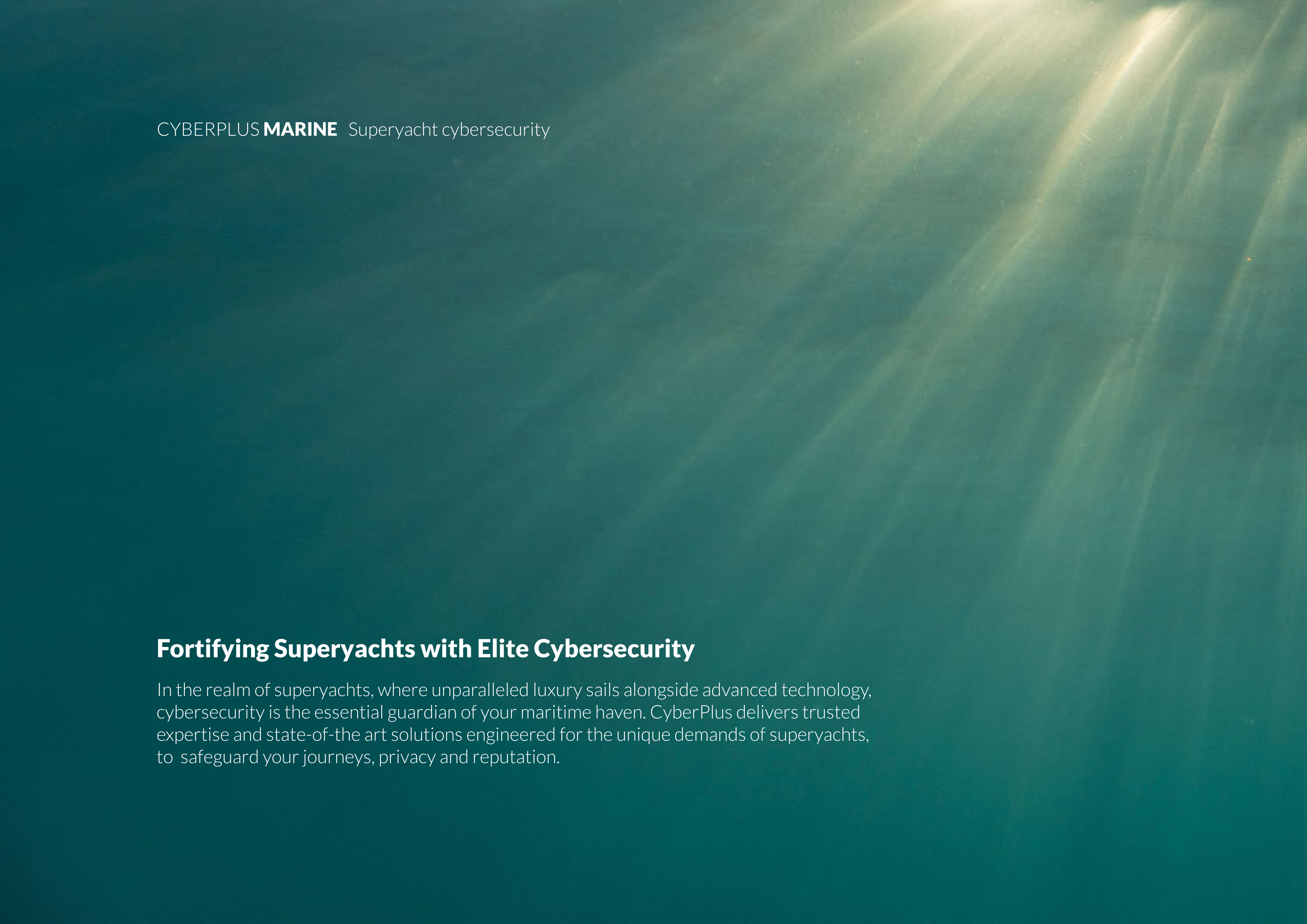
cyber MARINE

Safeguard Against Threats Unseen.

TRUSTED EXPERTS

For Elite Superyacht Cybersecurity.



Fortifying Superyachts with Elite Cybersecurity

In the realm of superyachts, where unparalleled luxury sails alongside advanced technology, cybersecurity is the essential guardian of your maritime haven. CyberPlus delivers trusted expertise and state-of-the art solutions engineered for the unique demands of superyachts, to safeguard your journeys, privacy and reputation.

cyber+MARINE

Privacy, Safety, and Reputation at Sea

For owners and their guests, privacy and safety are paramount. A yacht is not simply a vessel; it is a sanctuary where personal and professional lives intersect. That very exclusivity makes it a target, from intercepted communications to interference with onboard systems. Compliance with the IMO cyber mandate is only the starting point. Management must demonstrate beyond doubt that discretion, security and reputation are protected without compromise.

Assurance without Compromise

CyberPlus assesses onboard and shore side systems with precision to identify vulnerabilities that could expose owners, guests and crew. We then implement continuous resilience programs that combine technical safeguards, crew readiness and governance, thet go beyond IMO compliance and provide real, demontsrable operational security.

The PLUS

Owners gain confidence that their privacy and safety are protected, captains receive clear, practical procedures that preserve service and safety, and management teams receive audit ready evidence they can present to owners and insurers. With CyberPlus, cyber resilience is not just compliance; it is verifiable assurance for those who value discretion and security above all.

Fortifying Superyachts with Elite Cybersecurity

Superyachts represent the pinnacle of maritime engineering and luxury living, creating a landscape unlike any other. They blend high-tech operational systems with lavish guest experiences, all while navigating remote international waters. This exposes them to dynamic threats, including fluctuating connectivity, integration of diverse vendor technologies, and a constant influx of crew, guests, and service providers.

Isolation at sea amplifies vulnerabilities. Limited immediate access to expertise means a breach could strand you far from help, turning a minor glitch into a major crisis. Superyachts are high-value targets for cybercriminals, from state-sponsored actors to opportunistic hackers eyeing ransom demands.

The fusion of Operational Technology, Information Technology, and Internet of Things devices, coupled with transient personnel and high-net-worth individuals, creates interdependencies where privacy, safety and operational integrity hang in the balance. In this unique realm, cybersecurity must be agile, discreet and able to adapt to shifting seas while preserving the owners' freedom and confidence on board.

Why You Need Trusted Cyber Experts

If your cybersecurity is a black box, then you're being left in the dark, vulnerable to unseen threats that could compromise your vessel, privacy and peace of mind. CyberPlus was founded by cybersecurity veterans who have secured global enterprises, critical industry and maritime fleets, as well as the digital lives of high net worth individuals.

We've pioneered standards, authoring the IASME Maritime Cyber Baseline (MCB) and elevated cybersecurity practices in the sector. With CyberPlus you get proven experts who understand the nuances of superyacht security, delivering transparent, tailored strategies that illuminate risks and empower you to sail confidently into the future.

Where Risks Meets Reality

In the superyacht ecosystem, every system and individual is a potential entry point for cyber threats.
Protecting these assets isn't optional, it's essential to maintaining safety, privacy, and operational excellence.
Here are the key areas we secure:

Operational Technology (OT)

OT forms the backbone of your yacht's functionality, controlling critical systems that keep you afloat and on course and includes:

- Navigation and autopilot systems
  vulnerable to GPS spoofing or remote hijacking
- Engine management and propulsion controls
  tampering could lead to mechanical failures or stranded voyages
- Ballast and stability systems
  risking physical safety if compromised
- Environmental controls
  HVAC and water treatment could be exploited for sabotage

Information Technology (IT)

IT handles the data flow that powers communication and operations, making it a prime target for data breaches or espionage and includes:

- Onboard servers and networks
  stores sensitive voyage data and financial records
- Communication systems
  satellite internet and email servers, prone to interception
- Crew management software
  scheduling and payroll, which could expose personal information
- Guest entertainment systems
  streaming services and databases, ripe for unauthorized access

Internet of Things (IoT)

IoT devices add luxury and convenience but introduce numerous weak links through their connectivity:

- **Smart appliances in galleys and cabins** can be a foothold for lateral movement into critical systems
- **Security cameras and surveillance networks** compromise can expose privacy and enables spying
- **Wearable tech and fitness trackers** used by crew or guests, potentially leaking location data
- **Automated docking and mooring sensors** vulnerable to manipulation during critical maneuvers

OT NETWORK SECURITY EXPERTS

CyberPlus founders recognised by Fortinet as experts in OT security.

People

People are the most overlooked vulnerabilities and require targeted training and safeguards.

- **Crew** As the operational heart of the yacht, crew members face risks from phishing emails, unsecured personal devices, or social engineering tactics that could grant attackers insider access. Transient crews amplify this, with varying levels of cyber hygiene potentially ntroducing malware via USBs or shared networks

- **Owners and Guests** HNWIs and their entourages are high-profile targets for ransomware, identity theft, or extortion. Personal devices, VIP Wi-Fi zones, and shared media systems could expose confidential business data, family privacy, or even real-time locations, turning a leisurely cruise into a security nightmare

Cyber Resilience Framework

Our comprehensive approach to superyacht cybersecurity is built on a proven four-pillar framework: Assess, Protect, Monitor, and Respond. Our fusion of advanced technologies and maritime expertise creates defences that are seamless, reliable, and discreet, protecting your yacht without compromising its luxury experience.

ASSESS

We begin with a thorough vulnerability audit, testing from both internal and external perspectives to identify risks across OT, IT, IoT, and human factors. Aligned with all leading maritime and cybersecurity standards, from IMO to ISO 27001 and with class society notations, this audit delivers a clear, certifiable roadmap to resilience.

PROTECT

Our expertise extends across any security vendor and device, enabling seamless integration and support of your existing security stack, while leveraging additional advanced technologies such as AI-driven threat detection, machine learning for anomaly identification, and blockchain secured data vaults to fortify your systems, addressing any gaps found.

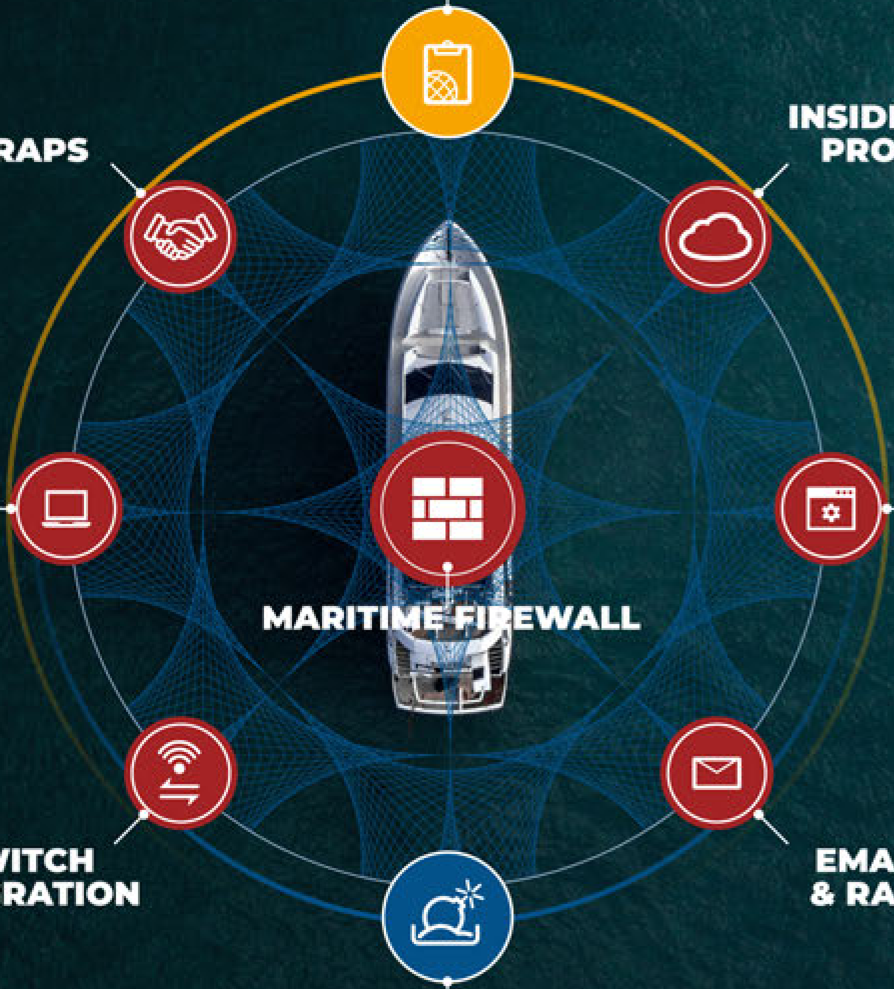
MONITOR

Continuous, real-time oversight is powered by AI-driven analytics and cloud-based dashboards. We enable physical and cyber security teams, onboard and remote, to act as one through shared intelligence. Live threat data, geo-tracking of devices and assets, and geofenced alerts provide actionable insights, ensuring both cyber and physical security coordinates seamlessly to neutralise risks before they escalate.

RESPOND

Global rapid-response teams are available on call 24/7 to investigate incidents, establish facts and take decisive action. Once stability is secured we preserve evidence, run discreet forensics and manage precision recovery. Trained crew act as the onboard first line, working seamlessly with remote specialists to resolve threats swiftly, protect reputation and restore operations with minimal disruption.

cyber MARINE



LOCATION BASED CYBER ANALYTICS

DECOY & DECEPTION TRAPS

INSIDER THREAT PROTECTION

OT SEGREGATION & PROTECTION

MARITIME FIREWALL

IT & AV TECHNICAL CONTROLS

WIFI, SWITCH & PC INTEGRATION

EMAIL PHISHING & RANSOMWARE

OWNER & CREW THREAT PROTECTION

Your Path to Cyber Assurance

Securing a superyacht demands precision and discretion. Our curated service pathways are designed to deliver immediate assurance, tailored to the expectations of owners and the operational realities of management teams.

1. Discovery Consultation

Embark on your yacht's security journey with a private, no-obligation consultation with CyberPlus's elite cybersecurity experts.

Conducted remotely for your convenience and discretion, this personalised session dives deep into your unique priorities, identifies critical risk areas specific to your vessel, and delivers a tailored roadmap for robust protection. Aligned with maritime cybersecurity standards, the outcome is a concise, actionable set of next steps, empowering you to safeguard your yacht with confidence and sophistication.

2. Core Assurance

Secure your yacht with a foundational cybersecurity suite designed for operational excellence and peace of mind.

Tailored for new builds or yachts establishing a security baseline, Core Assurance combines robust protection for operational, information, and connected systems with AI-driven monitoring and customized crew awareness training. Aligned with IMO cyber risk guidelines and the Mritime Cyber Baseline, Core Assurance packages deliver resilient, easy-to-implement solutions, ensuring your voyages remain secure and seamless.

cyber+MARINE

3. Bespoke Managed Security

Bespoke Managed Security is a private, white-glove cybersecurity service that begins with a thorough and discreet investigation and technical audit. Exactly aligned with your specific requirements, based on discovery and risk, we deliver continuous, elite non-intrusive protection across your entire digital footprint including core systems, navigation, communications, entertainment and personal devices.

We combine best of breed security controls, AI-driven monitoring, unified cyber-physical controls, real-time threat intelligence and a single point of VIP support to preserve privacy, reputation and uninterrupted luxury experiences.

Maritime Cyber Baseline

Developed by CyberPlus' founders in conjunction with IASME the UKs leading information assurance organisation, and supported by RINA (Royal Institution Naval Architects), the Maritime Cyber Baseline Certification scheme provides an affordable and practical way for vessel owners and operators to achieve compliance in accordance with the International Maritime Organisation (IMO) guidelines, namely:

- IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3)
- IMO resolution MSC.428 (98)

CERTIFICATION BODY
MARITIME CYBER BASELINE

PENETRATION TEST & IMO COMPLIANCE GAP ANALYSIS

- Remote external penetration test
- Internal penetration test
- Onboard penetration testing and vulnerability assessment of all electronic systems
- Technical assessment of firewall and cybersecurity measures
- IMO & Data Protection compliance gap analysis
- Risk assessment & breach impact assessment

IMO ALIGNMENT & IASME MCB CERTIFICATION PROGRAM

- IMO compliance policies and procedures pack customised for the vessel and owner
- Formal risk assessment, treatment and remediation plans
- Internal audit report of compliance
- Evidence of controls
- Certificate attesting to IMO & MCB compliance
- Includes 12 months of advisory & support

24/7 CYBER SECURITY MONITORING SERVICE

- External internet penetration test
- Onboard penetration test & vulnerability assessment of all electronic systems
- Firewall and cybersecurity technical assessment
- IMO & Data protection compliance gap analysis
- Risk assessment & breach impact assessmentafeguard your yacht with confidence and sophistication.

INTERNET DIGITAL FOOTPRINT & SECURITY SCORECARD

- Allows for the discovery of all publicly visible artefacts belonging to the vessel
- Identifies any compromised or leaked credentials belonging to the crew or owners
- Consolidates public-facing vulnerabilities into a single easily digestible report
- Detailed results on each discovered vulnerability to aid remediation
- Detailed view of your cyber environment and risks

Superyacht cybersecurity services

cyber MARINE

CYBER SECURITY TRAINING & AWARENESS COURSES

- CIPD and RINA certified training courses
- Online elearning or onboard/ shore-based training
- Effective training for crew, tech & engineering staff as well as for captain/ owners
- Basic awareness to in-depth Maritime Technical ETO training
- Continual program tests resilience and vulnerability to phishing, insider threat, ransomware & technical surveillance

CYBER ATTACK EARLY WARNING SYSTEM

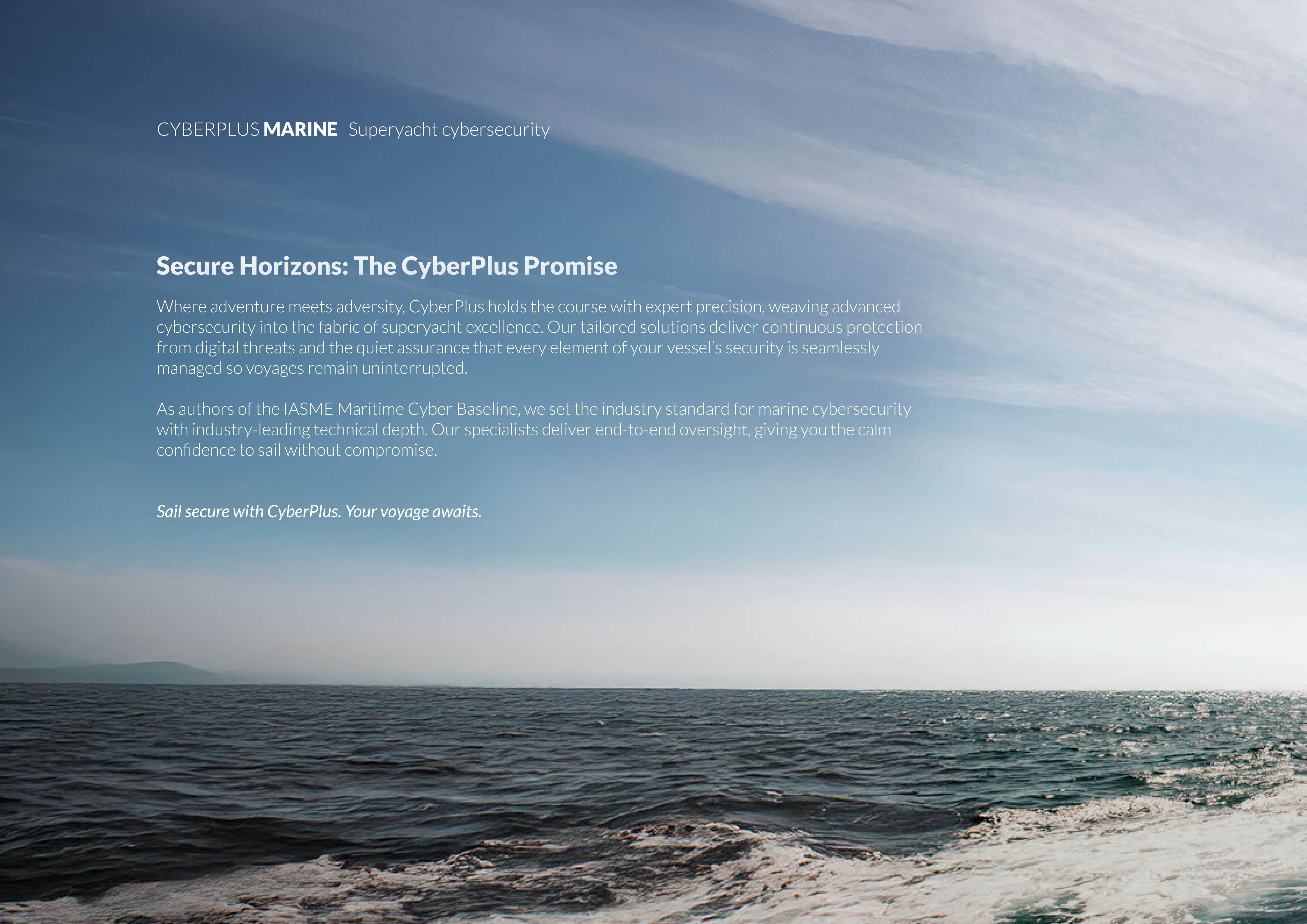
- Advanced detection system designed for maritime
- Provides immediate alerts and automated response to cyber attacks
- Zero false positives, only alert on malicious attack activity
- Decoy & deception system lures hackers into traps, so we can track & trace their activity
- Specific markers for targeted attacks across firewalls, networks, satcom and all IT/OT systems

DIGITAL ASSET MANAGEMENT SERVICE

- Managed asset register of all onboard electronic systems
- Discovery & IMO compliant documentation of all assets
- Identification & asset management of critical systems
- 24/7 risk assessment & alerting of high risk assets
- Monthly report of changes to digital assets

CYBER-PHYSICAL REAL-TIME THREAT INTELLIGENCE

- Real-time Threat Intelligence alerts and Geo-Fencing
- Addresses potential situational threats e.g. locations on course, that may increase exposure to risk
- Addresses potential targeted threats e.g. information discovered online, in social media, or the darkweb
- Automated alerts, based on type, shared with specific personnel for discretion
- Integrates cyber and executive protection teams



Secure Horizons: The CyberPlus Promise

Where adventure meets adversity, CyberPlus holds the course with expert precision, weaving advanced cybersecurity into the fabric of superyacht excellence. Our tailored solutions deliver continuous protection from digital threats and the quiet assurance that every element of your vessel's security is seamlessly managed so voyages remain uninterrupted.

As authors of the IASME Maritime Cyber Baseline, we set the industry standard for marine cybersecurity with industry-leading technical depth. Our specialists deliver end-to-end oversight, giving you the calm confidence to sail without compromise.

Sail secure with CyberPlus. Your voyage awaits.

Trusted Experts for Maritime Cybersecurity

Your sanctuary demands absolute security.

CyberPlus is a specialist consultancy and managed security services provider, headquartered in the UK and Germany, and experts in maritime cybersecurity for superyachts and commercial vessels. Creators of the IASME Maritime Cyber Baseline, we combine naval operational insight with enterprise threat intelligence to safeguard onboard systems, private communications and guest privacy.

At the heart of CyberPlus is a team of visionary cybersecurity experts, AI/AR technologists and seasoned strategists who apply targeted innovation and operational rigour to turn compliance into demonstrable resilience and strategic advantage. We deliver bespoke continuous readiness, anticipating threats, maintaining constant situational awareness and providing rapid proportionate response to protect people, systems and privacy while keeping life aboard uninterrupted.

Elevate your peace of mind. Speak to our specialists in confidence.

cyberplus.io

United Kingdom

167-168 Great Portland Street
5th Floor
London
W1W 5PF

Enterprise House
Ocean Village
Southampton
SO14 3XB

Germany

Barmbeker Straße 33
22303 Hamburg

All brand names, product names, and trademarks are the property of their respective owners. Certain trademarks, registered trademarks, and trade names may be used to refer to either the entities claiming the marks and names or their products. CyberPlus disclaims any proprietary interest in the marks and names of others. CyberPlus is not responsible for errors in typography or photography.