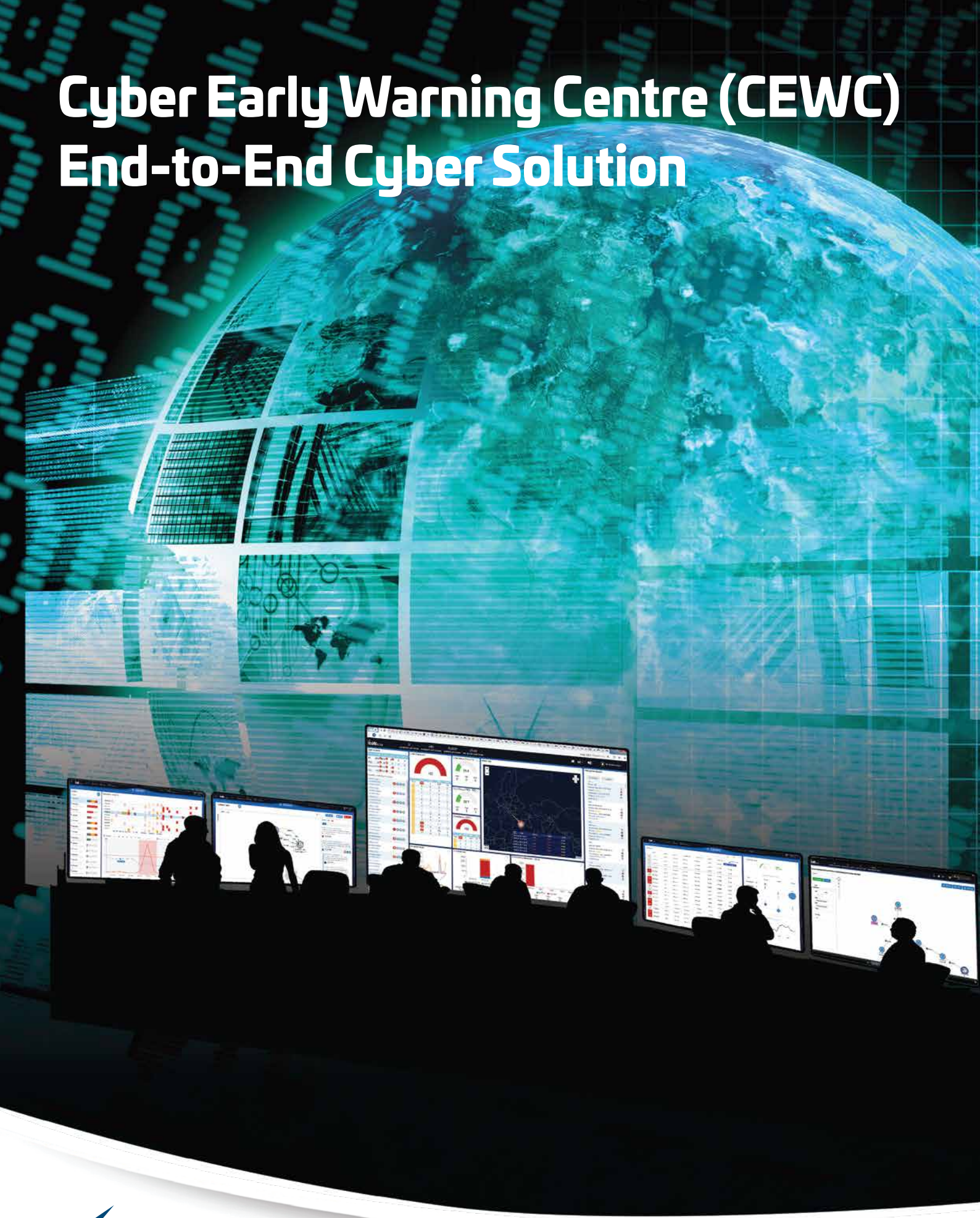
Cyber Early Warning Centre (CEWC)
End-to-End Cyber Solution



IAI

Where Courage Meets Technology™

Cyber Early Warning Centre (CEWC) End-to-End Cyber Solution

Nations around the world are seeing a growing trend of cyber-attacks against their critical infrastructures and sensitive civilian and military assets. The CEWC system offers a holistic approach to defend against these attacks by providing government agencies, ministries, regulators, critical infrastructures and defence forces with an end-to-end national-level cybersecurity solution tailored to their specific needs and threat landscape.

Cyber Early Warning Centre (CEWC) provides continuous surveillance of a customer's cyberspace providing a real-time situational awareness of a state's cyber security level. Security incidents and early-warning information are immediately and automatically disseminated to the relevant agencies. CEWC operates as a center to monitor local and national ICT networks, Industrial Control Systems, OT and communication proprietary protocols.

The solution supports SOC-of-SOC architecture resulting in a customer-centric methodology for cyber operations. CEWC is tailored to a nation's cyber strategy and integrated with premier commercial off-the-shelf solutions in the security market today. These solutions are part of the Israeli Cyber Companies Consortium (IC3). The IC3 is under the auspice of the Israeli Ministry of Economy and draws together a diverse group of Israel's foremost cyber companies. With IAI as the leader, the consortium includes **Check Point, CyberArk, Verint, ECI, Bynet, Clearsky, CyberX, BG Protect, XM Security and Mellanox Technologies.**

Figure : System Dashboard

The CEWC comprises the following elements:

- **Situational Awareness Picture** – displays different levels of situational awareness status of the current threats and attacks in various views (timeline, geography etc.) and enables drilling down to the sector and organizational level.
- **Cyber Threat Fusion Center** –is the core of the system and detects cyber threats through correlation and analysis of collected information, uses Machine Learning (ML) to recognize patterns and detect anomalies as they occur, provides timely alerts, generates cyber insights and disseminates them to the various end-users of the CEWC. It includes high-end cyber analytical tools allowing the analysts to analyze & investigate cyber events.
- **Cyber Threat Analysis Desk** – gathers intelligence from the open-source sites containing Common Vulnerabilities and Exposures (CVE) information. The data is filtered, cleaned, categorized and disseminated internally for analysis.
- **Incident Management & Response** – a ticketing system that supports the full event & incident management life cycle.

ELTA is committed to investing in R&D, partnering with leading security technology partners, and being associated with global security consortiums. This commitment ensures continual development and innovation in order to counter ever-evolving global cyber threats.

Where Courage Meets Technology

ELTA Systems Ltd
www.iai.co.il
market@elta.co.il