet
- Aplikasi *word processor*
- Tabel Risk Register (sudah disiapkan)

Durasi Praktikum

30 Menit

Catatan Khusus

- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan
- Jawaban bersifat subjektif, pastikan anda memiliki argumen yang jelas dalam membuat *risk register*

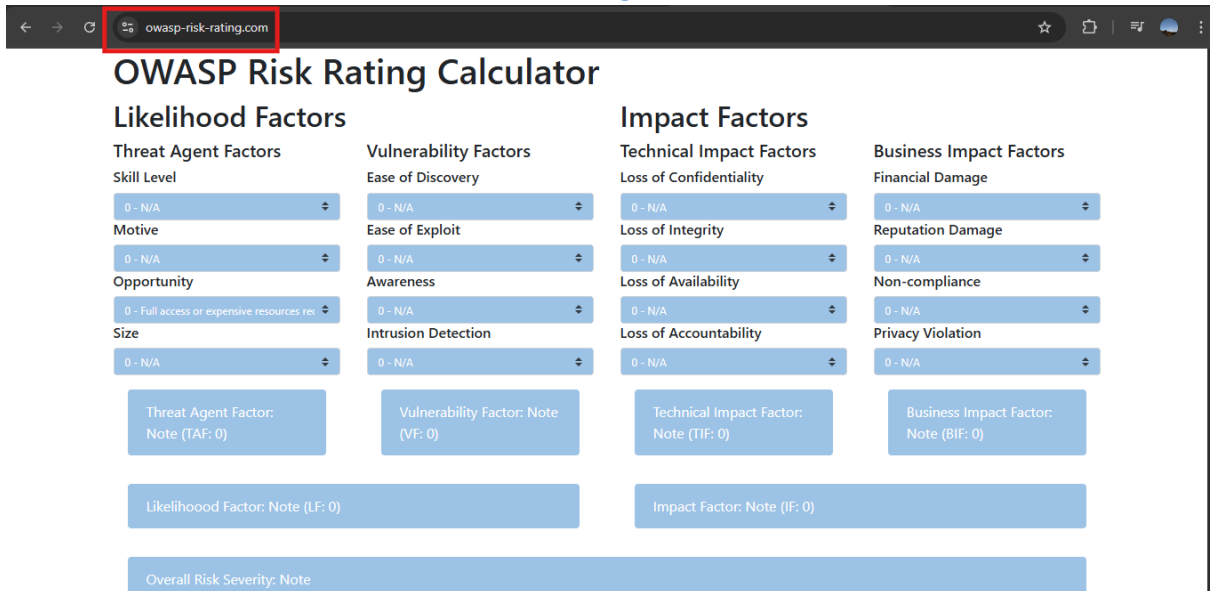
Langkah-Langkah

1. Unduh file contoh *risk register* pada *platform*, buka pada aplikasi *word processor* yang anda miliki

LEMBAR BANTU PRAKTIKUM L1 SOC ANALYST: RISK REGISTER

NO.	Daftar Aset	Deskripsi Resiko			CURRENT ACTIONS/CONTROLS TO MANAGE THE RISK				RISK TREATMENT	RISK MITIGATION	Penanggung Jawab
		LOSS EVENTS		Dampak	RISK						
	Nama Aset	Kerentanan (Vulnerability)	Ancaman (Threat)	Uraian Dampak	Kendali yang ada	Likelihood	Impact	Nilai Risiko	Mitigasi / Terima / Transfer / Hindari	Rekomendasi & Pendaanialan Baru	PIC
1	Web SPPD Kabupaten Lengkeng	Perusakan Kredensial Pengguna									
2	Web SPPD Kabupaten Lengkeng	SQL Injection									
3	Web SPPD Kabupaten Lengkeng	XSS									
4	Web SPPD Kabupaten Lengkeng	Penggunaan File Berbahaya									

- Isi kolom ancaman dan uraian dampak yang berhubungan dengan kerentanan, isi sedetail mungkin dengan dasar yang jelas. Ancaman dapat berbentuk orang, sistem, kejadian, atau tindakan yang bisa menyebabkan kerugian sedangkan dampak dapat berupa konsekuensi negatif yang timbul jika kerentanan berhasil dieksploitasi oleh ancaman.
- Pada kolom kendali yang ada dapat diisi tidak ada dikarenakan diasumsikan dalam skenario belum terdapat kendali apapun
- Untuk mengisi kolom *likelihood*, *impact* dan nilai resiko dapat menggunakan OWASP Risk Calculator. Buka browser pada dekstop anda dan buka OWASP Risk Calculator pada <https://www.owasp-risk-rating.com/>



- Klik pada bagian panah atas bawah, dan pilih sesuai level yang anda rasa tepat. Pastikan anda memiliki argumen yang kuat dan berdasar mengapa anda memilih level tersebut

OWASP Risk Rating Calculator

Likelihood Factors

How technically skilled is this group of threat agents?

0 - N/A

0 - N/A

1 - Security penetration skills

2

3 - Network and programming skills

4

5 - Advanced computer user

6 - Some technical skills

7

8

9 - No technical skills

Vulnerability Factors

Ease of Discovery

0 - N/A

Ease of Exploit

0 - N/A

Awareness

0 - N/A

Intrusion Detection

0 - N/A

Vulnerability Factor: Note (VF: 0)

Impact Factors

Technical Impact Factors

Loss of Confidentiality

0 - N/A

Loss of Integrity

0 - N/A

Loss of Availability

0 - N/A

Loss of Accountability

0 - N/A

Technical Impact Factor: Note (TIF: 0)

Business Impact Factors

Financial Damage

0 - N/A

Reputation Damage

0 - N/A

Non-compliance

0 - N/A

Privacy Violation

0 - N/A

Business Impact Factor: Note (BIF: 0)

Likelihood Factor: Note (LF: 0)

Impact Factor: Note (IF: 0)

Overall Risk Severity: Note

- Detail pada setiap poin dapat dilihat pada Materi Pembelajaran L1 SOC Analyst Unit Kompetensi Melakukan Analisis Keamanan Siber terhadap Insiden Keamanan Siber untuk Menentukan Kendali. Lakukan pengisian pada kolom *likelihood*, *impact* dan nilai resiko sesuai dengan apa yang anda hitung dari OWASP Risk Calculator
- Kolom *Risk Treatment* diisi dengan bagaimana organisasi akan menangani risiko yang sudah dinilai. Terdapat empat pilihan sebagai berikut

Penanganan	Penjelasan
Mitigasi	Mengurangi kemungkinan atau dampak risiko dengan tindakan teknis
Terima	Menerima risiko apa adanya karena dianggap risiko kecil atau biaya mitigasinya tidak sebanding
Transfer	Memindahkan risiko ke pihak lain, biasanya melalui asuransi atau kontrak pihak ketiga.
Hindari	Menghapus seluruh aktivitas yang menyebabkan risiko tersebut

- Kolom rekomendasi diisi dengan saran tindakan konkrit untuk menangani risiko dan mengontrol resiko.
- Kolom PIC diisi dengan organisasi atau entitas yang bertanggung jawab atas resiko tersebut.