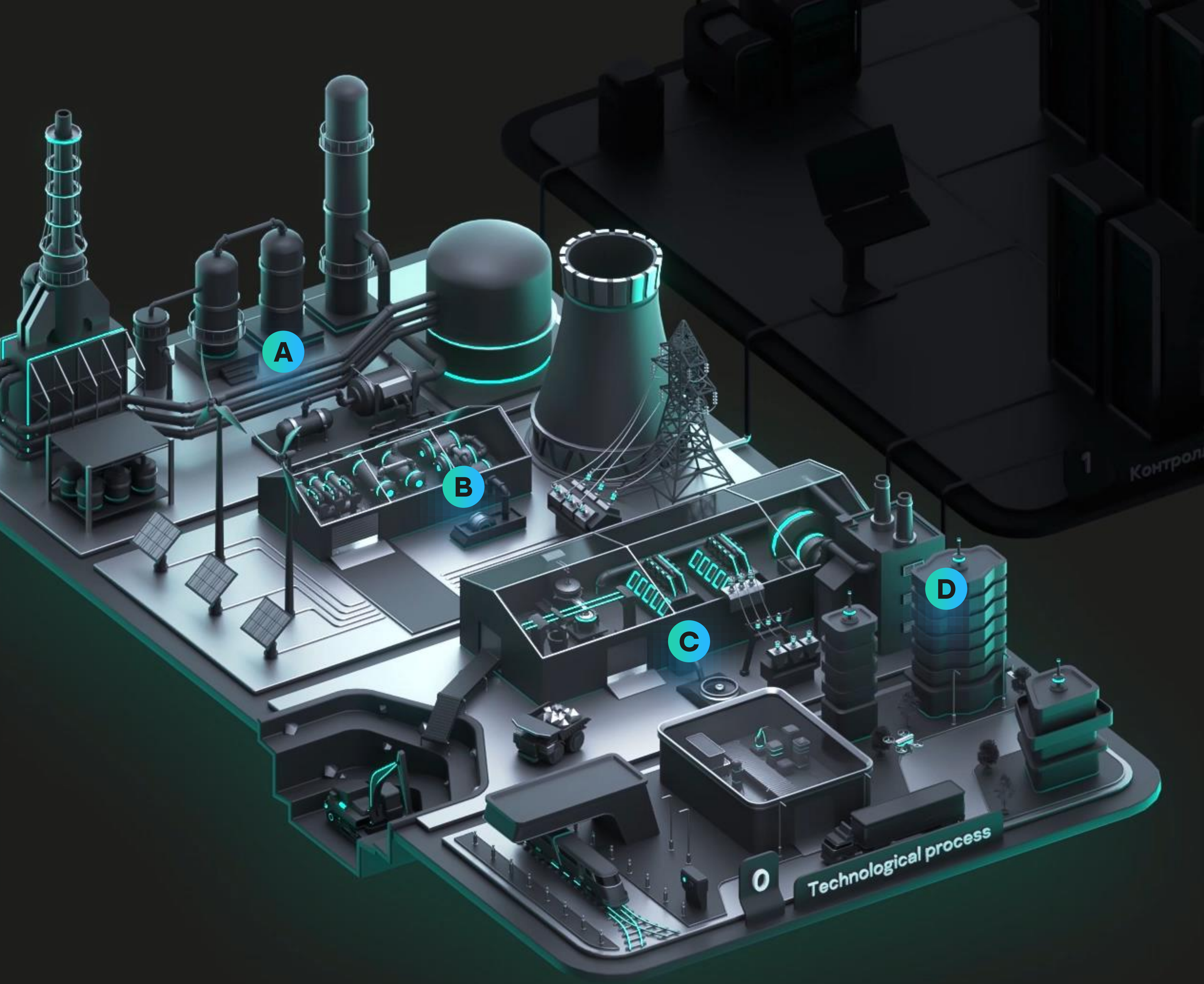
Kaspersky Industrial
Cybersecurity
Conference 2024

Evolution of OT cybersecurity

Kirill Naboyshchikov
Product Marketing Leader
Critical Infrascructure Protection

kaspersky

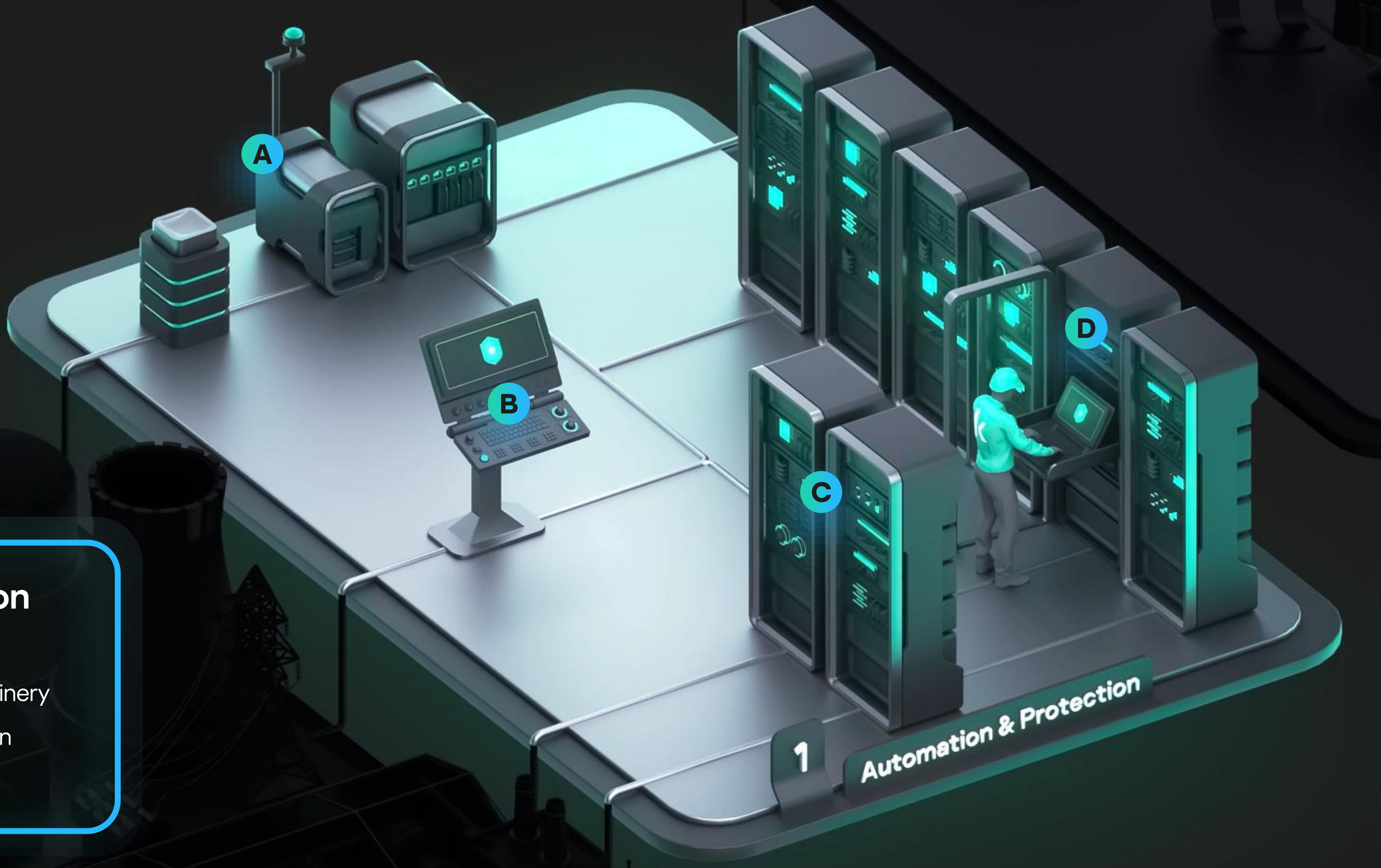
Industrial enterprises



Technological process

- A — Oil, gas, and chemicals
- B — Power, grid, and utilities
- C — Minerals, metals, and mining
- D — Critical manufacturing and transportation

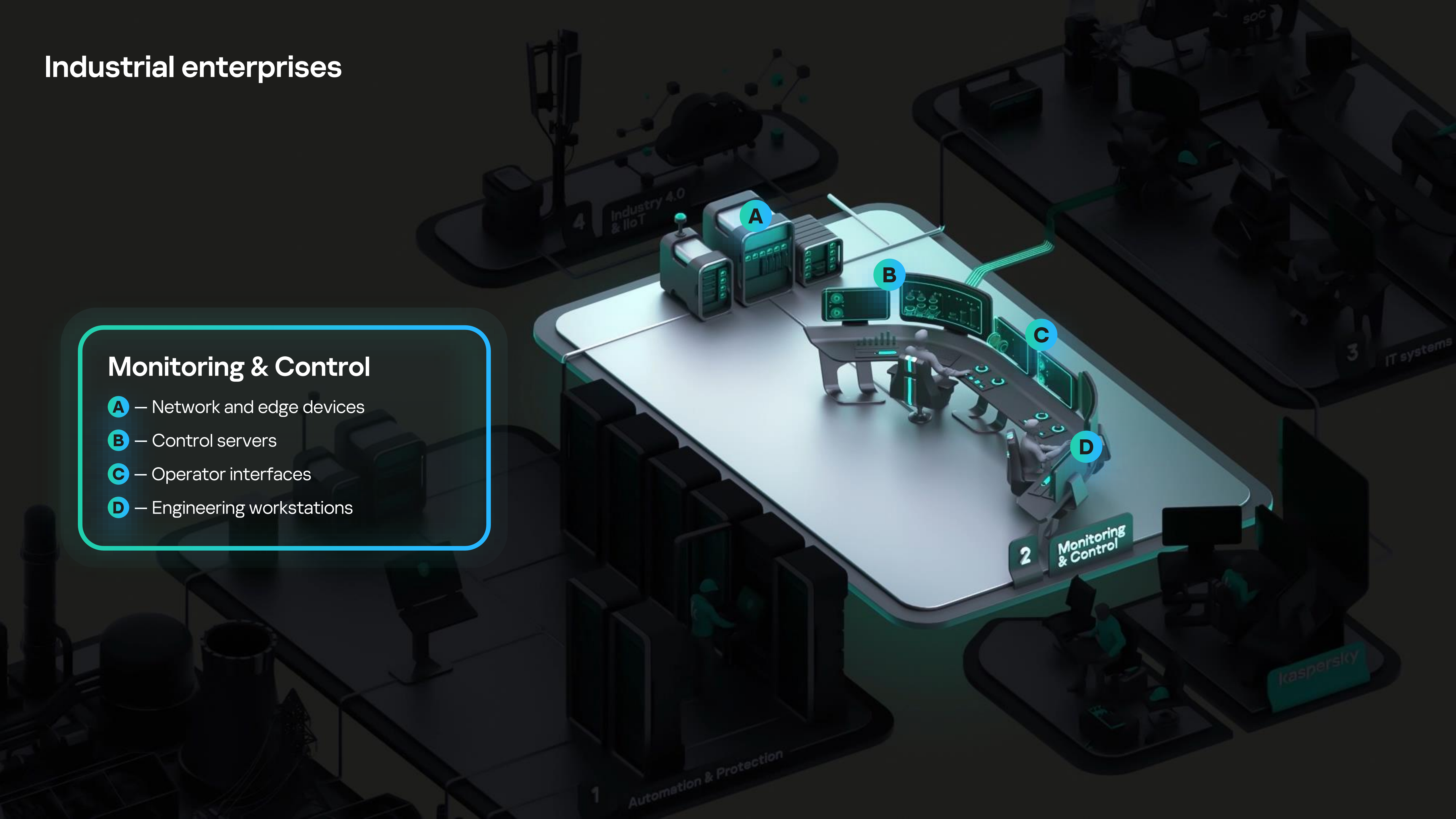
Industrial enterprises



Automation & Protection

- A — OT network, GPS, historian
- B — Standalone systems and machinery
- C — Controllers and relay protection
- D — Local HMI and EWS

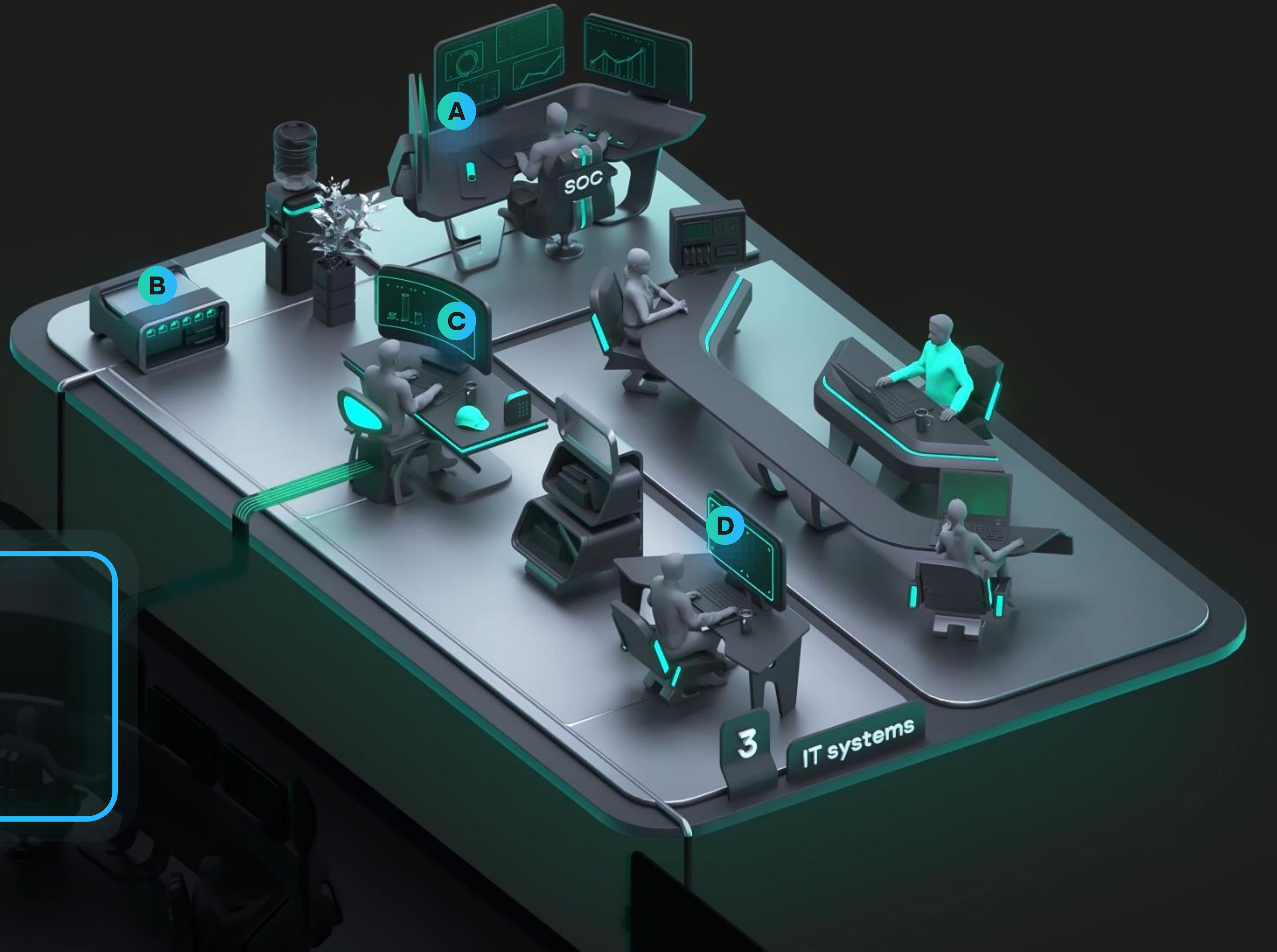
Industrial enterprises



Monitoring & Control

- A — Network and edge devices
- B — Control servers
- C — Operator interfaces
- D — Engineering workstations

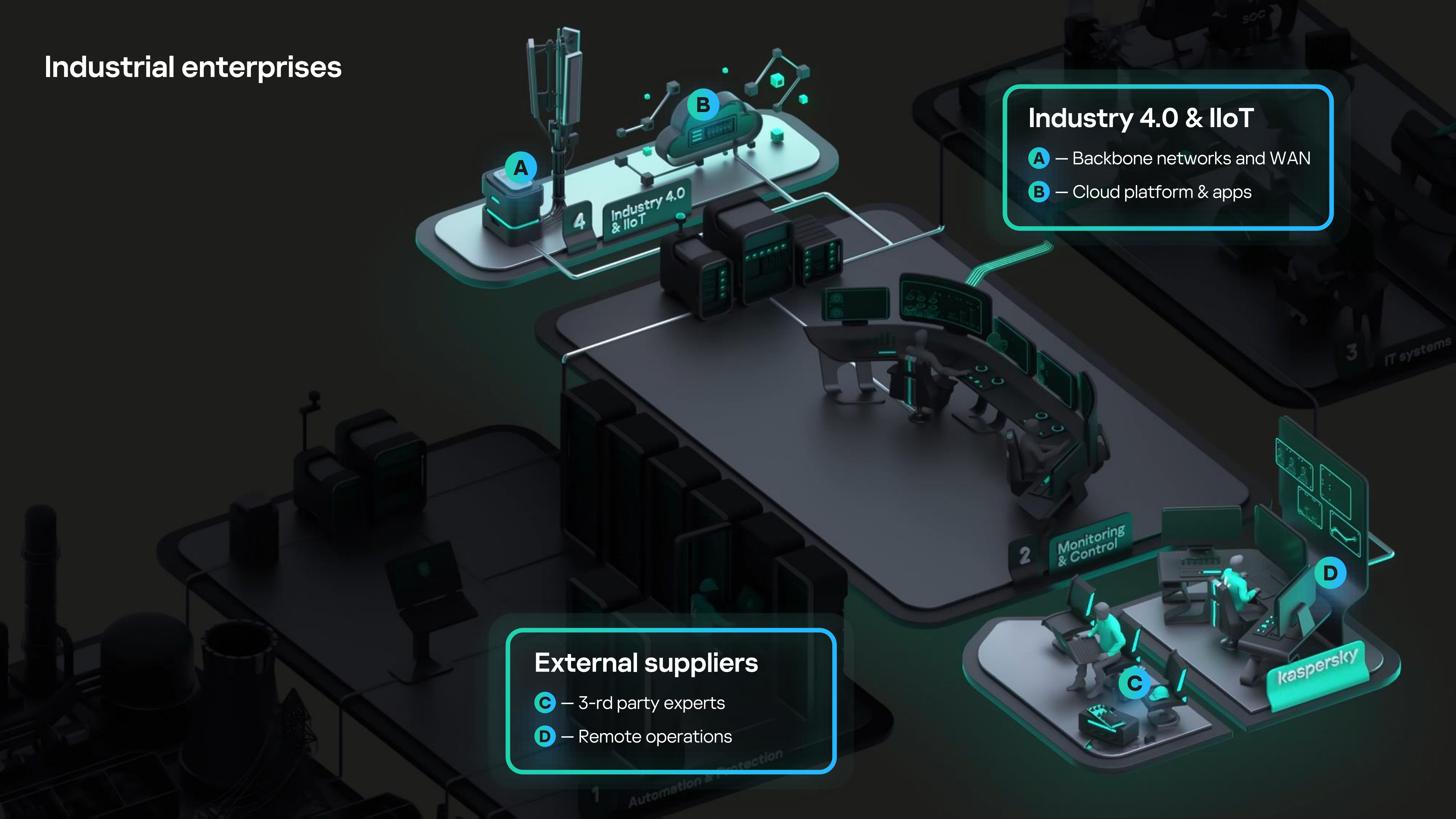
Industrial enterprises



IT systems

- A — Security team
- B — IT networks
- C — Business systems
- D — Remote workplace

Industrial enterprises



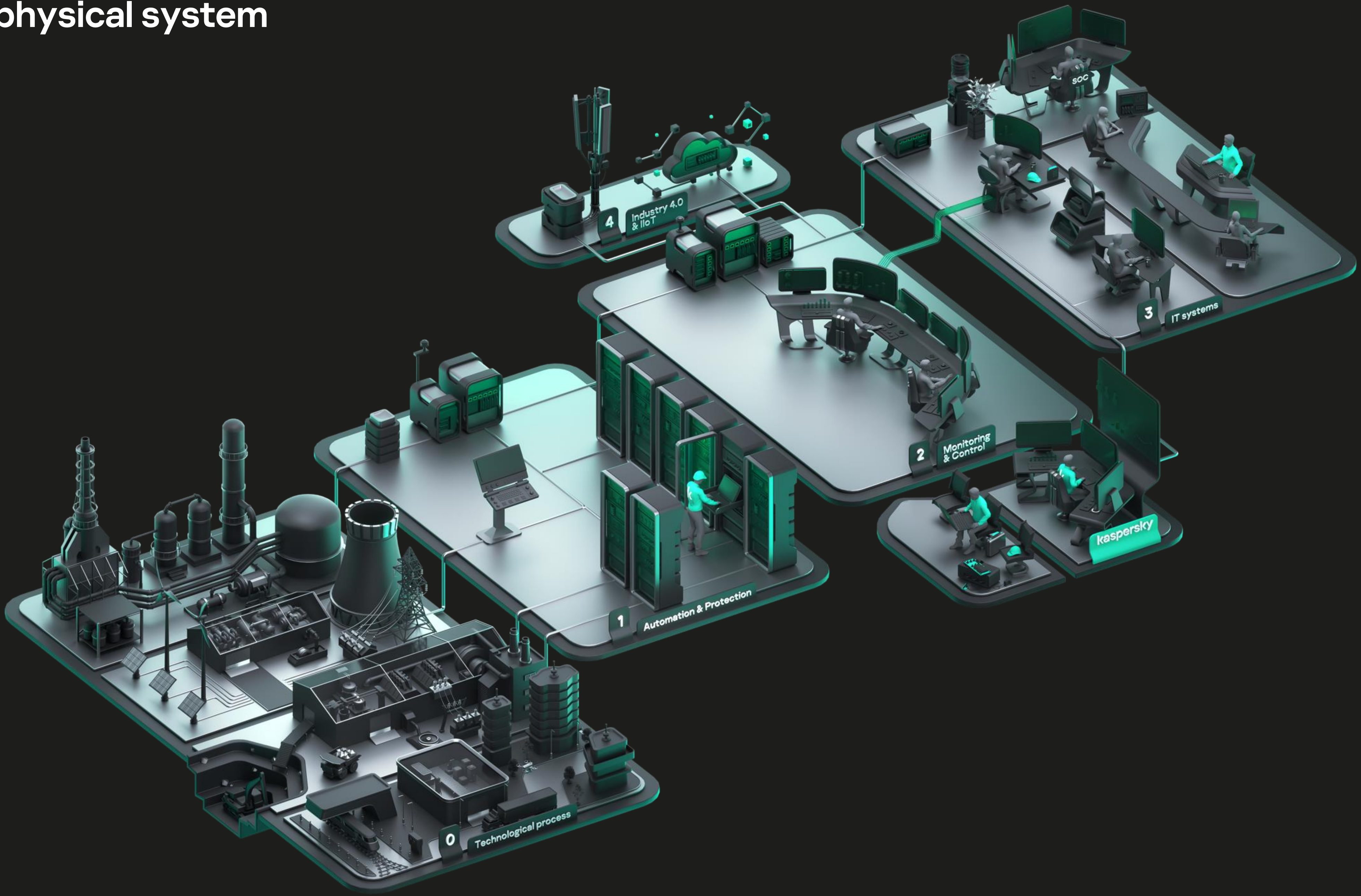
Industry 4.0 & IIoT

- A — Backbone networks and WAN
- B — Cloud platform & apps

External suppliers

- C — 3-rd party experts
- D — Remote operations

Cyber-physical system



Yesterday

Security by obscurity

Airgap, reactive approach,

basic

security measures borrowed from IT

Spec

designe

Inc

produc

Today

m IT

Specialized platforms

designed and tested for OT.

Industrial grade

product for Critical Infrastructure Protection

IT – C

eco

nati

technolo

Bring on the future

e

otection

IT – OT convergence

ecosystem of natively integrated

technologies, knowledge, and expertise

Bring on the future

OT security technology provider must:

Be transparent and a long-term **enterprise** grade supplier

Have the **right mix** of IT, OT, and IoT expertise and ecosystem offering

Provide a **platform** solving multiple challenges

Offer extended detection, **prevention** and secure by design products

Ensure **compliance** with standards, regulations and compatibility with ICS

AVTEST

Prove the **efficacy** of its technologies

kaspersky

Kaspersky Industrial CyberSecurity

Native OT XDR platform

ics.kaspersky.com

Industrial Enterprise

Native XDR

Kaspersky Industrial CyberSecurity

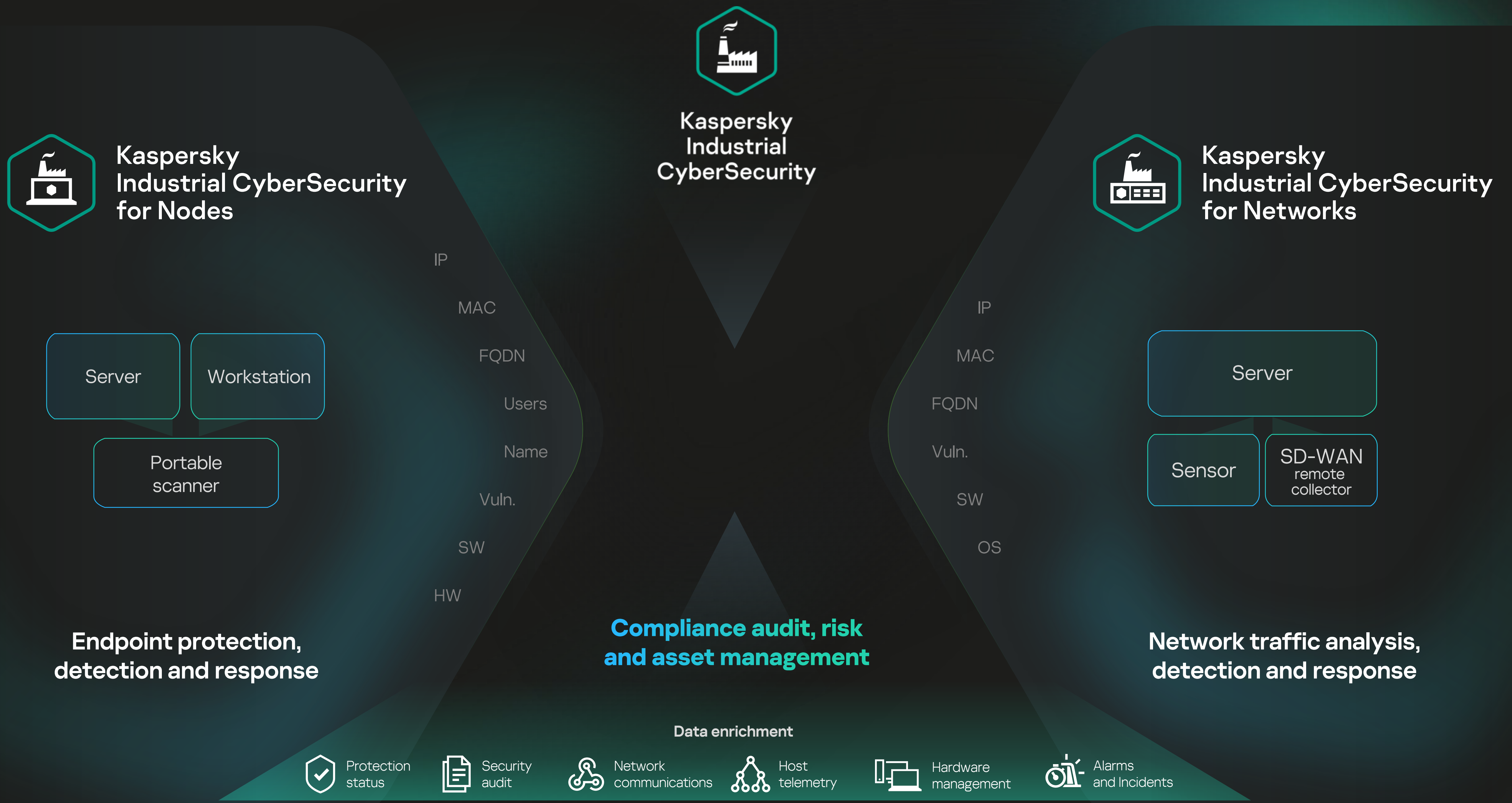
for Nodes
Endpoint protection, detection and response

×

for Networks
Network traffic analysis, detection and response

SOC
4 Industry 4.0 & IIoT
3 IT systems
2 Monitoring & Control
1 Automation & Protection
kaspersky

Platform for critical infrastructure protection



Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Server

Workstation

Portable scanner

IP
MAC
FQDN
Users
Name
Vuln.
SW
HW

Endpoint protection, detection and response

Kaspersky Industrial CyberSecurity for Networks

Server

Sensor

SD-WAN remote collector

IP
MAC
FQDN
Vuln.
SW
OS

Network traffic analysis, detection and response

Compliance audit, risk and asset management

Data enrichment

- Protection status
- Security audit
- Network communications
- Host telemetry
- Hardware management
- Alarms and Incidents

Kaspersky Industrial CyberSecurity key advantages

- IEC62443 secure development lifecycle
- KSN data processing
- AV DB development and release controls

Extensive program of testing the solution with leading automation system vendors

Serving the largest industrial enterprises worldwide from all major verticals

Rich functionality addressing various safety, security, management, and maintenance challenges.

Compliant

The platform and it’s core technologies are under industry-leading audits

IEC 62443-4-1

TÜV AUSTRIA CERTIFIED ISO/IEC 27001

ISO/IEC 27001

AICPA SOC

SOC 2 Type 2

Kaspersky Industrial CyberSecurity key advantages

IEC62443 secure development lifecycle

KSN data processing

AV DB development and release controls

Extensive program of testing the solution with leading automation system vendors

Serving the largest industrial enterprises worldwide from all major verticals

Rich functionality addressing various safety, security, management, and maintenance challenges.

Compatible

200+ tested systems from

70+ vendors

https://www.kaspersky.com/enterprise-security/industrial-cybersecurity/certification

Kaspersky Industrial CyberSecurity key advantages

IEC62443 secure development lifecycle

KSN data processing

AV DB development and release controls

Extensive program of testing the solution with leading automation system vendors

Serving the largest industrial enterprises worldwide from all major verticals

Rich functionality addressing various safety, security, management, and maintenance challenges.

Trusted

Results to date

240k+
Licenses shipped

1000+
Industrial customers

420+
Networks protected

250
Projects in 2023

Kaspersky Industrial CyberSecurity key advantages

IEC62443 secure development lifecycle

KSN data processing

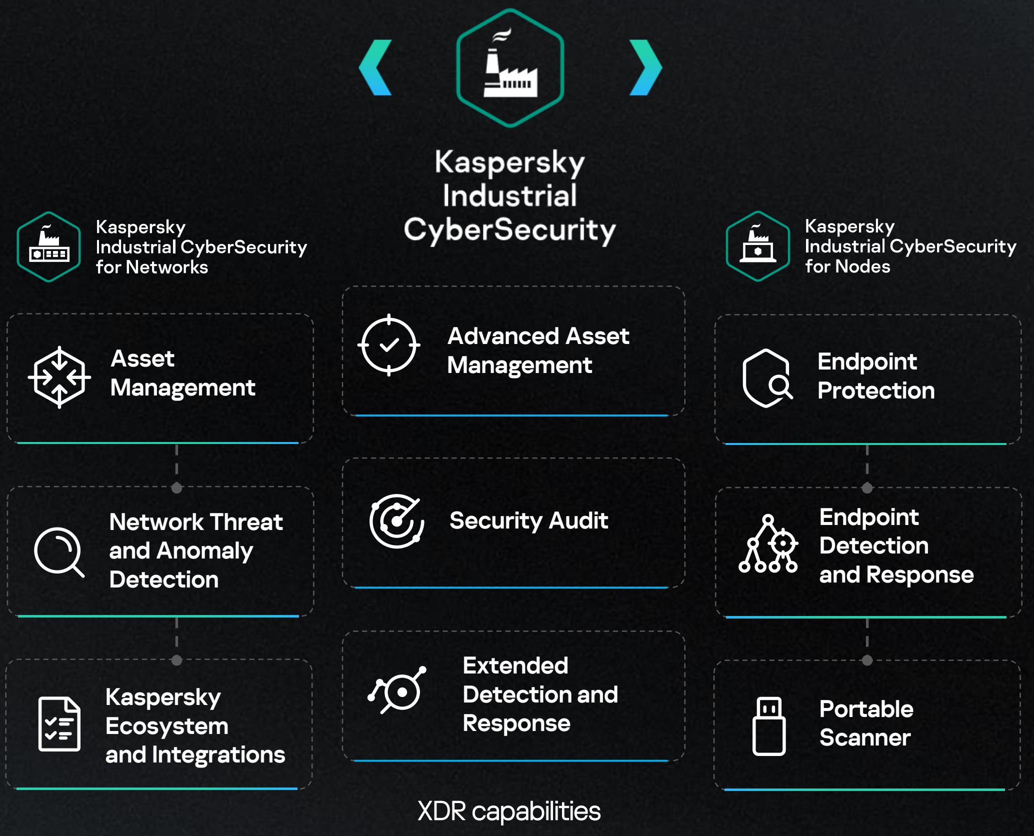
AV DB development and release controls

Extensive program of testing the solution with leading automation system vendors

Serving the largest industrial enterprises worldwide from all major verticals

Rich functionality addressing various safety, security, management, and maintenance challenges.

Native OT XDR



Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Networks

- Asset Management
- Network Threat and Anomaly Detection
- Kaspersky Ecosystem and Integrations

XDR capabilities

- Advanced Asset Management
- Security Audit
- Extended Detection and Response

Kaspersky Industrial CyberSecurity for Nodes

- Endpoint Protection
- Endpoint Detection and Response
- Portable Scanner

kaspersky

Kaspersky OT CyberSecurity

Cyber-physical security ecosystem
for industrial enterprises

kaspersky.com/enterprise-security/industrial-solution

Kaspersky OT CyberSecurity

Cyber-physical security ecosystem
for industrial enterprises

Kaspersky Next XDR Expert

IT-OT Convergence

Technologies

Specialized solutions

- Kaspersky Antidrone
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN

Native XDR

Kaspersky Industrial CyberSecurity

for Nodes
Endpoint protection, detection and response

for Networks
Network traffic analysis, detection and response

KasperskyOS solutions

- Kaspersky IoT Secure Gateway
- Kaspersky Thin Client
- Kaspersky Automotive Secure Gateway

Knowledge

Cyber hygiene

Kaspersky Security Awareness

Threat intelligence

Kaspersky ICS Threat Intelligence

Training

Kaspersky ICS CERT Training

Expertise

Discovery

Kaspersky ICS Security Assessment

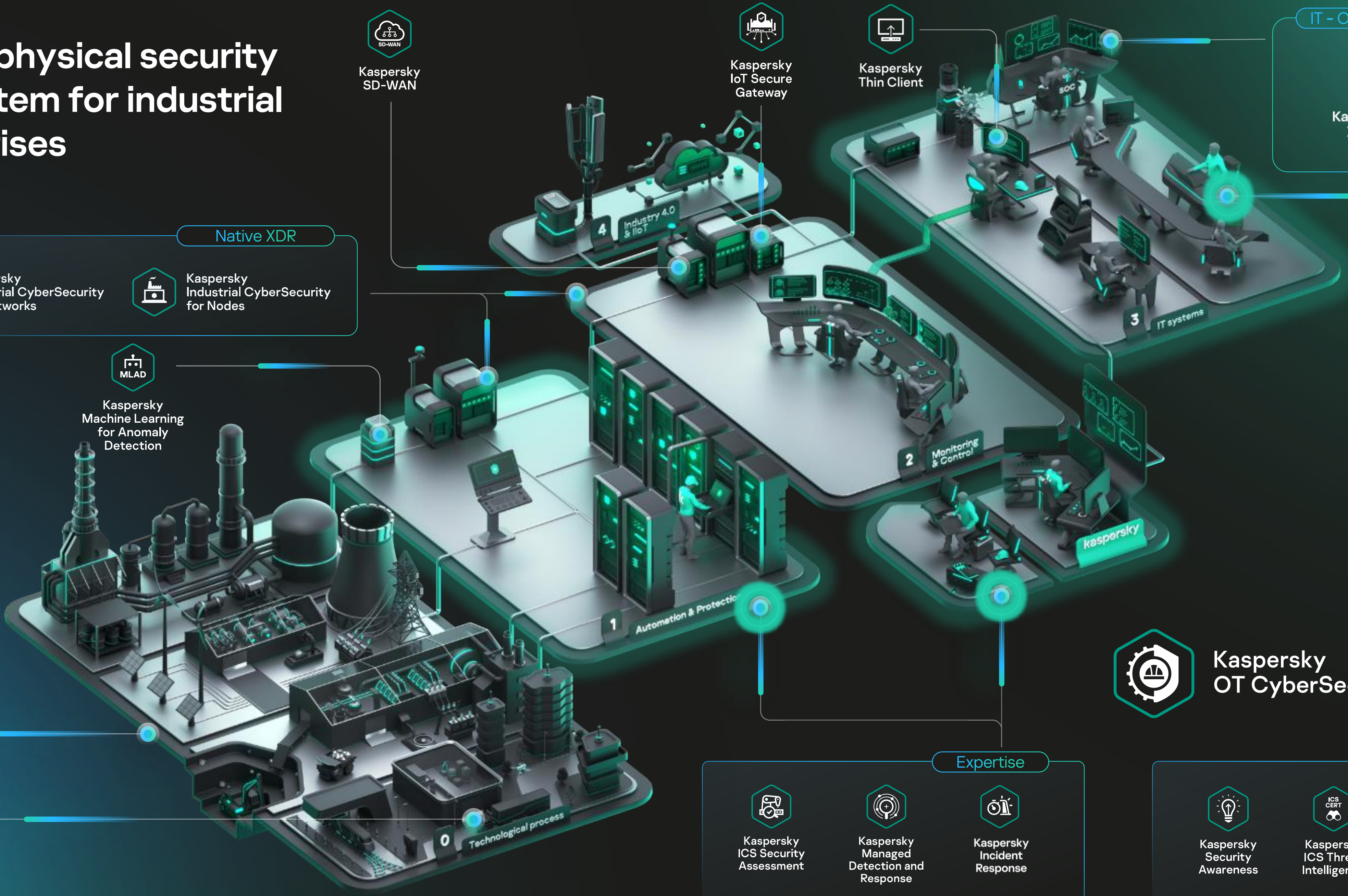
Managed Service

Kaspersky Managed Detection and Response

Response

Kaspersky Incident Response

Cyber-physical security ecosystem for industrial enterprises



Native XDR

- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Antidrone

MLAD

Kaspersky Machine Learning for Anomaly Detection

Kaspersky SD-WAN

Kaspersky IoT Secure Gateway

Kaspersky Thin Client

IT - OT convergence

Kaspersky Next XDR Expert

Kaspersky Automotive Secure Gateway

Kaspersky OT CyberSecurity

Expertise

- Kaspersky ICS Security Assessment
- Kaspersky Managed Detection and Response
- Kaspersky Incident Response

Knowledge

- Kaspersky Security Awareness
- ICS CERT Kaspersky ICS Threat Intelligence
- ICS CERT Kaspersky ICS CERT Training

O&G cybersecurity expertise to share

Analyzing:

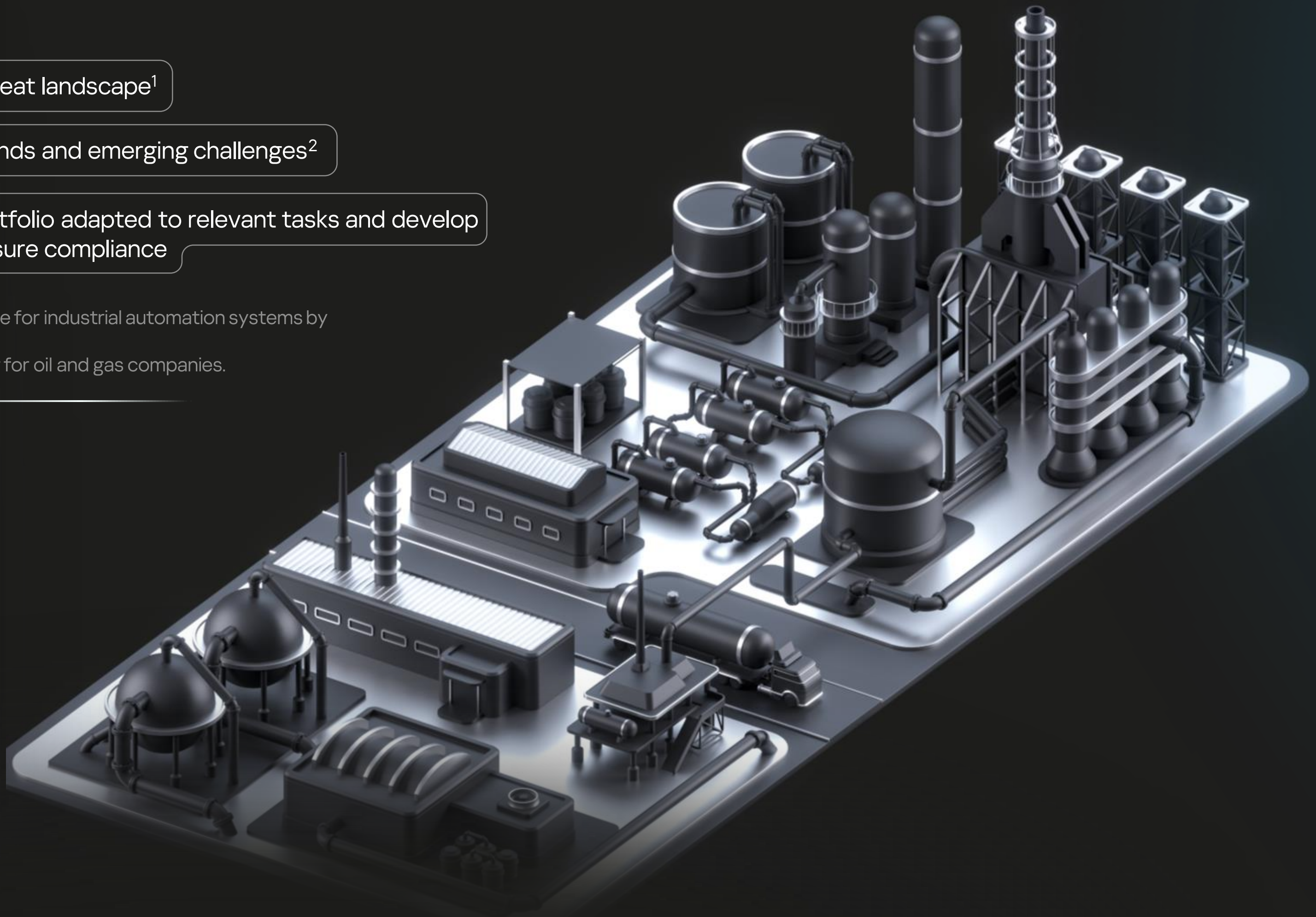
IT, IoT and OT threat landscape[1]

Digitalization trends and emerging challenges[2]

Our product portfolio adapted to relevant tasks and develop guidelines to ensure compliance

[1] Threat landscape for industrial automation systems by Kaspersky ICS CERT.

[2] Vertical offering for oil and gas companies.



12+ years

of experience in O&G sector

138 projects

completed

12%

Protecting O&G companies with 12% of a total world production

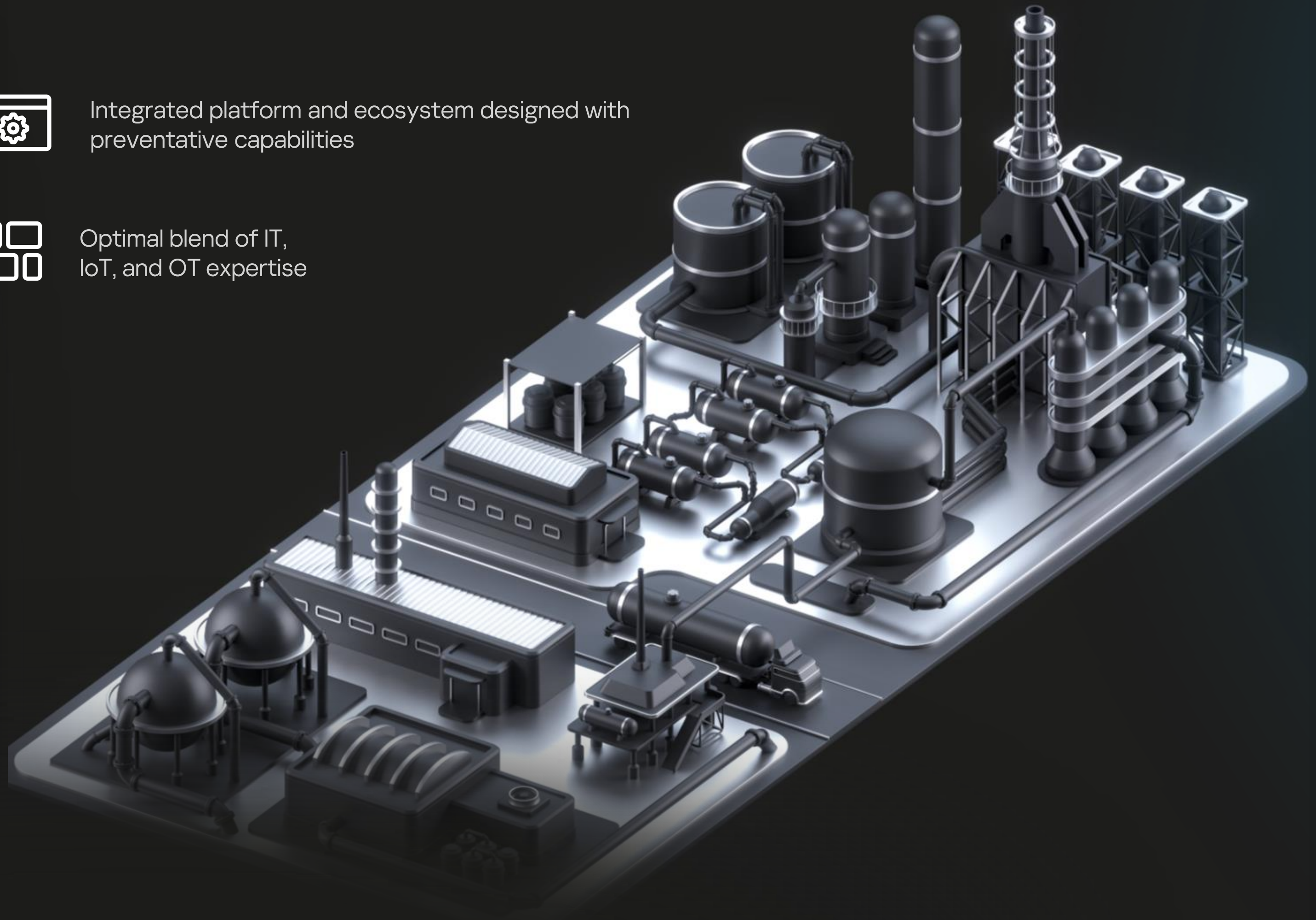
60 companies

already under protection

Cases in O&G cybersecurity

Integrated platform and ecosystem designed with preventative capabilities

Optimal blend of IT, IoT, and OT expertise



QazMunaiGaz
AMÓZ
ATYRAÝ MUNAI ÓNDEÝ ZAÝYTY

One of the largest oil refineries in the world

ROSNEFT

OOO «RN-BashNIPIneft»
Design and research institute

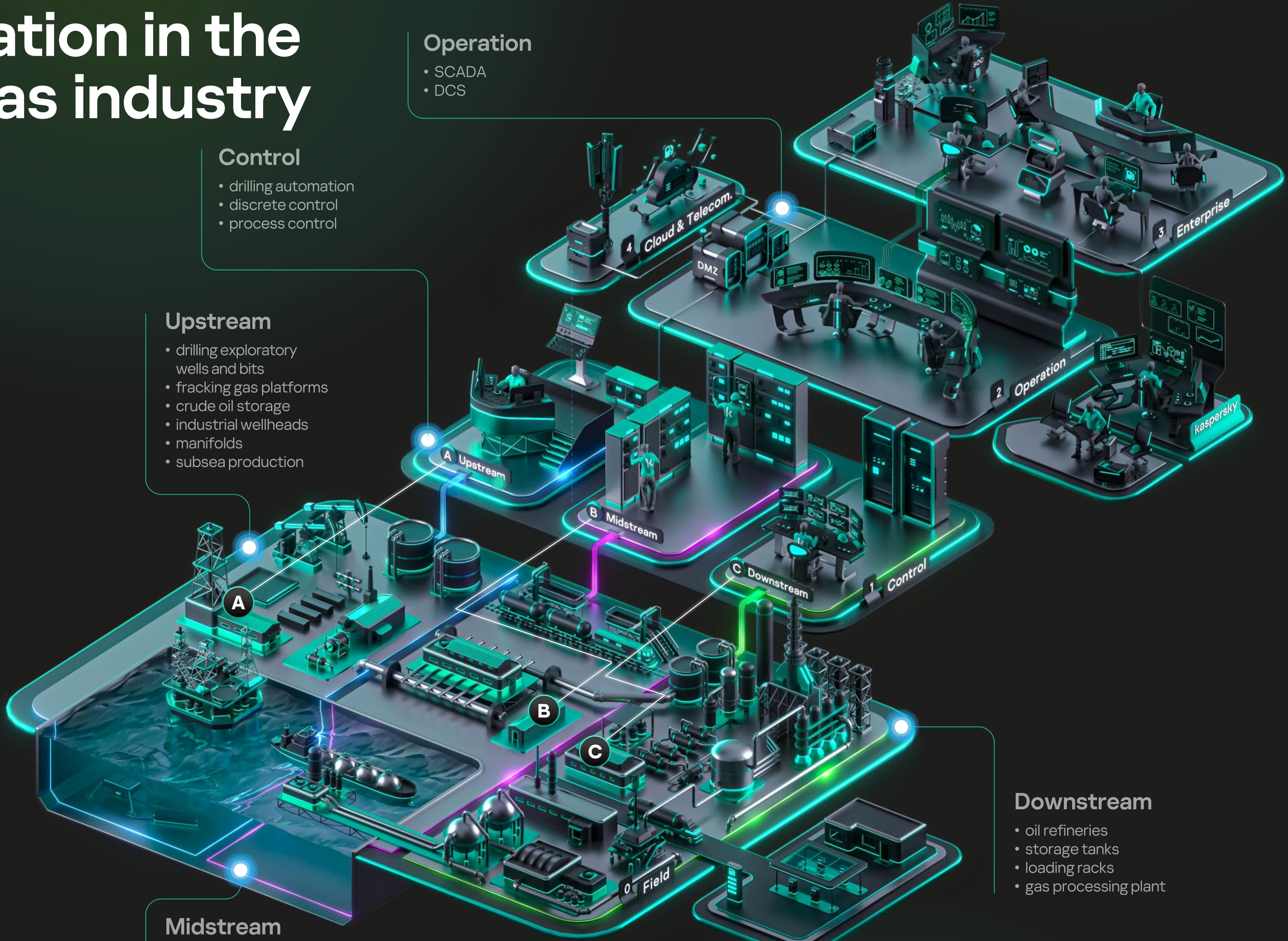
TATNEFT

TOP-5 largest O&G companies in the country

SIA VARS

The only petrochemical terminal in the Baltic region

Digitalization in the oil and gas industry



Operation

- SCADA
- DCS

Control

- drilling automation
- discrete control
- process control

Upstream

- drilling exploratory wells and bits
- fracking gas platforms
- crude oil storage
- industrial wellheads
- manifolds
- subsea production

Midstream

- pipelines
- LNG and oil tanker ships
- rail tank cars
- fluid compressors
- storage facilities

Downstream

- oil refineries
- storage tanks
- loading racks
- gas processing plant

Digitalization in the oil and gas industry

Digital transformation trends application

IIoT & Cloud

1. Seismic data acquisition and processing
2. Drilling optimization
3. Pipeline leak detection
4. Refineries monitoring
5. Routing optimization and warehouse monitoring

Industrial metaverse: AR, VR

1. Personnel training, collaboration, maintenance in virtual environments

Robotization and 5G

1. Unmanaged aerial and underwater robots for drilling inspection and work
2. Monitoring of pipeline condition in hard-to-reach places and data acquisition
3. Plants inspection and ability of quick shut down in case of an issue

Digital twins

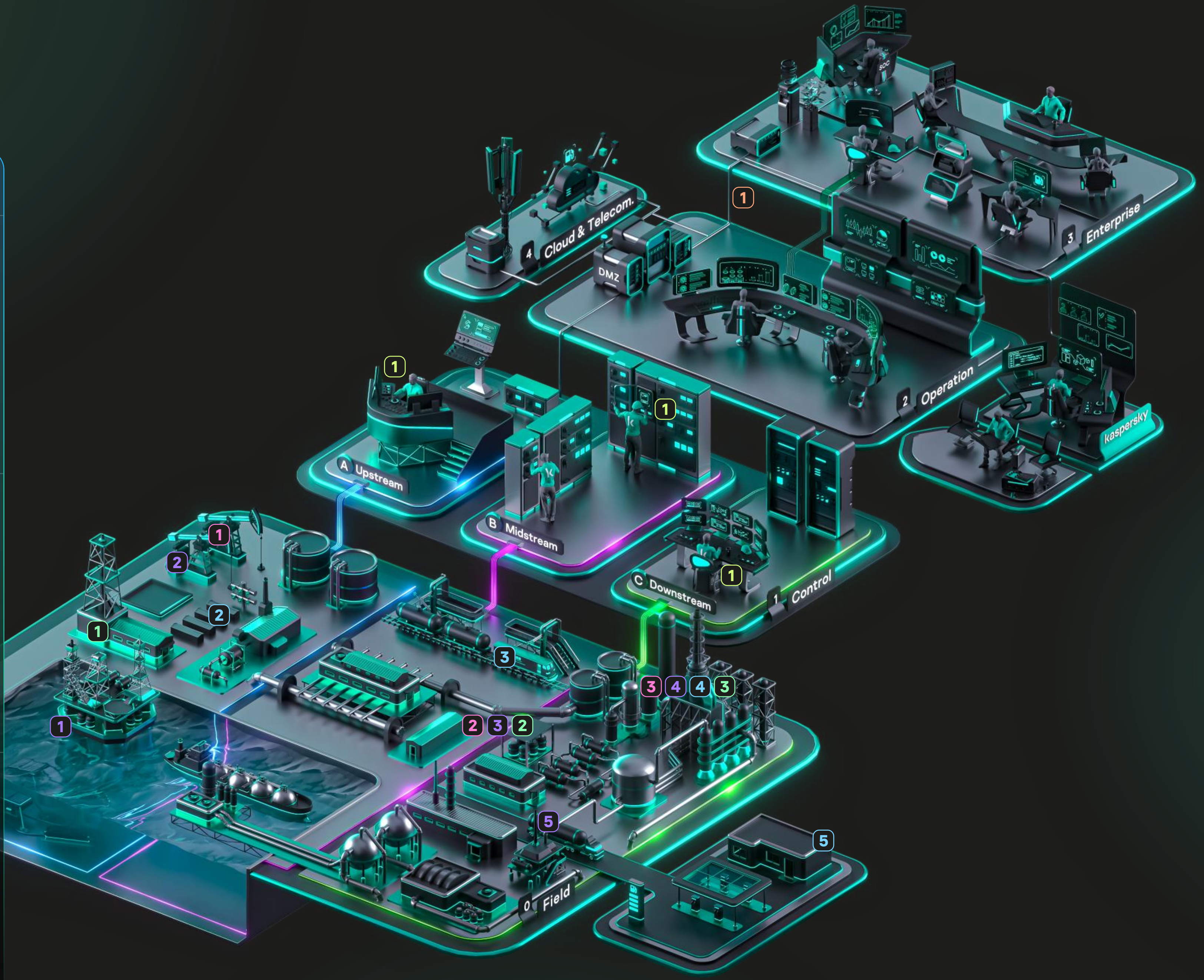
1. Modelling of drilling scenarios
2. Replicas of pipelines system for monitoring
3. Modelling oil refineries process to expose bottlenecks

Hyper automation, AI, ML, RPA

1. Locate and define drilling spots
2. Pump failures predictions
3. Data analytics of pipelines and transport
4. Refineries failures predictions
5. Customer demand forecasting

IT – OT convergence

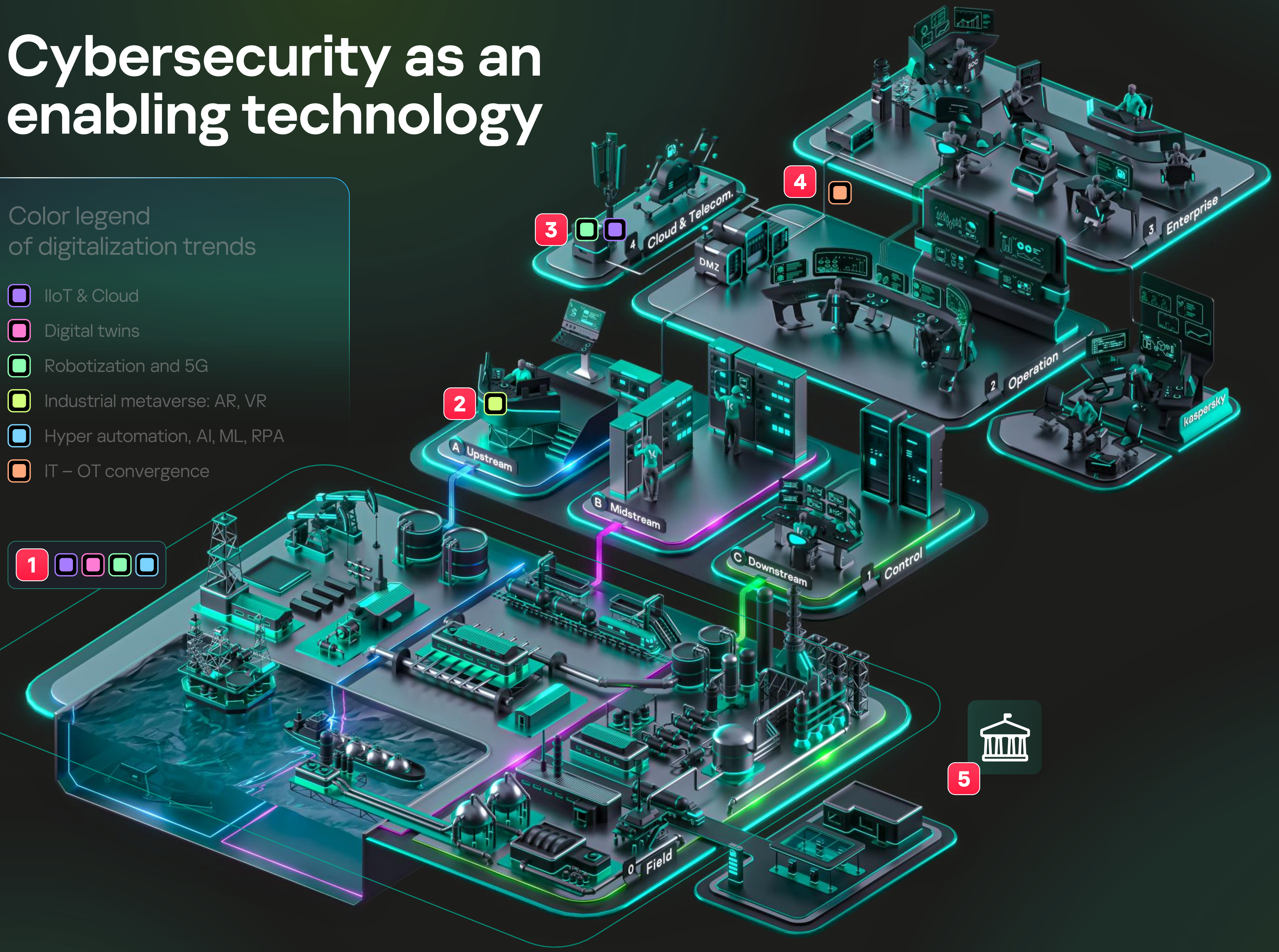
1. Interconnection of IT and OT networks and usage of IT hardware and software in OT



Cybersecurity as an enabling technology

Color legend of digitalization trends

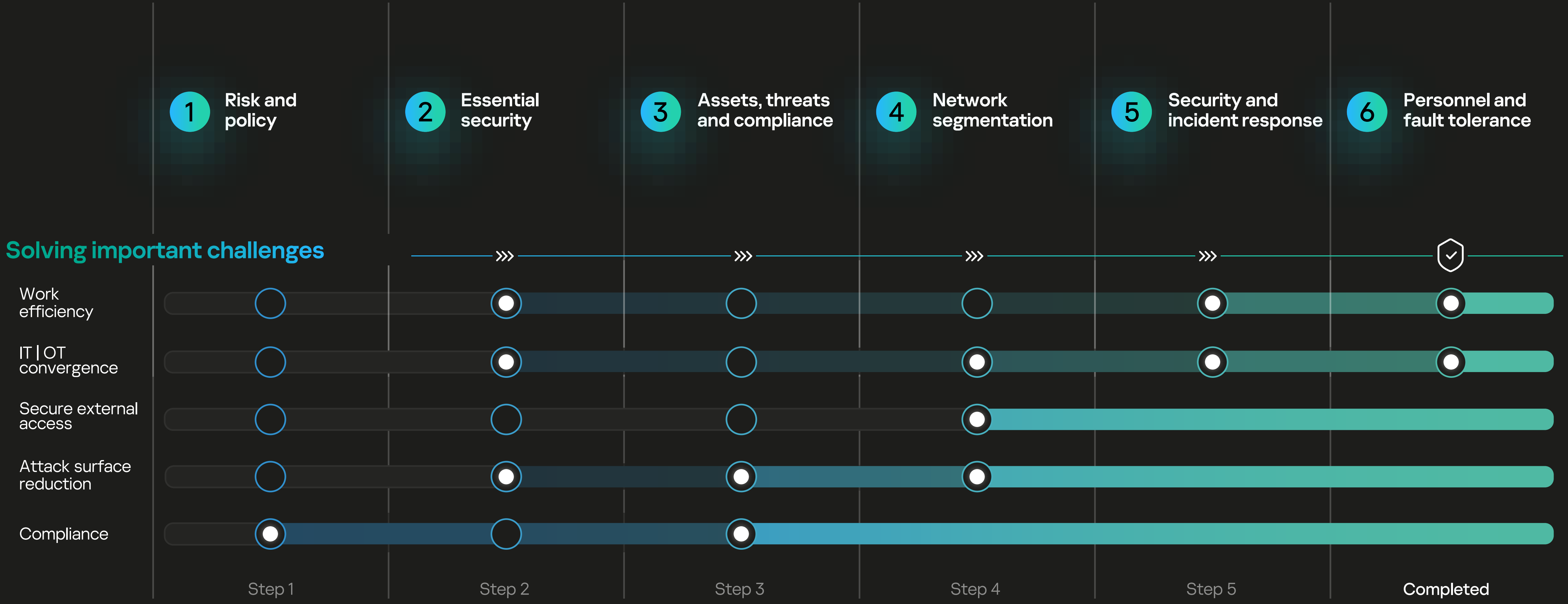
- 🟪 IloT & Cloud
- 🟥 Digital twins
- 🟩 Robotization and 5G
- 🟨 Industrial metaverse: AR, VR
- 🟦 Hyper automation, AI, ML, RPA
- 🟧 IT – OT convergence



At the same time, digital transformation in O&G industry goes hand in hand with security issues and challenges...

1. Attack surface expansion
2. Legacy infrastructure and uncontrolled connectivity
3. External access to OT infrastructure
4. Personnel deficit
5. CIP regulations compliance

Steps to secure your industrial enterprise



1 Risk and policy

2 Essential security

3 Assets, threats and compliance

4 Network segmentation

5 Security and incident response

6 Personnel and fault tolerance

Solving important challenges

	Step 1	Step 2	Step 3	Step 4	Step 5	Completed
Work efficiency	○	●	○	○	●	●
IT | OT convergence	○	●	○	●	●	●
Secure external access	○	○	○	●		
Attack surface reduction	○	●	●	●		
Compliance	●	○	●			

Partner you can trust

27 years of world-class experience and petabytes of threat-related data

Proven efficacy and compliance with regulations and standards

Awarded leader in IT/OT cybersecurity

Compatibility with 200+ automation systems is certified by 70 vendors

ICS CERT

Own international ICS CERT – center of ICS and IoT expertise

Customers around the world

- ROSATOM
- NORNICKEL
- Severstal
- NLMK
- KAMAZ
- TATNEFT
- EUROCHEM
- alperia
- РЖД
- КазМунайГаз
- PacificLight
- ROSSETI

kaspersky

Learn more about OT Ecosystem

Learn more about IT Ecosystem

Contact us