

DETECTION OF JAMMERS



Our GSM Jamming detection and monitoring module is a static wall or pole mounted device built to detect nearby signal jamming and to notify response teams in milliseconds of GSM or GPS jamming events. Digitpol's custom module can detect 2G 3G 4G and 5G jamming, detect interference in the cellular network such as rogue base stations, detection of IMSI catchers and detection of new nearby devices. The cloud platform contains a white list that enables the monitoring team to have a clear vision of alarms, known trusted nearby devices, cell towers and the rapid detection of new devices.

Passive Capturing Functions

Detection of illegal GSM Cell Towers (IMSI Catchers) GSM Jammer & GPS Jammers.

Capturing nearby WiFi MAC, Bluetooth MAC & IMSI

Contact

Office: +3155 844 8040
Email: info@digitpol.com

Working time

Phone Support Mon - Fri: 9:00 - 17:00 / 24/h Support via Email

Head Office

Digitpol HQ, Boogschutterstraat no. 1, 7324 AE Apeldoorn
The Netherlands

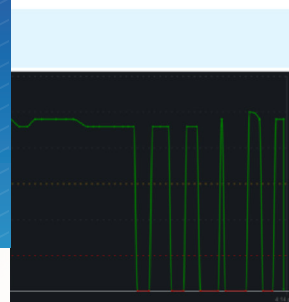
Cloud based detection of Signal Jamming

Digitpol's detection module is the ultimate in the detection of espionage on a site from jamming to rogue activity, when used with several modules a mesh is created, this ensures a high level of security within the mesh. The Jammer Detector can alert responding or monitoring agents by SMS, email, API or in the portal. This module and platform is developed at Digitpol in The Netherlands.



VEHICLE CRIME

Digitpol's Detect module will detect illegal jammers in use to steal vehicles and jammers used in vehicle crime.



DRUG TRAFFICKING

It has been proven that criminals transporting drugs deploy jammers to defeat law enforcement tracking, tracing and surveillance.

SECURED BUILDINGS & VEHICLE

Secured vehicles or buildings, banks, embassies, police stations, government and similar buildings may come under attack by illegal jammers or rogue cellular networks

Use Cases:



VEHICLE & CARGO THEFTS

Digitpol's JamDetect module will detect illegal jammers in use for Vehicle thefts.

Jammers are used by criminals to defeat vehicle OEM tracking and aftermarket tracking systems, jammers also defeat onboard navigation and all levels of monitoring or tracking systems.



DRUG TRAFFICKING

It has been proven that criminals transporting drugs deploy jammers to defeat law enforcement tracking, tracing and surveillance.

Drugs trafficking is difficult to detect and Digitpol's Jam Detect module can alert Police to a passing vehicle, container, shipment that a jammer is in use.



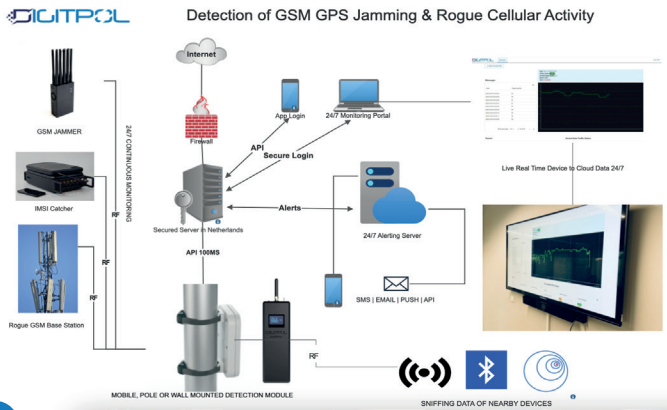
CAR PARK SECURITY

Digitpol's JamDetect will detect GPS Jammers in use at car parks and can alert a control room, security guards, law enforcement within seconds of detection. The detection of a jammer can prevent car thefts, robberies and crime. An output is also available to trigger a siren or LED that a jammer is detected.



SECURED BUILDINGS & VEHICLES

Secured vehicles or buildings, banks, embassies, police stations, government and similar buildings may come under attack by illegal jammers or rogue cellular networks, the detection is vital as a Jammer can block alarm systems, fire systems and prevent control rooms from receiving security alerts and a rogue cell site could intercept data. Digitpol's detector can be installed in our outside buildings and will alert control rooms instantly if jamming is detected.



The Hardware

- The Static Detector, a waterproof module for pole or wall mounting.
- Detector is supplied with an IOT Data sim and data for 1 years.
- Provided with a range of power supplies to be agreed with client, (5V. 12V, 220V).
- Supplied with internal backup battery (24h backup power).
- Can be supplied with an internal rechargeable battery for 1 month remote operation.
- Detects jamming of 2G / 3G / 4G / 5G.
- Detects jamming of GPS / GLONASS / GALILEO.
- Detects jamming of Wi-Fi / Bluetooth.
- Detection of IMSI Catchers & Rogue Cellular towers or base stations.
- Passive collection of nearby Wi-Fi SSID, MAC and metadata.
- Passive collection of nearby Bluetooth devices (MAC).
- Passive collection of nearby IMSI (LEA only).
- This module can be installed into a vehicle or a static post.
- Fully customizable, more capabilities on collection are possible.
- Working temperature -15 ° C ~ + 55 ° C



The Software

- A secured API between the Detector and Cloud enables 24/7 access to data. Spectrum scope of real-time activity, this scope is in 200ms real-time and can display history.
- A rich database of real-time and historic signal data, GSM activity cellular Towers by connected and nearby towers (LAC, Cell ID, PWR), nearby SSID, MAC and IMSI.
- Lifetime logs of Jamming events all stored with a timestamp and metadata, these logs can be exported in CSV and PDF.
- Lifetime logs of connected Cellular Towers all stored with a timestamp and metadata, these logs can be exported in CSV and PDF.
- Lifetime logs of nearby Cellular Towers all stored with a timestamp and metadata, these logs can be exported in CSV and PDF.
- Lifetime logs of detection of IMSI Catchers, these events are stored with a timestamp and metadata, these logs can be exported in CSV and PDF.
- Lifetime logs of detection of nearby Wi-Fi SSID, MAC and signal strength (other data available for LEA) these logs can be exported in CSV and PDF.
- Lifetime logs of detection of nearby Wi-Fi SSID, MAC and signal strength, these logs can be exported in CSV and PDF).
- The cloud allows for multiply users and administrators can select which users will receive an alert when an event is triggered.