

# CYDOME Solution Brief

Leading cybersecurity solution designed for maritime IT, OT & communication requirements. Providing comprehensive support for IMO 2021 regulations for vessels and fleets.



## AWARD WINNING MARITIME CYBER SOLUTION



## Complete fleet wide cyber solution built for maritime.

We provide vessel-wide and fleet-wide cybersecurity monitoring, prioritization and mitigation. This is best in class multi-layered protection designed specifically for maritime IT, OT, and 3rd party integrations, which includes ongoing compliance with maritime regulations (IMO, IACS, and others).



### End-to-End Cyber Coverage

Coverage of all your assets on board, IT, OT & Communication for protection at every layer – your assets, network, vulnerabilities & compliance.



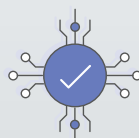
### Comprehensive Vessel & Fleet SIEM

Complete monitoring and management at both the whole fleet level and on individual vessels – even when they are offline – with streamlined UI dashboard design.



### Maritime Context Aware AI Detection

Advanced detection of cyber threats based on deep AI metadata analysis of maritime anomalies.



### Cyber Risk Management Solution

Embedded risk scoring analyses with prioritization and mitigation recommendation.

## Built for Shipping

- **Smart Bandwidth Utilization**  
Intelligent and dynamic bandwidth utilization to overcome limited or no connectivity limitations.
- **On Prem or On Cloud**  
Designed to provide flexibility and available both on-premises and on the cloud.
- **Zero Touch Deployment** solution (VM or appliance).
- **Easy to Deploy** on all vessel types, and integrates with legacy and new systems.

## Industry certifications



*"Chemical and oil tankers need the highest level of cyber protection. We get this protection from Cydome. The tech is super sophisticated but simple to use."*



## Cydome Solutions



### Comprehensive Asset Inventory

**Eliminate blindspots across the vessel's network.**

- Full coverage of IT, OT, Communication and Third Party access
- Accurately map all onboard assets to identify vulnerabilities
- Receive automatic alerts on anomalies.
- Segment networks to reduce the attack surface.



### Real-time detection

**Advanced Intrusion Detection and Prevention Systems (IDS/IPS).**

- Catch signs of intrusions before they break through.
- Expose and report on all possible attacks.
- Keep systems isolated and uncompromised.
- Receive automatic recommendations to address threats and mitigate damage.



### Vulnerability Scanning

**Know your weak points.**

- Detect real time cyber threats from on and offshore.
- Monitor the latest known threats for comprehensive risk management.
- Get detailed recommendations and mitigation steps whenever threats are found.



### Embedded Maritime Compliance

**Automated compliance wizard.**

- Continuously updated cyber security manual.
- Maintain continuous compliance with IMO2021 standards with built-in tools.
- Cruise confidently and compliantly into 2024, when IACS Unified Requirements E26 and E27 become mandatory.
- Automate away manual compliance tasks, for accurate and seamless reporting to inspectors.

# Features and Specifications

Assets Layer	Asset Mapping	<p>Continuous asset mapping of the vessel's IT and OT assets.</p> <ul style="list-style-type: none"> <li>• Detailed inventory of assets and the relationships between them.</li> <li>• Identify and prioritize risks, vulnerabilities, to develop effective mitigation strategies.</li> <li>• Make more informed decisions, allocate resources more efficiently, and improve overall security and resilience.</li> </ul>
	Inventory Management	<p>Enables security teams to maintain an accurate and up-to-date inventory of all hardware and software assets, including servers, workstations, applications, and other IT and OT resources.</p>
	Asset Anomaly Detection	<p>Detects unusual activity related to physical and digital assets. Security teams are alerted to deviations from normal patterns of asset usage.</p> <p>Provides real-time insights into potential security incidents:</p> <ul style="list-style-type: none"> <li>• Unauthorized access</li> <li>• Port changes</li> <li>• Disconnections</li> <li>• Other behavioral changes</li> </ul>
Network Layer	Network Segmentation Monitoring	<p>Ensures the security and integrity of the vessel's network infrastructure. Monitor network traffic to detect any unauthorized attempts to access or move between network segments.</p>
	Intrusion Detection System (IDS)	<p>Continuously monitors the vessel's network for signs of malicious activity or intrusions and generates notifications when potential incidents are detected.</p> <p>Analyses of all internal and external passing traffic using deep packet inspection and matching with a built-in library of known attacks, policies, and anomaly detection..</p> <p>An inline solution (Intrusion Prevention System IPS) is also available, please contact us for more details.</p>
	Isolation Breach Detection	<p>Monitoring of isolated devices, such as Electronic Chart Display and Information Systems (ECDIS), with breach detection.</p> <p>Isolation breaks increase the risk of unauthorized or malicious users compromising sensitive systems, and ultimately, the entire ship.</p> <p>When a breach is detected the onboard and/or onshore security team receives an alert to take appropriate action.</p>
Vulnerabilities Layer	Attack Simulation & Vulnerability Scanning	<p>Identifies potential weaknesses and attack vectors on vessels. Automatically scans for vulnerabilities of all onboard systems and generates detailed reports.</p> <p>This feature enables organizations to:</p> <ul style="list-style-type: none"> <li>• Proactively detect and address potential security weaknesses.</li> <li>• Reduce the risk of security incidents.</li> <li>• Enhance the security posture of their operations.</li> </ul>
	Risk Scoring	<p>A centralized interface and a single source of truth helps organizations to proactively identify, assess and mitigate potential cyber risks.</p>
	Mitigation	<p>The vulnerability scanner provides mitigation steps when threats are detected. Efficiently manage security posture, reduce the likelihood of incidents, and reduce the work required from IT teams.</p>
Compliance Layer	Compliance Automation & Management	<p>Automate workflows, streamline reporting, and manage policies and procedures. Reduce the cost and complexity of compliance management, while improving compliance outcomes in line with IMO, TMSA3, LR, and more.</p>
EndPoint Layer		<p>Comprehensive Endpoint Security across all shipboard devices, systems, equipment, and other infrastructure.</p>
Fleet Layer	Vessel SIEM	<p>Security Information and Event Management (SIEM) continuously collects and analyses fleet-wide security data. The SIEM can work effectively on an individual ship as well as entire fleets. The system supports integrations with third party industry SIEM platforms.</p>
	Multi-fleet support	<p>Manage and monitor multiple fleets from a single platform. Gain a better understanding of the fleets' performance, optimize operations, minimize downtime, and enhance the safety of crew and vessels.</p>





## Who we are

Speedcast is a leading communications and IT services provider, delivering critical communications services to the Maritime, Energy, Mining, Media, Telecom, Cruise, NGO, Government, and Enterprise sectors. Speedcast is an authorized reseller and integrator of Cydome, an advanced maritime cybersecurity solution.

Cydome empowers IT managers to detect threats and act effectively to overcome them, while ensuring continual compliance to a higher standard than any other product on the market. Our customers include Top 100 shipowners.