POSSIBILITIES

Cyber intelligence report executive summary

2026

ANYWHERE

Key insights from Marlink's 2026 Cyber intelligence report, highlighting the risks, trends, and priorities for the maritime, enterprise, and critical infrastructure sectors.

MARLINK | OMNIACCESS | TELEMAR TNL | MARLINK CYBER

Welcome from our Marlink Cyber President — Nicolas Furge

What our people are seeing in the field is clear. As IT and OT environments become increasingly connected, cyber risk is growing faster than many organisations can manage. The findings of our report show that around 60% of the sites and vessels we assess rely on shared IT/OT infrastructure that is poorly documented and inadequately secured, leaving critical operations exposed.

Attackers recognised this shift long before many organisations did. Rather than forcing their way in, they exploit stolen credentials and move undetected through networks for weeks or even months. We have entered an era where the priority is no longer solely to prevent intrusions, but to detect them quickly and contain them before they impact operations.

Against this backdrop, regulatory expectations are intensifying (NIS2, DORA, IACS UR E26 and E27) raising the baseline for cyber resilience. Compliance is important, but it is only the starting point. Real resilience is the ability to detect attacks, respond effectively, and keep operating when disruption occurs.

This executive summary distils the key findings, insights, and recommendations from **our full cybersecurity intelligence report** into a concise briefing. I encourage you to use these insights to assess your own organisation's preparedness and identify opportunities to strengthen resilience. Those who act today will be best placed to meet tomorrow's challenges.

Nicolas Furge
President, Marlink Cyber

60%

Around 60% of sites and vessels assessed relied on shared IT/OT infrastructure, with undocumented assets and poorly secured connections creating cyber exposure.

Critical infrastructure remains exposed

7,793

Reported ransomware attacks rose from 5,740 in 2024 to 7,793 in 2025, with critical sectors accounting for more than half of incidents.

Critical industries remain a prime target

69%

Compromised credentials accounted for 69% of identified risks, compared with just 12% linked to vulnerability exploitation.

Attackers now prefer stolen credentials over software flaws, and the gap is widening.

Find the full report here

Key findings

This report draws on insights from **more than 200 cybersecurity assessments** conducted across our monitored sites, we assessed many vessels and facilities multiple times to track maturity over time. These **include 160 technical security tests** and red-team engagements across maritime, offshore, and critical infrastructure environments. Together, they reveal the key trends, attack patterns, and risks shaping today's cyber threat landscape.

What the data tells us.

33%

of technical assessments identified vulnerabilities that could have a significant impact on operations if exploited.

1 in 3 environments contained critical security weaknesses

20%

of phishing recipients clicked malicious links, reinforcing that stolen credentials remain one of the easiest ways into an organisation.

Attackers don't hack — they log in

82%

of observed attacks focused on operational environments, with maritime IT and crew networks accounting for the vast majority of activity.

Operational environments remain the primary target

Our red-team ethical hacking exercises repeatedly showed that attackers could achieve full domain compromise by chaining together multiple moderate vulnerabilities rather than exploiting a single critical flaw.

Attackers don't need one big flaw, they exploit several small ones

Key takeaways

- Cyber attacks are increasingly identity-driven, with attackers exploiting legitimate credentials and everyday tools rather than sophisticated malware.
- Organisations must move beyond prevention alone and focus on early detection, governance, and resilience to reduce operational risk.

Sector deep dive: maritime cybersecurity

Crew networks dominate detected maritime cyber alerts

As operational technology becomes more connected, threats detected in crew or IT networks can create wider vessel exposure. Although fewer than 1% of alerts were attributed to OT/ICS environments, limited visibility across legacy OT means threats may be harder to detect—and their operational impact can be critical.

82%

of alerts were detected in crew network zones.

17%

of alerts were detected in network support environments.

<1%

of alerts were attributed to OT/ICS, but limited visibility may mask exposure.

Why it matters

Connected crew, business and operational environments can allow a compromise to reach critical vessel systems. With limited visibility across legacy OT, threats may remain undetected until they disrupt operations, affect safety or create regulatory and financial exposure.

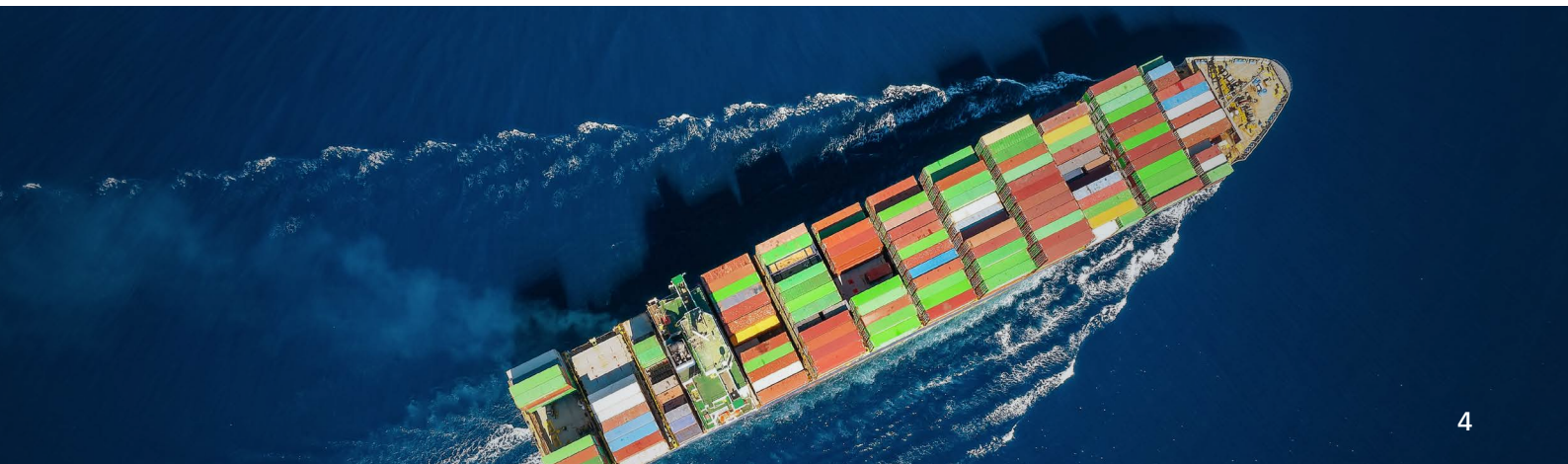
Find the full report here

Key takeaways

01 **Separate critical environments**
Segment crew, business and OT networks to restrict pathways and limit the spread of threats

02 **Build visibility safely**
Discover assets and passively monitor OT activity without disrupting sensitive vessel systems

03 **Assess and prepare**
Identify technical and governance gaps, prioritise action and prepare for incident response



Sector deep dive: energy, enterprise, and critical infrastructure

Cyber risk in energy and infrastructure shifts from compliance to enforcement

Regulation (NIS2, DORA, and CRA) is pushing energy, enterprise and critical infrastructure organisations from box-ticking compliance toward demonstrable resilience. Attackers increasingly operate inside trusted environments, prioritising discovery and credential access over noisy execution, while IT/OT convergence and third-party access continue to widen the attack surface.

20%

Mapping systems and accounts was attackers' top tactic, cited in 20% of SOC-observed incidents in 2025

60%

SOC now focuses mainly on host-level activity to catch attackers moving internally

41%

Peak suspicious-message reporting rate reached in phishing simulations

Find the full report here

Why it matters

For energy and critical infrastructure operators, this shift means resilience — not just compliance — will determine regulatory standing, operational continuity and safety outcomes. Weak identity governance, IT/OT segmentation, and third-party oversight leave critical systems exposed to disruption.

Key takeaways

01 **Strengthen identity and access governance**
Enforce strong authentication, review privileged access and monitor identity activity for misuse

02 **Improve visibility across hybrid IT/OT**
Correlate host, network and identity telemetry to detect anomalies across cloud and OT

03 **Govern third-party and supply access**
Enforce vendor authentication, monitor access pathways and assess supplier cyber maturity

Outlook and looking ahead

Cybersecurity is entering a new phase. The evidence in this report shows that attacks are becoming more sophisticated, more targeted and more closely linked to operational resilience. Looking ahead, five trends are expected to shape the threat landscape over the coming years:

01 **Cyber operations become a routine geopolitical tool**
Nation-state activity will increasingly expose organisations to wider geopolitical tensions.

02 **Physical operations become a primary target**
Connected and autonomous systems will increase the operational and safety consequences of cyber attacks.

03 **AI evolves from accelerating attacks to orchestrating them**
AI will enable attackers to automate, coordinate and adapt campaigns at greater speed.

04 **Digital supply chains become critical infrastructure**
Software, suppliers and third parties will remain attractive routes for compromising multiple organisations.

05 **Identity becomes the new security perimeter**
Cloud and remote operations will make identity and privileged access increasingly critical.

Turn intelligence into action

Use the insights in this report as the starting point for a conversation. Our cybersecurity specialists can help you assess your current posture, identify your highest risks and build a roadmap to strengthen resilience across your operations.

Contact us
Email: contactus@telemargroup.com
Web: https://telemargroup.com

Methodology

Find the full report here

We aggregate and anonymise data from Marlink's Security Operation Center.
We do not disclose customer or vendor information without explicit permission.

Data sources:

- SOC monitoring globally distributed assets across maritime, enterprise, and critical infrastructure
- 200+ cybersecurity assessments, including 160 technical security tests and red-team engagements
- Controlled phishing simulations, multiple campaigns across sectors
- Threat intelligence analysis, APT tracking, ransomware leak-site monitoring, EASM

IMPORTANT NOTE: Findings reflect indicative patterns from observed environments — not exhaustive measurements of global cyber activity. Monitoring depth varies by asset accessibility and deployment scope.