CYBERSECURITY MANAGEMENT SYSTEM FOR PROTECTION GRIDS ASSETS FROM CYBER THREATS

Issues / prerequisites

Due to the war, number of targeted cyber attacks on the OT infrastructure of Ukraine had increased drastically

As a result of missile strikes, we need constantly replace the equipment. This increases the risk of unauthorized installation of harmful devices in OT

Hacker groups, sponsored by the aggressor, use various modern tools for hacking and disabling of OT systems

Technological network is not fully tiered and cyber attack may go deep inside the OT, leading to catastrophic consequences

Objectives

1. Reducing risks of cyber attacks by implementing Cybersecurity Management System
2. Implementing tools for prompt detection of devices that were connected to the OT infrastructure without proper authorization
3. Implementing the following systems: grid monitoring, grid protection, OT resources access management, traffic management, advanced attacks protection
4. Complete isolation of the OT network from other networks and division of the OT network into separate control and management segments

1 PROJECT SCOPE

1.1 Improving resistance of the OT infrastructure to cyber attacks
1.2 Building Cybersecurity Events Control and Management Center
1.3 Isolating and dividing OT network into different segments

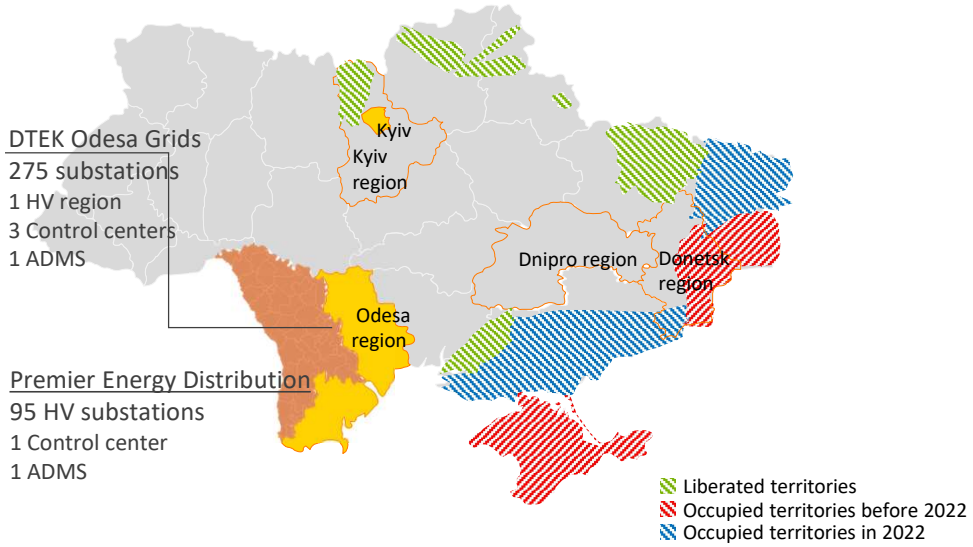
2 PROGRESS TO-DATE

2.1 Creating cyber security management system development plan
2.2 Conducting pilot project of OT cyber security and events monitoring
2.3 Planning of the OT grid segmentation

3 TIMEFRAME

3.1 Implementation of the cybersecurity program by the end of 2025
3.2 Conducting a pilot project of the monitoring center by 2025
3.3 Division and segmentation of the grid by 2027

Overview of current parameters

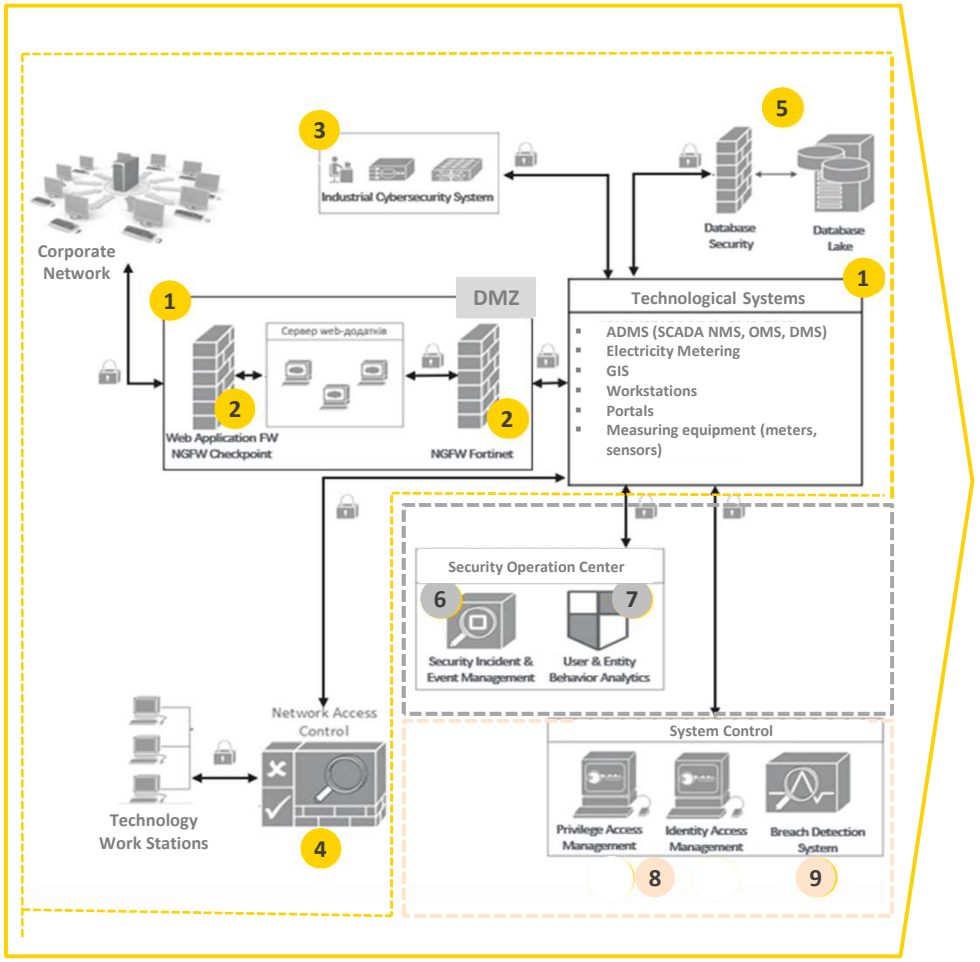


Project KPI (DTEK)

	CURRENT	GOAL
1 Countering cyber attacks on OT	5%	100%
2 Timely response to cybersecurity events	N/A	15 min
3 Protection of the OT grid from an unauthorized interference	Medium	High
4 Segmentation of the OT grid	55%	100%

IT/OT Systems

Challenge/Area



Target systems

Implementation of target systems to protect the OT infrastructure at all DSOs:

SYSTEMS FOR DETECTION AND ANTI-INVADERS

1. Separation of IT and OT infrastructures
2. Protection of external web resources of the company
3. Implementation of a comprehensive protection system for technological systems
4. Control of device connections to the corporate network
5. Ensuring database security to control data access

SYSTEMS FOR MONITORING AND ANALYSIS OF CYBER SECURITY

6. Real-time analysis of security events
7. Analysis users and entities by behavioural models to detect cyber threats

CONTROL SYSTEMS FOR USERS AND ADMINISTRATORS OF TECHNOLOGICAL SYSTEMS

8. Access rights management
9. Protection against targeted high level attacks

COST DATA

Roadmap / stages of project

2025

- Regulation of CS processes
- Segmentation of the OT grid 20%
- Identification of OT assets
- Estimation of CS risks
- Selection of SIEM solution
- Development of SOC concept
- ICSS configuration

2026

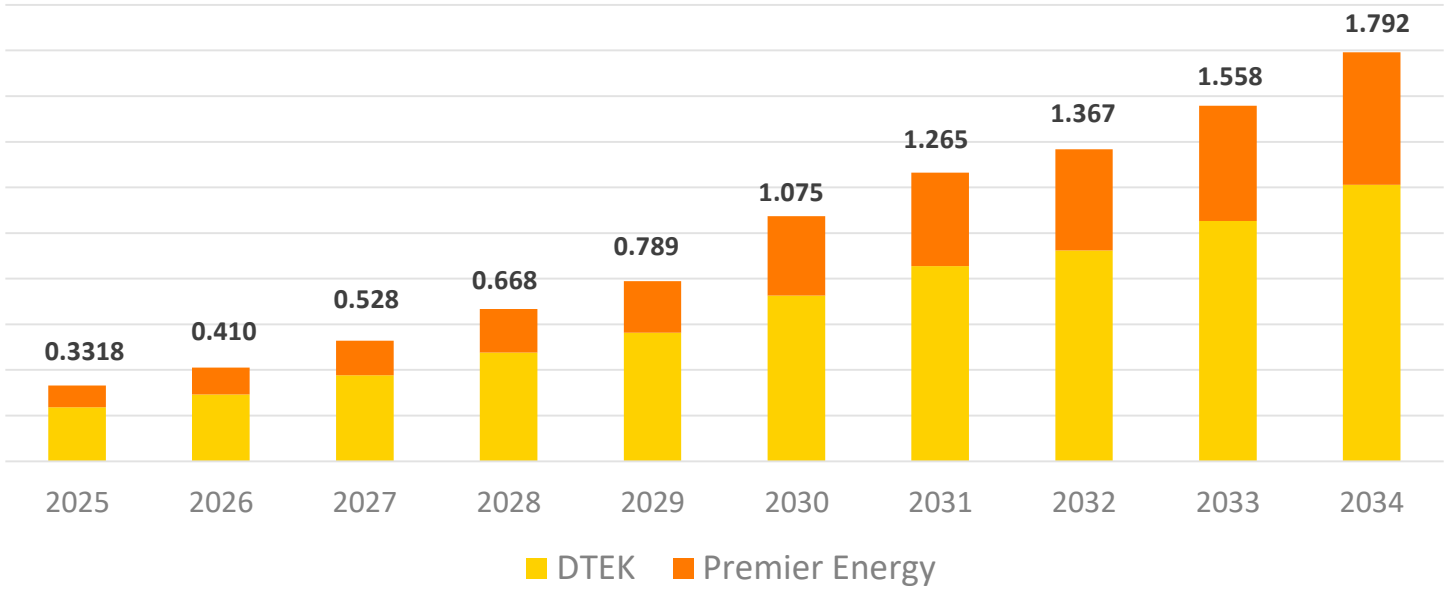
- Implementation of CS management system
- SOC pilot project
- Segmentation of the OT grid 30%
- Implementation of SIEM (1 stage)
- Implementation of PAM
- Commercial operation of ICSS

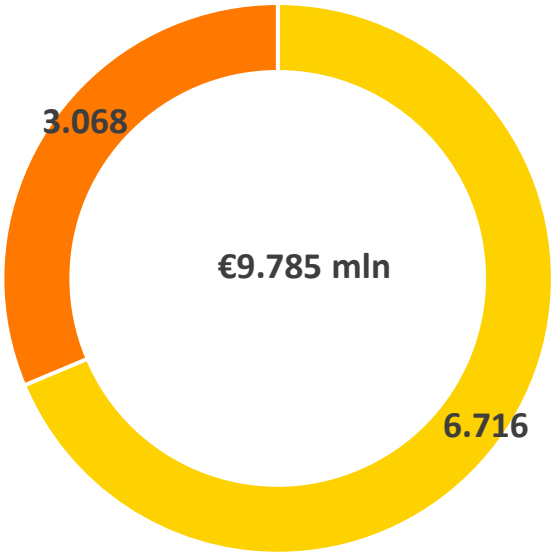
2027-2034

- Segmentation of the OT grid 100%
- Implementation of SIEM (2 stage), UEBA
- Creation of a full-fledged SOC
- WAF
- IAM
- NAC
- DBS, BDS

Project investment plan

mln EURO





ELIGIBILITY OF THE PROJECT ACCORDING TO TEN-E REGULATION

Smart electricity grids

any equipment or installation, digital systems and components integrating information and communication technologies (ICT), through operational digital platforms, control systems and sensor technologies both at transmission and medium and ***high voltage distribution level***, aiming to ensure a more efficient and intelligent electricity transmission and distribution network, increased capacity to integrate new forms of generation, energy storage and consumption and facilitating new business models and market structures***,…, to support innovative and other solutions involving at least two Contracting Parties with a significant positive impact on the Energy Community 2030 targets*** for energy and climate and the 2050 climate neutrality objective***, to contribute significantly to the sustainability of the Energy Community***

General criteria

the potential overall benefits of the project outweigh its costs

the project involves two Contracting Parties by directly or indirectly, via interconnection with a third country, crossing the border of two or more Contracting Parties

Specific criteria

(i) ***security of supply***, including through efficiency and interoperability of electricity transmission and distribution in day-to-day network operation, avoidance of congestion, and integration and involvement of network users;
(ii) market integration, including through ***efficient system operation*** and use of interconnectors;
(iii) ***network security***, flexibility and ***quality of supply***, including through higher uptake of innovation in balancing, flexibility markets, ***cybersecurity***, ***monitoring, system control and error correction***;
(iv) ***smart sector integration***, either in the energy system through linking various energy carriers and sectors, or in a wider way, favouring synergies and coordination between the energy, transport and telecommunication sectors;

Additional criteria

The project satisfies the following criteria (significant cross-border impact):
(i) it involves ***1 000 000 users***, generators, consumers or prosumers of electricity;
(ii) it captures a consumption area of at least ***6 800 GW hours/year***