Angel

What is it?

ANGEL is the first cybersecurity service that has been designed and developed to meet the unique and diverse requirements of the merchant marine sector. It has been created to secure the vessel's business, IoT and crew networks by providing oversight, security threat alerting and control of the vessel's entire network. With enhanced web filtering, antivirus protection, intrusion detection and prevention, application control, Honeypot and ICS/Scada protection, it delivers multi-layered protection of vessels.

Who is it directed at?

ANGEL is directed towards the maritime sector which due to the emergence of digitized systems such as VDR (voyage data recording), AID (automatic identification system) and ECDIS (electronic chart display and information system) has become more vulnerable to cyber-attacks.

Why is it important?

A customized daily report is produced for the Cyber security health status of the fleet. The service is monitored on a 24/7 basis and upon discovery of potential Security Incidents the SOC analysts notify the clients' representatives with incident details and possible recommended actions / countermeasures to be taken. Also, ANGEL utilizes a continuously updated threat intelligence database, which is hosting heavily reported malicious IPs reported for malware / ransomware and C&C. Every external destination IP address from the vessels is compared with the IPs in the Threat Intelligence Database for potential matches. In case of a match an alert is raised and examined by the SOC team. If the alert is indeed related to a potential security incident, then the client is notified.

Where is it taking place?

The systems core component is Junipers Unified Threat Management platform which works through Infinity to separate business, IoT and crew traffic, providing separate secure network traffic flows. This is all backed up by a team of security specialists dedicated to handling any security issues based at Navarino's Security Operations Centre in Athens.

When is it going to make an impact?

These systems on their own are not equipped to meet the threats of the 21st century. Each of these essential systems can present easy access to an attacker, with potentially devastating consequences. What was traditionally an attempt to obtain sensitive data has transformed into highly sophisticated and complex attacks that attempt to inflict damage to property and operations. Aside from any commercial or reputation damage, the insurance sector is becoming more aware of cyber security threats.

How will it affect your business?

All these security features are continuously monitored and analyzed by Neurosoft’s SOC team, which consists of information security skilled personnel, to (a) track potential security incidents when occurring and (b) inform the client of these incidents, in this way actively protecting ANGEL’s clients on a 24/7 basis. The Cyber Attack Exclusion Clause (CL 380) 10/11/2003 has appeared on marine policies for the past 10 years. It excludes any loss, damage, liability caused either directly or indirectly using a computer and its associated systems and software as a means of inflicting harm. Furthermore in 2017, the IMP issued resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems. This takes effect in 2021 and encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management stems as defined in the ISM code. ANGEL helps the maritime sector to comply with these upcoming steps that are designed to keep marine cyber secure. ANGEL also present maritime insurers with evidence that your ships have advanced cyber protection which can lower your insurance premiums.