Version: Aug 2025

Mikhail Chekalin

Cybersecurity for Critical Infrastructure

Kaspersky Industrial CyberSecurity

kaspersky

Why do we need Industrial Cybersecurity solutions?

Digitalization

is a focus for the majority of mature industrial enterprises because OT is the fuel for:

- Quality control
- Process automation
- Revenue growth
- Safety

Consequences

Disruption of production processes due to cyber attacks or staff mistakes

- Attack surface increases
- No & cost of incidents
- Strick legislation & policies
- Risks for supply chain

OT challenges

There are barriers to implement and maintain OT cybersecurity tolls

- Compliance with legislation
- IT-OT conflict
- Skills gap, staff shortage
- Deployment, integration and management inefficiencies

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

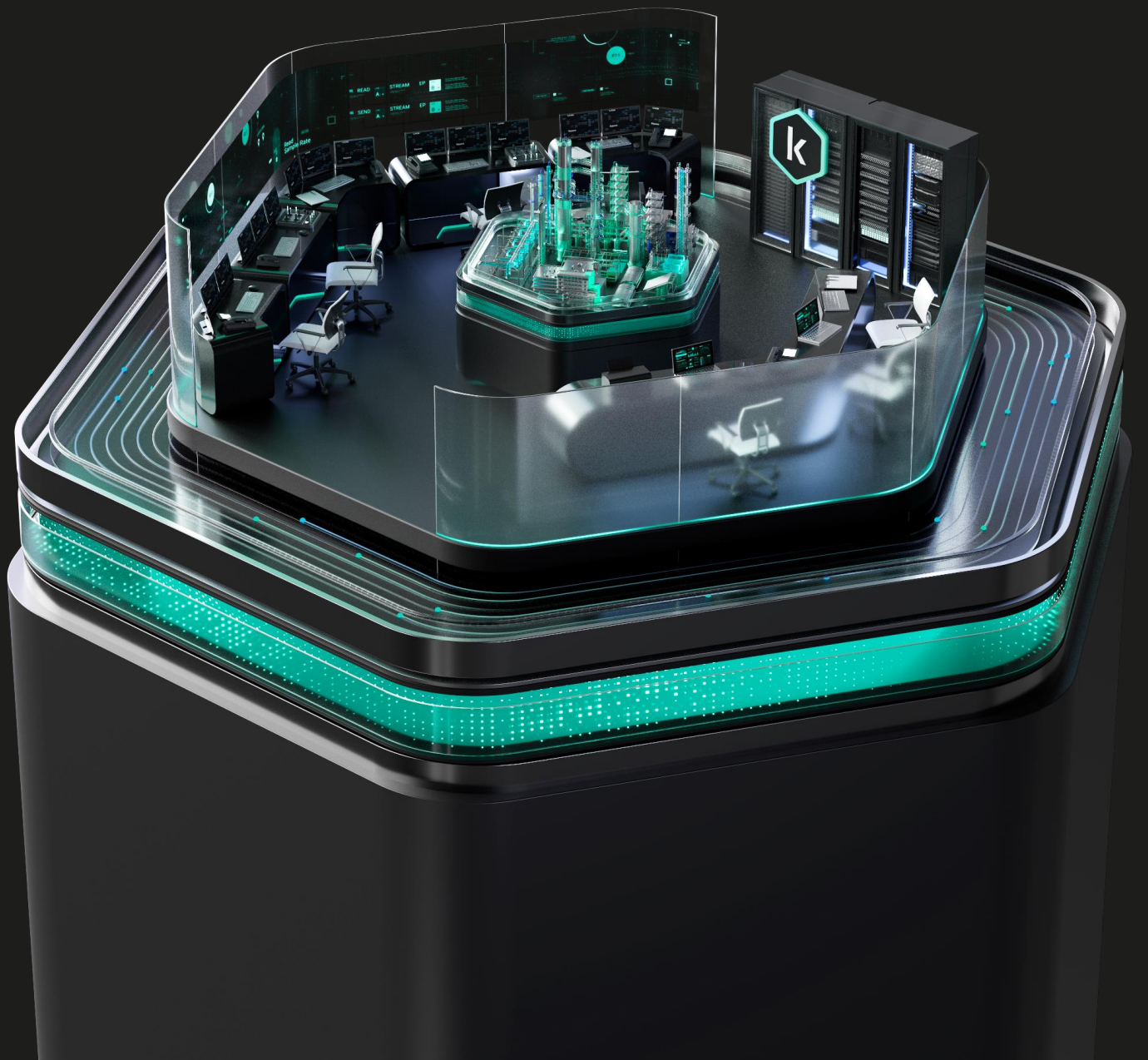
Offer extended detection, **prevention** and secure by design products

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

AV-TEST IEC 62443-4-1

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

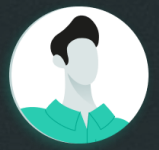
Kaspersky expertise



Kaspersky at a glance

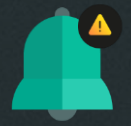
IT

28Y On cybersecurity market



5000+ Highly-qualified specialists

200+ Countries and territories where we operate



450K+ Amount of new malware samples daily

OT

15Y OT cybersecurity experience

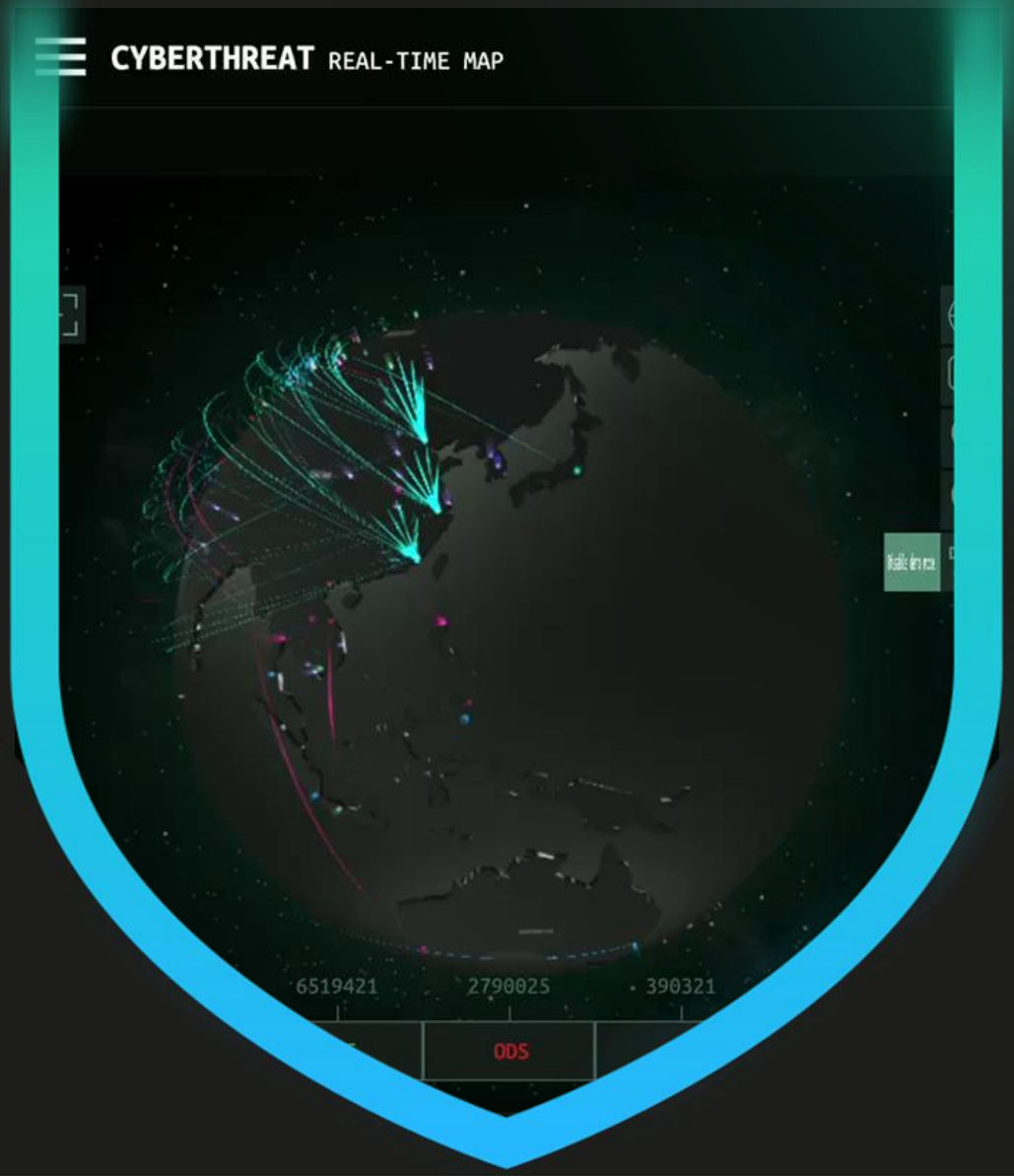
300+ OT cybersecurity cybersecurity experts

1000+ Industrial customers in track record

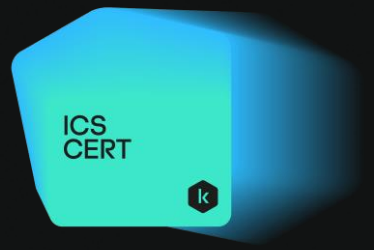
IEC/ISO Industry-leading audits

Today, Russia faces the most cyber attacks of any country

This unique position provides us with unparalleled awareness of global cyber trends, combining expertise from both East and West.



ICS CERT expertise



World-top experts in ICS threat and vulnerability.

Real-life experience.

Authorized to assign CVE identifiers to vulnerabilities and publish CVE records.

TRAINING — Empower your workforce with cybersecurity knowledge

- Industrial Cybersecurity Awareness
- Fuzzing-Based Vulnerability Research
- Digital Forensics
- Incident Response in ICS
- IoT Vulnerability Research

CONSULTING — Ensure best practices and customer experience

- Assessment of Product Security Maturity
- Product Vulnerability Assessment
- Methodology and Frameworks Assessment
- Product Design Assessment
- Policies and Procedures Development
- Regulation and Standards

Kaspersky AI Technology Research Center

For more than 20 years

Kaspersky has been empowering its solutions with ML / AI technologies, enabling us — and our customers — to stay ahead of whatever cyberattackers unleash.

Key focus areas

- Incorporating AI and machine learning into our cybersecurity products and services
- Developing guidelines for the secure use of AI and participation in the AI Alliance
- Tracking AI-driven threats to uncover emerging attack vectors
- Researching generative AI technologies with the help of our in-house LLM infrastructure
- Conducting research on AI algorithm security and developing principles for responsible AI use
- Applying AI approaches to detect anomalies and ensure continuity of manufacturing processes

IEC 62443 Coverage

Level 3 to IEC 62443 4-1

KICS was the first in the world in its category to reach the ML-3 maturity level

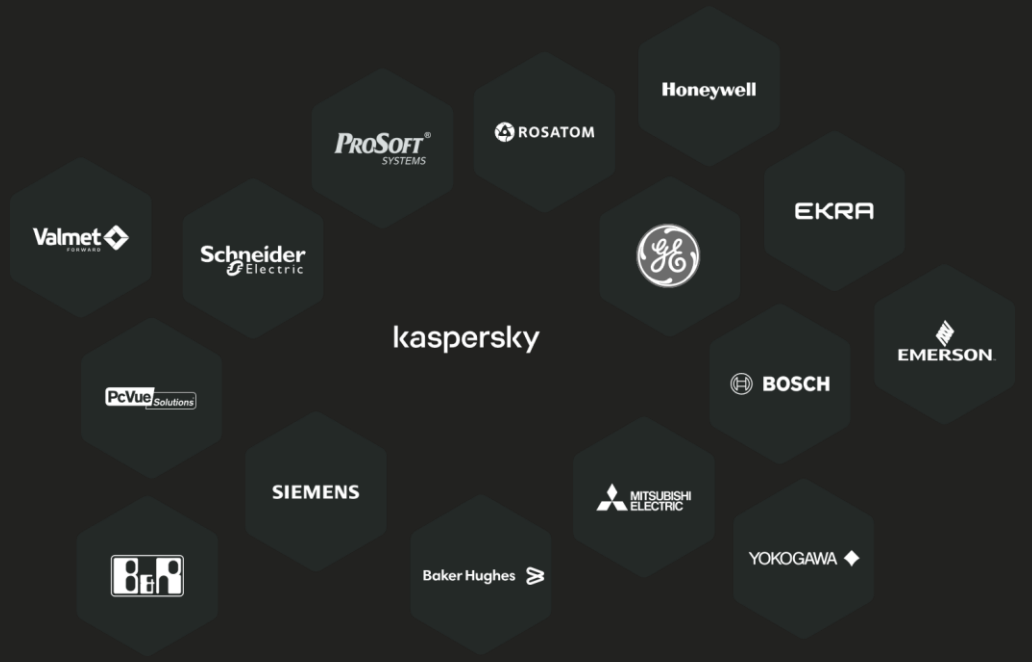
88% requirements of IEC-62443 3-3

covered by KICS and organizational measures (all requirements and all security levels)

Extensive program of testing the solution with leading automation system vendors

Compatible

240+ tested systems from 70+ vendors



Serving the largest industrial enterprises worldwide from all major verticals

Trusted

Results to date

270k+	1000+
Licenses shipped	Industrial customers
420+	230
Networks protected	Deployment partners

kaspersky

Kaspersky solutions for OT

kaspersky.com/enterprise-security/industrial-solution

Kaspersky Industrial Cybersecurity Platform (KICS)

KICS for Networks

A proprietary protocol-level solution for Network Traffic Analysis (NTA), detection and response

KICS for Nodes

Industrial-grade, tested and certified Endpoint Protection, Detection and Response software

Portable Scanner

Non-intrusive secure scanning & auditing for isolated or legacy machines and devices

360° situational awareness and risk exposure control for critical infrastructure

Unify workflows and strengthen internal alignment across OT, SecOps, IT and business

Gain the advantages of data sovereignty and transparent ownership costs

Simplify internal, regulatory and industry-specific compliance journey

Benefit from seamless integration with Kaspersky's best-in-class IT cybersecurity portfolio

Kaspersky OT CyberSecurity

IT – OT Convergence

Kaspersky Next XDR Expert

Kaspersky Industrial CyberSecurity

Native XDR

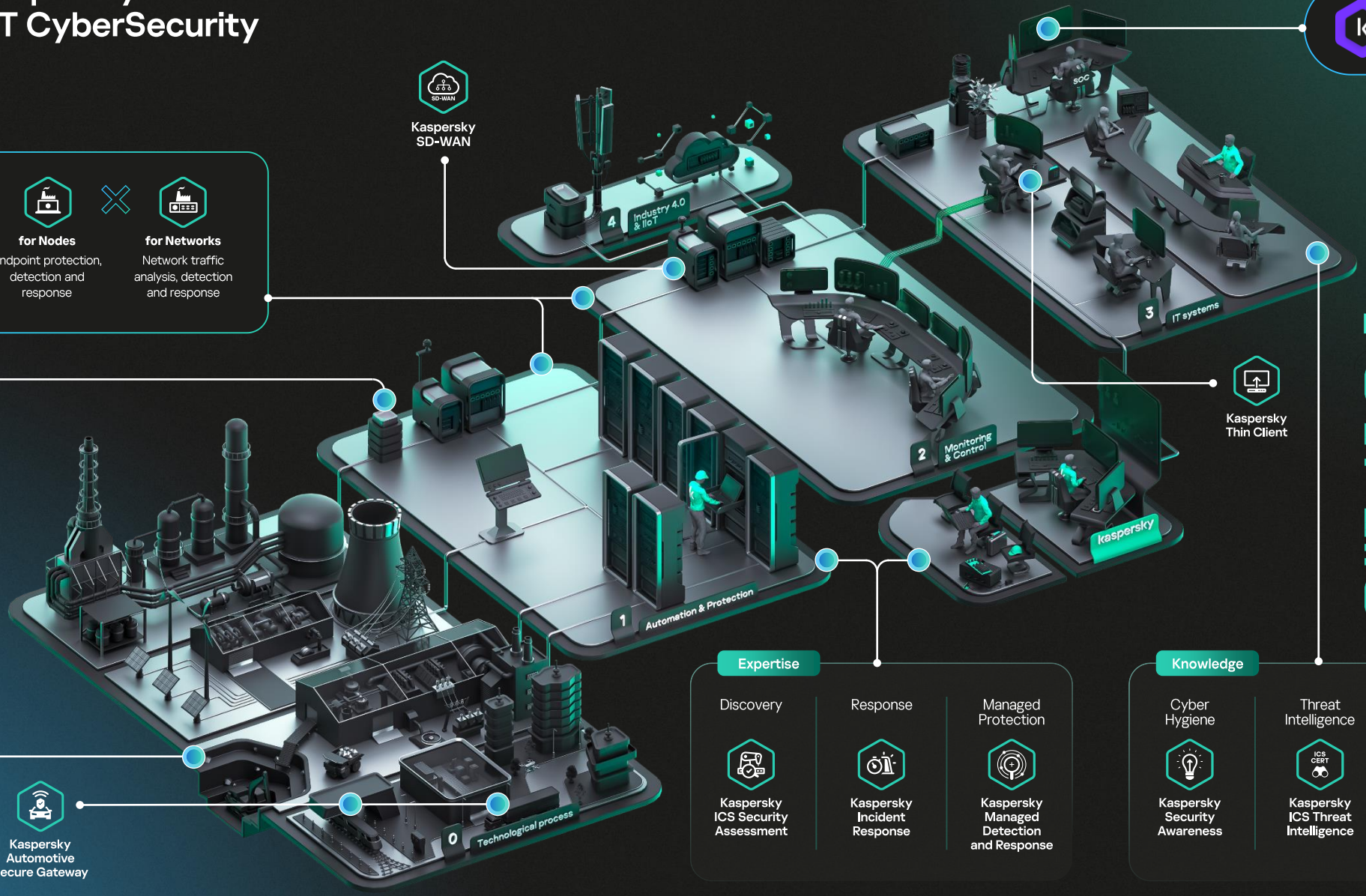
for Nodes
Endpoint protection, detection and response

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

Learn more

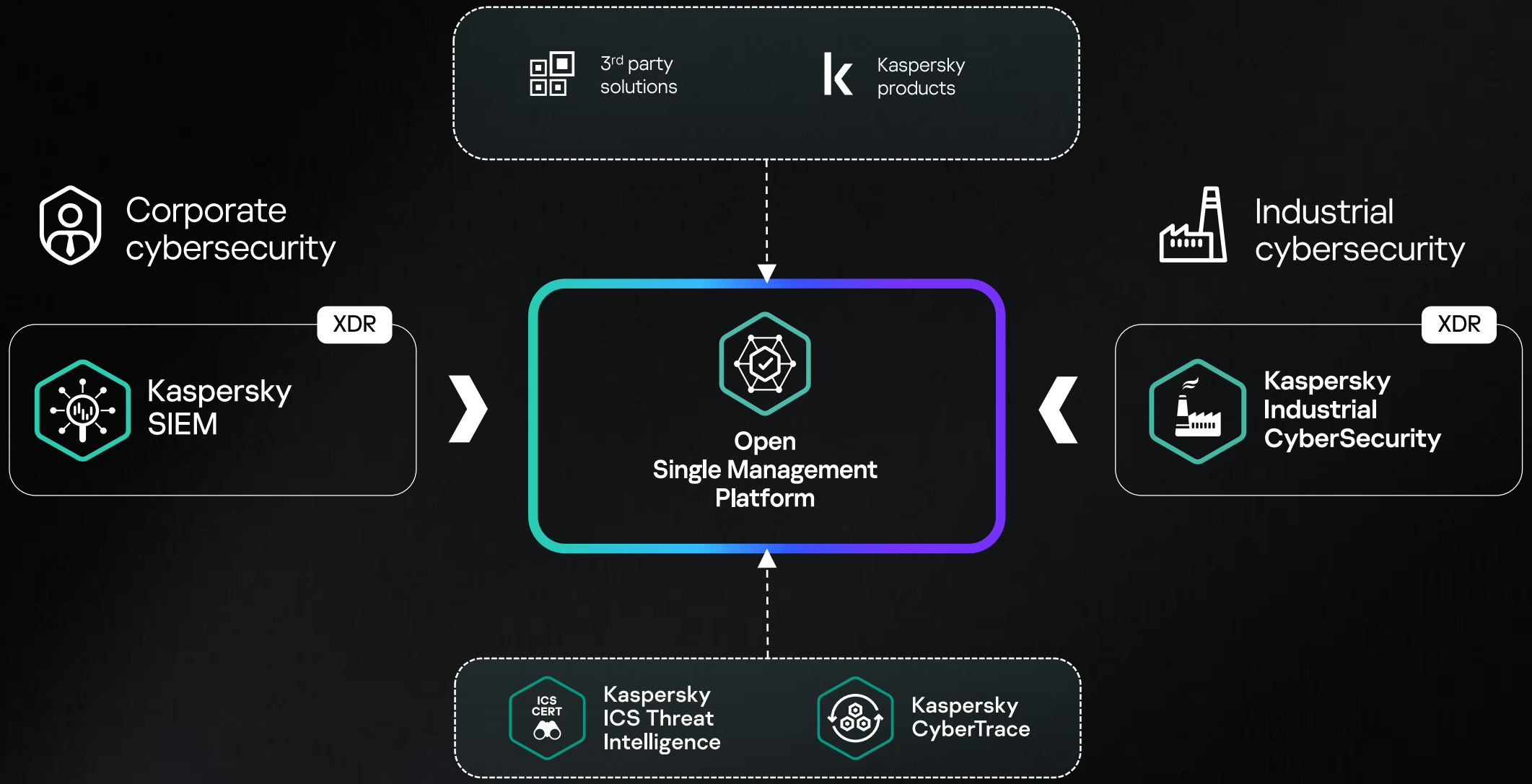
Expertise

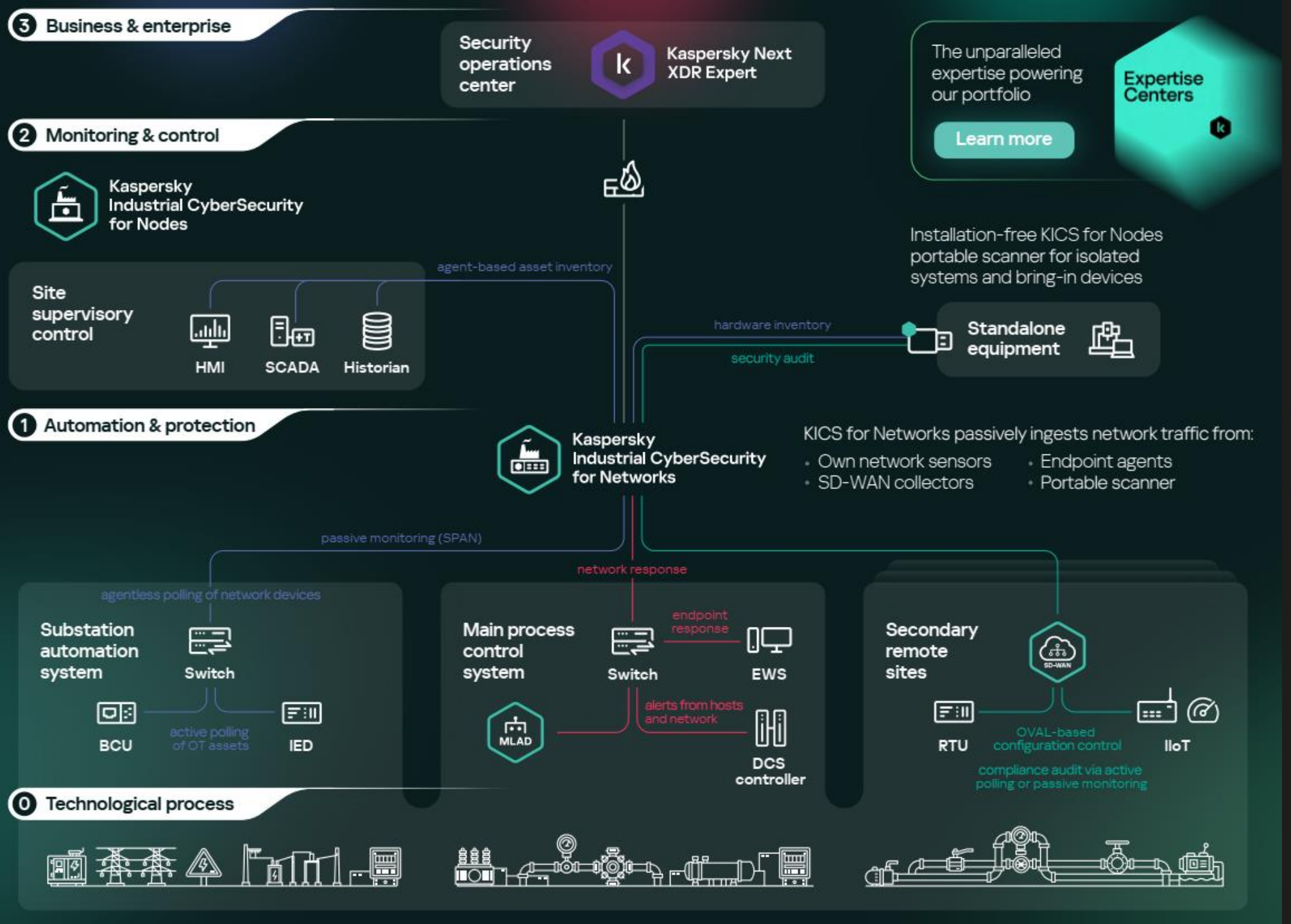
Discovery	Response	Managed Protection
Kaspersky ICS Security Assessment	Kaspersky Incident Response	Kaspersky Managed Detection and Response

Knowledge

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

Convergence of IT and OT environments





Solution architecture and use cases

Advanced assets management and with AI profiling

Extended detection and response

Continuous security audit

Integrations

+ Next XDR Expert for complex protection

+ MLAD for anomaly detection and predictive maintenance

+ SD-WAN for distributed infratructure

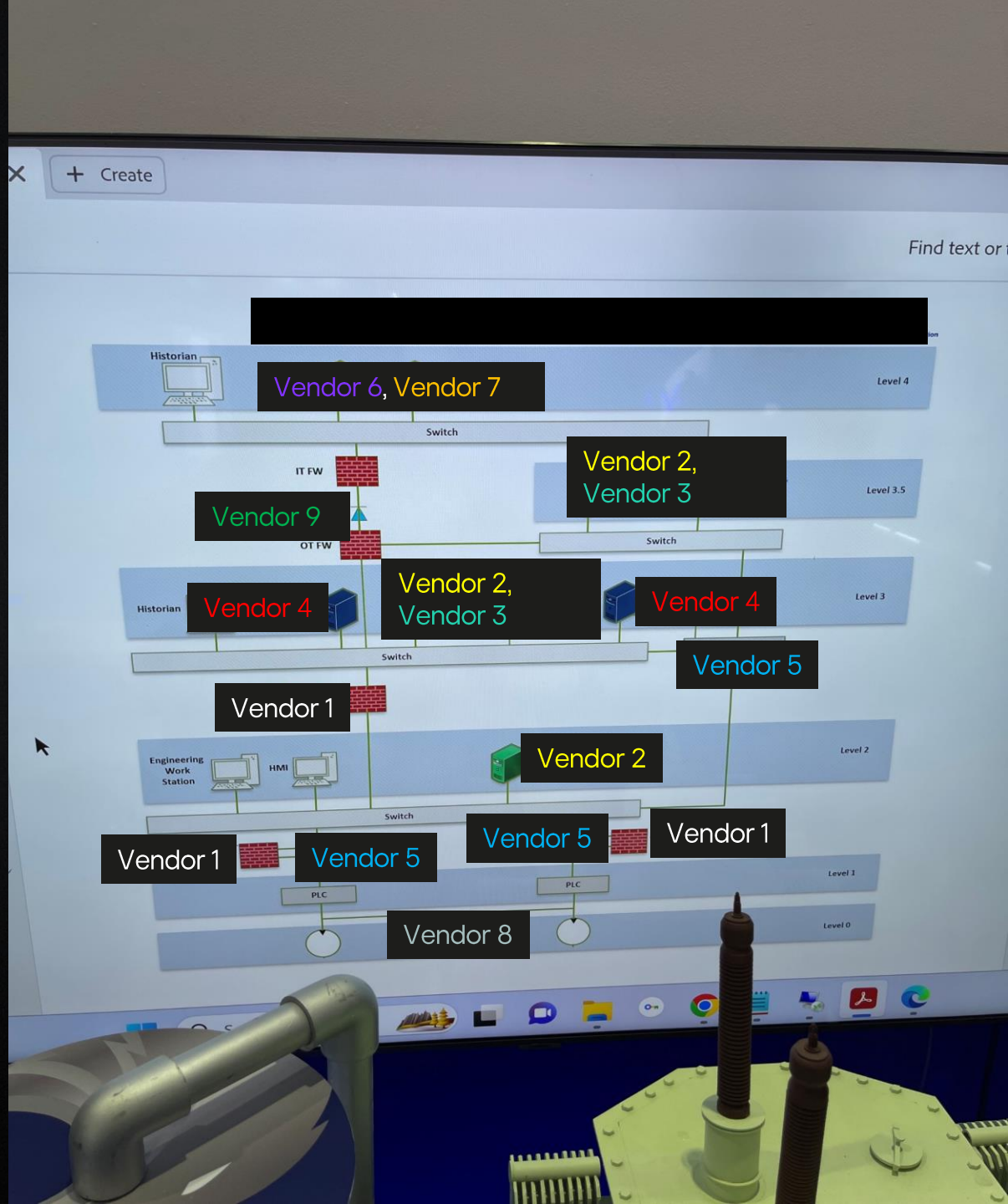
Confidential

- Multiply support teams
- Difficult to prescribe
- Multiply cross-solution failure points
- Difficult to deploy
- Difficult to maintain
- Extensive training on each individual product
- Difficult to troubleshoot
- Sophisticated licensing

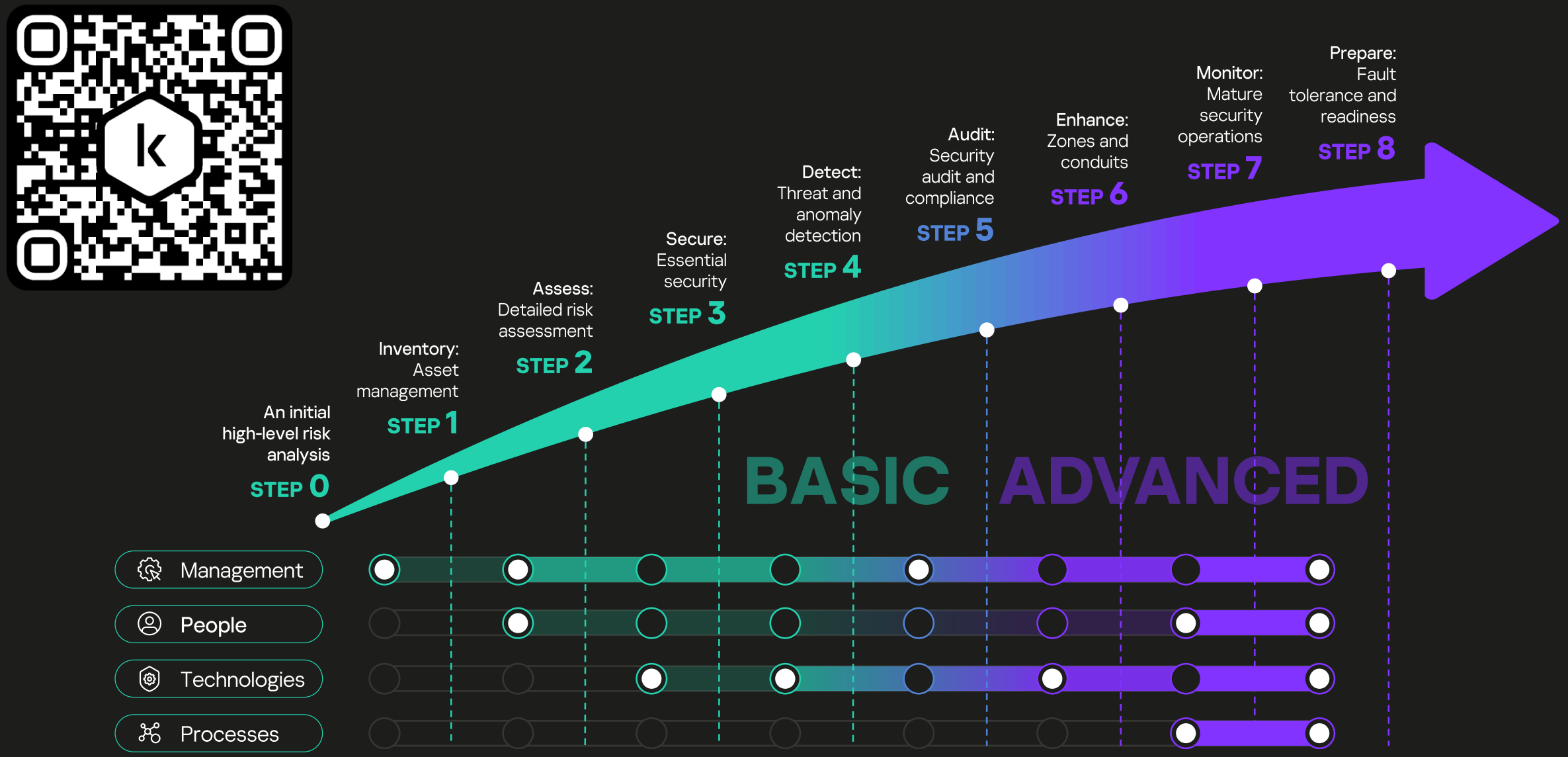
60%

Prefer to obtain comprehensive solution from a single vendor*

* Sing OT with Purpose-built Solutions, 2025 © VDC Research



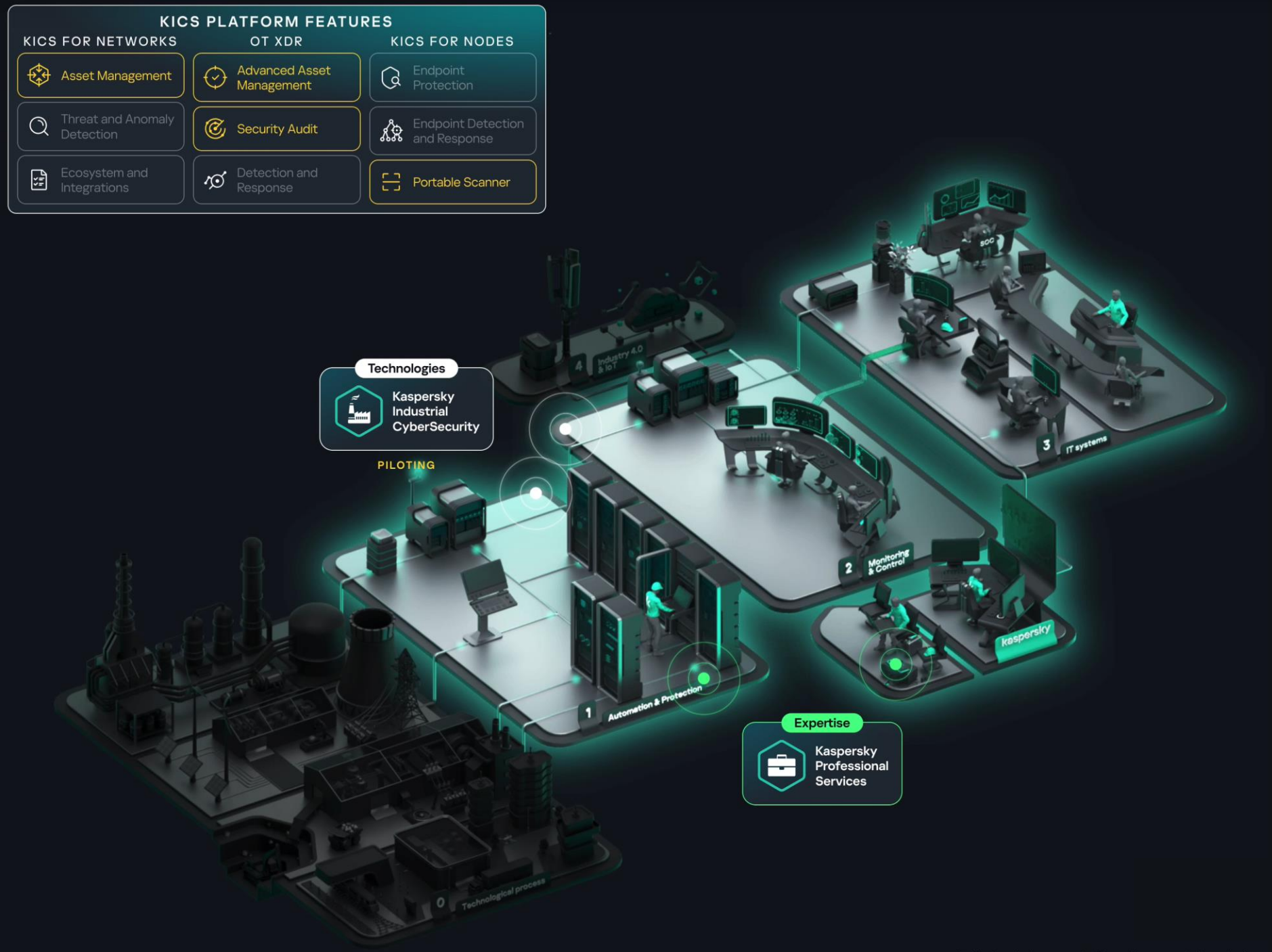
Transition from being a solution supplier to a trusted advisor to unlock greater value



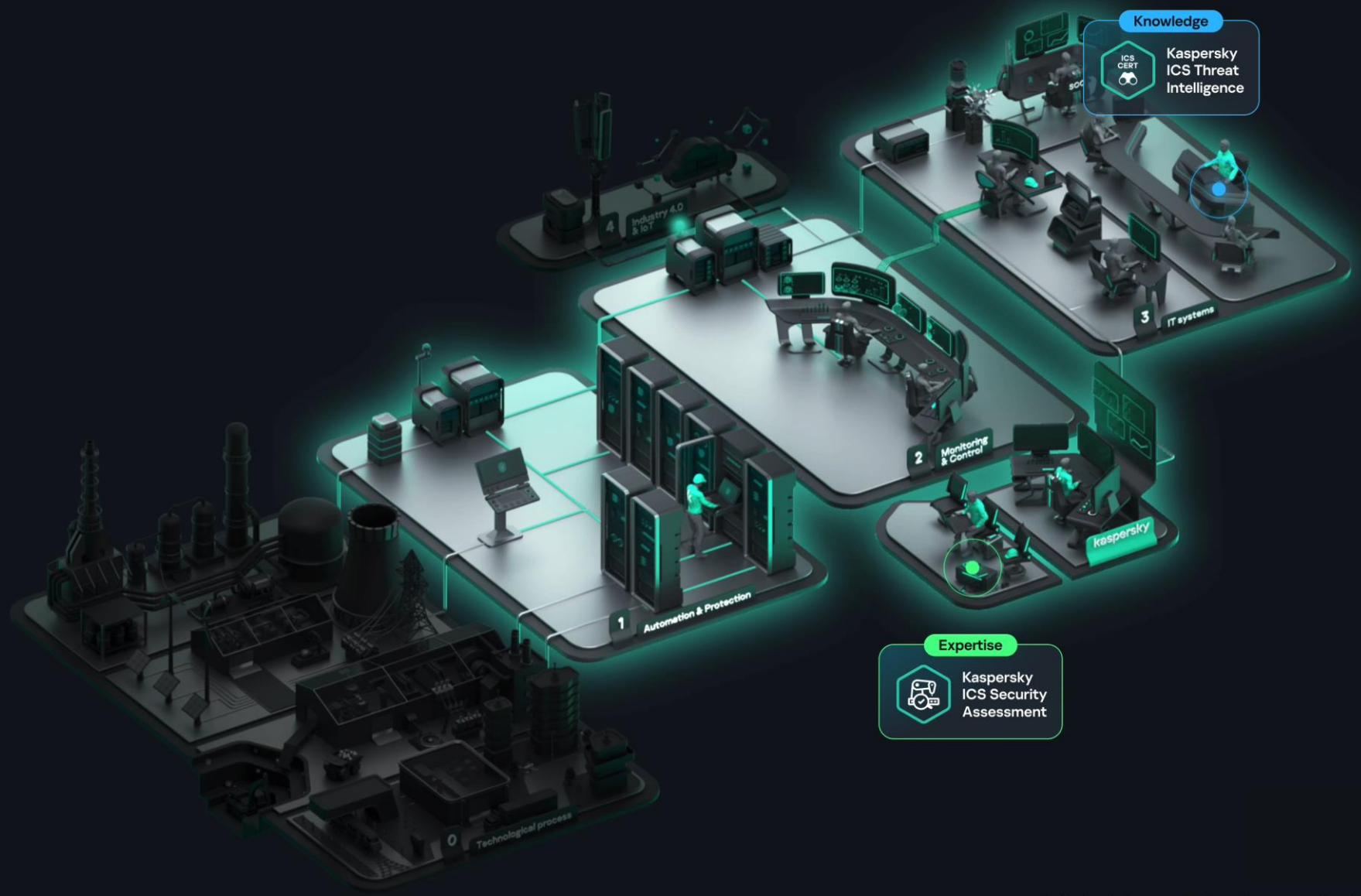
Industrial cyber resilience

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.



IEC 62443-3-3	SR 1.1*; SR 1.2; SR 1.3; SR 7.8^
IEC 62443-3-3	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



Industrial cyber resilience

8 steps to secure your enterprise

1
2
3
4
5
6
7
8

Assess: detailed risk evaluations

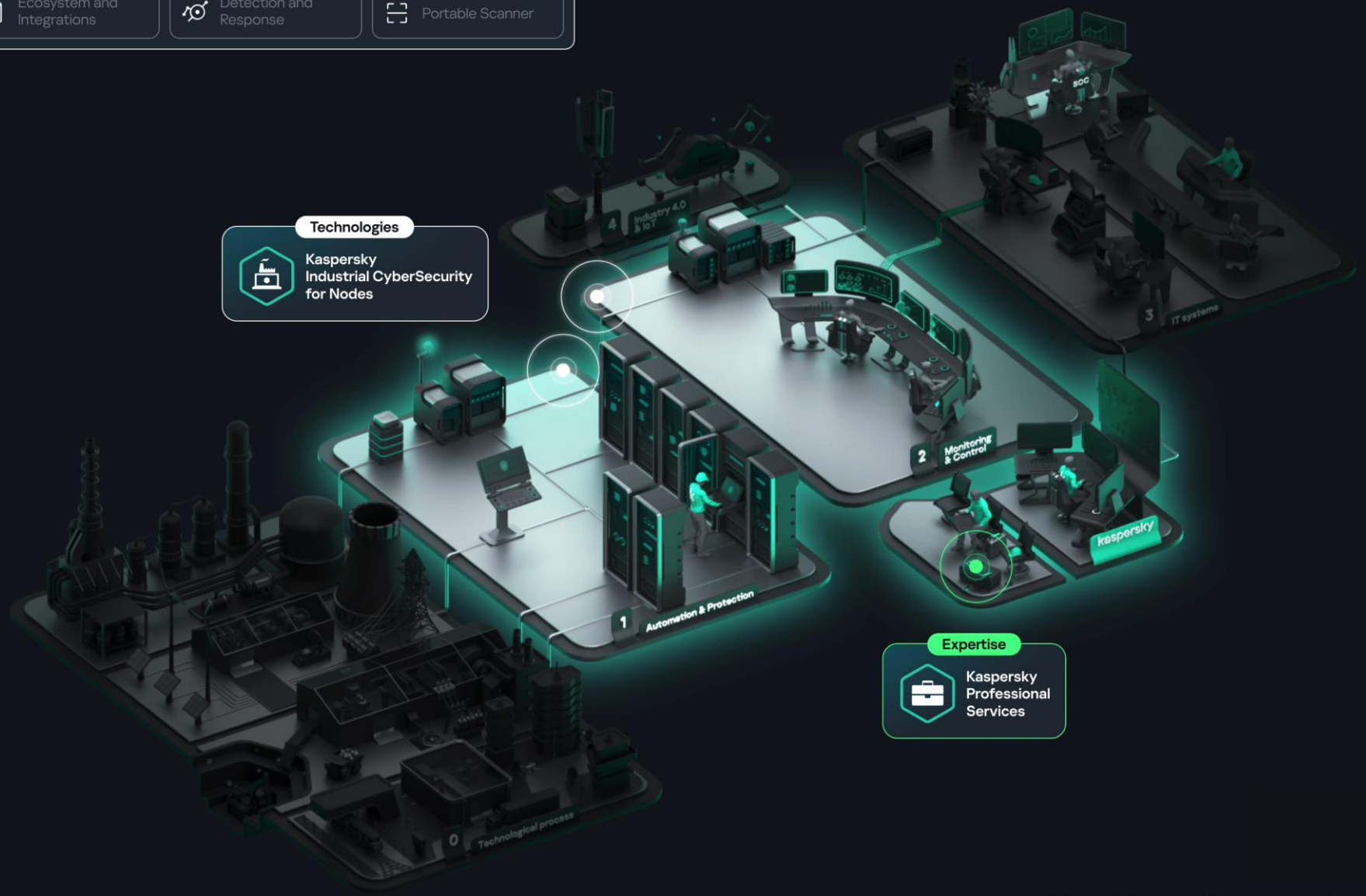
- 2.1 Identify vulnerabilities
- 2.2 Assets threats
- 2.3 Analyze impacts
- 2.4 Risk prioritization
- 2.5 Consider compliance

IEC 62443-3-3	ZCR: 3.*; 5.1; 5.2; 5.3; 5.4; 5.5; 5.8; 5.10; 5.12^; 5.13^
NIS2	A. 21: p. 2 (a, f); A. 22: p. 1
NIST SP 800-82r3	3.3.6; 6.1.3

Technologies · Expertise · Knowledge

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
2
3
4
5
6
7
8

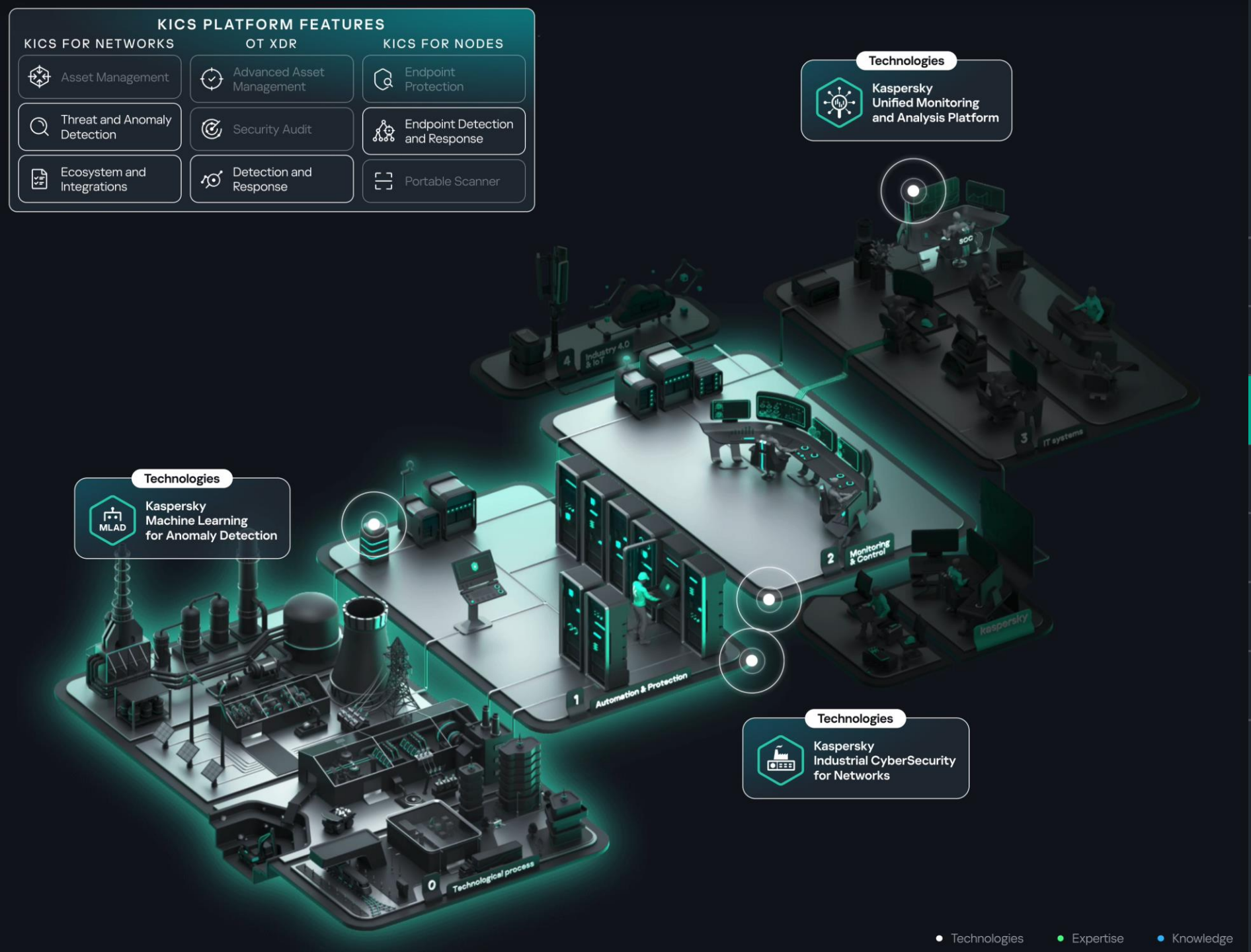
Secure: essential protection

- 3.1 Harden and configure your endpoints
- 3.2 Configure baseline of system integrity
- 3.3 Deploy EPP
- 3.4 Implement access control

IEC 62443-3-3	SR 1.1*; SR 1.2; SR 1.3; SR 7.8^
IEC 62443-3-3	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

Industrial cyber resilience

8 steps to secure your enterprise



1
2
3
4
5
6
7
8

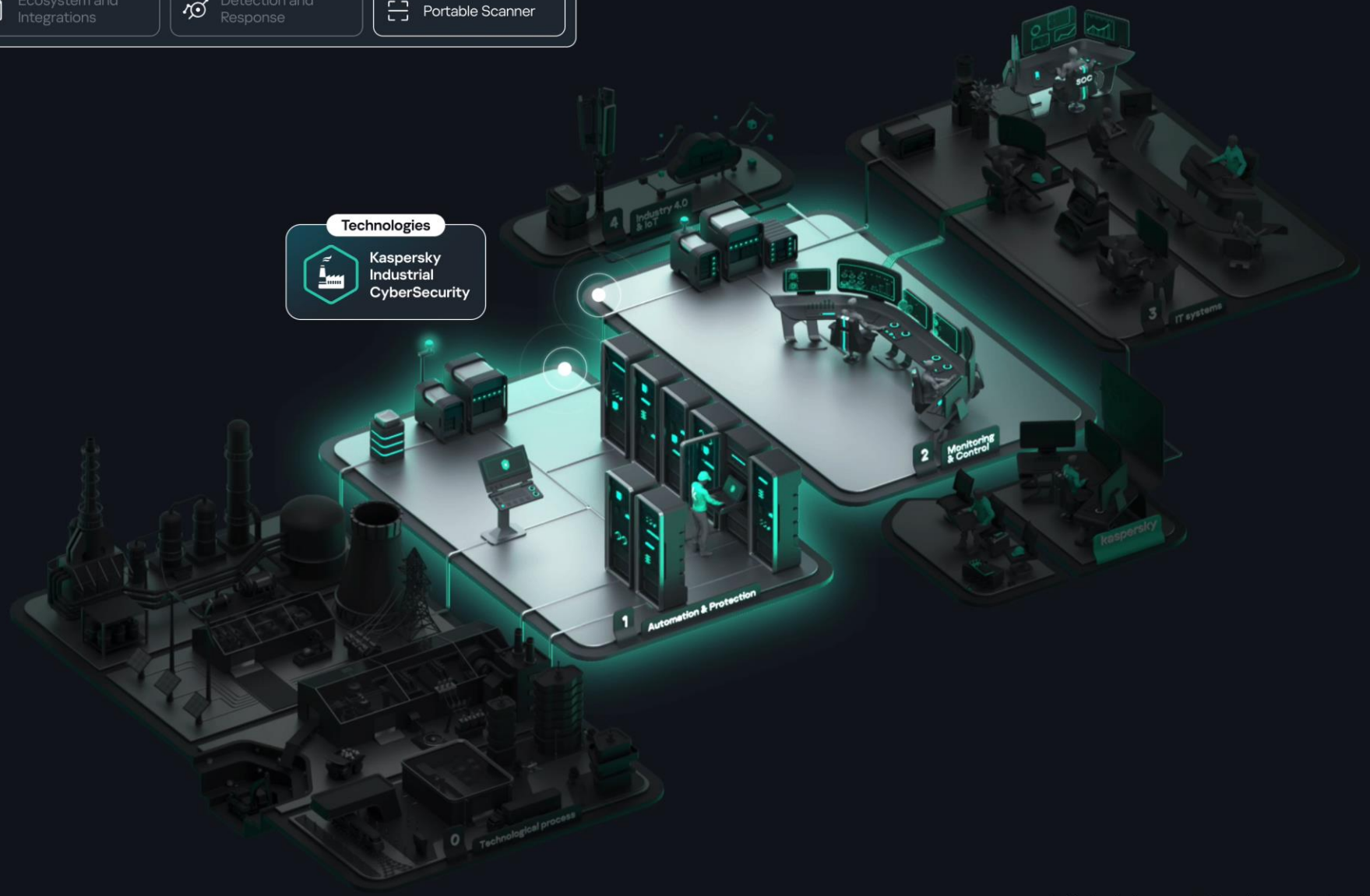
Detect: spot threats and anomaly

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

IEC 62443-3-3	SR 1.1*; SR 1.2; SR 1.3; SR 7.8^
IEC 62443-3-3	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

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

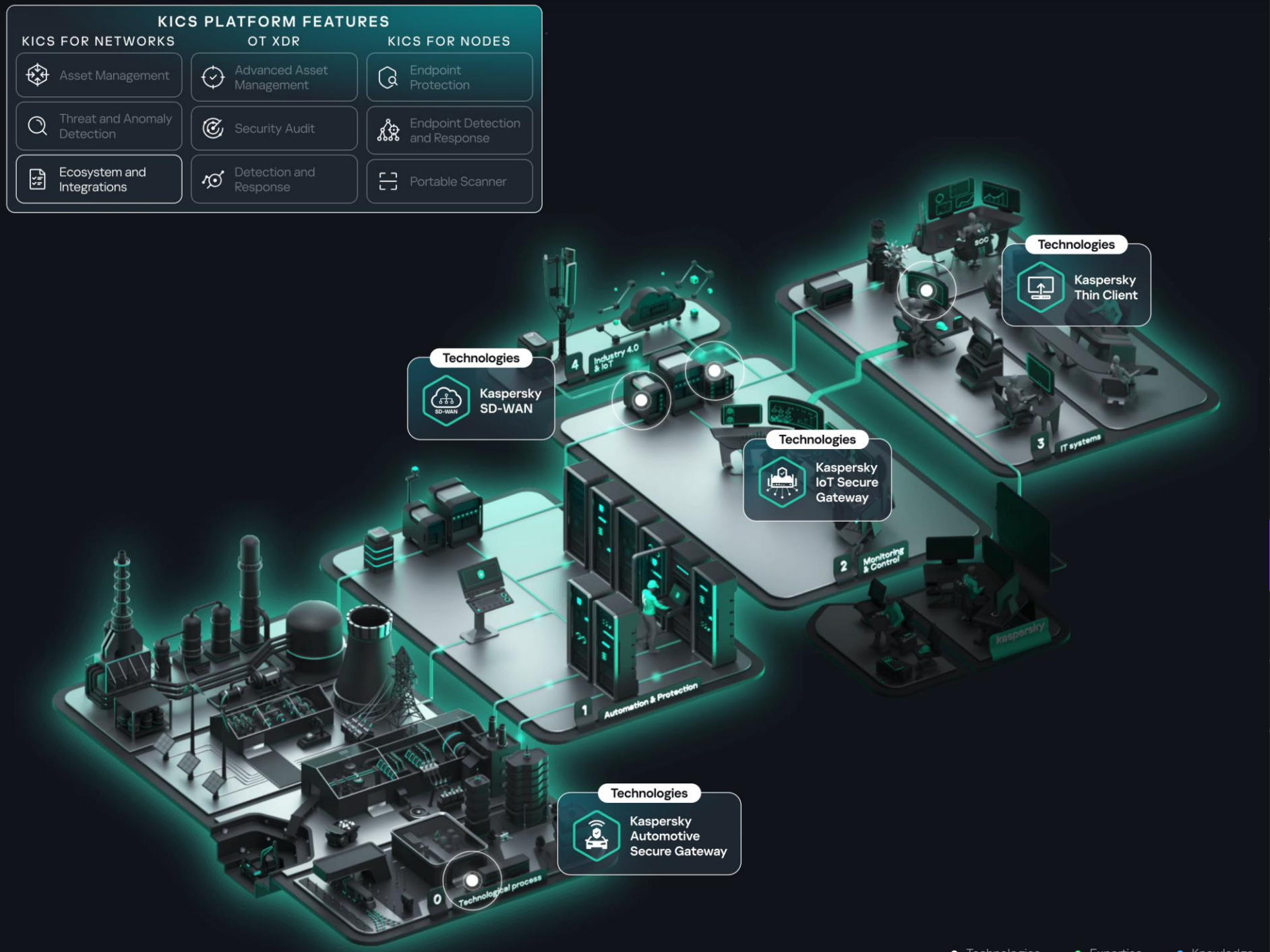
8 steps to secure your enterprise

1.
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.

IEC 62443-3-3	SR 1.1*; SR 1.2; SR 1.3; SR 7.8^
IEC 62443-3-3	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

Industrial cyber resilience

8 steps to secure your enterprise

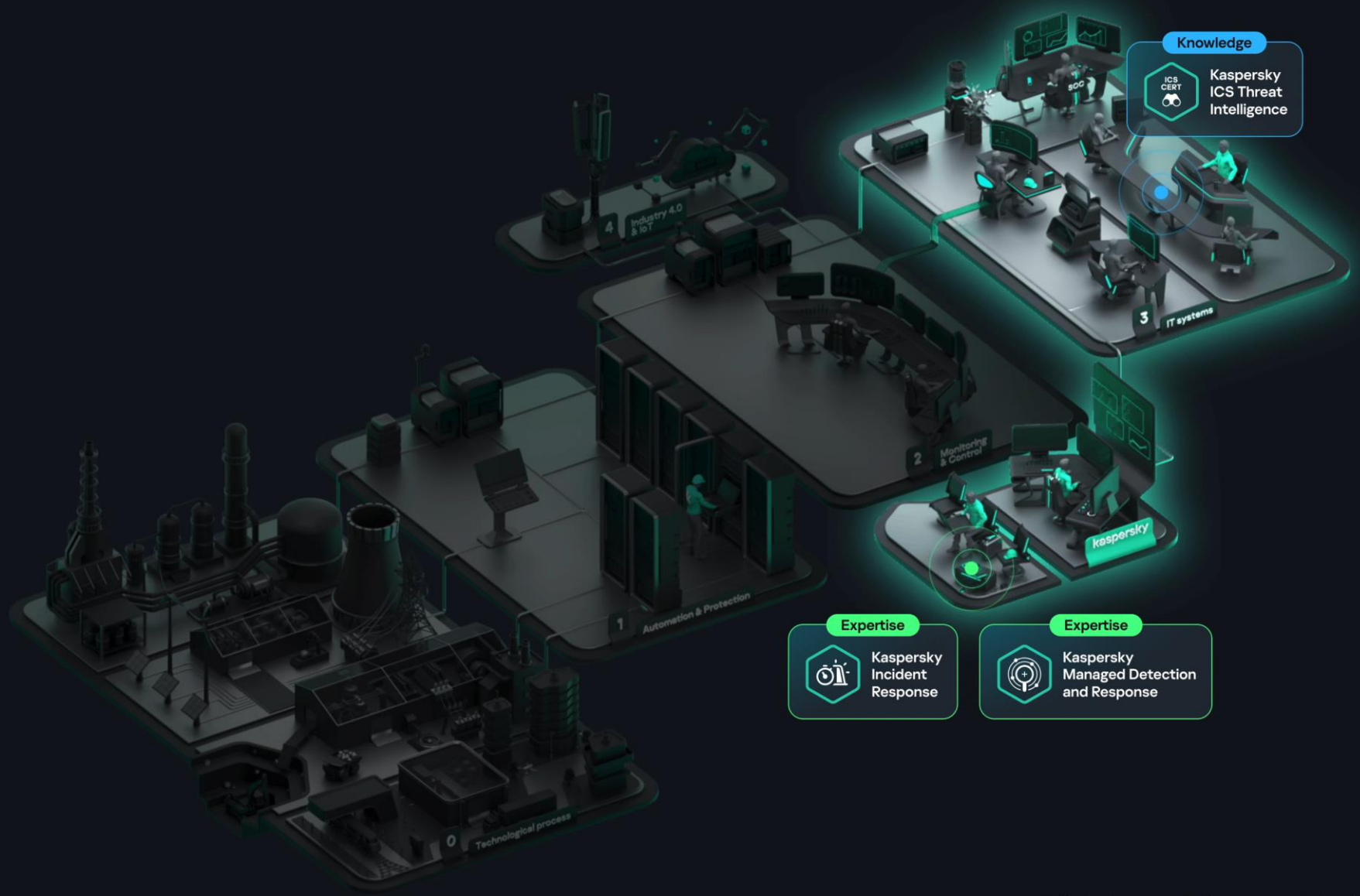


1.
2.
3.
4.
5.
6. **Enhance: zones and conduits**
   - 6.1 Continuously improve network segmentation
   - 6.2 Map zones
   - 6.3 Model conduits
   - 6.4 Implement and configure
   - 6.5 Test your setup
7.
8.

IEC 62443-3-3	SR 1.1*; SR 1.2; SR 1.3; SR 7.8^
IEC 62443-3-3	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

Industrial cyber resilience

8 steps to secure your enterprise



1
2
3
4
5
6
7
8

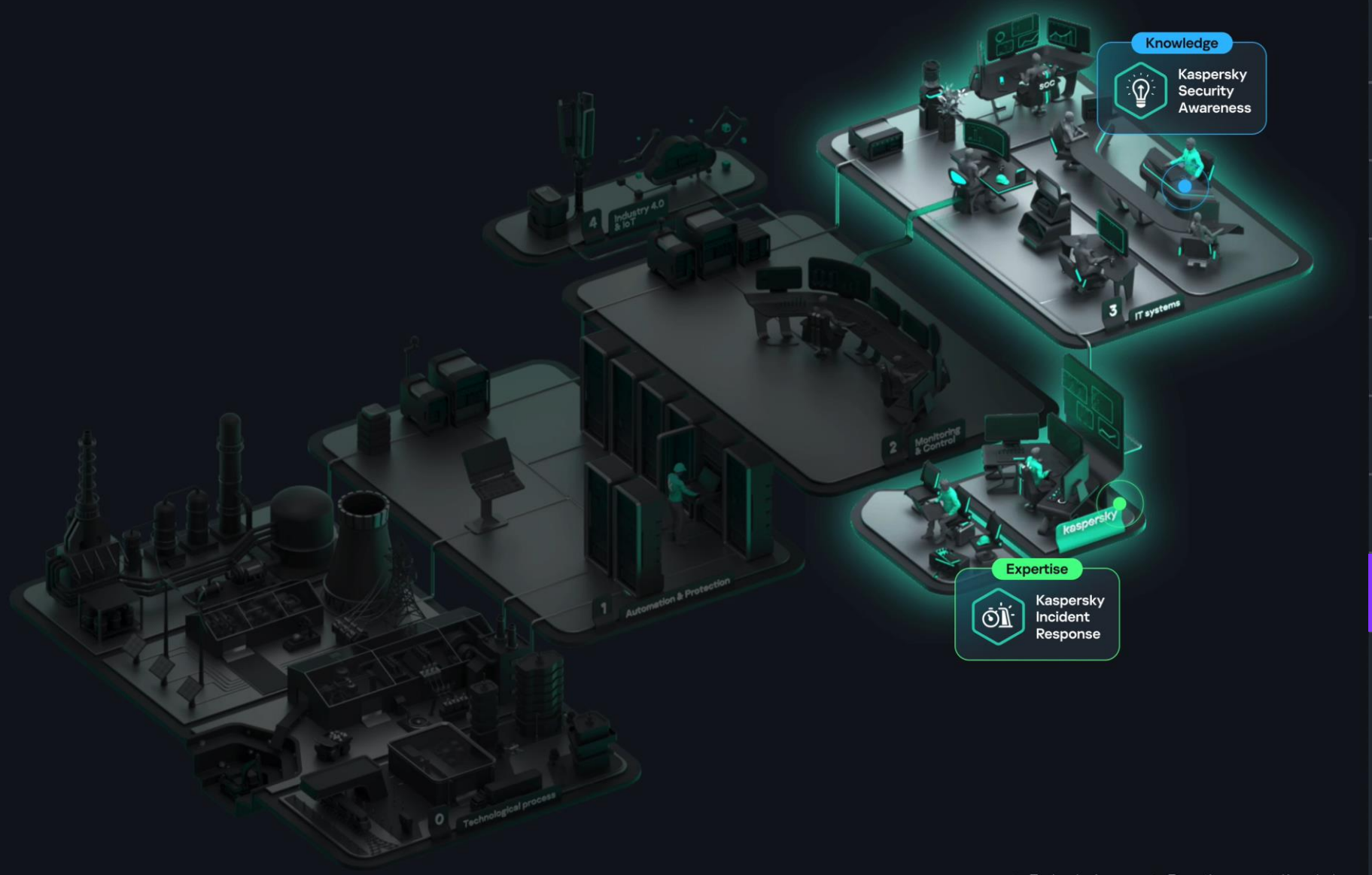
Monitor: mature sec. operations

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

IEC 62443-3-3	SR 1.1*; SR 1.2; SR 1.3; SR 7.8^
IEC 62443-3-3	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

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

IEC 62443-3-3	SR 1.1*; SR 1.2; SR 1.3; SR 7.8^
IEC 62443-3-3	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

Technologies · Expertise · Knowledge

Vertical Solutions: speaking your customer's language.

LAUNCHED IN 2025

EXPECTED IN 2026

- Logistics (Airports, Marinas)
- Stadiums & Smart Buildings
- Chemicals
- MMM
- OT SOC

Customer engagement path

FREE ASSESSMENT BY KICS PILOTING*

(Asset inventory & Risk Assessment)

- Assets discovery
- Applications, & users identification
- Network topology map
- Communication paths and conduits
- Threats & Vulnerabilities
- OVAL-based compliance audit

* IEC 62443 says that an organization must account all of assets and systems as well as conduct risk assessment before implementing everything.

1. Define facility test area, its availability, and success criteria's
2. Run pilot + tests with OT HW/SW are possible at this stage
3. Report on the findings with expert insights

OUTCOMES

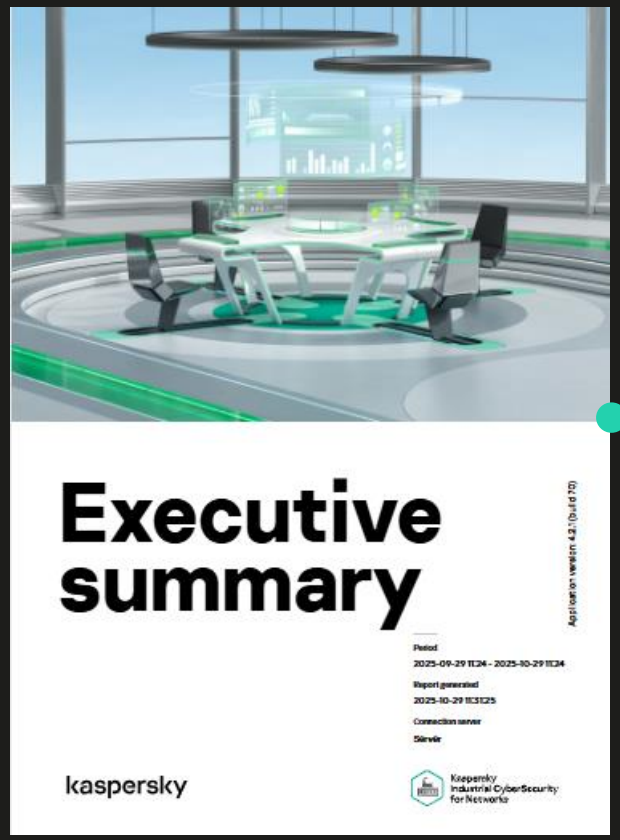
- Full visibility of infrastructure
- Assets inventory
- Assets behavior
- Blind spots identification
- Vulnerabilities detection
- Compliance score
- Risk score

HELPS TO UNDERSTAND

achieved level of cybersecurity

prioritize further countermeasures and steps

PoC results - Situational awareness



- Network topology and communication map
- Device identification, inventory and categorization
- Device parameters
- Device security status
- Events and detected malicious actions
- Security risks and abnormal activity
- Vulnerabilities
- Active risks scoring
- Mitigation actions

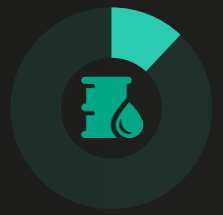
Kaspersky Industrial Cybersecurity: results to date

15+ years
of experience in multiply segments

1000+
industrial customers

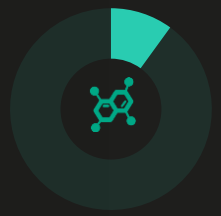
240+
tested systems from 70 vendors

IEC/ISO
Industry-leading audits: IEC 62443-4-1, ICS/IEC 27001, SOC 2 Type 2



12%
Protecting #60 O&G companies with 12% of a total world extraction

15%
Protecting 15% of commercial nuclear reactors



10%
Protecting 10% of global petrochemical production (varies by products)

Learn more

Contact us