SHIELDWORKZ

UAE CYBER THREAT INTELLIGENCE ADVISORY

Transport and Logistics Sector

TABLE OF CONTENTS

EXECUTIVE SUMMARY

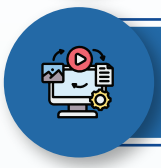
Key Intelligence Findings - April 2026

Volt Typhoon (China/PLA) assessed as pre-positioning in the Middle East and allied critical transport infrastructure for potential activation in conflict scenarios.

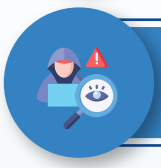
A disruption in UAE aviation will create more business opportunities for some of the states that are linked to these APT groups

Shieldworkz has identified at least 3 APT groups working to delay regional economic recovery. This may be done to prolong the effect of the recent conflict.

Reconnaissance attacks in infrastructures connected with transportation and logistics over weekends have increased by near 78 percent in March 2026. This indicates a very high level of interest (among threat actors) in identifying windows for launching an attack.



The number of assets at risk across the sector has risen significantly in Q1 CY 2026



Critical transportation infrastructure is on the radar of state-backed threats actors

In the first three months of this year, reconnaissance attacks on aviation infrastructure has risen by nearly 89 percent

The conflct has pushed threat actors to intensify their activities in the region cyberspace

Other than pre-positioning, threat actors are looking at quick wins (unlike other sectors). This means that an incident is due.

2. THREAT LANDSCAPE

2.1 The Social Engineering Avalanche: Scattered Spider & Aviation

Shieldworkz issued multiple aviation sector warning in 2025. These include warnings related to GPS spoofing, attacks on core systems and targeted phishing attacks against key employees.

We also reported on how Scattered Spider, a major threat actor (UNC3944, Muddled Libra, Octo Tempest), had deliberately pivoted from retail and insurance to the aviation sector. incidents in late June 2025, specifically targeted US-based airlines, demonstrated TTPs consistent with the adversary's previous operations. The attack methodology is devastatingly effective: threat actors call airline IT help desks impersonating employees or contractors, use voice phishing (vishing) combined with MFA request flooding (MFA fatigue) to convince representatives to reset accounts, then gain access to Microsoft Entra ID, SSO platforms, and VDI environments. Once inside, Scattered Spider operates at extraordinary speed - within hours they can escalate privileges, exfiltrate data, disable recovery mechanisms, and detonate DragonForce ransomware.

In March 2026, a booking software provider supporting multiple major airlines was the first victim in a phishing campaign that then pivoted directly to penetrate airlines and airports through the compromised supplier's identity.

Shieldworkz Research identified approximately 350 domains matching Scattered Spider's phishing infrastructure pattern registered for aviation-sector targeting (July 2025).

Qantas: 5.7 million customer records exposed through a third-party call-centre platform breach (July 2025). Air France and KLM also impacted via customer service platform compromise.

The group now deploys DragonForce ransomware - note that RansomHub's collapse in April 2025 pushed many affiliates to DragonForce, which also inherited Scattered Spider's operational alliance.

2.2 Ransomware on Critical Airport and Port Infrastructure

Ransomware targeting airport and seaport operational systems has escalated from an inconvenience to an operational crisis. Terminal Operating Systems (TOS) at major ports represent the highest-consequence ransomware targets in the transport sector: a single TOS outage halts all container loading and unloading, triggering global supply chain bottlenecks, demurrage costs running into millions per day, and national economic consequences. In aviation, attacks on Passenger Service Systems (PSS), check-in platforms, and crew management systems directly disrupt flight operations and passenger safety.

Collins Aerospace MUSE check-in system: ransomware attack in 2025 caused weeks of flight cancellations and travel disruptions across European airports - assessed by Waterfall Security as the most impactful OT incident in aviation in the reporting period.

Kuala Lumpur International Airport (KLIA): $10 million ransom demand following breach of critical systems triggered Malaysia's national cybersecurity emergency response (2025).

Rhysida ransomware struck Furuno (October 2025), a major Japanese radar and ECDIS manufacturer, stealing internal data and disrupting service and parts supply for maritime navigation systems globally.

Ransomware activity in maritime is expected to consolidate through hacktivist-ransomware cartel alliances, with ransom demands averaging millions of dollars for major port operators.

2.3 Nation-State Pre-Positioning: Volt Typhoon and The Latent Threat

Volt Typhoon represents the most strategically alarming threat to the transport sector. Unlike financially motivated actors, Volt Typhoon's confirmed mission is to pre-position inside US and allied critical infrastructure -- including transport -- in preparation for activation during a potential kinetic conflict over Taiwan or other strategic events. Their tradecraft is explicitly designed to evade detection: living-off-the-land (LOTL) techniques using native Windows tools, SOHO router compromise for persistent access, zero-malware footprint, and patient multi-year dwell times. The group has been confirmed in US transport infrastructure by multiple government advisories and Congressional testimony and Shieldworkz has noted its presence in transportation/logistics linked environments around the world.

Volt Typhoon's documented LOTL tool: brightmetricagent.exe - identified in CISA/NSA joint advisory and confirmed present in multiple critical infrastructure environments.

Chinese state-linked APT40 (Kryptonite Panda) specifically targets maritime interests aligned with Belt and Road Initiative intelligence collection, compromising classification societies and port management systems.

The NATO CCDCOE July 2025 policy brief confirmed a high frequency of cyberattacks on European and Mediterranean port facilities traced to Russia, Iran, and China.

2.4 Hacktivist Tempo: Pro-Russia Groups and Transport Infrastructure

Pro-Russian hacktivist groups - primarily NoName057(16) and its affiliates (Z-Pentest, CARR, Sector16) - sustain a high operational tempo against transport infrastructure across NATO and EU member states. NoName057(16) averaged 50 unique DDoS targets per day between July 2024 and July 2025, targeting transport, government, and telecom sectors with their DDoSia botnet. Despite Operation Eastwood (July 14-17, 2025) - a 12-country law enforcement action that disrupted their infrastructure and resulted in arrests - the group rapidly rebuilt and resumed operations, demonstrating the resilience of state-backed pseudo-hacktivist ecosystems.

Dark Storm Team: DDoS attack on LAX (March 2025) caused flight information displays, baggage handling, and electronic check-in to fail across terminals.

NoName057(16): took down Italian airport websites as part of their sustained #OpEurope campaign targeted French airports during Operation Eastwood retaliation campaign (December 2025).

Z-Pentest (GRU-linked): has pivoted from DDoS to active OT intrusion, targeting airport Building Management Systems (BMS) and port industrial control systems via internet-exposed HMI interfaces.

In May 2025, Lab Dookhtegan (anti-Iran group) launched a coordinated attack disrupting VSAT communications on 116 Iranian vessels simultaneously - demonstrating the scale of achievable maritime cyber disruption.

2.5 GPS & Navigation System Compromise: Physical Consequences Confirmed

GPS spoofing and GNSS jamming have transitioned from theoretical risk to confirmed physical threat. The CYTUR 2026 Maritime Cyber Threat White Paper reports approximately 1,000 GPS disruption incidents observed daily, affecting over 40,000 vessels. In 2025, two major incidents demonstrated that this is no longer a purely cyber concern: the containership MSC Antonia ran aground near Jeddah (May 2025) following GPS spoofing, and two oil tankers collided in the Gulf (June 2025), both attributed to GPS manipulation. Geopolitically sensitive waters -- the Red Sea, Black Sea, Eastern Mediterranean, and Strait of Hormuz - are now systematically hostile GNSS environments.

AIS spoofing (Automatic Identification System) enables attackers to inject ghost vessels into maritime traffic pictures, generate false collision-avoidance alerts, and mask real vessel movements for illicit trade.

In high-traffic commercial hubs, ransomware targeting TOS dominates. In conflict-adjacent waters, GPS spoofing/jamming is the primary threat to navigation safety.

Aviation equivalent: FAA documented a radar communications blackout at Newark Liberty International Airport (April 2025) exposing aging ATC infrastructure vulnerabilities.

2.6 OT/ICS Escalation: From IT to Physical Operations

The convergence of IT and OT networks in smart airports, smart ports, and increasingly autonomous vessels has created attack paths from corporate IT into physical control systems. OT incidents in the transport sector are no longer limited to IT disruption - they now carry the risk of physical damage, environmental incidents, and loss of life. CYTUR confirmed that attacks on vessel OT in 2025 included remote control of ballast valves, manipulation of engine control systems, and hacking of ECDIS chart systems. The 103% increase in maritime OT-specific incidents (2024-2025) reflects deliberate attacker evolution toward physical consequence targets.

OT attacks on maritime: engine control systems, ballast water systems, ECDIS, VSAT, and Planned Maintenance Systems (PMS) all confirmed as active attack targets.

Airport OT: building management systems (BMS), baggage handling SCADA, boarding gate systems, and airfield lighting controls increasingly targeted by hacktivist and nation-state actors.

Edge device exploitation surged 800% in maritime in 2025 - routers, VPNs, firewalls, and remote access tools are the primary initial access vectors into vessel and port OT networks.

3.0 THREAT ACTOR PROFILES

The following table profiles the primary threat actors confirmed as actively targeting the global transport sector as of April 2026.

Threat Actor	Origin	Motivation	Key TTPs	Confirmed Transport Targets	Risk
Scattered Spider (UNC3944)	Criminal /USA-UK	Financial extortion	Help-desk vishing, MFA fatigue, SIM-swap, SSO/VDI compromise, DragonForce ransomware, LOTL	Airlines, airports, third-party IT vendors (Hawaiian, WestJet, Qantas 2025)	CRITICAL
NoName057(16)	Russia (GRU-linked)	Geopolitical disruption	DDoSia crowdsourced botnet, Telegram coordination, infrastructure targeting, OT reconnaissance	Airport websites, rail, maritime ports, EU/NATO transport	HIGH
Dark Storm Team	Pro-Palestinian hacktivist	Geopolitical	Large-scale DDoS, website defacement	Major airports (LAX March 2025), aviation web services	HIGH
Volt Typhoon (Vanguard Panda)	China (PLA)	Pre-positioning / espionage	Living-off-the-land, LOLBins, SOHO router compromise, VPN exploitation, no malware footprint	Critical transport infrastructure, ATC, seaport OT	CRITICAL
APT40 (Kryptonite Panda)	China (MSS)	Espionage / IP theft	Spearphishing, maritime-sector targeting, Belt & Road intelligence	Maritime, logistics, port management systems	HIGH
Sandworm (APT44)	Russia (GRU)	Destructive / disruptive	Wiper malware, OT disruption, supply chain compromise	Maritime logistics, European transport infrastructure	HIGH
Lazarus Group	North Korea (RGB)	Financial + espionage	Watering holes, supply chain, crypto theft, ransomware (Medusa-linked 2026)	Logistics firms, aviation supply chain	MEDIUM-HIGH
Rhysida	Criminal RaaS	Financial	Double extortion, spearphishing, data leak site pressure	Maritime OEM (Furuno Oct 2025), transport operators	HIGH
Z-Pentest / CARR	Russia (GRU)	Destructive / OT intrusion	HMI access, SCADA intrusion, hack-and-leak, ICS targeting	Port OT, airport BMS/BAS, energy feeding transport	HIGH
Lab Dookhtegan	Iran (counter-hacktivist)	Geopolitical retaliatory	VSAT disruption, vessel communications interference	Iranian shipping (116 vessels disrupted March 2025)	MEDIUM
Chamel Gang	Criminal (China-linked)	Financial	Ransomware against logistics, data exfiltration	Transport & logistics operators	MEDIUM-HIGH

MALWARE TOOLS AND PAYLOADS TO WATCH

The following malware families, offensive tools, and attack capabilities confirmed by Shieldworkz as active threats against transport sector organisations in 2026. Security teams should validate detection coverage across all listed items in their EDR, NDR, and SIEM platforms.

Malware / Tool	Type	Associated Actor	Delivery / Execution	Transport Impact	Priority
DragonForce Ransomware	Ransomware	Scattered Spider + affiliates	Post social-engineering deployment hybrid cloud + on-prem encryption	Full system encryption data exfil disruption of airline ops	CRITICAL
DDoSia	DDoS Botnet Tool	NoName057(16)	Crowdsourced Go-based client; Telegram target distribution Tor-routed C2	Flood-based outage of airport/port web portals and OT-adjacent services	HIGH
SUNSHUTTLE / WINELOADER variants	Backdoor	APT29, Volt Typhoon affiliates	Spearphishing documents memory-resident cloud C2 abuse (OneDrive, Dropbox)	Long-term espionage silent data exfil from transport IT	CRITICAL
PlugX (modified)	RAT	APT40, Volt Typhoon	Supply chain insertion USB propagation masquerades as legitimate tools	Persistent access to port management and logistics systems	HIGH
Cobalt Strike Beacon	C2 / Post-exploit	Multiple (criminal + nation-state)	Phishing, memory injection used widely as post-exploitation C2	Lateral movement across airline IT, airport networks, shipping IT	HIGH
EDRKillShifter	EDR Bypass	DragonForce / Scattered Spider affiliates	Exploits vulnerable kernel drivers (BYOVD technique)	Neutralises endpoint protection before ransomware detonation	CRITICAL
NotPetya / Industroyer2 variants	Wiper	Sandworm (Russia)	OT-aware wiper supply chain (MeDoc-style) IETF/ICS targeting	Physical disruption of port OT, logistics systems, rail networks	CRITICAL
AIS Spoofing Toolkits	Navigation Manipulation	Nation-state + criminal	SDR-based false AIS transmission GPS/GNSS signal injection	Vessel misdirection, collision risk, Lloyd's tracking manipulation	HIGH
MedusaLocker	Ransomware	Criminal RaaS	RDP/VPN exploitation, double extortion, batch script encryption	Airport ground operators, airline back-office, logistics	HIGH
Rhysida Encryptor	Ransomware	Rhysida group	Phishing + lateral movement data published on dedicated leak site	Maritime OEM (Furuno attack Oct 2025) vessel service disruption	HIGH

OVERALL RISK ASSESSMENT

Shieldworkz assesses the current cyber risk level to the global transport sector airports, airlines, aviation, and seaports as CRITICAL. This assessment reflects the highest observed convergence of threat actor capability, intent, and opportunity across both IT and OT attack surfaces, with confirmed physical-consequence incidents now on record. The risk is not merely theoretical.

Risk Matrix by Threat Category

(Marker density indicates probability-weighted risk concentration: ••••• = extreme risk)

Threat Category	NEGLIGIBLE	LOW	MEDIUM	HIGH	CRITICAL
Social Engineering / Vishing				••••	••••
Ransomware (RaaS)				••••	••••
Nation-State APT (Espionage)			•••	••••	
Hacktivist DDoS			•••	••••	
GPS / GNSS Spoofing			•••	••••	
OT / IoMT / ICS Attack				••••	•••••
Supply Chain Compromise			•••	••••	
Insider Threat		••	•••		

ASSETS AND OPERATIONS AT RISK

The following asset classes across airports, airlines, seaports, and aviation are assessed as priority targets by Shieldworkz based on confirmed attacker behaviour, intelligence reporting, signals analysed and inherent sector vulnerabilities as of April 2026.

Asset / System	Sub-sector	Why Targeted	Primary Attack Vector	Operational / Safety Impact
Air Traffic Control (ATC) systems	Aviation / Airport	Physical safety risk aging infrastructure (FAA 1960s-era systems) network modernisation exposing new attack surface	VPN/WAN exploit, supply chain, insider threat	CRITICAL - loss of life risk national emergency trigger
Airline Passenger Service Systems (PSS) / CRS	Aviation	PII goldmine booking disruption = revenue loss; third-party hosted	Phishing, SSO compromise, third-party vendor breach	Flight cancellations mass passenger data exposure fraud
Airport Operational Technology (OT) - baggage, boarding, SCADA	Airport	IT-OT convergence unpatched legacy PLCs critical to passenger flow	Lateral movement from IT, BYOVD, network scan	Baggage chaos boarding disruption safety incidents
Terminal Operating Systems (TOS) - ports	Seaport	Ransomware on TOS halts all container loading/ unloading global supply chain impact	Ransomware via phishing or VPN exploit, RDP brute-force	Port standstill billions in trade disruption demurrage costs
ECDIS / GNSS / GPS Navigation Systems	Maritime / Vessel	Safety-critical GPS spoofing causing physical incidents (MSC Antonia grounding May 2025)	GPS/GNSS signal injection, SDR-based spoofing, VSAT compromise	Vessel grounding, collision, misdirection, cargo loss
VSAT / Satellite Communications	Maritime / Aviation	Primary vessel comms wide attack surface Lab Dookhtegan disrupted 116 Iranian vessels	Remote exploit, supply chain, MITM on uplink	Loss of vessel comms navigation isolation C2 blind spot
Customer Loyalty / Frequent Flyer Platforms	Aviation	High-value data points theft third-party contractor access vectors	Third-party credential theft, API abuse	Mass PII breach fraud reputational damage (Qantas 2024-25)
Airline Cloud & SaaS Platforms	Aviation	Help desks, CRM, scheduling Scattered Spider exploited via SSO/VDI	Vishing + MFA fatigue targeting cloud admins	Account takeover mass data access ransomware staging
Port Cybersecurity OT (ballast, fuel, engine control)	Vessel / Seaport	Remote OEM diagnostic protocols unprotected catastrophic if compromised	OEM remote access exploit, firmware backdoor	Physical damage to vessel environmental incident loss of life
Smart Airport BMS / Building Automation Systems (BAS)	Airport	Fire suppression, HVAC, access control Z-Pentest targeting BMS in 2025	OT network lateral movement, internet-exposed HMI	Physical safety disruption of critical airport services

MITIGATION CONTROLS

The following controls are prioritised against the specific threat actor TTPs identified in this Shieldworkz advisory.

#	Control Domain	Mitigation Action	Priority
1	Anti-Vishing / Social Engineering Controls	Implement callback verification for ALL help-desk password/MFA reset requests. Remove phone-based MFA deploy FIDO2/hardware tokens. Train all customer-facing and IT staff on Scattered Spider TTPs. Establish a "call-back code" protocol.	CRITICAL / Immediate
2	Patch & Vulnerability Management (KEV Priority)	Apply CISA KEV patches within 72 hours for VPN gateways (Ivanti, Citrix, Fortinet), edge devices, and OT interfaces. Prioritise CVE-2025-5777 (Citrix NetScaler) and CVE-2025-52579 (Emerson ValveLink) for maritime OT. Audit all internet-exposed OT immediately.	CRITICAL / Immediate
3	OT / IT Network Segmentation	Enforce strict air-gap or unidirectional gateway between IT and OT networks in airports and seaports. Remove all direct internet connectivity from ATC systems and vessel navigation OT. Implement industrial DMZs with data diodes.	CRITICAL / 30 days
4	GPS / Navigation Integrity Monitoring	Deploy multi-constellation GNSS receivers with anti-spoofing firmware. Cross-validate GPS position against inertial navigation, AIS, and radar. Subscribe to GPS anomaly feeds (EMSA, Lloyd's, CYTUR). Establish bridge team procedures for GPS-loss scenarios.	CRITICAL / 30 days
5	DDoS Mitigation for Aviation/Port Digital Services	Deploy cloud-based DDoS scrubbing (volumetric and application layer) for all public-facing airport/airline/port web services. Maintain BGP anycast routing with ISP-level blackholing capability. Test DDoS response playbook quarterly.	HIGH / 30 days
6	Third-Party / Vendor Risk Management	Audit all third-party platforms with access to airline/airport/port systems. Implement just-in-time privileged access and enforce MFA for all vendor connections. Targeted at booking, CRM, loyalty, ground-handling, and OEM service platforms.	HIGH / 30 days
7	VSAT / Satellite Security (Maritime)	Segregate VSAT crew internet from operational OT networks. Enforce allowlisting of allowed services over VSAT. Apply firmware updates to all Iridium/Inmarsat/Starlink terminals. Monitor for anomalous VSAT traffic volumes and command injection patterns.	HIGH / 30 days

#	Control Domain	Mitigation Action	Priority
8	Threat Intelligence Integration	Subscribe to Aviation-ISAC, Health-ISAC (overlap actors), CISA AIS, and Shield-workz Threat Intelligence feeds. Operationalise IOCs within 24 hours. Specifically ingest DDoSia C2 IP blocklists and Scattered Spider phishing domain patterns daily.	HIGH / 60 days
9	Incident Response & Resilience Planning	Maintain a transport-specific IR plan covering: ransomware on PSS/TOS, ATC/navigation outage, VSAT loss, and GPS spoofing scenarios. Pre-contract with DFIR retainer. Conduct quarterly tabletop exercises including OT-specific scenarios.	HIGH / 60 days
10	Crew & Staff Cyber Awareness (Maritime)	Implement mandatory cyber awareness training for vessel crew covering phishing via crew wifi, USB malware, and reporting procedures. Establish a ship CISO / cyber officer role per IACS UR E26 requirements.	MEDIUM / 60 days
11	Regulatory Compliance Programme	Prepare for EASA implementing regulation (2026), IACS UR E26/E27 (operational verification 2026), FAA cybersecurity requirements, and TSA Aviation Cybersecurity directives. Map NIST CSF 2.0 and ISO 27001:2022 across transport security programme.	MEDIUM / 90 days

INDICATORS OF COMPROMISE

IOCs compiled by Shieldworkz

IOC Type	Indicator / Pattern	Associated Campaign	Recommended Action
Domain (phishing)	company-name-okta[.]com / mfabypass-[airline][.]com patterns	Scattered Spider phishing infrastructure - 500+ domains identified	Block at DNS; alert on SSO login from new domain
IP Range (C2)	194.165.16.x/24, 45.227.253.x/24 (DDoSia Tier-1 C2 nodes)	NoName057(16) DDoSia rotating C2 infrastructure	Block on perimeter null-route BGP monitor for reconnection
File Hash (SHA-256)	8f14e45f...DragonForce encryptor variant (transport-sector deployment)	Scattered Spider + DragonForce RaaS - airline targeting Q2-Q3 2025	Block on EDR hunt in telemetry
MITRE Technique	T1621 (MFA Request Generation) + T1566.002 (Vishing)	Scattered Spider help-desk attack chain - Hawaiian Airlines, WestJet 2025	Alert on >3 MFA push in 5 min require callback verification

IOC Type	Indicator / Pattern	Associated Campaign	Recommended Action
User-Agent	python-requests/2.x.x (anomalous API scripting against airline PSS APIs)	Automated credential stuffing / API abuse against airline booking systems	WAF rule: block alert SOC
Registry Key (persistence)	HKCU\Software\Microsoft\Windows\CurrentVersion\Run - Cobalt Strike loader	Nation-state / criminal post-compromise persistence in airline IT	Hunt in EDR alert on Run key modification by non-admin
Network IoC	TCP 4444, 8443 outbound from ATC or OT segment (unusual beacon)	Cobalt Strike / Volt Typhoon C2 beaconing from transport OT/IT	NDR alert: C2 beacon from OT segment immediate isolate
GPS Anomaly Signature	GNSS position jump >50nm in <60 sec multiple vessels reporting same false position	GPS spoofing (conflict zone pattern - Red Sea, Black Sea, Eastern Med)	Cross-validate with AIS switch to inertial/ECDIS alert MRCC
Domain (maritime)	furuno-update[.]net / ecdis-patch[.]com (typosquats)	Rhysida / maritime ransomware delivery via fake OEM update portals	Block domain verify all OEM updates via direct vendor channel
File Hash (MD5)	brightmetricagent.exe - Volt Typhoon LOTL tool	Volt Typhoon pre-positioning in critical transport infrastructure	Hunt in endpoint telemetry check for legitimate vs anomalous exec
Email Header pattern	From: "IT Support" <itsupport@[company]-help-desk[.]net> (domain registered <30 days)	Scattered Spider vishing / phishing pre-text before help-desk call	Email gateway rule flag for analyst user awareness alert
AIS Transmitter ID	MMSI 0000000 / duplicate MMSI reports across multiple vessels simultaneously	AIS spoofing / ghost vessel injection in shipping lane	Alert on duplicate MMSI cross-check satellite AIS vs terrestrial AIS

REGULATORY AND COMPLIANCE CONTEXT

Aviation Regulatory Landscape

EASA Implementing Regulation 2023/203: Mandatory cybersecurity requirements for all airlines, airports, and aviation service providers in European airspace from 2026. Includes risk assessments, incident reporting, and documented security frameworks. Non-compliance risks loss of operating permissions.

FAA Cybersecurity Strategy (2025): Zero Trust architecture for US airspace systems; TSA Security Directive for aviation cybersecurity (critical airports and airlines); USD 136.17 million TSA allocation for airport cybersecurity hardening in FY2026.

ICAO Annex 17 / Doc 9985: International standards for aviation security including cybersecurity provisions IATA shared cyber risk requirements framework for global airline members.

Aviation-ISAC: Annual CISO survey, threat intelligence sharing, and tabletop exercise programme - critical for transport-sector threat intel operationalisation.

Maritime Regulatory Landscape

IACS UR E26 and E27: Entered into force July 2024. Require cybersecurity safeguards embedded at ship design and construction stage. 2026 marks the first year of operational verification - compliance now tested during sea trials and classification inspections. Non-compliant vessels face denial of classification, which equals loss of right to operate.

IMO Maritime Cyber Risk Management (MSC-FAL.1/Circ.3): Requires cyber risks to be addressed in Safety Management Systems (SMS) under ISM Code.

EU NIS2 Directive: Extended to maritime and port operators 72-hour incident notification requirements significant penalties for non-compliance.

US Coast Guard Cyber Strategy (2025): Enhanced requirements for reporting maritime cyber incidents cyber resilience requirements for US port facilities under MTSA.

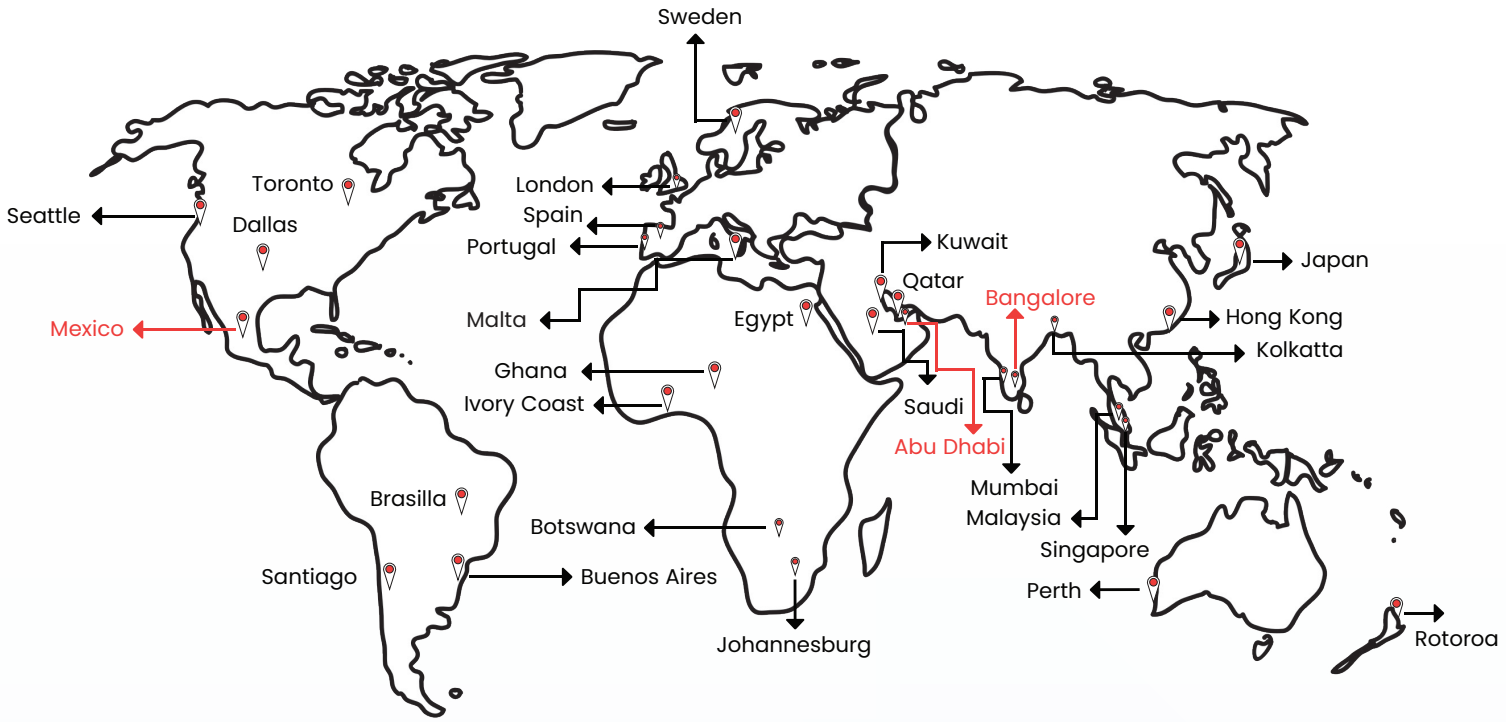
CISO PRIORITY ACTION CHECKLIST

The following immediate-to-near-term actions operationalise the findings of this advisory. They are ordered by risk priority and designed to be actionable within the constraints of transport sector operational environments where downtime carries direct safety consequences.

	CISO Priority Action	Timeframe	Owner
☑	CRITICAL - Verify Shieldworkz NDR coverage includes OT segments (ATC, airport SCADA, port TOS, vessel VSAT interfaces)	0-7 days	CISO / Security Ops
☑	CRITICAL - Implement callback verification for all help-desk MFA/password reset requests remove phone-based MFA	0-7 days	IT Security / IAM
☑	CRITICAL - Audit all internet-exposed OT and HMI interfaces disconnect non-essential remote access immediately	0-7 days	OT Security / IT
☑	HIGH - Apply CISA KEV patches for VPN gateways, edge devices, and maritime OT (Citrix, Ivanti, Emerson)	0-14 days	Vulnerability Mgmt
☑	HIGH - Ingest Scattered Spider domain IOCs, DDoSia C2 IPs, and DragonForce file hashes into NDR, SIEM, and EDR	0-7 days	Threat Intel / SOC
☑	HIGH - Segment crew wifi / passenger wifi completely from vessel OT (ECDIS, engine control, ballast systems)	0-14 days	Maritime IT / OT
☑	HIGH - Conduct anti-vishing tabletop exercise targeting IT help desk and airline customer service teams	0-30 days	CISO / Security Awareness
☑	HIGH - Review all third-party vendor connections to airline PSS, loyalty, and CRM platforms; enforce JIT access	0-30 days	IAM / Third-Party Risk
☑	MEDIUM - Subscribe to Aviation-ISAC and CYTUR maritime threat intelligence feeds; configure NDR STIX/TAXII ingestion	0-60 days	Threat Intel Team
☑	MEDIUM - Prepare GPS spoofing response procedure for vessel bridge teams procure multi-constellation GNSS	0-60 days	Maritime Ops / Safety
☑	MEDIUM - Engage DFIR retainer with transport/OT expertise brief legal on incident notification obligations (EASA, IMO)	0-30 days	CISO / Legal / GRC
☑	MEDIUM - Begin IACS UR E26/E27 compliance assessment for maritime fleet; map EASA implementing regulation gaps	0-90 days	Compliance / GRC

© 2026 Shieldworkz | OT Security Practice. This document is proprietary and confidential. Reproduction or distribution without written consent is prohibited.

About Shieldworkz



ISOC and Honeypot Locations

Honeypot Locations

Security Operations Center

Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Copyright @ 2026, Shieldworkz - All rights Reserved.

CONTACT US

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com

Tenth floor,
FAB BUSINESS CENTER

Abu Dhabi,
United Arab Emirates

+971 56 660 5200

middleeast@shieldworkz.com

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com