

XTREME SECURITY

FROM ARMED PROTECTION ON THE HIGH SEAS, TO CYBER SECURITY AND TECHNICAL SECURITY MEASSURES

XTREME SECURITY

info@xtremesecurity.eu

info@xtremesecurity.eu

TABLE OF CONTENT

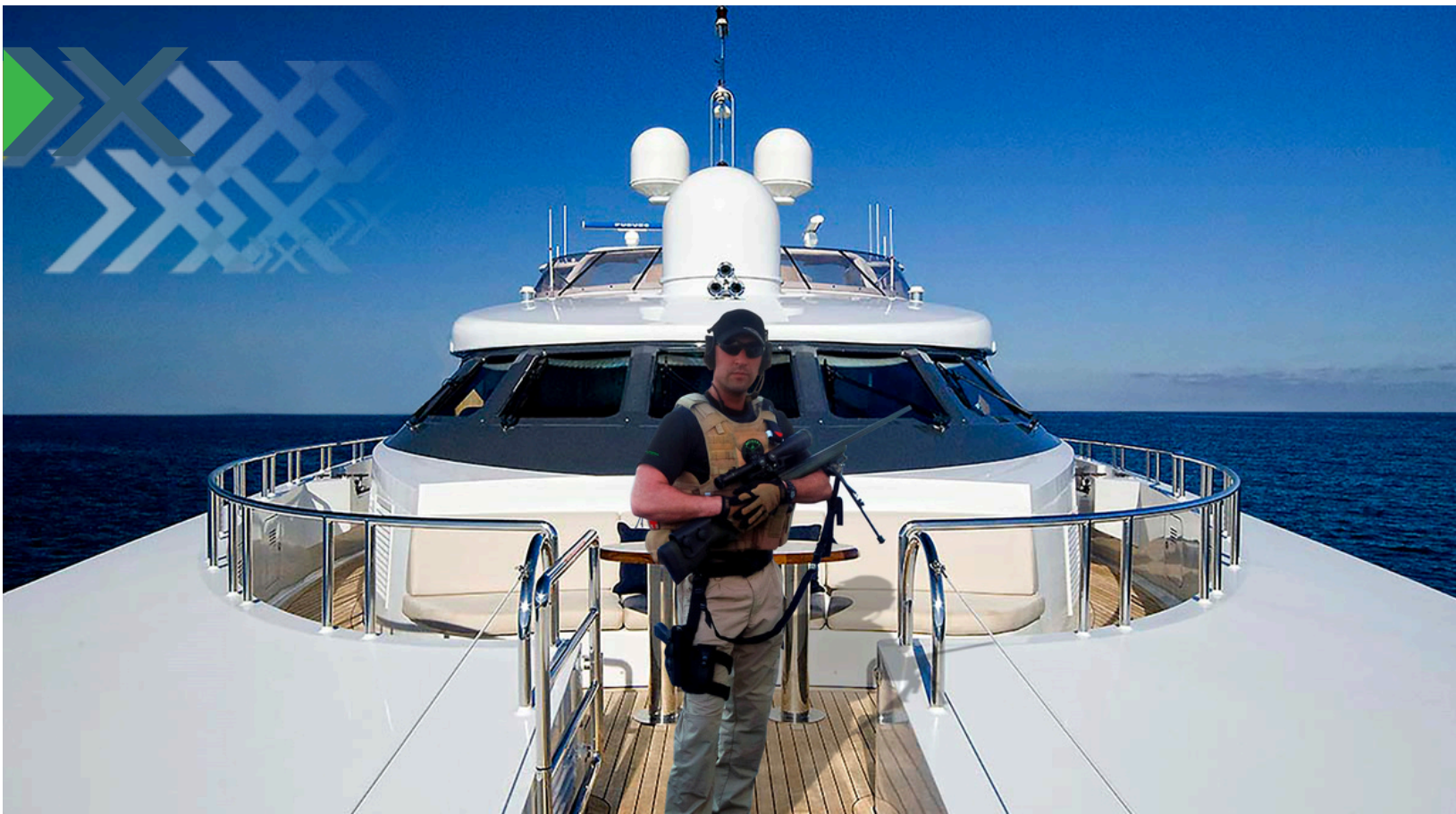
01: Secret-service level security

02: Cyber security on a Superyacht

03: Recovery is harder than prevention!

When It Comes to Superyacht Security, Nothing Is Impossible

Theft and burglary, unwanted paparazzi attention, personal attacks, kidnapping, and even pirate assaults are significant risks for superyacht owners. Technological advancements have transformed these threats, making the central computer systems of ships vulnerable to hacker cyberattacks. Privacy risks are heightened by remote-controlled drones and underwater submersibles. In response, yacht owners have adopted military-grade security technologies. We can now create a 'virtual bubble' around the vessel with infrared thermal imaging cameras, short-range radar, and diver-detecting sonar, ensuring any object—whether on the surface, in the air, or underwater—is detected and tracked around the clock





Secret-Service Level Security and Premier Facilities Onboard

Some owners of custom-built superyachts choose secret-service level protection and seclusion on board, primarily becausethey appreciate cutting-edge gadgetry or want to maintain their regular lifestyle while at sea. From anti-drone systems to motion- detecting smart flooring, the future technology we're accustomed to seeing in action movies isn't that far off from the reality of today's top-tier security and privacy solutions for huge bespoke superyachts, so lets dive into some of it;

CITADEL

In the rare event that an unwelcome guest boards the yacht, some owners take comfort in knowing there's a secure place to retreat to. These safe areas, known as 'citadels,' were first used in commercial shipping before being adapted for yachting. A citadel offers independent, secure access to the yacht's navigation and satellite communication systems, allowing full control even from afar. These rooms are fortified with reinforced doors and walls capable of ballistic protection. They are equipped with their own ventilation, as well as water and food supplies, making them completely autonomous for at least 72 hours.

A citadel acts as a naval panic room, offering a safe haven in case of personal danger. While most owners



might not be on board as the yacht passes through high risk waters, citadels primarily serve to protect the crew.

In situations where a citadel is not pre-installed, finding a defensible location on board to improvise as a safe haven is crucial. This temporary solution must be secure enough to protect several people on board until the threat is neutralized. In many cases, pirates unable to gain control of a yacht or rob the crew might resort to arson as a last-ditch effort. Therefore, it's clear that while such measures can delay criminals, they are ultimately just a temporary reprieve while awaiting assistance.



How to Build One?

Creating a citadel on a superyacht is akin to establishing a panic room in a residence. Numerous companies in the market specialize in constructing citadel rooms for superyachts. We encourage you to contact us for a comprehensive evaluation of all available builders. We aim to provide the optimal solution, saving you from unnecessary expenses. In collaboration with your yacht broker, we strive to implement all possible security measures, including citadels, before construction begins, ensuring a comprehensive approach to onboard security.

Our security consulting service transcends standard brokerage and commission-based cooperation. We prioritize your needs, recommending security measures that suit your specific requirements, not influenced by any commission-based partnerships with manufacturers. Should we have partnerships, we leverage these relationships to negotiate lower prices on your behalf, always working within your budget to apply the most effective tactics.

Anti-Piracy

In the early stages of addressing piracy, our CEO was instrumental in establishing a maritime security company in Djibouti. Operating with minimal resources, sometimes only a two or three-person team armed with a single rifle, they faced logistical challenges due to the high demand for protection across numerous vessels.
Their creative solutions included spreading broken glass on decks, tying fire hoses to railings, placing rubber dolls in military uniforms aboard, installing razor wire, preparing Molotov cocktails, and having flare guns ready on the bridge.



These improvisations were designed to delay pirate boardings and deter attacks by presenting the illusion of a more formidable defense.
Such improvisations are generally not suitable for superyachts, particularly those that are chartered. Despite these limitations, the essence of our approach—creativity and making do with available resources—remained effective in ensuring the safety of ships and their crews. However, technology alone cannot mitigate all high-seas threats, such as piracy.



Sometimes, powerfully zig-zagging the yacht to create a wave to knock the smaller boat off balance and trailed ropes in the water to snag in the pirates' propellers is more efficient than hi-tech gadgets. Therefore, although piracy has declined, areas like the Red Sea, Gulf of Aden, the Strait of Malacca, and even the Caribbean remain high-risk. In such zones, the presence of an armed security force on board is crucial.



Superyachts, often designed for luxury rather than security, present unique challenges. Features like large swim decks and non-bulletproof glass make them vulnerable. Moreover, the speed discrepancy between superyachts and pirate skiffs—where superyachts might travel at 17 mph against skiffs moving at 35 to 40 knots—further complicates security.

Effective yacht security necessitates not only James Bond's technology but combines high-tech solutions with the expertise of specialists capable of improvisation and drawing from real-life experience to ensure safety.



Superyachts in High-Risk Waters

In a world where warmer weather is often preferred, the yachting scene shifts to warmer climates during the winter months. Popular winter charter destinations include Middle Eastern countries like Bahrain, Oman, Dubai, and Abu Dhabi, especially for the renowned F1 Race. Additionally, destinations within the Indian Ocean region, such as Madagascar, Mauritius, Seychelles, and the Maldives, are highly sought after. Despite the presence of Naval Forces in the Red Sea and Indian Ocean, the threat from Somali pirates remains a concern and now the concern of Houthis. The term 'pirates' might conjure images of galleons and treasure, yet for commercial sailors and superyacht owners, piracy represents a significant threat.

The shipping industry continues to combat piracy, with The International Chamber of Commerce International Maritime Bureau's Piracy Reporting Center reporting that in the first quarter of 2019, 27 vessels were boarded, seven were fired upon, and there were four attempted attacks. Currently, areas like parts of the Philippines, the Gulf of Aden, and the coast of West Africa are considered 'red-alert' areas for pirate activity, while some parts of the Caribbean are deemed 'Amber', indicating a need for caution. The conflict in Yemen, tensions near the Iranian coast, and the activities of the Al-Shabaab terrorist group in East Africa have heightened risks for tourists and instilled a profound sense of uncertainty in these regions. These circumstances also affect nearby cruising destinations such as Northern Madagascar, the Seychelles, and even Mozambique, highlighting the potential dangers of sailing in these areas.

Although some Caribbean areas are safe, others have become notorious for pirate attacks on passing vessels. The southern and eastern regions of the Mediterranean have also become increasingly perilous due to conflicts in Libya and Syria, and the use of waters around Sicily and Gibraltar by human traffickers. Potential yachting hotspots have quieted down due to fears of robbery or harm from piracy.

The International Maritime Bureau (IMB) reported a concerning rise in maritime piracy incidents in 2023, with 120 incidents of piracy and armed robbery against ships recorded compared to 115 in 2022. The report highlights that 105 vessels were boarded, nine attempted attacks, four vessels hijacked, and two fired upon. The number of crew taken hostage and kidnapped significantly increased, emphasizing the escalating threats in maritime security. The report also documented the first successful hijacking off the coast of Somalia since 2017, marking a concerning resurgence in piracy activities in the region.

Additionally, the Gulf of Guinea remains a significant hotbed for piracy, accounting for the majority of hijackings, crew kidnappings, and reported crew hostages in 2023. Despite a slight increase in reported incidents compared to the previous year, the IMB urges for continued caution and robust regional and international naval presence to address these crimes.

In South America, incidents at Callao anchorage in Peru and other ports in Brazil, Colombia, and the surrounding regions highlight the widespread nature of piracy, affecting various parts of the globe beyond the traditionally recognized high-risk areas. The IMB stresses the importance of immediate reporting to improve the accuracy of risk assessments in these unstable maritime regions. The rise in piracy incidents is not confined to traditional hotspots like the Gulf of Guinea but has also been observed in the Singapore Strait, the Malacca Straits, and the Indonesian archipelago, indicating a global concern for maritime security. The shipping industry and international bodies are urged to continue their efforts in combating piracy, emphasizing the need for comprehensive strategies and cooperation to ensure the safety of seafarers and maritime assets across the world.

Since it is responsible for facilitating the transit of commodities across the oceans of the world, the shipping sector continues to be an essential component of international trade. However, maritime security continues to be a serious concern, particularly in light of piracy and other hazards that are associated with marine environments. The purpose of this research is to investigate the present condition of marine anti-piracy measures, the increasing issues in maritime security, and especially to investigate the impact that the Houthi attacks have had on shipping in the Red Sea.

The Global Anti-Piracy Effort

Through its Piracy Reporting Centre, the International Chamber of Commerce's International Maritime Bureau (ICC-IMB) is able to play a significant part in the battle against piracy on a global scale. Seafarers have access to a service that is available around the clock—the centre offers notifications on occurrences involving armed robbery and attacks by pirates. The International Criminal Court and International Maritime Bureau says that there has been a fluctuating pattern of pirate operations throughout the years, with certain locations having a greater number of occurrences than others.

Known hotspots for piracy

Notable high-risk areas for piracy include the Gulf of Aden, some portions of the Philippines, and the coast of West Africa. These regions are all located in the Atlantic Ocean.

In particular, the Gulf of Aden has been a flashpoint due to the strategic value it has as a maritime route and the instability that exists in the surrounding region, particularly in Yemen. In addition, there has been a notable increase in the number of instances of piracy along the coast of West Africa. These episodes sometimes involve violent assaults on ships and the kidnapping of crew members for ransom.

There are regions in the Caribbean where piracy and armed robbery at sea pose a danger to maritime security, despite the fact that the Caribbean are generally safe. In a similar vein, the southern and eastern Mediterranean regions are confronted with difficulties as a result of the ongoing crises in Libya and Syria, as well as the operations of people traffickers in the waters surrounding Sicily and Gibraltar.

The Houthi Attacks in the Red Sea

An increase in the number of security risks has been seen in the Red Sea, which is an essential maritime corridor for international trade. This is especially true in light of the attacks carried out by the Houthi rebels. The Houthi movement, which is participating in the conflict in Yemen, has targeted commercial shipping boats, which poses a huge concern to the marine security in the region. Not only do these assaults have the potential to endanger the crew, but they also have the potential to disrupt the global supply chain, which highlights the necessity of enhancing marine security measures.

Response and Countermeasures

International coalitions and naval troops have been sent to monitor high-risk zones as a reaction to the threats that have been coming from these directions. Operations such as the Combined Maritime Forces (CMF) and the European Union Naval Force (EU NAVFOR) Operation Atalanta have been extremely important in preventing acts of piracy and maintaining the safety of maritime routes. As part of these measures, commerce vessels are being escorted, monitoring is being carried out, and direct action is being taken against pirate gangs.

In addition, maritime corporations have implemented Best Management Practices (BMP) in order to defend themselves against piracy. These BMPs include measures like as travelling at faster speeds, employing armed guards, and utilising secure communication channels in order to report and receive warnings on pirate concerns.

Challenges and Prospective Courses of Action

Even with all of these efforts, there are still obstacles. It is impossible to entirely eradicate piracy and marine threats due to the flexibility of pirate organisations, the breadth of maritime areas that require patrols, and the political instability that exists in crucial places. The complicated nature of marine security in conflict-prone regions is shown by the current situation in the Red Sea, which has been made worse by the attacks carried out by the Houthis. This circumstance highlights the necessity of adopting a multi-pronged approach that includes political, military, and diplomatic measures.

As we look to the future, it will be essential to improve legislative frameworks and enhance international coordination in order to combat piracy and ensure marine security. When it comes to addressing the underlying reasons of piracy, this includes providing support for regional projects, enhancing the sharing of intelligence across governments, and encouraging economic growth in regions that are prone to piracy

Final Thoughts

In order to ensure the future success of the global shipping sector, maritime security continues to be an important concern, which calls for sustained attention and collaboration among international players. The current scenario in the Red Sea, along with pirate hotspots located all over the world, exemplifies the multifaceted and ever-changing character of maritime dangers. It is possible for the international community to achieve great progress in preserving the safety of marine routes and protecting global trade if they combine military, legal, and developmental tactics.

As a result of the sector's reaction to maritime threats and piracy, the industry has demonstrated the resilience and adaptation that is necessary to handle the hurdles that modern-day piracy presents.

Nonetheless, since dangers continue to develop, the techniques that are used to counteract them must also adapt. This highlights the need of taking a proactive and collaborative approach to maritime security practices.

How to Pirate-Proof Your Superyacht?

These events are concerning, but they should not be allowed to ruin your yacht's ability to travel freely, that is why we are here to help. There's nothing like having a team of ex-Royal Marine Commandos aboard, armed and mounting a 24-hour guard when your superyacht is in dangerous waters. Xtreme Security is a specialist SuperYacht security provider that takes pride in delivering anti-piracy services and has been doing so since 2011.

Xtreme Security has expert personnel, mainly with previous military experience, that carry out periodic training and theoretical, technical, and tactical phases, combining and perfectly integrating the experience of theresources used with the technologies used. This is what keeps our security personnel so sharp.

Our manpower is core to our business. We only employ individuals with an extensive Maritime background, who have experience in providing anti-piracy service onboard Super Yachts, in an effort to provide the best possible service. Our team is capable of ultimately mitigating the risk involved in traversing high-risk areas such as the Arabian Sea, Gulf of Aden, and the Red Sea.

To ensure your safe passage through the critical area of the Gulf of Aden and the Red Sea, we can provide you with an armed escort with ex-Royal Marine Commando operatives and the best possible equipment.





Our comprehensive superyacht security services are tailored to consider all aspects of security, factoring in the unique requirements of each yacht we protect. Our approach involves designing specific security protocols and assigning professionals to vessels based on their routes, size, event participation, and type. While our expert personnel are adept at implementing anti-piracy measures, we have also partnered with a leading marine security company to enhance our security standards for superyachts navigating through high-risk waters.

All firearms and controlled goods are owned by our affiliated company, specializing in maritime security services, and are licensed by the UK Government under an Open General Trade Control License (OGTCL) issued by the Department for International Trade. This authorization allows us to transport controlled goods (weapons and security equipment) across different jurisdictions legally.

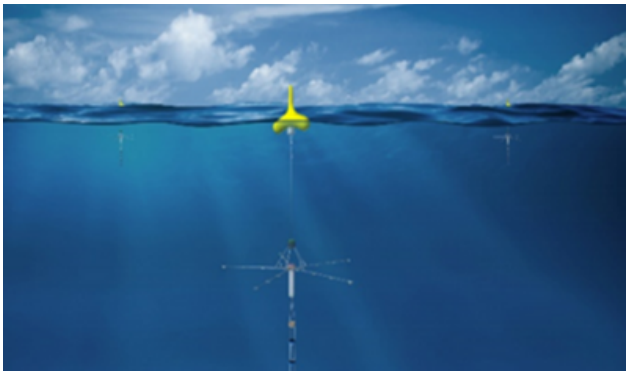
Furthermore, our sister company complies with BIMCO GUARDCON standards, ensuring the implementation of proper safeguards and the acquisition of appropriate licensing.

Shipping vessels are a valuable target for pirates, but they are also large and generally well-guarded targets, making them more difficult to board and rob. On the other hand, yachts, cruise ships, and other personal vessels aresmaller and easier targets for pirates. With the rate of piracy kidnappings and hostage situations having risen in recent years, security is becoming a necessity during sea travel for all vessels in international or dangerous waters.

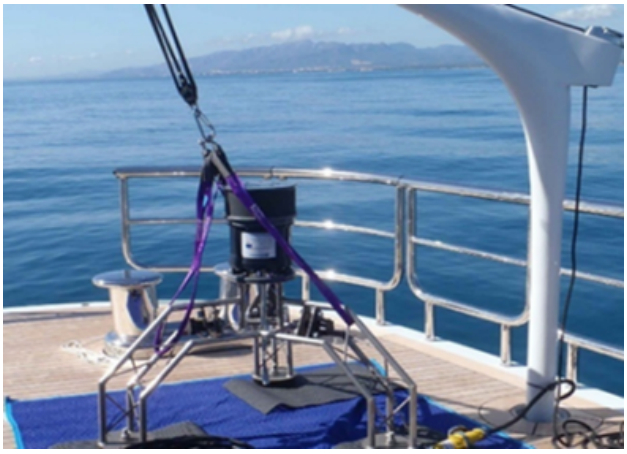
For more information about our equipment and our prices for anti- piracy services in high-risk waters, you can look here;
https://xtremesecurity.eu/anti-piracy-services/

Diver Detectors for Intruders

Could someone stealthily approach your superyacht using a wetsuit and dive gear? Consider this;



Some superyachts are already equipped with sonar systems capable of detecting, tracking, and identifying divers or submersibles from any direction.



Intruder Detection Sonars are widely used by naval vessels, commercial ports, and luxury yachts. These systems can detect divers within a range of up to 1000 meters, are portable, and can even be mounted on a yacht's tenders to extend situational awareness.



For information on the sonar systems available on the market, please feel free to contact us.
info@xtremesecurity.eu

Hospitals Onboard Superyachts



On-Call Doctor

Because yacht owners are essentially secluded in their foreign settings, onboard medical protection is a vital requirement. Or perhaps the Owners are older and have certain ailments that necessitate the reassurance of an on-site doctor or nurse.

In any case, an onboard hospital is a common feature requested by bespoke superyacht owners.

These facilities are equipped similarly to an emergency department in a private hospital, complete with oxygen tanks, defibrillators, specialist medications, and intravenous fluids. Additionally, many vessels include rehabilitation equipment for injuries, such as decompression chambers for extensive scuba diving expeditions.

Should a patient need more specialized medical attention, most modern luxury yachts are equipped with a helipad, facilitating medical air services directly to the vessel or enabling helicopter evacuation to a larger hospital on land.

Furthermore, many yachts come with advanced monitoring systems, allowing medical professionals to monitor vital signs remotely, even from thousands of miles away. Recall the scene in "Casino Royale" where James Bond uses a remote medical

diagnostic system while doctors assist him through his medical emergency with all his vitals displayed on their screens? This technology is more reality than fiction.

With the right diagnostic equipment on board, crew members or health professionals can connect to a remote medical support line. This enables a team of doctors to assess the patient's condition in real time and provide guidance on treatment or medication to stabilize the patient.

Keep this in mind when formulating a security strategy for your superyacht. If you require further details on integrating medical facilities and services into your yacht's design, please do not hesitate to contact us.



Superyacht Al Salamah Hospital Room with Underwater Treadmill for Physical Therapy

We can connect you with a select group of helicopter and medical equipment manufacturers. Contact Us.

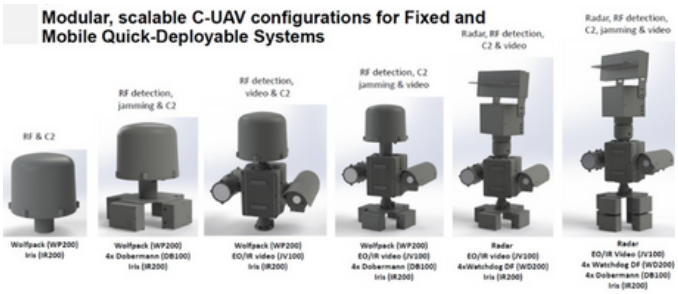


ANTI DRONE SERVICES

Originally, drones were utilized for missions considered too "dull, dirty, or dangerous" for humans. While primarily used for military applications, their usage has rapidly expanded to commercial, scientific, recreational, agricultural, and numerous other applications. This includes product deliveries, photography, video production (films, TV, documentaries), and building inspections, and infrastructure assessments (pipelines, cell towers, railroads, waterways).
However, they are increasingly being used for criminal activities such as drug smuggling, weapon smuggling, espionage, and terrorist attacks. Some drones can even intercept Wi-Fi signals and hack into important data.

In an era where drones have soared in popularity due to their versatile capabilities, it's undeniable that they present both benefits and challenges, especially to the serene and exclusive atmosphere of yachts.

This was demonstrated by the case of seven guests aboard a superyacht moored in Portocolom, Mallorca, in June 2017 who were filmed by a drone as they sunbathed naked on the deck of their yacht.



The paparazzi are a constant worry for celebrities.
It used to be fine to slip off a bathing suit to enjoy some full sun when you are anchored far from the beach, but now there's the worry of a camera being in the sky.
A yacht represents an elegant space for leisure and business, prized for its seclusion. As symbols of leisure and luxury—and occasionally as business retreats—yachts offer an escape with a promise of privacy and security away from public eyes.

THE BEST ANTI DRONE SOLUTION ON THE MARKET



However, the advent of drone technology, particularly in photography and videography, has introduced new concerns over privacy breaches and unauthorized surveillance, unsettling the once unquestionable tranquility of yacht goers. This underscores the critical need for comprehensive yacht security measures, including surveillance systems, access control, trained security personnel, and the increasingly essential anti-drone technology.

In addition to violating a yacht owner's personal privacy, there also is the possibility that drones could be used by criminals to gain a bird's eye view of a vessel and highlight its vulnerabilities.

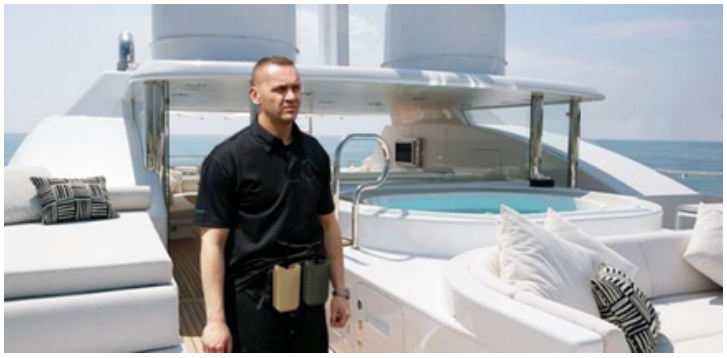


Mechanisms Against UAV (Unmanned Aerial Vehicle) – Drone

An anti-drone system serves as a technological fortress designed to detect, track, and neutralize unauthorized drones that could compromise privacy or safety. Utilizing a combination of radar, radio frequency (RF) detection, and jamming techniques, anti-drone systems stand at the forefront against intrusive drones, safeguarding sensitive locations like yachts, events, and critical infrastructure. By integrating radar, RF sensors, and optical sensors, these systems excel in identifying unauthorized drones by their signals, movements, speeds, or even the location of their operators, ensuring any potential threats are swiftly mitigated.

We are able to provide you anti-UAV devices to monitor all dimensions of an event space, on the ground or on the yacht. Our Anti-UAV System offers temporary installments for special events, – or as a permanent solution.
Keep Reading to find out more;

Commercial drones operate in frequency bands 433MHz, 915MHz, 1.2GHz, 2.4GHz, 5.2GHz, and 5.8GHz. We can detect all these bands and alert the security guard, captain, and ship security officer of an approaching drone from up to 3-5 km away. With the detector connected to the jammer, the jammer will create a fence up to 1km away, ensuring the drone cannot come too close.



The MyDefence jammer employs a jamming algorithm that counters frequency-hopping drones. This means if a drone detects frequency noise from the jammer or another source of environmental interference, such as 2.4GHz, it will switch frequency to 5.8GHz and continue flying, while our jammer's algorithm counters that and jams the drone regardless. With a conventional jammer, the drone would sense the interference and switch frequency bands, rendering the jammer ineffective. Another advantage of the MyDefence jammers we use is their 60-degree coverage, eliminating the need for the operator to visually locate or aim at the drone.



A small drone 100m to 200m away is difficult to detect and target with a typical jamming rifle, making these jammers significantly more effective.

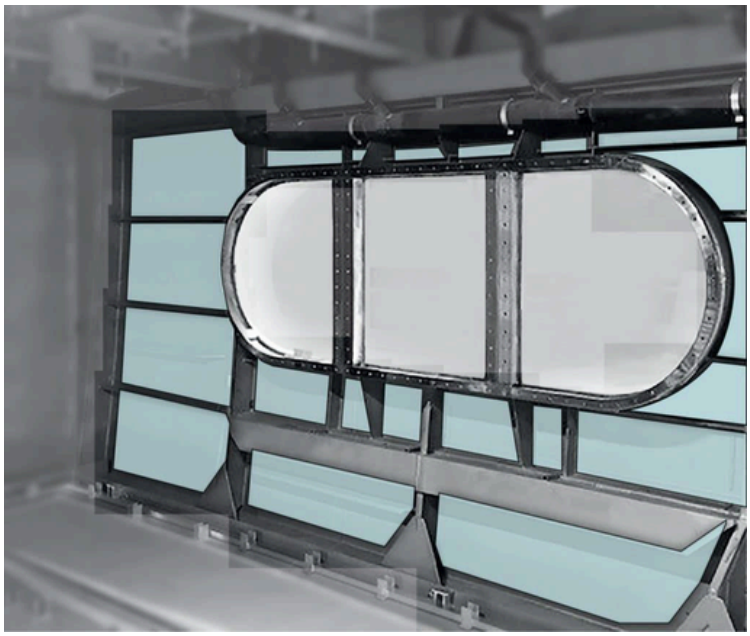
Anti-Drone Equipment is Legal or not?

In the US, individuals purchasing drone technology must register their drones with the US Federal government to obtain a legal flying license. The drone itself is merely a cargo vehicle capable of carrying technology and even weapons. In most EU countries, drones of up to 5kg capacity are allowed for use without any restrictions. However, "Drone law" is not yet a formally established concept. The attitude of "If I am going 90 miles an hour in a 55-mile-an-hour zone, if I don't get caught, who cares?" applies similarly to adherence to current FAA policy and other regulations. Currently, no one is getting caught, and no one is issuing tickets.

The most compelling argument for the use of anti-drone technology is the realization that terrorists have access to off-the-shelf drone technology, which is available for just a few hundred dollars with a few clicks online. However, traditional defense mechanisms against UAVs, such as shooting them down, are not viable within the U.S. and EU under current regulations. "You cannot shoot down a drone as it is considered an aircraft," stated Mark Dombroff at a recent drone conference, the International Drone Expo in Los Angeles, California. He may be correct, but this has not deterred some individuals from destroying invasive drones that have violated their privacy.

The use and acquisition of jammers are prohibited for private individuals not only in the US but also in some other countries within the EU. Similarly, only government agencies currently have the authority to use such anti-drone devices without repercussions. "The most effective counter-drone technology to detect and then neutralize a threat is essentially to take over the communication between the drone and the ground controller to command it to do something else, and we're not permitted to do that because it's akin to hacking into someone else's computer. ***To be frank, the most effective technologies are the ones that are illegal," said Anh Duong, UAS program executive officer with the DHS Science and Technology directorate.***

However, some anti-drone gadgets can be utilized in the consumer sector if the appropriate legislation is met, and we are here to help you with that. Contact Us! *mydefence@xtremesecurity.eu*



Windows as Tough as Steel

The ingenious minds at A60 have taken the concept of reinforced safety glass to new levels. Our partner compound glass windows, crafted from hot extruded steel or stainless-steel profiles, offer up to an hour of fire resistance. They come in various thicknesses while maintaining low optical distortion and high light transmission.
These windows can undergo thermal or chemical hardening, lamination, thermal isolation, and can be made soundproof or bulletproof.
The glass is set in a frame using a specialized U-profile method, enhancing flexibility and minimizing environmental rusting risks over time. For protecting what lies behind a yacht's windows, A60 windows are the preferred choice.
For privacy and security, tinted windows are a sensible option. If windows are not tinted, ensure your crew patrols the yacht in the evenings to close all curtains. For more serious threats, options include metal weatherproof plating over windows or ballistic Kevlar curtains, for which we can also provide assistance.

TO SUMARIZE, DEFEND TACTICS YOU CAN USE ARE;

- Armed Security Team: Necessary for particularly hazardous routes, though this option has its complexities.
- Long Range Acoustic Device (LRAD): A non-lethal method to deter attackers with overwhelming noise. However, effectiveness may vary against pirates accustomed to loud engine noises. Comprehensive coverage is essential for efficacy.
- Laser Threat Deterrent System: Can dazzle attackers, effectively blinding them from seeing the yacht.
- Infrared Imaging: Enhances night visibility, allowing crew and security to detect approaching threats more effectively than standard infrared cameras.
- Bullet-Proof and Tinted Windows: Essential for both privacy and security.
- Metal Weather Plating and Ballistic Protection: Such as Kevlar curtains for additional security measures.
- Deployable Submersibles: Serve as escape pods if evacuation becomes necessary.
- High-Resolution CCTV Cameras and Motion Detectors: Independent of yacht's Wi-Fi, utilizing LTE and solar power.
- Satellite and Infrared Imagery, and Sonobuoys: For comprehensive surveillance, detecting underwater threats like swimmers or divers.
- MMWC Propeller Arresters: Long lines deployed to entangle assailants' prop shafts.
- Fog/Smoke Cloaking System: The GOST Cloak releases a glycol mist, creating a dense smoke that disorients intruders.
- Remote GPS Tracking: Allows for remote yacht tracking using a Google Earth interface.
- Immobilizers: Effective in safeguarding tenders and toys from theft.
  Motion Detector floors, etc.

These strategies and technologies provide a robust framework for superyacht security, ensuring safety and peace of mind in high-risk waters. We have a privilage to explore all the solution available on the market, when we built the security plan for one yacht owner.

Cyber Security on a Superyacht

Superyachts are vulnerable to two major cybersecurity threats.

The first involves data theft, encompassing the unauthorized access and theft of funds, images, and other sensitive information.

The second vulnerability lies in the potential hacking of the yacht's control systems, including its navigational apparatus.



Consider Captain Jack Sparrow, but with a laptop.

Consider yourself on a superyacht, traveling beautiful tropical oceans among islands of swaying palms and dazzling white sandy beaches. As you relax on a sun-drenched veranda, chilled by the ocean wind, an attentive waiter waits by with exotic beverages. You suddenly notice a shift in the crew's demeanor. They begin to move quickly and nervously.

What's going on?

The boat seemed to be moving quickly.

That island it was going for is no longer visible.

The news travels quickly across the ship: the computer systems have been compromised, and someone is operating the boat remotely. It is being directed at full speed towards a dangerous reef, where it will be destroyed very soon if a ransom is not paid.

Doesn't that seem like something out of a late-night movie channel? It's not. It's the world's wealthiest boat owners' worst nightmare.

Cyber-hijacking is a very serious issue that has sent shivers down the spines of ultra-luxe superyacht owners. With the awareness that technology has opened up an entirely new chance for piracy, nagging concerns about security have rapidly become full-fledged anxiety as super- and mega yacht ownership develops at a rapid rate.

Despite the increasing incidents of cyber hijacking targeting superyachts, these crimes are seldom reported.



Extortion: The Most Critical Concern

In the contemporary maritime world, superyachts are often managed by a single central system that controls navigation, engine management, entertainment systems, lighting, air conditioning, and, notably, allows remote operation from iPads and other devices. This convenience, however, leaves the vessel vulnerable to a wide range of cyber security threats, both internal and external, extending even to personal devices connected to the system.

In today's digital age, there's a universal push for easy and fully automated access to digital information, with a significant portion of data being stored on the cloud for easy access. Consider your personal email account, which, in a single day, connects to a multitude of platforms such as social networks, cryptocurrency wallets, and banking services. The extensive information linked to your email alone underscores the potential for catastrophic online privacy breaches.

The yachting industry has historically been marked by minimal security standards. It wasn't until just recently that a basic safety standard was introduced, and it remains in a trial phase.

Shockingly, the **International Maritime Organization (IMO)** only recently implemented basic standards for superyachts exceeding 500 gross tons (GT), leaving many older vessels with outdated infrastructures facing significant investment challenges to comply.
However, the greatest obstacle lies in altering the ingrained habits and culture onboard, often summarized by the adage, **"If it's working, don't touch it."**



In 2017, Mark Oakton, a Security Director at Infosec Partners, conducted research at the Monaco Yacht Show to assess the vulnerability of superyachts at port. The findings were alarming: out of over 600 WiFi connections identified from superyachts, only 17 were secured and hidden, leaving the majority susceptible to unauthorized access.

Further illustrating the risk, Campbell Murray, a cybercrime specialist from BlackBerry, demonstrated how easily financial data, personal images, and vessel navigation could be compromised. Within an hour of opening his laptop, Murray had gained complete control of a neighboring multimillion-dollar superyacht, including its satellite communications, telephone system, WIFI, and navigation systems. He could erase any evidence of his actions, highlighting the significant vulnerability posed by high-power WIFI routers which extend the network far beyond the ship, potentially to other vessels and the shore.

Simpler vulnerabilities also exist. For instance, if a crew member shares the ship's location on social media, it invites extortionists to exploit this information. Streaming on the ship's WiFi can inadvertently reveal the ship's internet presence to anyone watching the video who knows how to find it. This risk has led many superyacht owners to prohibit their crew from using platforms like Facebook or Instagram.

Addressing these vulnerabilities requires stringent crew vetting and background checks, highlighting the importance of cybersecurity measures as an integral component of modern yachting operations.

The Weakest Point: The Inside Threat

A colleague from another security firm recently conducted a sweep on a yacht purchased from a previous owner who had used it as a charter. During the inspection, they uncovered three hidden cameras. These devices were most likely installed by crew members or individuals with access to the owner's master suite or the yacht during a refit period. This raises a critical question: Who has access to your cabin?

Especially in the context of chartered yachts, it's essential to conduct thorough background checks on crew members. Our services include comprehensive reports that cover a crew member's character, general reputation, personal characteristics, lifestyle, and credit standing.

The information obtained may include social security number verifications, address history, credit reports, criminal records, public court records, driving records, accident history, workers' compensation claims, bankruptcy filings, educational and employment history verifications, personal and professional references check, professional licensing, and certification checks, as well as drug/alcohol testing results. These details can be sourced from government agencies, educational institutions, former employers, and through personal interviews with neighbors, friends, and associates.

If information related to a crew member's creditworthiness, credit standing, or credit capacity is obtained for reasons beyond legal requirements, it will be used to evaluate the potential risk of theft or dishonest behavior in their job role.

How well do you really know your crew?

Many yachts enforce policies to restrict the use of mobile phones, social media, and photography onboard. However, signing a non-disclosure agreement (NDA) does not guarantee adherence to these rules.

"If I were targeting a superyacht, I'd start by profiling the crew to identify the weakest links for a successful attack. I would craft a tailored malicious email based on their profiles, confident in its success. The aim would be to steal photos, financial data, money, corporate secrets, or other sensitive information." - says one expert,

Even listing their work position on LinkedIn could place you at risk. With tools like a "rocket search engine," it's possible to find someone's email and their real-time location if they're active on social media. Following their interests on social media and sending malware-infected emails can lead to easy hacking.

For instance, a yacht undergoing refueling was targeted after someone surveilled the captain. They send a fraudulent invoice for the refueling via email, which, once opened by the captain, granted them access to the yacht's systems.

The majority of cyber attacks initiate from phishing emails, personalized to pique the interest of the recipient and trick them into clicking a link or opening an attachment. A simple preventive measure is to require crew members to deactivate all their social media profiles.

The risk of maritime cybercrime is not hypothetical. Hackers have previously infiltrated a billionaire's bank account, extracting over £100,000.

Several ships have been coerced into paying ransoms to regain control of their navigation systems after threats of releasing embarrassing photographs

Yachts as Vulnerable Tracking Devices

Yachts have become highly susceptible tracking devices. Given their use by High Profile Individuals, including perhaps yourself, as remote offices, they are prime targets for those seeking financial gain through extortion, theft, and other malicious means. We will refrain from detailing the methods by which yachts can be located and hacked; however, further explanation is available in this video:

https://youtu.be/hSFz2diUTvE

Until recently, it was also possible to follow a yacht in real-life on one website, which is currently shut down. However, I believe that there are some others that are not currently known to the public. By googling the biggest yachts in the world, you will quickly find out who owns them, and I think that says it all.

Until recently, it was also possible to follow a yacht in real-life on one website, which is currently shut down. However, I believe that there are some others that are not currently known to the public. By googling the biggest yachts in the world, you will quickly find out who owns them, and I think that says it all.

https://www.pentestpartners.com/security-blog/tracking-hacking-ships-with-shodan-ais/

Any superyacht may be exposed to cyber dangers, just as any house or workplace, and will likely opt to secure itself from intruders collecting private and sensitive data. With remotely operated devices onboard, yachts that do not provide an additional layer of technical protection may leave themselves vulnerable to hackers.

What Should You Do?

- **Threat Assessment:** Understand the potential risks and motives of attackers.
- **Cyber Sanitization - Sweeping:** Regularly check for vulnerabilities and unauthorized devices.
- **Segmentation:** Carefully vet everything and everyone, including guest lists.

A well-defended system can significantly mitigate the impact of an attack. Restricting workstation rights onboard ensures that ransomware impacts only the infected system rather than the entire yacht. Consistent, strong backups are crucial for recovery from ransomware attacks, minimizing data loss and system downtime. A robust software-patching routine and strong antivirus software, coupled with diligent email practices, can prevent many attacks.

Threat Assessment:

Consider the motive and potential attackers. Evaluate whether the yacht is used personally or chartered, as each scenario presents different vulnerabilities.

Sweeping - TSCM:

If chartering your yacht, conduct thorough sweeps after each charter to detect and remove unauthorized devices.

Maintain discretion and secrecy across all levels, from family members to yacht management and crew. Limit information sharing to essential personnel only, ensuring all involved understand the importance of this discretion.

A Cautionary Tale:

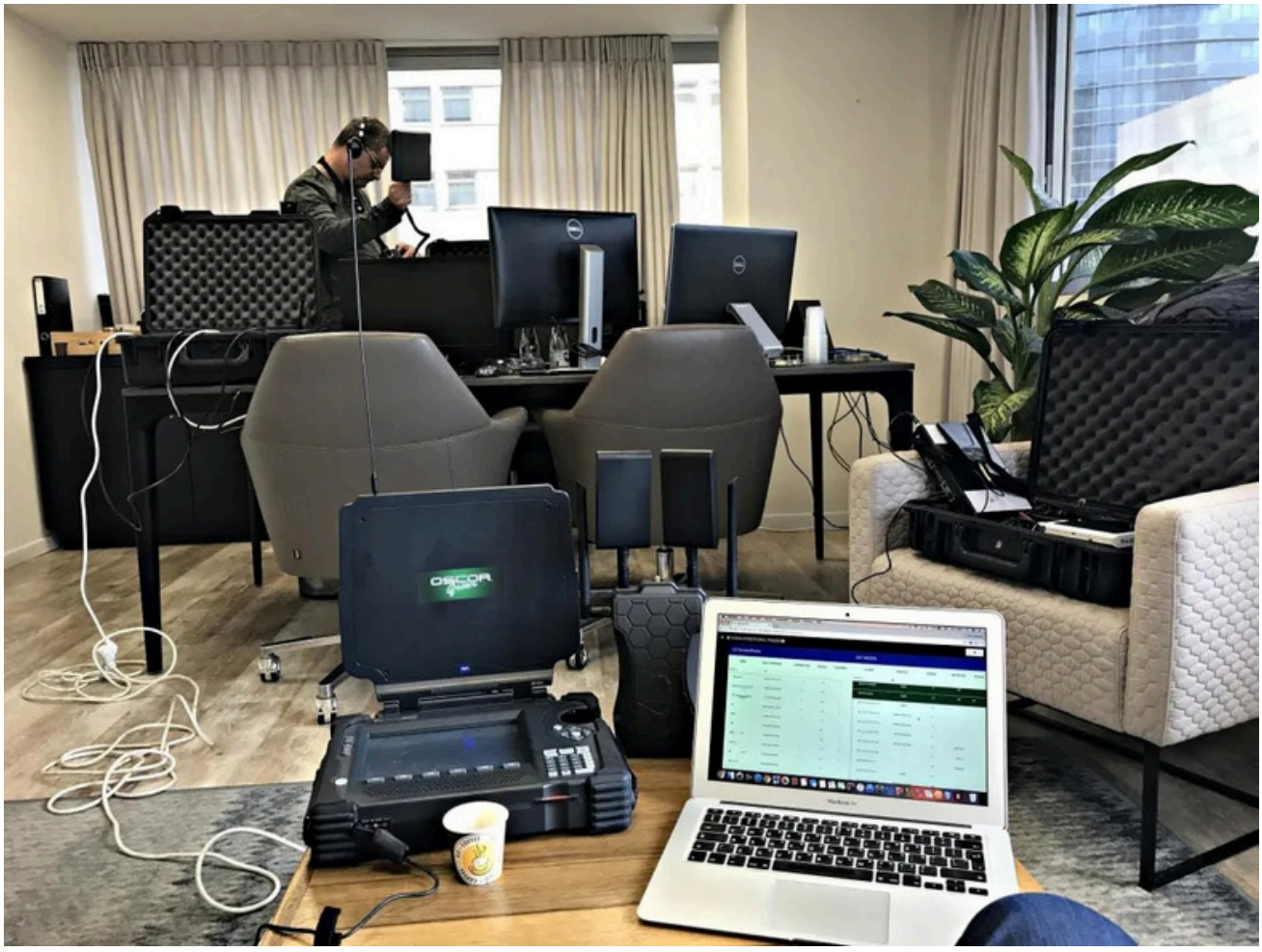
Consider the experience of Bob Denison, president and founder of Denison Yachting, who announced on 10 February 2020, that his business had been the victim of a cyber-attack. His story, shared here:

https://www.superyachtnews.com/technology/bob-denison-on-the-recent-cyber-attack

Which serves as a stark reminder of the vulnerabilities facing the yachting industry.

HAVING SO MANY PEOPLE INVOLVED LEADS TO SO MANY BACK DOORS. YOU NEED KEEP CLOSED ALL THE DOORS!

For those involved in the yachting industry, whether owners or charterers, the risk of cybercrime is significant. With numerous individuals involved in the operation and maintenance of a yacht, the potential for security breaches increases. It's essential to implement stringent security measures and conduct regular checks to safeguard against cyber threats.



For more information on our TSCM services, contact us;
info@xtremesecurity.eu



Recovery Is Harder Than Prevention

To effectively combat cybercrime, our focus must be on three critical areas: technology, governance, and people. Technology includes tools such as firewalls, encryption, and secure passwords, often considered the more straightforward aspects of cybersecurity. However, governance and personnel are arguably more significant to the security process.

Governance encompasses the regulations and practices concerning IT and social media use onboard, as well as the overall behavior of the workforce. In many yachts, existing protocols that prevent crews from using cell phones or social media and prohibit taking photos onboard prove beneficial for security.

People are the most crucial factor. Despite the sophistication of technology and governance systems, cyber attackers frequently exploit human vulnerabilities, often due to simple mistakes such as links. In 2015, around 90% of successful cyber-attacks involved an employee unknowingly compromising system security.

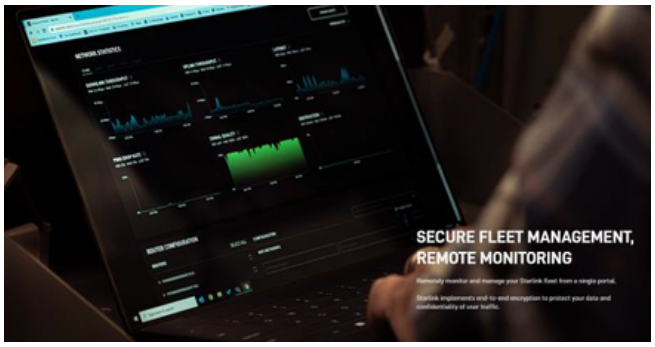
People are the most crucial factor. Despite the sophistication of technology and governance systems, cyber attackers frequently exploit human vulnerabilities, often due to simple mistakes such
links. In 2015, around 90% of successful cyber-attacks involved an employee unknowingly compromising system security.

Information is a powerful tool for hackers, who can profile crew members or owners based on personal details like names, hobbies, and social circles to tailor their attacks. Phishing emails, especially sophisticated ones, are designed to capture the recipient's interest, leading to the installation of malicious software. Once compromised, a device can serve as a gateway for attackers to access the yacht's IT network, seeking as much information as possible.

To mitigate these risks, some yacht owners have restricted the use of social media onboard. Additionally, employing professionals to conduct a comprehensive evaluation of the vessel's systems is a prudent investment compared to the overall expenditure on superyachts. For instance, a security sweep and ongoing monitoring services might cost around $20,000 – a relatively small price for enhanced security.

The necessity for robust Wi-Fi connections on superyachts, often required by high-profile and busy owners, can inadvertently extend the network's range, making it more susceptible to hacking.

As Security Consultants, we advise against using the yacht's Wi-Fi. Alternative satellite internet solutions can provide secure, isolated infrastructure, incorporating safe browsing practices, VPNs, encrypted emails, two-factor authentication, password management, and more. Such as STARLINK.



Specialized companies offer combined IT and Security Monitoring Services, including 24/7 network surveillance, cyber security training for the crew, bespoke intrusion alerts, and internet and dark web monitoring of client-related information.

Contact us and we will introduce you with some of them, pro bono.

According to IMO guidelines, the first step is to inventory all connected devices onboard. A popular solution we use is Inmarsat Fleet Secure, which offers crew training and Fleet Secure Endpoint security:

https://www.inmarsat.com/en/solutions-services/maritime/services/fleet-secure.html

The excellent news is that cyber protection does not necessitate a large investment.

"A little bit of awareness and proper practice enhances your (protection) level".

Fortunately, enhancing cyber protection doesn't require substantial investment. Awareness and adherence to best practices significantly improve security levels. However, all precautions become moot if someone bypasses the rules, such as using an infected USB drive or visiting a prohibited website.

It's essential to consider who has access to passwords, onboard and cloud files, and who manages these credentials, ensuring they are revoked when crew members leave.

These pragmatic steps enhance security without significant time or financial investment.

Have you implemented the simple yet crucial protocol of changing passwords when crew members or guests leave your yacht? This practice is a foundational element of maintaining a secure environment onboard.

Crew Vetting

- Prior to boarding, all crew members should complete cybersecurity training, which we can provide online.
- Additionally, consider hiring us for conducting crew background checks and Technical Surveillance Counter Measures (TSCM) services for your yacht

"Confidentiality clauses have long been a standard in crew contracts. Crew members must always remember the caliber of individuals they serve," said William MacLachlan, a senior associate at Holman Fenwick Willan law firm. "Owners are often high net worth individuals, possibly with significant public profiles, requiring utmost discretion to prevent accidental or intentional leaks of sensitive information."

Crew Compliance

The biggest danger to superyachts in terms of any attacks is crew complacency.

The weakest link is the crew

It is unreasonable to expect the captain or charterer to single-handedly monitor all potential threats. Given their extensive responsibilities, including navigating the ship, managing personnel, and ensuring guest satisfaction, they cannot maintain vigilance around the clock.

However, to safeguard both guests and crew, it's essential to provide training on conduct following capture. While the prospect of kidnapping and ransom may seem distant, this training also covers conflict resolution skills, preparing individuals for any violent situations, such as an armed robbery.

Crew members, and sometimes guests, especially in larger groups, should be educated on how to behave during a crisis. We emphasize the importance of familiarizing the crew with security procedures and protocols well in advance of the arrival of owners and guests. Our goal is to ensure that all security measures and responses are clearly understood and implemented effectively.

The greatest threat to superyacht security is crew complacency. The most vulnerable point is often the crew themselves. We encourage a security-conscious mindset among crew members, urging them to report anything unusual, even if it turns out to be a false alarm.

In a notable incident, the crew and passengers of a 41m charter superyacht, Legenda, successfully neutralized a threat, leading to the assailant's arrest by the police department of Southern Corsica. A judicial investigation into the incident is underway. More details can be found at Yacht Harbor News.

https://yachtharbour.com/news/41m-charter-superyacht-legenda-attacked-with-passengers-aboard-3385

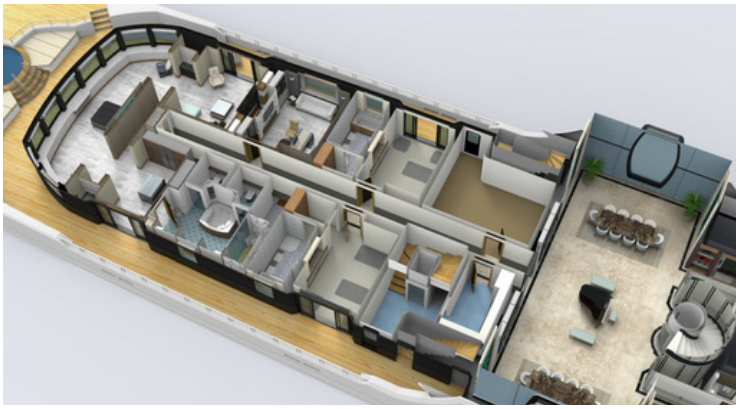


CAPTAIN OF LINDA LOU

"The most important thing we did was develop a plan, and then drill, drill, drill with the crew," says Schueler. "That helped us more than anything. We also deployed barbed wire on our swim platform, had flare guns to shoot flares into their boats, and had line launchers to shoot in front of the approaching skiffs to ensnare the propellers and disable their vessels.

While it may not be the prettiest solution, barbed wire is an effective one: It is rolled out across the beach-club deck and kept there the entire time the yacht remains in dangerous waters. Ideally, no guests are on board during such risky crossings, so no one is swimming. "

Yacht Risk Assessment



- Identify potential dangers.
- Determine who may be harmed onboard and how an event may occur.
- Document our findings and implement them.
- Regularly review and update the current assessment.
- Mitigate travel risks through national and regional assessments.

The cornerstone of excellent security practice is the development of a comprehensive set of security plans and procedures to ensure preparedness for any situation.

Our operatives will conduct a detailed survey of your superyacht to provide tailored security recommendations. A panic room or citadel will be designated, and the vessel will be evaluated to identify the most effective hardening measures. Security and safety strategies are bespoke; regular inspections are essential to ensure the vessel is fully operational and secure.

Country Risk Assessment

Our client-focused Travel Risk Mitigation solution delivers a thorough intelligence overview of the superyacht's environment, encompassing Worldwide Relations, Civil Unrest, Crime, Kidnapping, Political Violence, Environmental, Medical, and Maritime risks. These analyses provide Yacht Managers, Charter Managers, and Captains with a Geopolitical Threat Analysis for ports, marinas, countries, regions, or specific journey itineraries. This comprehensive review can be conducted just before charters commence or during the planning phase of a cruise to ensure the yacht, her crew, and her guests are well-informed of any potential dangers.

Our port and marina risk assessment offers yacht captains and yacht management teams the tools to evaluate operational risks for the vessel and all personnel onboard. When assessing risks in a specific port or marina, we apply expert judgment as a fundamental component of the scoring process, acknowledging that some subjectivity may influence the assessment.

Identifying risk management strategies is a crucial step, utilizing our hazard list and employing a "most probable" and "worst possible" scenario approach for consequence evaluation. Risk control strategies are identified and assessed once our hazard list has been created, reviewed, and rationalized. These strategies are then tailored to address the primary risks, which are highlighted at the top of the ranked hazard list.

A Crucial Aspect of Health and Safety Management on Boats and Superyachts

A risk assessment plays a vital role in health and safety management on any boat or superyacht. Its main objective is to identify necessary actions to comply with statutory duties and associated regulations, aiming to reduce the occurrence of incidents and accidents onboard. These competencies are crucial for conducting an "adequate and sufficient risk assessment" on your vessel.

Given the varying levels of risk in ports, land destinations, and open seas, it is imperative for captains, owners, and operators of yachts and superyachts to understand that previous risk assessments must be regularly reviewed and updated as necessary.

Creating a Proper Security Plan

While we hope for the best, preparing for emergency situations is essential. The ideal emergency plan includes preparedness for safety, security, and medical crises, with support available 24/7 for medical evacuations and extraction services. Our teams are ready to respond swiftly to any situation, thanks to regular drills and partnerships with diverse service providers equipped to assist in emergencies.

Executive Protection

To attain the maximum level of safety and security for yacht own, their family members, visitors, and last but not least, the crew, 24/7 security consultancy and physical security presence is required as well.

Obviously, as the owner of a yacht, you would prefer to spend time with your family or visitors on board at anchor in a quiet setting after a full day at work, without being intruded on by additional crew on board - your security staff.

Therefore, good social dynamics - soft skills are also required while having security guards on board.

In these scenarios, we offer a unique service within the superyacht security sector by implementing our "Executive Protection" strategies with operatives experienced in working with celebrities and corporate executives, who understand the importance of privacy.

We can also forego traditional onboard security personnel in favor of sea-based operators who patrol around on tender inflatable boats to protect the privacy of you, your family, or your guests onboard. This approach, utilizing the latest technological equipment as mentioned in this document (which we can lease from certain companies), ensures that unauthorized access by paparazzi and organized criminal groups to your protected anchorage is prevented, maintaining privacy both above and beneath the waterline.





Limo & Chauffeured Service

Yachting offers a unique and luxurious way to discover secluded spots, though it's not without its challenges. The opulence of yacht travel, regardless of size, is accompanied by potential complications, including ground transportation issues.

While docked in ports, our trained professionals are strategically placed at entrances and around the perimeter to safeguard against any unauthorized access, ensuring heightened security, especially during nighttime hours. Through our sister company XS Travel Management, we guarantee peace of mind for both your company and clients, ensuring a restful sleep.

Our team, with comprehensive travel access throughout Europe, is prepared to provide land transportation as needed. Our drivers are available to stay nearby the yacht while it is docked, offering passengers convenient and secure transportation options at any moment. Should your clients choose to explore a port city on foot, our trained personnel can escort them, guaranteeing their safety at every turn.

For more information, please visit our Travel Management website:
https://www.xs-travelmanagement.com/

Case Studies:

History of Previous Incidents, Robbery, Boarding, Kidnapping Incident Rehearsals

Our relevant experience, combined with day-to-day reports from our sources and the media, has revealed an appreciable increase in incidents of criminal and terrorist activities worldwide. In this context, a lax approach to handling such risks could cause significant damage to yacht owners' and operators' image and assets. This could lead to occasional incalculable, crisis-type effects on the continued existence of their high-value assets and could endanger all individuals on board a yacht. Although no superyacht has been hijacked to date, pirates have targeted similar vessels.



La Ponant:

The 88-meter Le Ponant, a small cruise liner, was seized in April 2008, and her crew of 30 was only released once a ransom of $2.15 million was paid. Superyachts, with their low freeboards and slow speeds relative to large tankers, present a temptingly soft target, suggesting it might only be a matter of time before one is taken, as there have already been some close encounters.

- RFI report on Somali Pirates' trial;
  https://www.rfi.fr/en/africa/20120522-sixsomali-pirates-trial-paris-over-capture-le ponant
- Vanity Fair's Real-Life Story from La Ponant Yacht;
  https://www.vanityfair.com/news/2009/04/somali-pirates200904

Ocean Swan, Shady Lady, Mi Marra:

- *https://www.yachtingmagazine.com/pirates - return/*

The 52-meter Alloy Yachts sloop Red Dragon

regularly transits through the Indian Ocean and in 2008 faced a real pirate threat.

"We saw the mother ship, a large dhow, approach to about four miles away, then it stopped and launched six fast boats that headed straight towards us," says skipper Ben Marshall. Fortunately, the yacht carried ex-Special Forces operatives from Ironsides Associates, deterring the pirates.

Luxury yacht Golden Eagle

managed to escape an attempted pirate attack at the end of January 2019 in the Caribbean Sea off the east coast of Nicaragua. Caribbean pirate attacks — including robberies on yachts — surged 160% in one year, highlighting the growing threat in regions previously considered safe.

Caribbean pirate attacks — including robberies on yachts — surge 160% in one year

https://www.marketwatch.com/story/caribbean-pirate-attacks-including-robberies-on-yachts-surge-160-in-one year-2018-05-24

55 metre Tiara

The 178-foot (55-meter) Tiara,
commissioned by Israeli millionaire
Jonathan Leitersdorf moored off Porto Vecchio, was boarded by four masked gunmen, who robbed the crew and charter guests of nearly $200,000 in cash and an undetermined amount in jewelry and artwork.

The 21 metre yacht was attacked by an 18 metre fishing vessel while transiting from
Colon in Panama, to Roatá n in Honduras.

- https://www.boatinternational.com/destinations/owners-warned-after-luxury-yacht-attacked-by-pirates-near-nicaragua--29365

More on attack from captain;

- https://www.dockwalk.com/news/tiara-captain-clears-air-on-pirate-attack

An **Italian boat attacked in Croatia**

highlights the unpredictability of threats even in European waters.

The 39-year-old local goes crazy and
threatens to kill Enrico. Then, he takes a mooring rope, he wraps it around the anchor chain and tries to trip the boat by towing it with his tender.
Enrico's wife invites him to go away and threatens to call the police while the girl is crying on board.
Enrico's boat dangerously gets close to another boat docked near there but, fortunately, a few minutes later the islander gives up and goes away.

- Yachting News on Italian Boat Attacked in Croatia;

https://www.yachtingnews.com/italian-boat-attacked-in-croatia/

Superyacht Antipodean

Pirates have raided and robbed media magnate Kerry Stokes' 35.9-metre Oceanfast superyacht Antipodean off the coast of Papua New Guinea targeted by three thieves armed with bush knives
The thieves are said to have approached Antipodean as she was anchored near Krangket Island, close to Madang, on Papua New Guinea's east coast. The thieves reached the yacht by row
boat and once on board took mobile phones, laptops, diving equipment, cash and watches. The thieves were confronted by crew who were on board.

- ABC News Report on Antipodean Robbery;

https://www.abc.net.au/news/2014-10- 07/pirates-rob-media-boss-kerry-stokes-yacht-in-png/5796654

Tourist Boat

New Caledonia: a tourist boat tackled by pirates armed with swords Pirates attacked a luxury yacht Monday afternoon, off the island of Ouvea, New Caledonia, armed with swords and rifles. They looted the ship and destroyed the electronic equipment.
The attackers fired shots in the air, in the windshield and fender of the boat, before boarding. "The skipper was taken apart, beaten and put on the ground with a rifle on the temple," also told the radio stationnn1st , Vincent Ventrella, operator of the boat.

- Teller Report on Tourist Boat Attacked by Pirates;

https://www.tellerreport.com/tech/2019- 06-27---new-caledonia--a-tourist-boat tackled-by-pirates-armed-with swords-.r1ZXLbgfeH.htm

Superyacht Legend

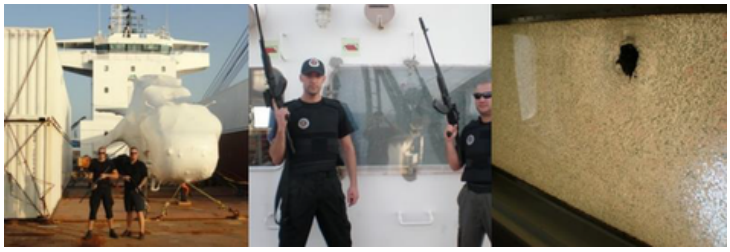
On July 30, around 07:30 in the morning, a 43-year-old resident of Corsica armed with a knife has entered a 41-metre superyacht Legend a, with charterers of Russian nationality aboard, reports Corse Net Infos.
The superyacht flying the flag of the Cayman Islands, was anchored less than 2 km from the the Port of Taverna, Corsica.
The crew and the passengers made
themselves safe disarming the individual,
who was arrested and taken to the police department of Southern Corsica. A judicial investigation of the accident has been initiated.

- Hello Monaco on Superyacht Legenda Attacked;

https://www.hellomonaco.com/news/lates t-news/41m-charter-superyacht legenda-attacked-with-passengers aboard-and-other-yacht-news/

Resources

This document may incorporate excerpts from various articles, blogs, quotes from captains, recommendations from other security professionals, and reports on previous incidents.



Written by



Tomislav is the Founder and CEO of the Xtreme Security GmbH

Tomislav Pahljina

Performance driven Security Professional with invaluable experience within the private security industry, conducting security operations within politically sensitive and strategically challenging environments in the theatres of Afghanistan, Iraq and across Africa, but also within private sector around Europe including Monaco and Switzerland.

Tomislav's professional career includes 6 years in the Office of the President as part of the Croatian Ministry of Defense. In addition to his military career, Tomislav has served as an independent contractor for U.S. security companies within Iraq and Afghanistan.

In a time of anti-piracy, back in 2011, he conducted around 50 missions with the successful protection of cargo and tanker ships despite 3 recorded pirate attacks. After operational experience on the sea, he became a Country Manager for Anti Piracy operations in the Red Sea.



ISO 28007-1:2015

Armed Security Services

Xtreme Security GmbH is proud to announce our achievement of the ISO 28007-1:2015 accreditation! This milestone reflects the growing demand for our superyacht security services in high-risk maritime areas and underscores our commitment to excellence.

The ISO 28007 certification enhances our organization's credibility by demonstrating our capability to provide appropriate Privately Contracted Armed Security Personnel (PCASP) services on

board yachts. It reassures yacht owners and stakeholders of our adherence to best practices in addressing both internal and external challenges related to PCASP. ISO PAS 28007 sets the global benchmark for private maritime security companies, indicating that a company and its operatives are legally, safely, and effectively equipped to secure shipping.

XTREME SECURITY GmbH

Am Heidebruch 1b.

81375 Munich

GERMANY

+49 (0) 1577 864 8351

XTREME SECURITY

info@xtremesecurity.eu