**TRIPLE DEFENCE**

MARITIME



The maritime sector, which until now was considered safe due to the lack of Internet connectivity and the isolated nature of ships in the sea, is showing a 900% increase in cybersecurity breaches on operational technology as it enters the digital era.

Therefore, ensuring the safety and security ons ship cannot be ensured and necessitates a novel security approach which supports connectivity between all of the various systems onboard and onshore.

# 

Maritime organizations need to take appropriate steps to identifying, analyzing, assessing, and communicating cybersecurity risks, and accepting, avoiding, transferring, or mitigating them to an acceptable level. This requires an overall organizational approach of risk management, which involves:

1. Ensuring a clear overview over the various hardware and software systems deployed for delivering different services. In the context of maritime transport, such systems involve Information Technology (IT) as well as Operational Technologies (OT), and how these systems connect and integrate with the shore side, including public authorities, marine terminals and stevedores.

2. Identifying and evaluating key ship board operations, which are vulnerable to cyber-attacks, and performing cybersecurity risk assessments (including assessing potential operational impacts and likelihood of occurrence) which should take into account emerging threats, known vulnerabilities, and operational data in relation to the systems in scope.

Where appropriate, making the link to security assessments carried out for ships (SSAs), port facilities (PFSAs), and ports (PSAs) as set out by EU maritime security legislation. These identify possible security threats to port infrastructure and security weaknesses. Additionally, maritime organizations such as the International Maritime Organisation (IMO) and maritime ISACs may provide insights on threats targeting maritime transport.

3. Ensuring that risk assessments also cover the risks related to personnel daily activities ( e.g. social media usage, personal device usage, data processing, information sharing, etc.).

4. Identifying and implementing risk treatment measures and plans mitigating cybersecurity risks. For example, implementing a comprehensive Information Security Management System (ISMS) and a Privacy Information Management System (PIMS), aligned with other management systems such as Safety Management Systems (SMS) in accordance with the International Safety Management (ISM) Code.

Such management systems (i.e. ISMS and PIMS) involve implementing security (as well as data protection and privacy) controls in order to mitigate and prevent emerging threats affecting security of maritime services and systems (including their data).

5. Taking into account any constraints concerned with asset management and resource planning (that is, constraints that may affect the delivery, maintenance and support of critical systems for operations of essential functions in maritime transport). As for assessments, make a cross-reference where appropriate to requirements of the ISM code, Safety management Systems (SMS) and security plans carried out according to EU maritime safety and security legislation..

Cleopatr@ And Maritime

Maritime safety is a crucial aspect of the shipping industry and technological advances have made it possible to ensure safe and efficient operations at sea. The Cleopatra safety Network module is one of those innovations that has revolutionized the way maritime safety is ensured. This model is designed to provide real-time information on the location, speed and direction of vessels, as well as weather conditions and other critical data that can affect safety at sea. By using this module, ship operators and authorities can make timely and informed decisions to prevent accidents and ensure the safety of crew and cargo.

Maritime Incidents

The impact of the Cleopatra security network module on maritime security. Several case studies have demonstrated the effectiveness of the Cleopatra security network module in improving maritime security. An example of this is the implementation of the module by the port of Rotterdam in the Netherlands. By using this module, the port was able to reduce the number of incidents and accidents, improve ship traffic management and improve communication between ships and port authorities. This resulted in significant improvements in safety, efficiency and profitability for the port and the wider shipping industry.

We worked hard to develop the best existing solution to avoid and protect your vessels and cargo, anywhere from shorter trajects to no fire incidents or other types of disasters.

It provides real-time information on vessel movements and environmental conditions to generate alerts and warnings in case of potential security risks. The module also enables seamless communication between ships, ports and other stakeholders, ensuring better coordination and collaboration for safe and efficient operations.

The Cleopatra Safety Network Module offers several benefits to the shipping industry, including improving safety, efficiency and profitability. By providing real-time information on vessel movements and environmental conditions, the module enables better decision making for safe and efficient operations, it also helps reduce the risk of accidents and minimize the impact of any incidents that may occur.

Additionally, the module can help optimize ship routes and reduce fuel consumption, resulting in cost savings and environmental benefits. Overall, the Cleopatra security network module is a game-changer for maritime security and has the potential to transform the shipping industry.

ADAPT BEFORE TOO LATE.

© TRIPLE DEFENCE

Backoffice@tripledefence.com