Cyber Security for the Maritime Industry.

PENETRATION TESTING

Identify how an attacker could breach your network security and mitigate risks before they are exploited by a third party.

Penetration Testing is a simulated attack which attempts to breach some or all of that system's security, using the same tools and techniques as a hostile third party.

The goal is to identify how a hacker could attack the applications, networks, mobile devices and wireless networks, and give confidence that the products and security controls tested have been configured in accordance with good practice and that there are no common or publicly known vulnerabilities in the tested components, at the time of the test.

With Cyber Security as part of the ISM (IMO MSC FAL.1/Circ.3) Penetration Testing ensures that shipping companies are mitigating risk as part of the Identify and Protect requirements under the guidelines that came into force in January 2021.

Service Overview

SDSD's penetration tests are customized to the shipping company's environment and requirements, assessing specific aspects of the security program, critical systems, networks and applications.

We utilize three types of Penetration Testing across your network and devices, to ensure security.

External Penetration Tests – we show you the risk to assets exposed to the Internet. Our testing checks for vulnerabilities in systems, services, and applications that are exposed and could be exploited.

Internal Penetration Tests – our Consultants help you to understand the risk to your network from a breach caused by a flaw. We use specialist tools to simulate the actions of an insider or an attacker who has acquired access to an end-user system, such as escalating privileges, installing custom-crafted malware or exfiltrating critical data.

Web Application Assessments – these tests verify the security of applications that provide access to critical data. We examine all web and mobile applications for flaws that could lead to unwanted access or data leakage.

Benefits

1. Find out if any of your critical assets are at risk
2. Detect and mitigate sophisticated security
3. flaws before they are exploited by an attacker
4. Obtain realistic conclusions and detailed
5. Recommendations
6. Meet regulatory compliance and standards
7. Requirements

What we provide

1. Summary report for executive and senior-level
2. Technical details that provide enough detail to replicate our findings
3. Tactical recommendations for immediate improvement
4. Strategic recommendations for longer-term improvement

The information shared by our Consultants will help you to implement security upgrades to plug up any vulnerabilities discovered during the test. Keeping your assets secure and helping you comply with **IMO guidelines.**


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


sales@sdsd.com


www.sdsd.com