Cyber Security for the Maritime Industry.

VULNERABILITY ASSESSMENTS FOR VESSELS AND SHORE-BASED ASSETS

SDSD offers a full range of application and infrastructure vulnerability assessments designed to identify and evaluate security vulnerabilities and recommend risk mitigation strategies.

These services assist businesses in enhancing their current security posture while reducing the danger of a major attack in offices and across the fleet.

Why do Shipping Companies need to take Vulnerability Assessments seriously?

The first two IMO MSC-FAL.1/Circ.3 functional elements regarding Cyber Security as part of the ISM are identify and protect. With cyber threats increasing in the maritime industry, companies should do a risk assessment of assets and take appropriate measures to reduce risks to acceptable levels.

The Vulnerability Assessment is a process that will assist you and prove that you have completed the required process properly and as per industry standards.

SDSD's tried and trusted security process and experienced methodology improves safety by comparing your security to industry standards.

1. Identifies at-risk assets
2. Validates the suitability of security controls
3. Creates inventories of all the devices on the network, including their purpose, system information and specific vulnerabilities
4. Defines the level of risk present on the network

Protect your assets, with consultant supported assessments from SDSD, understand your current vulnerabilities with clear guidance and make improvements quickly.

The assessment is based on your specific setup and will be planned accordingly. Typically, the assessment will cover the following types of systems:

1. Bridge systems
2. Cargo handling and management systems

3 Propulsion and machinery management and power control systems

4 Access control systems

5 Administrative and crew welfare systems

6 Communication systems

Vulnerability Assessment Services include:

1 External network vulnerability assessments

2 Internal network vulnerability assessments

3 Network architecture reviews

4 Device configuration reviews (host and network)

What our Consultants provide:

1 An executive report for the management

2 A separate detailed technical report with observations and recommendations to improve the security level and hardening of the IT and OT infrastructure.

3 Peace of mind that you are adequately protecting systems and data from malicious attacks and meeting regulatory requirements.

+44 20 3588 6740, +65 3158 7545
+30 21 1198 4479, +971 529957617

sales@sdsd.com

www.sdsd.com