MATERI L1 SOC ANALYST

UNIT KOMPETENSI 3

Memberikan Tiket Terhadap Insiden Keamanan Siber

MEDIA PEMBELAJARAN L1 SOC ANALYST

Unit Kompetensi

Memberikan Tiket Terhadap Insiden Keamanan Siber

Elemen Kompetensi

1. Memproses tiket terhadap insiden keamanan siber
    a. Jenis tiket diidentifikasi sesuai kebutuhan
    b. Tiket ditentukan sesuai dengan parameter
2. Mendistribusikan tiket terhadap insiden keamanan siber
    a. Sistem tiket diidentifikasi sesuai kebutuhan.
    b. Layanan tiket dilaksanakan sesuai hasil identifikasi sistem tiket

A. TICKECTING

Mengenal Ticketing

Ticketing merupakan metode terstruktur untuk mengelola dan menangani insiden, pertanyaan, atau permintaan keamanan.

Ticketing memiliki manfaat sebagai berikut:

1. Pengelolaan insiden menjadi lebih sistematis dan efisien
2. Pencatatan alur kerja pengelolaan insiden
3. Pembagian kerja

Kategori Jenis Ticketing Berdasarkan Objek Terdampak

1. Server
2. Perangkat Jaringan
3. Perangkat Pengguna
4. Aplikasi

Kategori Jenis Ticketing Berdasarkan Objek TerdampakSpesifik Insiden Kamsiber

1. *Account Compromised*
   Account compromised terjadi ketika akun pengguna atau sistem berhasil diakses oleh pihak yang tidak berwenang, biasanya karena pencurian kredensial seperti kata sandi atau token autentikasi. Hal ini bisa disebabkan oleh serangan *phishing, malware*, atau kebocoran data dari layanan lain.
2. *Data Theft*
   Data theft adalah tindakan pencurian informasi sensitif, seperti data pribadi, kredensial login, atau dokumen rahasia, oleh pihak yang tidak sah. Ini sering terjadi melalui serangan siber seperti peretasan basis data, eksploitasi celah keamanan, atau bahkan dari dalam organisasi oleh karyawan yang tidak jujur.
3. *Weak Configuration*
   Weak configuration merujuk pada pengaturan sistem atau perangkat lunak yang tidak aman, seperti kata sandi default yang tidak diubah, izin akses yang terlalu longgar, atau fitur keamanan yang dimatikan. Kondisi ini membuat sistem rentan terhadap serangan karena penyerang dapat dengan mudah menemukan dan memanfaatkan celah tersebut untuk mendapatkan akses tanpa izin.
4. *Weak Architecture*
   Weak architecture terjadi ketika desain infrastruktur teknologi sebuah sistem memiliki kelemahan mendasar, seperti kurangnya pemisahan antara komponen penting atau ketergantungan pada teknologi usang. Kelemahan ini bisa dimanfaatkan penyerang untuk menembus sistem secara keseluruhan, bahkan jika konfigurasi individual sudah diperkuat.
5. *Unpatched Software*

Unpatched software adalah perangkat lunak yang belum diperbarui untuk menutup celah keamanan yang sudah diketahui. Ketika pembaruan atau patch tidak diterapkan, penyerang dapat menggunakan kerentanan tersebut untuk menyusup ke sistem, mencuri data, atau menyebabkan kerusakan.

6. *Network Penetration*
   Network penetration adalah proses di mana penyerang berhasil masuk ke dalam jaringan yang seharusnya aman, biasanya dengan memanfaatkan kerentanan seperti *firewall* yang lemah atau protokol yang tidak terenkripsi. Setelah masuk, penyerang bisa memantau lalu lintas data, mencuri informasi, atau meluncurkan serangan lebih lanjut ke sistem lain dalam jaringan.
7. *Service Distruption*
   Service disruption terjadi ketika layanan atau sistem menjadi tidak tersedia, baik karena serangan sengaja seperti DDoS (*Distributed Denial of Service*) maupun kegagalan teknis.
8. *Vulnerability*
   Vulnerability adalah kelemahan atau celah dalam sistem, perangkat lunak, atau jaringan yang dapat dimanfaatkan oleh penyerang. Ini bisa berupa bug pemrograman, kesalahan konfigurasi, atau desain yang buruk. Jika tidak diatasi, kerentanan ini menjadi pintu masuk bagi berbagai jenis serangan siber.
9. *Phising*
   Phishing adalah teknik penipuan di mana penyerang menyamar sebagai pihak tepercaya (misalnya bank atau perusahaan) untuk menipu korban agar memberikan informasi sensitif, seperti kata sandi atau nomor kartu kredit. Biasanya dilakukan melalui email, pesan teks, atau situs web palsu, *phishing* sangat efektif karena kelengahan manusia daripada kelemahan teknologi.

Parameter dan Cakupan Layanan Internet

Parameter tiket

1. Jenis tiket
2. Deskripsi
3. Tingkat kegentingan insiden keamanan siber (*Low, Medium, High*)
4. Tingkat sensitivitas insiden keamanan siber
5. Kategori sharing information atau *Traffic Light Protocol* (TLP) yang umum digunakan respon insiden keamanan siber (*RED, AMBER, AMBER STRICT, GREEN, WHITE*)
6. Tujuan/pihak pelaksana tiket (merujuk struktur organisasi SOC terkait)
7. Dll

Cakupan layanan tiket

Layanan tiket mencakup bisnis proses dari organisasi, sistem tiket, dan distribusinya.

Ticketing Sample Field

1. *Reference number*
    - Nomor unik yang diberikan untuk setiap tiket yang dibuat
    - Digunakan untuk referensi dan pelacakan status tiket
    - Bisa berupa format tertentu, misalnya INC-20250323-001 (INC = Incident, tanggal, nomor urut)
2. *Contact Information*
    - Informasi kontak dari pelapor masalah atau insiden
    - Bisa mencakup nama, email, nomor telepon, dan departemen
    - Jika insiden dilaporkan oleh sistem otomatis, bisa berupa alamat IP atau hostname
3. *Date and Time (report, activity, discovery)*
    - *Report Time*: Waktu ketika masalah dilaporkan
    - *Activity Time*: Waktu ketika aktivitas atau troubleshooting dilakukan
    - *Discovery Time*: Waktu ketika masalah pertama kali ditemukan atau diperkirakan mulai terjadi
4. *Description of problem (category and priority, overview, in depth technical information, actions taken, impact and scope)*
    - *Category and Priority*: Menentukan jenis masalah (misalnya, jaringan, keamanan, aplikasi) dan prioritasnya *(Critical, High, Medium, Low)*
    - *Overview*: Ringkasan singkat tentang masalah yang terjadi
    - *In-depth Technical Information*: Detail teknis mengenai permasalahan (*log error, screenshot*, langkah replikasi, dll.)
    - *Actions Taken*: Langkah-langkah yang sudah dilakukan untuk menangani masalah
    - *Impact and Scope*: Seberapa luas dampaknya? Apakah hanya satu sistem, beberapa pengguna, atau seluruh organisasi?
5. *Systems affected (owner, criticality and mission, software and patch version)*
    - *Owner*: Pemilik sistem yang terdampak (individu atau tim yang bertanggung jawab)
    - *Criticality and Mission*: Seberapa penting sistem ini bagi operasi organisasi? (misalnya, sistem pembayaran vs. sistem internal)
    - *Software and Patch Version*: Versi perangkat lunak yang digunakan, termasuk apakah sudah diperbarui atau masih menggunakan versi lama
6. *Assigned staf*
    - Nama staf atau tim yang bertanggung jawab menangani tiket ini
    - Bisa mencakup lebih dari satu orang, terutama jika masalah kompleks
7. *Action items*

- Daftar tugas yang harus dilakukan untuk menyelesaikan masalah
- Bisa berupa investigasi lebih lanjut, perbaikan sementara, atau implementasi solusi permanen

8. *Staff contacted*
   - Siapa saja yang dihubungi selama penanganan masalah?
   - Bisa mencakup tim internal, vendor, atau pihak ketiga lainnya
9. Supemental data gathered
   - Data tambahan yang dikumpulkan selama investigasi, seperti log sistem, *capture* jaringan, *screenshot*, atau data dari *monitoring tools*
10. *Cost of damage*
    Perkiraan kerugian akibat insiden, baik dalam bentuk *downtime*, kehilangan data, atau biaya operasional tambahan
11. *Cost of recovery*
    Biaya yang diperlukan untuk memulihkan sistem, termasuk tenaga kerja, perangkat keras/software baru, atau layanan eksternal
12. *Time to resolve*
    Waktu yang dibutuhkan untuk menyelesaikan masalah sejak dilaporkan hingga dinyatakan selesai bisa dihitung dalam hitungan jam, hari, atau minggu, tergantung tingkat keparahan masalahnya
13. *Resolution*
    - *Final Fix*: Solusi akhir yang diterapkan untuk menyelesaikan masalah. Bisa berupa patch, konfigurasi ulang, restart layanan, atau upgrade perangkat lunak
    - *Root Cause Analysis* (RCA): Analisis penyebab utama insiden. Apakah karena kesalahan manusia, bug software, serangan siber, atau faktor lain?
    - *Preventive Measures*: Tindakan pencegahan agar masalah serupa tidak terjadi di masa depan (misalnya, meningkatkan monitoring, menambah sistem keamanan, atau menerapkan prosedur baru)
    - *Verification & Confirmation*: Apakah sistem sudah diuji dan dikonfirmasi normal kembali? Siapa yang melakukan verifikasi?
    - *Closure Notes:* Catatan akhir yang mencakup apakah semua pihak yang terdampak sudah diinformasikan, serta apakah ada tindakan lanjutan yang diperlukan

KARAKTERISTIK TICKETING SYSTEM

1. *Front-end data entry* dan *query interface*
   Front-end adalah bagian yang dilihat dan digunakan langsung oleh pengguna, seperti analis SOC atau petugas helpdesk, untuk memasukkan data (misalnya, detail insiden seperti waktu, deskripsi, dan tingkat keparahan) serta melakukan pencarian (query) terhadap tiket yang sudah ada dan dirancang agar intuitif, responsif, dan mudah digunakan, dengan

formulir untuk input data dan fitur pencarian yang memungkinkan pengguna menemukan tiket berdasarkan kata kunci, status, atau ID tiket.

2. *Back-end database*
   Tempat semua data yang dimasukkan melalui front-end disimpan, dikelola, dan diproses. Ini biasanya berupa sistem basis data (seperti MySQL, PostgreSQL, atau Elasticsearch) yang menyimpan informasi tiket, log aktivitas, dan metadata dalam struktur yang terorganisir. Back-end memastikan data tetap aman, dapat diakses dengan cepat, dan mendukung operasi seperti pembaruan status tiket atau pelaporan.
3. *Multiple user roles*
   Kemampuan ticketing system untuk mendukung berbagai peran pengguna dengan hak akses yang berbeda-beda Fitur ini biasanya diatur melalui sistem izin (permissions) seperti admin, editor, atau viewer, yang memastikan kolaborasi tim berjalan lancar sambil menjaga keamanan data.
4. *Methods of automation*
   - *Entry*
     Ticketing system dapat secara otomatis membuat tiket baru tanpa intervensi manual yang mendeteksi ancaman dan langsung menghasilkan tiket berdasarkan aturan tertentu Proses ini menghemat waktu, mengurangi kesalahan manusia, dan memastikan insiden segera ditangani.
   - *Export*
     Memungkinkan ticketing system untuk secara otomatis mengekspor data tiket ke format lain (seperti CSV, PDF, atau JSON) atau ke sistem eksternal tanpa perlu pengguna melakukannya secara manual lalu data tiket bisa dikirim atau disimpan otomatis, misalnya ke email atau cloud.
   - *Flexible explore capabilities*
     Memungkinkan pengguna untuk mencari, memfilter, dan menganalisis tiket secara dinamis dengan bantuan fitur otomatis. Ini bisa berupa dashboard yang memperbarui statistik secara real-time, filter cerdas berdasarkan tag atau prioritas, atau bahkan saran otomatis untuk langkah respons berdasarkan pola insiden sebelumnya.

B. Distiribusi Ticketing

Apa itu Distirbusi Ticketing

Proses pengalokasian dan penugasan tiket terkait insiden keamanan siber kepada personel atau tim yang tepat dalam suatu organisasi

Alur Distribusi Ticketing

TLP

The Traffic Light Protocol (TLP) diciptakan untuk memfasilitasi pembagian informasi yang berpotensi sensitif dan kolaborasi yang lebih efektif. Pembagian informasi terjadi dari sumber informasi, kepada satu atau beberapa penerima. TLP adalah sekumpulan empat label yang digunakan untuk menunjukkan batasan pembagian yang akan diterapkan oleh penerima. Hanya label yang tercantum dalam standar ini yang dianggap valid oleh FIRST.

v1	v2	R	G	B	Keterangan
TLP:RED	TLP:RED	255	43	43	Hanya untuk penerima atau personel yang terlibat saja, dan tidak untuk diungkap & diteruskan kepada siapapun. Contoh: dalam konteks sebuah rapat/pertemuan, informasi dengan TLP:RED diperuntukan bagi peserta rapat saja.
TLP: AMBER	TLP: AMBER	255	192	0	Hanya untuk kalangan terbatas, di mana penerima informasi hanya dapat membagi/meneruskan informasi kepada kalangan **internal organisasi dan pemangku kepentingan** yang **dianggap perlu mengetahui** informasi tersebut.
	TLP: AMBER+STRICT				Hanya untuk kalangan terbatas, di mana penerima informasi hanya dapat membagi/meneruskan ifnormasi kepada kalangan **internal organisasi** yang **dianggap perlu mengetahui informasi**.
TLP:GREEN	TLP:GREEN	51	255	0	Hanya untuk kalangan terbatas, di mana penerima informasi dapat meneruskan informasi tersebut ke **lingkup komunitasnya**.Contoh: komunitas pertahanan atau keamanan siber. Contoh: Materi TTX, sample simulasi drill, dll.
TLP: WHITE	TLP: CLEAR	255	255	255	Penerima dapat meneruskan informasi kepada semua orang tanpa batasan. Isi informasi dapat dilabeli TLP:CLEAR ketika tidak terdapat atau berpotensi menimbulkan risiko.

PAP

Permissible Action Protocol (PAP) dirancang untuk menunjukkan bagaimana informasi yang diterima dapat digunakan. PAP memiliki empat level berbeda, dengan kode warna yang identik.

Level	Keterangan
PAP:RED	Hanya tindakan yang tidak terdeteksi. Penerima tidak boleh menggunakan informasi PAP:RED di jaringan. Hanya tindakan pasif pada log, yang tidak terdeteksi dari luar.
PAP: AMBER	Penerima dapat menggunakan informasi PAP: AMBER untuk melakukan pemeriksaan online, seperti menggunakan layanan yang disediakan oleh pihak ketiga (misalnya VirusTotal), atau menyiapkan honeypot pemantauan
PAP:GREEN	Tindakan aktif diperbolehkan. Penerima dapat menggunakan informasi PAP:GREEN untuk melakukan ping ke target, memblokir lalu lintas masuk/keluar dari/ke target atau secara khusus mengkonfigurasi honeypots untuk berinteraksi dengan target.
PAP: WHITE	Tidak ada batasan dalam menggunakan informasi ini.

Platform Ticketing

1. TheHive
   TheHive alat untuk tim keamanan siber (SOC) yang membantu mengelola dan menangani insiden keamanan. Digunakan untuk membuat tiket, melacak ancaman, dan berkolaborasi antar tim.
2. OSTicket
   OSTicket adalah aplikasi open-source untuk mengelola tiket bantuan (helpdesk). Cocok untuk tim IT atau layanan pelanggan yang perlu menangani permintaan atau masalah dari pengguna.
3. Zendesk
   Zendesk adalah platform untuk layanan pelanggan. Membantu membuat tiket dari email, chat, atau telepon, dan mengelola pertanyaan atau keluhan pelanggan dengan mudah.
4. GLPi
   GLPi adalah alat open-source untuk manajemen IT, termasuk ticketing. Digunakan untuk melacak masalah IT, mengelola aset, dan membantu tim IT menangani permintaan.
5. Jira Service Desk
   Jira Service Desk (sekarang disebut Jira Service Management) adalah alat untuk tim IT atau layanan. Membantu membuat tiket, melacak masalah, dan mengatur alur kerja tim.
6. Freshdesk
   Freshdesk adalah aplikasi untuk layanan pelanggan. Membantu tim menangani tiket dari pelanggan, seperti keluhan atau pertanyaan, dengan fitur otomatisasi dan laporan.
7. HelpScout

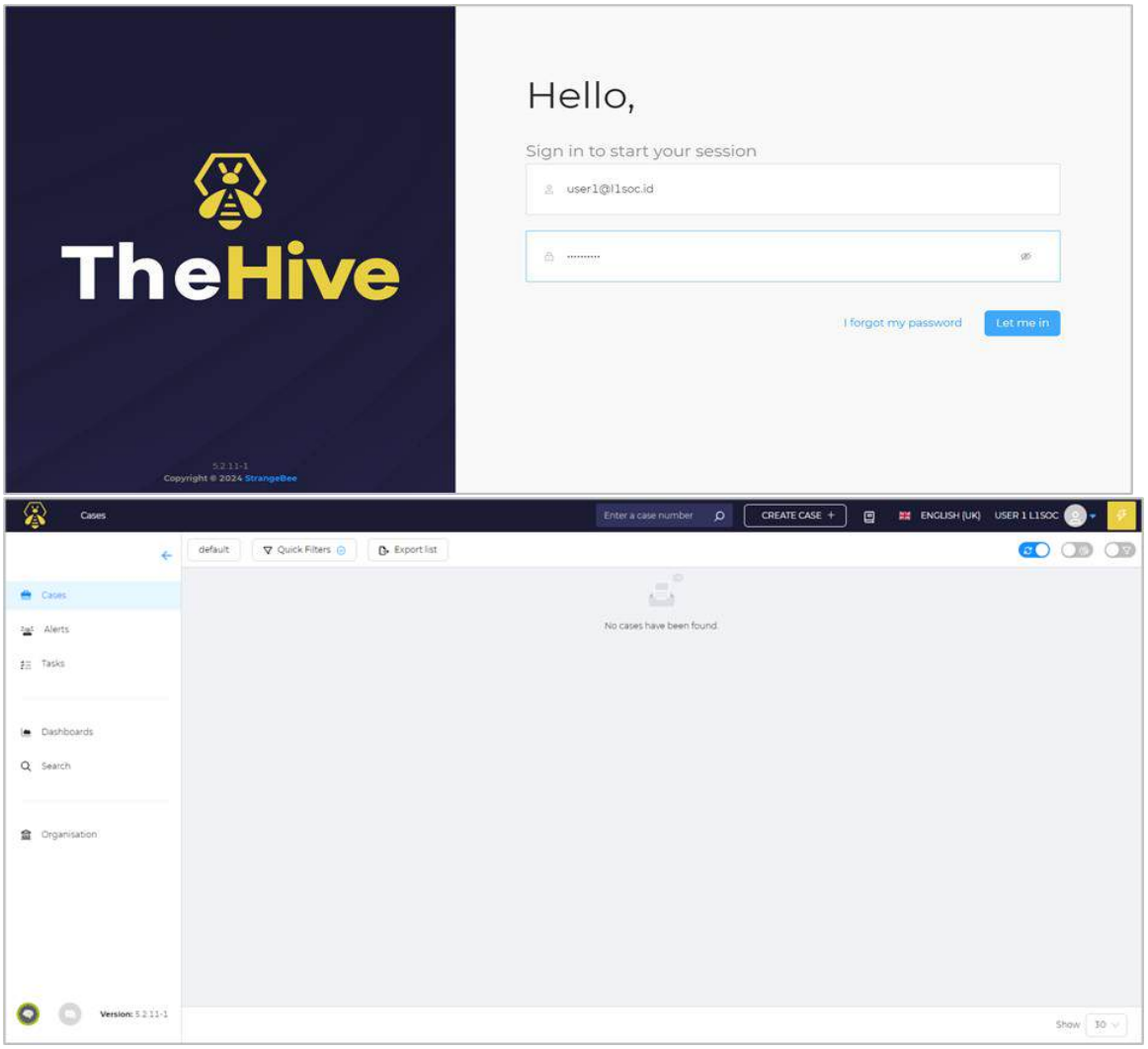
HelpScout adalah alat untuk tim dukungan pelanggan. Fokus pada komunikasi dengan pelanggan melalui email, dengan sistem ticketing yang sederhana dan ramah pengguna.

8. ServiceNow
   ServiceNow adalah platform besar untuk manajemen layanan IT (ITSM). Digunakan untuk ticketing, otomatisasi proses IT, dan mengelola operasi perusahaan secara luas.

C. THE HIVE

Apa itu TheHive?

TheHive adalah platform open-source untuk tim keamanan siber (SOC, CERT, CSIRT) yang digunakan untuk mengelola, melacak, dan menangani insiden keamanan siber, seperti malware atau phishing, dengan fitur manajemen kasus, kolaborasi tim, dan integrasi alat lain.

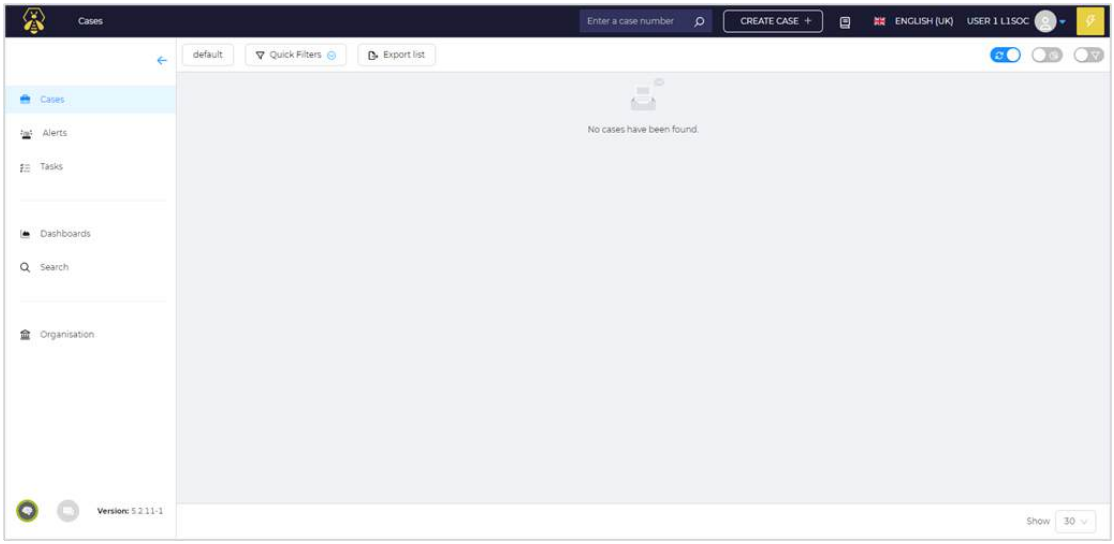


Alur *WorkFlow* aplikasi The Hive

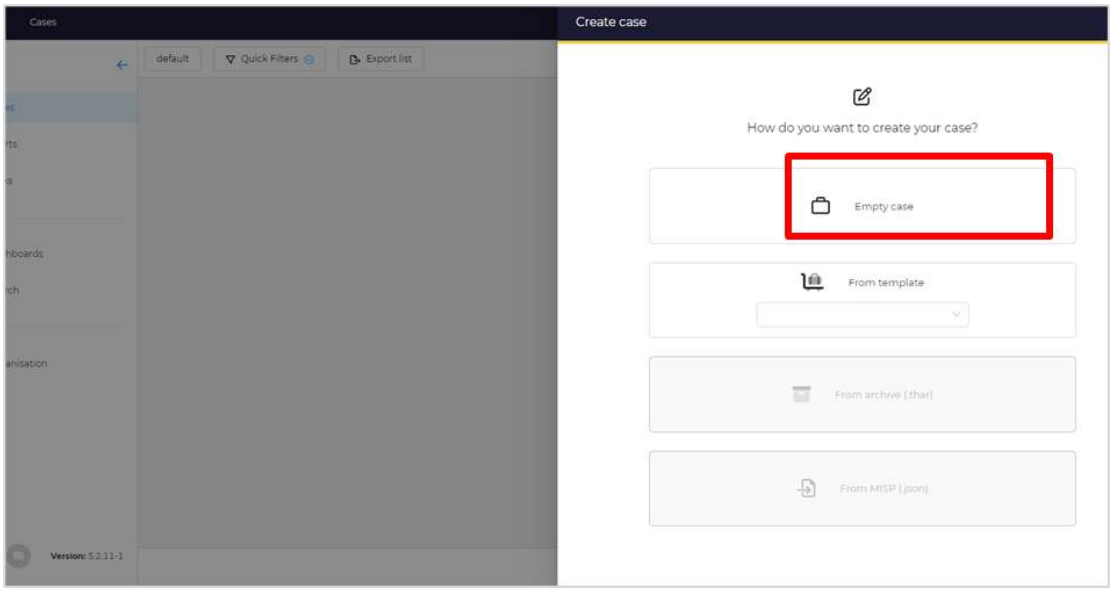
1. Open Case (Buka Kasus)
   Langkah pertama, sebuah kasus (case) dibuat untuk mencatat insiden keamanan, misalnya serangan malware atau phishing.
2. Open Task (Buka Tugas)
   Dalam kasus tersebut, tugas (task) dibuat untuk menangani insiden, seperti "periksa log" atau "analisis file".
3. Observable (Observasi)
   Tim mengumpulkan dan mencatat data terkait insiden, seperti alamat IP penyerang, URL mencurigakan, atau file berbahaya.

4. Give Task (Berikan Tugas)
   Tugas-tugas yang sudah dibuat diberikan kepada anggota tim yang sesuai, misalnya analis SOC level 1 atau 2.
5. Close Task (Tutup Tugas)
   Setelah tugas selesai (misalnya analisis selesai), tugas ditutup dan hasilnya dicatat.
6. Close Case (Tutup Kasus)
   Setelah semua tugas selesai dan insiden terselesaikan, kasus ditutup secara resmi.

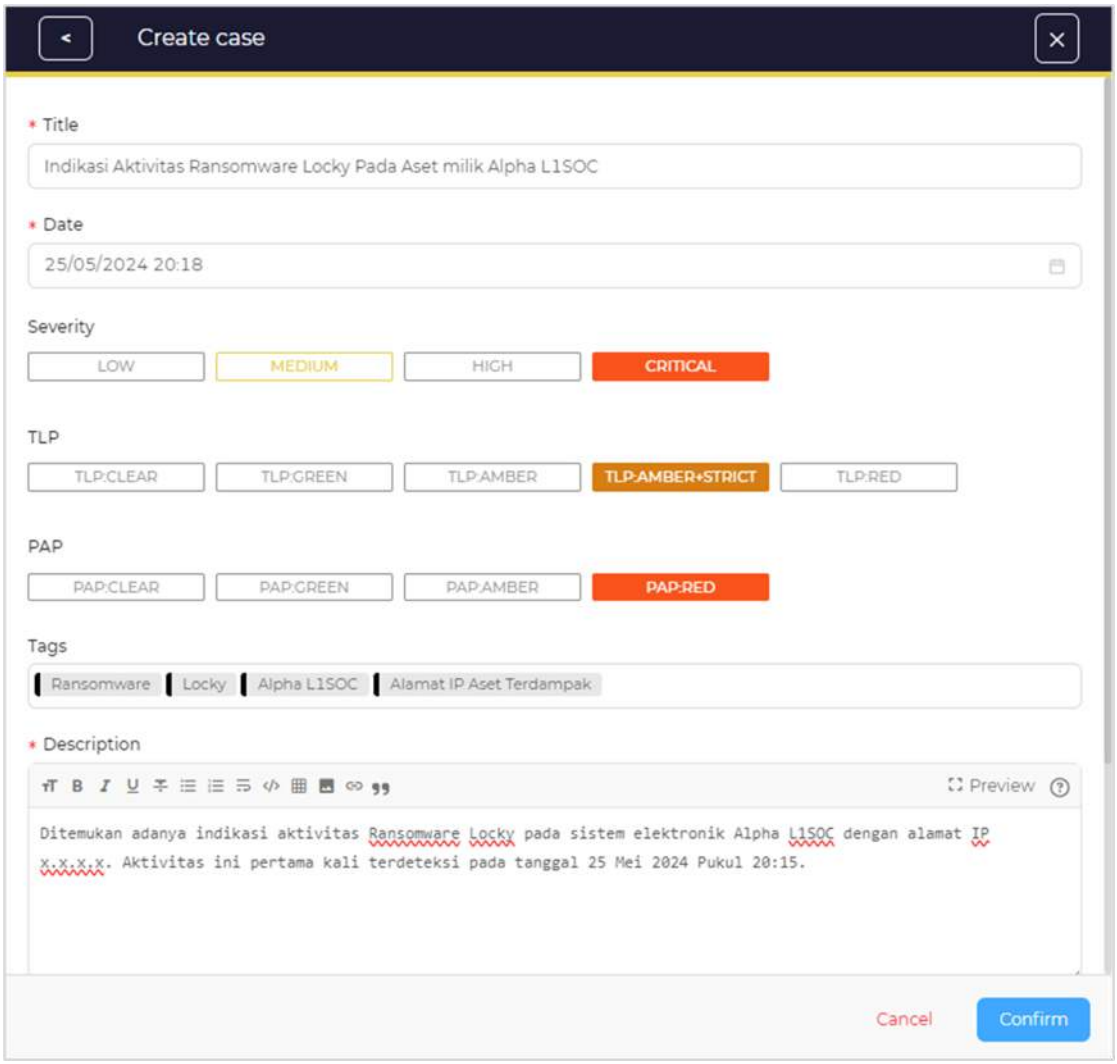
Open case The Hive



Gambar ini menunjukkan antarmuka utama dari TheHive, sebuah platform ticketing untuk tim keamanan siber, pada tab "Cases" (Kasus). Di bagian atas, terdapat tombol "CREATE CASE" yang dilingkari merah, yang digunakan untuk membuat kasus baru terkait insiden keamanan. Di sisi kiri, ada menu navigasi dengan opsi seperti Cases, Alerts, Tasks, Dashboards, Search, dan Organisation, yang memungkinkan pengguna mengakses berbagai fitur. Bagian tengah layar menunjukkan pesan "No cases have been found" karena belum ada kasus yang dibuat. Antarmuka ini dirancang sederhana agar tim SOC dapat dengan mudah memulai proses ticketing.



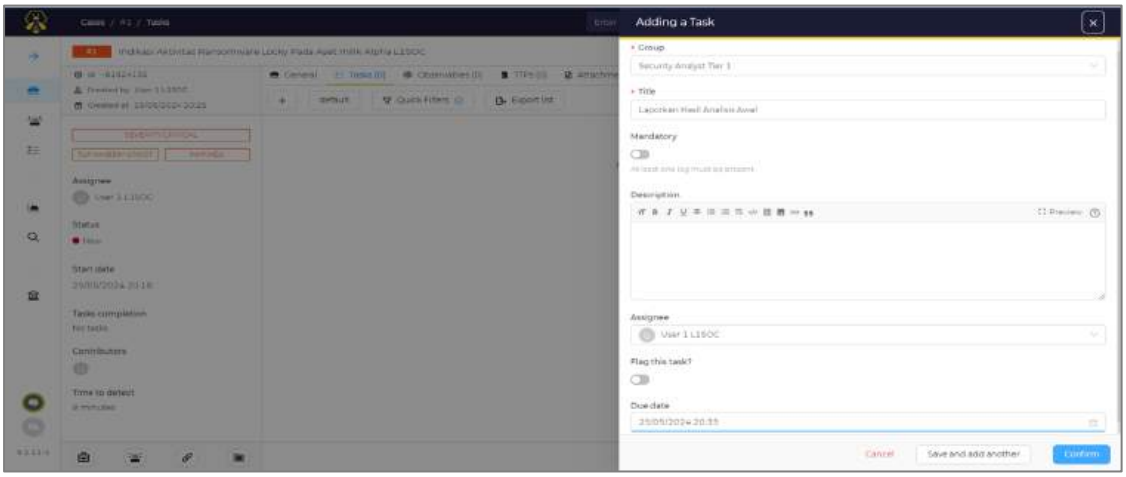
Tampilan jendela pop-up yang muncul setelah tombol "CREATE CASE" diklik. Jendela ini bertanya, "How do you want to create your case?" (Bagaimana Anda ingin membuat kasus?) dengan beberapa opsi. Opsi yang dilingkari merah adalah "Empty case" (Kasus kosong), yang berarti pengguna dapat membuat kasus baru dari nol tanpa template. Opsi lain termasuk "From template" (dari template), "From archive (.thar)" (dari arsip), dan "From MISP (json)" (dari MISP). Fitur ini memberikan fleksibilitas kepada pengguna untuk memilih cara membuat kasus sesuai kebutuhan, seperti memulai dari awal atau menggunakan data yang sudah ada.



Ini merupakan laman tampilan saat ingin membuat lamporan nya (case)

1. Title: Ditulis lengkap, tidak boleh disingkat atau akronim, memuat nama stakeholder
2. Tanggal Create Case: Ditulis dengan format "DD-MM-YYYY TT:TT"
3. Severity: Menunjukkan persepektif teknis mengenai ancaman, potensi dampak, dan resiko ancaman
4. TLP: Menentukan batas penyebaran informasi sensitif
5. PAP: Menentukan aksi yang boleh dilakukan ketika melakukan analisis insiden siber
6. Tags: Penulisan sensor, nama sistem, nama stakeholder, kerentanan, jenis laporan.
7. Deskripsi: Mengisi deskrripsi dengan menggunakan "5W+1H"
    - What : Insiden apa
    - When : Timeline kejadian
    - Where : Aset mana yang terdampak
    - Who : Siapa pemilik aset tersebut
    - Why : Indikasi penyebab insiden tersebut terjadi
    - How : Bagaimana insiden terjadi

Open Task The Hive



1. Buka Kasus (Case)
    - Navigasikan ke daftar kasus yang tersedia.
    - Pilih kasus yang ingin dikerjakan (contoh: "Indikasi Aktivitas Ransomware Locky...").
    - Setelah masuk ke dalam kasus, buka tab Tasks (terlihat pada area yang diberi kotak merah dalam gambar).
2. Tambahkan Tugas Baru
    - Klik tombol Tambah Tugas (+ Task).
    - Akan muncul jendela Adding a Task.
    - Isi detail tugas, seperti:

        Group (contoh: "Security Analyst Tier 1").

        Title (contoh: "Laporkan Hasil Analisis Awal").

        Assignee (pengguna yang bertanggung jawab).

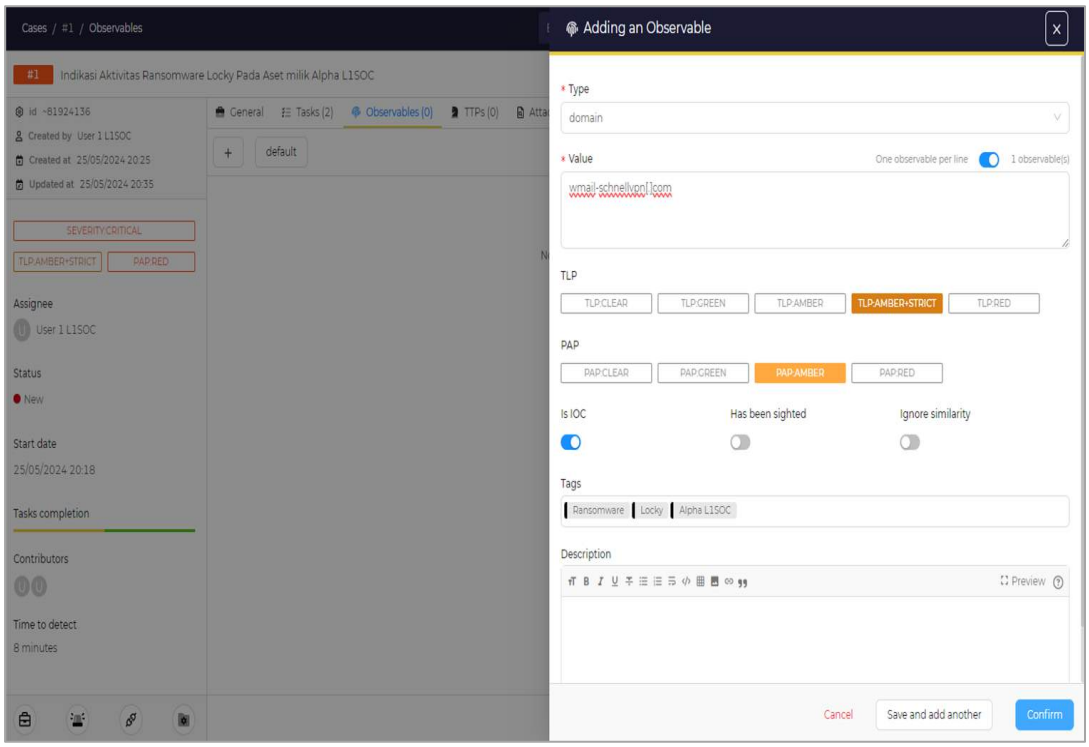
        Due Date (batas waktu pengerjaan tugas).

        Setelah mengisi semua informasi yang diperlukan, klik Confirm atau Save and add another jika ingin menambahkan tugas lain.
3. Mulai Pengerjaan Tugas

    Setelah tugas berhasil dibuat, tugas akan muncul di daftar Tasks. Untuk memulai tugas, Klik tombol tiga titik (:) pada tugas yang telah dibuat (terlihat pada bagian kanan daftar tugas). Pilih opsi Start dari menu yang muncul. Tugas akan berubah statusnya menjadi aktif.

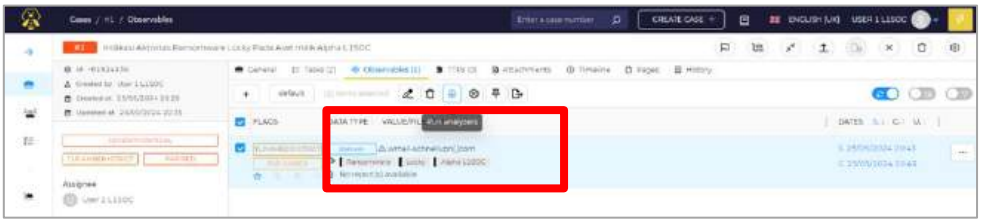
4. Proses Selanjutnya
   Setelah tugas dimulai, pengguna bisa mengupdate statusnya sesuai dengan progres pengerjaan. Jika tugas selesai, bisa diubah statusnya menjadi Completed atau memberikan laporan hasil analisis.

Observables The Hive

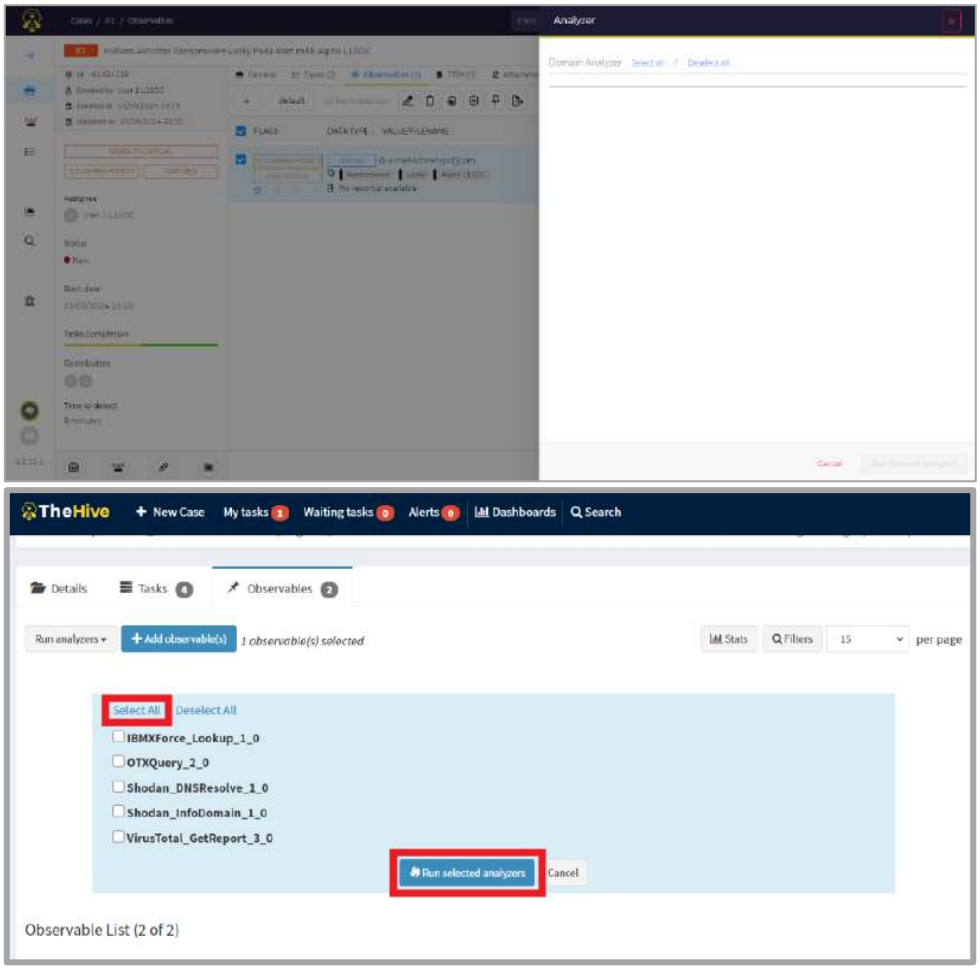


Gambar tersebut menjelaskan komponen penting dalam pendataan *Indicators of Compromise* (IOC) pada analisis insiden siber. Setiap IOC memiliki jenis observables seperti domain, IP, hash, file, dan lainnya yang dimasukkan pada kolom "Value". Informasi ini dilengkapi dengan TLP (*Traffic Light Protocol*) untuk mengatur tingkat kerahasiaan informasi, serta PAP (*Permissible Actions Protocol*) yang menentukan tindakan yang diizinkan saat analisis dilakukan. Terdapat juga kolom penanda apakah data tersebut merupakan IOC dari insiden, serta tags dan deskripsi untuk menjelaskan aktivitas yang berkaitan dengan nilai IOC tersebut.

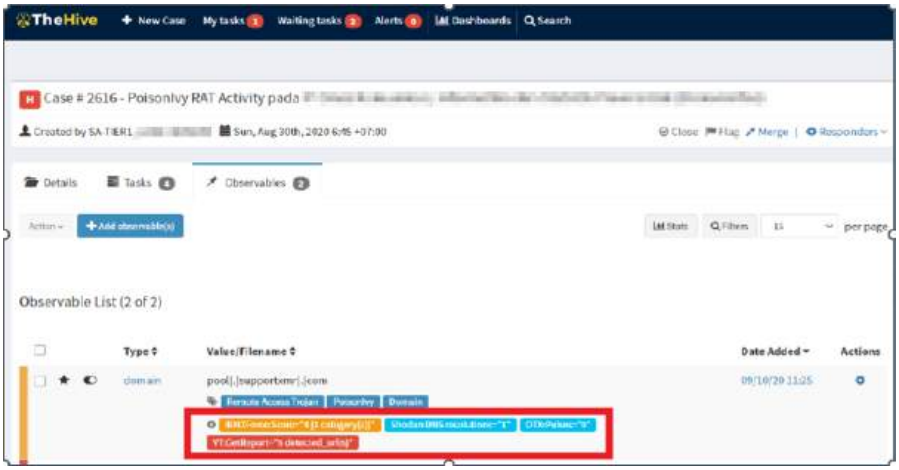
Menjalankan Analyzer pada TheHive



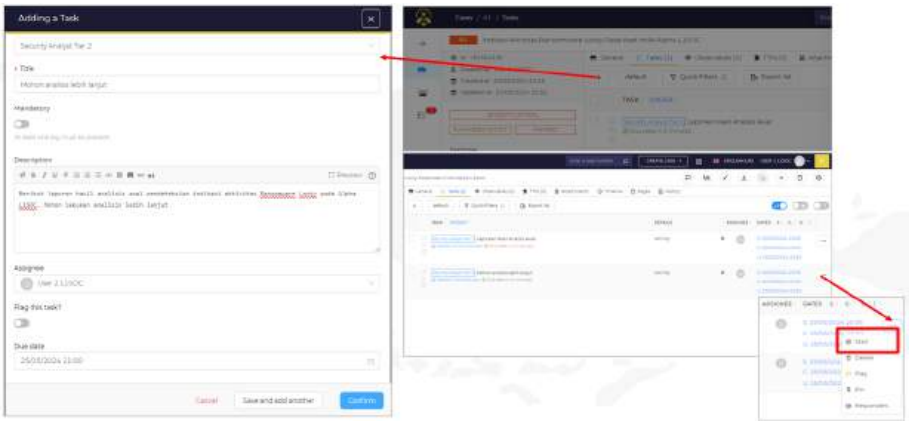
Setelah observable (misalnya domain) ditambahkan, klik ikon 🔍 "Run analyzers" di bagian atas halaman Observables. Aksi ini akan mengirimkan observable ke tool analisis eksternal seperti VirusTotal, AbuseIPDB, MISP, atau analisa lokal via Cortex.



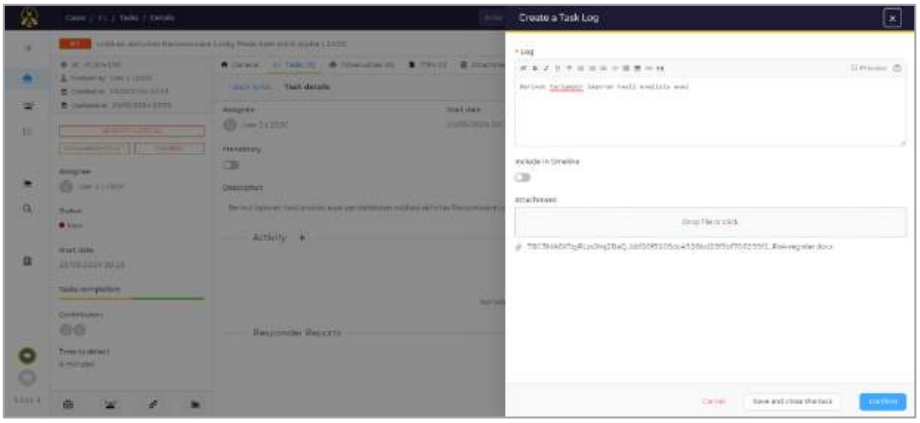
Pilih analyzer yang tersedia, terdapat banyak pilihan seperti pada gambar lalu *Run selected analyzers. Proses penggunaan analyzer dalam TheHive adalah otomatisasi* analisis IOC sehingga tidak perlu manual copy-paste ke situs VirusTotal atau AbuseIPDB. Sehingga dapat mempercepat pengambilan keputusan: hasil analisis bisa langsung menunjukkan apakah domain/ip/hash itu malicious atau tidak.



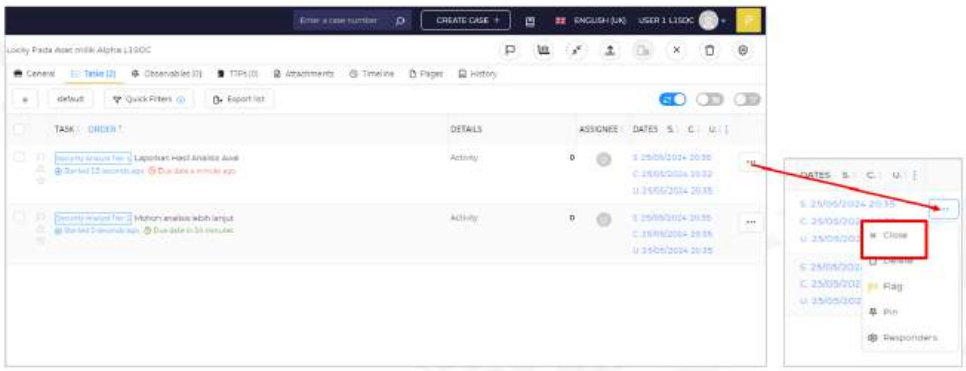
Memberikan Task



Mengerjakan Task



Menutup Task



Menutup Kasus