MARITIME SECURITY @ SEA

DETER

Discouraging access

Securing access to systems and infrastructure and **discouraging** unauthorized entry:

- **Physical**: deny access to unauthorized individuals and deter intrusions in areas or systems

- **Cyber**: establishing resilient IT and OT-infrastructure, enhancing system security, and preventing illegal activities

- **Data**: safeguarding data and confidential information from unauthorized access

DETECT & IDENTIFY

Detect & identify suspicious patterns or anomalies, reducing false alarm rates within a well-defined perimeter

- **Detection** by continuously **monitoring** of the environment around offshore infrastructure and ports, above and below water.

- **Identification** by using relevant **data** from real-time monitoring systems, using advanced **analytics and machine learning** alogrithms

- **Reducing false positives and response time** by continuously optimizing alert procedures and systems, sharing intelligence **(threat level identification/ risk analysis)**

- Ensuring **rapid dissemination of alerts and information**

RESPOND

Minimising time between detection and response, adequate and fast action in the event of intrusions

- Ensuring **readiness to respond** promptly and effectively to any security breach (systems and persons) using **adequate instructions** to respond

- **Effective handling of** security incidents

- Ensuring an **aligned coordination** between different authorities and emergency services

- **Evaluation** & follow-up of incidents and actions to improve resilience