



S.A.L.T CI · PRODUCT BRIEF

SENTINEL

Intelligence Surveillance System

Turns the cameras you already own into a sovereign eye that detects, alerts, searches and writes its own reports, on your own servers, with no camera replacement and no video leaving the premises.

Any camera, any VMS

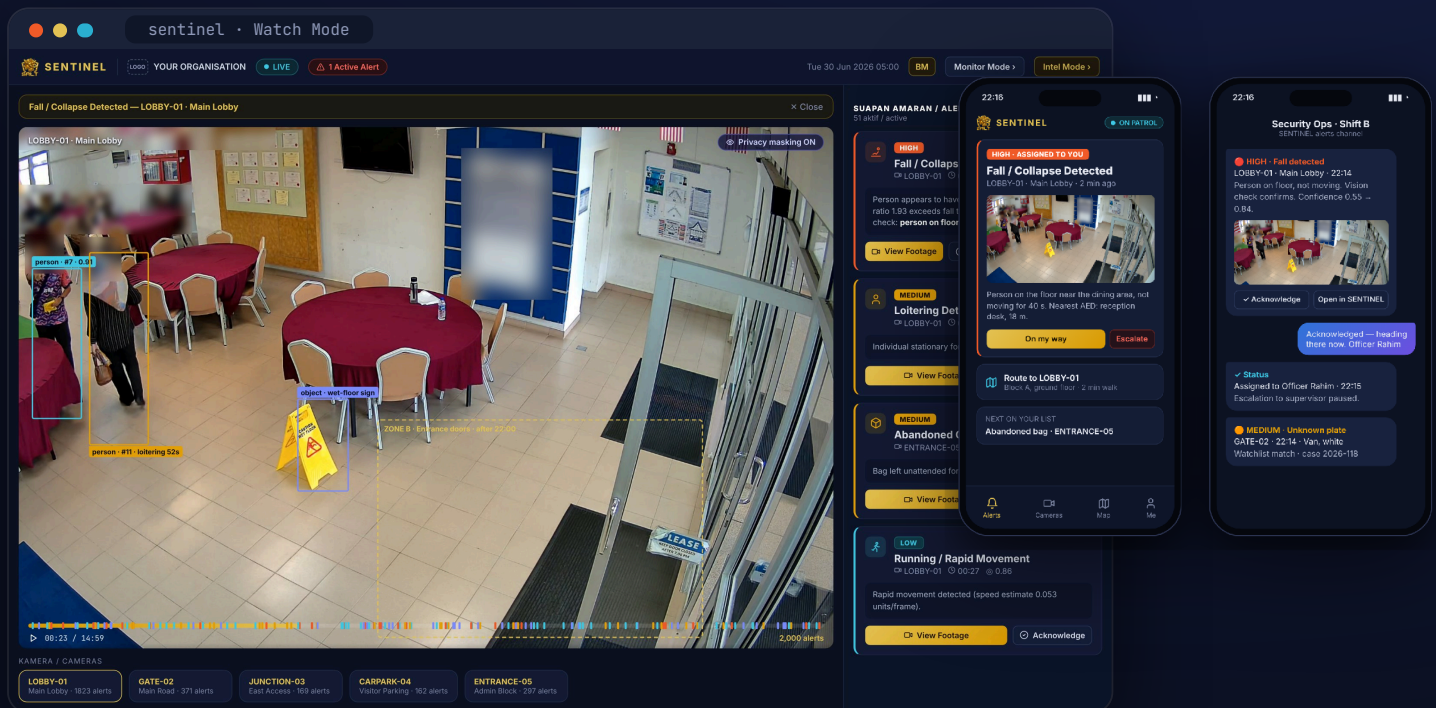
12 detector families

Watch · Monitor · Intel

AI reports in BM & EN

Plain-language search

On premises & air-gapped





CONTENTS

Inside this brief

What SENTINEL is, how it works, what each operator sees, how it fits your existing cameras and systems, and how it is deployed, governed and rolled out.

01	Executive summary	02	The gap SENTINEL closes
03	Product overview and principles	04	Architecture
05	The unified alert and integration paths	06	Detection modules
07	Watch mode	08	Monitor mode
09	Intel mode	10	Industry solutions
11	Integration	12	Privacy, ethics and compliance
13	Deployment and sizing	14	From assessment to go-live
15	Part of the S.A.L.T CI platform	16	Why SENTINEL

SENTINEL at a glance

12

detector families, switched on per camera, zone and schedule

50+

behaviours, from a fall or a tailgate to grass that needs cutting

3

operating modes for duty officers, supervisors and analysts

1

alert format for every detector, so one console, one search, one report engine

2

languages for every report and screen: Bahasa Melayu and English

0

video copies sent outside the site; nothing goes to a cloud unless you allow it

SENTINEL in one line

Turn any existing CCTV network into an intelligent, sovereign eye that detects, alerts, searches and reports on your own servers, with no camera replacement and no video leaving the premises.

This brief describes the complete SENTINEL 1.0 product. Screens shown are from the SENTINEL console with illustrative data; camera names, organisation details, plates and people are anonymised, and faces are shown with privacy masking on.



01 · EXECUTIVE SUMMARY

Cameras that record everything and understand it

Most CCTV networks record everything and understand nothing. Footage is reviewed only after something has gone wrong, no team can watch hundreds of screens, and finding one event in a week of video can take days.

SENTINEL is the intelligence surveillance system of the S.A.L.T CI platform. It adds a real-time and investigative layer on top of the camera network an organisation already owns: it watches every enabled camera, detects what matters, sends the right alert to the right person, finds incidents in recorded footage in minutes, and writes the incident report itself.

Commercial video analytics usually means new cameras, a vendor's cloud, per-camera subscriptions or analytics locked to one camera brand. SENTINEL takes a different path. It works with existing cameras and recorders of any brand, keeps video and every detection on the organisation's own servers, and runs on **TERAS**, S.A.L.T CI's sovereign AI core, so its reasoning, search and reports come from AI models the organisation controls.

What the organisation gets



No camera replacement

IP cameras over RTSP and ONVIF, analogue cameras through encoders, and any VMS or NVR. Your VMS stays the system of record.



Modular detection

Twelve detector families, switched on per camera, zone and schedule. New detectors drop in without changing the platform.



One alert, one console

Every detector produces the same alert, so one console, one rule engine, one search and one report engine serve every camera.



Reports, not raw detections

Incident narratives, shift summaries and investigation reports written by AI, in Bahasa Melayu or English.



Investigations in minutes

Search footage by object, face, plate, colour, place and time, or simply ask in plain language.



Sovereign and lawful by design

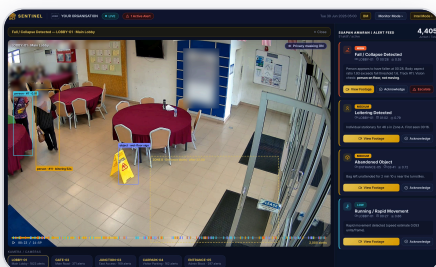
On premises or air-gapped, with roles, retention, privacy masking and a full audit trail, aligned with Malaysia's PDPA.

From one building to a city

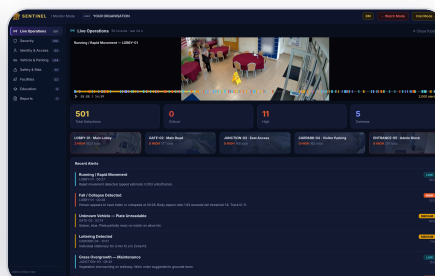
A single server for one building, edge boxes beside camera clusters, or many sites linked through TERAS federation with a central command view and shared watchlists.

People stay in charge

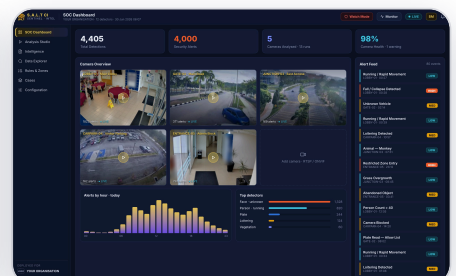
SENTINEL detects, ranks and explains. A person confirms before any action is taken against anyone, and every face or plate match shows its evidence and confidence.



Watch · the duty officer



Monitor · supervisors and management



Intel · analysts and investigators



02 · THE GAP SENTINEL CLOSES

Most camera networks are **recorders, not sensors**

Organisations have invested heavily in cameras. What they rarely have is a way to turn that video into timely action, evidence and insight without buying everything again.



Screens nobody watches

One operator can follow a handful of feeds. A network of hundreds of cameras is, in practice, unwatched until someone asks for footage.



Investigations that take days

Finding a white van, a person or a moment across many cameras means scrubbing timelines by hand, camera by camera.



Analytics that lock you in

New cameras, one brand, a vendor gateway, per-camera monthly fees, and a roadmap you cannot influence.



Data that leaves your control

Cloud analytics send faces, plates and video to servers abroad, a real concern for government, defence and regulated sectors.

How the day changes

Moment	Today, with cameras only	With SENTINEL
Something happens	Seen only if an operator happens to be looking	Detected in seconds, ranked by severity, pushed to the right person
An alert fires	A beep and a camera number	An evidence frame, a short clip, an AI summary and three clear actions
Nobody responds	The alert is lost in the noise	Escalation: operator, then supervisor, then duty officer, until acknowledged
A complaint arrives	Hours or days of manual scrubbing	Plain-language search across cameras, a cross-camera timeline in minutes
Management asks what happened	Someone writes it up from memory	An AI incident report on your template, in Malay or English, with evidence hashes
The grass, the leak, the broken fence	Found when someone complains	Detected by the same cameras and sent as a work order

The SENTINEL approach

Keep the cameras, keep the recorders, keep the VMS. Add intelligence on top, on your own servers, and let every detector speak the same language, so one console, one rule engine, one search and one report engine work for all of them.

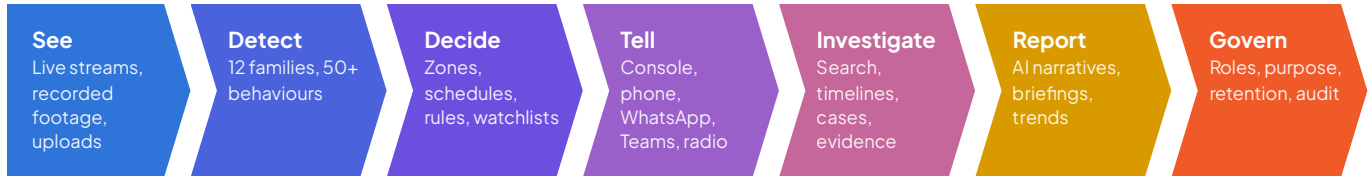


03 · PRODUCT OVERVIEW AND PRINCIPLES

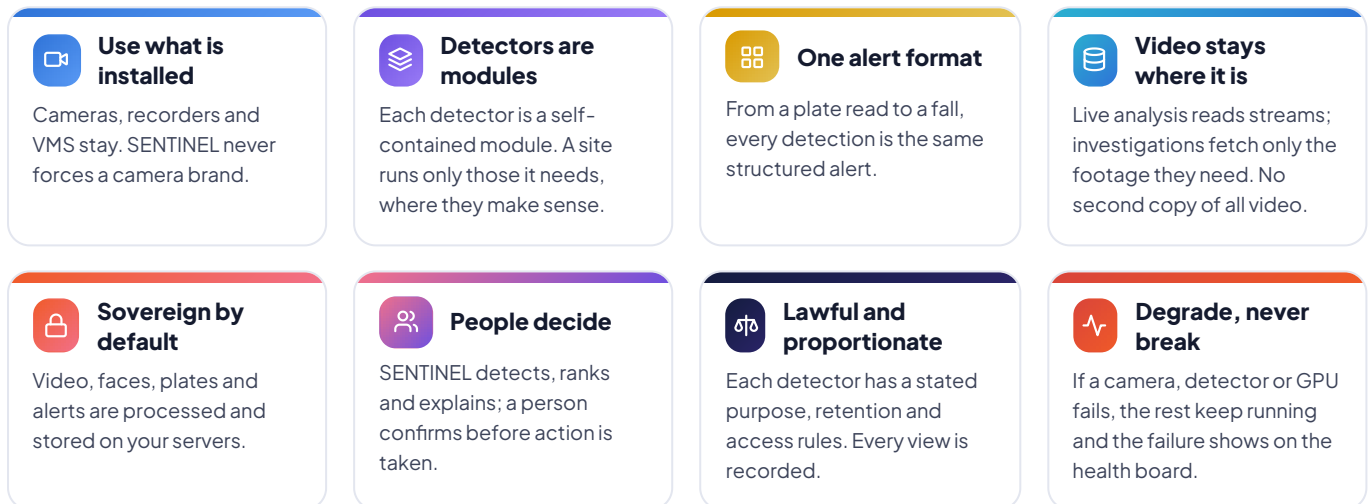
A set of services **beside** TERAS

Operators use the SENTINEL console in a browser, on a video wall or on a phone. Other systems use the SENTINEL API and its MCP tools, and TERAS models and agents can call SENTINEL to look, search and report.

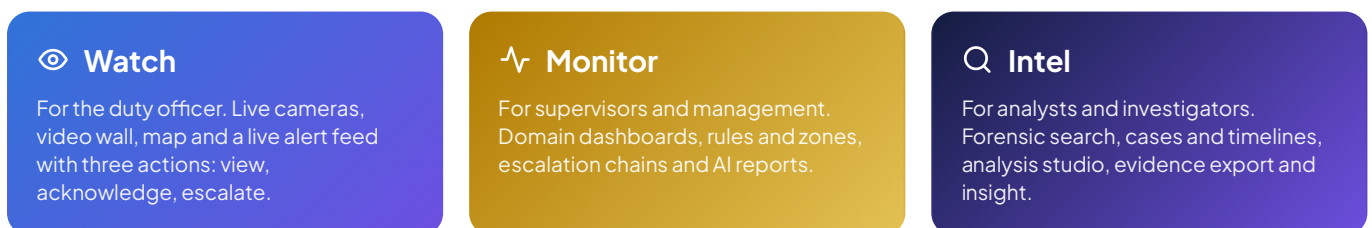
What SENTINEL does, end to end



Eight design principles



Three modes, three audiences





04 · ARCHITECTURE

A pipeline from pixels to decisions

Video comes in, the detector registry runs the right detectors on it, every result becomes one standard alert, and the three operating modes put those alerts to work. Reasoning — confirmations, summaries, reports and plain-language search — comes from TERAS.

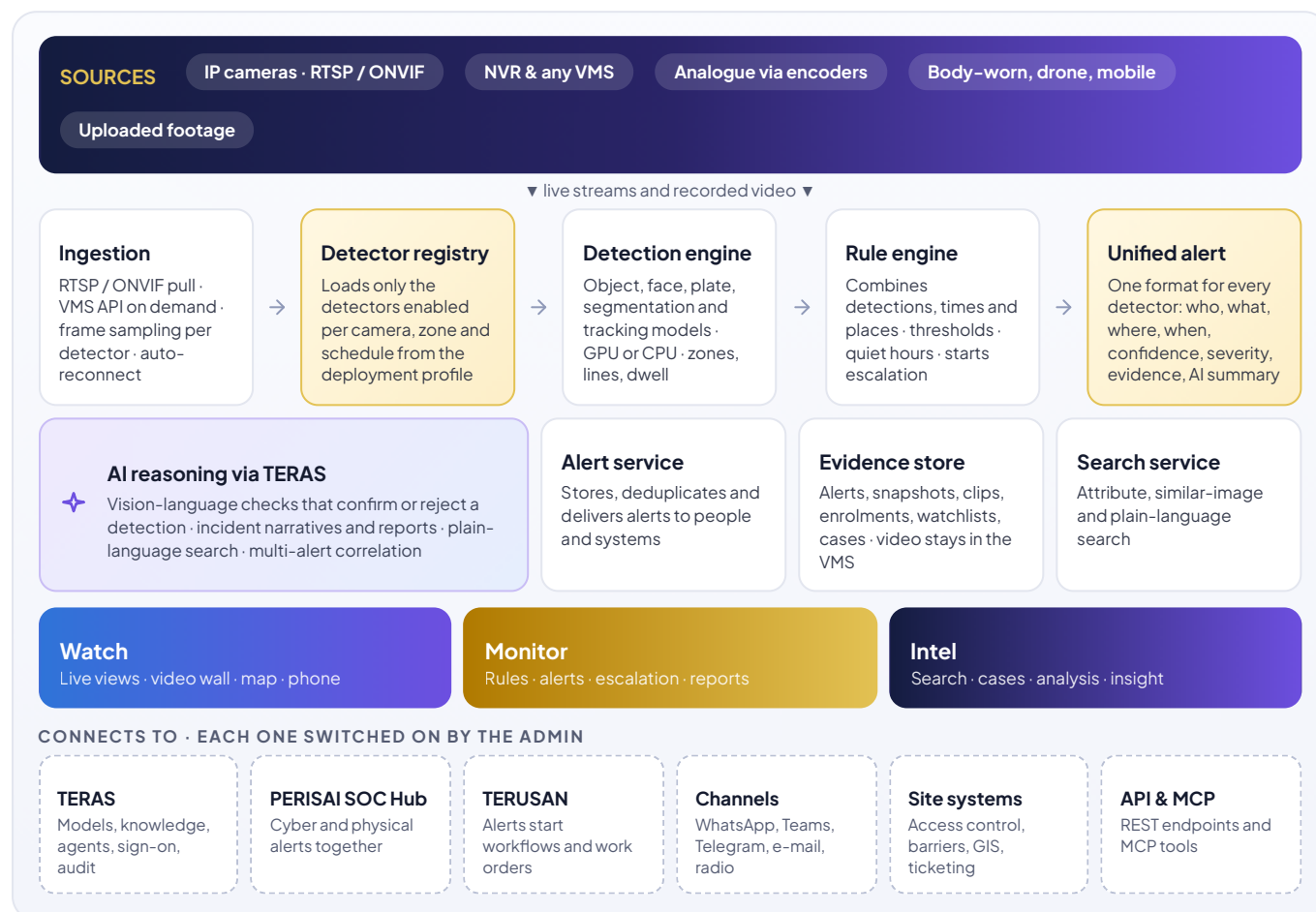


Figure 1 · SENTINEL architecture. Gold marks the parts that make SENTINEL modular; dashed boxes are connected systems.

Component	Responsibility
Ingestion	Connects to cameras over RTSP and ONVIF, to VMS and NVR APIs and to uploaded files; samples frames at a rate set per detector; reconnects automatically and reports camera health
Detector registry	Loads the detectors enabled in the site's deployment profile, per camera, zone and schedule; a new detector is a module dropped into the registry
Detection engine	Runs detection, recognition, segmentation and tracking models on GPU or CPU; applies zones, line crossings and dwell times; tracks objects across frames and cameras
Rule engine	Combines detections into events (for example, a vehicle not on the allow list at the gate after 11 pm), applies thresholds, severities and quiet hours, and starts escalation
Alert, evidence and search	Stores every alert with its evidence, deduplicates repeats, delivers to people and systems, and indexes attributes and visual features for search
Report engine	Asks TERAS models to write incident narratives, shift summaries and investigation reports from structured alerts, on the organisation's templates
Console, API and MCP	Watch, Monitor and Intel in the browser, on video walls and on phones; every capability as REST endpoints and MCP tools



05 · THE UNIFIED ALERT AND INTEGRATION PATHS

Every detector speaks the same language

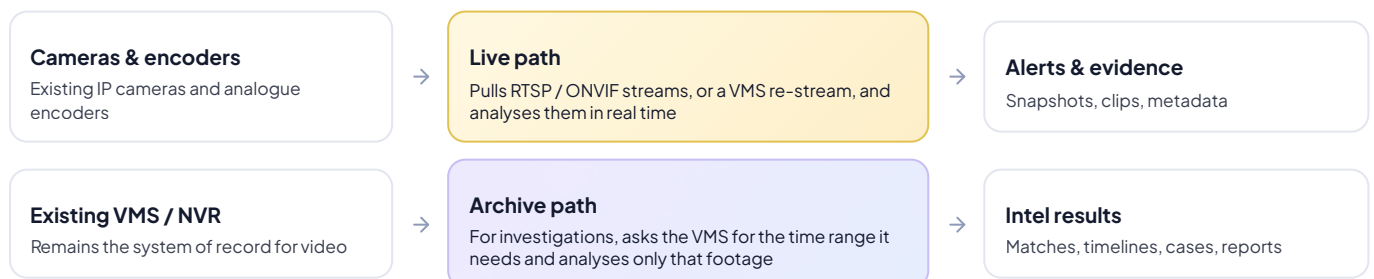
Every detector, on every camera, produces the same structured alert. That single decision is what lets one console, one rule engine, one search and one report engine serve every detector without special cases.

```
{
  "alert_id": "a1_7f3c2e91",
  "timestamp_local": "2026-06-30T00:28:14+08:00",
  "camera_id": "LOBBY-01", "zone": "A · dining",
  "detector": "person.fall",
  "category": "safety",
  "confidence": 0.84, "severity": "high",
  "track_id": 11, "bbox": [412, 233, 518, 401],
  "attributes": { "aspect_ratio": 1.93,
    "vision_check": "person on floor, not moving" },
  "evidence": { "snapshot": "ev/.../f.jpg", "clip": "ev/.../c.mp4",
    "sha256": "9b1e...c40a" },
  "purpose": "occupant safety",
  "ai_summary": "A person fell near table 3 and has not moved for 40 s",
  "status": "assigned", "assignee": "patrol-2"
}
```

An alert as it leaves the alert service (abridged)

Field	Meaning
alert_id	Unique identifier
timestamp_utc / _local	When it happened, in UTC and the site's time zone
camera_id, zone	Where it happened
detector	Family and behaviour, e.g. person.fall, vehicle.wrong_way, plate.watchlist
category	Security, safety, facilities, environment or operations
confidence, severity	How sure the detector is (0–1) and the site's severity rule
bbox, track_id	Where in the picture, and the object's track across frames and cameras
attributes	Detector-specific details: plate text, vehicle colour and type, face match and score
evidence	Snapshot and clip references with integrity hashes
purpose	The stated purpose of the detector that raised it
description, ai_summary	Short machine description and the AI-written narrative
status	New, acknowledged, assigned, resolved or false alarm — with who and when

Two paths, no duplicate video storage



The same detectors serve both paths, so moving a site from recorded-footage analysis to live operation changes only the input — and the VMS remains the single system of record for video.



06 · DETECTION MODULES

Twelve families, fifty-plus behaviours

Detectors are grouped in families. Each family offers several behaviours, and each behaviour is enabled per camera, zone and schedule with its own thresholds. A site runs only what it needs.

Person

Presence and counting, zone intrusion, line crossing, loitering, running, falls, tailgating, crowding and density, wrong-way movement

📍 Entrances, perimeters, corridors, halls, wards

Face

Detection, recognition against enrolled people, watchlist matches, unknown-person alerts, privacy blurring of everyone else

📍 Entrances, lobbies, checkpoints

Licence plate (ANPR)

Plate reading in Malaysian formats, allow lists and watchlists, entry and exit logs, dwell time

📍 Gates, car parks, roads

Vehicle

Type and colour, counting and flow, illegal parking, wrong way, stopped vehicles, speed estimate

📍 Roads, junctions, car parks, loading bays

Object

Abandoned or removed objects, suspicious items, waste and illegal dumping, overflowing bins, blocked exits

📍 Lobbies, public areas, roadsides

Animal

Intrusion and damage by monkeys, stray dogs, wild boar and snakes; counts by species

📍 Campuses, housing, plantations

Vegetation

Grass and hedge height, overgrowth onto walkways, fallen trees and branches

📍 Grounds, roadsides, parks

Structural

Cracks, damage, leaks and flooding, fallen ceilings, broken fences and barriers

📍 Buildings, drains, perimeters

Fire and smoke

Flames and smoke indoors and outdoors, open burning — from camera video alone

📍 Labs, kitchens, stores, open land

Education

Exam-hall integrity (phones, unusual movement, seat changes), attendance counts, room occupancy

📍 Exam halls, lecture rooms

Safety and PPE

Helmets, vests and other protective equipment, people near moving machines, restricted-area entry

📍 Factories, sites, plants

Camera health

Camera offline, blocked, moved, out of focus or tampered with

📍 Every camera

Attendance from the same cameras

Once people are enrolled with consent, face recognition at chosen entry points logs arrival, departure and time on site, replacing manual registers and stopping proxy attendance — no new hardware.

Built for local conditions

Malaysian plate formats, wildlife that actually visits Malaysian sites, monsoon flooding, grounds that grow fast, and reports in Bahasa Melayu as well as English.



06 · DETECTION MODULES

How detection actually works

Speed where it is needed, understanding where it matters. Fast models screen every frame; reasoning is spent only on the frames that need it, which keeps hardware modest and false alarms low.



1 · Fast models first

Specialised detection, recognition, plate-reading and segmentation models run on every sampled frame, on GPU or CPU.



2 · Reasoning second

Where a frame needs understanding — is this person in distress? smoke or steam? — SENTINEL asks a vision-language model through TERAS to confirm.



3 · Tracking across time

Objects are tracked across frames, so dwell, loitering, direction and abandonment are measured, not guessed. Re-identification follows a person or vehicle across cameras.



4 · Tuned per site

Thresholds, zones and schedules are set per camera. Detectors can be fine-tuned on the site's own footage with S.A.L.T CI training tools.

A vision check that cuts false alarms



Detector · possible flame, confidence 0.41

Vision check via TERAS · “Sun glare on a windscreen. No flame or smoke visible.”

Result · alert suppressed, recorded as a rejected detection for tuning

Illustrative: a low-confidence flame detection checked by a vision-language model before anyone is alerted.

Adding detectors

A new detector is a module that registers with the detector registry and returns the unified alert. It appears in the console, rules, search and reports at once. S.A.L.T CI and its partners add detectors for new sectors; an organisation's own developers can add theirs with the SENTINEL detector kit.

Sampling per detector

Typical

Licence plate, tailgating

5–10 fps

Person, vehicle, falls

2–5 fps

Object, animal, fire

1–2 fps

Vegetation, structural

every few minutes

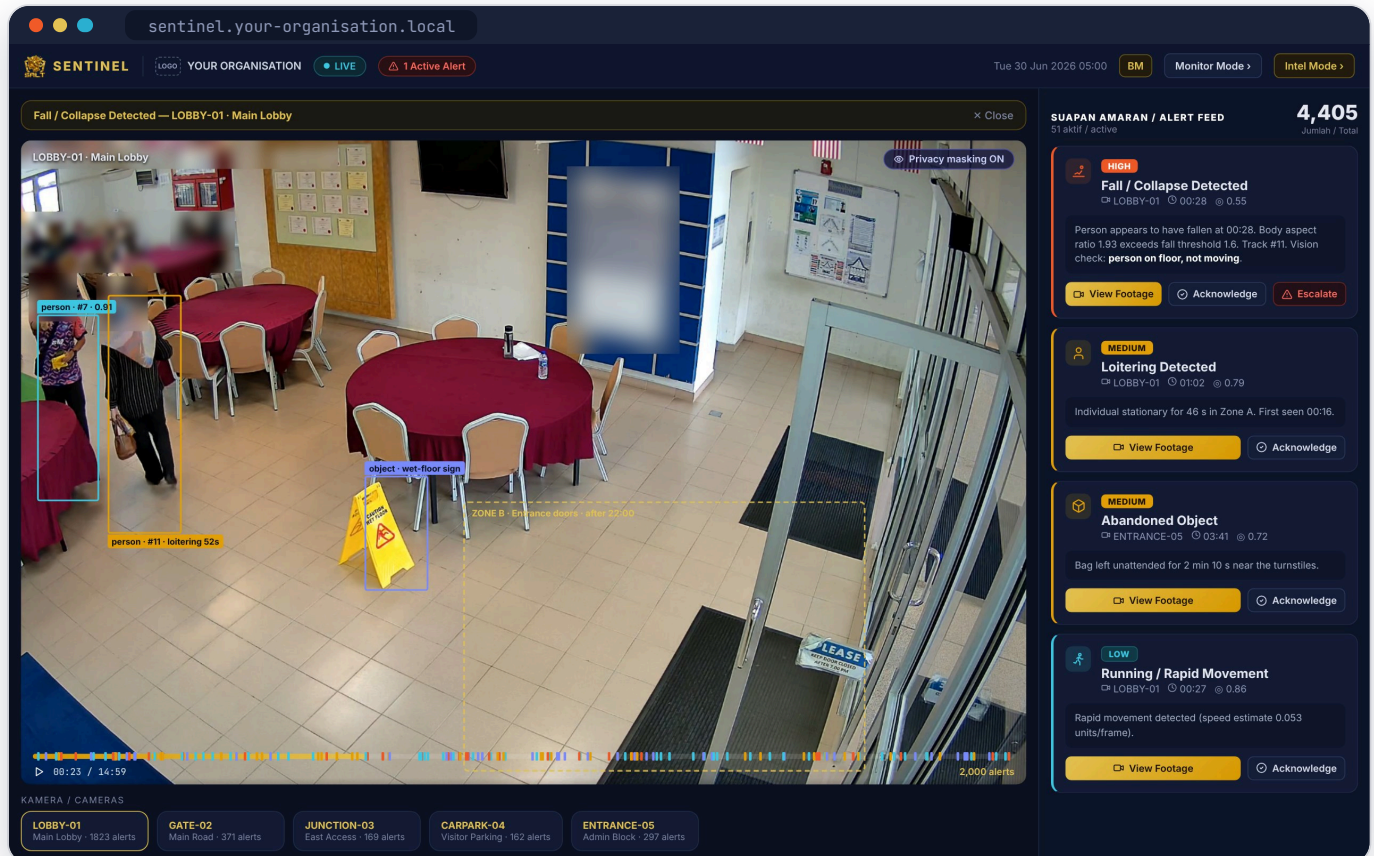
Set per site; one GPU serves many cameras because each detector reads only the frames it needs.



07 · WATCH MODE

The duty officer's console: see it, act on it

Large, clear alert cards. Three actions only: view footage, acknowledge, escalate. Bilingual in Bahasa Melayu and English, on any screen from a control-room wall to a tablet, with a PIN gate in front of deeper analysis.



Watch mode - a fall detected in the main lobby, with tracks, zones and privacy masking drawn on the live picture



Detections on the picture

Boxes, track IDs, zones and lines drawn live, so the operator sees why an alert fired, not just that it did.



A feed that ranks itself

High first. Every card carries an evidence frame, a short clip, the confidence and an AI summary in plain words.



One click, recorded

Acknowledge, assign, escalate or mark as a false alarm. Every action is logged, and false alarms tune the thresholds.



Bahasa Melayu · English

One toggle switches every label, alert and summary, so each officer works in the language they think in.



PIN-gated depth

Duty officers stay in Watch; moving into Monitor or Intel needs a PIN or the right role, and the switch is audited.



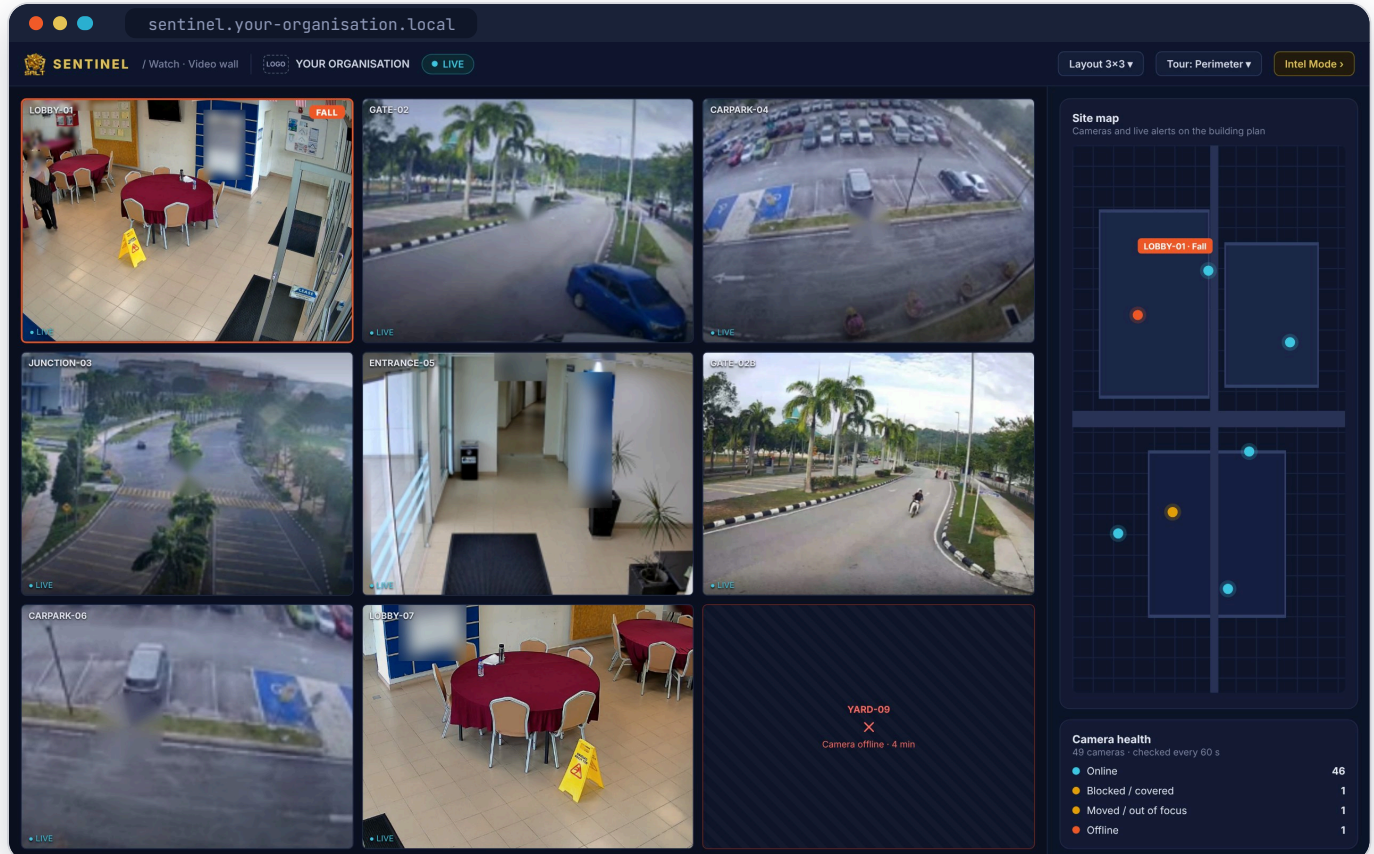
Any screen

Control-room wall, desktop, tablet or phone — the same console, laid out for the screen it is on.

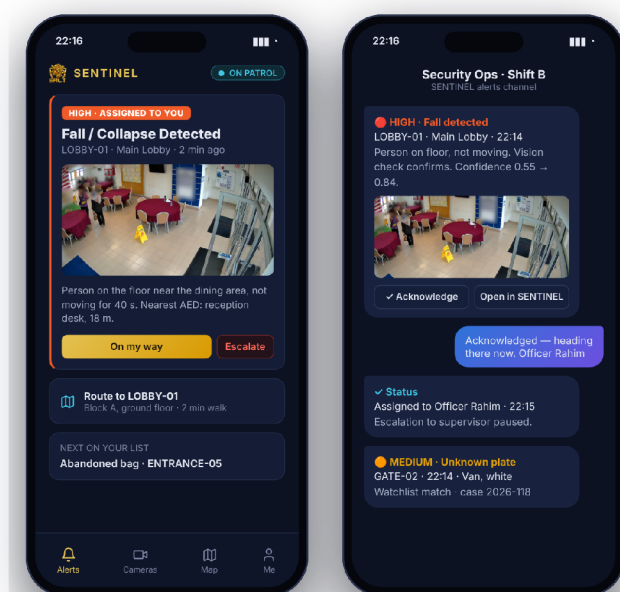
07 · WATCH MODE

From the control room to the patrol officer

Camera grids, tours and video-wall layouts for the control room; a site map and camera-health board so nothing silently goes dark; and a phone view that puts the alert, the evidence and the route in a patrol officer's hand.



Video wall with site map and camera health · an offline camera is flagged within the minute



Alerts that reach people where they are

- **Patrol app** — assigned alerts with evidence frame, AI summary, route and the next task on the list.
- **Channels** — the same alert in WhatsApp, Microsoft Teams, Telegram, e-mail or radio dispatch, with acknowledge and open-in-SENTINEL actions.
- **Closed loop** — acknowledging on the phone pauses escalation and updates every console in the room.
- **Map view** — cameras and live alerts on building plans or GIS maps for campus and city views.

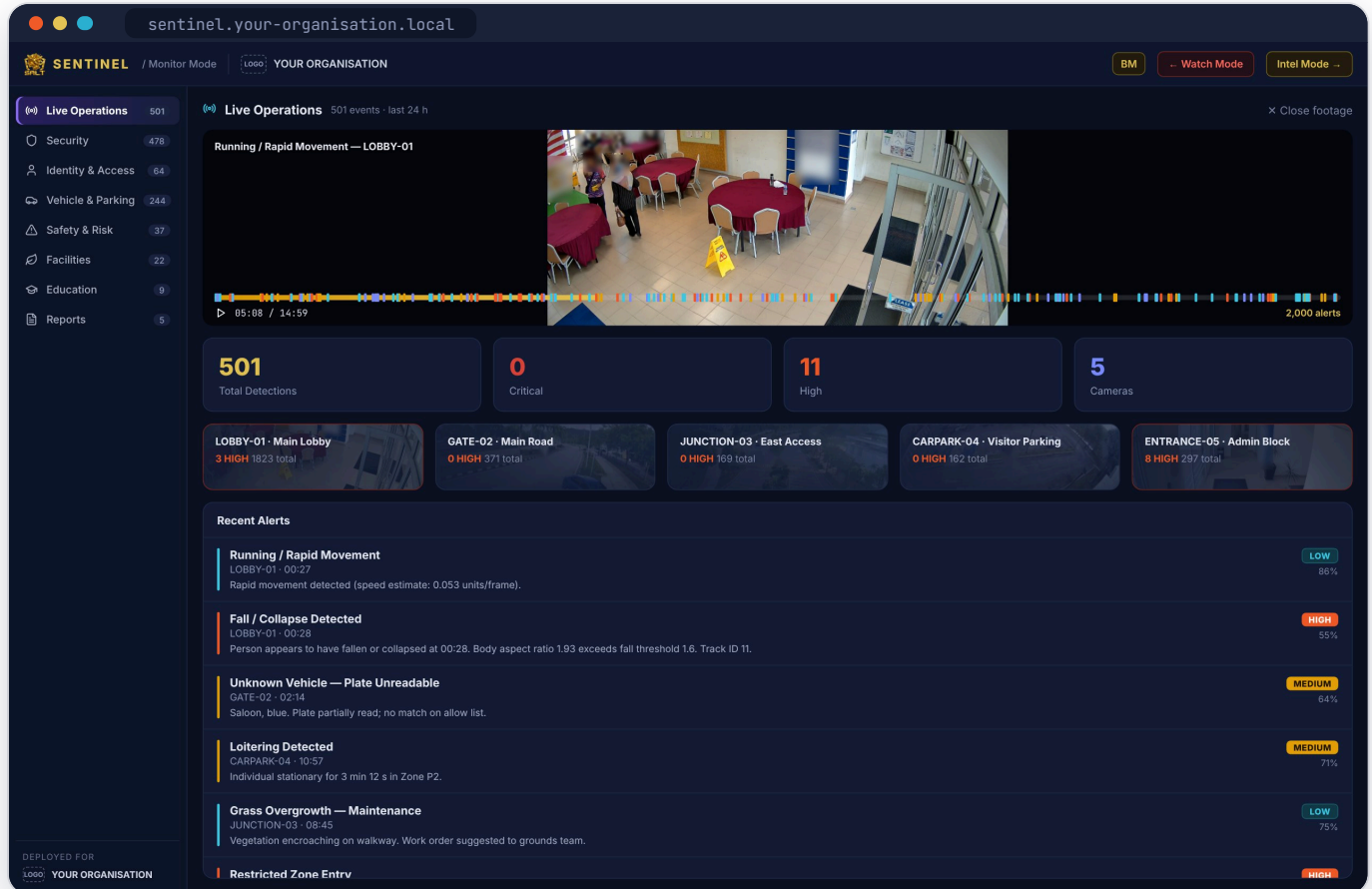
Camera health board: offline, blocked, moved, out-of-focus or tampered cameras are shown at once, and can raise their own alerts.



08 · MONITOR MODE

For supervisors: the whole site by domain

Monitor mode organises everything SENTINEL sees into domain dashboards, each filtered to what that team cares about, so security, facilities, safety and management each get their own view of the same cameras.



Monitor mode · Live Operations, with per-camera severity and recent alerts

Eight domain modules

Live Operations

Security

Identity & Access

Vehicle & Parking

Safety & Risk

Facilities

Education

Reports

Domain, not camera

Facilities sees the grass, the leaks and the animals; security sees intrusions, plates and faces; safety sees falls, fire and PPE. One deployment, many teams.

Counts that mean something

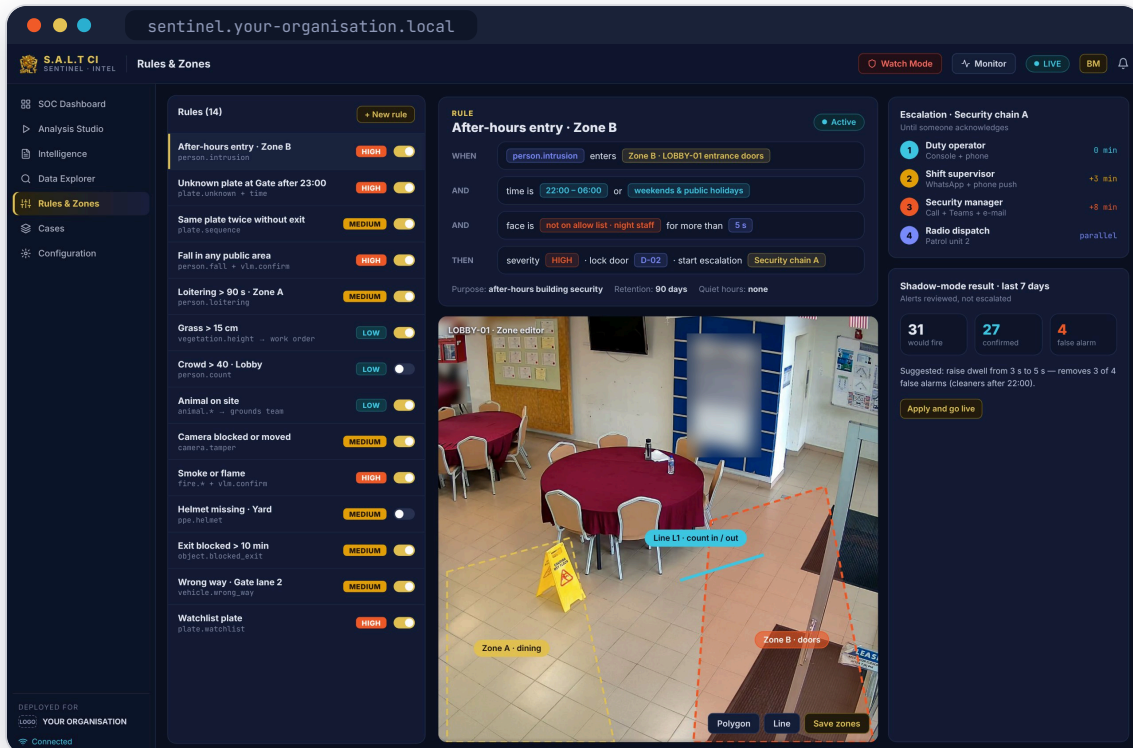
Totals by severity and by camera, hotspots and peak hours, so supervisors see where attention is needed before they open a single clip.



08 · MONITOR MODE

Rules, zones and escalation that fit the site

Draw zones and lines on each camera, combine detectors with places and times, decide who hears about it and in what order, and prove the rule in shadow mode before it ever wakes anyone up.



Rules & Zones : a rule that combines a zone, a schedule and an allow list, with its escalation chain and shadow-mode result



Zones and lines

Restricted areas, gate lines, counting lines and no-parking boxes drawn on each camera.



Rules that combine

“Person in the substation zone outside working hours” or “same plate entering twice without leaving”.



Escalation chains

Operator, then supervisor, then duty officer, by console, phone, WhatsApp, Teams, e-mail or radio, until acknowledged.



Noise control

Repeats are grouped into one alert; every false-alarm mark feeds threshold tuning; quiet hours per detector.

Rules people actually write

Rule	Detectors combined	Typical action
Vehicle not on the allow list at the gate after 23:00	plate.unknown + time window + camera	Gate officer, then supervisor
Same plate entering twice without leaving	plate.sequence across entry and exit cameras	Flag for investigation
Person in the substation zone outside working hours	person.intrusion + zone + schedule + allow list	High alert, lock door, radio
Person near a moving forklift without a vest	ppe.vest + vehicle.forklift + proximity	Supervisor and siren
Fall in a ward, confirmed by vision check	person.fall + vlm.confirm	Nurse station and phone



08 · MONITOR MODE

Reports written for you, not by you

The report engine asks TERAS to turn structured alerts into a written account: what happened, where, when, how sure the system is, and what to do next — per camera, per shift, or across the whole site, on the organisation's own template.

The screenshot displays the S.A.L.T SENTINEL Monitor Mode interface. The top navigation bar includes the S.A.L.T SENTINEL logo, the text 'Monitor Mode', a user profile icon, and the text 'YOUR ORGANISATION'. On the right, there are buttons for 'BM', 'Watch Mode', and 'Intel Mode'. The left sidebar lists various categories: Live Operations (501), Security (478), Identity & Access (64), Vehicle & Parking (244), Safety & Risk (37), Facilities (22), Education (9), and Reports (5). The main content area is titled 'Reports 501 events' and features a 'Generate Master Site Report' button, along with 'Shift summary' and 'Weekly briefing' tabs. The report itself is titled 'Master Site Intelligence Report' and includes a 'Download PDF' button. The report content is structured as follows:
SITE-WIDE EXECUTIVE SUMMARY: Analysis of five cameras across the site over the reporting window produced 2,822 alerts. The dominant categories are unknown-face detections, loitering and unreadable vehicle plates. The cumulative risk is assessed as MEDIUM, with two items requiring follow-up today.
CROSS-CAMERA FINDINGS: Unknown-face detections account for 1,328 alerts, largely because no faces are yet enrolled. 244 vehicle detections had partly read or unreadable plates. The system also recorded 124 loitering events, 39 grass-overgrowth alerts and 21 vegetation-encroachment alerts, which point to grounds maintenance rather than security risk.
HIGHEST PRIORITY INCIDENTS: LOBBY-01 raised the most alerts (1,823), including one fall at 00:28 confirmed by a vision check and repeated loitering near the entrance doors. ENTRANCE-05 recorded eight high-severity events, including after-hours entry into Zone C.
RECOMMENDED ACTIONS: 1. Enrol staff faces and the vehicle allow list to remove most unknown-face and unknown-vehicle noise. 2. Raise the loitering threshold in Zone A to 90 s during lunch hours. 3. Raise a grounds work order for JUNCTION-03. 4. Review the Zone C entry at 23:12 with the duty supervisor.
Below the report, there are five summary cards:
- LOBBY-01 - Main Lobby: 1823 detections · 25 Jun
- GATE-02 - Main Road: 371 detections · 25 Jun
- JUNCTION-03 - East Access: 169 detections · 25 Jun
- CARPARK-04 - Visitor Parking: 162 detections · 25 Jun
- ENTRANCE-05 - Admin Block: 297 detections · 25 Jun

Monitor mode · Master Site Intelligence Report generated from five cameras



Shift and daily summaries

Handover notes that write themselves, with the incidents that need follow-up at the top.



Weekly AI briefings

Trends, hotspots, peak hours, parking occupancy and recurring issues for management.



Bahasa Melayu or English

Every report in either language, on the organisation's template, with evidence frames and confidence.

Laporan syif · contoh ringkasan

"Sepanjang syif malam, 41 amaran direkodkan; dua memerlukan tindakan. Pada 00:28, seorang individu dikesan terjatuh di LOBBY-01 dan disahkan oleh semakan visual; peronda tiba dalam dua minit. Sebuah van putih dalam senarai pantau memasuki GATE-02 pada 09:14 — kes 2026-118 dibuka."

What every report carries

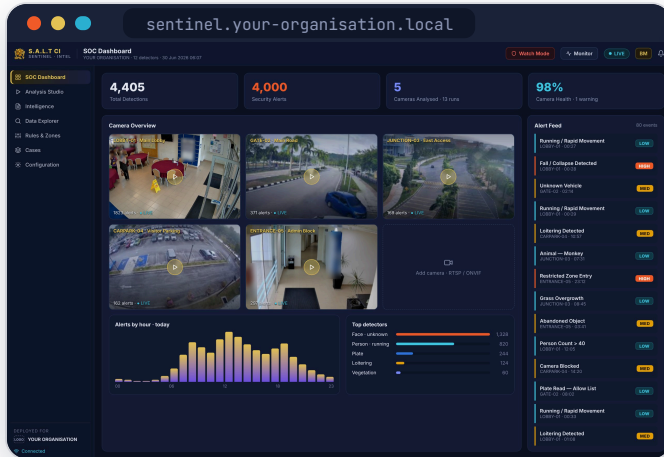
- Times, places and cameras, with evidence frames
- Detector confidence and vision-check outcome
- Risk assessment and recommended actions
- Evidence hashes for anything exported
- The organisation's logo, footer and template



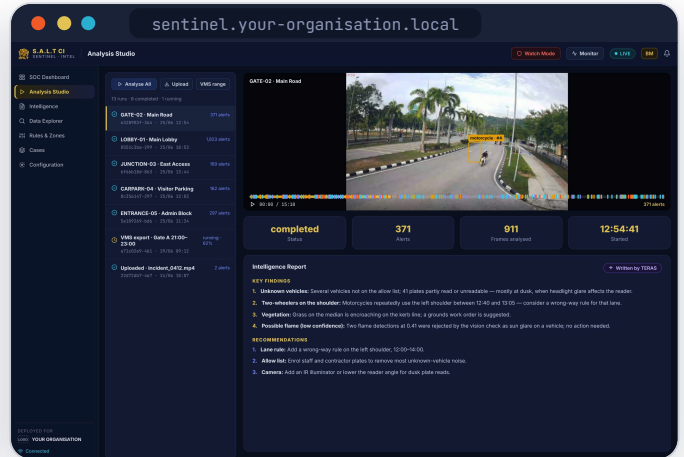
09 · INTEL MODE

For analysts: the investigation workspace

Intel mode is the analytical environment for security analysts and IT administrators: a SOC dashboard across all cameras, an analysis studio for recorded and uploaded footage, and AI intelligence reports for every run.



SOC Dashboard · camera overview, live alert feed and activity by hour



Analysis Studio · recorded, VMS-range and uploaded footage, with an AI report per run



Analyse any footage

Run detectors over a VMS time range, an export or an uploaded clip — the same detectors as the live path.



Insight over time

Counts, trends, heatmaps, peak hours and recurring hotspots across cameras and sites.



Per-run intelligence

Every analysis ends with findings, a risk assessment and recommendations written by TERAS.

Intel tool	What it does
SOC Dashboard	All cameras, live alert feed, activity by hour and top detectors, with camera health at a glance
Analysis Studio	Runs detectors over a VMS time range, an export or an upload; shows progress, alerts, frames analysed and the AI report
Data Explorer	Plate, face and alert explorers and subject trace, filtered by camera, zone, time and attributes
Cases	Timelines across cameras, notes and evidence, shared only with permitted colleagues
Intelligence	Per-camera and master reports with findings, risk assessment, recommendations and breakdowns

Built for the question “what happened?”

Most incidents are investigated after the fact. Intel mode is designed so that answering that question takes minutes: search, follow, assemble, report and export — without copying a week of video anywhere.



09 · INTEL MODE

Ask in plain language, follow across cameras

Type what you are looking for the way you would say it. SENTINEL turns the question into a structured search, finds matches across cameras, and helps build a case with a timeline, notes and sealed evidence.

The screenshot displays the S.A.L.T CI Intel Mode interface. At the top, the address bar shows 'sentinel.your-organisation.local'. The left sidebar contains navigation options: SOC Dashboard, Analysis Studio, Intelligence, Data Explorer, Rules & Zones, Cases (selected), and Configuration. The main area shows a search query: 'a white van at the main gate this morning after 9 am, and where it went'. Below the query, it states 'Understood as: vehicle.type=van · colour=white · camera=GATE-02 · 30 Jun 09:00-12:00 · follow across cameras · 4 cameras · 9 matches'. A 'Search' button is visible. The 'Matches' section displays four camera feeds: GATE-02 (09:14:33), JUNCTION-03 (09:16:02), CARPARK-04 (09:19:47), and ENTRANCE-05 (09:23:10). Each match includes a timestamp and a brief description. On the right, a 'CASE 2026-118 White van · repeat visit' is shown, with a timeline of events: 09:14:33 Enters at GATE-02, 09:16:02 Passes JUNCTION-03, 09:19:47 Parks at CARPARK-04 bay C12, 09:23:10 Person walks to Admin Block, and 09:51:05 Exits at GATE-02. Buttons for 'AI incident report' and 'Export evidence' are at the bottom.

Cases · a plain-language search, cross-camera matches and an investigation timeline



Attribute search

Person, vehicle type and colour, plate, face, object, camera, zone and time.



Plain-language search

"A white van at the main gate this morning after 9 am" — through TERAS.



Similar-image search

Start from a snapshot and find the same person or vehicle on other cameras.



Evidence export

Clips and frames exported with hashes, so they can be shown to be unchanged.

From question to sealed evidence

Ask

A question in plain words, or a snapshot

Find

Matches across cameras and time

Follow

Re-identify the subject camera to camera

Assemble

A case timeline with notes and evidence

Report

An AI incident report on your template

Export

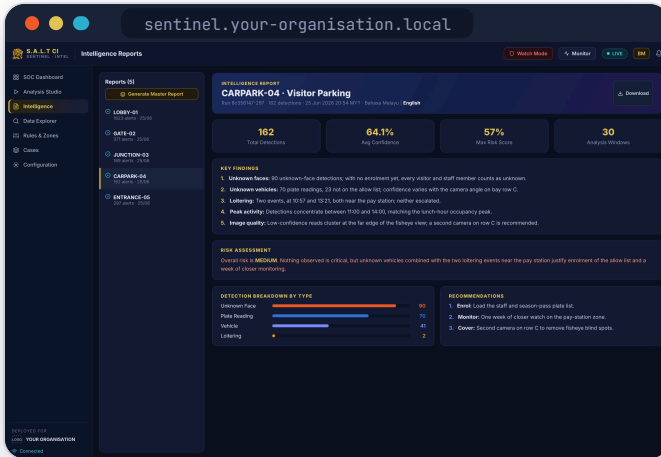
Clips and frames with SHA-256 hashes



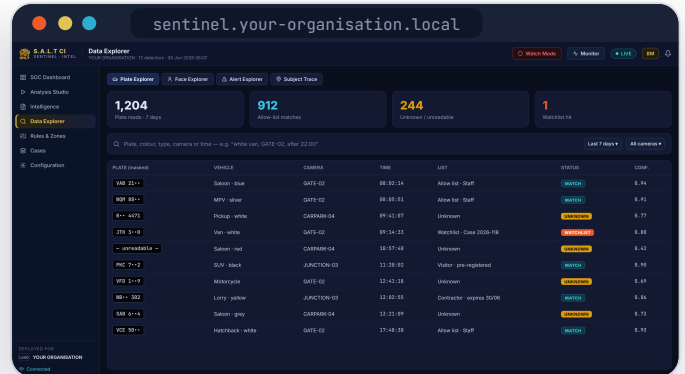
09 · INTEL MODE

Every detection, searchable and accountable

The Data Explorer gives authorised roles a direct view of plate reads, faces, alerts and subject traces, with masking applied by default. Each report can be read, downloaded and shared with permitted colleagues.

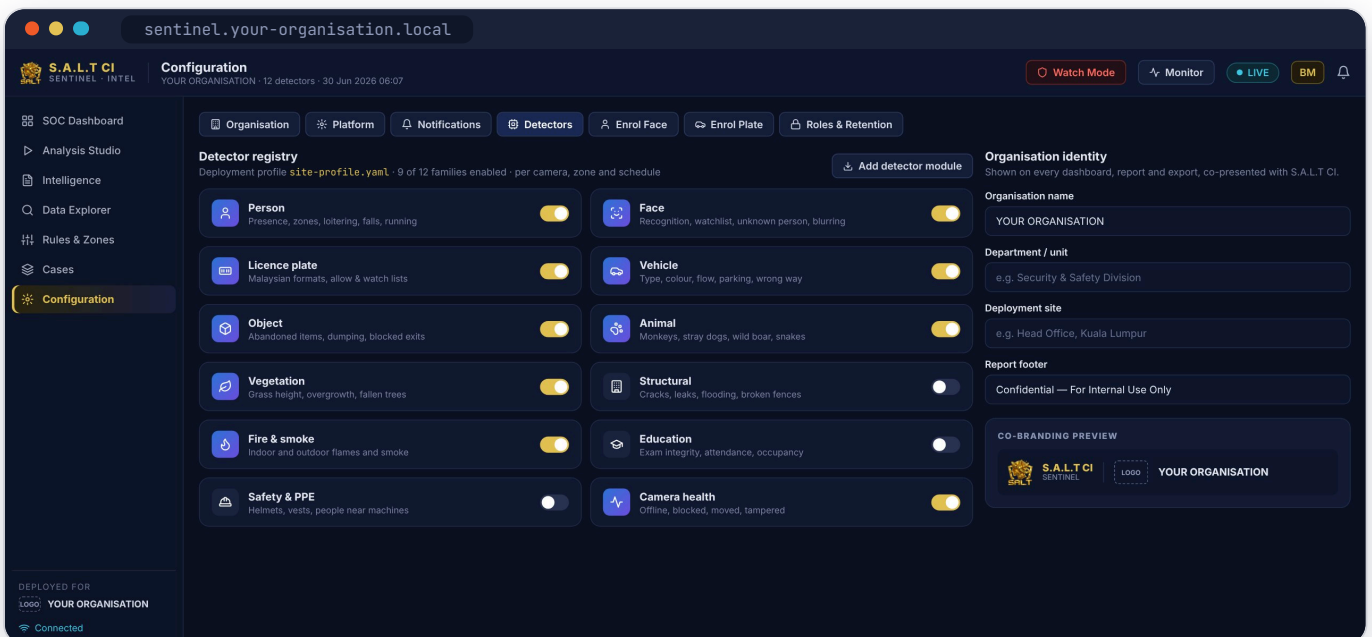


Intelligence report for one camera: findings, risk and breakdown



Data Explorer · plate reads, masked, with list status and confidence

Configured, branded and governed in one place



Configuration · the detector registry and the organisation's own identity, co-presented with S.A.L.T CI



10 · INDUSTRY SOLUTIONS

One product, configured for every sector

Any organisation that runs a camera network and needs it to do more than record. The detectors, rules and reports differ by site; the product does not.



Universities & schools

Campus safety, gates and parking, hostels, exam halls, wildlife, grounds upkeep, attendance

Person · face · plate · animal · vegetation · education



Local authorities

Public CCTV, traffic and junctions, parking enforcement, markets, illegal dumping, flood points

Vehicle · plate · object · structural · crowd



Police, defence & security

Perimeters, checkpoints, watchlists, cross-camera investigations, air-gapped command rooms

Face · plate · person · vehicle · object



Factories & plants

Safety zones, PPE, forklifts near people, fire and smoke, restricted areas, loading bays

Person · PPE · vehicle · fire · object



Critical infrastructure

Substations, water plants, ports and airports; intrusion and camera tampering

Person · vehicle · fire · structural · camera health



Commercial & retail

Access, occupancy and queues, after-hours intrusion, incident evidence for claims

Person · face · crowd · object



Hospitals & care

Falls, wandering, restricted wards, car parks, visitor flow

Person (fall, loitering) · face · plate



Estates & townships

Guardhouses, visitor plates, perimeter fences, common areas, stray animals

Plate · person · animal · structural

Three scenarios



A plant at 2 am

A person enters the press-line zone without a helmet while the line runs. SENTINEL raises a high alert, the supervisor's phone rings, and the morning report records it with the clip.



A council junction

A lorry stops on a yellow box during rush hour and rubbish is left by the roadside. Traffic sees the first; TERUSAN opens a work order for the second.



A campus car park

A plate on the watchlist enters at 22:14. The gate officer is told, the vehicle is followed across three cameras, and an evidence pack is sealed for the police.



11 · INTEGRATION

Fits the systems **you already run**

SENTINEL is a good neighbour. It reads from what is there, writes to where people already work, and exposes every capability as REST endpoints and MCP tools so other applications and AI agents can use it.



System	How SENTINEL works with it
Cameras	Any IP camera with RTSP; ONVIF Profile S and T for discovery and control; analogue cameras through encoders; body-worn, drone and mobile feeds
VMS and NVR	Direct RTSP, VMS re-streams, or the VMS's own API for recorded footage — common VMS and NVR products, without replacing them
TERAS	AI models for summaries, reports and search; vision-language checks; single sign-on, roles and audit; site procedures; agents that call SENTINEL tools
PERISAI SOC Hub	Physical alerts beside cyber alerts for one security picture, with correlated incidents (a badge used at one door while a camera sees a stranger at another)
TERUSAN	Alerts start workflows: a fallen tree becomes a grounds work order, a broken fence a maintenance ticket, a watchlist match a security procedure
Access control and barriers	Open a barrier for an allowed plate, lock a door on an intrusion, or log a mismatch between a badge and a face
Monitoring and other systems	Camera, detector and server health to Quantum Quill (Zabbix); signed webhooks and REST for ticketing, records and command-centre systems



12 · PRIVACY, ETHICS AND COMPLIANCE

Powerful enough to matter, governed enough to trust

Surveillance touches people's rights. SENTINEL is designed so that an organisation can use it lawfully and proportionately — and show that it does.



Purpose per detector

Each detector is enabled with a stated purpose and scope (cameras, zones, hours); the purpose is shown on every alert it raises



Data stays on site

Video, faces, plates and alerts are processed and stored on the organisation's servers; air-gapped operation is supported



Least access

Roles decide who may see live video, faces, plates, search results and exports; sensitive views can require a reason



Privacy masking

Faces of people not on a watchlist, windows of private property and screens can be blurred in live view and exports



Retention

Separate retention periods for alerts, snapshots, clips, enrolments and cases, with automatic deletion



Human decision

Face and plate matches show the evidence and score; acting on a match requires a person's confirmation



Accountability

Every view, search, export and change is recorded in a tamper-evident audit log



Enrolment control

Faces and plates are enrolled only by authorised roles, with a reason and an expiry; individuals can be removed on request



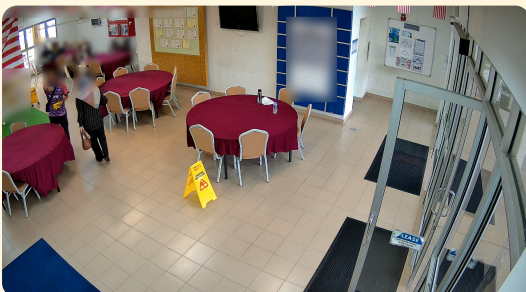
Accuracy checks

Detector accuracy is measured on the site's own footage before go-live and reviewed regularly, including false-match rates

PDPA-aligned by design

SENTINEL supports compliance with Malaysia's Personal Data Protection Act and the organisation's own security and privacy policies. The organisation remains responsible for how it uses the system; S.A.L.T CI provides a data-protection checklist for every deployment.

What privacy looks like on screen



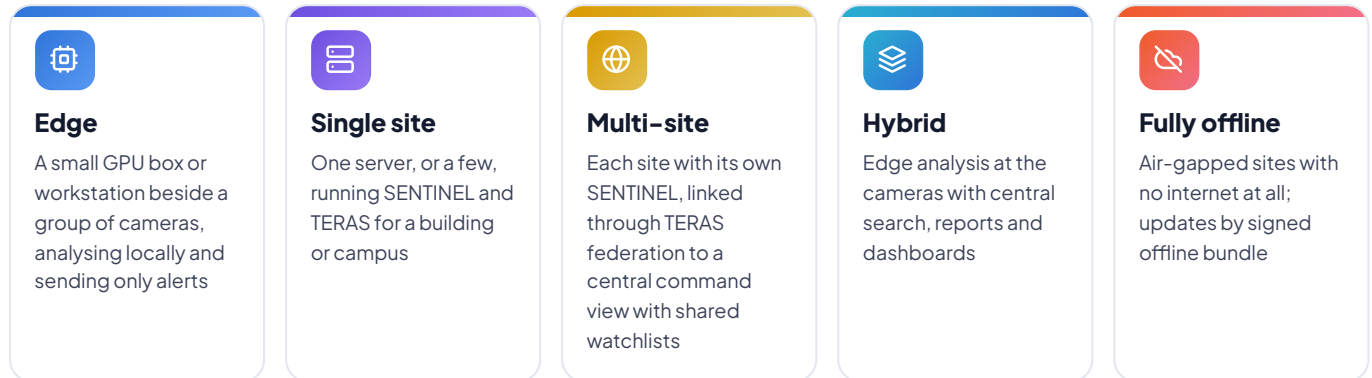
In this brief, every screen runs with privacy masking on: bystanders' faces and identifying signage are blurred, plates are partly masked, and only enrolled or watchlisted subjects would be shown in full — to the roles allowed to see them, with the view itself written to the audit log.



13 · DEPLOYMENT AND SIZING

Runs on **your infrastructure**, at your scale

SENTINEL is not tied to any camera brand, server or GPU. It adapts to the site's infrastructure and grows with it — on bare metal, virtual machines, private or public cloud, or Kubernetes.



Sizing, the simple way

Capacity depends on the number of cameras, the detectors on each, the frame rate analysed and the resolution. Because SENTINEL samples frames per detector — a plate reader needs more frames than a vegetation check — one GPU serves many cameras.



Scale	Cameras	Typical hardware
Small	Up to 50	One server with one GPU, or CPU only for light detectors
Medium	50–500	A few GPU servers or edge boxes, plus TERAS for reporting and search
Large	500+	GPU clusters or edge fleets across sites, with central search and command view through TERAS federation

Hardware-agnostic

NVIDIA, AMD and Intel GPUs, Apple silicon and CPUs, on x86 or ARM. The organisation can use servers it already owns.

Camera considerations

Most existing cameras work. Accuracy improves with 1080p or better, good night vision and angles chosen for analysis; the site assessment identifies any camera worth repositioning or upgrading.



14 · FROM ASSESSMENT TO GO-LIVE

Proven on your footage **before it goes live**

Every deployment follows the same path: measure on the site's own video first, tune in shadow mode, and switch on escalation only when the alerts are worth acting on.

1 Site assessment

Camera inventory, stream checks, sample-footage analysis and detector accuracy on the site's own video

2 Install

Containers beside TERAS on the site's servers or edge boxes; one script detects GPUs and starts the services

3 Connect cameras

Discover ONVIF cameras or add RTSP addresses; import a camera list from the VMS

4 Configure

Deployment profile per site: detectors per camera, zones, schedules, thresholds, watchlists, escalation

5 Shadow mode

Alerts reviewed but not escalated; thresholds tuned against real activity

6 Go live

Escalation switched on; Watch, Monitor and Intel users trained

7 Operate

Health board, accuracy reviews, false-alarm feedback, monthly AI briefings

An honest note on accuracy

Any AI surveillance system, SENTINEL included, starts noisy on a cold deployment: default thresholds, cameras placed for human viewing, older codecs and nobody enrolled yet.

That is why SENTINEL measures accuracy on the site's own footage, tunes thresholds per camera and zone, enrolls the allow lists, and agrees an accuracy target per detector before go-live — then keeps measuring.

Operations, built in

- Signed update packages, online or offline
- Detectors updated independently of the platform
- Alerts, enrolments, cases and settings in TERAS encrypted backups
- Camera, detector and server health to the monitoring stack

Ways to buy

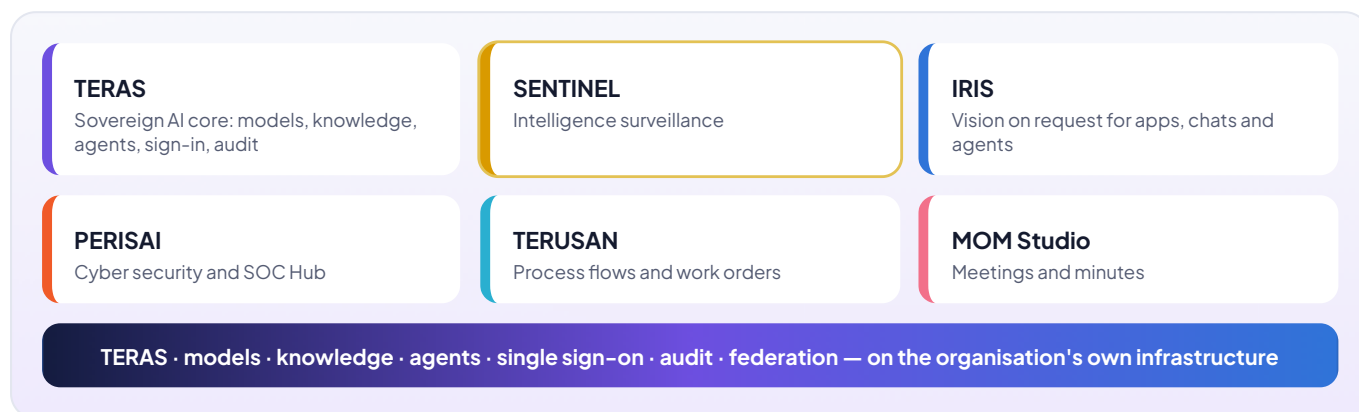
A site licence the organisation owns, sized by cameras and detector families, with annual support and updates. Delivered directly or through authorised S.A.L.T CI partners, with white-label rights under the S.A.L.T CI Framework agreement. No per-camera cloud fees.



15 · PART OF THE S.A.L.T CI PLATFORM

One sovereign core, many intelligent applications

SENTINEL is one of the S.A.L.T CI intelligence applications built on TERAS. It shares TERAS's sign-in, models, knowledge, audit and infrastructure — so a site that runs SENTINEL already has the core for the rest.



SENTINEL and IRIS

	IRIS	SENTINEL
Job	Answer a question about an image or clip	Watch a camera network and manage what it sees
Input	A picture, capture or clip, on request	Continuous camera streams and recorded footage
Output	A description, an analysis, an answer	Alerts, cases, reports, statistics
Users	People in chats, apps and agents	Security, facilities and operations teams

SENTINEL uses IRIS-style vision-language checks through TERAS when a detection needs understanding, not just recognition.

Open-source foundations

SENTINEL's platform — ingestion, registry, rule engine, alert service, search, reports, console and API — is written by S.A.L.T CI. It uses established open-source components, each under its own licence and listed in the product's NOTICE file. Detector models can be swapped for alternatives with other licences where a deployment requires it.

Component	Used for	Licence
Ultralytics YOLO	Object, person, vehicle, fire and plate-region detection	AGPL-3.0, or Ultralytics Enterprise licence for closed distribution
DeepFace	Face detection and recognition	MIT (face models carry their own licences)
EasyOCR	Plate and text reading	Apache-2.0
OpenCV	Video and image processing	Apache-2.0
PyTorch	Model runtime	BSD-style
FFmpeg	Stream and file decoding	LGPL
FastAPI, Uvicorn	Services and API	MIT / BSD



16 · WHY SENTINEL

What other approaches **leave out**

SENTINEL compared with the common ways organisations add intelligence to CCTV. Categories describe typical offerings; individual products differ.

Capability	Cloud video analytics	Analytics in the VMS	AI cameras	S.A.L.T SENTINEL
Works with existing cameras of any brand	◀ often needs a gateway	◀ within that VMS	— new cameras	✓
Video and detections stay on site	—	✓	◀ varies	✓
Runs fully air-gapped	—	◀ varies	◀ varies	✓
Many detector families, per camera and zone	◀ varies	◀ varies	◀ per camera model	✓
One alert format and console for all detectors	◀ varies	◀ varies	—	✓
AI-written incident reports in Malay and English	◀ some	—	—	✓
Plain-language search of footage	◀ some	◀ some	—	✓
Vision-language checks to cut false alarms	◀ some	—	—	✓
Workflows, work orders, cyber-physical correlation	◀ integrations	◀ some	—	✓ TERUSAN, PERISAI
Add new detectors for local needs	◀ vendor roadmap	◀ some	—	✓ detector kit
No per-camera cloud subscription	—	◀ varies	✓	✓
Same platform reused for other AI applications	—	—	—	✓ TERAS

✓ included · ◀ partly, or depends on the product or add-ons · — not typical

Glossary

Term	Meaning
Detector	A module that finds one family of things or behaviours in video
Detector registry	The part of SENTINEL that loads and runs the detectors enabled for each camera
Deployment profile	A site's configuration: cameras, detectors, zones, schedules, thresholds, watchlists
Unified alert	The single structured format every detection becomes
Zone / line	An area or line drawn on a camera view that rules refer to
Watchlist / allow list	Enrolled faces or plates that raise, or suppress, alerts
ANPR	Automatic number plate recognition
Shadow mode	Running detection without escalating, to tune before go-live
Vision-language check	Asking an AI model to describe a frame, to confirm or reject a detection

CONCLUSION

The cameras are already there. **SENTINEL** makes them see.

S.A.L.T SENTINEL turns an existing camera network into a sovereign intelligence layer: it detects what matters, tells the right person, finds what happened in minutes and writes the report — on the organisation's own servers, under its own rules, in its own languages.

1 · Site assessment

We analyse sample footage from your own cameras and measure what SENTINEL finds.

2 · Pilot in shadow mode

A handful of cameras and detectors, tuned against real activity, with no escalation.

3 · Go live and grow

Switch on escalation, train the teams, and add cameras, sites and detectors as you go.



Prepared by **CAPT ZEDs**
Founder and Creator of S.A.L.T.CI
www.salt.ci · info@salt.ci



PEMANGKIN
TEKNOLOGI

PEMANGKIN TEKNOLOGI REKA PLT · 202604002776 (LLP0048022–LGN)
F-9-1 Block F, Jalan PP 25, Putra Walk Commercial Centre, 43300 Seri Kembangan, Selangor
+60 3-8750 2789 · www.pemangkin.tech · info@pemangkin.tech
Catalysing Sovereign Intelligence