SIYTE System Overview

The SIYTE platform, illustrated in Figure 1, acts as the central intelligence and command layer for data aggregation, analysis and actions.

Figure 1: SIYTE Architecture

Inputs - Data Aggregation

SIYTE is hardware agnostic and integrates data from multiple sources in real time including:

- Fixed CCTV, PTZ or thermal cameras (whether at day, in low light or utilising infrared), whether:
  - Intelligent CCTV cameras with in-built analytics sending object detection meta data
  - "Dumb" CCTV cameras, the stream can be analysed on edge compute nodes running PurpleMV software
- IoT Sensors such as vibration and PIR sensors
- Other external sources and systems, which may be public data such as weather data, third party sensing systems or other relevant data sources, such as train information.

New data sources can be integrated on request.

Data Analysis (SIYTE CORE)

Figure 2: SIYTE Workflow

The SIYTE Core layer analyses data as it arrives, correlating different data sources using SIYTE's embedded workflow engine.

SIYTE can validate 'machine vision' detections from cameras (whether smart cameras or analysis of camera feeds using "PurpleMV" software on small on-site devices).

It does this to reduce false alerts by re-checking the machine vision 'inference' against other computer vision models.

For instance, a flow might be that we first check it really is a person and then ensure they are not wearing security personnel uniform.

Agents (SIYTE GUARDIAN)

Any detection can initiate an AI Agent process, initiated by a step in a workflow such as the one above. For instance, if a camera detects someone outside the perimeter who appears to be loitering (e.g. dwell time > 10 seconds), this could initiate a Agent process to analyse the person's behaviour in more detail. This is an 'agentic AI' process that can perform a much more detailed analysis of a potential detection.

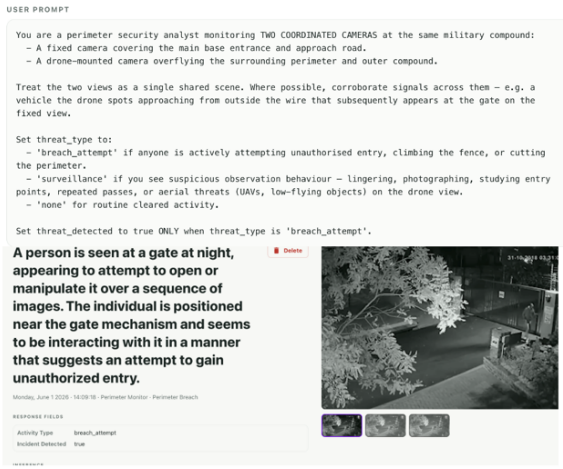

Figure 3: SIYTE Guardian

As illustrated in Figure 3, Agents are trained to search data and images for threats such as suspicious behaviour on a perimeter.

Data, including video images can be analysed in great depth to provide the context required to determine a response. This enables detection of threats to become proactive, moving beyond detecting a perimeter breach to identifying suspicious behaviour before a breach.

They can also analyse data patterns to understand anomalies to determine whether the identified activity is suspicious.

Outputs and Actions

Once a full analysis has been completed, another workflow can be initiated to take the appropriate action. This might be:

- Alerting: Send an alert via the appropriate channel, e.g. to the control room or to a member of mobile security staff on a mobile device.
- Logging: Log all alerts and notifications so that these are available for review but also for later AI analysis (e.g. low-level suspicious behaviour that may be reconnaissance may not require immediate response, but still needs to be logged so that patterns of such behaviour can be understood)
- Automated Actions: Actions by external systems (such as speaker announcements) can be automatically initiated.

Visualisation

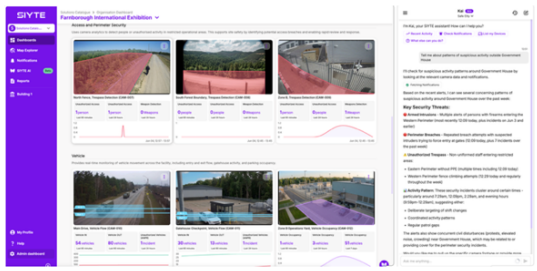

Figure 4: SIYTE User Interface

SIYTE has a UI (Figure 4) that can present analytics information from CCTV cameras, sensors and other systems from both a real time and historical perspective. This is extremely flexible and adapted to different stakeholders and scenarios.

SIYTE also provides a conversational LLM interface, SIYTE AI, for querying data and events. This is extremely useful for analysing data to establish patterns, identify anomalies and search for events.