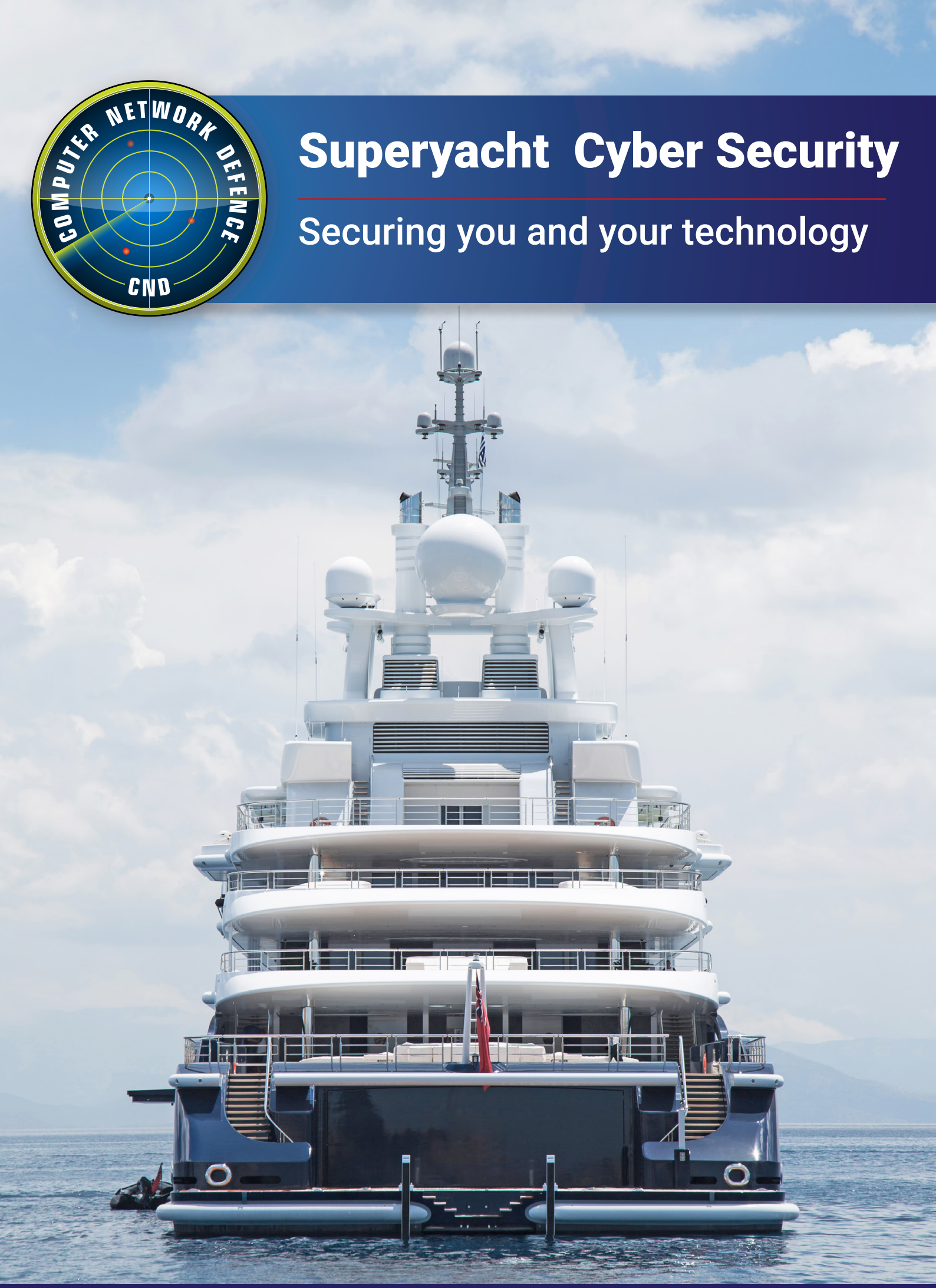
Superyacht Cyber Security

Securing you and your technology

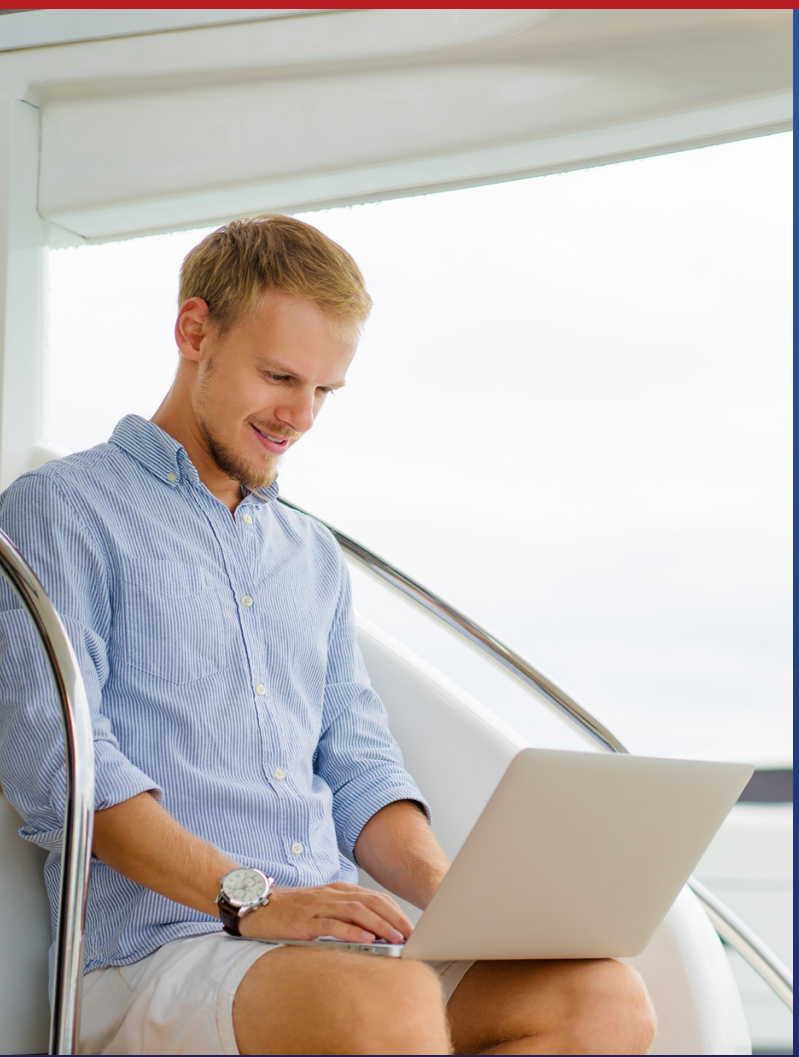


www.cndltd.com cnd.enquiries@cndltd.com +44 (0)1225 811 806

ABOUT US

Computer Network Defence Ltd (CND) Have been delivering cyber security capability into maritime clients for over 11 years.

Whilst the bulk of our work has been with naval forces, such as the European Union Naval Force and the British Royal Navy, CND have recently seen an increasing demand for our services with VIPs and their superyachts.



ABOUT OUR SUPERYACHT SECURITY SERVICE OFFERING

Superyacht owners are being increasingly targeted by a number of adversaries, such as journalists, criminals and even Nation States. The attack methods used are becoming ever more elaborate and diverse.

As a result of this increasing threat, CND have produced a modular service, which can be adapted and scaled to counter every likely scenario.

With our superyacht service, we look at all aspects of cyber security from the user aboard right through to the destination of the network traffic and a plethora of other associated activity external to the yacht.

www.cndltd.com cnd.enquiries@cndltd.com +44 (0)1225 811 806

AN OVERVIEW OF OUR CYBER SECURITY MODULES

The following modules may be selected either individually or in groups, dependent upon your requirements and the cyber security threats which you feel that you may be facing. An account manager will discuss the various scenarios and modules available to help define the requirements for the engagement with us.

1. Secure by Design
2. Wireless Security
3. Network Connected Devices
4. Virtual Private Network (VPN)
5. Security Monitoring
6. Security Architecture
7. Penetration Testing
8. Supply Chain Security
9. Crew Security Vetting
10. Cyber Threat Intelligence
11. Cyber Security Awareness Training
12. Cyber Security Health Check
13. High Level Security
14. Permanently Equipped Hidden Device Detection
15. Mobile Phone Interception Detection
16. Temporary Mobile Phone Interception Detection
17. TEMPEST
18. GPS Navigation Attack
19. Automatic Identification System (AIS) Evaluation
20. Voyage Data Recorders (VDR) aka Blackbox
21. Physical Security
22. Guarding and Hostage Situations

1. SECURE BY DESIGN

The ideal time for cyber security to be considered is at the vessel design stage, or during refit. This enables us to undertake our work more effectively and without the client having to face the higher costs of keeping any re-engineering aesthetically pleasing. Shipbuilders now recognise the need for cyber security as part of their integral design due to increasing demand from their clients.

2. WIRELESS SECURITY

Most yachts have wireless access points to provide passengers and crew with Internet access from laptops and phones, off ship connectivity is usually via Satcom, 3G or a hybrid solution. The actual wireless access points may be visible some distance from the vessels. We look at fine tuning the Wi-Fi signal such that it's reach is minimised but usable, whilst optimising the security of the Wi-Fi configuration. This reduces the risk of journalists and criminals cracking the Wi-Fi and accessing the vessels network. We can also carry out a penetration test and try to hack into the wireless network.

3. NETWORK CONNECTED DEVICES

There may be a number of pieces of equipment connected to the internal network on the vessel, from control systems, navigation through diagnostics to servers. With Fly-By-Wire and other industrial control systems having so many potential vulnerabilities, a lack of protection could be disastrous. We perform a network mapping exercise and vulnerability assessment to see what is connected and whether they are vulnerable. We may also recommend segregation of the network especially for guests visiting the vessel, keeping them away from the critical infrastructure and client data.

4. VIRTUAL PRIVATE NETWORK (VPN)

As the vessel moves around the globe it will have to rely on locally provided communications, or satellite communications both of which are susceptible to interception. We can provide an encrypted tunnel between the vessel and our Isle of Man datacentre, as the traffic enters or leaves the tunnel in the Isle of Man it will pass through some sophisticated monitoring equipment which will look for threats which may suggest compromise. We have successfully designed and implemented a similar solution for the UK Ministry of Defence.

5. SECURITY MONITORING

Where there are a number of network security devices on-board we may suggest that security events from the vessel are sent to our Security Operations Centre in Douglas, where we will analyse them and notify the clients if we detect anything suspicious.

6. SECURITY ARCHITECTURE

For more complex network topologies we will undertake a security architecture review and advise on the use of firewalls, Intrusion Prevention Systems, etc. The architectural security advice extends into applications and cloud provisioned services such that a defence in depth approach is recommended.

7. PENETRATION TESTING

With your prior approval our consultants will attack your network boundaries as though they were a hacker using the same methods. Where permitted by the service provider we will ensure that your cloud provisioned services and social media platforms are configured securely.

8. SUPPLY CHAIN SECURITY

It is important to check that your suppliers also meet an appropriate level of cyber security which is commensurate to the level of trust you afford them and the access granted to your systems, thereby ensuring that they will not be used as the weak link to attack your vessel or compromise your sensitive information or intellectual property.

9. CREW SECURITY VETTING

We are able to carry out vetting of the crew to provide some assurances that they meet the necessary standards and haven't been planted or are working for their own nefarious gain.
We can also periodically review their Internet presence through social media, etc. to ensure they aren't divulging client information or bringing the client into disrepute.

10. CYBER THREAT INTELLIGENCE

In a similar vein to checking the crew we can set an alert into our cyber threat intelligence service to detect any open source discussion on the Internet, including the dark web. You supply us with key words such as the ships name, or individuals such as the captain, crew, owner, including their email addresses and we'll alert you if we detect anything untoward.

11. CYBER SECURITY AWARENESS TRAINING

Through our VIP Domestic Staff cyber security awareness training, we appraise crew of the threat and what they can do to be more secure online, from hidden metadata in photographs to online dating. The course was originally designed to prevent children being targeted through inadvertent compromise of information from house staff.

12. CYBER SECURITY HEALTH CHECK

This is often the most cost effective way of engaging our services; one of our Principal Cyber Security Consultants will discuss the threat with the client and ascertain the size and scope of the task at hand. The client will then purchase a number of days on a call off basis. The CND team will prioritise which modules to check and adapt their progress according to what they find, discussing their findings with the various stakeholders throughout.

13. HIGH LEVEL SECURITY

Some clients have good reason to want a higher level of security as they may be targeted by criminals, journalists and even Nation States. We offer a Technical Surveillance Countermeasures (TSCM) sweep where we look for hidden monitoring devices, more commonly known as a bugsweep, which combined with our cyber security health check takes the vessel security to the next level. Unlike many such service offerings we can detect devices which are dormant and have been hidden within walls, ceilings, furniture, etc.

14. PERMANENTLY EQUIPPED HIDDEN DEVICE DETECTION

We can also permanently install equipment which provides a real time alerting mechanism to detect any new transmitting devices which have been brought aboard as the vessel goes about its travels.

15. MOBILE PHONE INTERCEPTION DETECTION

A new service for high risk targets, the equipment will be permanently installed on the vessel and identifies and alerts on numerous attack characteristics across 2G, 3G, 4G LTE and CDMA networks, from basic DIY built IMSI catchers to sophisticated Nation State systems. The equipment will also triangulate to the source of the attack.

16. TEMPORARY MOBILE PHONE INTERCEPTION DETECTION

When a vessel is destined to spend some time alongside in a high-risk port, or if a client is holding a sensitive meeting, etc. we can provide an operative to monitor and secure the vessel from eavesdropping and/or mobile phone interception.

17. TEMPEST

A cold war phenomenon used by Nation States to reconstitute data from the enemy, whilst such an attack is extremely rare and very expensive, some of the countermeasures are cheap and easy to implement. Our GCHQ trained staff will give guidance on how to defend against compromise over RF transmission such as VHF, UHF and SHF.

18. GPS NAVIGATION ATTACK

Given the right equipment and opportunity, attackers are able to alter a ship's course through feeding false GPS information "spoofing". Our military trained electronics experts can reconfigure your navigation systems to minimise the risk.

19. AUTOMATIC IDENTIFICATION SYSTEM (AIS) EVALUATION

The configuration of the vessels AIS will be evaluated to balance the risk of inadvertent disclosure of information (security) against the legal requirements within the Safety of Life at Sea Chap V, Regulations 19 and 19-1 or the regulations pertinent to the country of registration or waters where the vessel is used (safety).

20. VOYAGE DATA RECORDERS (VDR) AKA BLACKBOX

Whilst allegedly tamper-proof, there are numerous cases where they have been hacked, corrupted or data manipulated, some have remote connectivity. Our penetration testers will evaluate your VDR and report on any vulnerabilities.

21. PHYSICAL SECURITY

As part of our Cyber Security Health Check we can perform a physical penetration test to ensure that security controls and The International Ship and Port Facility Security Code (ISPS) compliance are in place. We can review all aspects of security and risk management on board, at sea, and in port in line with Best Management Practice 4 (BMP4).

22. PROTECTION AND HIJACK RESPONSE

We have specialist partners who provide prevention training, on board protective services and hijack response services. They are retained by leading marine insurers and have resolved piracy cases for merchant vessels and pleasure craft in West Africa, the Gulf of Aden and the Indian Ocean.

CONTACT DETAILS

Contact us now to explore how we can defend your business and improve your cyber security posture:

22 St Lawrence Street, Bath, UK, BA1 1AN

www.cndtd.com
cnd.enquiries@cndltd.com
+44 (0)1225 811 806