



Digital Public Safety Agentic AI Service

G-Cloud 15 Service Definition Document

Crown
Commercial
Service
Supplier



Contents

Digital Public Safety Agentic AI Service.....	3
Tackling Anti-Social Behaviour, Trespass and Crime	3
Keeping people safe and reducing risks	3
Optimising Public spaces and enriching visitor experience.....	3
The Purple Transform SiYtE platform	3
Management Interface	4
Example Use Cases.....	4
Anti-Social Behaviour.....	4
Protecting people and infrastructure	6
Public space optimisation.....	9
Support and Service Management	10
Managed Service Desk	10
Ticket notifications and updates	10
Incident Management.....	10
Escalation Procedures.....	10
Major Incident Management	11
Hardware and Software Lifecycle	11
Maintenance updates	11
Reporting and analytics.....	11
Change requests.....	11
Co-management	12
Staff training	12
Documentation	12
Account Management	12
Regular Service Management Meetings.....	12

Digital Public Safety Agentic AI Service

The Database for Business Digital Public Safety Platform is based upon the Purple Transform SiYtE platform. Key benefits of our Digital Public Safety Agentic AI Service include the following:

Tackling Anti-Social Behaviour, Trespass and Crime

- ✓ The Purple Transform SiYtE platform utilises 'ethical AI' to process camera footage from any camera system, using the latest visual language processing to identify instances of trespass, anti-social behaviour and crime.
- ✓ The platform anonymises people faces, making it easier to share alerts to mobile devices and even outside organisations to alert to issues.

Keeping people safe and reducing risks

- ✓ A further benefit of this technology is that it can log and locate issues across Public realm, enabling identification of use cases such as trip and fall risk areas, whilst also using behavioural intelligence to learn and even predict particular behaviour, enabling a preventative approach.

Optimising Public spaces and enriching visitor experience

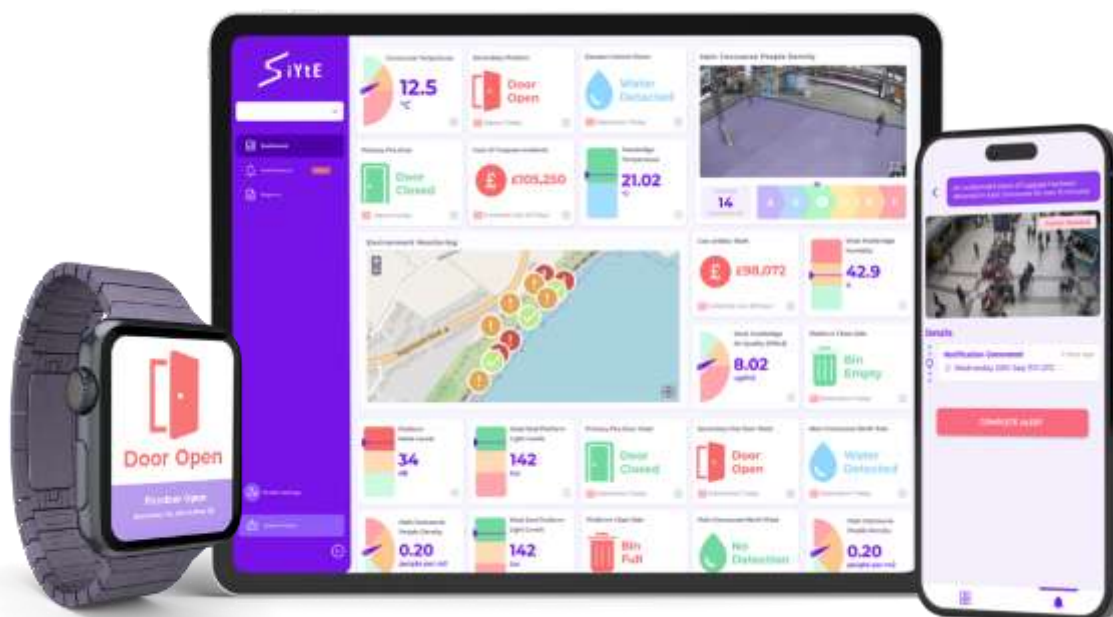
- ✓ By identifying people flow and alerting to crowding, poor air quality or water leaks by ingesting both camera and sensor data, visitor experience can be improved, whilst monitoring escalators, lifts and fire exits can ensure people remain safe.

The Purple Transform SiYtE platform

- ✓ Purple Transform's SiYtE platform ingests camera and sensor data from any platform and presents information into a single easy to use portal with complete access to information.
- ✓ The platform is also able to trigger alerts, based upon complex rule flows to improve accuracy. By anonymising the faces of people recorded on the cameras, this also overcomes traditional data sharing and privacy challenges, allowing data to be shared and alerted to multiple organisations and agencies.

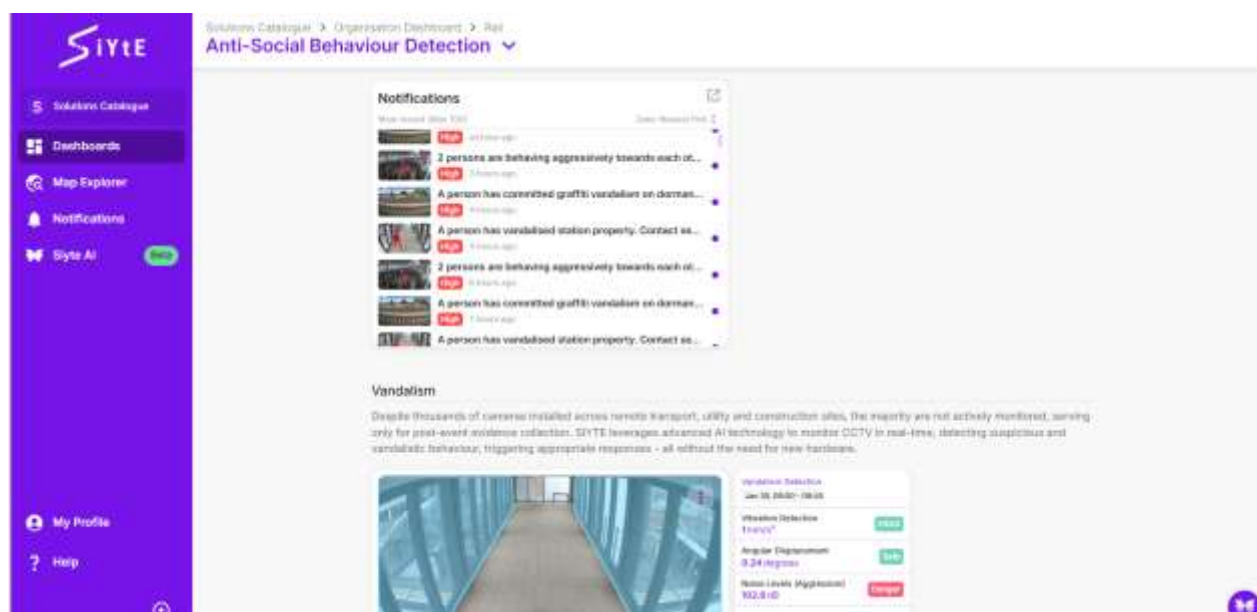
Management Interface

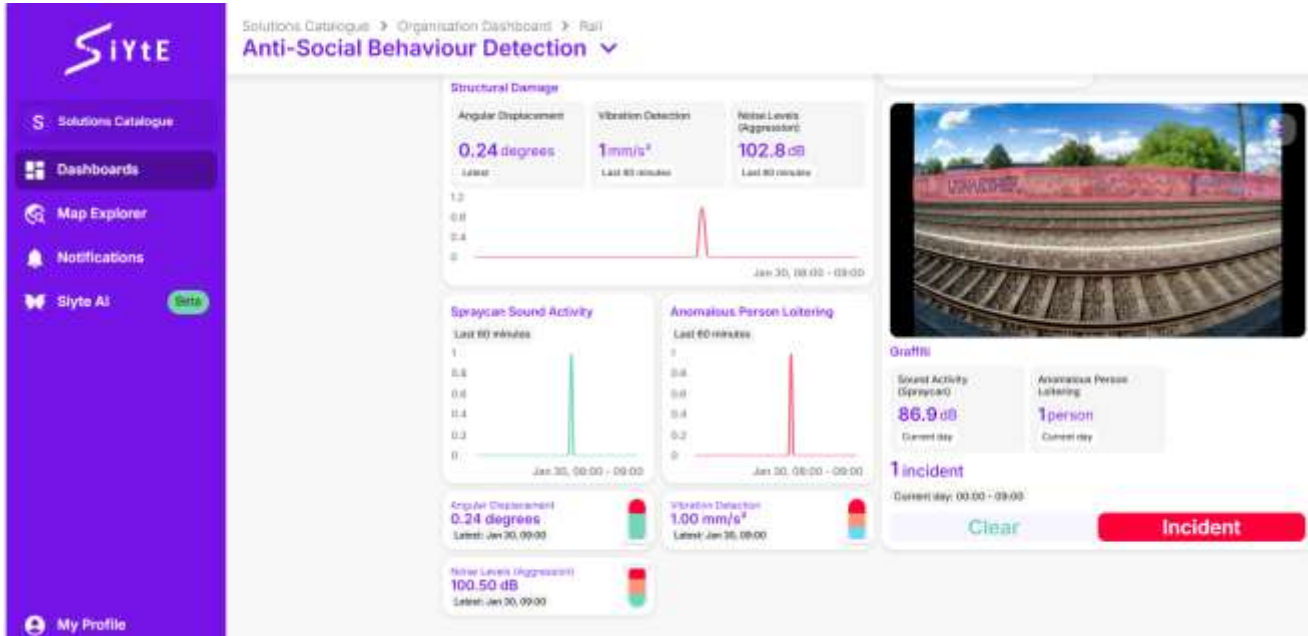
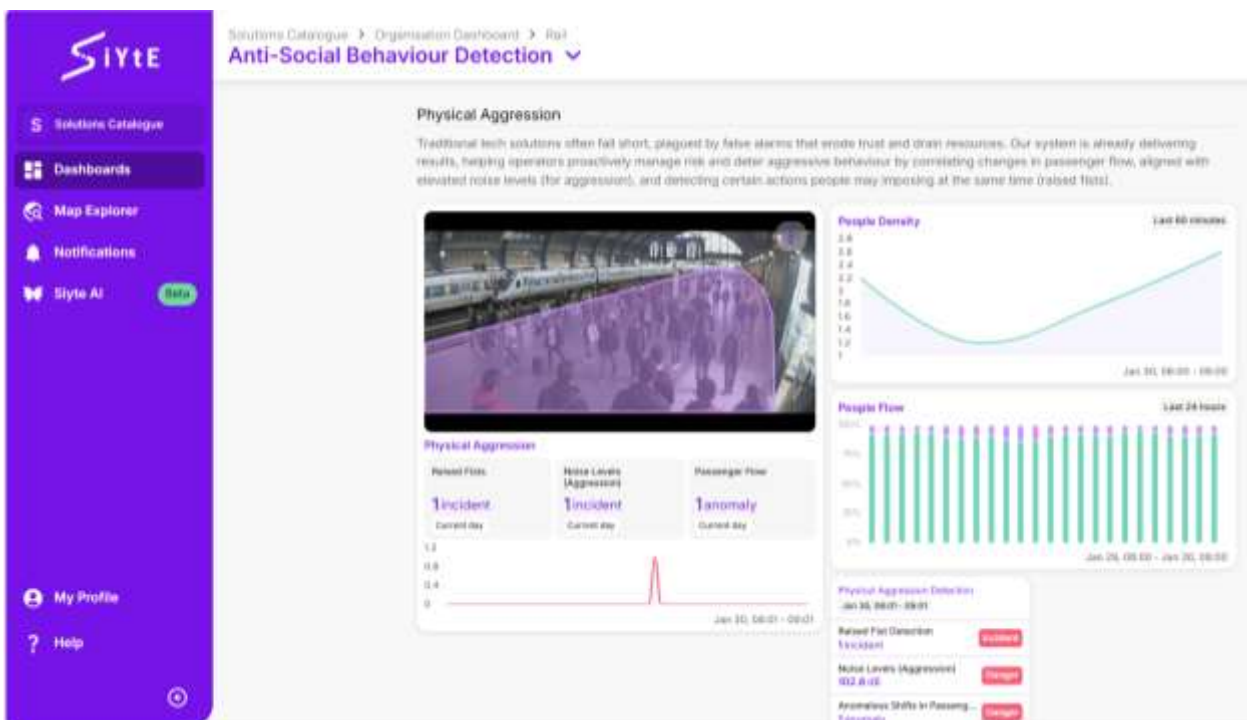
All aspects of the Digital Public Safety Agentic AI Service are managed through a single pane of glass – the SiYtE Platform.



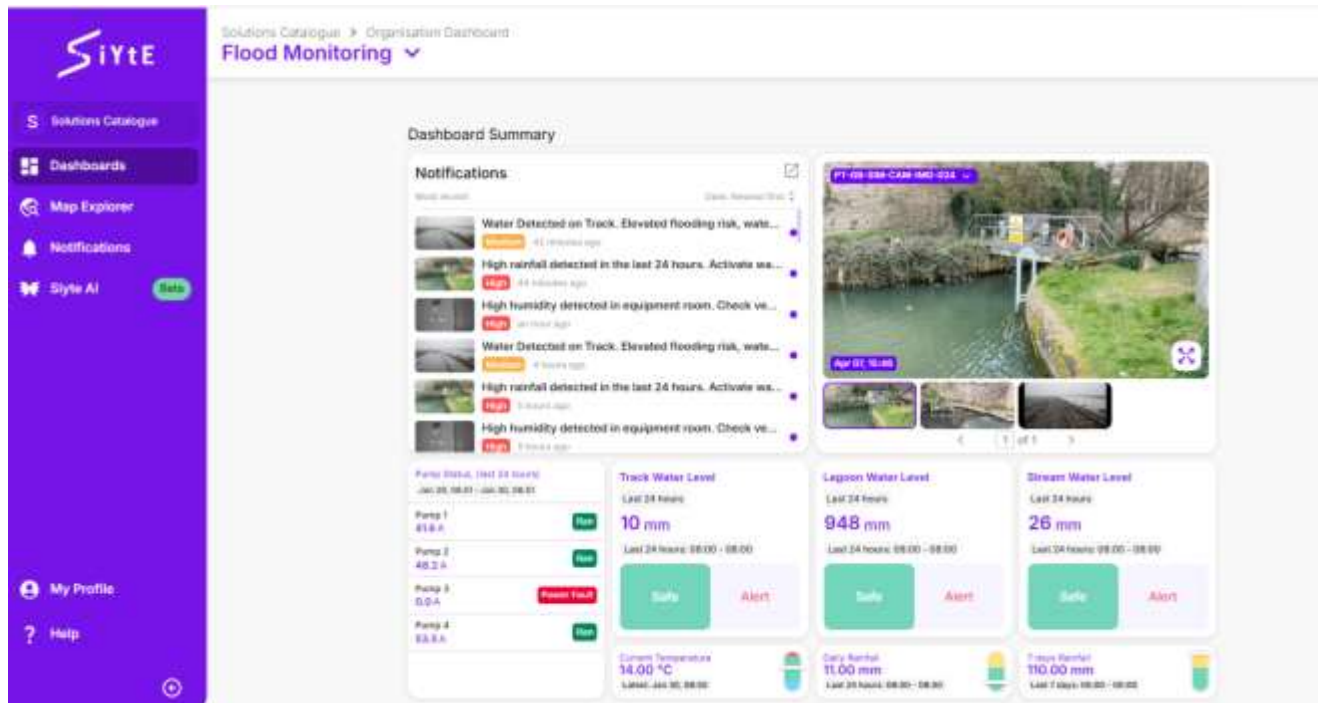
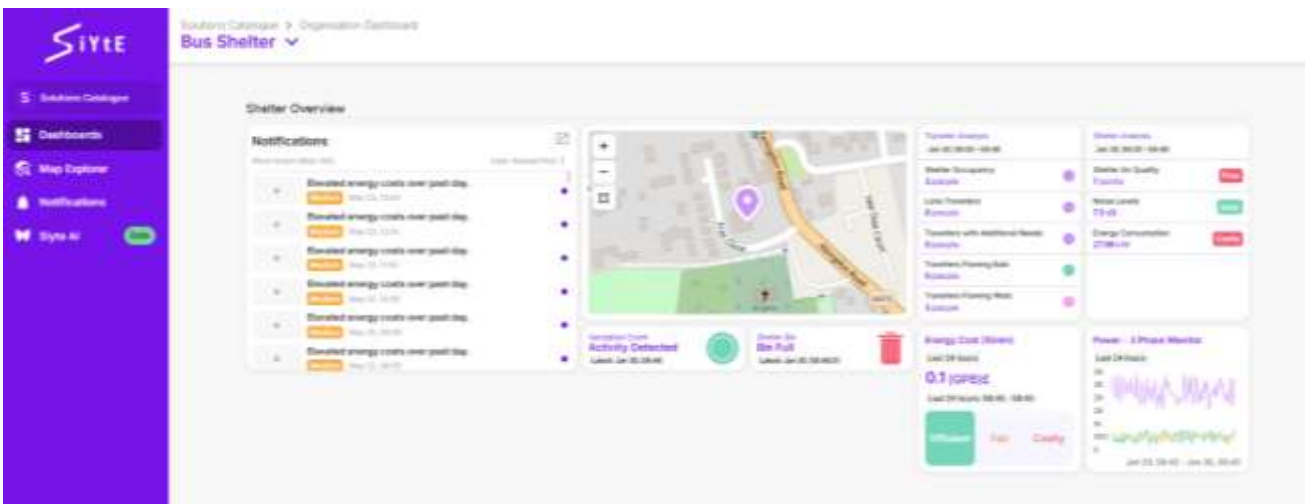
Example Use Cases

Anti-Social Behaviour





Protecting people and infrastructure





- S Solutions Catalogue
- Dashboards**
- Map Explorer
- Notifications
- SIYTE AI Beta
- My Profile
- Help

Solutions Catalogue > Organisation Dashboard

Healthcare (Integrated Care Board) ▾

Executive Overview

Notifications

Most recent (Max 100)

- High Temperature threshold has been exceeded in Ward 3. ... 0 minutes ago
- High Patient Aggression detected from Bed 3 in Ward 2. Im... 10 minutes ago
- Medium Energy Consumption higher than usual from lighting s... 15 minutes ago
- High Temperature threshold has been exceeded in Ward 3. ... on hour ago
- Medium Energy Consumption higher than usual from lighting s... on hour ago
- High Patient Aggression detected from Bed 3 in Ward 2. Im... on hour ago

Person Overview

Jan 30, 08:00 - 08:55

- Low Worker Safety 0 breaches
- Unauthorized Storage Trespass 0 breaches
- Unsupervised Patients 0 breaches
- Ward Emergency Button Press 0 breaches
- Reception Crowding 0 breaches

Operational Overview

Jan 30, 08:00 - 08:55

- A&E Energy Consumption 0 breaches
- Ward Energy Consumption 0 breaches
- Storage Rm. Energy Consumption 0 breaches
- Parking Bay Energy Consumption 0 breaches

Venue Overview

Jan 30, 08:00 - 08:55

- Unlicensed Cars in Ambulance Bay 0 breaches
- Drop-off Zone Wait Time 0 breaches
- Parking Level Capacity 0 breaches
- Unknown Vehicles in Staff Parking 0 breaches



- S Solutions Catalogue
- Dashboards**
- Map Explorer
- Notifications
- SIYTE AI Beta
- My Profile
- Help

Solutions Catalogue > Organisation Dashboard > Education

Vape Detection ▾

Campus Overview

Vape detection levels indicate the concentration of airborne particulates consistent with aerosol or vapor presence over a defined time period. Elevated readings may suggest vaping activity but are not, on their own, confirmation of individual behavior. Snapshots and level data are recorded to support trend analysis, identify repeated occurrences, and assist staff in monitoring high-risk areas. This information helps inform appropriate responses in line with campus safety and wellbeing protocols.

Notifications

Most recent (Max 100)

- High Alert: Vaping activity detected in the bathroom at Jan... 3 hours ago
- High Alert: Vaping activity detected in the bathroom at Jan... 3 hours ago
- High Alert: Vaping activity detected in the bathroom at Jan... 3 hours ago
- High Alert: Vaping activity detected in the bathroom at Jan... 5 hours ago
- High Alert: Vaping activity detected in the bathroom at Jan... 6 hours ago
- High Alert: Vaping activity detected in the bathroom at Jan... 6 hours ago

Main Locker Room

Last 60 minutes

18 Level

Last 60 minutes: 07:55 - 08:55

Clear
Detection

Changing Rooms

Last 60 minutes

24 Level

Last 60 minutes: 07:55 - 08:55

Clear
Detected

Equipment Room

Last 60 minutes

22 Level

Last 60 minutes: 07:55 - 08:55

Clear
Detected

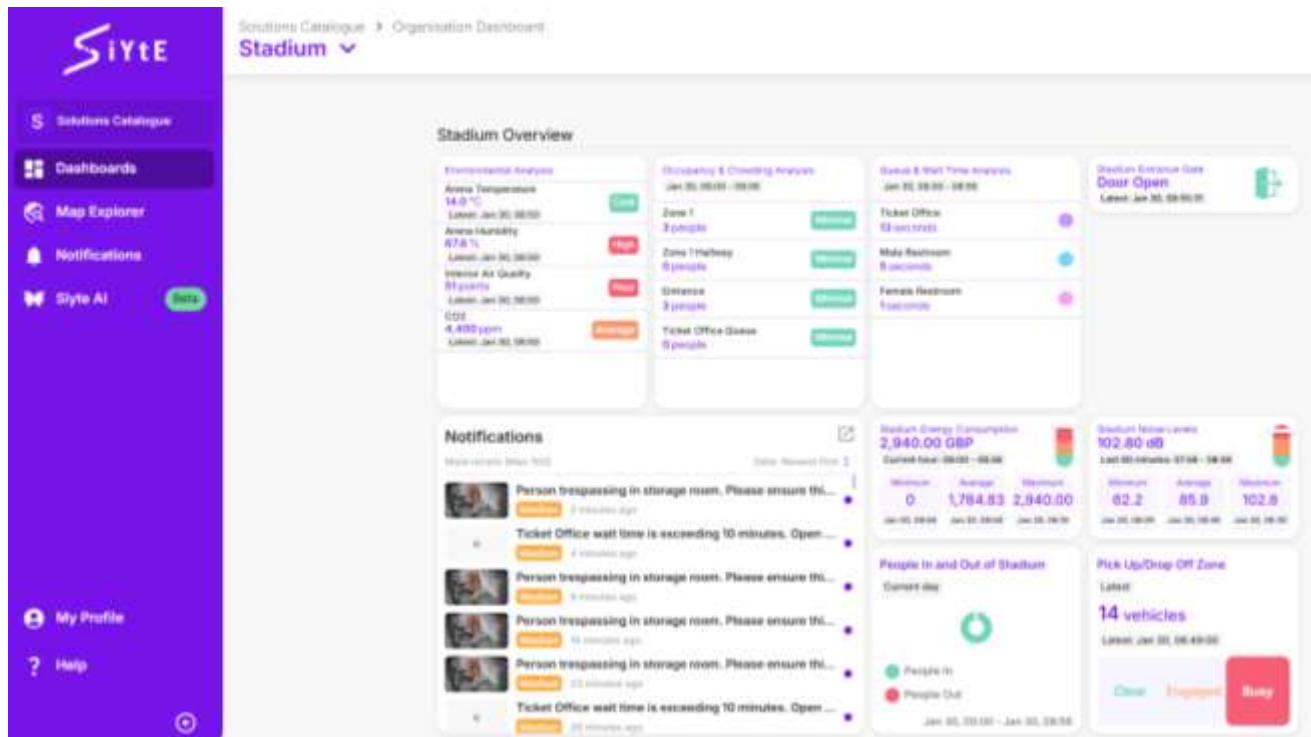
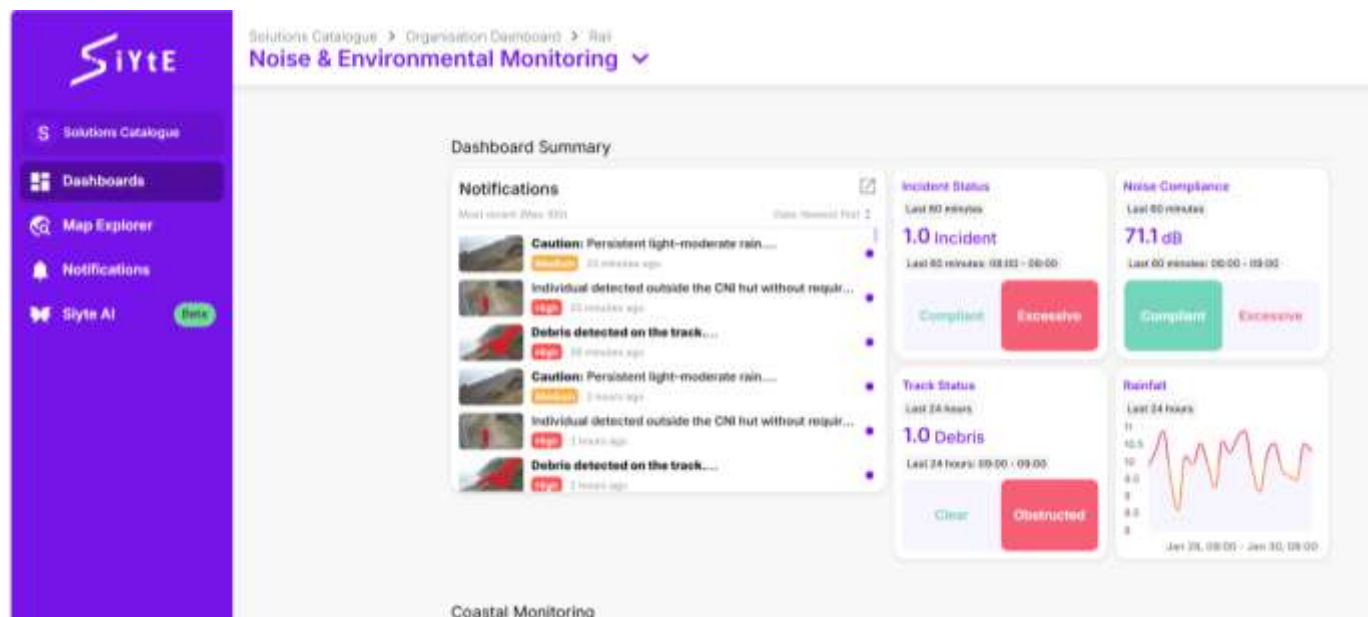
Ground Floor Toilets

Last 60 minutes

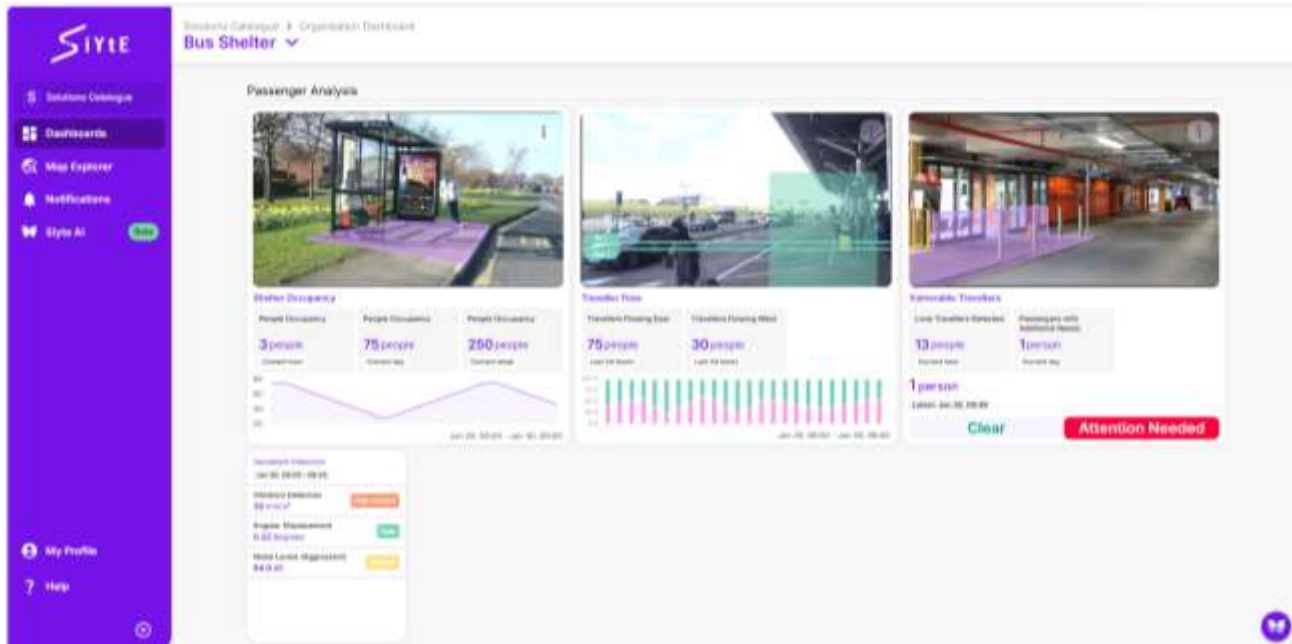
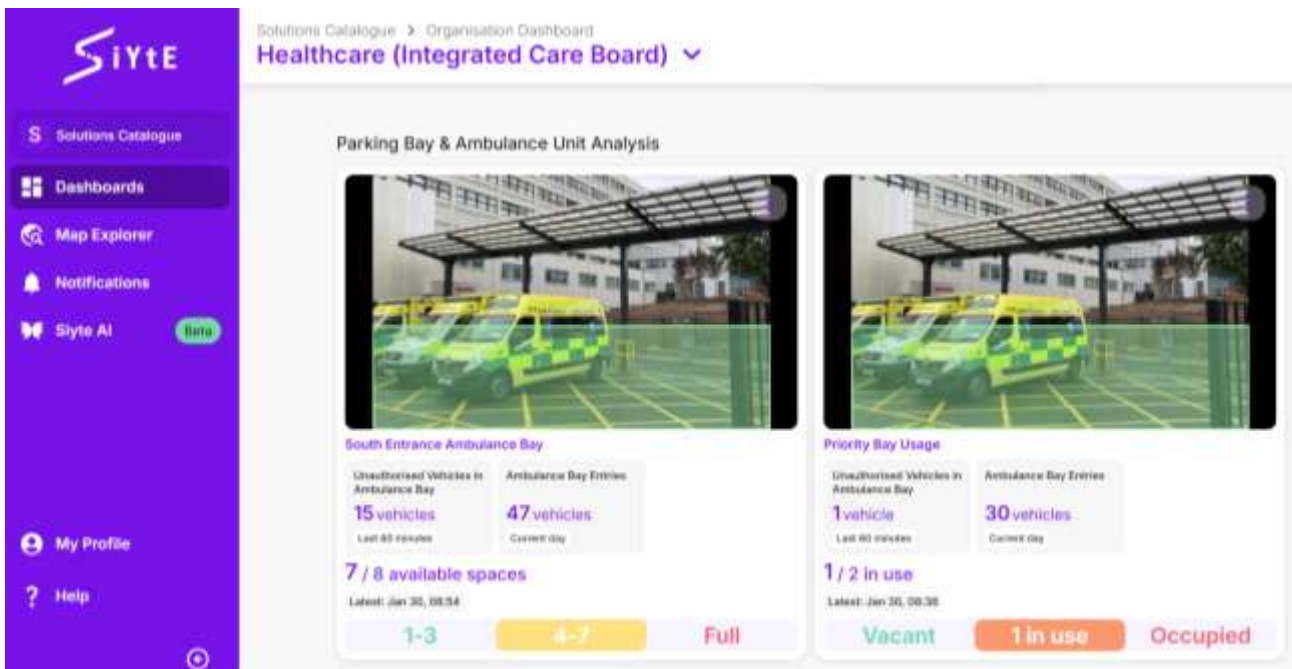
80 Levels

Last 60 minutes: 07:55 - 08:55

Clear
Detected



Public space optimisation



Support and Service Management

Managed Service Desk

We will provide a dedicated, single point of contact responsible for the ongoing managed support. Tickets are raised by authorised buyer staff through the Service Desk and then all subsequent communication and updates will be managed by the desk which is accessed via phone or email.

Ticket notifications and updates

As part of the Managed Service Desk, any new tickets and alerts will be notified to nominated contacts to advise users and analysts of new calls, resolutions, breaches change notifications and reports. This will include both buyer generated tickets or those raised by automated monitoring facilities.

Incident Management

dbfb will investigate, manage, and support any faults or issues on the service from the technical service desk. Once identified and logged, the service desk will provide you with remote assistance to rectify the issue or advise and implement remediation actions to reduce the likelihood of the issue recurring. Where on site hands are required, these will be provided by dbfb on site engineers. Additionally, dbfb will manage the provision and support of transmission circuits. Where an issue is not immediately identifiable as a hardware issue, our service desk team will work to reduce the impact and resolve.

Escalation Procedures

As detailed in the Incident Management Process Flow diagram, tickets will generally be initially handled by first line level engineers. Where technical escalation is required, we have access to 2nd line, 3rd line, support consultants and support architects.

Where needed the Managed Services team would contact the vendor and fully co-ordinate investigations until a resolution is found. The escalation contacts will be notified internally based on the triggers identified below:

- ✓ Level 1: Duty Manager: Contacted when 50% of any P1 or P2 is reached, or when any ticket's SLA has breached.
- ✓ Level 2: Contacted when 75% of any P1 is reached, or when any ticket's SLA has breached.
- ✓ Level 3: Contacted when 90% of any P1 is reached, or when any P2 ticket's SLA has breached.

Major Incident Management

We have a robust Major Incident Management (MIM) process in place. The process aligns with the ITIL framework and can be summarised in four main areas:

- ✓ Identification – The incident will be identified and triaged. If required, a major incident will be declared and all key stakeholders will be informed.
- ✓ Containment – A Major Incident Manager will be appointed. Conference bridge calls will be set up with key technical resources. Stakeholders will be updated at regular intervals.
- ✓ Resolution – A resolution will be identified. An emergency change will be raised to implement the fix. All stakeholders will be updated by the MIM.
- ✓ Maintenance – A Root Cause Analysis (RCA) will be performed. The RCA will be shared with the buyer. If required, actions will be implemented to prevent reoccurrence of the issue.

Hardware and Software Lifecycle

As part of the Managed Service we will perform quarterly reviews of the hardware and firmware running on supported devices within the buyers environment. These reviews would be presented as part of a regular monthly service review meeting.

Maintenance updates

Notification of any planned maintenance activity will be provided via email to the designated maintenance contact, with a minimum of 14 days notification.

Reporting and analytics

We will collate a range of reporting and analytical information as part of monthly service reviews for performance monitoring, analytics, trend analysis and troubleshooting. This will include collating data from both the SiYtE platform and other sources of information including the performance, utilisation and availability of circuits and any mobile data sim cards. In addition to providing regular reports, we will build intuitive dashboards within platforms such as PowerBI, for your team to access, in order to undertake regular assessment of the performance of the services and support future planning.

Change requests

The Digital Public Safety Agentic AI Service includes unlimited requests. Any change requests will be handled through the service desk using ITIL-defined processes for change review and approval, in accordance with your requirements.

Co-management

Included in the service will be the ability for buyer authorised staff to co-manage the solution by having access to make necessary small adds, moves, and changes (i.e. – firewall policy changes).

Staff training

Where specified the Digital Public Safety Agentic AI Service will include training via access to Cisco learning credits, to enable buyer staff to be trained on the solution and become Cisco accredited.

Documentation

Full documentation, change control processes, knowledgebases and reference guides will be provided and kept updated as part of the ongoing managed service.

Account Management

You will be provided with an assigned Account Manager and Service Manager throughout the contract who will be available for your team to contact and who will attend monthly service reviews.

Regular Service Management Meetings

In addition to informal Account and Service Management, we will hold Monthly Service Management meetings, either online via Microsoft Teams, or on site at the buyers or dbfb offices. It is expected that such meetings may need to be more regular, for example weekly or bi-weekly during the early stages of the contract.