CyberShield Command Core

Managing the cyber battlefield and the proactive cyber defense array - to ensure confidentiality, availability and integrity of critical cyber assets

Elbit Systems
Land and C4I

CyberShield Command Core

Managing the cyber battlefield and the proactive cyber defense array - to ensure confidentiality, availability and integrity of critical cyber assets

Protecting critical infrastructure from cyber-warfare, cyber-espionage and cyber-crime has created complex challenges for security teams and network managers, as well as national leaders, commanders and executives charged with protecting their organizations from cyber-attacks. General cyber-threats and Advanced Persistent Threats (APTs) take on many forms posing a major risk to governments, militaries and civilian infrastructure.

Elbit Systems' CyberShield Command Core enables the prevention and protection of computer networks and critical systems from cyber-incidents and threats, while providing high-fidelity defense of critical cyber-assets. As an integral part of Elbit Systems' CyberShield solution, CyberShield Command Core's technology supports all phases of the cyber-defense process, providing a comprehensive solution.

CyberShield Command Core's modular infrastructure allows for data collection and transportation, information sharing and data dissemination, as well as long-term scalable storage for analysis, advanced detection and data mining. With its end-to-end cyber incident management capabilities and comprehensive situational awareness, CyberShield Command Core ensures data and network confidentiality, availability and integrity.

Effective Cyber Strategy:

Active Defense

Elbit Systems' CyberShield's proactive approach is supported by technological solutions and includes five phases to defend against cyber threats and attacks: data gathering, analysis, management, response and prevention.

Gathering: monitoring and identification of events and traffic from networks, along with intelligence gathering. Data is collected and stored in long-term scalable storage for further correlation and analysis.

Analysis: enrichment, aggregation and correlation of gathered information using high-end technologies and advanced detection methods and algorithms, as well as impact analysis tools.

Management: end-to-end cyber incident management, from the detection phase to the mitigation and reaction phases. Workflow, tasking, and documentation capabilities are supported, while decision support recommendations and essential data for event analysis are automatically provided to the user, together with comprehensive cyber situational awareness.

Response: containing and mitigating the event using interfaces to the proactive cyber defense array, post-event analysis, management and documentation.

Prevention: implementation of smart enforcement tools for monitoring network compliance, proactive protection arrays and cyber defense training.

CyberShield Command Core

Managing the cyber battlefield and the proactive cyber defense array - to ensure confidentiality, availability and integrity of critical cyber assets

Smart Infrastructure Supporting the Complete Cyber Defense Process

- CyberShield Command Core is a modular system consisting of four functional units with a common infrastructure to enable the provision of end-to-end protection of critical networks within a rapidly changing cyber domain. The modular system can be tailored to the customer's cyber defense doctrine and is comprised of the following units:

- **Command and Control (C2)** – providing real-time monitoring and management of cyber incidents, cyber situational awareness, decision support, impact analysis, and management of the cyber response array.

- **Active Defense and Research** – APT detection and active hunting using designated tools and algorithms. The system is ideal for silent attack detection, anomaly detection, pattern analysis, and vulnerability research. This module provides research, analysis, and data retrieval capabilities used for event investigation during and after the event.

- **Cyber Intelligence** - acquisition and extraction of cyber-defense intelligence, combining collection systems, data management and alert generation mechanisms for closing the intelligence-C2 operational loop. This module also includes receipt of intelligence from various sources (including open sources) in order to provide information on threats and vulnerabilities. It also performs processing and analysis to support operational processes, enrich detection algorithms and generate intelligence-based cyber alerts.

- **Enforcement** – smart and automatic enforcement and regulation of cyber policy, including risk assessment and compliance evaluations for detection of policy violation and configuration changes. This module enables enforcement-based alert generation for closing the enforcement-C2 operational loop.

Operational Benefits

- **Designed for governments, military and critical infrastructure organizations**
- **Implementation of a proactive approach to cyber defense**
- **Modular infrastructure ensuring comprehensive protection**
- **Closing the intelligence-C2 and the enforcement-policy-C2 operational loops**

Key Features

- **Real-time monitoring and control of the cyber domain**
- **Continuous operational cyber situational awareness**
- **End-to-end cyber incident management and information sharing**
- **Comprehensive response management**
- **Threat intelligence alert generation**
- **Information sharing and knowledge management**

Elbit Systems Land and C⁴I

Elbit Systems Land and C⁴I Ltd.
2 Ha'machshev St., Netanya 42507, Israel
E-mail: landc4i@elbitsystems.com www.elbitsystems.com/landc4i