C-FALCON

Maritime Cyber Resilience

POWERED BY GRAMAX

Protect your maritime assets from cyber-attacks, comply with global maritime cybersecurity regulations & guidelines, and secure vessel IT/OT systems with C-Falcon – your trusted maritime cybersecurity platform.

C-FALCON

Maritime Cyber Resilience

C-Falcon is a purpose-built cybersecurity solution for the maritime sector, designed to meet its distinct operational and regulatory demands. It defends a vessel's critical systems and networks, delivers real-time monitoring across IT, OT, and IoT environments, and enforces cybersecurity compliance to ensure mission continuity at sea.

C-Falcon is powered by GRAMAX and is built on the same DNA that has safeguarded aviation for decades - an industry where precision, resilience, and zero downtime are non-negotiable. That experience now extends to maritime, where the stakes are just as high.

BLIND SPOTS

IN MARITIME CYBER RESILIENCE

The maritime sector faces a growing array of cyber threats. Vessels operate with limited connectivity, have hybrid IT-OT environments, and often use outdated systems that are not patched regularly.

01 **Fragmented Command**
Gaps in Cyber Governance and Asset Control

02 **Unprepared for the Unknown**
Gaps in Cyber Hygiene and Zero-Day Defense

03 **The Invisible Threat**
Gaps in Continuous Monitoring and Intelligence

04 **The Response Gap**
Weakness in Cyber Crisis Handling

NOTABLE ATTACKS SEEN

NotPetya (2017)

Ransomware crippled maritime logistics, leading to $300M+ loss, 76 ports disrupted, 45,000 devices affected in leading marine company.

Death Kitty (2021)

Ransomware encrypted port systems halting Durban, Cape Town ports with 30,000+ containers backlogged.

Container Vessel (2022)

Navigation system (ECDIS) compromised using a known exploit from cybercrime forums, impacting Bridge systems.

Manager (2023)

SaaS ransomware exposed vendor risks and lack of fallback mechanisms leading to fleet-wide disruption at large marine company.

C-FALCON

COMPLETE CONTROL OVER MARITIME CYBER RISKS

C-Falcon delivers true cyber resilience by protecting people, processes, and technology as one. It closes the gaps left by single-point tools through layered defense, continuous monitoring, and command-level control. Built on the NIST framework and expanded for the maritime domain, it's a comprehensive solution tailored to the sector's unique risks and operating realities.

01

Identify & Govern

- C-Falcon identifies and maps critical OT, IT, and IoT assets, giving vessels full visibility of what must be protected and exposing security gaps that demand immediate action.

02

Protect

- C-Falcon secures people, processes, and technology—hardening critical systems, enforcing access controls, and safeguarding maritime operations against evolving threats.

03

Detect

- C-Falcon delivers proactive detection and real-time alerting of cyber threats to vessels, powered by contextualized maritime threat intelligence to spot risks before they escalate.

04

Respond & Recover

- C-Falcon delivers real-time threat alerting, in-depth analysis, and rapid mitigation support for the crew, while continuously learning from every incident to refine defenses, update training, and strengthen maritime cyber readiness

COMPLIANCE WITH GLOBAL MARITIME CYBERSECURITY STANDARDS

Adhering to leading regulations and guidelines that shape maritime cyber resilience:

✅ IMO 2021
✅ BIMCO Cyber Security Guidelines
✅ IACS UR E26/E27
✅ ISO 27001 & IEC 62443

C-FALCON ADVANTAGE

COMPREHENSIVE FEATURES FOR END-TO-END PROTECTION

IDENTIFY & GOVERN

1. Asset Discovery & Management (IT, OT, IoT)
2. Vessel cybersecurity posture & compliance visibility (with Dashboard)

PROTECT

3. Periodic Cyber Hygiene Risk Assessment
4. Phishing simulation
5. Advance End point security with Neural Intelligence AI/ML Defense and Zero-day protection
6. Automatic Backup
7. Patch Management
8. Data Loss prevention with Device Control, Privacy Control and Print activity monitoring
9. Email Anti-Spam Protection
10. Advanced Web Protection
11. Host Firewall
12. Application Control
13. Advanced Ransomware Protection
14. AI powered Network Intrusion Detection System (IT, OT, IoT)*
15. Vulnerability Assessment
16. Crew Training & Awareness

DETECT

17. 24x7 managed Security Operations Monitoring and Alerting
18. Maritime Honeypot and Threat Intelligence

RESPOND & RECOVER

19. Incident Response & Management
20. Cyber Crises Management Support

* Requires additional hardware: Computer and managed switch.

Vessel version + Enterprise Version

C-FALCON

CENTRALISED 24X7 THREAT MONITORING

Uses deep intelligence (AI/ML) and modern technology for forensic investigation, threat hunting and threat simulation

24 x 7 Cyber Threat Detection & Incident Management capabilities, with highly skilled personnel capable to handle and implement Cyber Crises plan effectively.

Advanced Cyber threat detection powered by Next-Gen SIEM solution, enabled with Automated Response, Behaviour Analytics and Anomaly Detection

Provides bird’s eye view and support in maintaining internal security posture with the company policies and regulatory requirements

Powered by Cyber Range platform to continuous train Cybersecurity team on new scenarios and simulate threat in the environment.

Enterprise Security capabilities include Vulnerability Assessment, & Penetration Testing, Red Teaming, Attack Surface Monitoring, Cloud & Infrastructure Security, Crises Simulation

Continuous alignment of company’s Cybersecurity Strategy with on-ground ICDC intelligence

Integrated with the Marine Honeypot to deliver centralised threat intelligence and stronger maritime cyber defence.

Equipped with infrastructure and functional support to effectively manage Cyber Crisis.

C FALCON BENEFITS

C-FALCON
Maritime Cyber Resilience

01 ONE DASHBOARD FOR VISIBILITY, GOVERNANCE, & COMPLIANCE

Simplify visibility & control

02 FASTER IDENTIFICATION MITIGATION OF ANOMALIES

Improved response times to potential cyber incidents.

03 COMPLIANCE READINESS ACHIEVED WITHIN FIRST YEAR

High level of adherence to cybersecurity regulations and standards

04 REDUCTION IN REPEAT INCIDENTS

Through training-loop interventions

GRAMAX

WWW.GRAMAX.AI

Scan to Connect on LinkedIn

Project Office, New Udaan Bhawan, Opposite T3 Terminal,
IGI Airport, New Delhi, 110037