The purpose of the European Union's Resilience of Critical Entities (CER) Directive 2022/2557 is to protect designated critical infrastructure "entities" (facilities which provide services that are vital to societal, economic and political well-being) from physical threats that could disrupt service, cause harm or result in severe economic loss. The directive encourages Member States and EU economic sectors to establish new (or delegate to existing) responsible regulatory bodies that will oversee risk management processes, encourage cooperation, and establish enforceable regulations.

CER Article 13 mandates that critical entities enact technical, security and organisational measures to ensure their operational resilience and mitigate vulnerabilities identified during mandatory risk assessments. The enacted measures should improve physical security capabilities via the following functions:

• **DETER**: Prevent incidents from occurring (risk reduction)

• **DETECT**: Intrusions and other security threats via physical protection systems

• **RESPOND**: Respond to, resist, and mitigate the consequences of incidents

In the interests of effectiveness and accountability, critical entities should describe the measures they take, with a level of detail that sufficiently achieves the aims of effectiveness and accountability, having regard to the risks identified, in a resilience plan or in a document or documents that are equivalent to a resilience plan, and apply that plan in practice.

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, December 2022

DETECTION AND DETERRENCE AT THE PERIMETER

A security fence along the perimeter of a facility is the first line of defense. But, by itself, it is only a minor deterrent to determined intruders – they can cut-through or climb it in seconds. Even without accessing any on-site buildings, intruders can threaten service, cause extensive damage, steal supplies, and/or injure themselves or others.

Senstar offers a range of products that bring intelligence out to the perimeter. Intelligent lighting functions as an active deterrent while sensors and surveillance cameras detect and locate intrusion attempts. Perimeter detection enables a range of security responses, including triggering the site's alarm system, queuing up camera systems, and engaging deterrence devices like audio messages or additional lighting.

Interior areas can also be protected. As Senstar sensors share common communication protocols, a mix of sensors may be deployed at a site without adding additional infrastructure.

FUNCTION	PRODUCT	BENEFIT
DETER	Senstar LM100	Intelligent lighting and intrusion detection illuminates the perimeter. Can strobe at intrusion location.
	All Senstar sensors	Senstar intrusion detection sensors can trigger on-site deterrence devices like security lights or sirens
	Video analytics	Enable deterrence devices (lights, audio) via early pre-intrusion detection
	Senstar Symphony VMS	Software allows two-way audio support which enables voice down capability, so security personnel can speak to intruders
DETECT	FlexZone	Fence-mounted perimeter intrusion detection (cable)
	Senstar LM100	Perimeter intrusion detection (accelerometers in luminaires)
	FiberPatrol	Fence-mounted perimeter intrusion detection (fiber optic cable)
	Wireless Gate Sensor	Gate protection (accelerometer)
	UltraWave	Gate and area protection (microwave)
	Video analytics	Detect and track intruders and vehicles near, at, and inside the perimeter

Senstar LM100 Hybrid Perimeter Intrusion Detection and Intelligent Lighting System protecting an electrical storage yard.

ASSESS, COMMUNICATE AND RESPOND TO SECURITY THREATS

Senstar's video management software (VMS) and video analytic technologies complement perimeter sensors by providing assessment, communication, and response capabilities:

- Efficiently monitor hundreds of remote substations from a central location
- View surveillance video from all major camera manufacturers, including video from low-light and thermal devices
- Employ video analytics to enhance monitoring capabilities while reducing operator requirements
- Use sophisticated intelligent search for post-incident analysis

STREAMLINED VIDEO MANAGEMENT

The Senstar Symphony Common Operating Platform enables operators to control their entire video surveillance system from a central location. Operator features include:

- Integrated sensor, video analytic and access control events
- On-site I/O device control, including 2-way "talk-down" intercoms
- Automated detection and tracking of vehicles and people

MOBILE SUPPORT FOR ON-CALL STAFF

Senstar Symphony can support on-call staff with a variety of functionality from their mobile device, including email/SMS alerts (with captured images), access to individual cameras, and on-device video recording.

FUNCTION	PRODUCT	BENEFIT
ASSESS	All Senstar sensors	Zone or distance-based locating. Direct PTZ cameras to intrusion location.
	Senstar LM100	Uniform lighting along the perimeter enhances the assessment value of video cameras
	Senstar Symphony	Camera callup, auto-PTZ and video analytic overlays
	Video analytics	Identify vehicles and people via license plate recognition and face recognition
COMMUNICATE	Senstar Symphony	Streamline display of alarm, video, and location data
RESPOND	Senstar Symphony	Provide response forces with key data, including mobile apps, and accurate location information
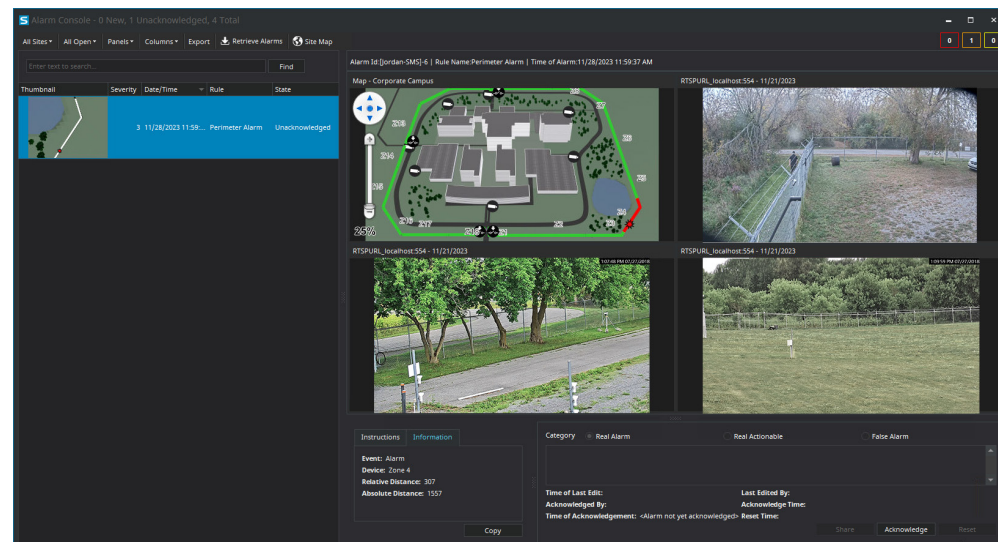
Senstar Symphony's Alarm Console links sensor, video analytic, and access control events to multiple cameras, graphical maps, and event-specific instructions.

EQUIPMENT AND SOFTWARE DESIGNED FOR CRITICAL INFRASTRUCTURE

In addition to effective assessment and response tools, critical entities require scalable solutions that are suitable for deployment across large numbers of sites, are ultra-reliable, maintain a low nuisance alarm rate, and incorporate robust architectures that avoid downtime and unscheduled maintenance visits.

MADE FOR HARSH CONDITIONS

Senstar sensors are designed for use in harsh environments. The outdoor equipment is designed to operate across a wide temperature range (typically –40 to 70 °C) and includes advanced algorithms that minimize nuisance alarms generated by wind, rain, and snow.
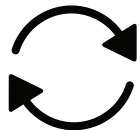
ON-SITE FAULT TOLERANCE

Senstar sensors include support for bi-directional loop networks as well as redundant processors, power supplies and network connections, so that a failure of one component or sensor does not bring down the entire system.

REMOTE MANAGEMENT AND LOCAL FALLBACK

Site sensors can be managed by the E5000 Physical Security Appliance, designed for use at unmanned sites. It offers remote management, WAN/SCADA support, video storage, and local fallback capabilities if network connectivity is lost.

NO-MAINTENANCE VIDEO APPLIANCE

Senstar's Thin Client provides a simple, low-cost way to display live and recorded video, as well as export video to common formats for post-incident analysis. The compact Linux appliance requires no maintenance or regular software updates, making it an easy way to bring surveillance video to those who need it.
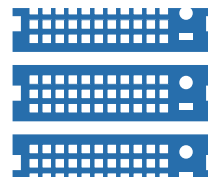
SCALABLE, MULTI-SITE VIDEO MANAGEMENT SOFTWARE

The Senstar Symphony Common Operating Platform uses a scalable architecture that offers a feature set ideal for critical infrastructure operators:

- Edge storage – Video may be stored on-camera or edge devices to prevent the loss of critical video if network connectivity is disrupted.
- Licensing – Per-camera licensing makes Symphony ideal for gradual rollouts, as additional cameras can be added as required. Video analytic licenses are moveable – existing licenses can be repurposed to meet changing security demands.
- Built-in failover – Symphony includes support for redundancy and failover without the use of expensive Microsoft Clustering.

CLOUD-BASED DEVICE MANAGEMENT

The Senstar Enterprise Manager enables system administrators to centrally manage large numbers of video cameras and other security equipment. From a web-based interface, administrators can:

- Monitor the health of the video surveillance system
- Automate software and firmware updates
- Quickly identity offline cameras

PHYSICAL SECURITY SAMPLE PLAN

Physical threats	Equipment theft, vandalism, sabotage and trespassing
Operational threats	Unauthorized access to outdoor equipment Unauthorized access to buildings and indoor systems
General deterrence practices	• Security lighting • Automated PA system • Perimeter signage and warnings • Overt video surveillance • 2-way intercoms at entrances

TACTIC	DETERRENCE	DETECTION	DELAY	ASSESSMENT	COMMUNICATION	RESPONSE
Cut, climb or lift fence fabric	Security fence or wall with outrigging Perimeter lighting PA system	Fence sensor Outdoor people tracking analytic	High quality and maintained security fence or wall	Surveillance system Security lighting 2-way intercom	Automated electronic notifications Email SMS Mobile app) Site security events linked to specific procedures and contact information	Local security forces
Climb gate	Security gate with outrigging Perimeter lighting PA system	Fence or gate sensor Outdoor people tracking analytic	High quality and maintained security gate			
Break or bypass gate lock	Security hardware 2-way intercom Surveillance system	Fence or gate sensor Latch contact Outdoor people tracking analytic	Security hardware			
Tunnel under fence or gate	Below-ground fence structure Hardened surface (e.g. concrete) Surveillance system	Fence sensor Outdoor people tracking analytic	High quality and maintained security fence Hardened surface (e.g. concrete)			
Firearms and explosive devices	Ballistic fencing/walls	Outdoor people tracking analytic Audio sensors				
Ladder-assisted climb	Security fence with outrigging Perimeter lighting PA system	Fence or gate sensor Outdoor people tracking analytic	High quality and maintained security gate			
Vehicle ramming	Security fence or wall	Fence or gate sensor Outdoor vehicle tracking analytic	Security fence or wall			
Elevated position perimeter crossing	Security fence or wall with outrigging	Outdoor people tracking analytic	Security fence or wall with outrigging			
Access via false or misappropriated credentials	Access control system Surveillance system	Schedule-based access License plate and/or face recognition analytics				

1 DETECT INTRUDERS AT THE PERIMETER

Outdoor People and Vehicle Tracking Analytic
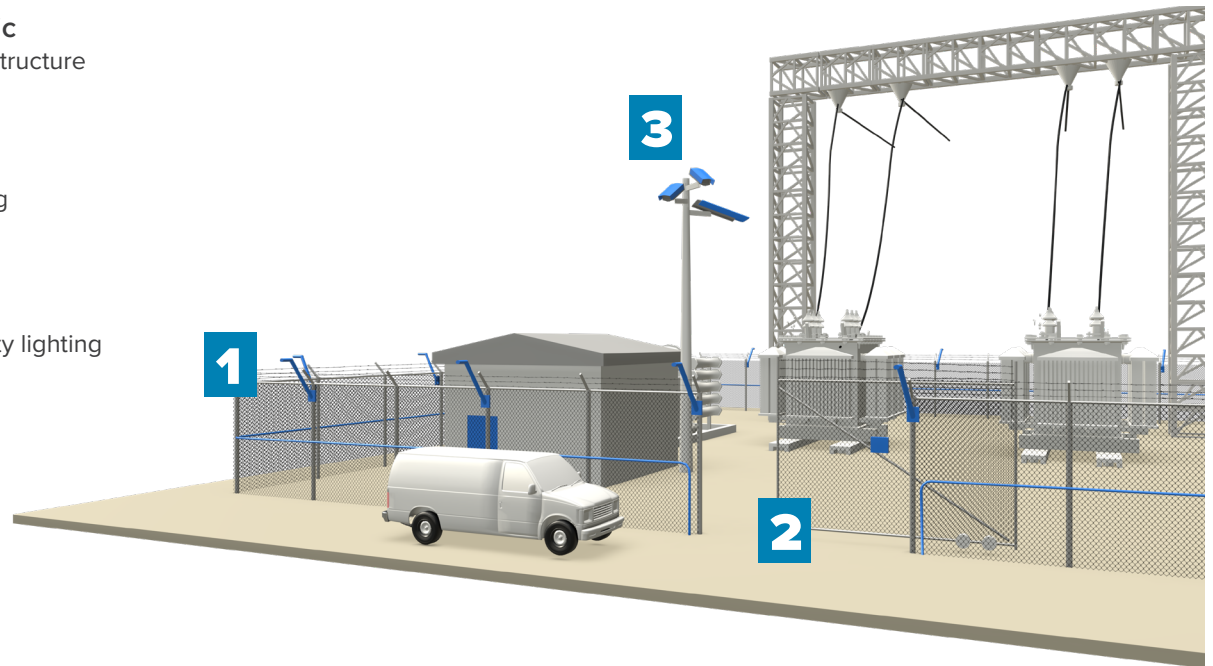Ideal for sites with comprehensive surveillance infrastructure

Senstar LM100
Ideal for new sites or those requiring security lighting

FiberPatrol
Fiber optic sensor, ideal for sites with existing security lighting

FlexZone
Ideal for sites with existing security lighting

2 MONITOR GATES AND OPEN AREAS

Sliding Gates
Monitor gate activity with Wireless Gate Sensor

Swinging Gates
Attach FlexZone, FiberPatrol, or Senstar LM100 directly to gate panels

Open Areas
Monitor open areas with UltraWave microwaves

3 TRANSFORM PASSIVE SURVEILLANCE INTO AN ACTIVE RESPONSE

Symphony supports cameras from all major manufacturers, including low-light and thermal models:

- Fixed cameras – Use outdoor video analytics to detect intruders outside and inside the fenceline

- PTZ cameras – Apply PTZ tracking analytics for hands-free camera control

- Intercoms – Use 2-way audio to deter intruders

- Device control – Trigger local deterent mechanisms, including security lights and pre-recorded messages

- Alert on-call staff – Provide on-call security staff with access to alarms, photos and video feeds, and mobile recording

- Privacy – Meet GDPR requirements via built-in privacy controls, include dynamic masking, configuration retention policies, and granular operator privileges