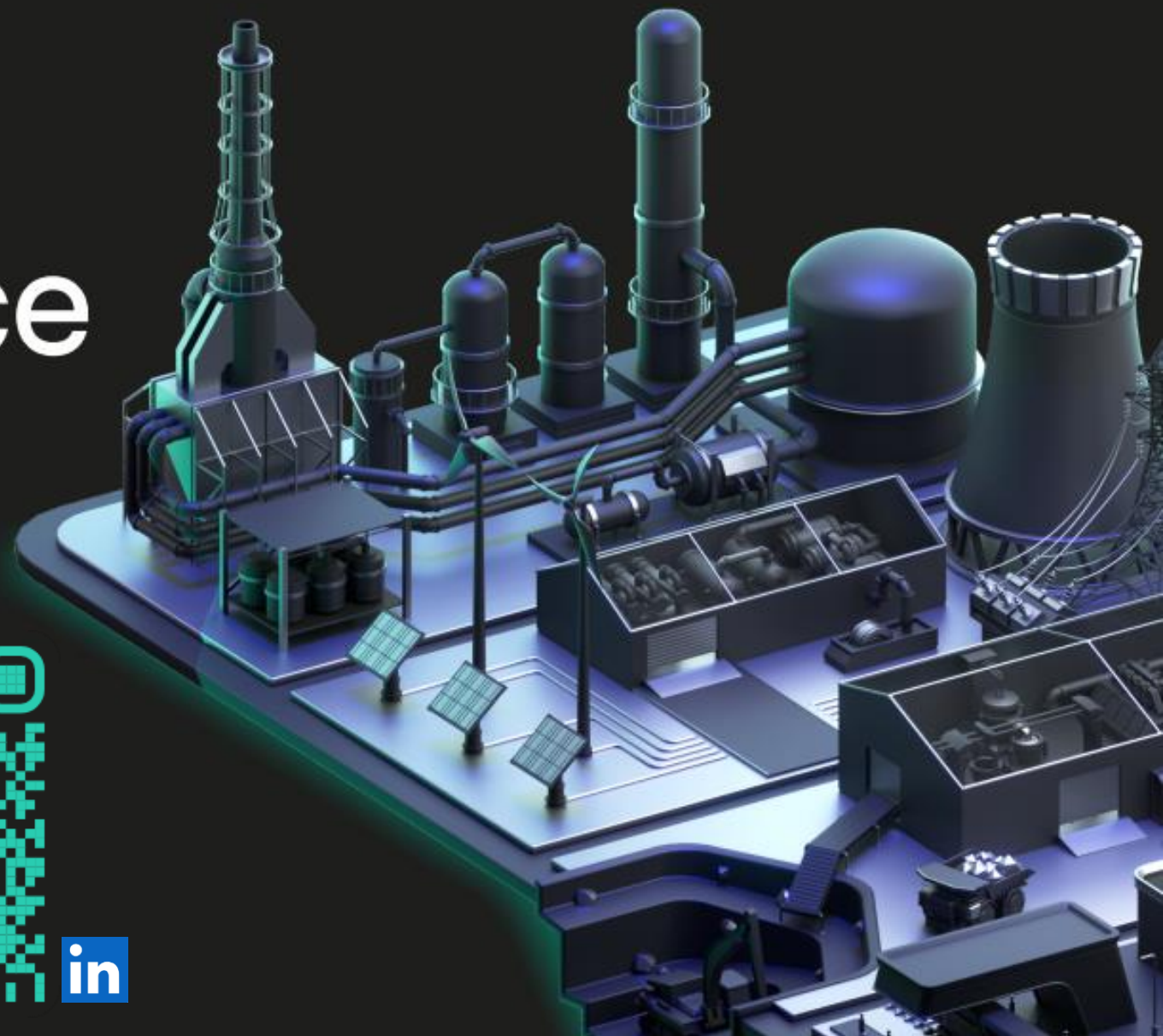
Eight steps to industrial cyber resilience



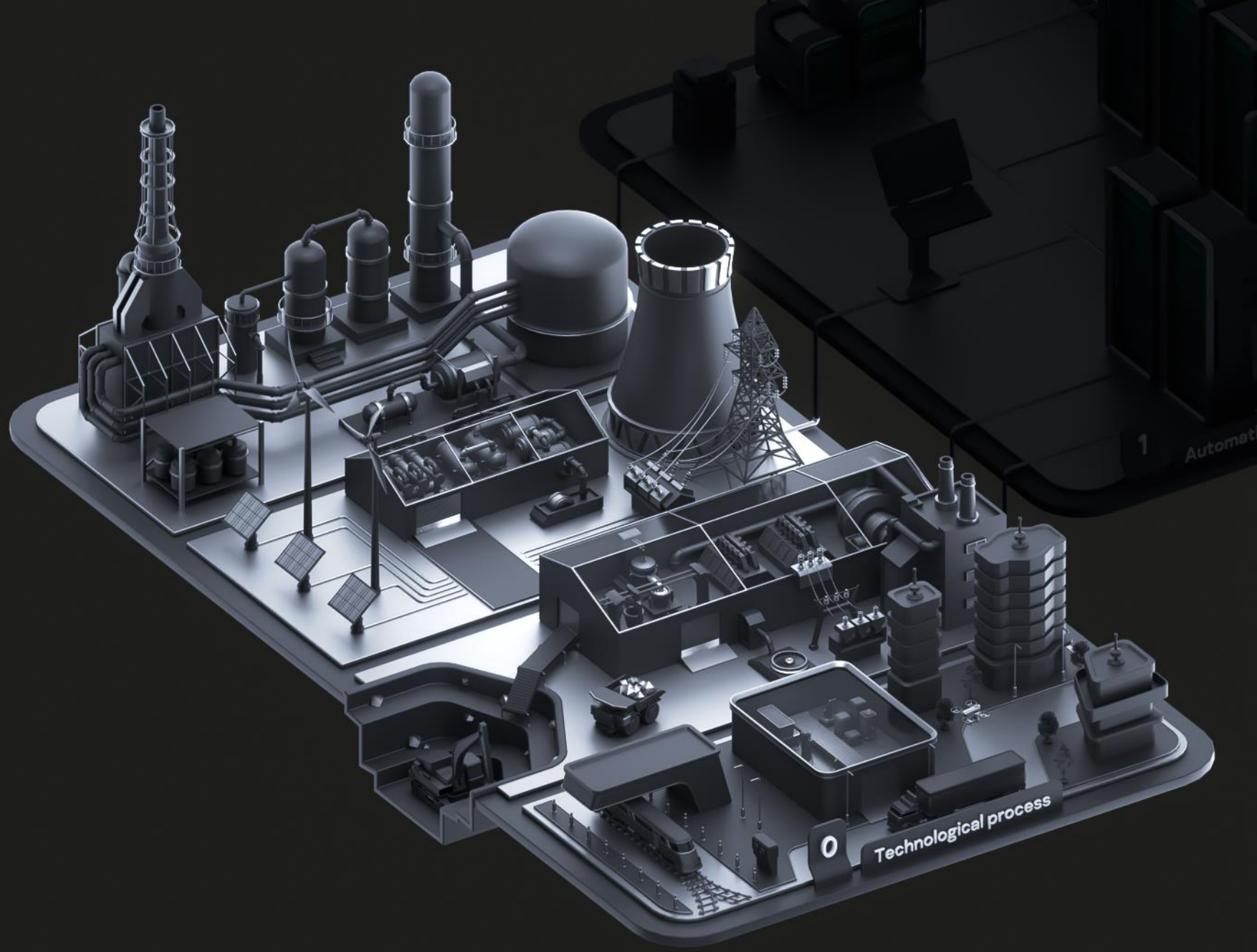
Kaspersky
OT CyberSecurity

Kirill Naboyshchikov
Product Marketing Director

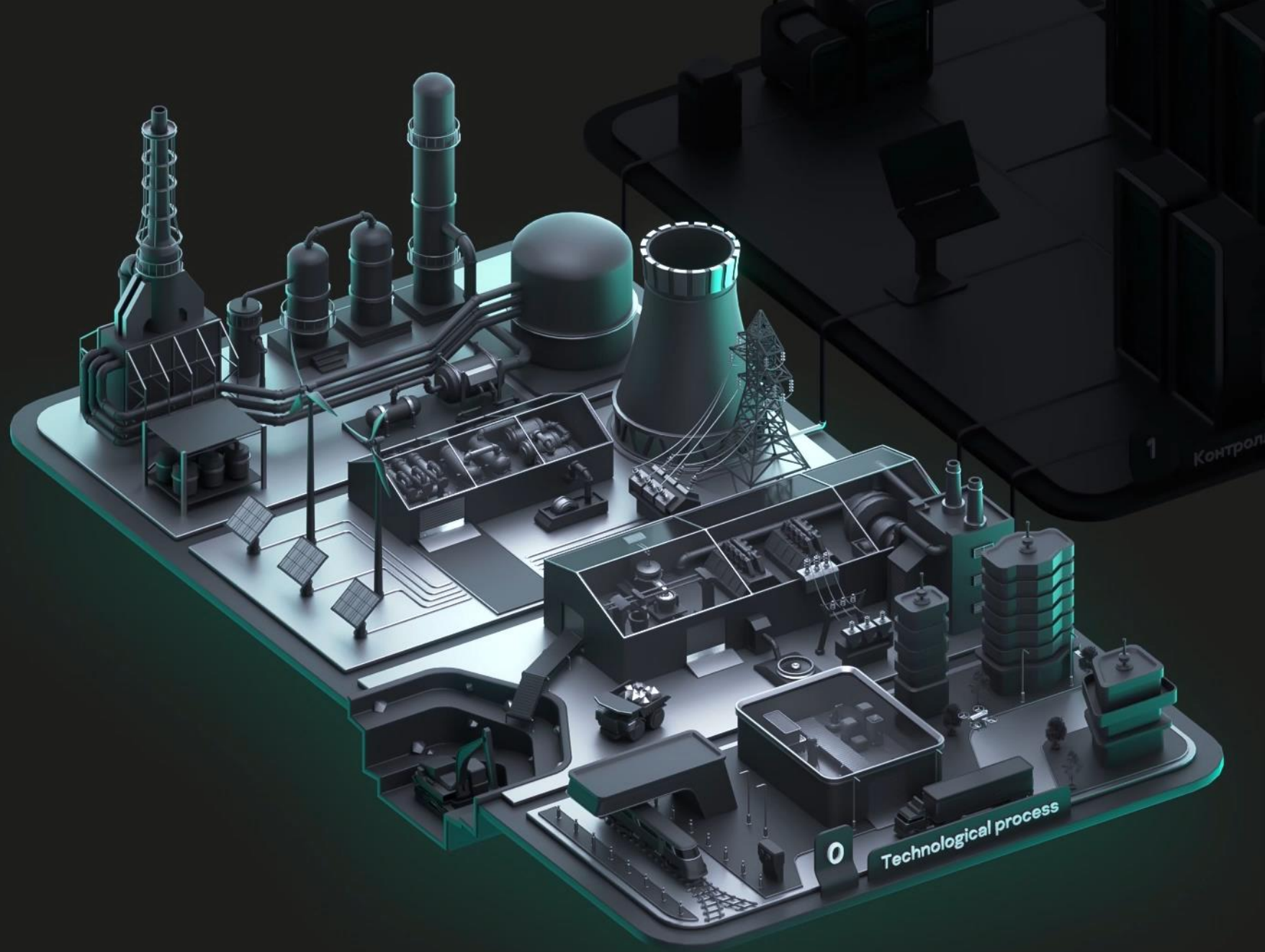
kaspersky bring on the future

Industrial enterprise

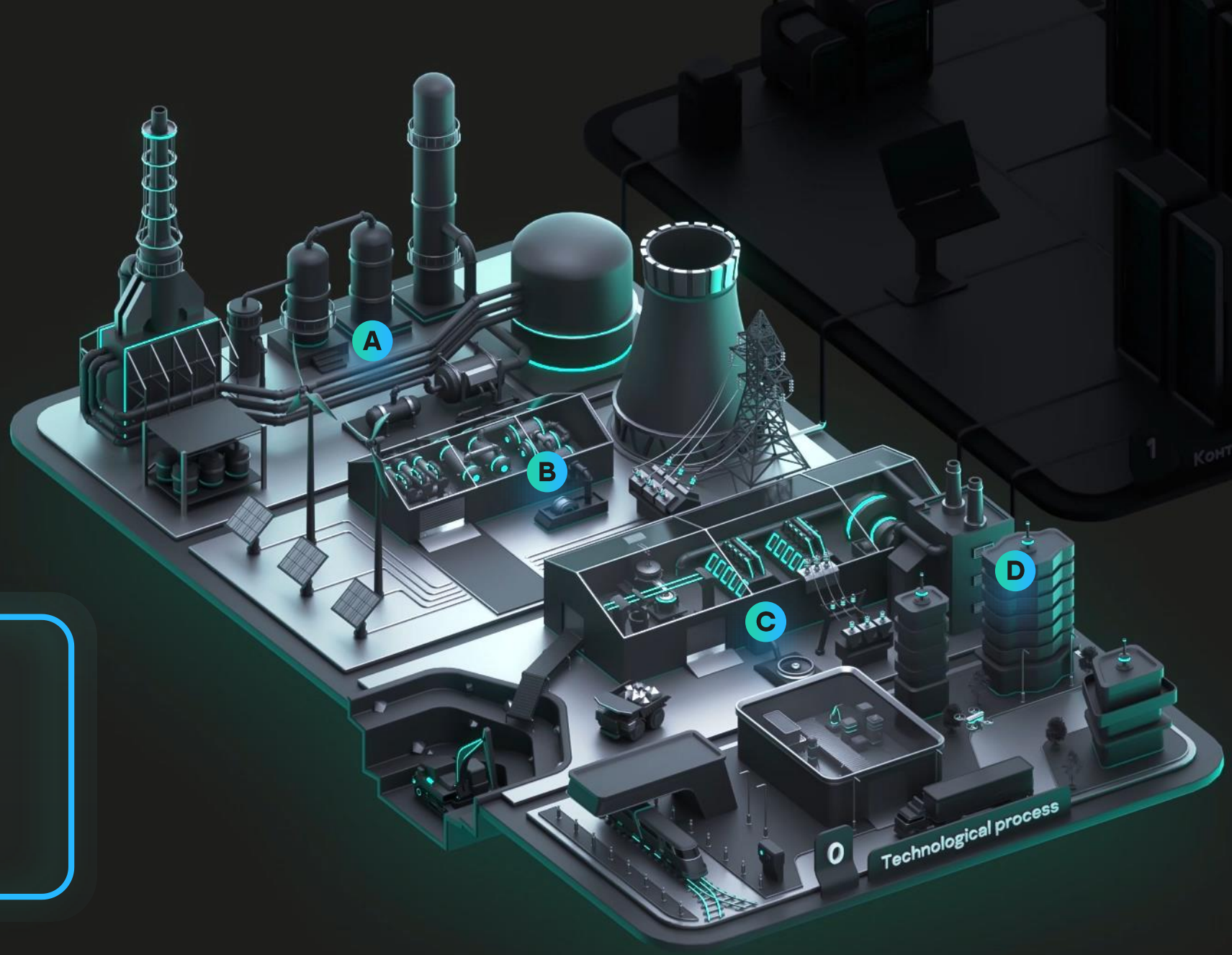
Industrial enterprise



Industrial enterprise



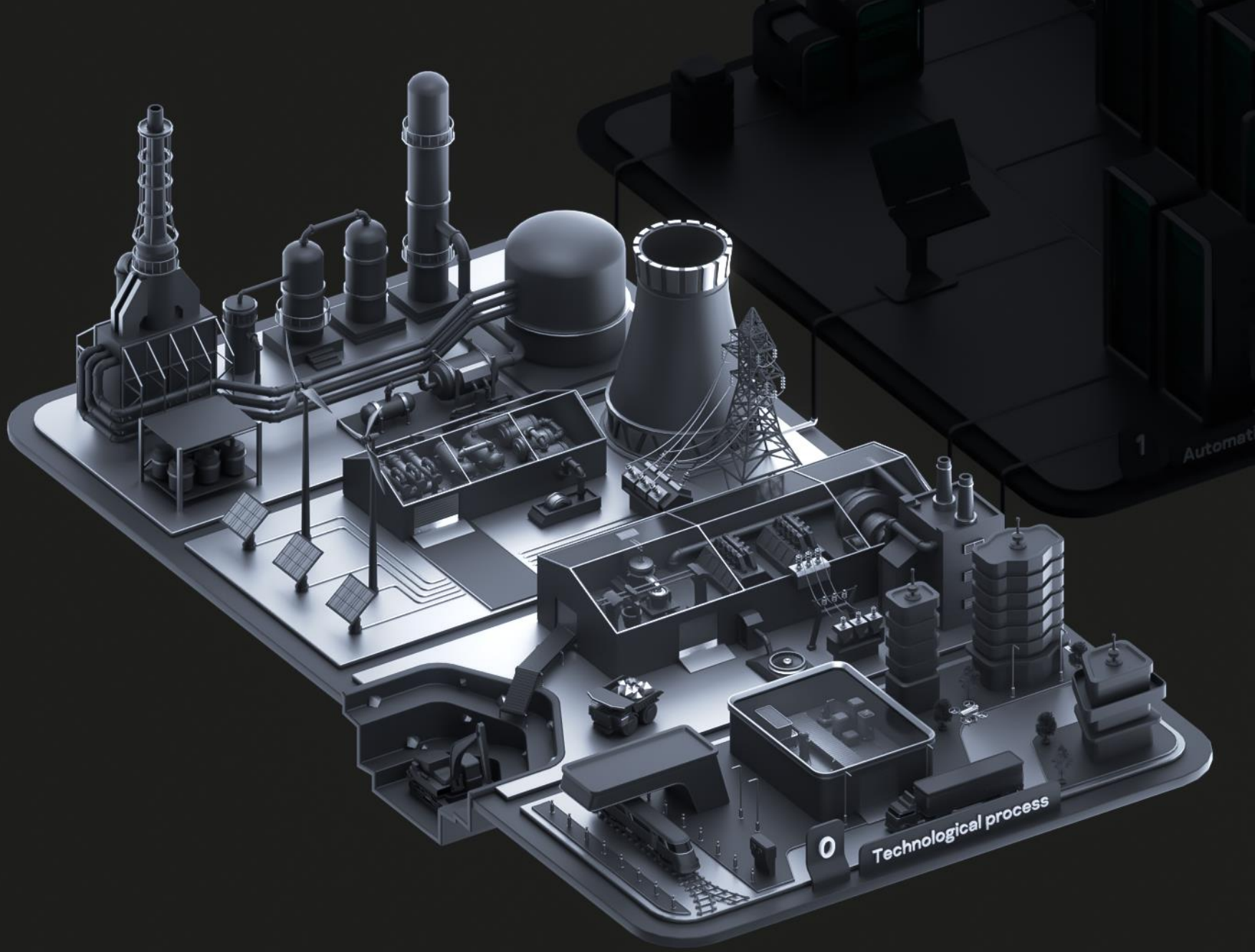
Industrial enterprise



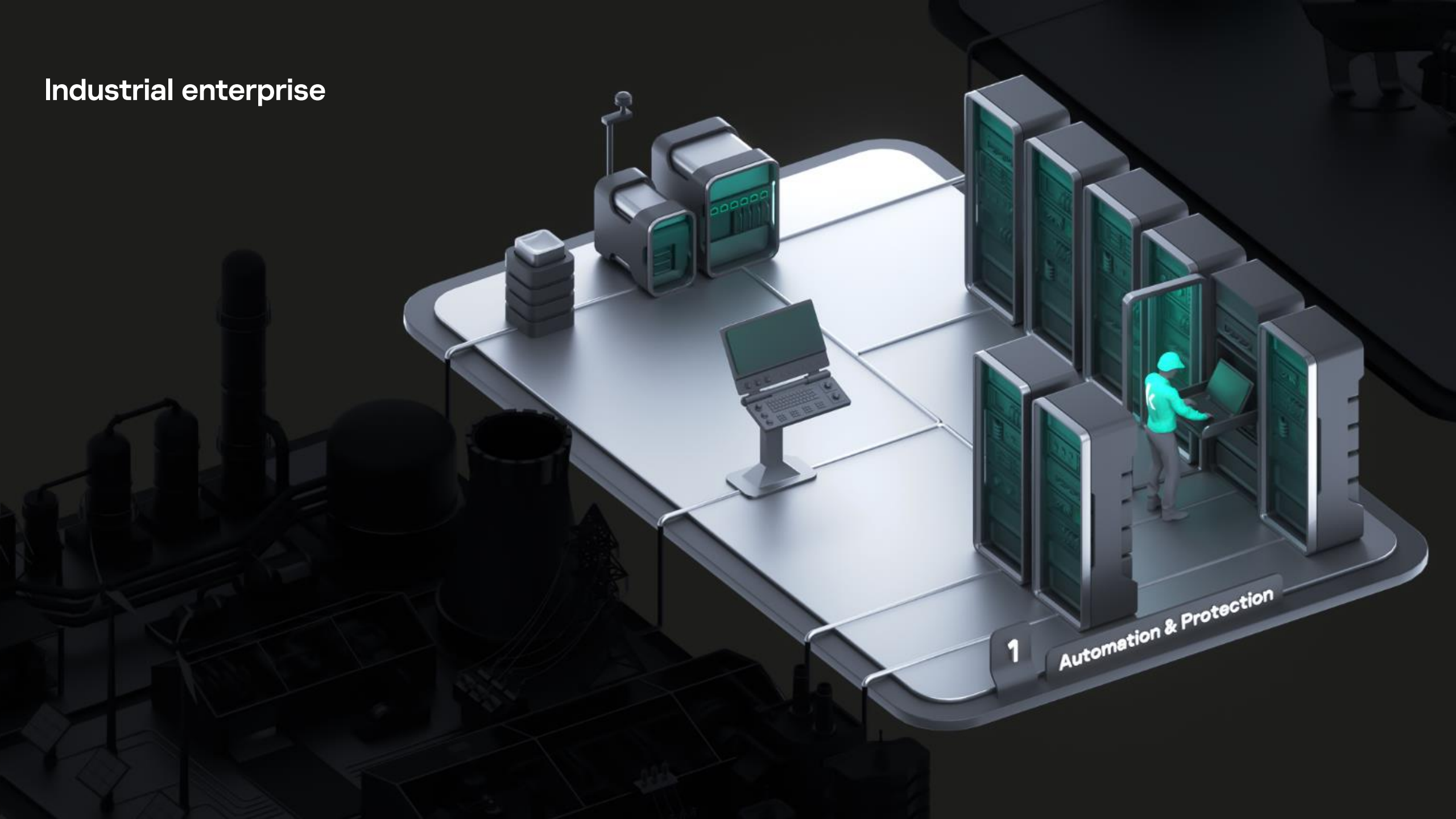
Technological process

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

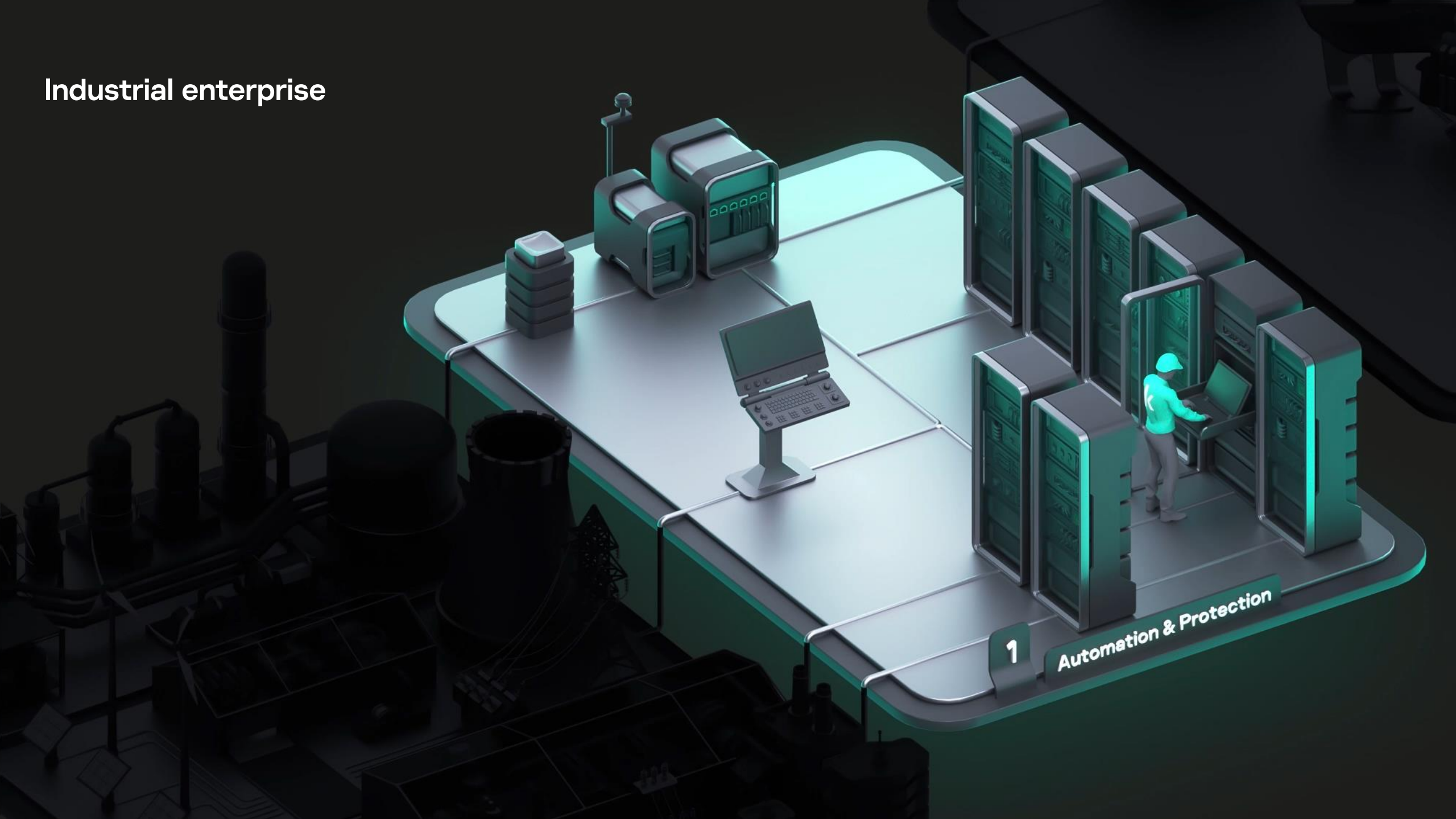
Industrial enterprise



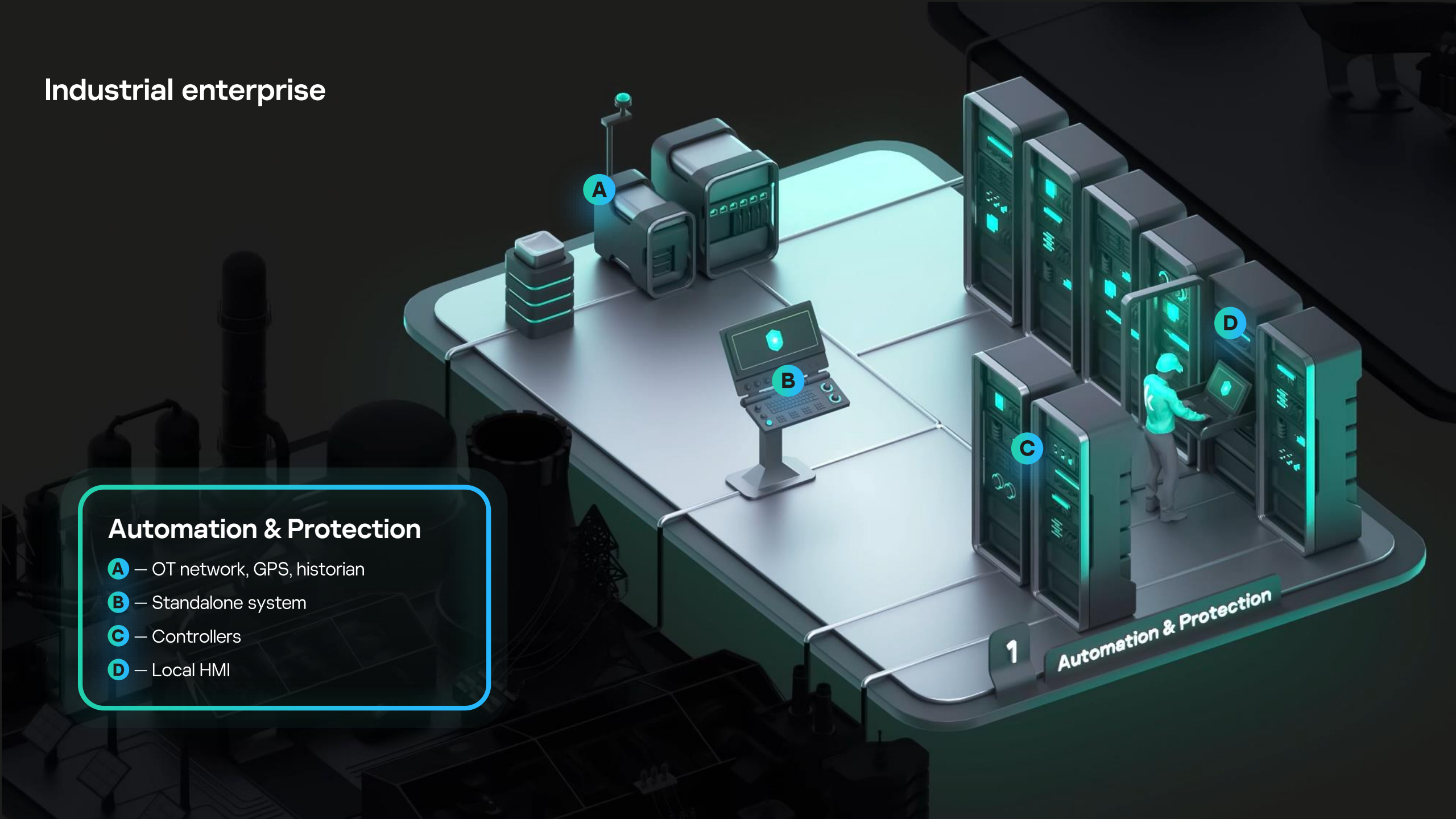
Industrial enterprise



Industrial enterprise



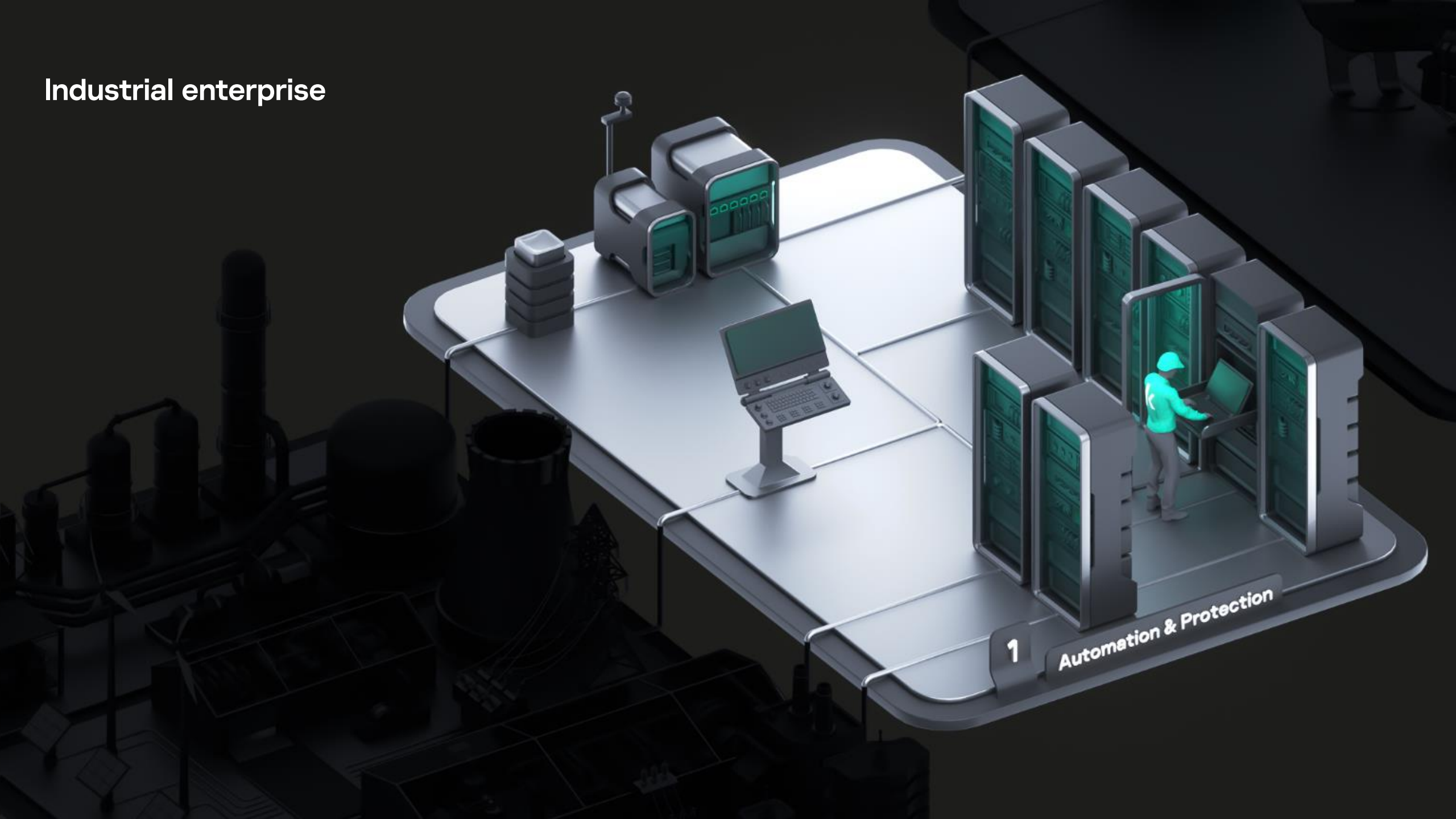
Industrial enterprise



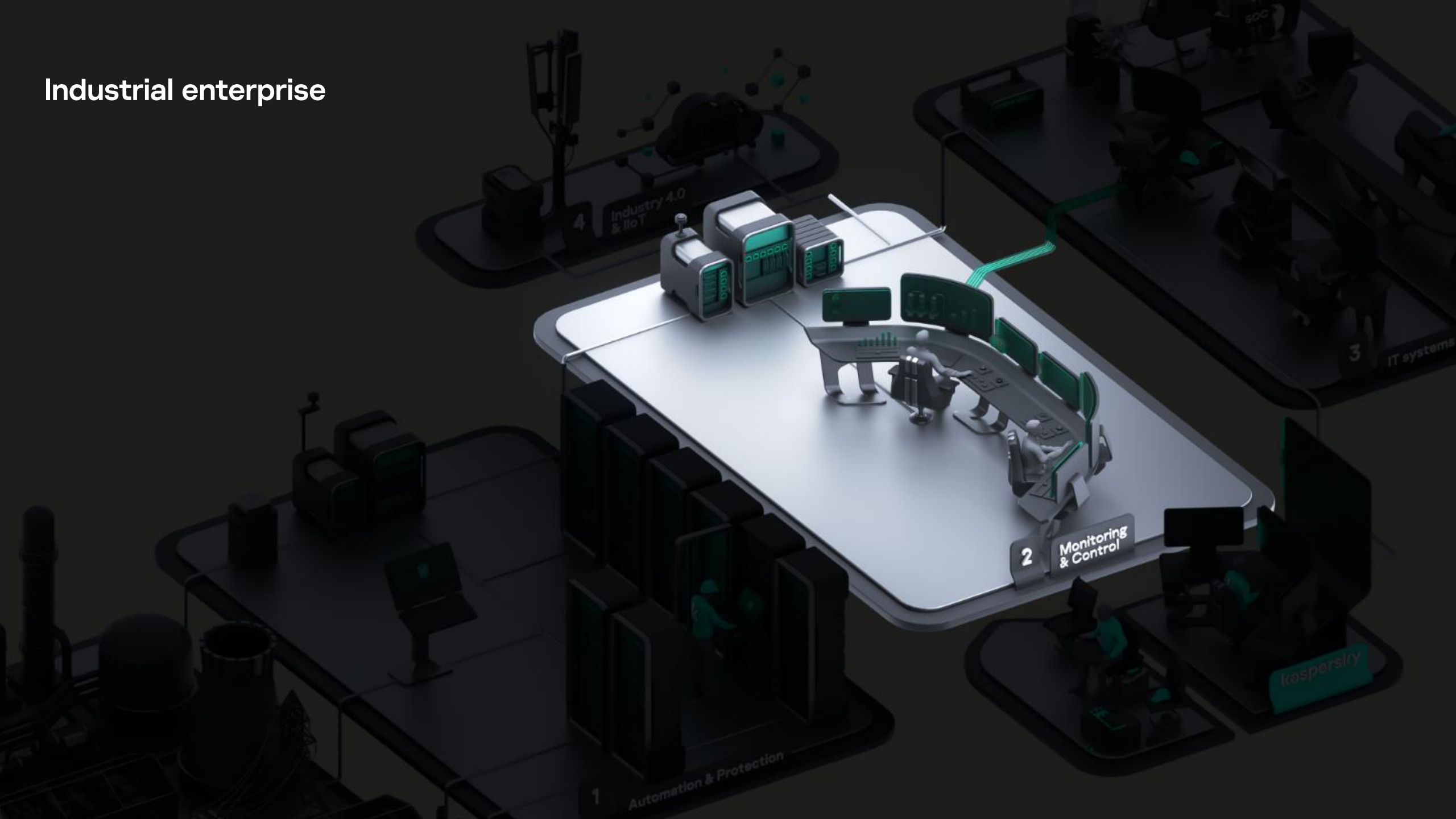
Automation & Protection

- A — OT network, GPS, historian
- B — Standalone system
- C — Controllers
- D — Local HMI

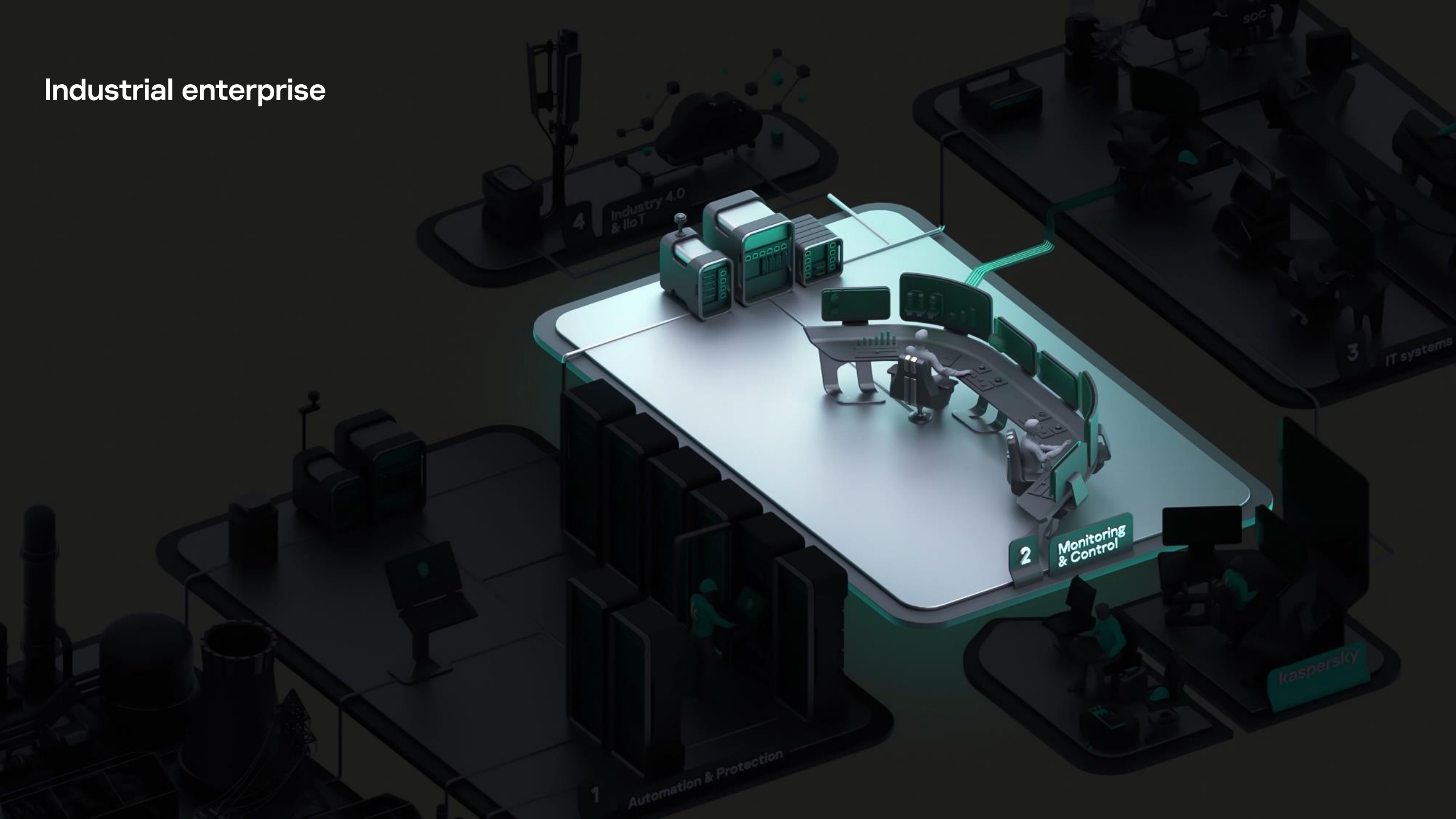
Industrial enterprise



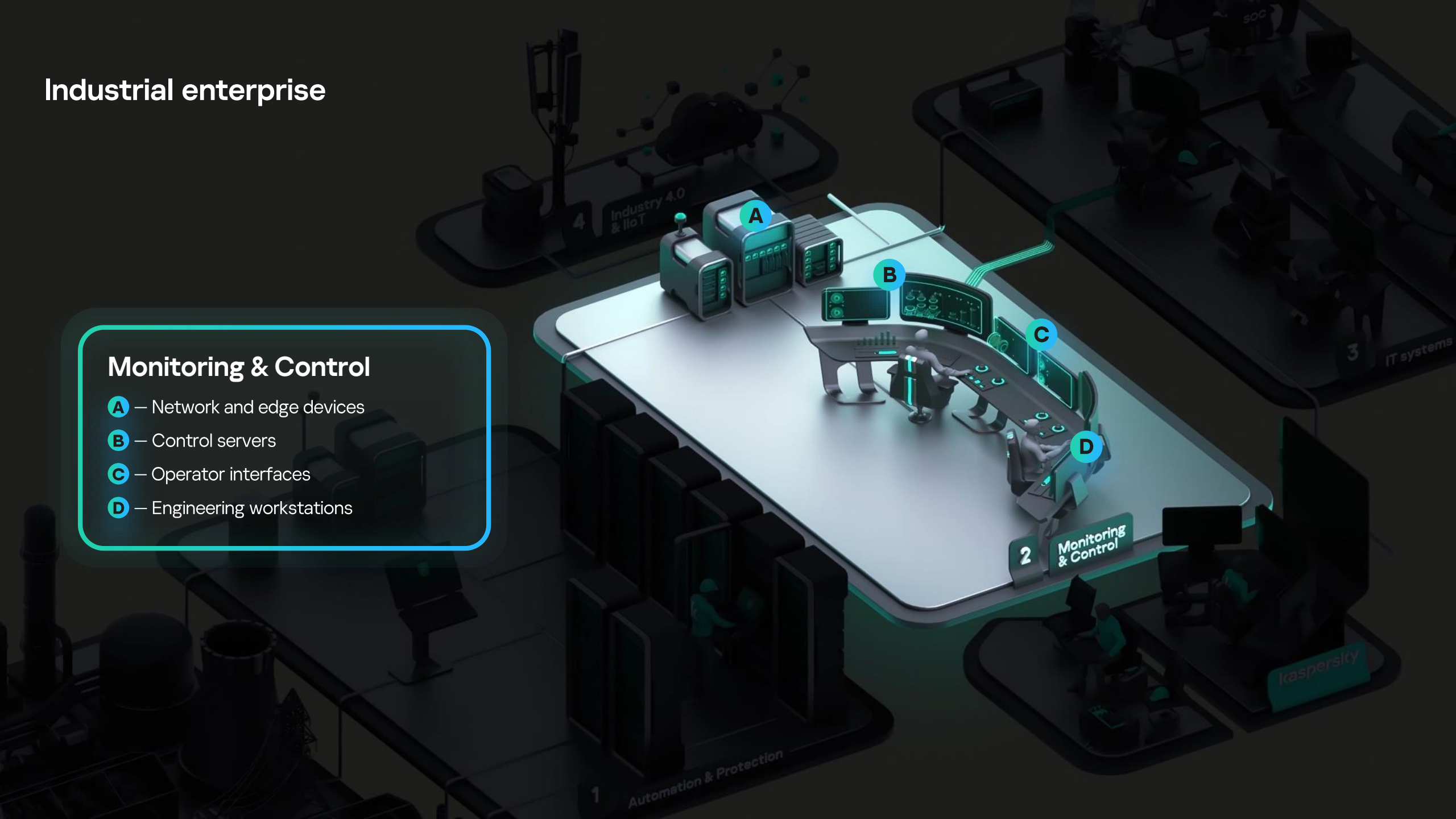
Industrial enterprise



Industrial enterprise



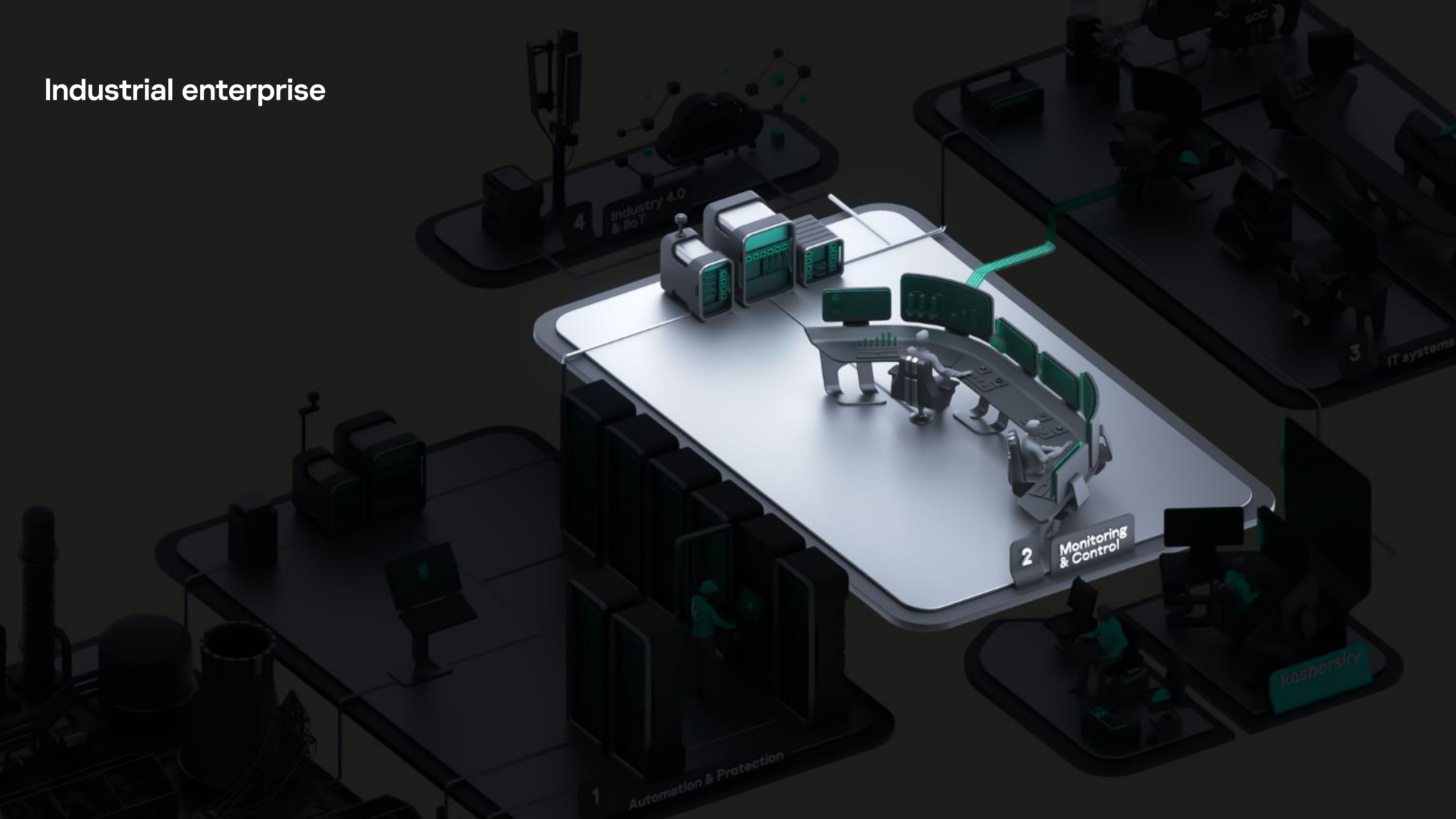
Industrial enterprise



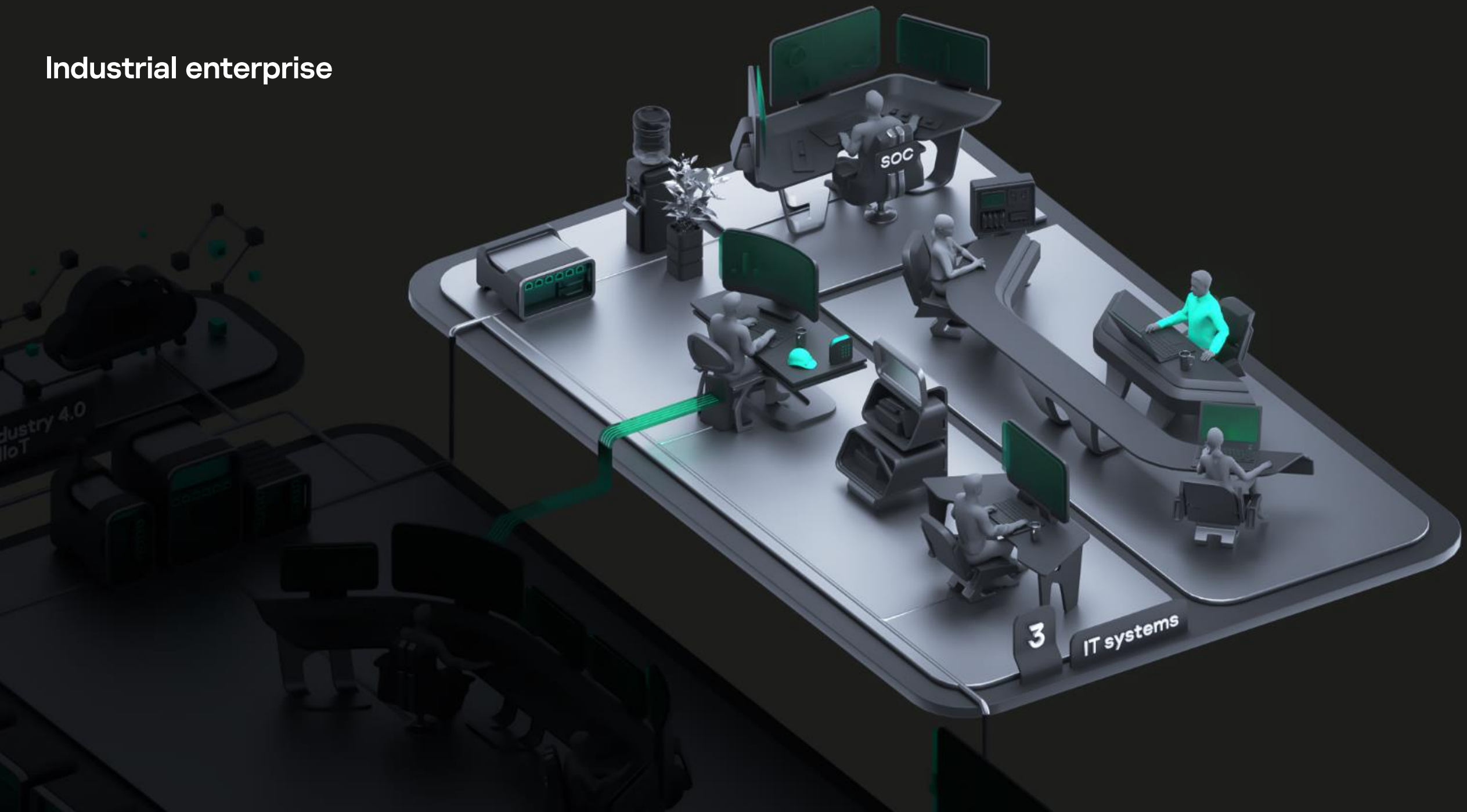
Monitoring & Control

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

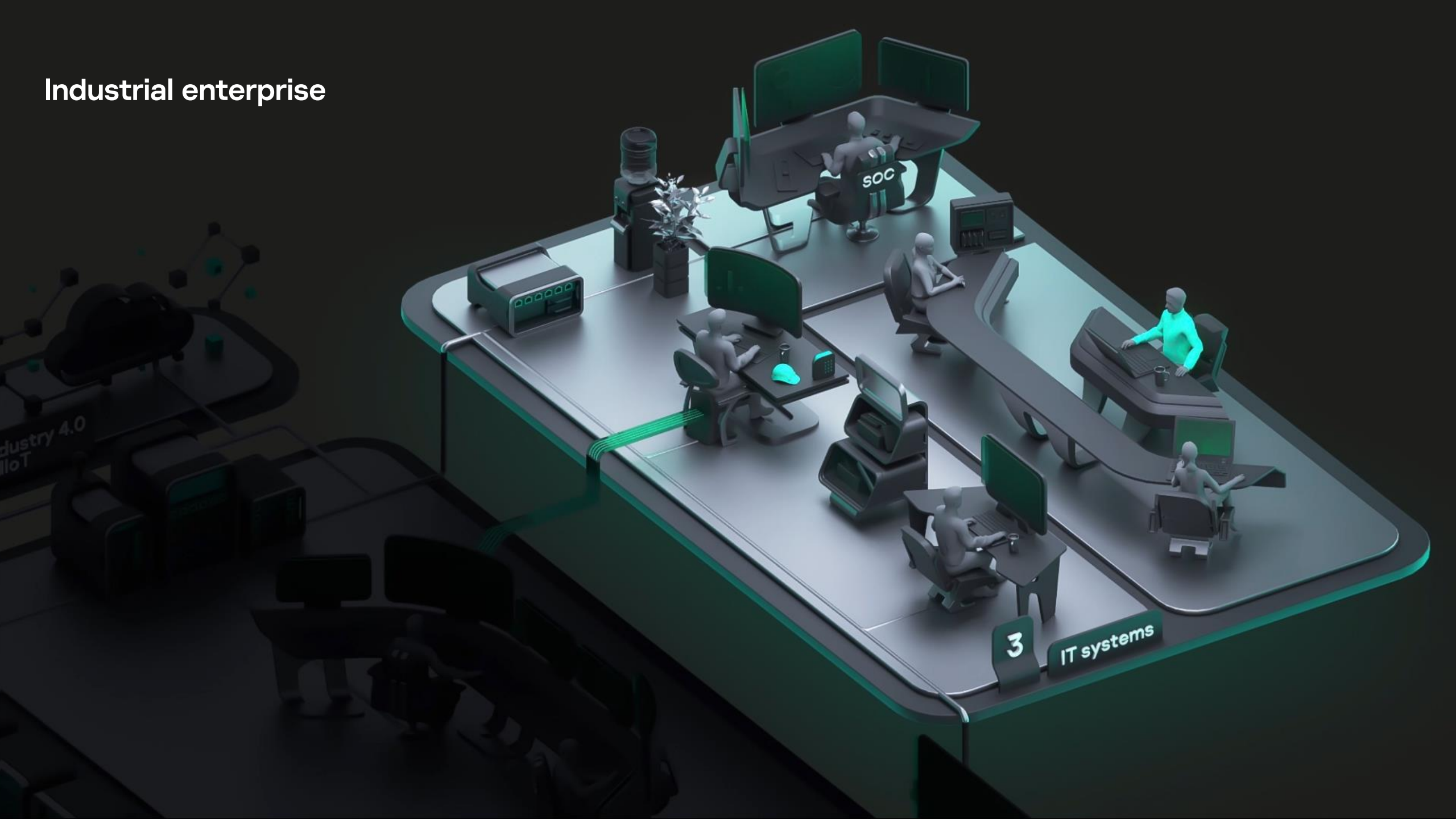
Industrial enterprise



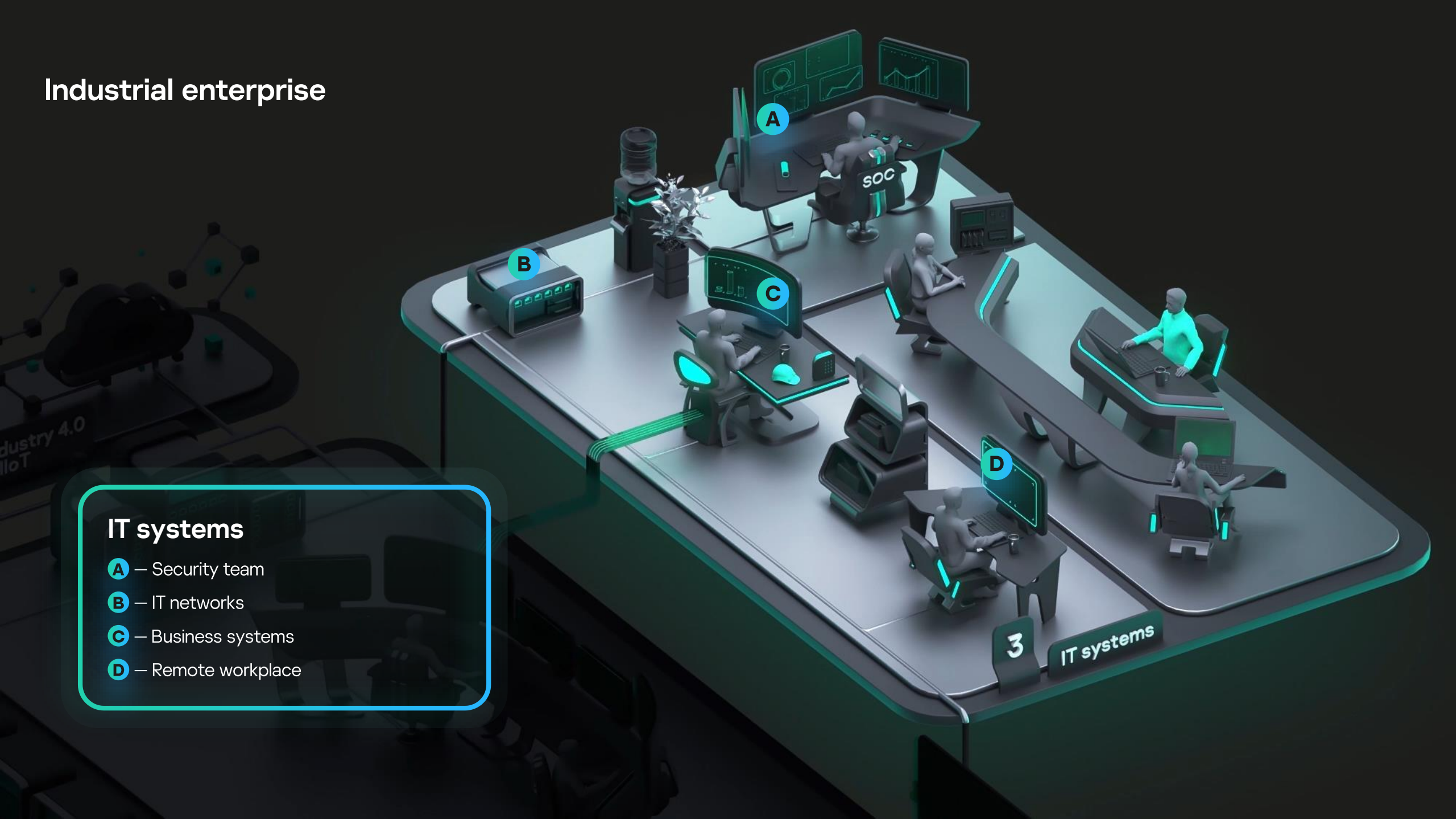
Industrial enterprise



Industrial enterprise



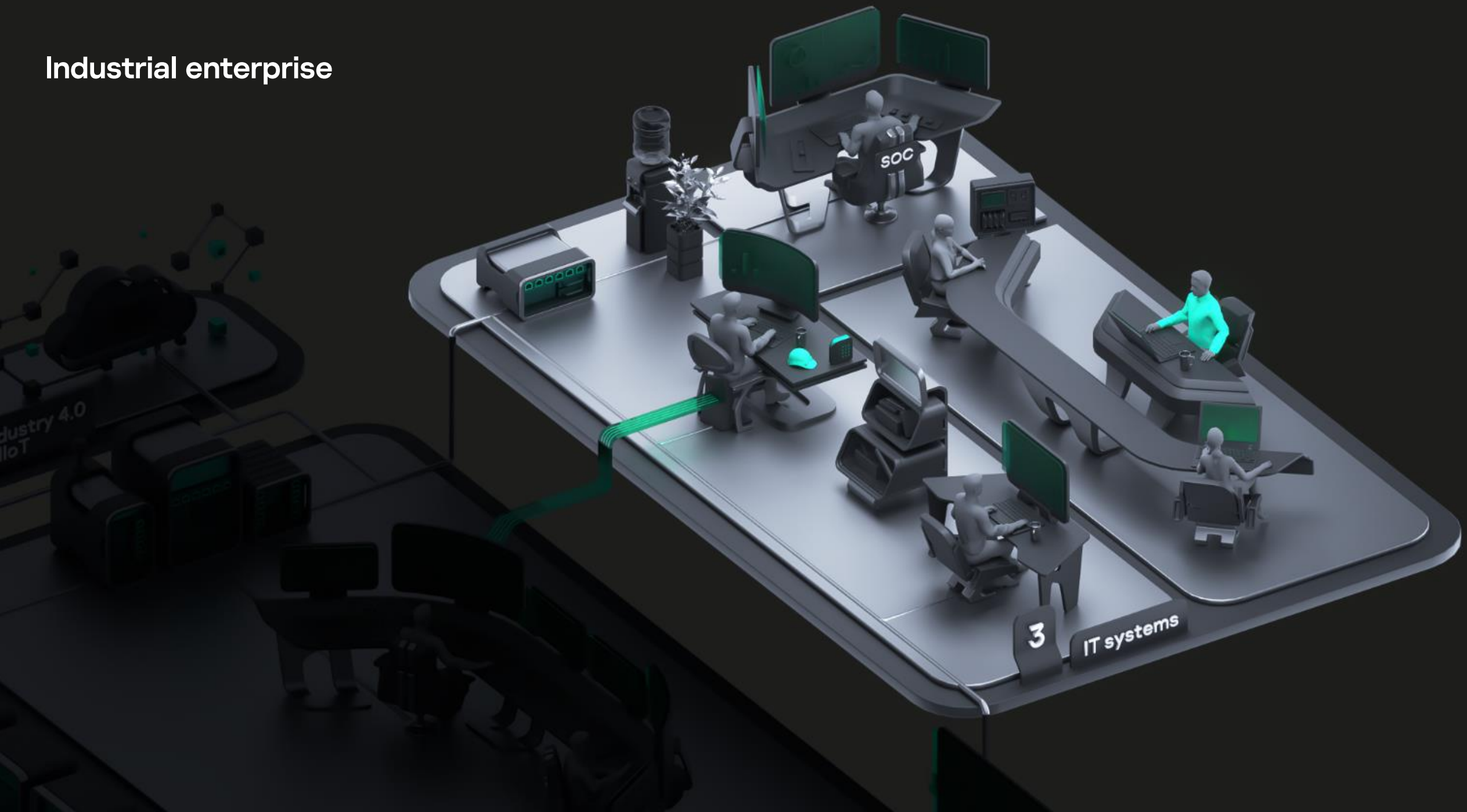
Industrial enterprise



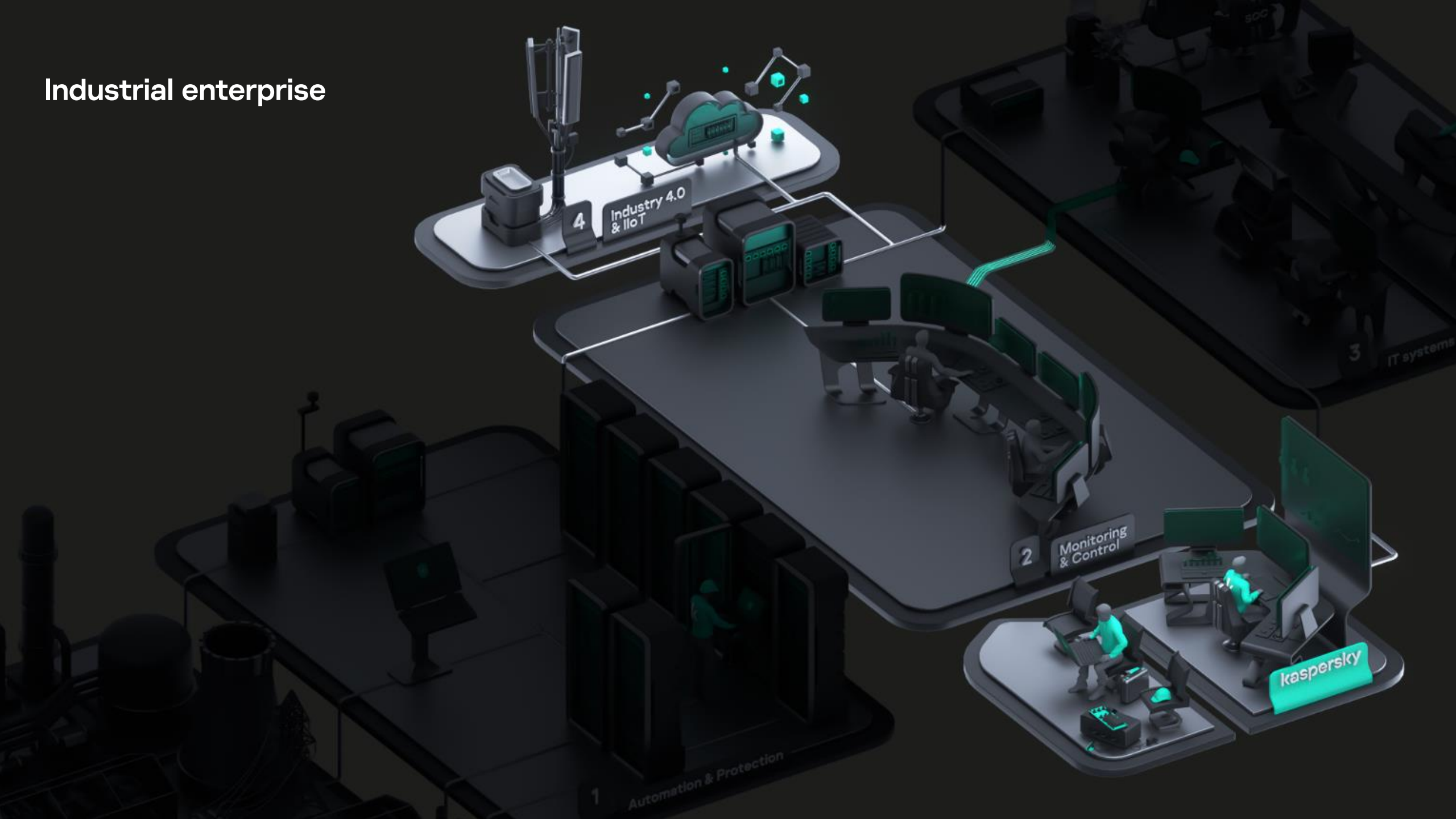
IT systems

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

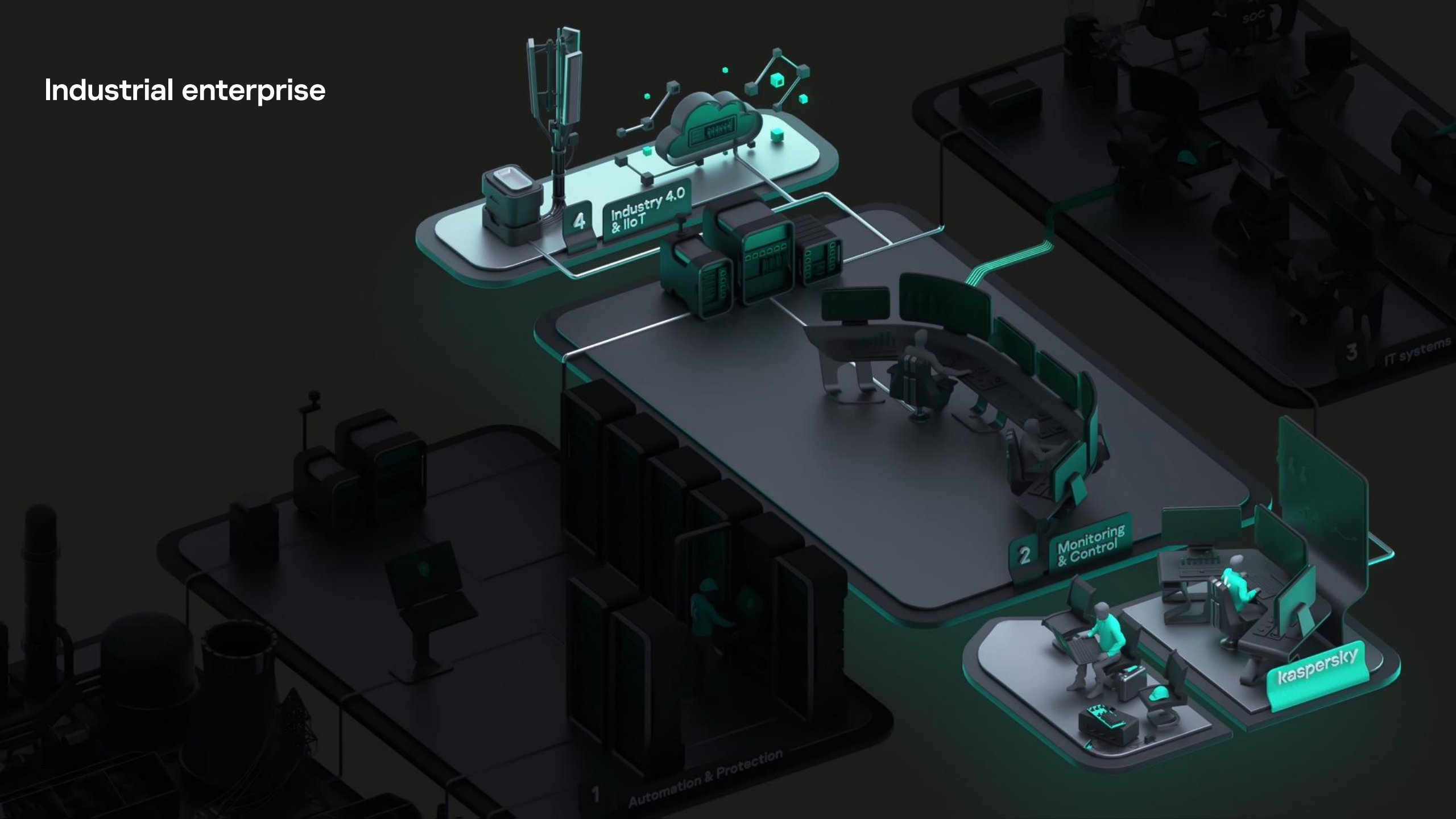
Industrial enterprise



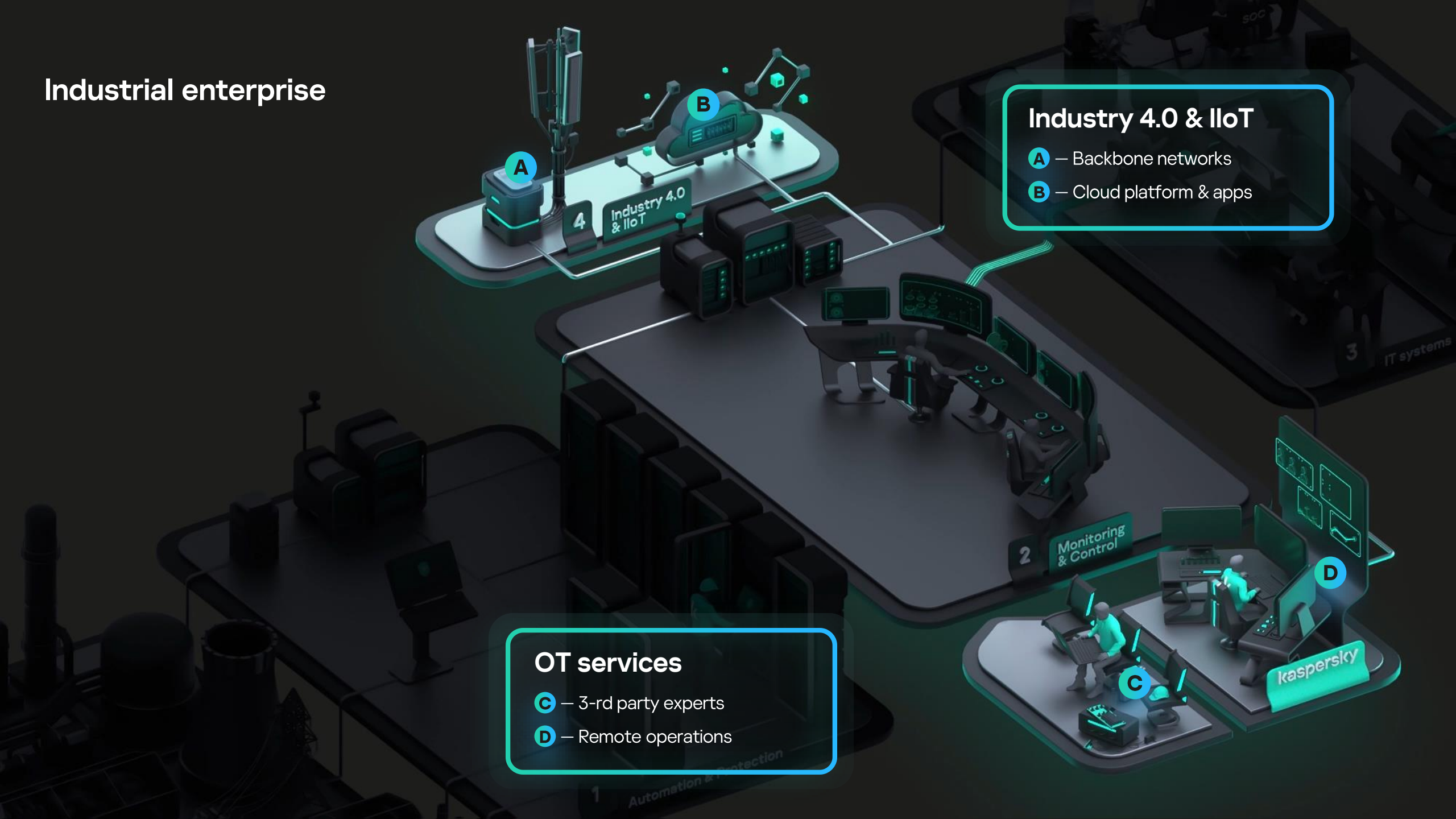
Industrial enterprise



Industrial enterprise



Industrial enterprise



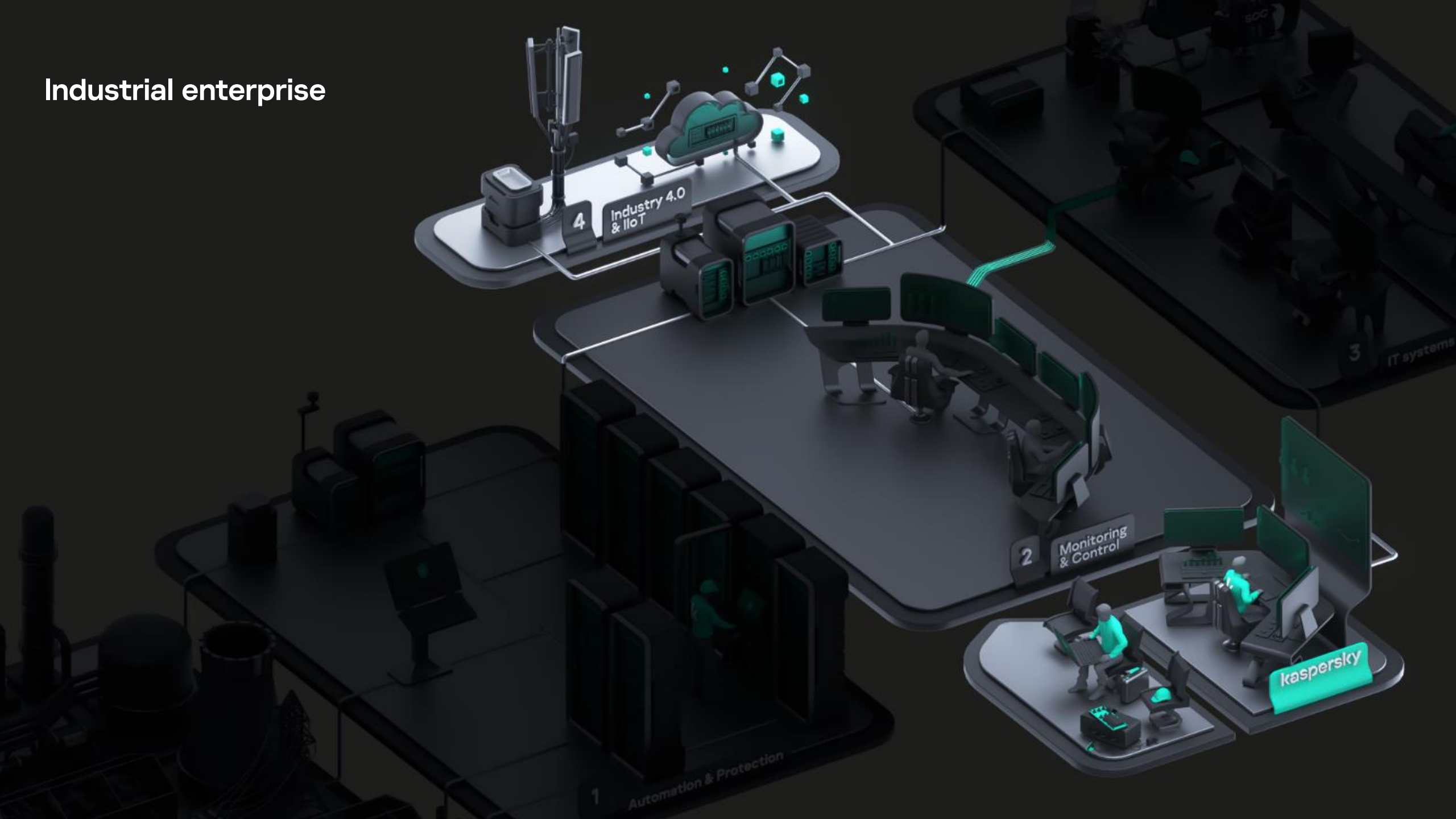
Industry 4.0 & IIoT

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

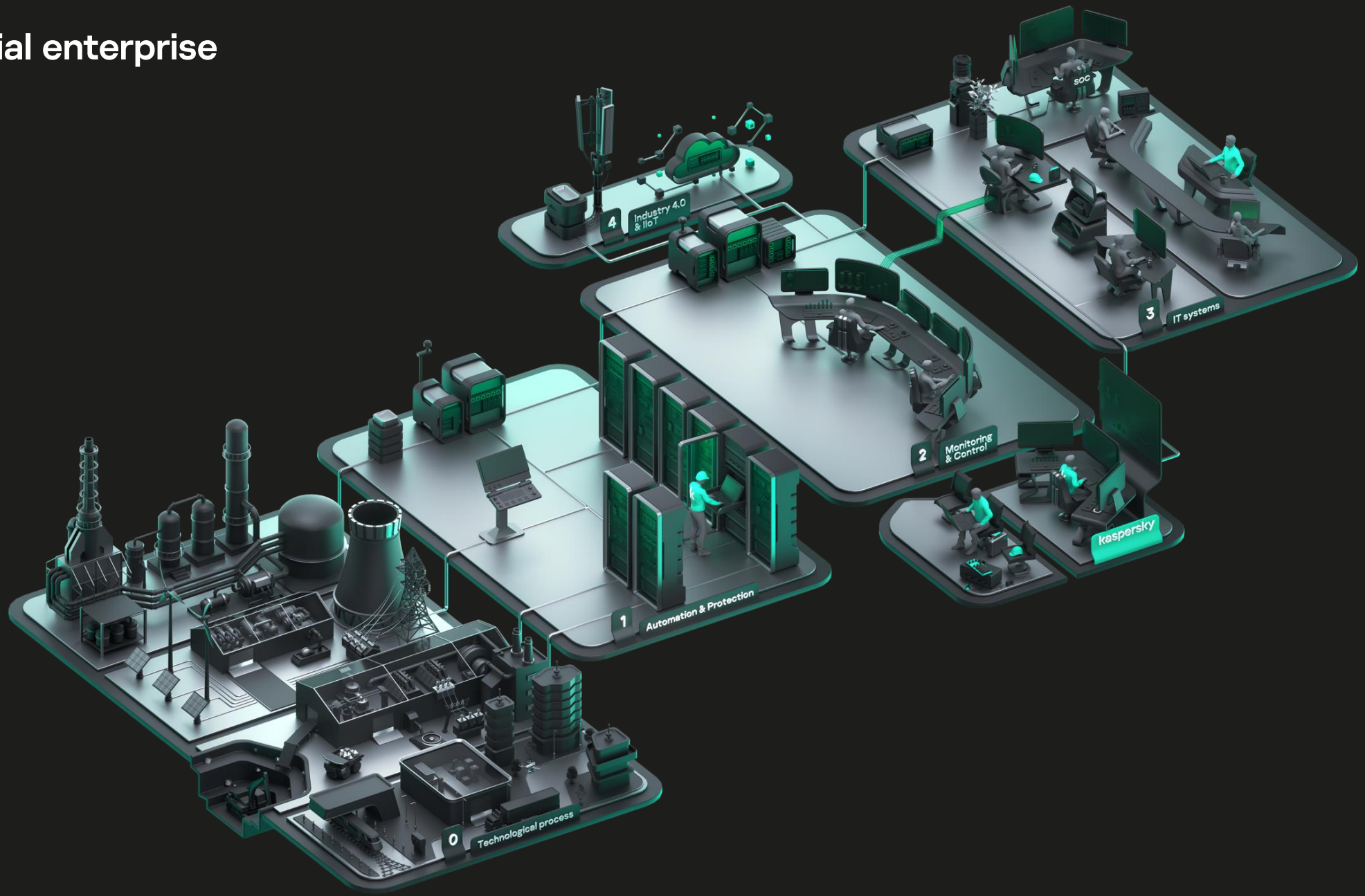
OT services

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

Industrial enterprise



Industrial enterprise



Yesterday

Security by obscurity

Airgap, reactive approach,

basic

security measures borrowed from IT

Spec

designe

Inc

produc

Today

Specialized platforms

designed and tested for OT.

Industrial grade

product for Critical Infrastructure Protection

Bring on the future

e

otection

IT – OT convergence

ecosystem of natively integrated

technologies, knowledge and expertise for Cyber-Physical Systems protection

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 IEC 62443-4-1

Prove the **efficacy** and **safety** of its technologies

kaspersky

Kaspersky Industrial CyberSecurity

Key element – Native OT XDR platform

ics.kaspersky.com

Industrial Enterprise

Native OT XDR

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

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Networks

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

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

Kaspersky Industrial CyberSecurity for Nodes

- Endpoint Protection
- Endpoint Detection and Response
- Portable Scanner

XDR capabilities

kaspersky

Kaspersky OT CyberSecurity

Cyber-physical security ecosystem
for industrial enterprises

kaspersky.com/enterprise-security/industrial-solution

Kaspersky OT CyberSecurity

IT – OT Convergence

Kaspersky Next XDR Expert

Kaspersky Industrial CyberSecurity

Native XDR

for Nodes
Endpoint protection, detection and response

for Networks
Network traffic analysis, detection and response

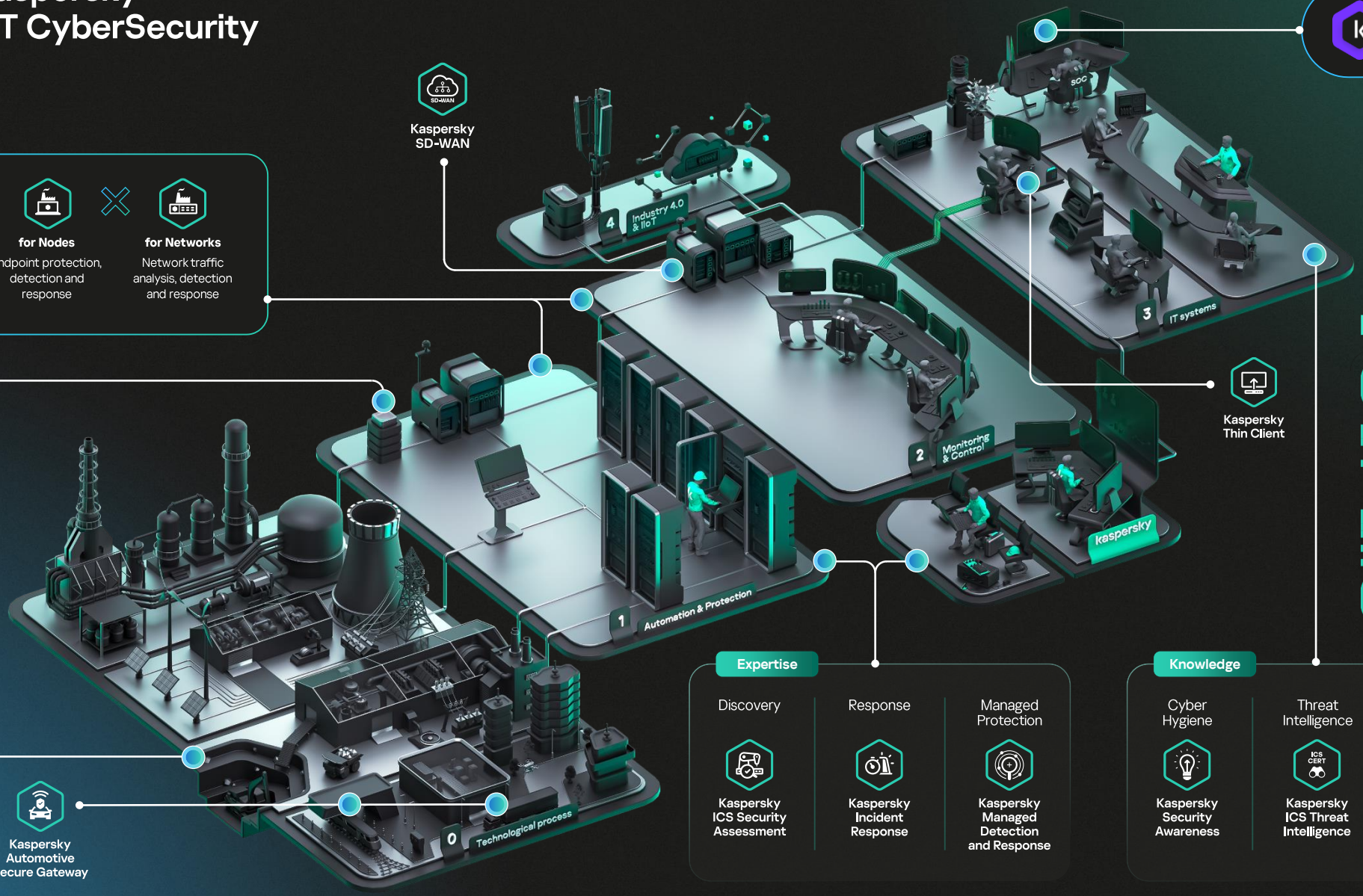
Kaspersky SD-WAN

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Thin Client

Kaspersky Antidrone

Kaspersky Automotive Secure Gateway



Expertise

Discovery	Response	Managed Protection
Kaspersky ICS Security Assessment	Kaspersky Incident Response	Kaspersky Managed Detection and Response

Knowledge

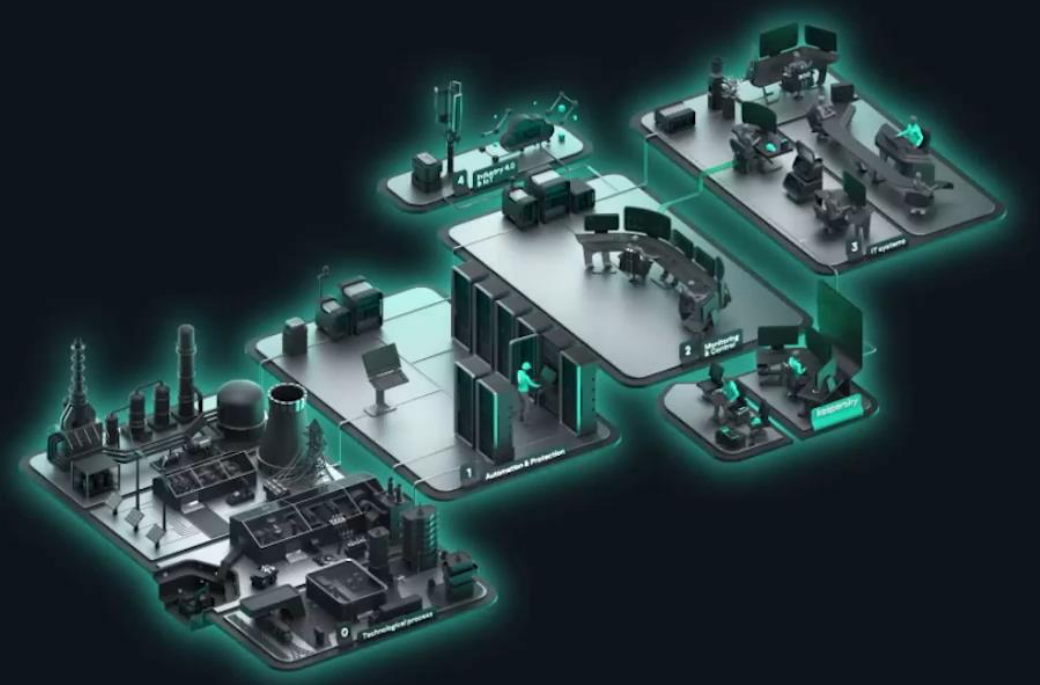
Cyber Hygiene	Threat Intelligence	Training
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

Learn more

kaspersky

Kaspersky OT Cybersecurity

Contact us



Industrial cyber resilience

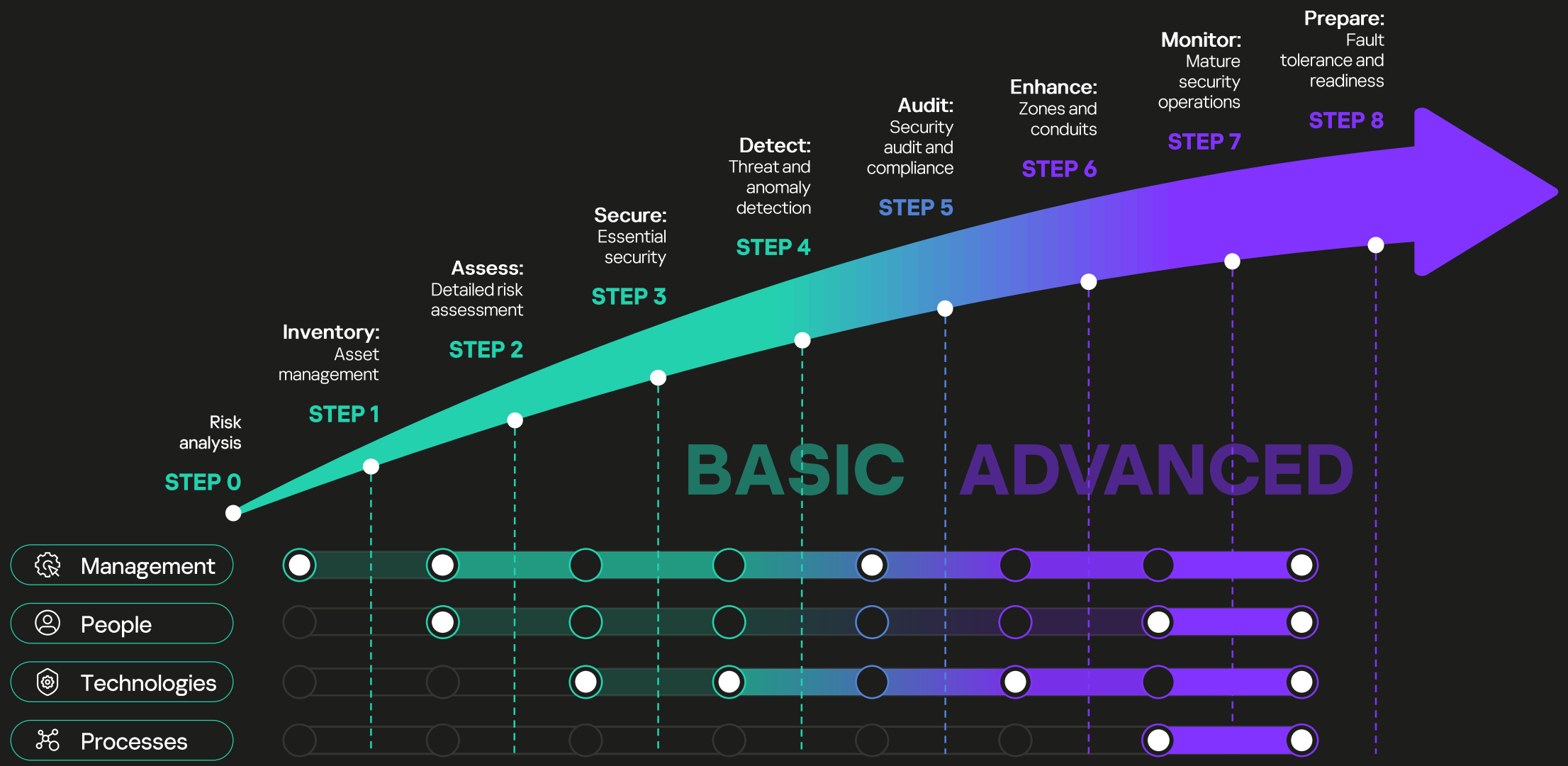
8 steps to secure your enterprise

1. **Inventory:** Asset management
2. **Assess:** Detailed risk assessment
3. **Secure:** Essential security
4. **Detect:** Threat and anomaly detection
5. **Audit:** Security audits and compliance
6. **Enhance:** Zones and conduits
7. **Monitor:** Mature security operations
8. **Prepare:** Fault tolerance and readiness

Download your guide

https://www.kaspersky.com/go/industrialcyberresilience

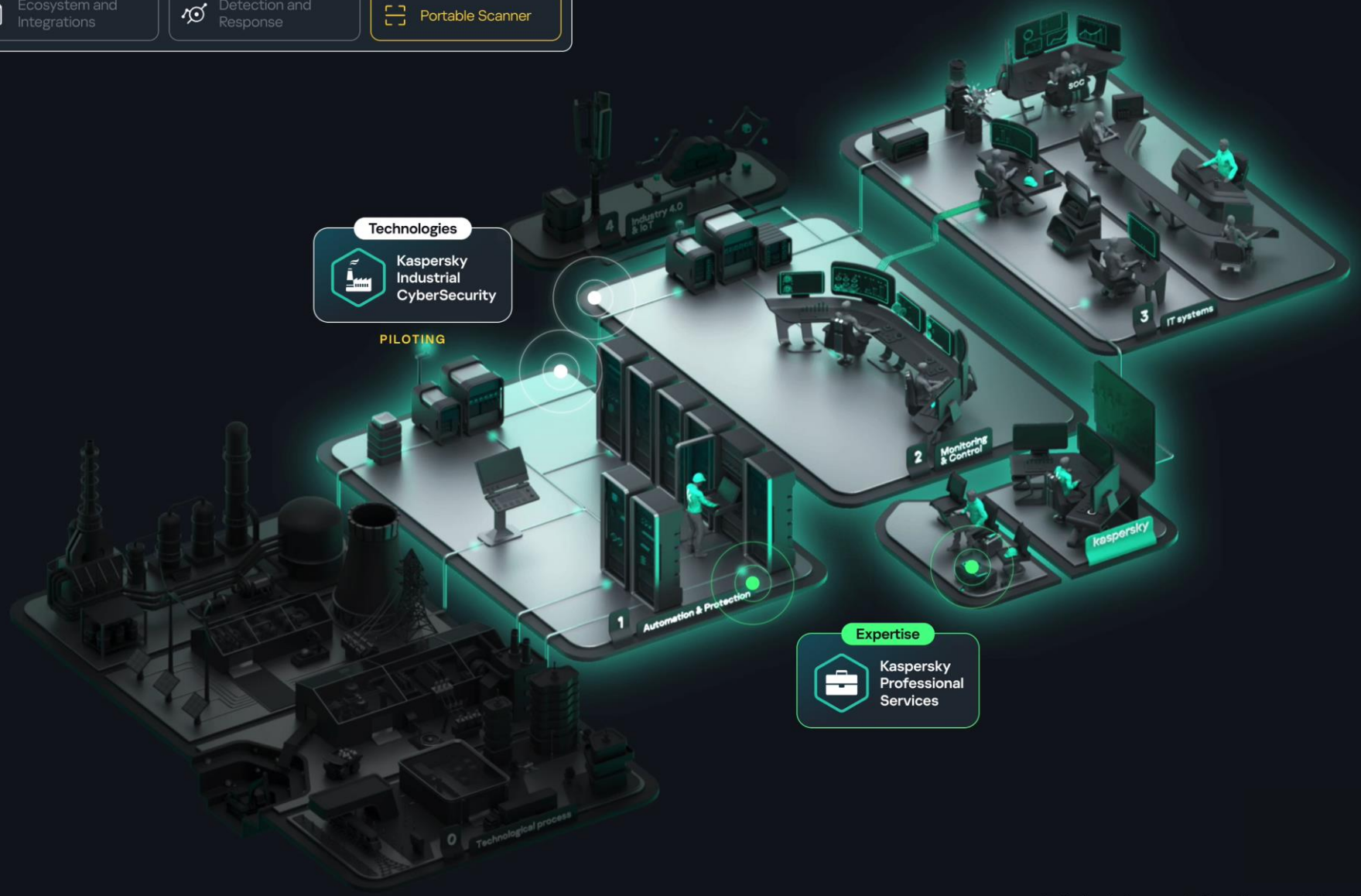
Transition from being a solution supplier to a trusted advisor to unlock greater value



https://www.kaspersky.com/go/industrialcyberresilience

KICS PLATFORM FEATURES

KICS FOR NETWORKS	OT XDR	KICS FOR NODES
Asset Management	Advanced Asset Management	Endpoint Protection
Threat and Anomaly Detection	Security Audit	Endpoint Detection and Response
Ecosystem and Integrations	Detection and Response	Portable Scanner



Industrial cyber resilience

8 steps to secure your enterprise

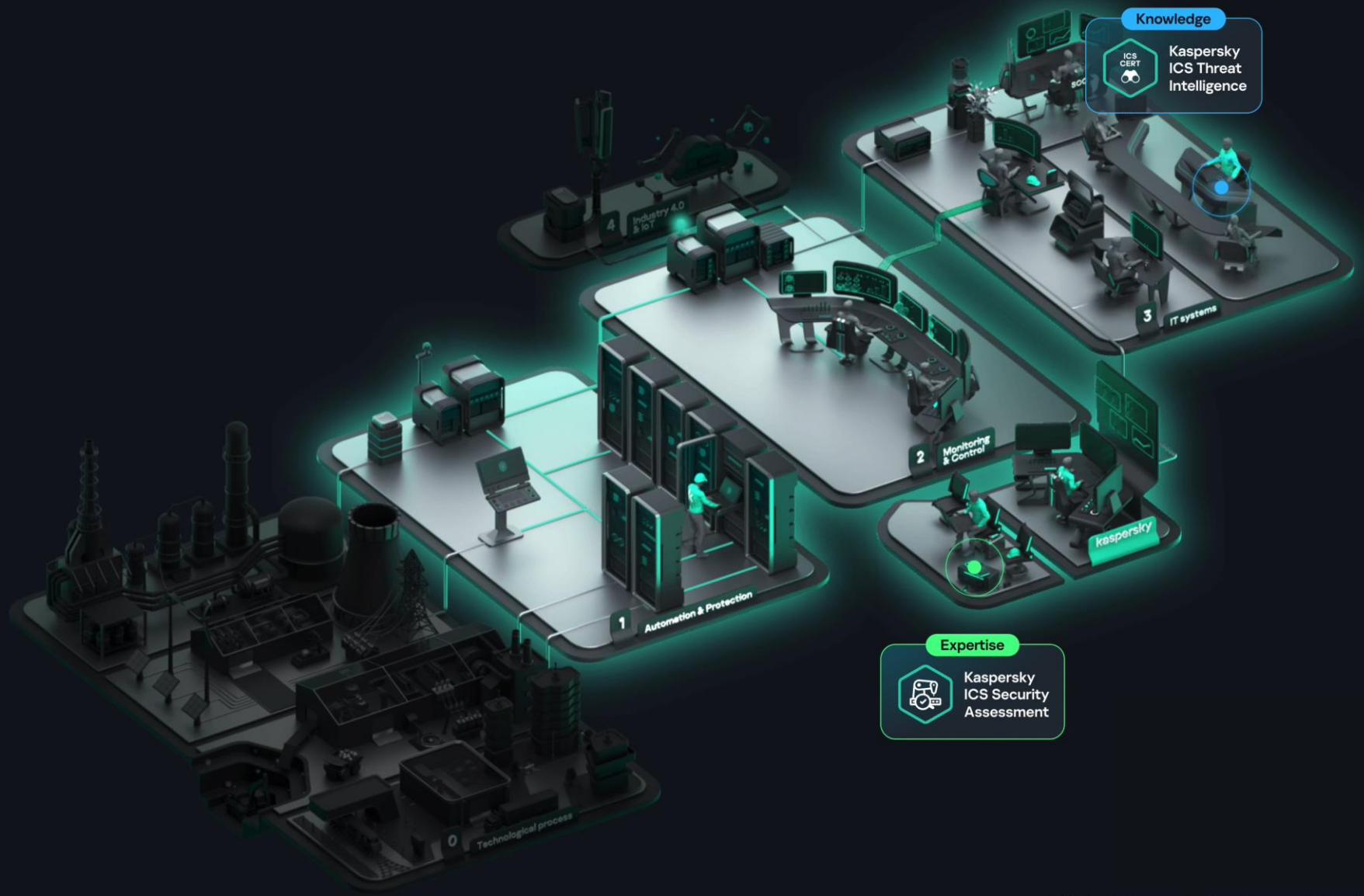
1. **Inventory: asset management**
   - 1.1 Outline objectives
   - 1.2 Prepare for discovery
   - 1.3 Use active pooling
   - 1.4 Map network
   - 1.5 Inventory
   - 1.6 Monitor continuously
2.
3.
4.
5.
6.
7.
8.

Standards and practices

IEC 62443-3-3	SR 1.1*; SR 1.2; SR 1.3*; SR 7.8^
IEC 62443-3-2	ZCR 1.1; ZCR 2.2
NIS2	Article 21: p. 2 (d, g, l), p. 3
NIST SP 800-82r3	6.1.1: Asset Management
GB/T 44462.1	7.3.5.5.2: Asset Management

Industrial cyber resilience

8 steps to secure your enterprise



1
2
3
4
5
6
7
8

Assess: detailed risk evaluations

- 2.1 Identify vulnerabilities
- 2.2 Assets threats
- 2.3 Analyze impacts
- 2.4 Risk prioritization
- 2.5 Consider compliance

Standards and practices

IEC 62443-3-3	ZCR: 3.(All); 5.1^; 5.2^; 5.3; 5.4; 5.5; 5.8; 5.10; 5.12^; 5.13^
NIS2	Article 21: p. 2 (a, f); 22: p. 1
NIST SP 800-82r3	3.3.6; 6.1.3
GB/T 44462.1	7.3.5.2 Security management

Technologies · Expertise · Knowledge

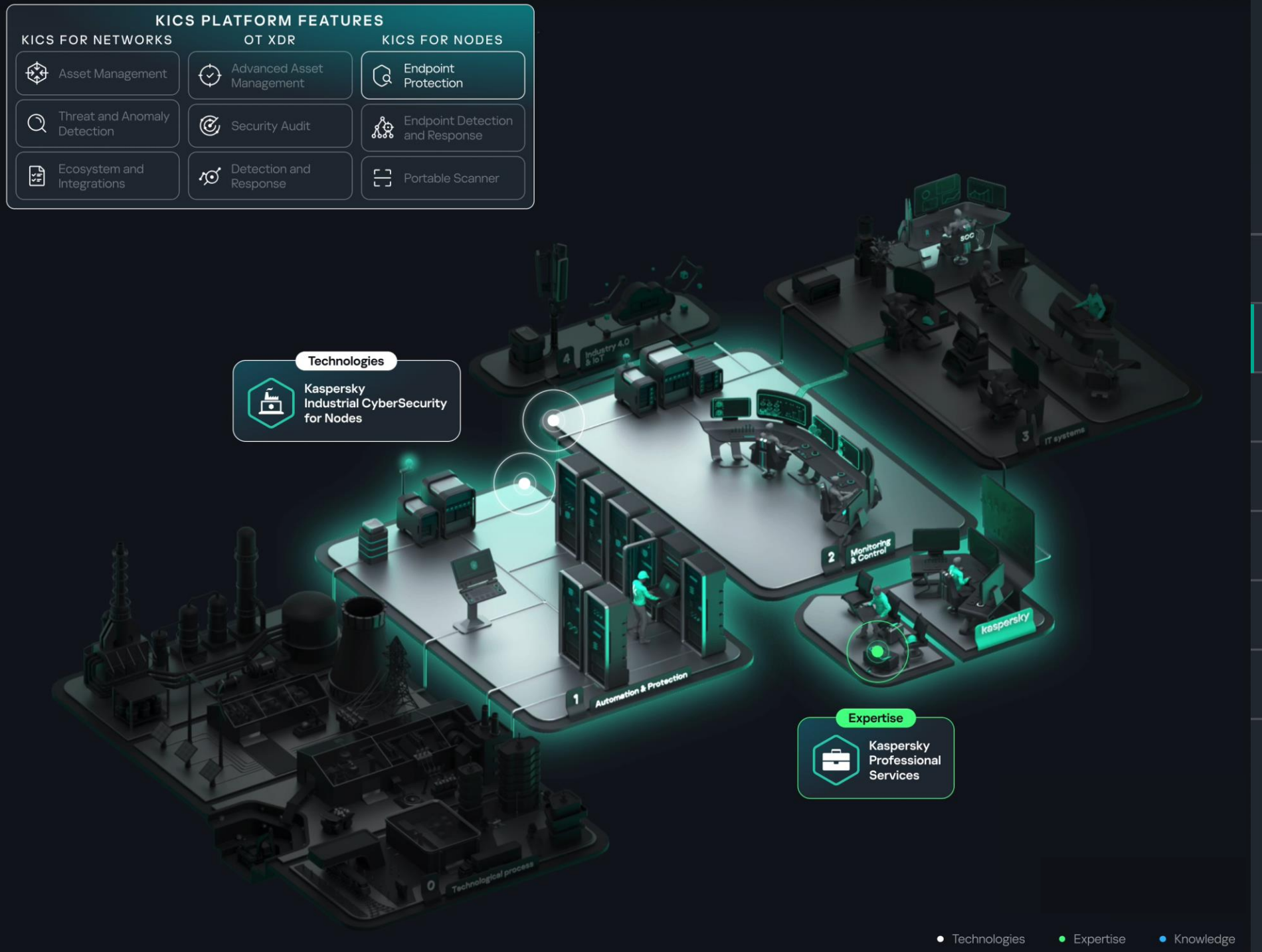
Industrial cyber resilience

8 steps to secure your enterprise

1	**Secure:** essential protection	
2	3.1	Harden and configure your endpoints
3	3.2	Configure baseline of system integrity
4	3.3	Deploy EPP
5	3.4	Implement access control
6		
7		
8		

Standards and practices

IEC 62443-3-3	SR: 1.6; 2.1; 2.3; 2.4; 2.5; 2.8; 3.2; 4.1*; 7.2^; 7.7
NIS2	Article 21: p. 2 (d, e, j); 25: p. 1
GB/T 44462.1	7.3.1.1 ICS host security



Industrial cyber resilience

8 steps to secure your enterprise

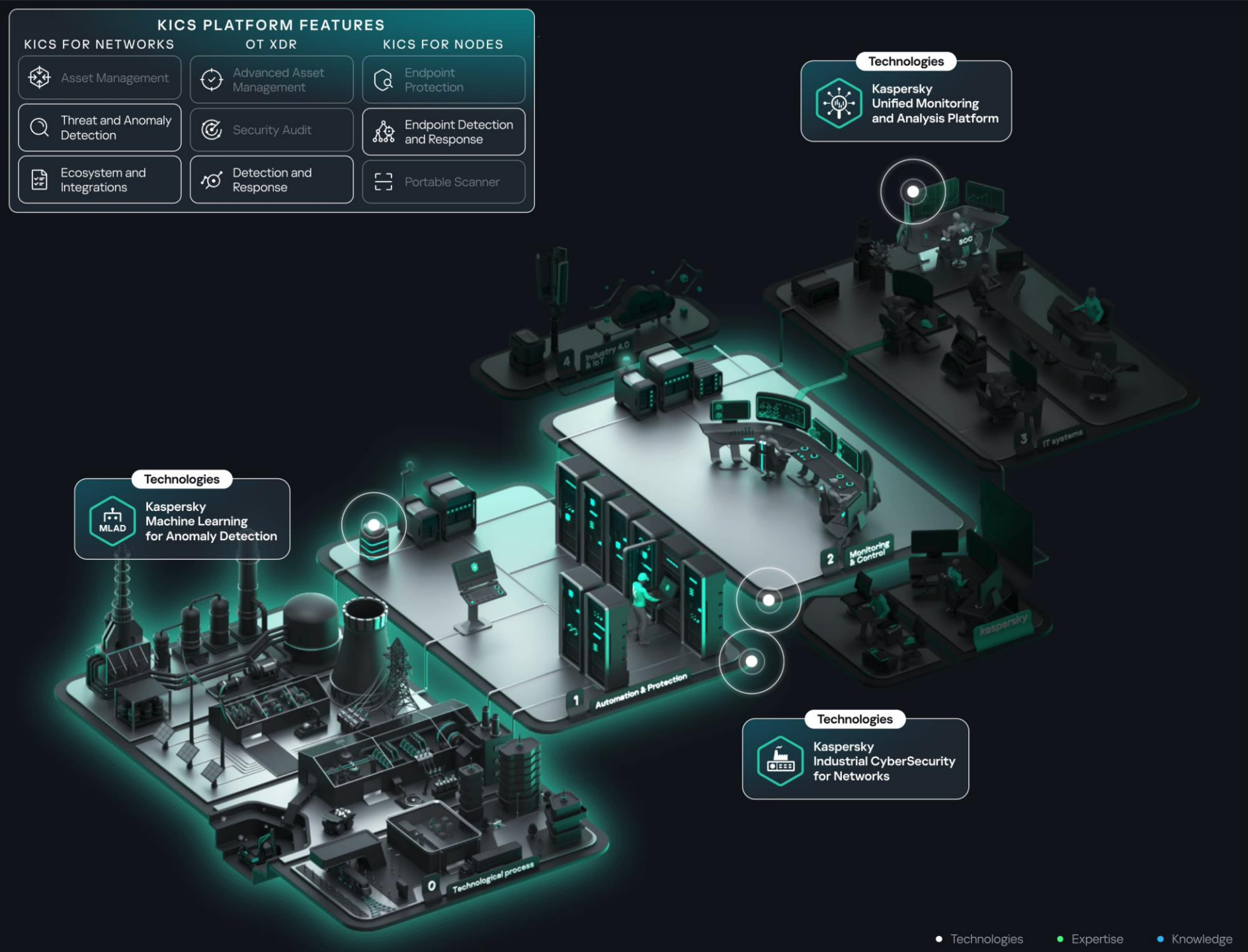
1. 2. 3. **4** 5. 6. 7. 8.

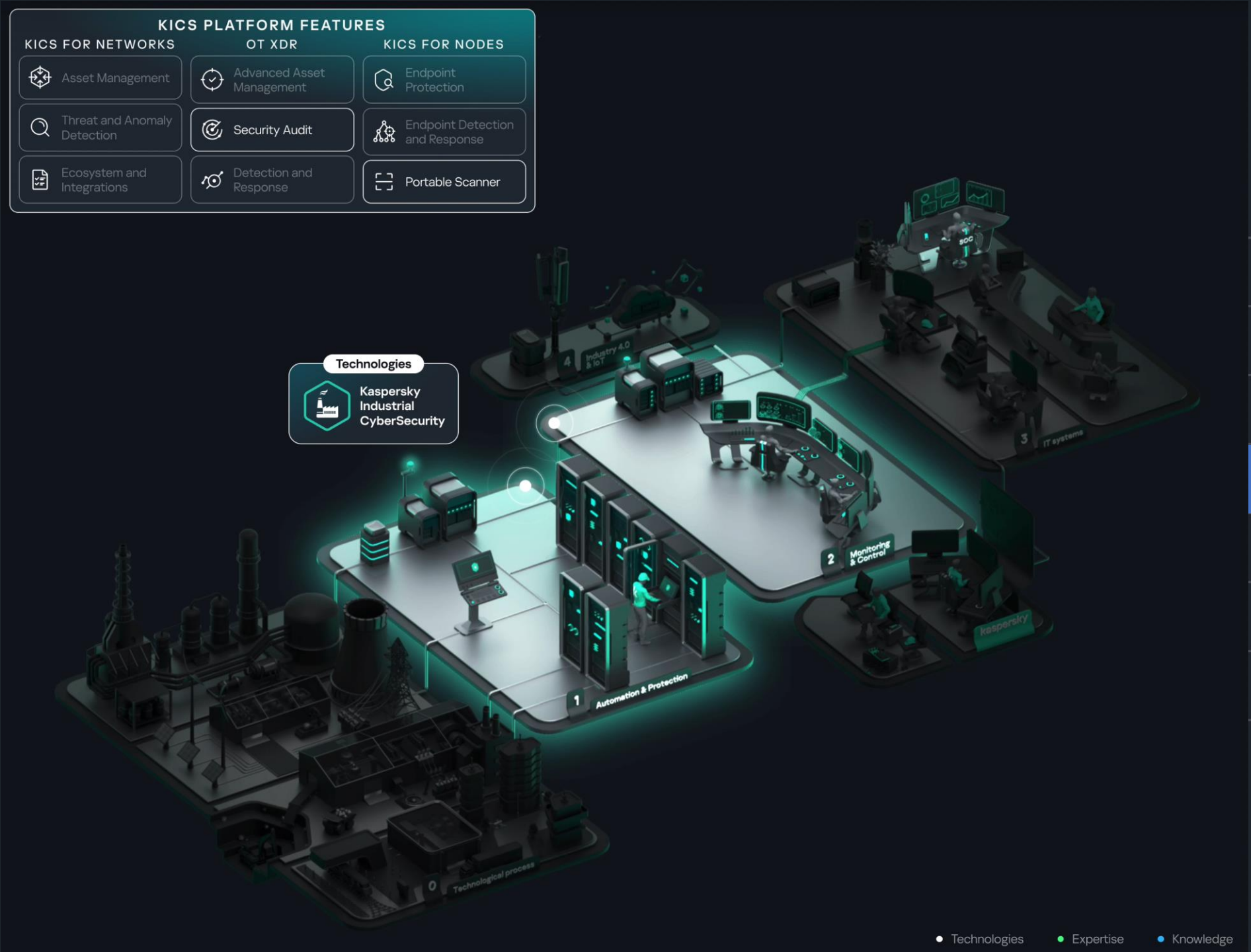
Detect: spot threats and anomaly

- 4.1 Implement toolset
- 4.2 Gather data
- 4.3 Establish baseline behavior
- 4.4 Seek anomalies
- 4.5 Remediate
- 4.6 Be futureproof

Standards and practices

IEC 62443-3-3	SR: 1.11; 2.2; 2.10; 2.21; 3.1^; 3.5^; 3.8; 5.3
GB/T 44462.1	7.3.3.2 Border Security
NIS2	Article 21: p. 2 (b, c, d, e); 23 p. 4
NIST SP 800-82r3	4.1: OT Risk Management





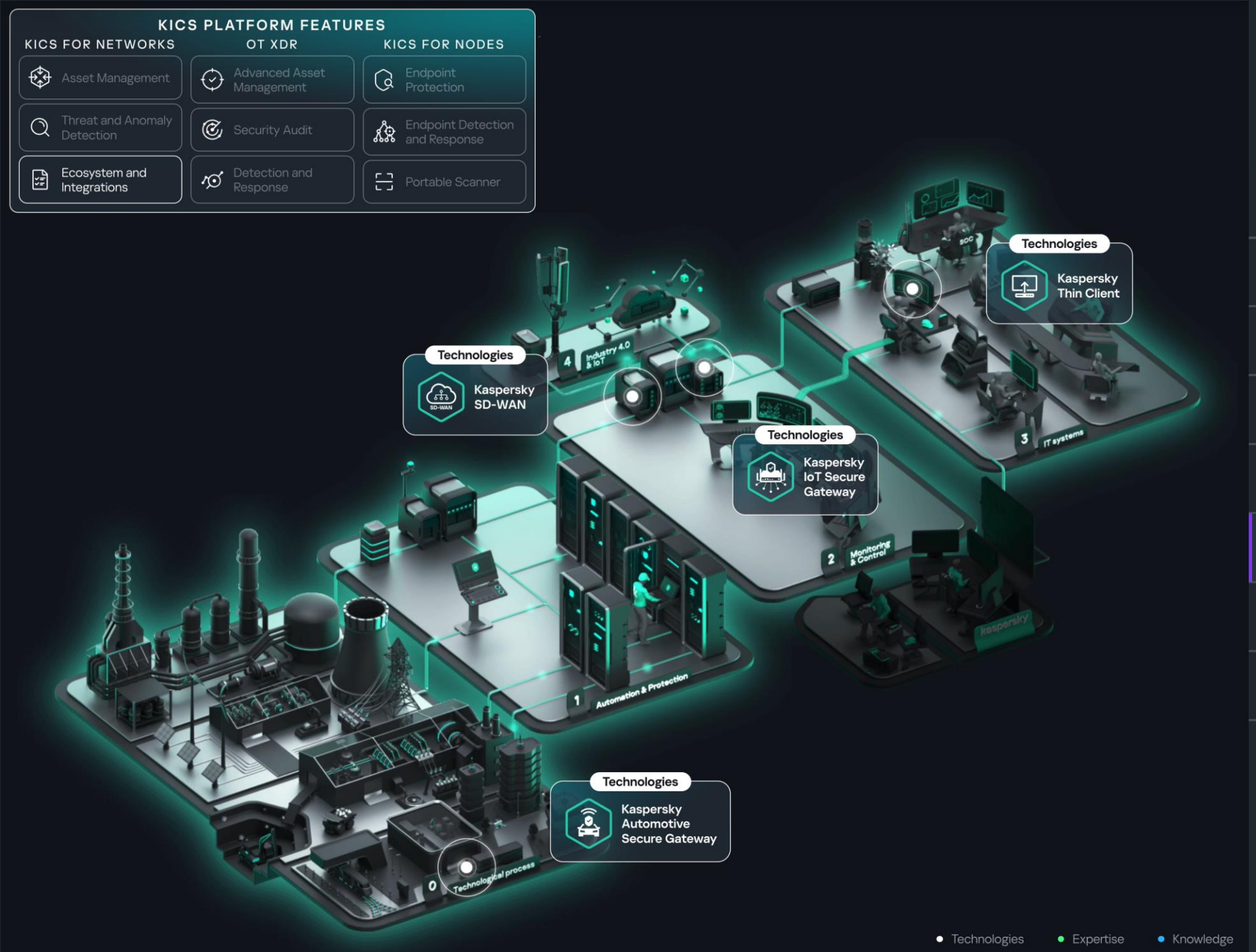
Industrial cyber resilience

8 steps to secure your enterprise

1.
2.
3.
4.
5. **Audit: compliance and vuln.**
   - 5.1 Identify frameworks
   - 5.2 Implement technical controls
   - 5.3 Hold risk assessment workshops
   - 5.4 Conduct security audits
6.
7.
8.

Standards and practices

IEC 62443-3-3	SR: 1.5; 1.7; 2.9; 2.11; 3.4; 3.7; 3.9; 6.1; 7.6^
GB/T 44462.1	7.3.2.3; 7.3.4.2
NIS2	Article 20 p.1; 21 p.2 (d, e, f, i)
NIST SP 800-82r3	3.3.1: Establish OT sec. Govern.



Industrial cyber resilience

8 steps to secure your enterprise

1
2
3
4
5
6
7
8

Enhance: zones and conduits

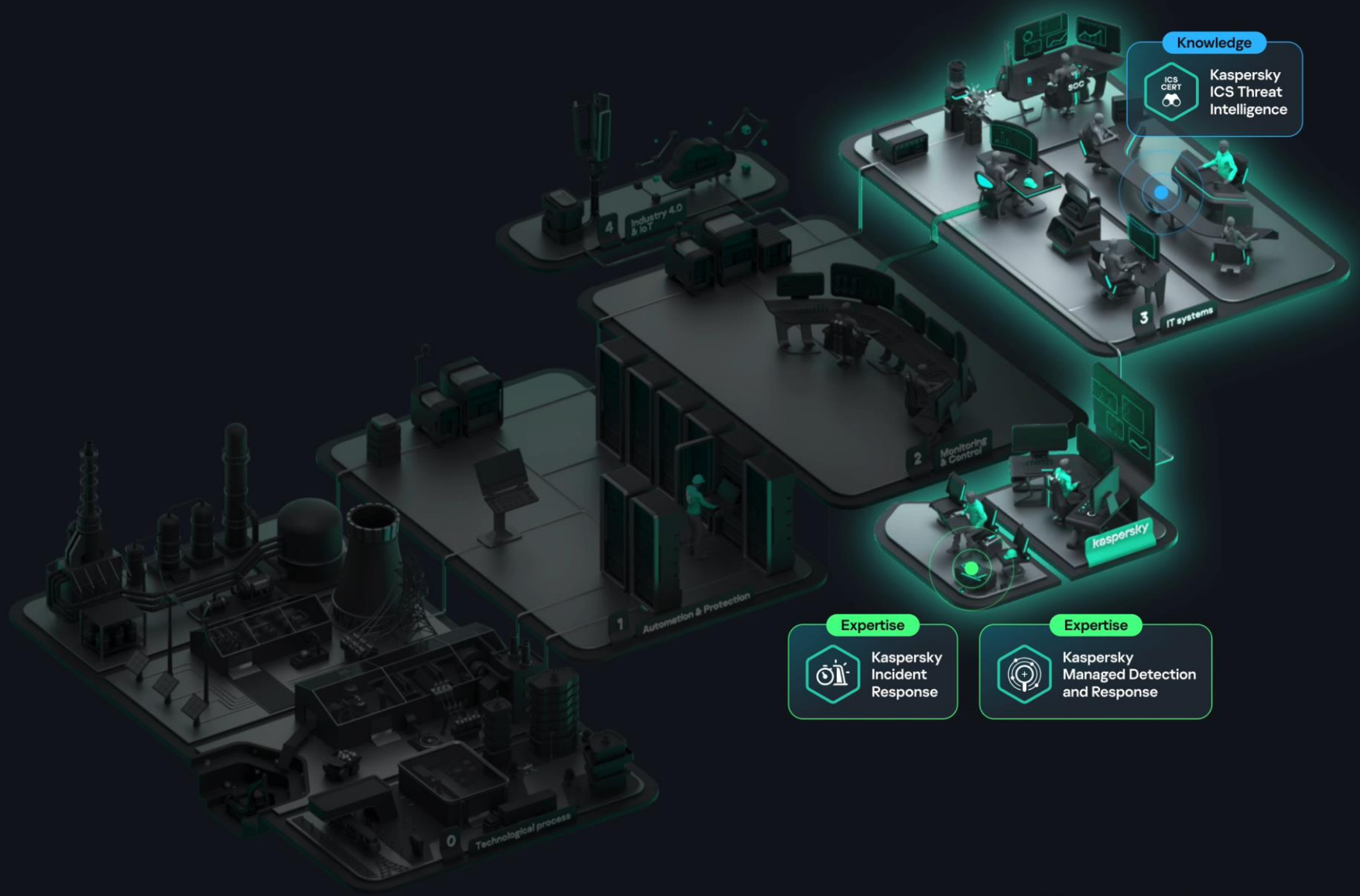
- 6.1 Continuously improve network segmentation
- 6.2 Map zones
- 6.3 Model conduits
- 6.4 Implement and configure
- 6.5 Test your setup

Standards and practices

IEC 62443-3-3	SR: 1.11; 1.13; 3.6; 5.1^; 5.2^
GB/T 44462.1	7.3.3.1 - Architectural security
NIS2	Article 21: p. 2 (h, I, j)
NIST SP 800-82r3	4.1 – OT risk management

Industrial cyber resilience

8 steps to secure your enterprise



1
2
3
4
5
6
7
8

Monitor: mature sec. operations

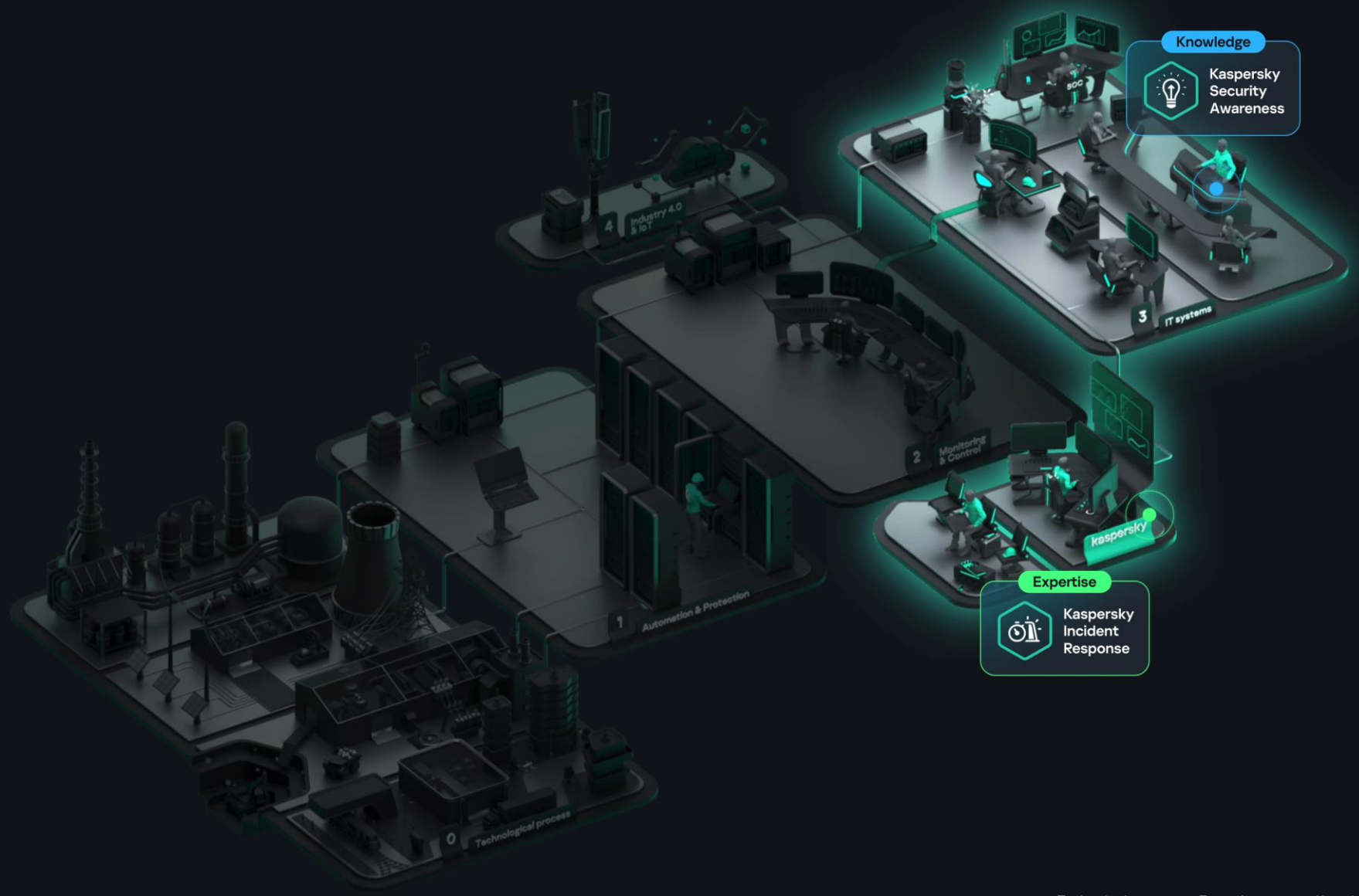
- 7.1 Set SOC goals
- 7.2 Develop SOC
- 7.3 Grow human skills
- 7.4 Form IR team
- 7.5 Refine IR plan

Standards and practices

IEC 62443-3-3	SR 3.3; SR 6.2^
GB/T 44462.1	7.3.5.5. Operations management
NIS2	Article: 21 p. 2 (b, c); 23 p. 4
NIST SP 800-82r3	3.3.8: Develop an IR Capability

Industrial cyber resilience

8 steps to secure your enterprise



1.
2.
3.
4.
5.
6.
7.
8. **Prepare: ensure resilience**

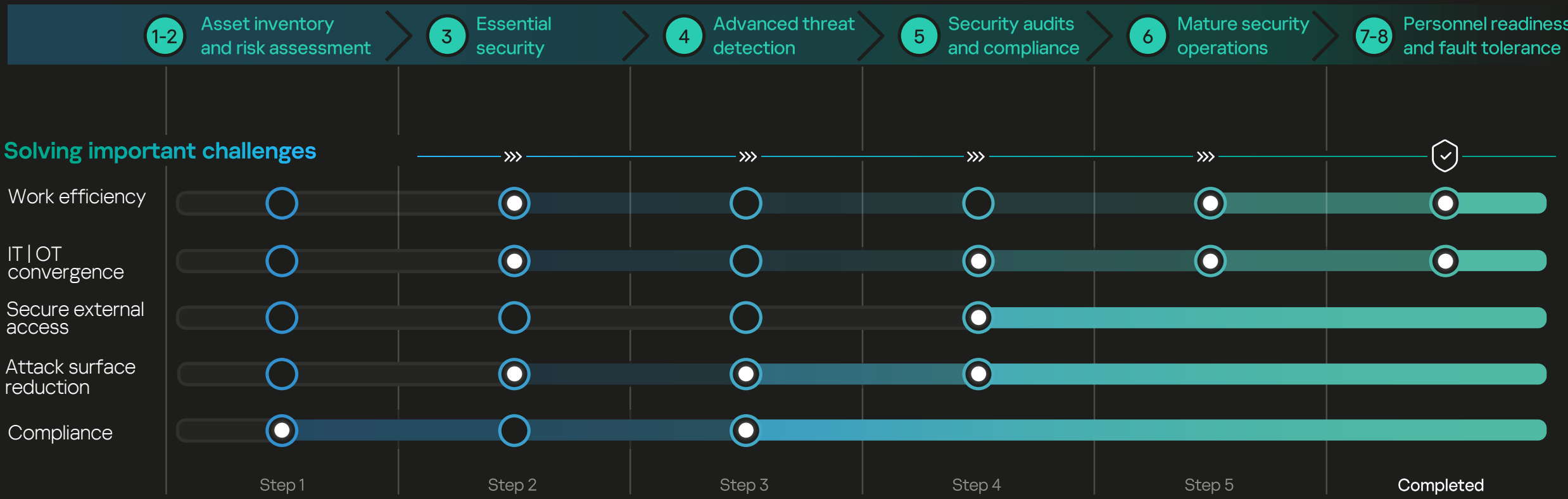
   - 8.1 Train your team
   - 8.2 Establish cross-team collaboration
   - 8.3 Practice
   - 8.4 Hold IR retrospective

Standards and practices

IEC 62443-3-3	SR 7.1; SR 7.4; SR 7.5
GB/T 44462.1	7.3.5 Security management
NIS2	Article 21: p. 2 (b, c, g)
NIST SP 800-82r3	3.3.2; 3.3.5; 4.3.5

Technologies · Expertise · Knowledge

Steps to secure your industrial enterprise



Kaspersky OT CyberSecurity

Power generation, transmission and distribution

kaspersky

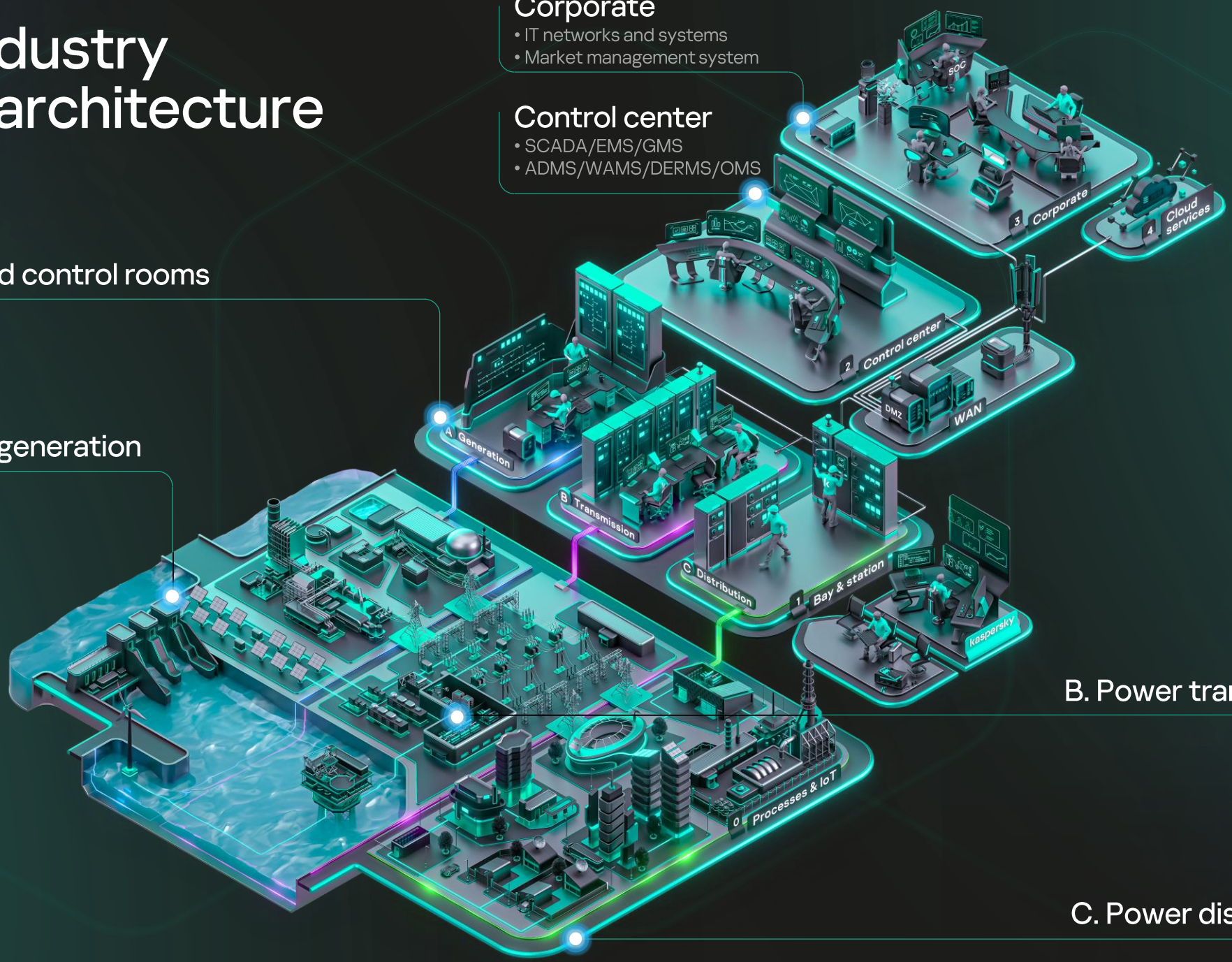
Power industry process architecture

Corporate
- IT networks and systems
- Market management system

Control center
- SCADA/EMS/GMS
- ADMS/WAMS/DERMS/OMS

Integrated control rooms

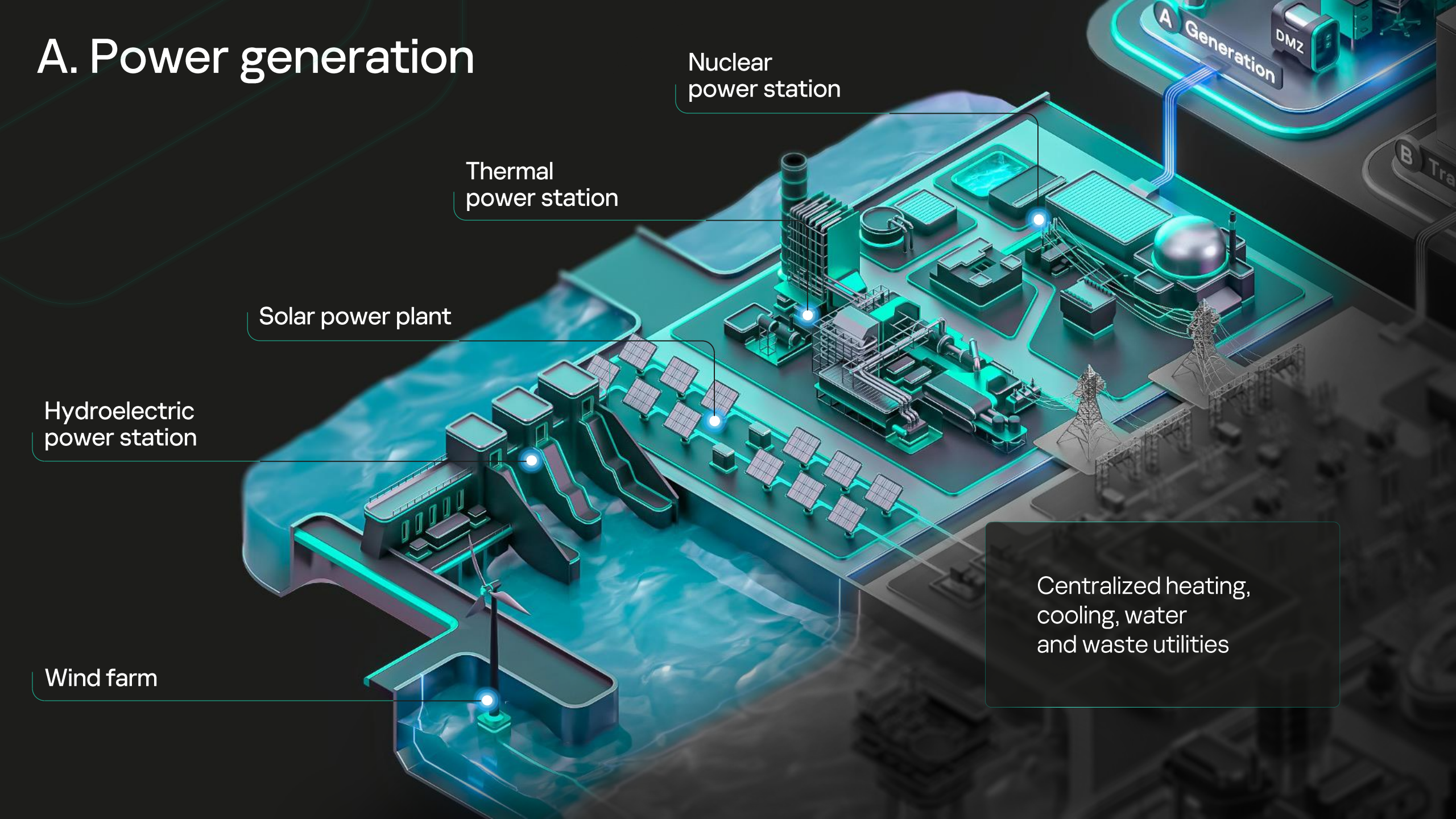
A. Power generation



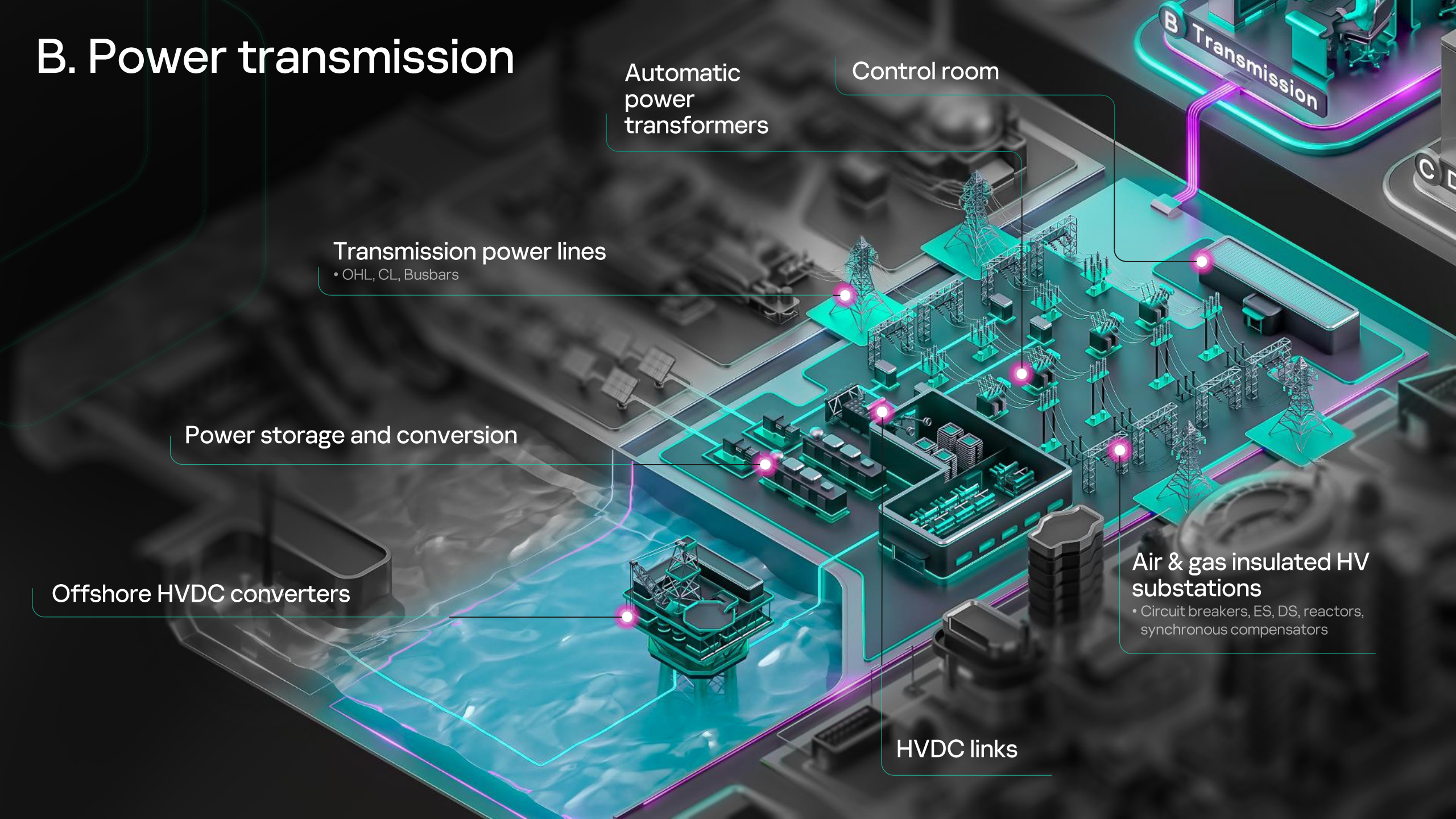
B. Power transmission

C. Power distribution

A. Power generation



B. Power transmission



C. Power distribution

Suburbs

- MV/LV unattended substations
- MV overhead wire lines
- Reclosers

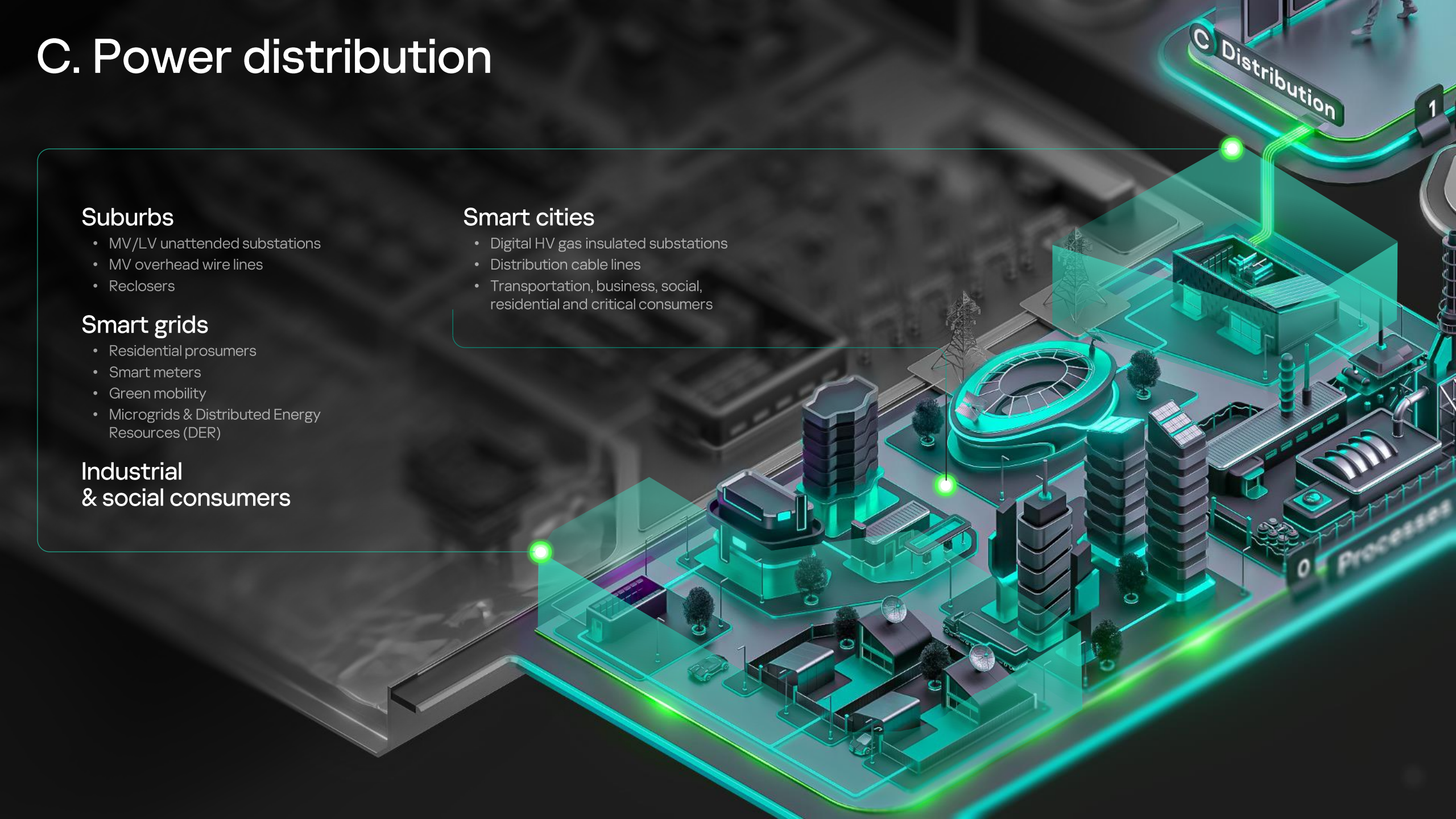
Smart grids

- Residential prosumers
- Smart meters
- Green mobility
- Microgrids & Distributed Energy Resources (DER)

Industrial & social consumers

Smart cities

- Digital HV gas insulated substations
- Distribution cable lines
- Transportation, business, social, residential and critical consumers



Power & Utilities case studies

EMC

Serbia's largest energy operator

Decisive factors for selection:

- Local partner presence
- Full compatibility with existing IT infrastructure

Implemented KICS for Nodes and KICS for Networks, planning to deploy our KUMA platform SIEM

€500 M
turnover

34
substations earmarked for KICS implementation

Learn more

Grid Company

Large power transmission company

More than 150 servers and workstations of the Grid Company Group's process loop are protected using KICS for Nodes, and monitoring of key segments of the technological network is ensured by 10 KICS for Network servers

19 239 MVA
Installed capacity

388
substations

Learn more

PacificLight

Electricity power generator and retailer

- Vulnerability assessment of their industrial networks to identify weaknesses and areas for improved security
- Simulated industry-specific attack vectors to uncover ulnerabilities, malicious activities and anomalies

1 M
households served

10%
of Singapore's total electricity generation

Learn more

ROSATOM

The #1 nuclear power plant in Russia by installed capacity

Implemented Kaspersky Industrial CyberSecurity to protect the infrastructure at all levels , from SCADA servers and operator workstations to programmable logic controllers (PLCs) and network equipment

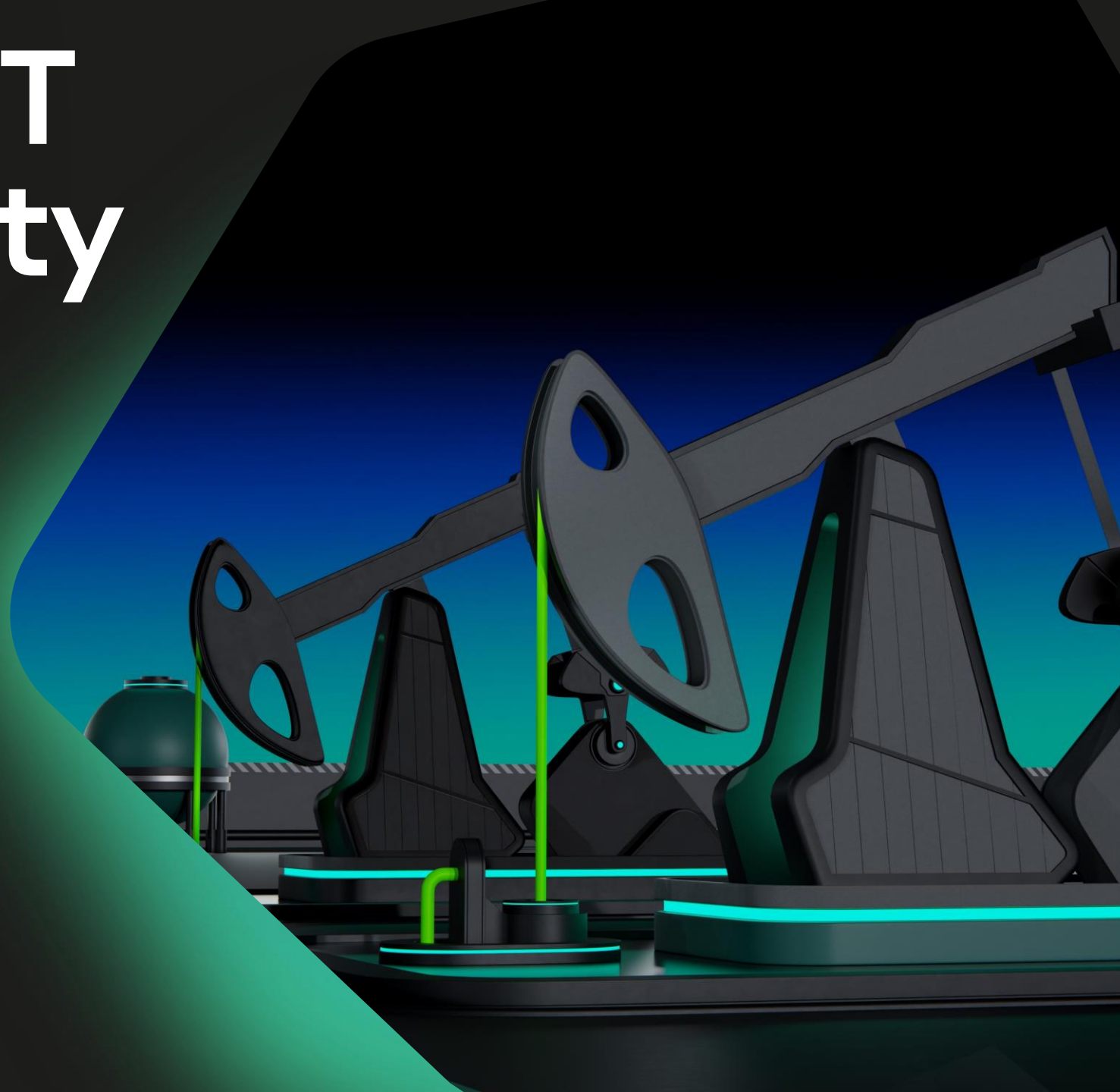
4337 MW
output

7 M
consumers

Request case study

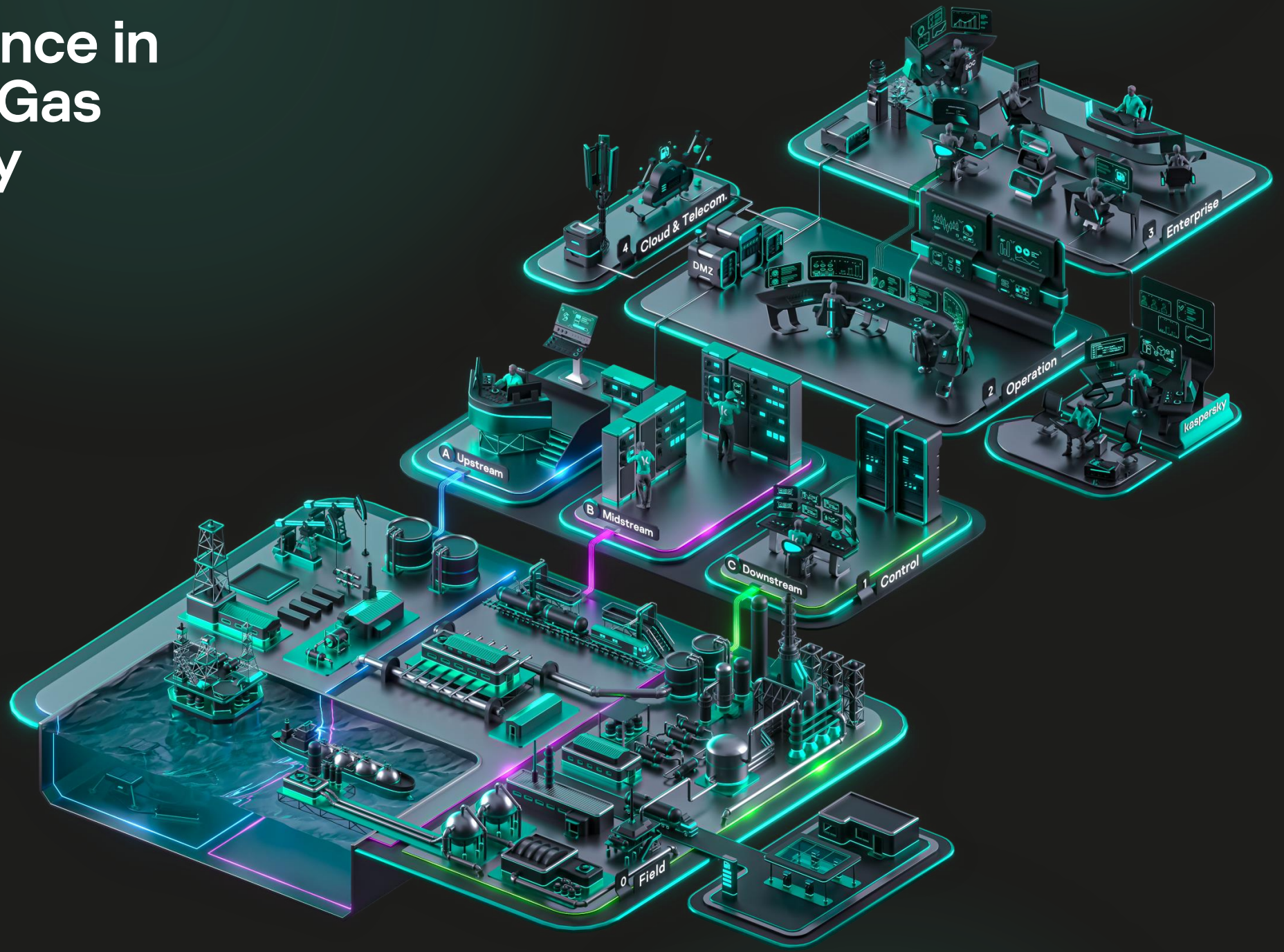
Kaspersky OT CyberSecurity

Oil, Gas,
chemicals and
petrochemicals



kaspersky

Experience in Oil and Gas industry

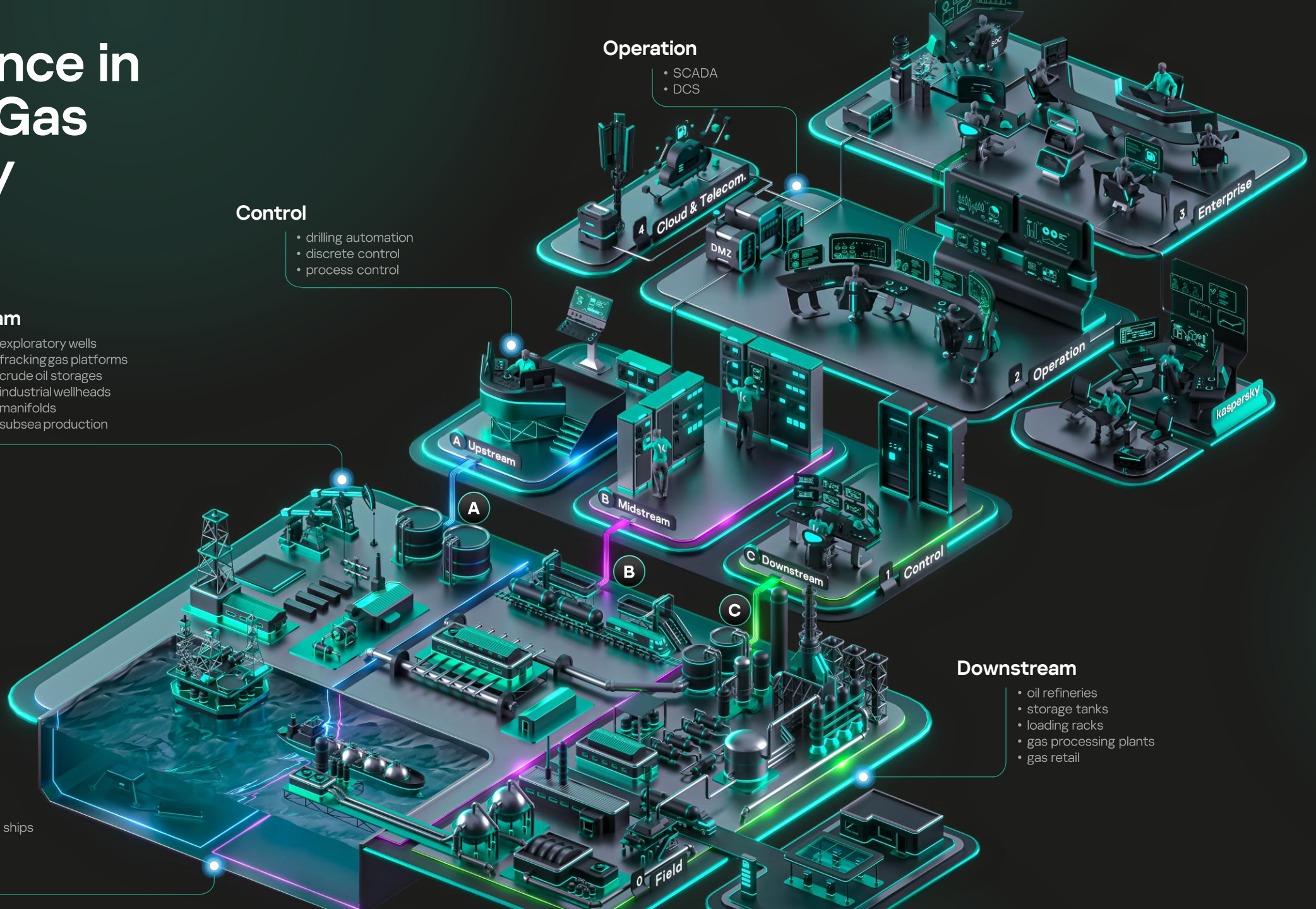


Experience in Oil and Gas industry

Operation
- SCADA
- DCS

Control
- drilling automation
- discrete control
- process control

Upstream
- exploratory wells
- fracking gas platforms
- crude oil storages
- industrial wellheads
- manifolds
- subsea production



Downstream
- oil refineries
- storage tanks
- loading racks
- gas processing plants
- gas retail

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

Successful case studies from O&G Industry

TATNEFT

TOP-5 largest O&G companies in Russia

- ICS protection using Kaspersky Industrial CyberSecurity solution
- Completed special training “Industrial Cybersecurity Awareness” based on real experience in investigating industrial cyber incidents

12 years
working with Kaspersky

Learn more

QazMunaiGaz AMÖZ
ATYRAU MUNAI ONDEU ZAVYTY

One of the largest oil refineries in the world

Opting for Kaspersky Industrial CyberSecurity (KICS) XDR resulted in:

- Stronger refinery information security
- Rapid detection of, and response to potential threats
- Better cybersecurity and production process monitoring and analytics

Learn more

ROSNEFT

RN-BashNIPIneft Major upstream R&D center

The centralized information security system is built on the entire ecosystem of Kaspersky products, ensuring strong protection against cyber threats and the optimized workload for cybersecurity personnel.

Learn more

SIA VARS

The only petrochemical terminal in the Baltic region

Using Kaspersky Industrial CyberSecurity solution to ensure reliable protection of automatic line control systems for the transshipment and storage of chemical products

Learn more

Partner you can trust

28 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 240 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
КАМАЗ
TATNEFT
EuroChem
Grid Company
РЖД
КазМунайГаз
PacificLight
ROSSETI

kaspersky

Let's meet at the demo zone!