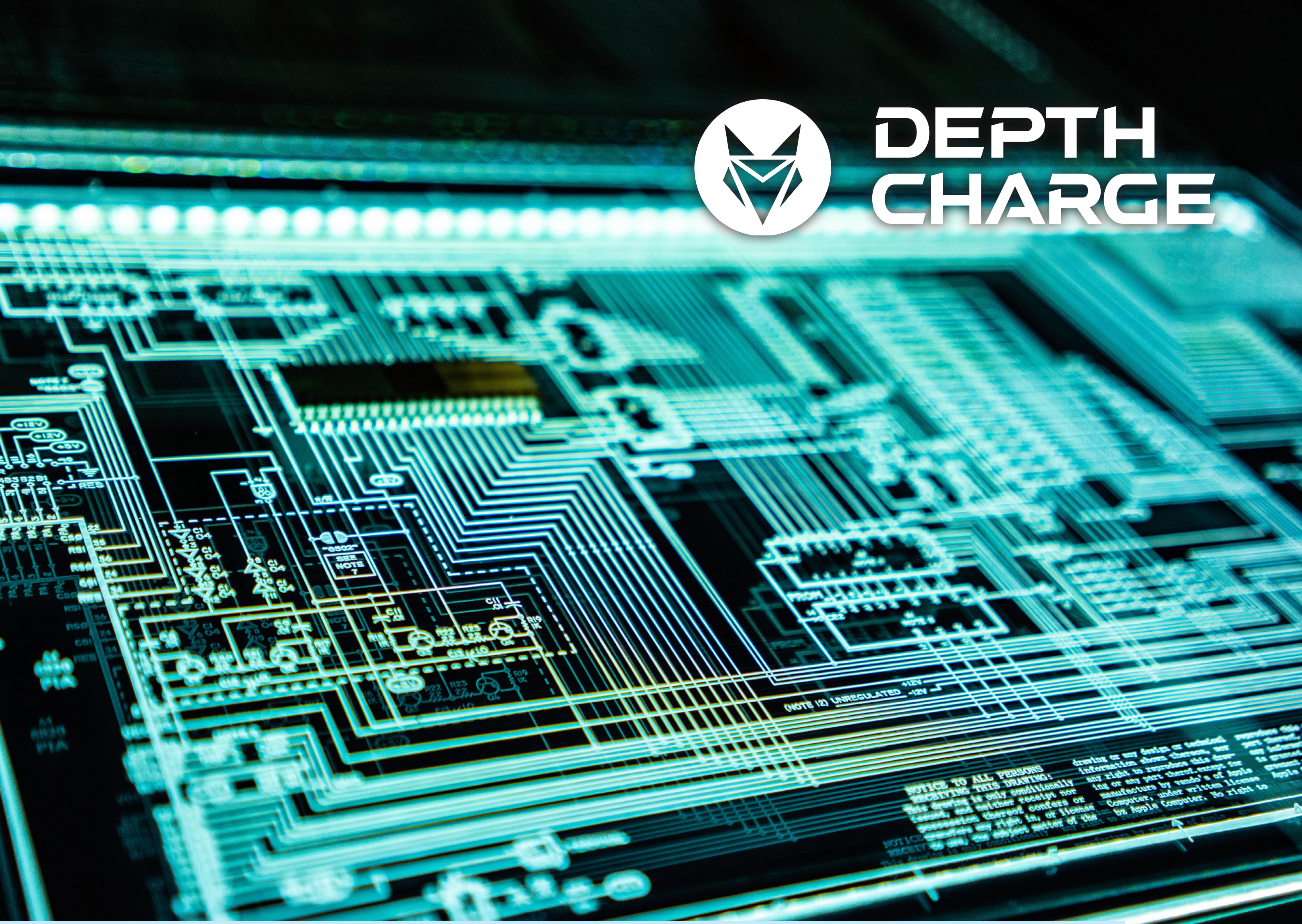


DEPTH CHARGE

MARITIME ADMINISTRATION

CYBER SECURITY AND DATA SERVICES

DEPTH CHARGE IS THE CYBER SECURITY ARM OF OCEANS HQ. OUR TEAM HAS A LONG HISTORY OF SECURING AND PROTECTING SENSITIVE SYSTEMS AND DATA FOR GOVERNMENTS AND MARITIME ADMINISTRATIONS AROUND THE WORLD.

OHQ CLOUD

WWW.OCEANSHQ.COM | PHONE: +44 (0)3300 881002 | EMAIL: INFO@OCEANSHQ.COM

Secure, Reliable Cyber Security Services

With an established team of highly experienced and skilled professionals, we can address specialised services tuned for your specific security case for either proactive or investigative analytics, assessments and audits.

We assist organisations defend against cyber-attacks and implement efficient preventive measures customised for each specific infrastructure, correlated with additional services for investigating vulnerabilities in a proactive manner.

With the help of our assessment results and test outcomes, we assist our partners in identifying technical weaknesses in their infrastructures and guide them to implement mitigations before such vulnerabilities will be exploited by real attackers. The goal is always to be one step ahead.

The in-depth expertise of our team covers a plethora of areas in the constantly expanding domain of IT Security. We offer a wide range of services, covering continuous vulnerability scanning, penetration testing, web application testing, mobile application testing and even Red Team simulated attacks.

Every member of our security team is continuously improving their skills to be up to date with the attack vectors and area trends. All services are flexible and can be seamlessly adapted to your specific needs and budget.

Securing systems and data is crutial in today's globally connected world

The MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management. The recommendations can be incorporated into existing risk management processes and are complementary to the safety and security management practices already established by IMO.

VULNERABILITY SCANNING

WEB APPLICATION, API AND NETWORK PENETRATION TESTS

RED TEAM PENETRATION TESTING

Vulnerability Scanning

One of the easiest ways for an attacker to step inside an organisation is to exploit an old version of a software component that is directly exposed to the Internet. Historically, that piece of software may have had a number of vulnerabilities that could be exploited by an attacker. Failing to implement proper patch management (updating software components to their last version, replacing obsolete software components) and exposing them to be accessed from the Internet may leave gates open for disaster.

Our Vulnerability Scanning service combines automated testing techniques with multiple open source toolchains that are used by Penetration Testers on their engagements. To present a realistic view of the vulnerabilities present on your Internet-exposed services, any finding presented by automated tools will be manually validated by our team to rule out false positives and time spent by your IT team trying to fix what's not broken.

When we engage with clients, our initial focus is defining the landscape of the organisation and the areas of highest risk before we drill down into specific sub-systems, integrations & connections.

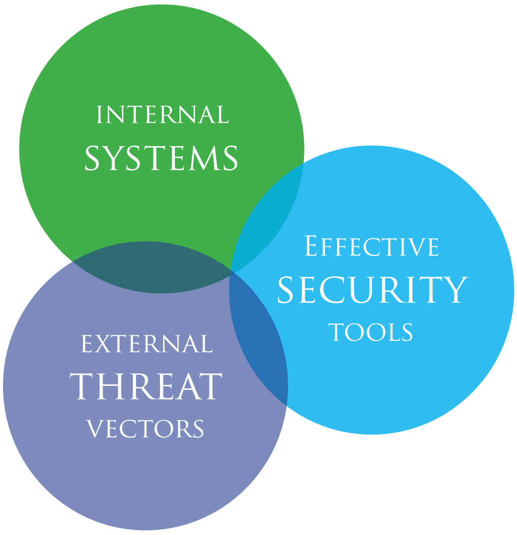
External Assessment

An external vulnerability assessment focuses on identifying known vulnerabilities that can be exploited from outside your organisation via services that are exposed to the public Internet. We look for systems that are not protected by firewalls and other security appliances, where attackers will use these services as potential a point-of-entry into your systems.

Internal Assessment

Here we focus on scanning for known vulnerabilities within your internal network, where security restrictions are not as tightly enforced as they are from the external perimeter. In addition, vulnerability scans can be conducted against web applications without manually testing for logical flaws covered by a dedicated Web Application security test, but still keeping track of any vulnerabilities that may apply to the software platform or framework exposing the web application to the internet.

Vulnerability Scanning is non-intrusive, poses minimal risk and enables you to stay ahead of possible attacks by keeping everything up to date.



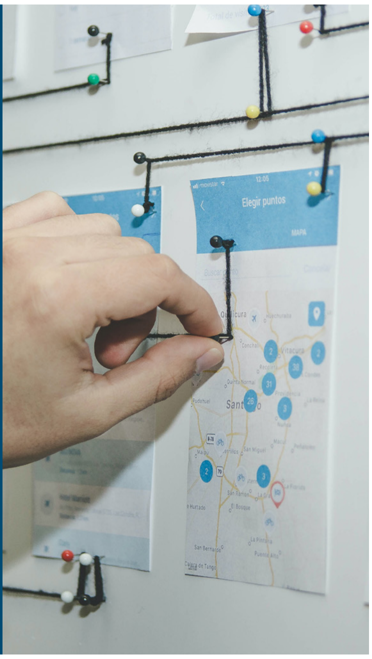
Web Application, API and Network Pen Testing

Penetration testing is a dedicated type of simulated attack that tries to discover any possible vulnerability in the web application code, API implementation and network, but goes one step further than a Vulnerability Assessment.

Any possibility of breach that has been identified will be attempted to be exploited to clearly identify the impact of a security breach compromise your infrastructure and what type of data would a potential attacker be able to obtain. The testing operation itself combines automated testing techniques with manually performed intrusions and exploits.

Penetration testing workflow

- Extensive information gathering using public sources (such as Google hacks, Shodan, NetCraft, other such services);
- Manual interaction with the application/API to learn its functionality and map its business logic;
- Automatic crawling to identify specific/known vulnerabilities followed by manual checks on each identified vulnerability;
- Improper validations that could lead to SQL injection, Remote Command Execution, LDAP injection;
- Cross site scripting (XSS) and cross-site request forgery (CSRF) tests;
- Testing of the authentication and authorization mechanisms, plus the session management;



Network Penetration Testing

A Network Pen Test targets your network's perimeter to identify weaknesses that could be exploited by an attacker to gain unauthorised network access. This type of test involves thorough examination on all the Internet facing systems in your organisation and tries to exploit their weaknesses to gain access to sensitive information or even straight access to the internal network.

In this scenario, the simulated attacker is located outside your organisation's network, impersonating anyone with an Internet connection and a will to create havoc. They will try to identify and exploit vulnerabilities in your network's defense systems.

Thorough evaluations of all exposed services (such as DNS, e-mail protocols, management protocols, file transfer protocols, VPN implementations and many others) will be performed in a layered approach, but with a focus on directly exploitable issues that provide an imminent danger. Tests include at least a set of operations similar to:

- Information gathering from public sources to identify organisation's public IP addresses and other public information;
- Exposed service scanning and Service identification to determine what type of software and which version is offering that service;
- Automated vulnerability scans, manual searches for vulnerabilities based on discovered information and exploitation of detected vulnerabilities;
- Brute-force attacks / password guessing to verify strength of user credentials.

Proven & Endorsed By Those In The Industry

Oceans HQ is a trusted and recognised brand within the maritime industry.

"Regular discussions are held with the team at Oceans HQ to continually ensure they understand our needs. They show us how existing features can fulfil our requirements and suggest suitable alternatives to keep on succeeding. The depth of knowledge on both the tech and importantly the maritime requirements blows my mind almost daily. There is no "them" and "us" – it's a true partnership that has been built with mutual trust at the core."

ST. KITTS & NEVIS
INTERNATIONAL SHIP REGISTRY

Liam Ryan, Chief Executive
St Kitts & Nevis International Ship Registry

Red Team Penetration Testing

This type of test is a direct comparison to a targeted hacker attack focusing solely on your organisation. It will not only verify your infrastructure strengths, but also how good would your employees act in the event of a targeted attack.

Historically, the weakest link in the IT security chain was and will remain the individuals within your organisation. Lack of security knowledge correlated with a lack of, or unsatisfactory training will continue to put employees in positions to expose confidential information – or worse.

The RED TEAM TEST is a black box test, with the primary focus of bypassing company defences, with the sole requirement being the name of the company to target. OSINT will be used to validate the ownership of in-scope networks and potential entry points. There is no particular path for the process to take place and is highly dependent on the component being tested.

Red Team takes a covert approach to testing and is as real as it can be compared to a normal, targeted attack against your organisation. The main goal of the test is gaining access to highly sensitive information, as it would be the case with a real attack.

Malware Analysis

Post-security incident analysis/audit, determining the impact, initial infection vector, malware functionalities, data exfiltration capabilities, persistence and propagation, removal and deterministic compromise indicators.

Incident Response

Following malware analysis, we work with your organisation and IT department to outline the steps required to clear the damage and protect against further similar occurrences.

ISO27001 Support

Our consultants have a wealth of knowledge relating to ISO27001, SOC2 and other information security management systems. We can work with your internal and external auditors to further strengthen organisational resilience.

Transparent Pricing

ALL CYBER SECURITY ENGAGEMENTS ARE PERFORMED ON A DAY-RATE BASIS ALIGNED TO THE AGREED SCOPE OF THE PROJECT.

NETWORK PENETRATION TESTING

Minimum 4 days testing, 1 day reporting. The day rate for this engagement is £750/ day exclusive of applicable taxes.

WEB, API AND MOBILE APPLICATION TESTING

Minimum 3 days testing, 1 day reporting. The day rate for this engagement is £750/ day exclusive of applicable taxes.

MALWARE ANALYSIS AND INCIDENT RESPONSE

Minimum 3 days testing, 1 day reporting. The day rate for the above items is £1050/ day exclusive of applicable taxes.

The cost of the vulnerability scanning service is dependent on the number of targets, the requirement for an internal scanning agent appliance and the number of scans per month.

Engagement Standards & Options

WHATEVER YOUR NEEDS, OCEANS HQ CAN PROVIDE TRAINING, SUPPORT AND CONSULTANCY IN MANY AREAS OF CYBER SECURITY AND DATA PROTECTION. WE ALSO OFFER A FULLY MANAGED SOFTWARE PLATFORM FOR MARITIME ADMINISTRATIONS CALLED OHQ CLOUD.

PEN-TESTING IN-HOUSE APPS

We regularly work with organisations that have developed in-house web applications in the maritime sector. With systems containing an array of personally identifiable information and sensitive data, your security defences are the front line in complying with your data protection obligations.

9 out of 10 in-house applications we test have at least 1 major security vulnerability that requires expedited remediation.

PEACE OF MIND

All vulnerabilities discovered during any of our engagements are bound by our vulnerability disclosure process and backed by our belief in the SOP's agreed upon. We respect privacy and focus on doing no harm in every penetration test we are involved in.

If you have unique requirements such as on-site training, specific system testing or custom security protocols that are essential, we can tailor our services to meet your needs.

Looking for a secure platform for your maritime administration?

For organisations that are looking for a secure maritime administration platform, consider OHQ Cloud. You can benefit from our on-going secuirty monitoring and protection while getting best-in-class software tools to support the operations of your registry, survey, seafarer divisions. Our unified platform is tailored for maritime administrations like yours.

OHQ CLOUD

MARITIME ADMINISTRATION PLATFORM

Simplify processes, increase security of transactions and bring customers closer

WWW.OCEANSHQ.COM

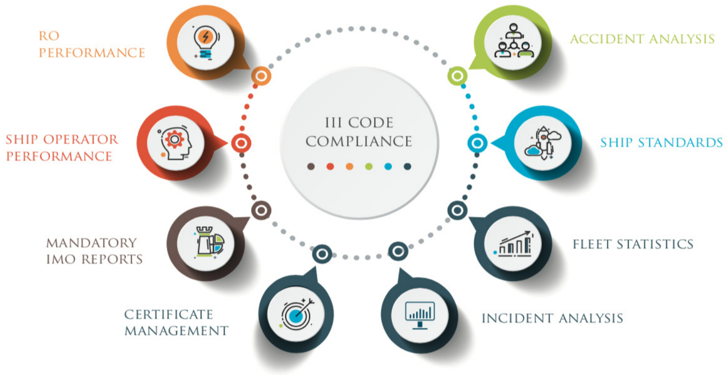
Seamless ISM Compliance and Superior Data Security

OHQ Cloud is a fully managed service with 24/7 support, deployed in the cloud, on-premise or hybrid as required by our clients.

WHAT WE DO AND HOW WE DO IT

TOOLS THAT MAKE COMPLIANCE EASY

OHQ Cloud provides a tool for every situation. Remove the pain of complying with the latest international regulations by using a platform continually fit-for-purpose. Every aspect of carrying out your business is now only a few clicks away. Detailed reporting engines and analytics make even IMO audits a breeze.



ONE PLATFORM, MULTIPLE TOOLS

··· VESSEL HQ	··· Ship registration, survey & management
··· SEAFARER HQ	··· Seafarer records & certification
··· FRONTIER	··· Digital self-service portal for your customers
··· PAYMENTS	··· Online and in-person payment processing
··· ATLAS	··· Staff training, education and upskilling
··· VOYAGER	··· Data streaming and migration from any source

* All services support legal electronic signatures via leading digital signature tools from Global Sign, DocuSign and Adobe.

JOIN THE OHQ COMMUNITY

GIBRALTAR SHIP REGISTRY

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

ADOMS
Antigua & Barbuda
Department of Marine Services
and Merchant Shipping

Government of the Virgin Islands

ST. KITTS & NEVIS
INTERNATIONAL SHIP REGISTRY

Maritime & Coastguard Agency

SIERRA LEONE
MARITIME
ADMINISTRATION

OHQ
CLOUD

OCEANS HQ LTD
71-75 SHELTON STREET
COVENT GARDEN
LONDON, WC2H 9JQ
UNITED KINGDOM

WWW.OCEANSHQ.COM
+44 (0)3300 881002