



**FRANCE CYBER MARITIME**

Safeguarding the Maritime Digital Community

# FRANCE CYBER MARITIME'S MISSION :

## « Contribute to the strengthening of cybersecurity of the maritime and port sectors »

### Action

Increase the resilience of maritime and port operations to cyber threats



Operate the M-CERT (*Maritime Computer Emergency Response Team*) which provides information and assistance to all maritime and port operators

### Action

Develop a network of expertise in maritime cybersecurity



Foster the creation of **high value-added services** adapted to the needs of the industry





## OUR MEMBERSHIP BOARDS:

- « **Public-sector Actors** » : administrations, state agencies and local authorities
- « **End Users** » : operators in maritime and port sector from **France and Europe**
- « **Solution Providers** » : qualified providers of cybersecurity solutions

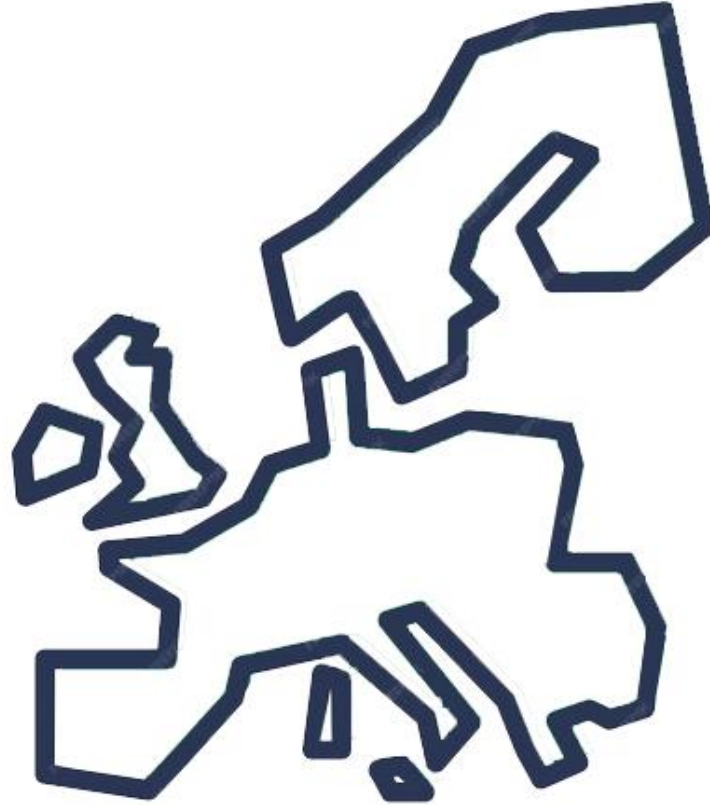




# OUR COMMUNITY



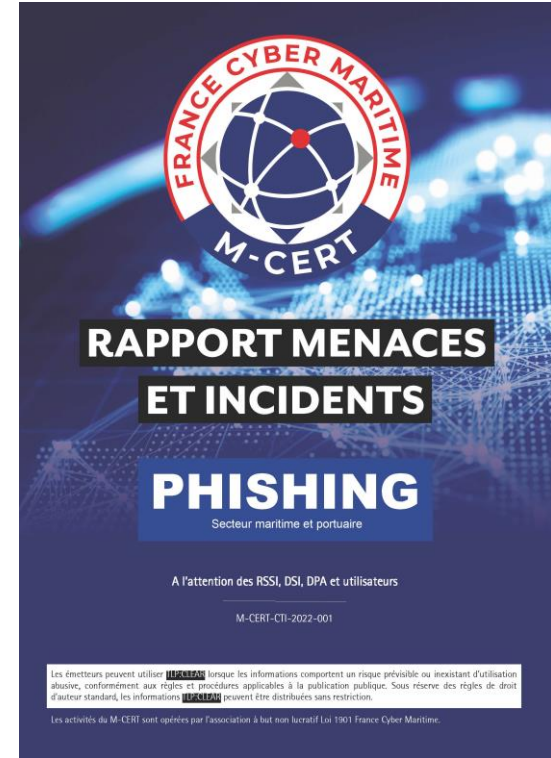
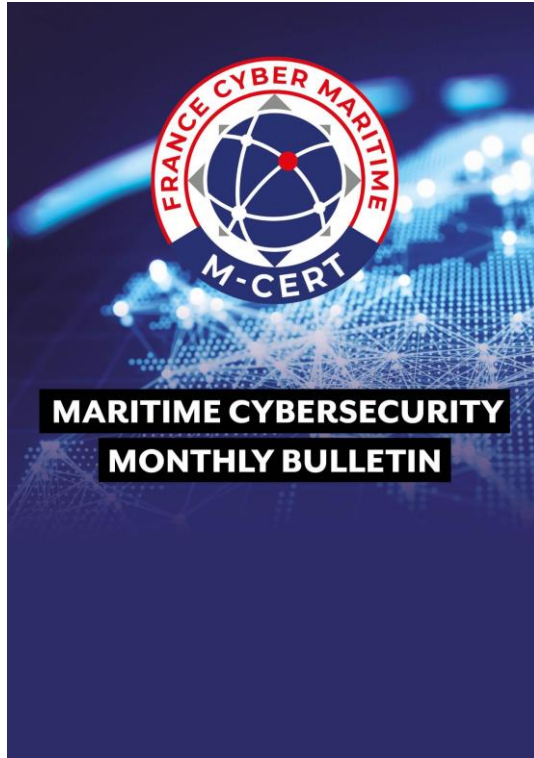
# Membership Open to the European Maritime & Port Sectors in 2025



# 1. M-CERT: ANALYSING, SHARING AND PROVIDING ASSISTANCE

The **M-CERT** (*Maritime Computer Emergency Response Team*) is a **national centre in charge of monitoring and analysing cyber threats as well as sharing information and providing assistance to the maritime and port sector.**

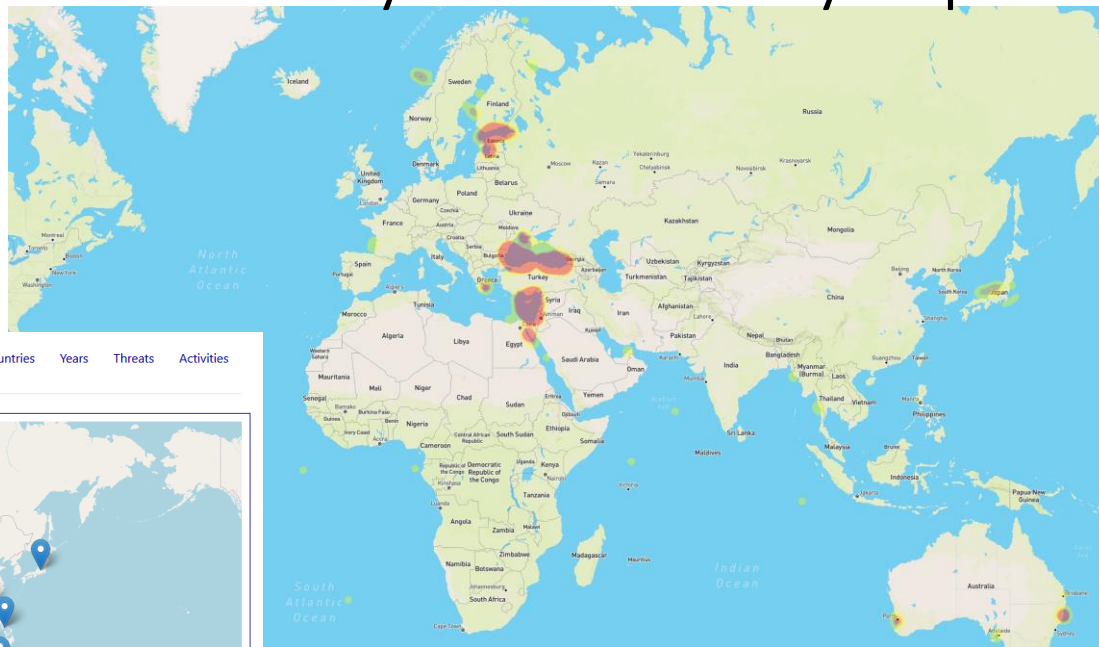






# Maritime Cybersecurity Incidents Dataset

## Twice-daily GNSS Inaccuracy Map



ADMIRAL dataset

Home **Map** Statistics Continents Countries Years Threats Activities



Leaflet | Source: France Cyber Maritime - M-CERT - ADMIRAL dataset | Map data © OpenStreetMap contributors

Files generated on Thursday, 02nd November 2023.

ADMIRAL is licensed under the Creative Commons license. Copyright © France Cyber Maritime 2023.





# National and International Sharing Agreements



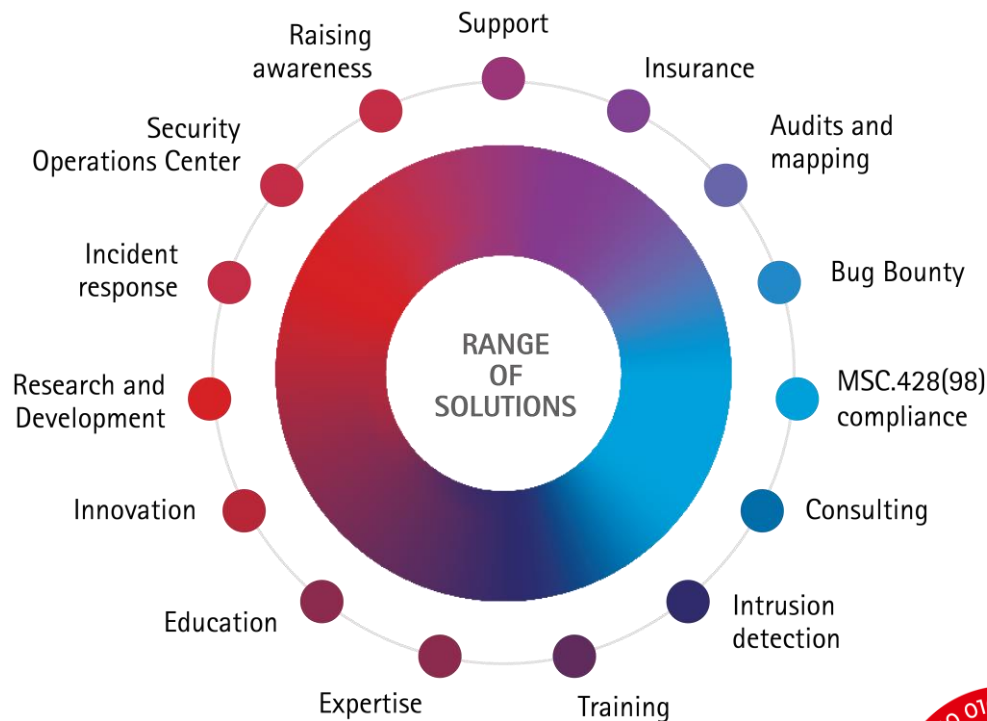
## Motion Design M-CERT



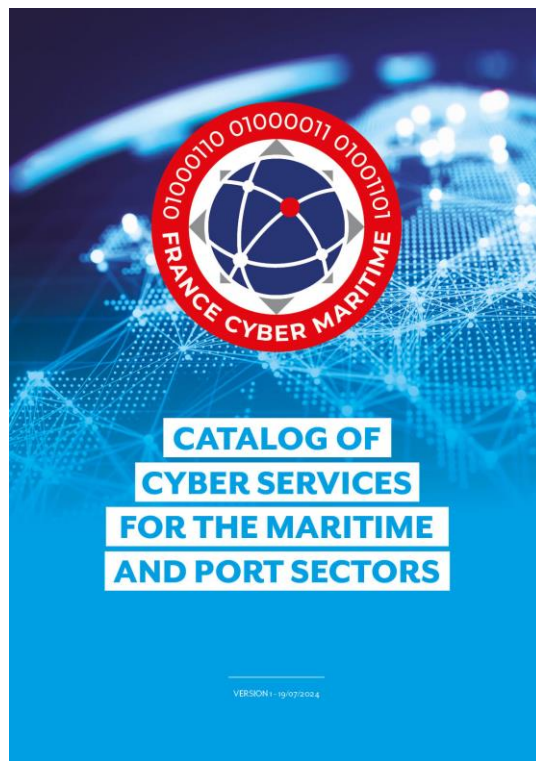
## 2. DEVELOP A NETWORK OF EXPERTISE

### TAILORED CYBER SECURITY SOLUTIONS FOR THE MARITIME SECTOR

With the support of its members, France Cyber Maritime analyzes the needs of maritime operators and advises them in order to identify the most suitable and efficient solutions.



## Catalogue of Services



## Maritime Bug Bounty

28 NOVEMBRE 2023

# Battleship

ÉDITION 2023

## APPEL À PARTICIPATION

**BUG BOUNTY, KESAKO ?**  
Un programme de Bug Bounty est une approche proactive mobilisant une communauté de hackers éthiques qui ont pour mission de détecter des failles sur des systèmes d'information afin d'identifier des vulnérabilités et de les résoudre en échange de primes (bounties).

**UNE PREMIÈRE ÉDITION RÉUSSIE !**  
En mai 2022, France Cyber Maritime et YesWeHack ont organisé en distanciel, le premier événement européen de Bug Bounty dédié au monde maritime et portuaire : Battleship.

Brittany Ferries a soumis pendant 48h certains de ses systèmes d'information à une dizaine de hackers éthiques. Résultat : plusieurs vulnérabilités détectées ont été corrigées en direct par l'armateur, permettant un renforcement immédiat de sa posture de cybersécurité.

**PRÉSENTATION DE BATTLESHIP**  
Après le succès de ce premier événement, France Cyber Maritime et YesWeHack ont décidé de renouveler l'expérience en 2023. Cette année, en plus de bénéficier à la communauté maritime et portuaire française, l'événement sera également proposé aux acteurs européens qui souhaitent renforcer leur posture de cybersécurité.

Battleship 2023 se déroulera à nouveau en distanciel, le **mardi 28 novembre 2023** pour une durée totale de 24 heures. De nombreux hackers éthiques seront mobilisés pour rechercher les vulnérabilités à corriger sur les systèmes d'information des participants.

Cette nouvelle édition sera valorisée lors des Assises de l'Économie de la Mer, principal rendez-vous du secteur maritime et portuaire français.

**POURQUOI ET COMMENT PARTICIPER ?**  
Pour vous, entreprises maritimes et portuaires, mettre à l'épreuve vos systèmes d'information vous permet d'identifier des vulnérabilités et de les résoudre en un temps record. Un tel événement est une occasion unique de rencontrer des chercheurs, comprendre leur mode de fonctionnement, discuter avec eux de leurs découvertes, et ainsi renforcer votre posture cyber.

Si l'événement vous intéresse et que vous souhaitez en savoir davantage sur les modalités pratiques, n'hésitez pas à nous contacter dès à présent par e-mail : [contact@france-cyber-maritime.eu](mailto:contact@france-cyber-maritime.eu)



YES WE H/CK

## Pooled & Shared M-SOC Project







## WHITE PAPER

### CYBERSECURITY OF MARITIME DRONES AND AUTONOMOUS SHIPS

07/11/2023



## WHITE PAPER

### AWARENESS, EDUCATION & TRAINING IN MARITIME CYBERSECURITY

Oct 2024



# Maritime Fairs and Awareness Tours

**Les escales —  
cyber  
— en régions**

Organisées par  


En collaboration avec  
  


**RÉGION  
HAUTS-DE-FRANCE**

**19 JUIN 2024**  
**CCI HAUTS-DE-FRANCE**  
299 Bd de Leeds, 59 000, Lille

France Cyber Maritime organise sa deuxième édition des « Escales cyber en régions » à la CCI des Hauts-de-France, le 19 juin prochain.

Ces escales sont l'occasion de rencontrer, d'échanger et de partager, le temps d'une journée, avec les acteurs locaux du monde maritime, portuaire et de la cybersécurité.

Cet événement s'intègre au séminaire de l'Axe Nord, organisé par la Préfecture des Hauts-de-France et NORLINK.

**INSCRIPTION**  
<https://my.weezevent.com/escale-cyber-en-region-hauts-de-france>

  
**LILLE**



# Technical Webinars

**WEBINAIRES**

**CAP SUR LA  
CYBER**

ORGANISÉS  
PAR  






**MSC.428(98)**





## CONTACTS

Xavier Rebour

Managing director

[xavier.rebour@france-cyber-maritime.eu](mailto:xavier.rebour@france-cyber-maritime.eu)

[www.france-cyber-maritime.eu](http://www.france-cyber-maritime.eu)

M-CERT

[contact@m-cert.fr](mailto:contact@m-cert.fr)







[www.france-cyber-maritime.eu](http://www.france-cyber-maritime.eu)

