CYBER, C4ISR

(EL) Cyber Threats and Incident Response Information Sharing Platform (CTISP)

(Established in March 2018)

For Public Release

PROJECT DESCRIPTION

The acknowledgement of Cyberspace as a military domain of operation implies an increasing need for Cyber Threats information sharing, in order to help EU Member States to efficiently cope with the constantly evolving Cyber Threat Landscape. The project aims at the sharing of cyber threats information, the strengthening of MS cyber defence capability and the strengthening of response in cyber incidents, demanding multinational cooperation.

OBJECTIVES/PRODUCTS

Sharing cyber threats information, for strengthening MS cyber defence capability and strengthen response in cyber incidents, demanding multinational cooperation. The project addresses the CDP priority “Enabling capabilities for Cyber Responsive” and the capability shortfall on Cyber Defence mitigating the HICG "Static Cyber Defence".

INDICATORS

Project Execution Year (PEY) and Project Completion Year (PCY):

DELIVERABLES ACHIEVED

The project is divided into three phases:

- First phase: The High-Level Operational Requirements were defined.
- Second phase: A TRL-7 industrial prototype was delivered and tested successfully through the EDIDP-2019 PANDORA project.
- The third phase is currently ongoing and involves the procurement, installation and operational use of the platform.

The project was not completed in 2024 as expected. However, the project is in its last phase, and it is estimated that a final operational capability (FOC) will be achieved in 2025. For this reason, the PCY was changed to 2025.

CRITERIA FOR SUCCESS

- The project would be considered successful if multiple pMS procure and install the platform in their networks and cooperate using the information sharing capabilities.

EL, CY, HU, IE, IT, PT

FR, LT, LU, PL, ES

IDEATION
INCUBATION
EXECUTION
CLOSING

Contribution to the more binding commitments
Yes

Capability Perspective

EU CDP priority
Cyber Warfare Advantage and Readiness

CARD references
Cyber Research and Technology

Operational Viewpoint

HICG
Static Cyber Defence

EDA support

No