L1 SOC ANALYST

Modul Praktikum 3

Memberikan Tiket terhadap Insiden Keamanan Siber

J.62SOC00.010.1

MODUL PRAKTIKUM L1 SOC ANALYST

Unit Kompetensi

Memberikan Tiket Terhadap Insiden Keamanan Siber

Tujuan Praktikum

Membuat Ticket Pada TheHive Dengan Parameter yang Tepat

Membuat Ticket Pada TheHive Dengan Parameter yang Tepat (P.10.1.A)

Skenario Praktikum I

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. Tepat pukul 10:42 WIB, hari ini anda sebagai L1 SOC Analyst melihat banyak sekali notifikasi muncul dari Wazuh "SQL Injection Attempt"

Sebagai L1 SOC Analyst anda segera menelusuri alert tersebut. Ia membuka log akses dari server aplikasi internal yang beralamat di 10.0.1.11 Aplikasi ini merupakan layanan SPPD dari kabupaten lengkeng. Rafi menyadari bahwa ini adalah percobaan SQL Injection klasik teknik ' OR 1=1-- yang bertujuan membypass login tanpa kredensial valid. Lebih lanjut, jumlah notifikasi yang muncul sangat masih dalam waktu yang singkat mengindikasikan bahwa serangan berasa dari tools otomatis. Beberapa alert menujukan bahwa terdapat satu serangan yang mendapatkan response 200 yaitu dengan payload IP asal serangan tercatat sebagai 10.0.1.97, Anda segera membuat laporan insiden dan membuka tiket di TheHive.

Tujuan Praktikum

Praktikum ini bertujuan untuk membantu perserta didik dalam membuat tiket insiden keamanan siber dengan tepat

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM The Hive
- VM dengan browser dan akses ke TheHive

Durasi Praktikum

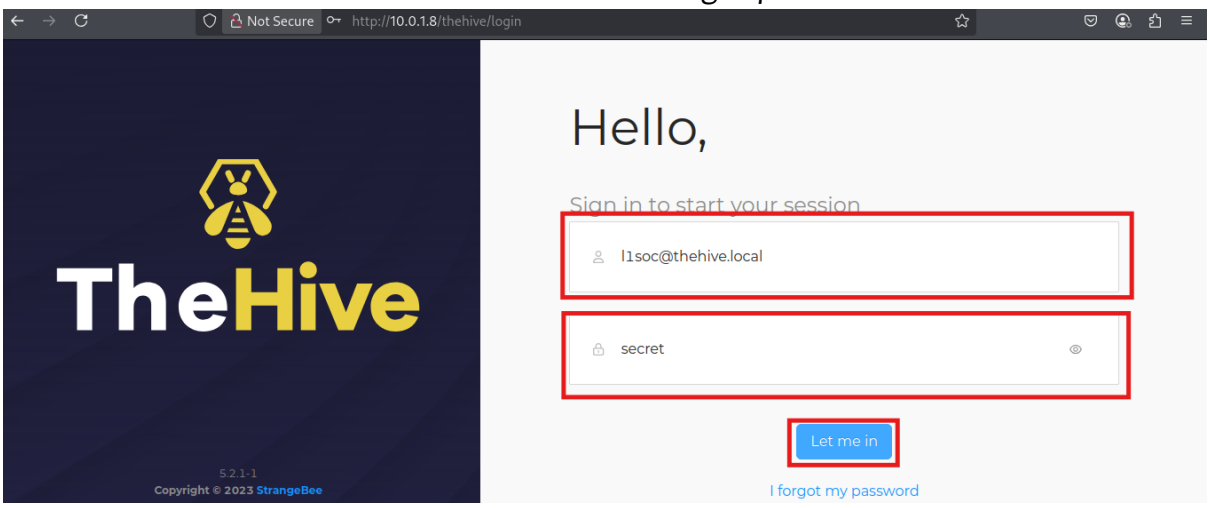
15 Menit

Catatan Khusus

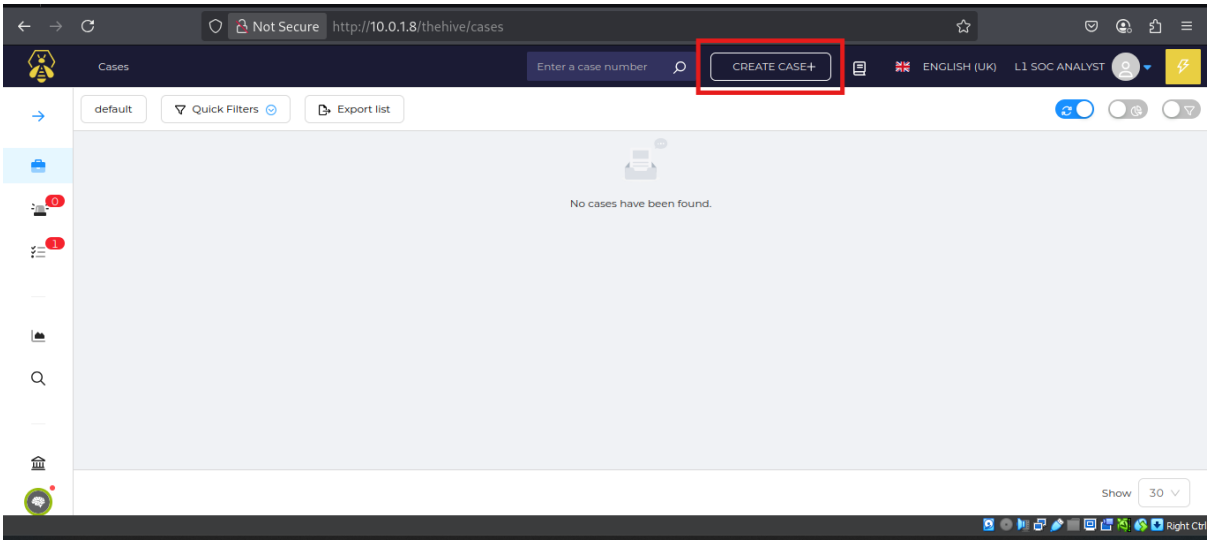
- Siapkan *enviroment* laboratorium virtual sesuai panduan installasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

Langkah-Langkah

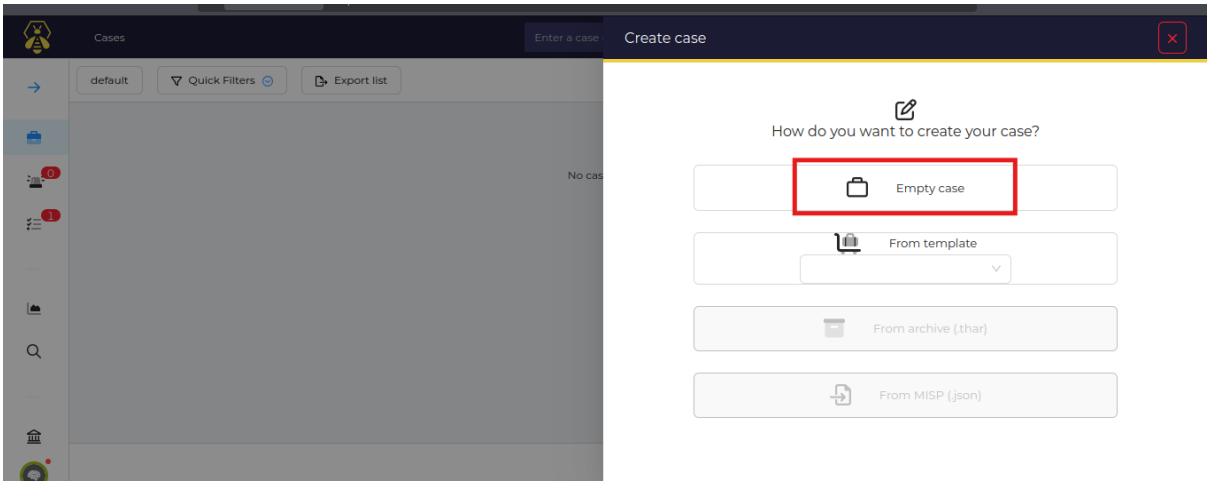
1. Siapkan Virtualbox dan nyalakan VM TheHive, buka melalui browser http://10.0.1.8/thehive/login. Sesuaikan IP jika tidak anda telah mengubah ip.
2. Masukan kredensial `l1soc@thehive.local` dengan *password* `secret`.



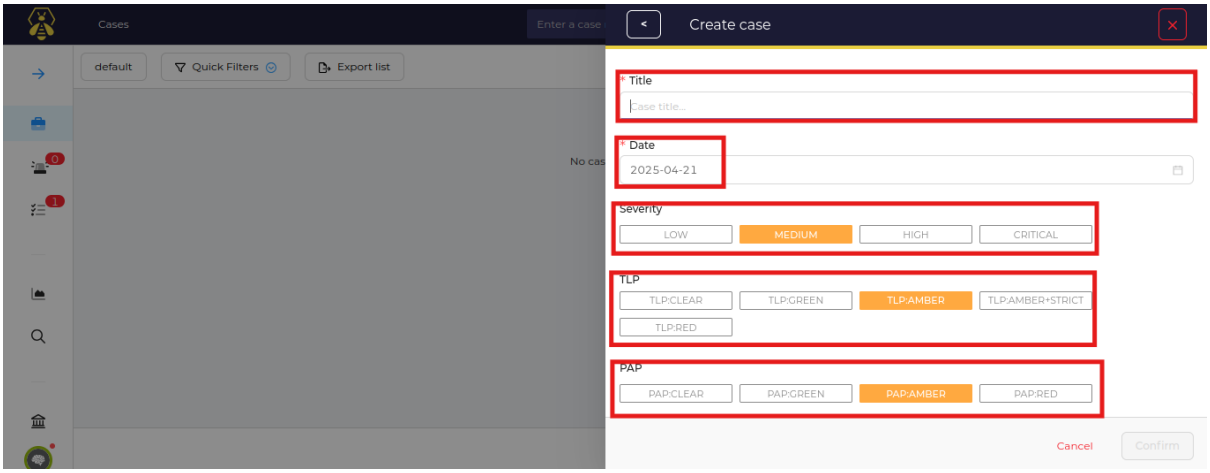
3. Tekan `CREATE CASE` untuk membuka tiket baru.



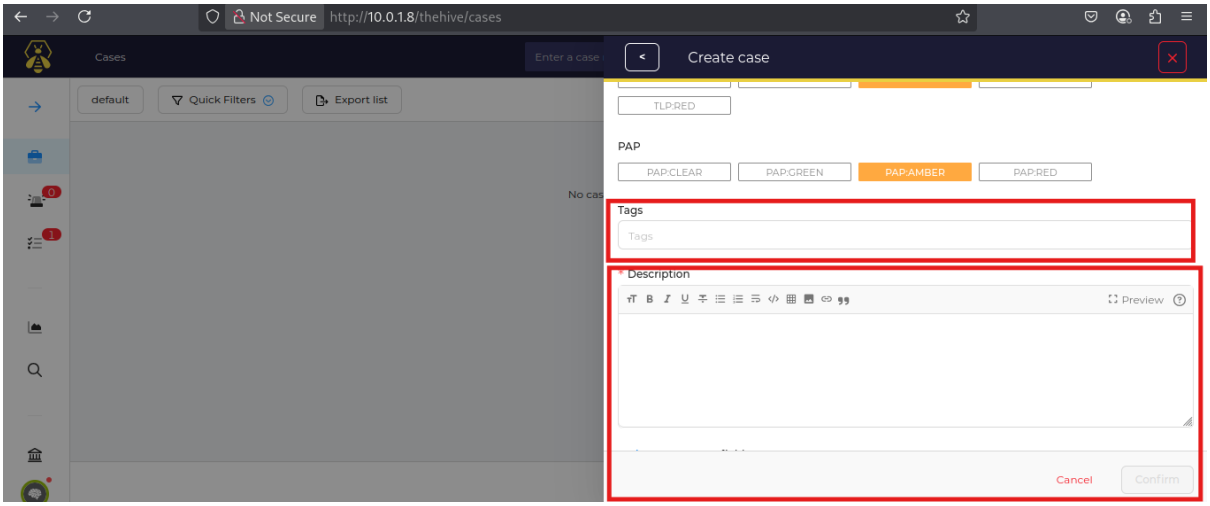
4. Pilih `Empty Case` untuk membuat tiket dari awal



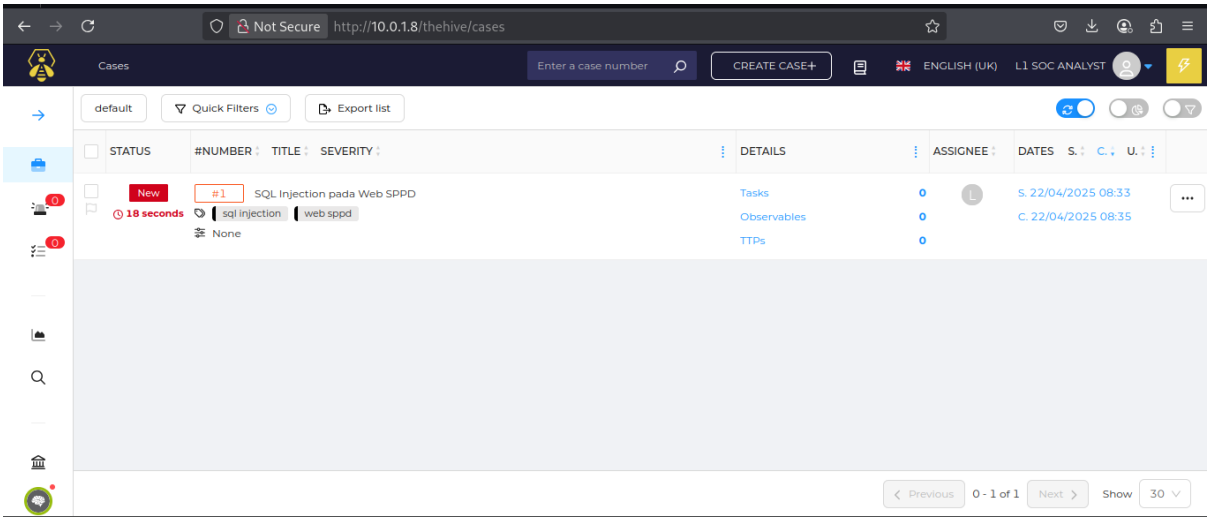
5. `Title` (judul) ditulis lengkap, tidak boleh disingkat ataupun akronim dan harus membuat nama *stakeholder*. Tanggal diisi waktu insiden terjadi. TLP diisikan dengan batas penyeberan informasi sensitif. PAP diisikan dengan aksi yang boleh dilakukan terhadap informasi.



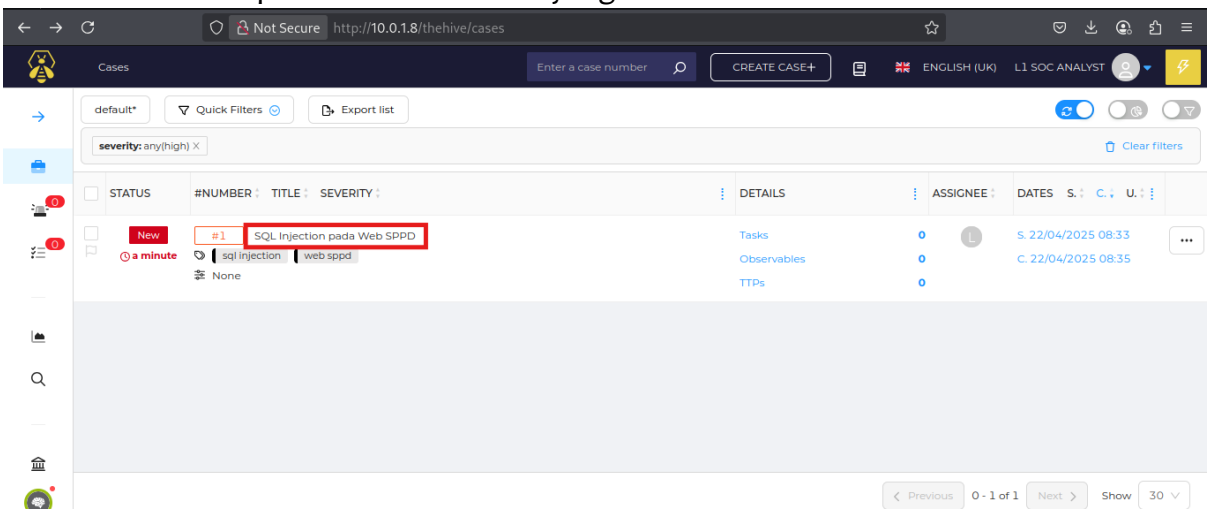
6. `Tags` diisi Penulisan sensor, nama sistem, nama *stakeholder*, kerentanan, jenis laporan. Deskripsi haruslah memuat 5W+1H.



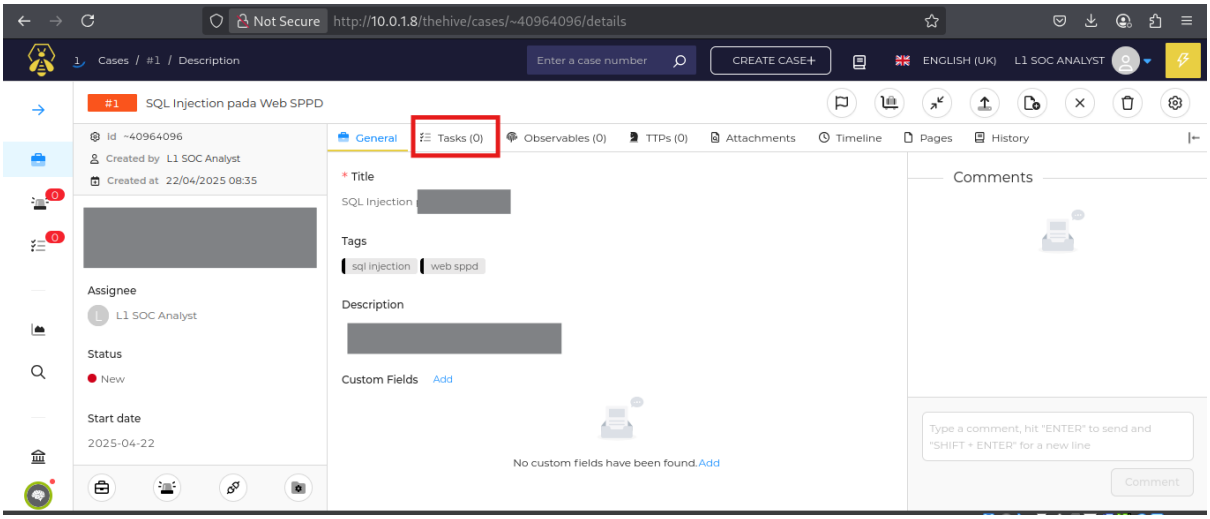
7. Hasil pembuatan tiket akan muncul pada halaman tiket.

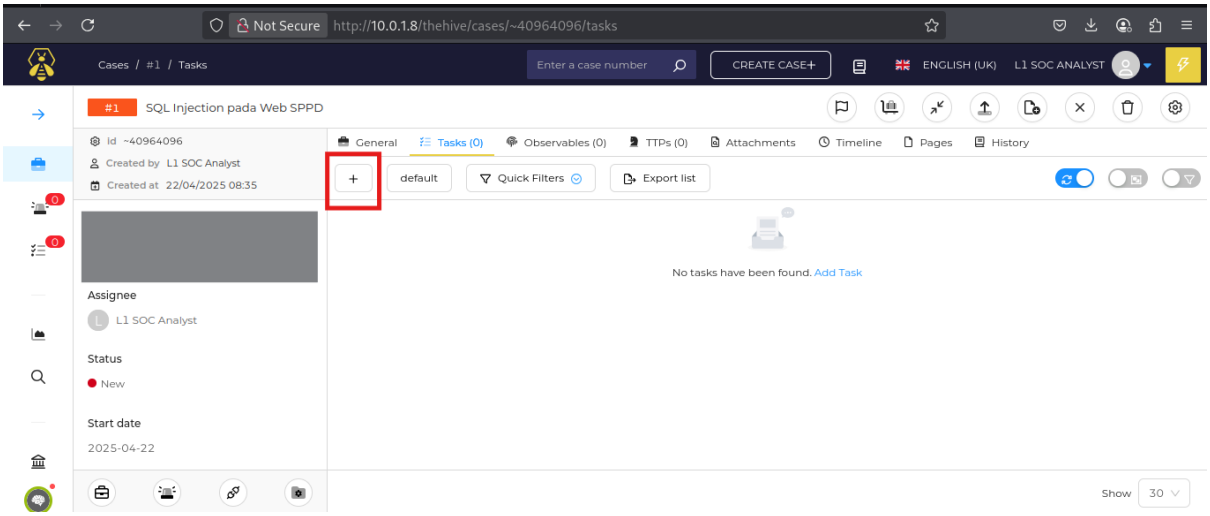


8. Selanjutnya untuk memberi tugas kepada *analyst* lain dapat dilakukan dengan memberikan tasks pada tiket. Buka tiket yang hendak diberikan tasks.

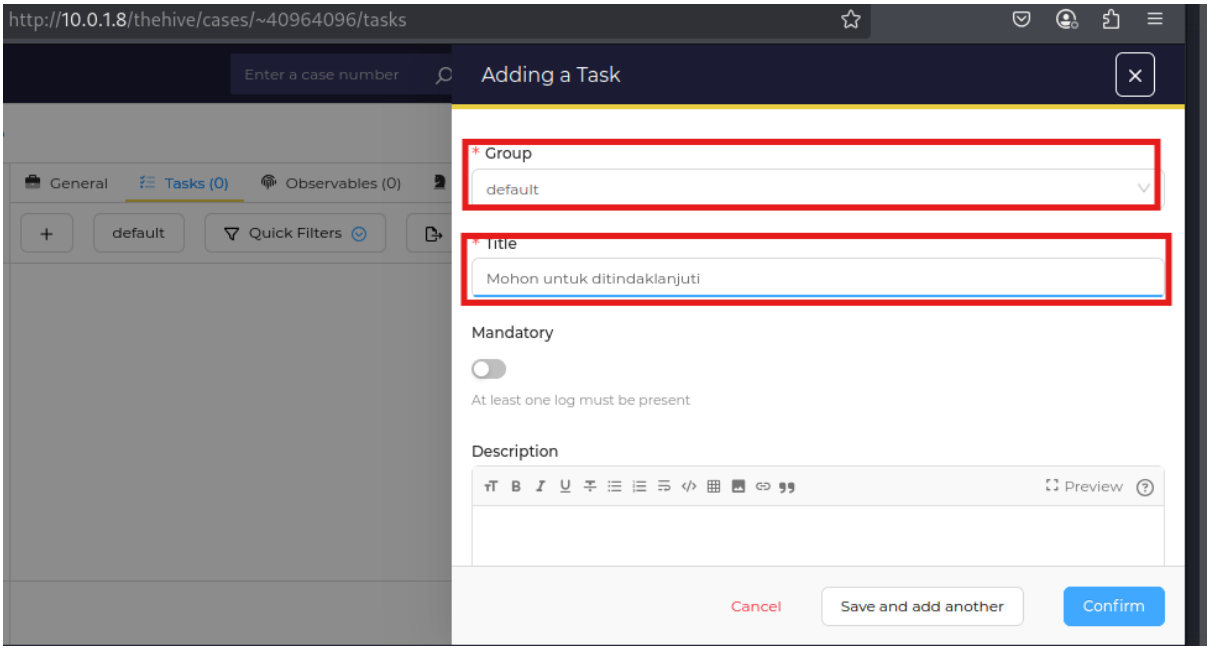


9. Tekan bagian `tasks` lalu akan muncul halaman kosong jika belum pernah ditambahkan task sebelumnya. Lalu tekan simbol tambah.

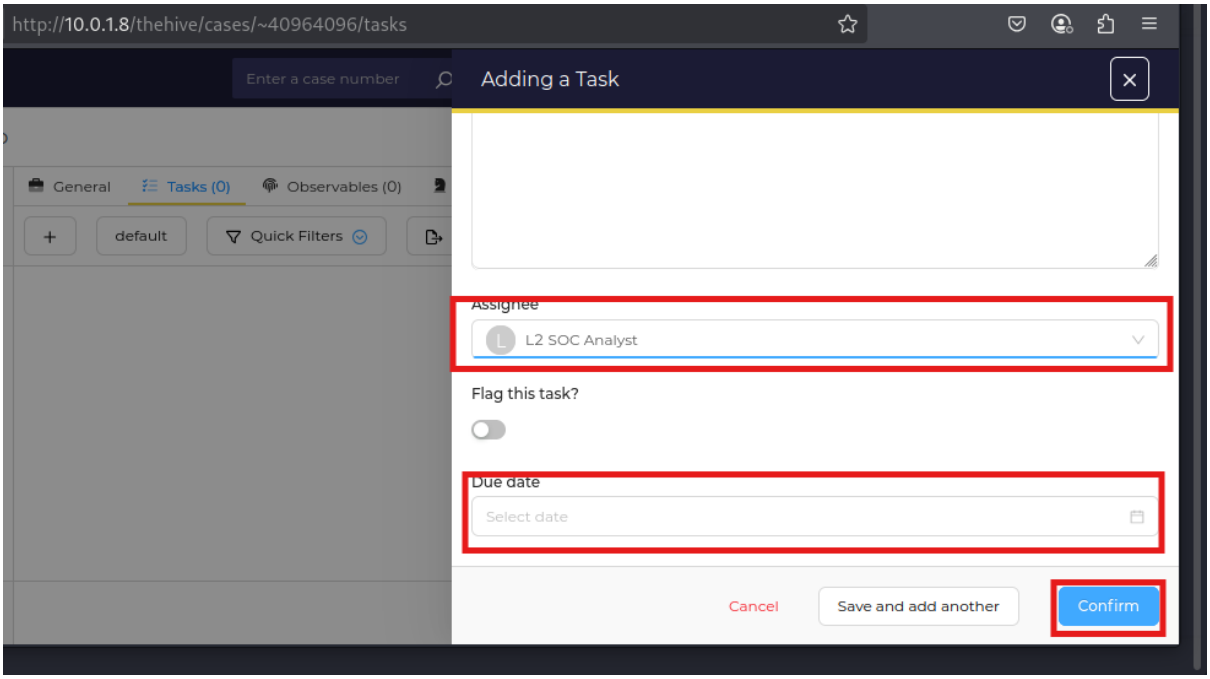




10. Untuk *group* dapat disesuaikan dengan *group* personel yang diberikan tugas. TheHive memiliki kemapuan untuk melakukan kustomisasi group. Pada lab ini tidak dilakukan kustomisasi *group* sehingga dapat dipillih default. Pada bagian judul tugas (`Title`) dapat diisikan mengenai judul tugas yang hendak diberikan.



11. Pada kolom `assigner` dapat dipilih kepada siapa tugas dapat diberikan. Dikarenakan anda sebagai seorang *L1 SOC Analyst* lalu tekan confirm.


http://10.0.1.8/thehive/cases/~40964096/tasks
Enter a case number
General
Tasks (0)
Observables (0)
default
Quick Filters
Adding a Task
Assignee
L2 SOC Analyst
Flag this task?
Due date
Select date
Cancel
Save and add another
Confirm

Membuat Ticket Pada TheHive Dengan Parameter yang Tepat (P.10.1.A)

Skenario Praktikum II

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. Tepat pukul 10:42 WIB, hari ini anda sebagai *L1 SOC Analyst* melihat banyak sekali notifikasi muncul dari Wazuh pada FIM yang menunjukan banyak file telah diubah pada server dengan IP 10.0.1.11. Server ini merupakan layanan SPPD yang digunakan oleh seluruh pegawai di lingkungan Pemerintah Kabupaten Lengkeng. Setelah melakukan penelusuran lebih dalam, Anda menemukan bahwa telah diunggah sebuah file mencurigakan ke direktori upload aplikasi. File tersebut tidak memiliki ekstensi .exe. File tersebut memiliki nilai hash 41050b2b9f619cdd9916e3bdd5b9f2f9

Anda menyadari bahwa file dalam server mulai berubah ekstensi menjadi .locked. Hal ini menandakan bahwa file mencurigakan yang diunggah tadi telah berhasil dijalankan dan memicu serangan ransomware yang mulai mengenkripsi data pada server aplikasi SPPD. Sebagai seorang *L1 SOC Analyst* anda harus segera membuat tiket dan melakukan identifikasi awal pada ransomware yang menyerang.

Tujuan Praktikum

Praktikum ini bertujuan untuk membantu perserta didik dalam membuat tiket insiden keamanan siber dengan tepat

Enviroment Laboratorium Virtual

Praktikum ini membutuhkan:

- VM The Hive
- VM dengan browser dan akses ke TheHive

Durasi Praktikum

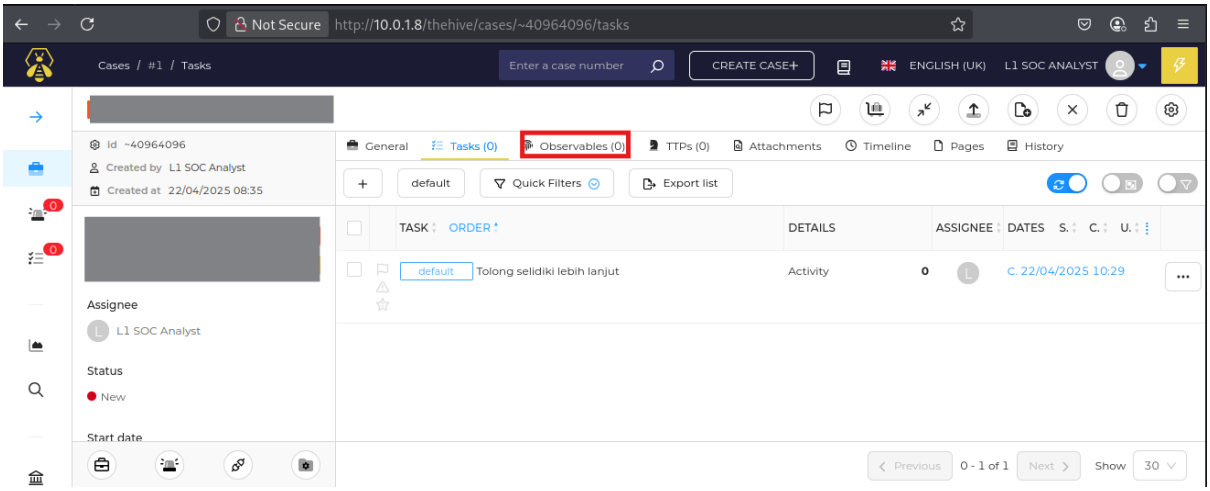
15 Menit

Catatan Khusus

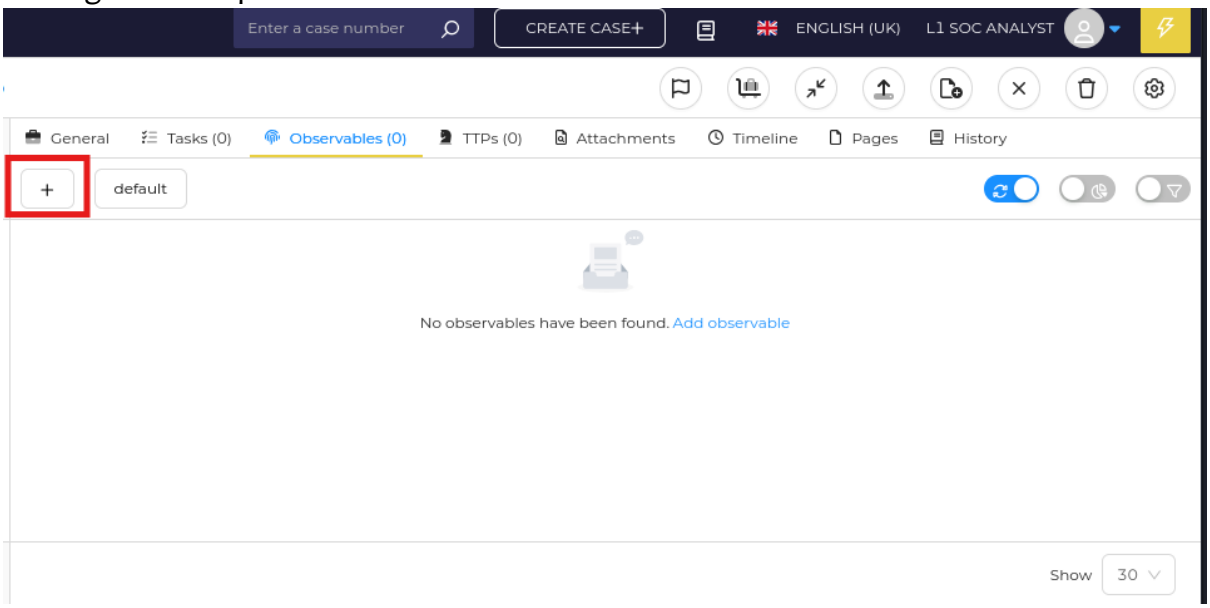
- Siapkan *enviroment* laboratorium virtual sesuai panduan installasi laboratorium virtual
- Dokumentasikan setiap langkah praktikum karena dapat membantu menjawab pertanyaan pada soal yang diberikan

Langkah-Langkah

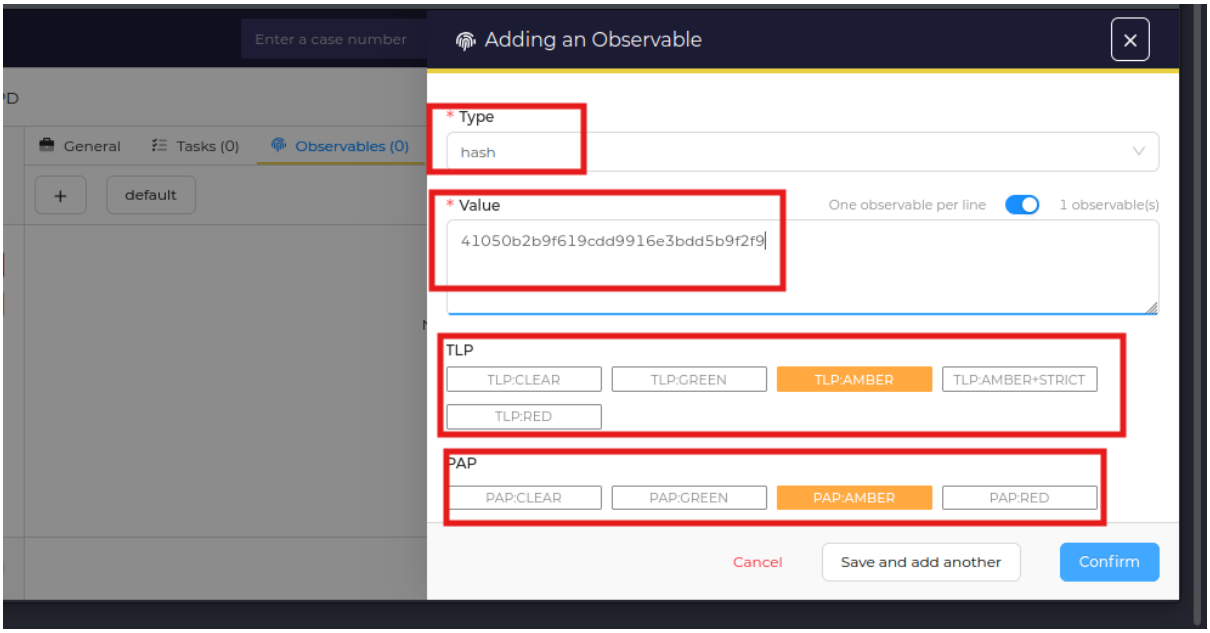
1. Buat tiket seperti biasa pada, sampai tahapan membuat task untuk *L2 SOC Analyst*. Selanjutkan anda harus menambahkan bukti bawa aset yang anda pantau terkena *ransomware*
2. Buka tiket yang telah dibuat, lalu tekan `Observables`.



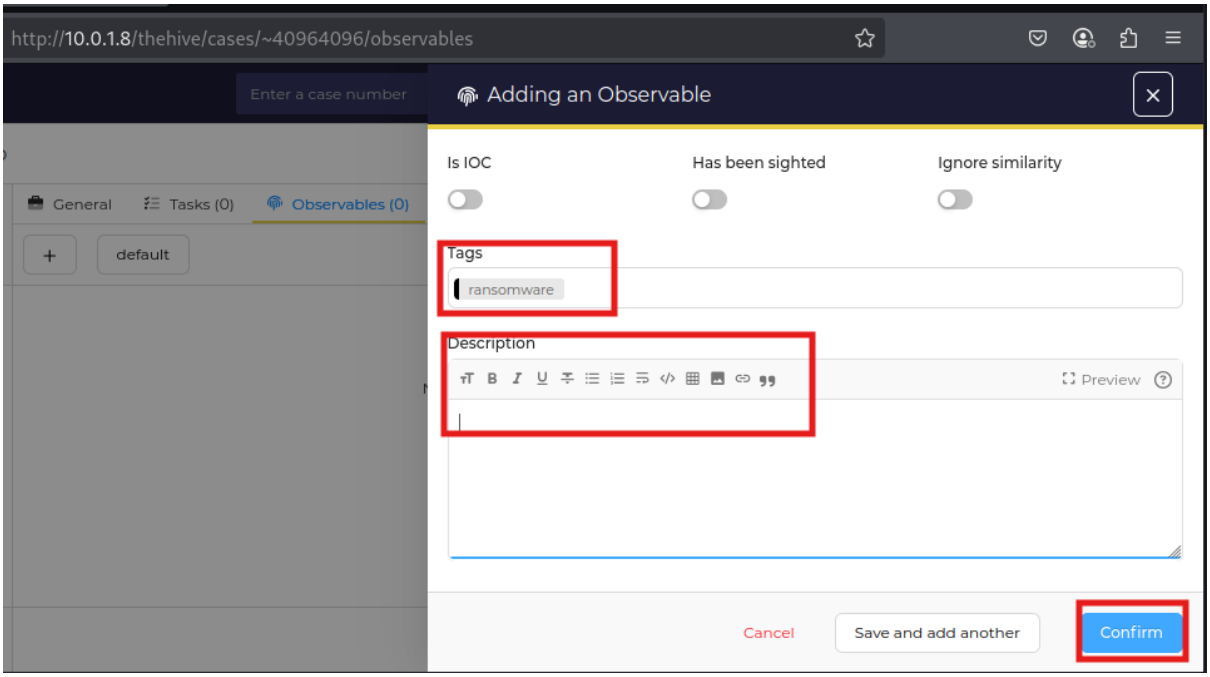
3. Klik logo tambah pada sebelah kiri.



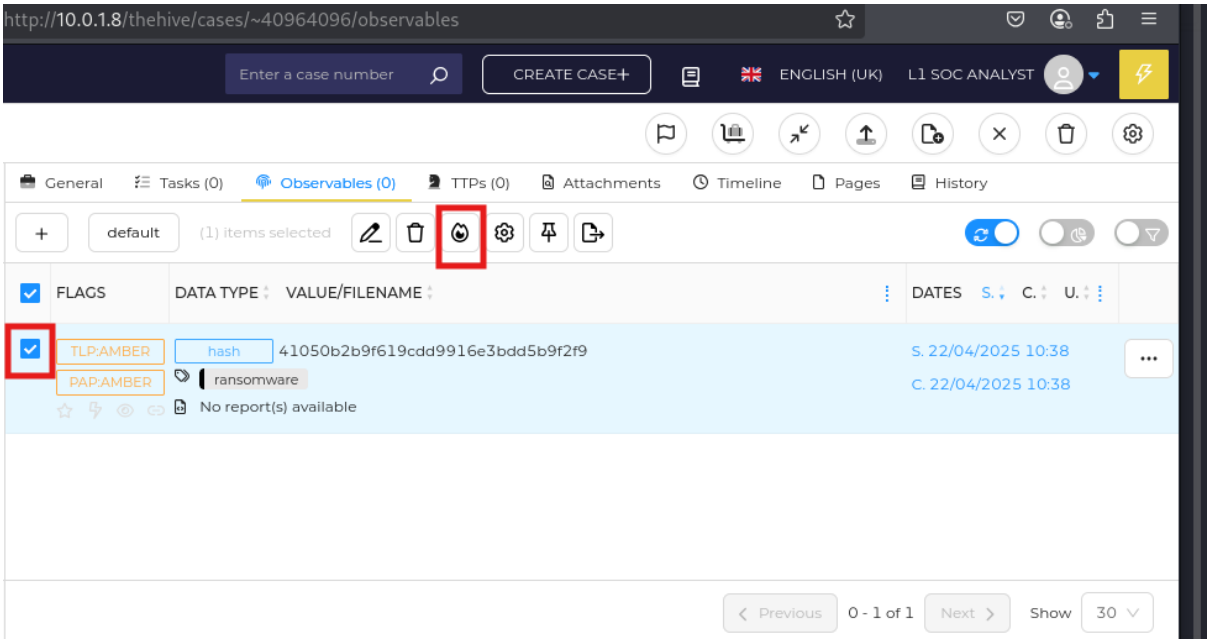
4. Type dapat dipilih berdasarkan bentuk yang akan dijadikan bukti, dikarenakan pada skenario ini anda hanya mendapatkan nilai hash, maka dapat dipilih hash. Masukan nilai hash yang telah anda peroleh dari skenario.



5. Masukan tag, seperti *ransomware*. Berikan deskripsi sedetail detailnya mengenai temuan bukti seperti bagaimana anda mendapatkannya. Terakhir tekan `Confirm`



6. Setelah menekan `confirm`, anda akan dibawa kehalaman `Observables`. Lakukan cheklist pada `obsevables` yang baru saja anda buat, lalu tekan logo *analyzer*



7. Pilih *Analyzer* yang akan dijalankan lalu tekan `Run Selected Analyzers`