MARLINK

H1
2024

Global maritime cyber threat report

Security
Operations
Centre

FORTINET sekoia paloalto NETWORKS CROWDSTRIKE AVANAN THE CLOUD SECURITY PLATFORM tenable CISCO Microsoft

Executive summary

During the first half of the year, Marlink's Security Operations Centre actively monitored more than 1800 vessels across the maritime industry, including cargo ships, cruise liners, research vessels, superyachts, tankers, and offshore support vessels. The monitoring process involved continuous surveillance and analysis of various cyber activities across these assets to ensure the security and integrity of critical maritime operations. The focus was set on identifying and mitigating potential cyber threats that could disrupt operations, compromise data, or lead to financial loss.

Malicious activity in the first half of this year has significantly increased compared to the previous year. We have observed a continued rise in common threats such as Command & Control (C&C) attacks, along with the evolution of botnet attacks, which are growing in both complexity and volume.

1800
Vessels monitored

Contents

Monitored devices

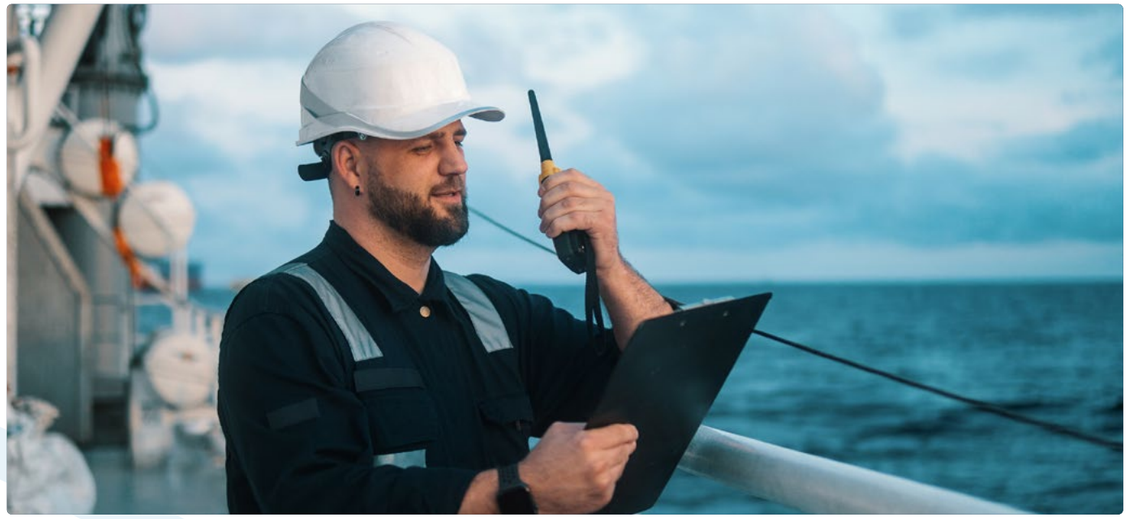
The SOC's effectiveness is significantly influenced by the number and type of devices monitored. These devices range from onboard systems on vessels to corporate network devices within the monitored vessels. Each device type presents unique security challenges, requiring tailored monitoring approaches.

13 K
Computers managed

1800
Firewalls managed

8700
EDR devices protected

8300
Mailboxes protected



Mail activity

E-mail remains a primary vector for cyber attacks, particularly through phishing and malware distribution. The SOC's e-mail protection efforts are critical in safeguarding the organisation's communication channels.

5.2 Mio Analysed e-mails = **4.3 Mio** Delivered e-mails + **900 K** Blocked e-mails

Endpoint security

10.8 K
Endpoints with EDR

23.4 K
Malware detections

178
Ransomware detections

The indicators above show that 10.8K endpoints are secured with Endpoint Detection and Response (EDR) systems, which provide real-time monitoring, threat detection, and automated response. EDR enhances visibility into endpoint activity and enables swift action against threats, minimising damage.

The detection of 23.4K malware instances highlights the effectiveness of EDR in identifying and containing widespread malware, while 178 ransomware detections show its capability to quickly mitigate more severe threats. EDR's presence strengthens an organisation's security posture, reducing the risk of cyberattacks and ensuring more resilient defences against both malware and ransomware.

Event metrics, alerts & incidents

The volume of ingested events is a key indicator of the SOC's activity level and its capacity to handle large-scale data analysis. Each event type represents a different facet of the monitored environment, contributing to a holistic view of the security landscape.

The SOC's primary function is to detect and respond to security alerts and incidents. The volume and nature of these alerts provide insights into the threat landscape and the effectiveness of the SOC's detection capabilities.

H1 2024 SOC insights

Firewall events
+50 Bio

Number of security events
+14.8 Bio

Number of alerts
+1.4 Mio

Number of managed major incidents
79

Most detected threats

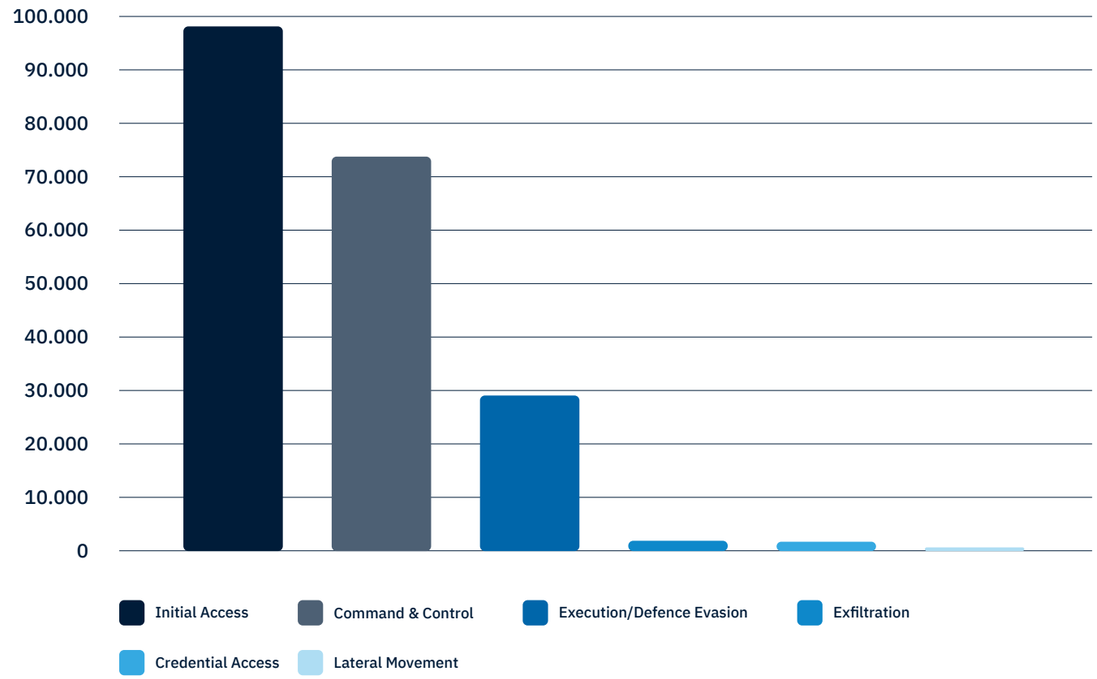
In the first six months, **Initial Access tactics** were the most prevalent, accounting for **48% of the 204,763 incidents**, primarily involving phishing fraud and spam abusive content. **Command & Control (C2)** followed closely at **36%**, driven largely by the execution of malicious files and links. **Execution and Defence Evasion tactics**, often seen through intrusion attempts, made up **14%** of the total incidents.

While **Exfiltration** (focused on data theft) and **Credential Access attacks** were less frequent, they still present significant risks, highlighting the importance of strong defences against both entry and persistence techniques.

The key takeaway from this analysis is clear: attackers are relentless in targeting multiple stages of the attack chain, from phishing to execution, and ultimately, command and control. A **well-equipped Security Operations Centre (SOC) is critical** in detecting and responding to these threats at every stage.

By providing continuous monitoring and rapid incident response, the SOC helps to minimise the potential impact of attacks. To stay ahead, organisations must implement a proactive, layered defence strategy, with the SOC serving as a key line of defence against both initial compromise and post-breach activities.

Cyber threats by tactics



The most common threats

01

Phishing fraud

Remains the primary threat:
Phishing fraud continues to be the leading tactic used by attackers to gain access to corporate networks. Customers need to be proactive in educating their workforce and implementing advanced e-mail security solutions.

02

C&C/Blacklist malicious traffic

Is a growing concern:
The increase in blacklisted malicious traffic highlights the importance of maintaining up-to-date threat intelligence feeds and applying strict security policies to prevent unauthorised connections to high-risk sites.

03

Spam abusive content

Is more than a nuisance:
While spam is often viewed as a simple annoyance, it serves as a vehicle for more dangerous attacks, including phishing and malware distribution. Vigilance against spam is a crucial defence strategy.

04

IDS alter intrusion attempts

Are early warning signs:
IDS alerts provide early detection of potential attacks, allowing security teams to act before full-scale compromises occur. Monitoring these alerts and responding promptly is critical to defending against advanced persistent threats.

Critical detected attacks

2024 Q1 and Q2: While the volume of botnet activity increased substantially, new botnets emerged, leveraging more advanced evasion techniques. AI-enhanced botnets began to surface, showcasing more sophisticated automation capabilities.

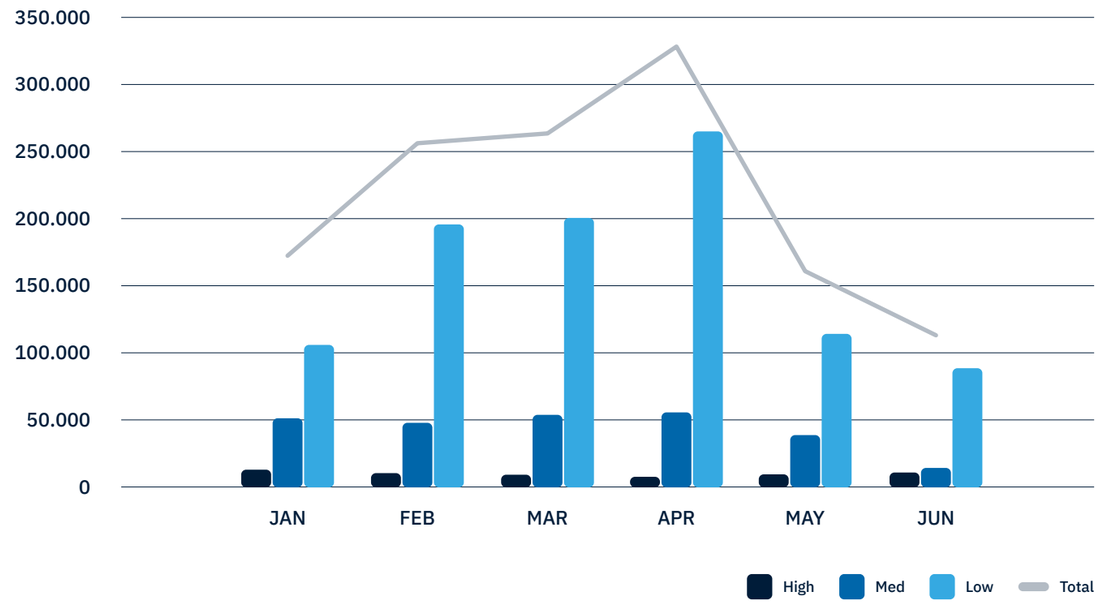
Mirai's Rise: The sharp increase in Mirai botnet activity in 2024 points to the rising importance of IoT security, as this botnet has historically targeted IoT devices.

Decline in Traditional Botnets: The disappearance of Prometei, SystemBC, and Torpig.Mebroot in 2024 suggests improved mitigation efforts, possible takedowns, or shifts in attacker focus away from these older botnets.

Shift in Attack Landscape: Overall, the data reflects a dynamic botnet landscape where certain botnets decline while others, like Mirai, gain prominence.

IDS_Attacks.signature	Q1 2023	Q2 2023	Q1 2024	Q2 2024
AAEH.Botnet				2
Bladabindi.Botnet	0	4	57	9
Bredolab.Botnet			4	
DarkGate.Botnet			9	
Gh0st.Rat.Botnet	0	2	29	7
Mirai.Botnet	0	0	71	269
Mozi.Botnet	22	63	2	30
Necurs.Botnet				2
NovaLite.Botnet				2
Prometei.Botnet			433	269
STRRAT.Botnet				2
Sality.Botnet	2	0		4
Supershell.Botnet			2	
SystemBC.Botnet			374	360
Torpig.Mebroot.Botnet			4129	1105
UDPoS.Botnet			39	77
Zeroaccess.Botnet			1	1
	24	**24**	**5150**	**2139**

Number of alerts by severity and month



During the first half of this year, the number of high alerts remained stable compared to those handled in 2023. However, medium and low alerts saw a significant rise, increasing from 100,000 in January to 270,000 in April, compared to an average of 75,000 in 2023.

This surge was mitigated in May and June thanks to optimisation efforts in detection and enrichment processes.

Enhancing vessel security in an evolving maritime landscape

Josep Estevez,
Maritime SOC Director

New insights reveal a surge in sophisticated cyber threats targeting vessel operations, pushing the boundaries of existing security measures and demanding a proactive approach to maritime cyber security.

During the first half of the year, the threat landscape in the maritime environment has continued to evolve and surprise us compared to what we saw in 2023.

Monitoring up to **1,800 vessels,** adding visibility into events from endpoint protection solutions (EDR), firewalls, and e-mail security, along with the context provided by intelligence capabilities, has allowed us to gain deeper insight into what actions to take to prevent attacks. Malicious actors are **evolving their attack patterns** and launching fraudulent campaigns that bypass previously effective security controls, **such as two-factor authentication,** forcing us to react and raise the security level to ensure operations are safeguarded.

Threat intelligence

Cyber activities targeting the maritime industry

In the first half (H1) of 2024, the Threat Intelligence team within Marlink's Security Operations Centre has observed the following activities carried out by malicious actors:

Phishing
Malicious actors sending fraudulent e-mails or messages to trick individuals into revealing sensitive information like passwords or financial details. Phishing attack trends include HTM/HTML documents with embedded links and QR codes to credential harvesting login landing pages hosted on difficult-to-block infrastructure (e.g. Microsoft), and typosquat and BEC senders. Phishing tactics included the use of open redirects and reverse proxies.

Commodity malware
Widely available malware typically sold or distributed for common use by cybercriminals, often used in large-scale, automated attacks. For example, Agent Tesla phishing payload used for information theft.

DDoS
Attacks where multiple systems overwhelm a target server or network with excessive traffic, causing it to become unavailable to users, especially port infrastructure and maritime transportation companies.

Typosquat domains and DMARC
Domains that mimic legitimate websites by using slight misspellings, aimed at tricking users into visiting them to steal information or distribute malware. Maritime organisations have been spoofed by different domains.

Password spraying
A type of brute-force attack where attackers try a few commonly used passwords across many accounts to avoid detection and gain unauthorised access. VPN gateway user accounts have been widely exploited by trying common passwords.

Scanning and probes
Systematic examining systems or networks for vulnerabilities or open ports to exploit by attackers, comprising application server protection violation attempts, SSH failed authorisation attempts, SQL scanning, vulnerability scanning, and firewall probing.

Main cyber threats & motivations

In the first half of the year, cyber attackers targeting the maritime industry had a few main motives:

Operational disruption
Attackers aim to disrupt or damage critical systems, causing significant interruptions to business operations, often with the intent of crippling an organisation or industry.

Financial fraud
Malicious actors exploit systems or individuals within the maritime industry to commit financial theft or fraud, often targeting monetary transactions, contracts, and sensitive financial data.

Espionage
Cyber actors engage in spying activities to steal sensitive or confidential information, often for competitive advantage, political gain, or military intelligence.

Hacktivism
Hacktivist groups disrupt maritime operations to make political or social statements, using cyber attacks as a form of protest or activism.

Threat actors/ most active groups

The main malicious groups observed during the period targeting the maritime sector include the following:

APT28

Also known as Fancy Bear, this group is known for cyber espionage and targeting government, military, and political organisations.

APT29

Also referred to as Cozy Bear, this group specializes in long-term cyber espionage campaigns targeting governmental, diplomatic, and healthcare sectors.

APT Callisto

A threat actor group focused on targeting political and military organisations through phishing campaigns and information-stealing attacks.

Pensive Ursa

A group known for advanced espionage operations, often targeting governments, defence contractors, and critical infrastructure in order to gather sensitive data.

Sandworm

A notorious cyber espionage and cyberwarfare group, responsible for disruptive attacks on critical infrastructure, including energy grids and media.

Stately Taurus

A cyber espionage group known for targeting high-profile organisations, often focusing on intellectual property theft and sensitive business or government information.

Volt Typhoon

A threat group that focuses on cyber espionage activities, primarily targeting organisations in the telecommunications and defence industries.

Earth Krahang

A cyber espionage group known for conducting attacks on government, military, and commercial entities, often using sophisticated phishing and malware campaigns.

Ransomware groups

Ransomware remained one of the primary threats to maritime targets in the first half of the year, as it significantly disrupts operations and causes considerable economic damage. Attacks have paralysed critical systems, delayed shipments, and compromised logistics, resulting in operational downtime and costly ransom demands. This combination of operational impact and financial loss makes ransomware remain a major concern for the maritime industry.

The ransomware groups that have been observed targeting organisations within the maritime industry are as follows:

AlphV/BlackCat

A highly sophisticated ransomware group that operates on a ransomware-as-a-service (RaaS) model, known for encrypting data and threatening to release stolen information unless a ransom is paid.

BlackByte

A ransomware group that has attacked multiple critical industries, including maritime, using advanced encryption techniques to lock data and demand ransom payments for decryption.

8Base

A relatively new but aggressive ransomware group that leverages double extortion tactics, threatening to leak stolen data if victims do not pay the ransom.

Akira

A ransomware gang that primarily targets medium and large enterprises, encrypting data and exfiltrating sensitive information for extortion purposes.

LockBit 3.0

One of the most prolific ransomware groups, known for its ransomware-as-a-service model, focusing on large-scale attacks, including on maritime organisations, through highly advanced encryption and extortion tactics.

Play

Known for its fast-evolving ransomware techniques, Play encrypts files and demands large ransoms, focusing on disrupting business operations across various industries, including maritime.

BianLian

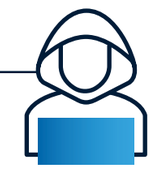
This group initially focused on data encryption but has since shifted to a strategy of pure extortion, threatening to expose sensitive data if victims refuse to pay.

BlackBasta

A ransomware group that specializes in double extortion, often targeting large organisations by encrypting their data and threatening to publicly release stolen files.

Cactus

A relatively stealthy ransomware group that uses encrypted communications and advanced evasion techniques to deliver ransomware payloads and demand high ransoms.



TOP 5 known exploited vulnerabilities by ransomware groups

During H1 ransomware actors conducted attacks that exploited the following product vulnerabilities:

Microsoft SharePoint Server

(CVE-2023-29357)
(CVE-2023-24955)

Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core

(CVE-2023-35082)

Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defence (FTD)

(CVE-2020-3259)

ConnectWise ScreenConnect

(CVE-2024-1709)

Fortinet FortiClient EMS

(CVE-2023-48788)

The rise of reverse proxy phishing

MJ Casado de Amezua, Threat Intelligence Analyst

The danger of reverse proxy phishing lies in its ability to bypass multi-factor authentication (MFA), making the victim feel like everything is normal while attackers gain full access to sensitive systems.

During the first half of 2024 (H1 2024), a significant portion of the threats neutralized by the SOC have continued to follow the most common attack vector seen since 2022: phishing. However, in this period, there has been a notable increase in a more advanced form known as 'reverse proxy phishing'.

Phishing is a classic cyberattack method where attackers impersonate legitimate entities (like banks or service providers) to trick users into providing sensitive information, such as login credentials or financial data. Traditional phishing often relies on fake websites or fraudulent e-mails to capture user data.

'Reverse proxy phishing', on the other hand, is a more sophisticated version. Instead of simply creating a fake website, the attacker sets up a 'proxy' that sits between the legitimate website and the victim. This proxy captures the user's credentials and, in real-time, forwards them to the actual site, making the victim feel like everything is normal. The danger of this method lies in the fact that it can bypass multi-factor authentication (MFA), which is commonly used to protect sensitive systems.

Reverse proxy phishing opens the door to serious cybersecurity threats such as Command and Control (C&C) systems, Botnets, and Remote Access Trojans (RATs). Once attackers gain access to a network, they can deploy C&C infrastructure to remotely control compromised systems. This could enable the creation of botnets—large networks of infected devices used for malicious activities like Distributed Denial of Service (DDoS) attacks. Additionally, attackers may install RATs, granting them full control over the victim's machine, allowing them to monitor activity, steal more data, or execute commands covertly.

In the maritime sector, these attacks can significantly impact operations, from the disruption of shipping logistics to the manipulation of sensitive communication systems. Delays, loss of reputation, and costly recoveries are just a few of the possible outcomes.

To combat these threats, it is critical that maritime companies adopt advanced security technologies. SOCs must enhance their monitoring capabilities with real-time threat detection, AI-driven behavioral analysis, Threat Intelligence, and stronger MFA solutions. By doing so, organisations can better protect themselves from this evolving cybersecurity threat, ensuring safer and more resilient operations.

Infostealing

During H1 the volume of cybersecurity incidents involving infostealers has increased significantly, and maritime victims have been no exception.

Infostealers are a type of malware designed to steal sensitive information from an infected system, such as login credentials, financial data, browser history, and other personal or corporate information.

The maritime industry relies heavily on interconnected systems and digital platforms to manage logistics, shipping routes, and vessel operations. If compromised by infostealers, these systems can expose the sector to significant risks, such as unauthorised access to operational controls, data breaches, financial fraud, and even larger-scale cyberattacks.

Among the most common infostealers spotted during H1 are: RedLine, Raccoon, Vidar, Mars Stealer, and LokiBot.

01

Initial infection

A malicious file is downloaded by the victim after clicking on malvertising unwillingly while web browsing.

02

Execution

The payload executes the malicious code. It uses an automated script that avoids detection by security software.

03

Credential and data collection

The infostealer searches the system for stored credentials and sensitive information (passwords, autofill data, cookies): web browsers, FTP clients, cryptocurrency wallets, and e-mail.

04

Data exfiltration

The stole data is encrypted and sent back to a remote command and control (C2) server controlled by the attacker.

05

Persistence mechanism

The infostealer installs persistence mechanisms to remain on the device and continue stealing information over time.

06

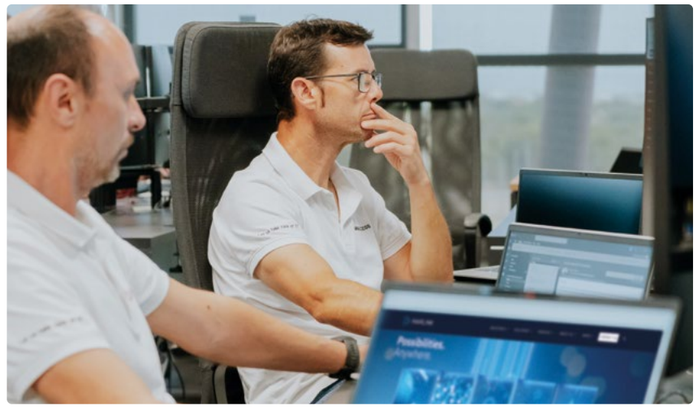
Exploitation of stolen data

The attacker uses the stolen credentials for further attacks (i.e. financial fraud), or sells the data on the dark web for profit.

Key strategies for strengthening your cyber security defences

Vigilance and proactive measures are essential

Regular training, strong e-mail security, and advanced detection systems play a vital role in reducing the risk of phishing, spam, and other malicious activities.



Timely incident response is crucial

SOC teams must remain vigilant and respond to alerts in real time to minimise potential damage. Automated response mechanisms can be implemented to reduce manual intervention and speed up threat containment.

Continuous improvement of security posture

As threat actors evolve, so must security defences. Continuous monitoring, updating blacklists, improving detection systems, and refining incident response processes are essential in staying ahead of the threat landscape.

SOC by
the numbers

Our SOC team operates around the clock to safeguard over **1800 vessels.** In addition to monitoring security alerts and incidents, we deliver **managed security services** and **professional services** to ensure end-to-end protection for these vessels.

+8700
EDR devices protected

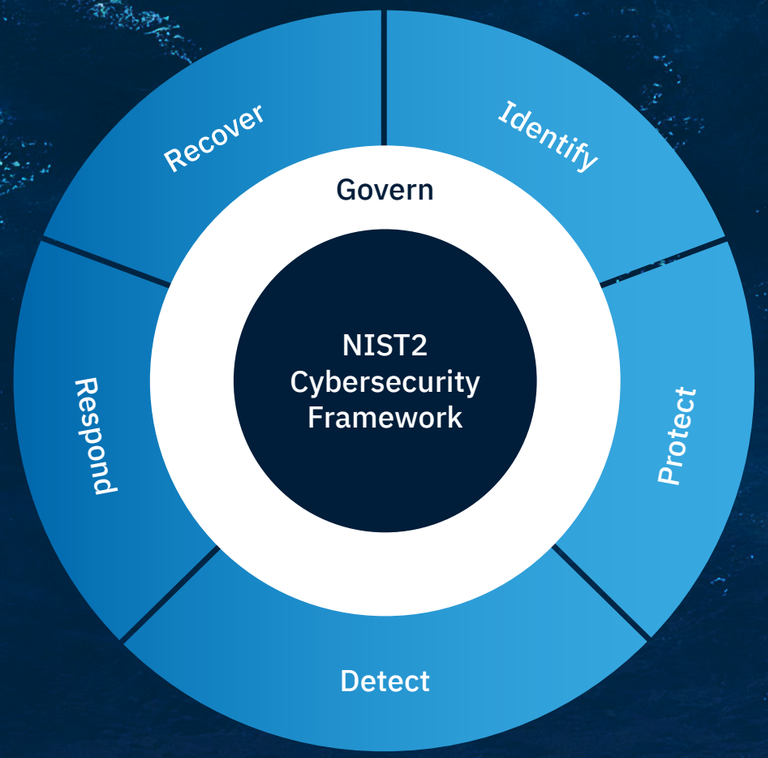
1800
Managed vessels

+1800
Firewalls managed

+161 K
High severity vulnerabilities identified

+8300
Protected mailboxes

+130
Reports submitted



Secure your
maritime operations

At Marlink, our cyber security solutions are designed to seamlessly protect both IT and OT systems, ensuring smooth, uninterrupted operations while defending against cyber threats. With real-time monitoring and rapid response capabilities, our solutions allow fleet managers to maintain robust security without compromising performance. Our security services deliver peace of mind, keeping your crew and vessels secure while ensuring operational continuity.

MARLINK

Contact Marlink for a Cyber Security Consultation

Americas: +1 (310) 616 5594 | +1 855 769 39 59 (toll free)
Asia Pacific: +65 64 29 83 11
EMEA: +33 (0)1 70 48 98 98
sales.americas@marlink.com
sales.asia@marlink.com
sales.europenorth@marlink.com
sales.emea@marlink.com
www.marlink.com