Viseum IMC and iVOS Level 1: End User Operational Training

This module is designed to enable professional CCTV security staff to fully exploit the spectrum of unique capabilities that Viseum cameras and iVOS software capability offer. To automatically address each remote site's security issues whilst freeing up monitoring staff for other tasks. This will enable the user to swiftly optimize situational awareness and security within any given single or multiple areas of responsibility of the Viseum network.

Start state:

- A fair knowledge of CCTV operations, or working knowledge of the security challenges within their area of responsibility.

Aim:

- To use the Viseum cameras in order to automatically generate situational awareness, heightened long-term security, surveillance and deterrence at each remote site.

Objectives:

By the end of this session students will be able to:

- Create automated site surveillance rules for risk management, suspect target allocation and prioritisation, for each remote site.
- Operate Viseum cameras in their live proactive operational mode to deal with automatically detected security threats.
- Operate Viseum cameras in decision support of security patrols and first responders, with situational awareness and initiative in order to act either prior to, or subsequent to, an offence.
- Operate Viseum cameras in their passive standalone operational mode and deal with evidence recovery.

A typical example of industry-standard security process without the use of Viseum cameras:

1) A suspect breach to a perimeter, potentially causing criminal damage, is automatically detected by a PIDS device and automatically alarmed to the command control.
2) A security operator first identifies the 'section' of the perimeter where the potential breach took place.
3) The security operator then spends valuable time:
    a. Locating and accessing the nearest PTZ Camera.
    b. Controlling this PTZ Camera to monitor the section of the perimeter in order to:
        i) Look around the area for the suspect.
        ii) Confirm if the incident should be dealt with further.

Heightened security and performance training with the use of Viseum cameras:

This training module will cover how **all of these actions are processed automatically** by the Viseum camera system, so that the security operator is fully primed with the complete ground truth for the correct immediate response.

Viseum IMC and iVOS Level 2: System Administrator

This module allows the system administrator to fully exploit and optimize Viseum's unique camera and iVOS software capabilities within their security hierarchy. For any given security area of responsibility, the number of Viseum cameras required will always be far fewer and more widely dispersed than for any other system. Also, due to the unrivalled capacity of the Viseum cameras, these cameras will be providing security and monitoring capability for numerous additional agencies. Therefore this module is designed to train a system administrator to optimize the network design, configure and manage the Viseum cameras in automated support of operator staff whilst meeting the multiple requirements, and optionally prioritise access levels of the various additional stakeholders of each Viseum camera installation.

Start state:

- Current knowledge in configuring and managing IT systems and conventional IP camera networks – experienced professional security staff and resources manager.

Aim:

- Manage the best practice implementation and use of the Viseum cameras and iVOS system.

Objectives:

By the end of this session students will be able to:

- Understand and exploit the unique aspects of the Viseum camera and iVOS operating software.
- Design a Viseum camera network and designation of appropriate automated monitoring mode for each remote site.
- Manage the overseeing of installation maintenance – 1st line fault diagnosis and reporting.

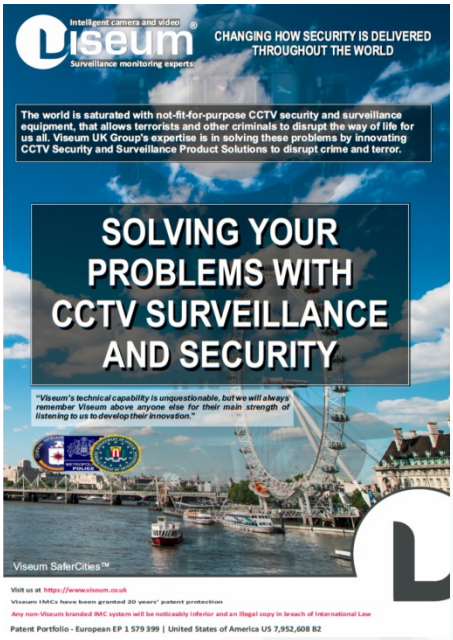
Typical examples of network design improvements:

1) The Viseum camera is installed 'plug and play' without the need for the otherwise lengthy procurement and installation processes of standard technologies, requiring considerable camera and cabling infrastructures.
2) Because of the automated Viseum camera and iVOS operating locally to the camera installation, many remote sites will no longer require costly high-bandwidth communications to the command control. This means for example; costly fibre connections can be replaced to benefit from lower bandwidth wireless 4G/5G connections.

Typical examples of performance improvements:

1) This new automated surveillance capability significantly changes how much time each remote site requires proactive camera control and viewing attention, and how many remote sites will now benefit from reactive surveillance.
2) This new performance will show greater operational savings with improved key performance indicators. **> Download UK savings example <**

Intelligent camera and video Viseum® Surveillance monitoring experts



> Viseum Technology and Support Strengths < This is a brochure presentation of our technical support and capabilities. It is very successful for Viseum sales training and provides our customers with confidence in our project support and delivery.

Legal Statement

We have invested heavily in the protection and policing of our intellectual property rights (IPR). Central to our business is the commercial protection we provide our partners in sharing these secured markets. We commit to the policing of this IPR in the following way: As with any infringement, its trade reseller is the primary target for legal action, which is, in turn, followed up by making the potential user aware of the infringing product's recall due to its illegal use. This is then followed up with full and complete legal action with the suppliers of such goods. This policy of proactive policing our markets in this way since 2002 has proven so successful that we have only ever identified one infringing party. A PLC entity was found to be trading with infringing goods and they can now no longer sell such goods, nor can they secure investment due to this breach.

Purchase of a Viseum-driven product from an authorised Viseum® supplier guarantees that it contains authentic Viseum® software, and carries with it a licence giving the purchaser permission to use the Viseum technology patents. Attempted use of Viseum® software without a valid licence is in breach of international law.

Patents Granted European Patent > EP 1 579 399 < & United States of America > US 7,952,608 B2 <

Registered Trade Marks Viseum® SafetyWatch®

Copyright

This document is for information only and does not constitute an agreement between Viseum and any 3rd party.

For further information on how to set up Sales Agent, Regional Reseller and Distribution agreements to become a Viseum Certified Corporate Partner, please contact your Viseum representative or write to us using the Viseum website.

> Viseum Group Profile <