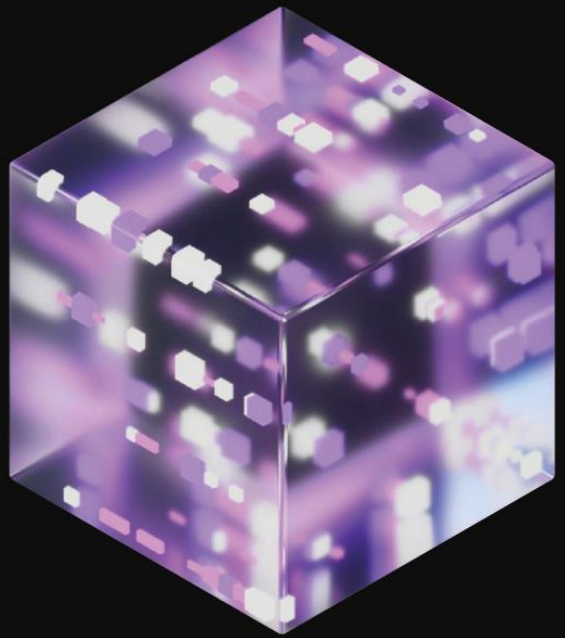
8 Bước Để Tăng Cường ATTT Cho Môi Trường Công Nghiệp

GIẢI PHÁP AN NINH MẠNG
KASPERSKY

kaspersky bring on the future



Agenda

01. Tổng Quan Về Kaspersky

02. Giải Pháp Hội Tụ An Toàn Thông Tin Môi Trường IT và OT

03. 8 Bước Để Tăng Cường ATTT Cho Môi Trường OT

Global expertise

200 countries and regions

5,000+ highly qualified specialists

30+ representative regional offices

50% of our employees are R&D

Africa
South Africa
Kenya
Rwanda

Asia
Vietnam
Greater China (China, Hong Kong)
India
Japan
Kazakhstan
Malaysia
Singapore
South Korea

Europe
Czech Republic
France
Germany
Israel
Italy
Netherlands
Portugal
Romania
Russia
Spain
Switzerland
UK

Middle East
Saudi Arabia
Turkey
UAE

Latin America
Brazil
Mexico

Transparency Centers
Zurich, Switzerland
Madrid, Spain
São Paulo, Brazil
Kuala Lumpur, Malaysia
Kigali. Rwanda
Singapore
Tokyo, Japan
Rome, Italy
Utrecht, the Netherlands
Riyadh, Saudi Arabia
Istanbul, Turkey

Chuyên Môn Làm Cốt Lõi

Every center contributes to Kaspersky's solutions and services

- Threat Research
- Incident Investigation

Kaspersky Global Research and Analysis Team

- Researches the most complex threats; APT, cyber espionage campaigns, global cyber epidemics, etc.
- Security of future-focused technologies
- Investigates sophisticated financial cybercrime

Kaspersky Threat Research

- Anti-Malware Research
- Content Filtering Research
- SSDLC & Secure-by-Design Methodologies

Kaspersky AI Technology Research

- AI Cybersecurity
- GenAI Research
- AI-Powered Threat Detection / Solutions

Kaspersky Security Services

- MDR
- Incident Response
- Security Assessment
- SOC Consulting
- Digital Footprint Intelligence

Kaspersky ICS CERT

- Critical Infrastructure Threat Analysis
- ICS Vulnerability Research and Assessment
- Technology associations, analytics and standards

Công Nghệ Tiên Tiến Kế Thừa Từ Chuyên Gia Toàn Cầu Và Công Nghệ AI

Nghiên cứu và điều tra

Nghiên cứu về mối đe dọa và điều tra sự cố hàng đầu thế giới là yếu tố cốt lõi trong danh mục sản phẩm của chúng tôi.

Bộ giải pháp bảo mật chúng tôi giúp khách hàng luôn đón đầu các mối đe dọa mới trên toàn cầu cũng như tại Việt Nam

Phòng vệ cùng công nghệ AI

Phương pháp "an ninh là trên hết" đối với trí tuệ nhân tạo đã được tích hợp vào các giải pháp của chúng tôi.

Phương pháp tiếp cận an toàn dựa trên trí tuệ nhân tạo xuyên suốt quá trình phản ứng sự cố.

Phát triển phần mềm an toàn

Áp dụng nguyên tắc bảo mật trong tất cả giai đoạn thiết kế sản phẩm.

Bảo mật được tích hợp trong mọi giai đoạn phát triển sản phẩm của Kasperksy. Cách tiếp cận nghiêm ngặt của chúng tôi đảm bảo các hệ thống an toàn, bền vững; đem lại
giải pháp đáng tin cậy cho người dung.

~5,000
Chuyên gia trình độ cao

50%
Nhân viên trong lĩnh vực Nghiên cứu & Phát triển (R&D)

Hơn 50
Chuyên gia an ninh mạng được công nhận toàn cầu

5
Trung tâm
Chuyên môn Đặc biệt

Ưu Tiên Sự Minh Bạch Trên Hàng Đầu

Đã được chứng minh.
Minh bạch.
Độc lập.

Sáng kiến Minh bạch Toàn cầu của Kaspersky được xây dựng dựa trên các biện pháp cụ thể, có thể hành động, cho phép các bên liên quan xác minh và kiểm tra độ tin cậy của sản phẩm, quy trình nội bộ và hoạt động
kinh doanh của công ty.

13
Transparency Centers ở toàn cầu

Đánh giá độc lập định kỳ
- Kiểm toán SOC 2
- Chứng nhận ISO 27001

Bug bounty

Sự công nhận quan trọng

Các sản phẩm của Kaspersky trải qua các đánh giá độc lập định kỳ từ các viện nghiên cứu hàng đầu, với chuyên môn về an ninh mạng của chúng tôi luôn được các nhà phân tích ngành hàng đầu công nhận.

Được kiểm tra nhiều nhất. Được trao giải nhiều nhất.

Trong suốt hơn một thập kỷ, các sản phẩm của Kaspersky đã tham gia 1022 bài kiểm tra và đánh giá độc lập, đạt được 771 kết quả đứng đầu và 871 vị trí trong top 3 - minh chứng cho khả năng bảo vệ hàng đầu trong ngành của chúng tôi.

95	91	70%
Bài kiểm tra & đánh giá	Vị trí đầu tiên	Vị trí TOP 3

Đóng Góp Cho An Ninh Mạng Toàn Cầu

Là một thành viên chủ chốt và năng động trong cộng đồng thám báo mối đe dọa toàn cầu, chúng tôi làm việc chặt chẽ với cộng đồng an ninh mạng để chống lại tội phạm mạng trên toàn thế giới.

INTERPOL

PARIS CALL FOR TRUST AND SECURITY IN CYBERSPACE 11 • 12 • 2018

industrial internet CONSORTIUM

AFRIPOL

Coalition Against Stalkerware

MITRE | ATT&CK®

Chúng tôi đóng góp thông tin tình báo mối đe dọa quan trọng cho các tổ chức toàn cầu, bao gồm MITRE, nhằm nâng cao độ chính xác của framework này.

Công việc của chúng tôi được hướng dẫn bởi các nguyên tắc đạo đức trong việc tiết lộ lỗ hổng bảo mật có trách nhiệm.

Kaspersky củng cố an ninh cho toàn ngành bằng cách phát hiện và giúp khắc phục các lỗ hổng zero-day cho các công ty hàng đầu như Adobe, Microsoft, Google, Apple, v.v.

Bên cạnh đó, Kaspersky đang hợp tác với các tổ chức quốc tế như INTERPOL, các cơ quan thực thi pháp luật, các CERT và cộng đồng bảo mật CNTT toàn cầu trong các cuộc điều tra và chiến dịch chống tội phạm mạng chung

Công nghệ

1

Trang bị cho các đội ngũ bảo mật của bạn tổ chức những công cụ cần thiết để phát hiện và phản ứng với các mối đe dọa mạng.

Tăng cường khả năng phòng vệ

Tiếp cận các chuyên gia bên ngoài để đánh giá, phản ứng sự cố ngay lập tức và đưa ra chỉ dẫn chiến lược.

Kiến thức

2

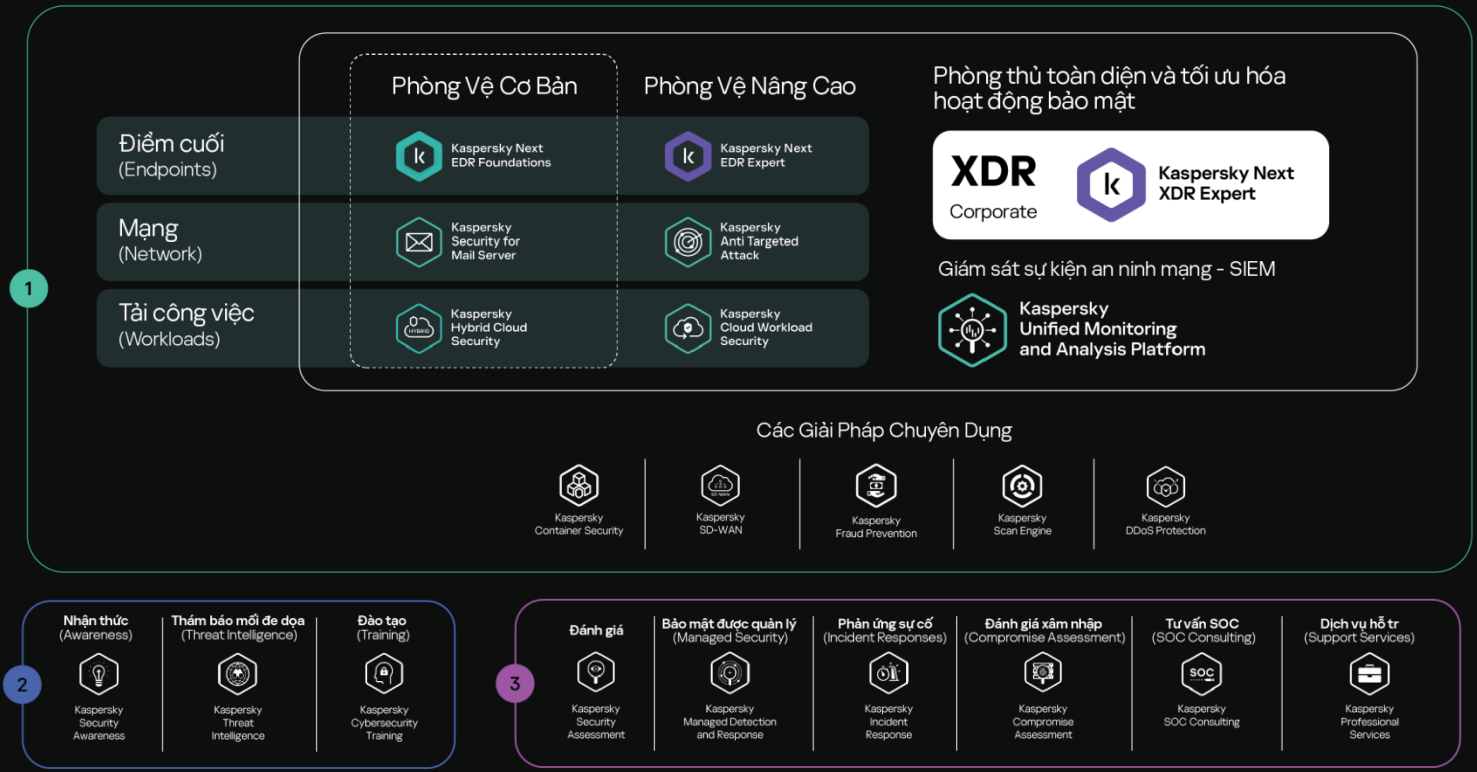
Cập nhật thông tin về các mối đe dọa đang phát triển, liên tục nâng cao kỹ năng cho đội ngũ của bạn để xử lý sự cố hiệu quả và thúc đẩy nhận thức về an ninh.

Chuyên môn

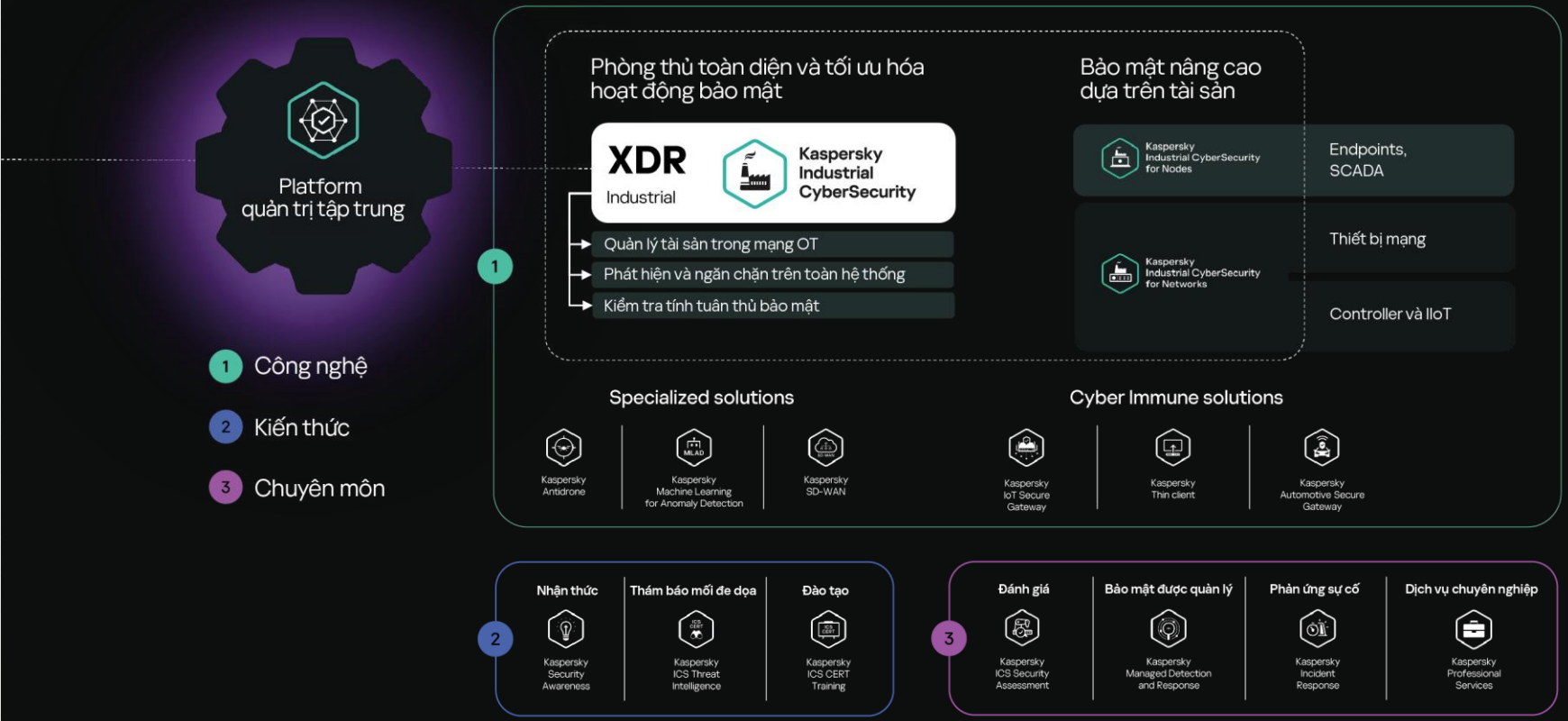
3

Đồng hành các chuyên gia của Kaspersky để đánh giá, phản ứng sự cố ngay lập tức và đưa ra các khuyến nghị cần thiết cho chiến lược phòng vệ.

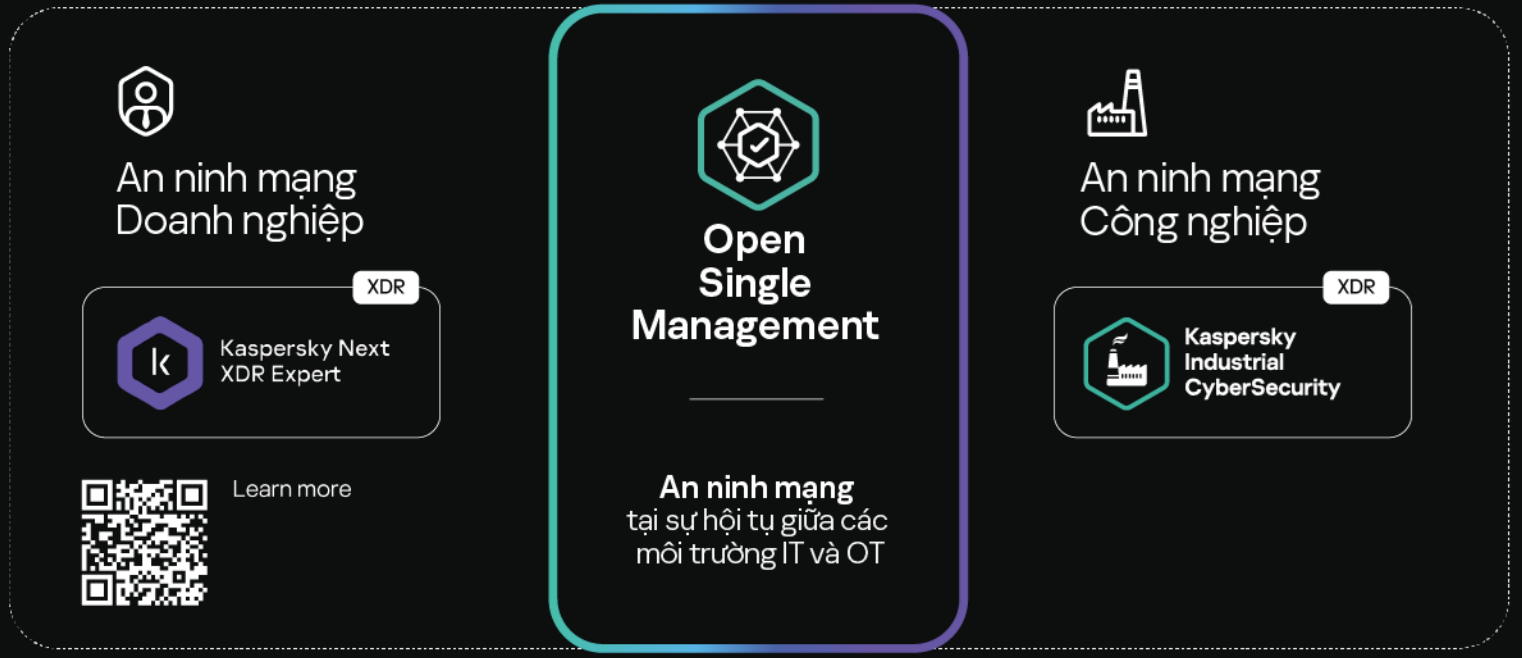
Kaspersky: Bộ Giải Pháp Bảo Mật Toàn Diện Cho Môi Trường IT



Kaspersky: Bộ Giải Pháp Bảo Mật Toàn Diện Cho Môi Trường OT



Nền Tảng Hội Tụ An Toàn Thông Cho Các Môi Trường IT, OT Và Môi Trường Hybrid

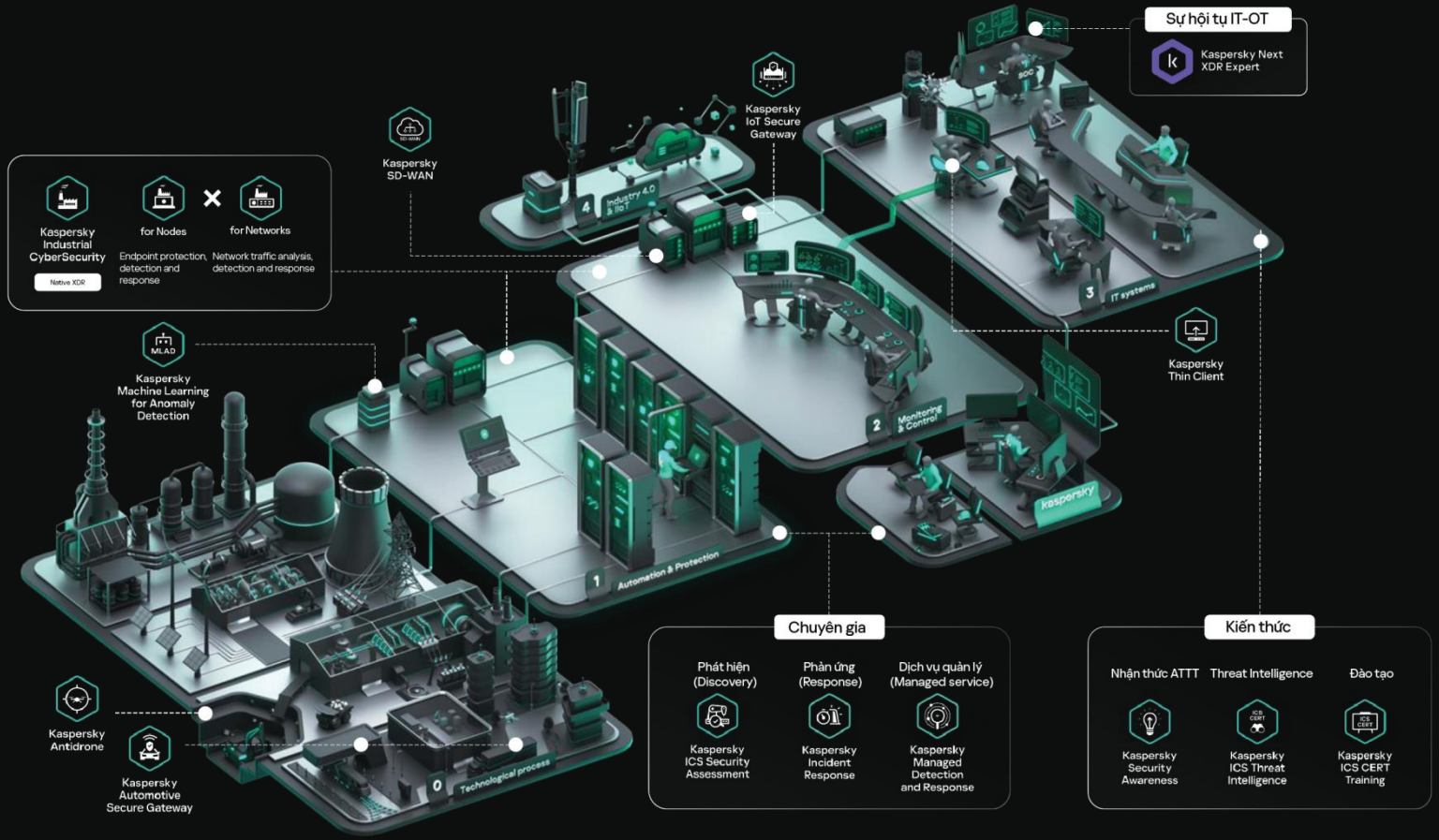


Kaspersky
OT CyberSecurity

8 Bước Để Tăng Cường ATTT Cho Môi Trường OT

Đảm bảo sự an toàn thông tin cho hệ thống OT, kết hợp các công nghệ, kiến thức và chuyên môn cần thiết để bảo vệ các doanh nghiệp công nghiệp ở mọi cấp độ.

Bảo Vệ Toàn Diện Cho Các Doanh Nghiệp Công Nghiệp Và Năng Lượng



Nền Tảng OT XDR Cho Bảo Vệ Cơ Sở Hạ Tầng Trọng Yếu

Native OT XDR

Kaspersky Industrial CyberSecurity

for Nodes
Endpoint protection, detection and response

×

for Networks
Network traffic analysis, detection and response

Native OT XDR

Nền Tảng OT XDR Cho Bảo Vệ Cơ Sở Hạ Tầng Trọng Yếu

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 OT CyberSecurity

IT – OT Convergence

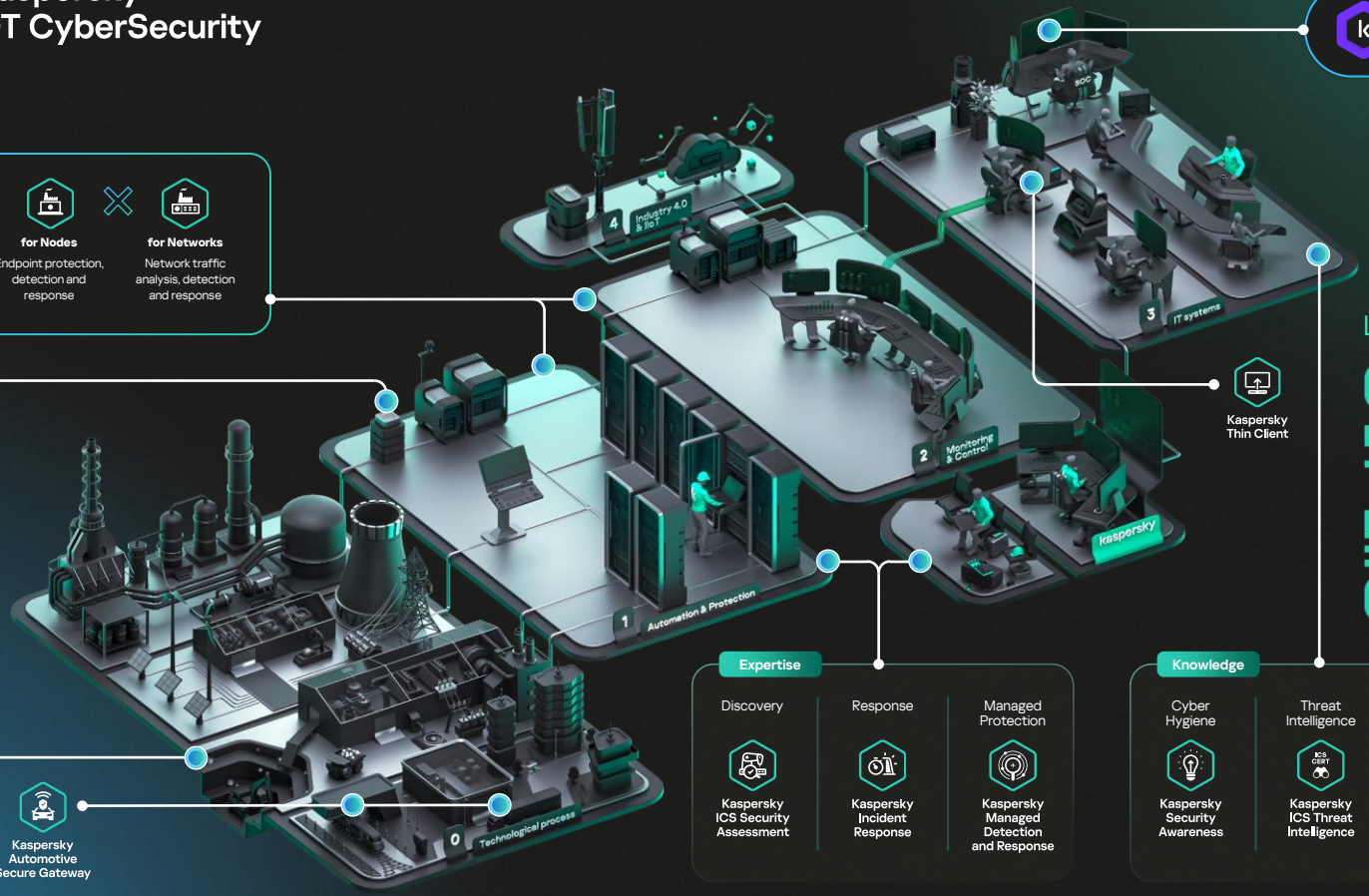
Kaspersky Next XDR Expert

Kaspersky Industrial CyberSecurity

Native XDR

for Nodes
Endpoint protection, detection and response

for Networks
Network traffic analysis, detection and response



Kaspersky Machine Learning for Anomaly Detection

Kaspersky Thin Client

Kaspersky Antidrone

Kaspersky Automotive Secure Gateway

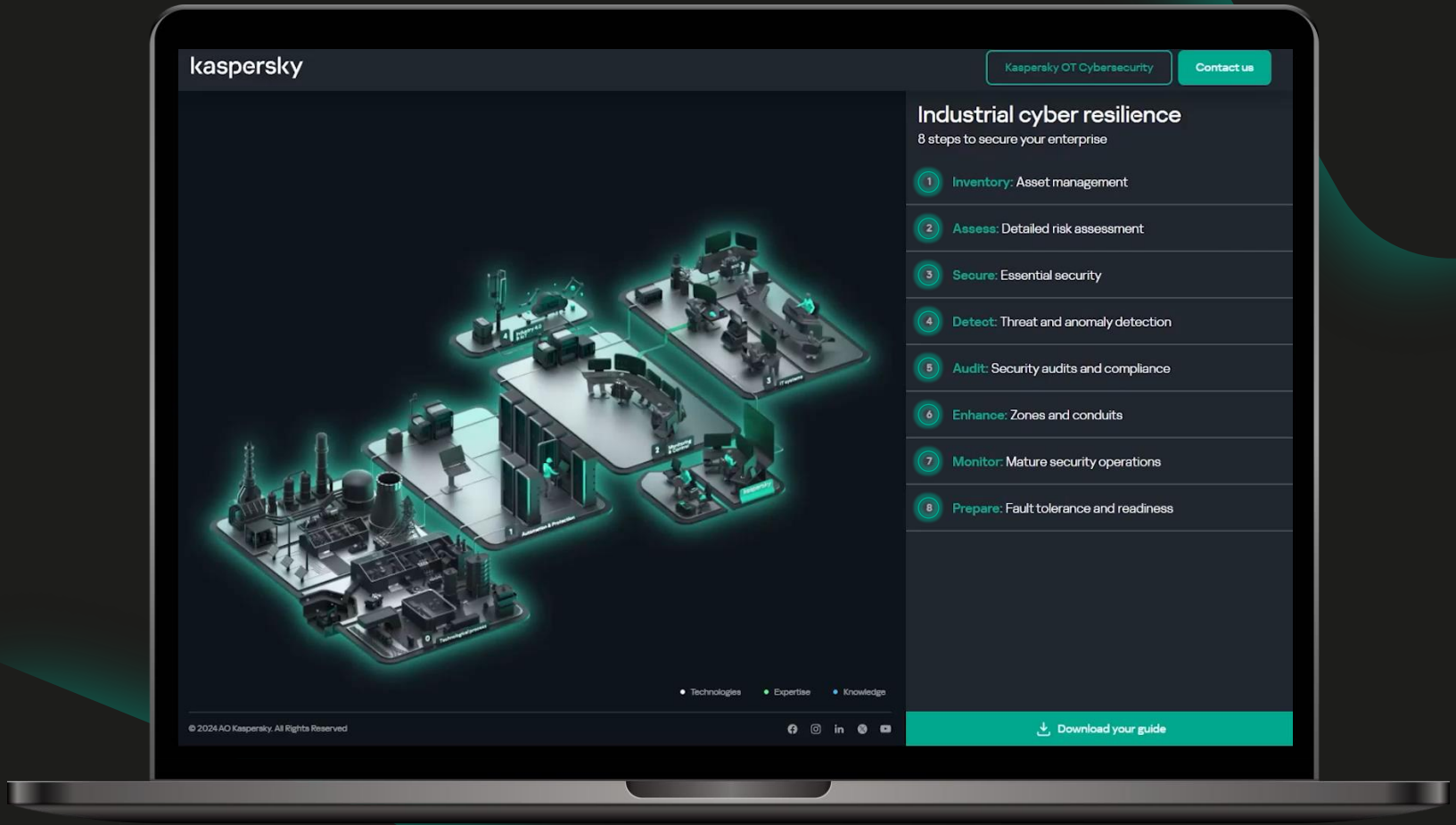
Learn more

Expertise

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

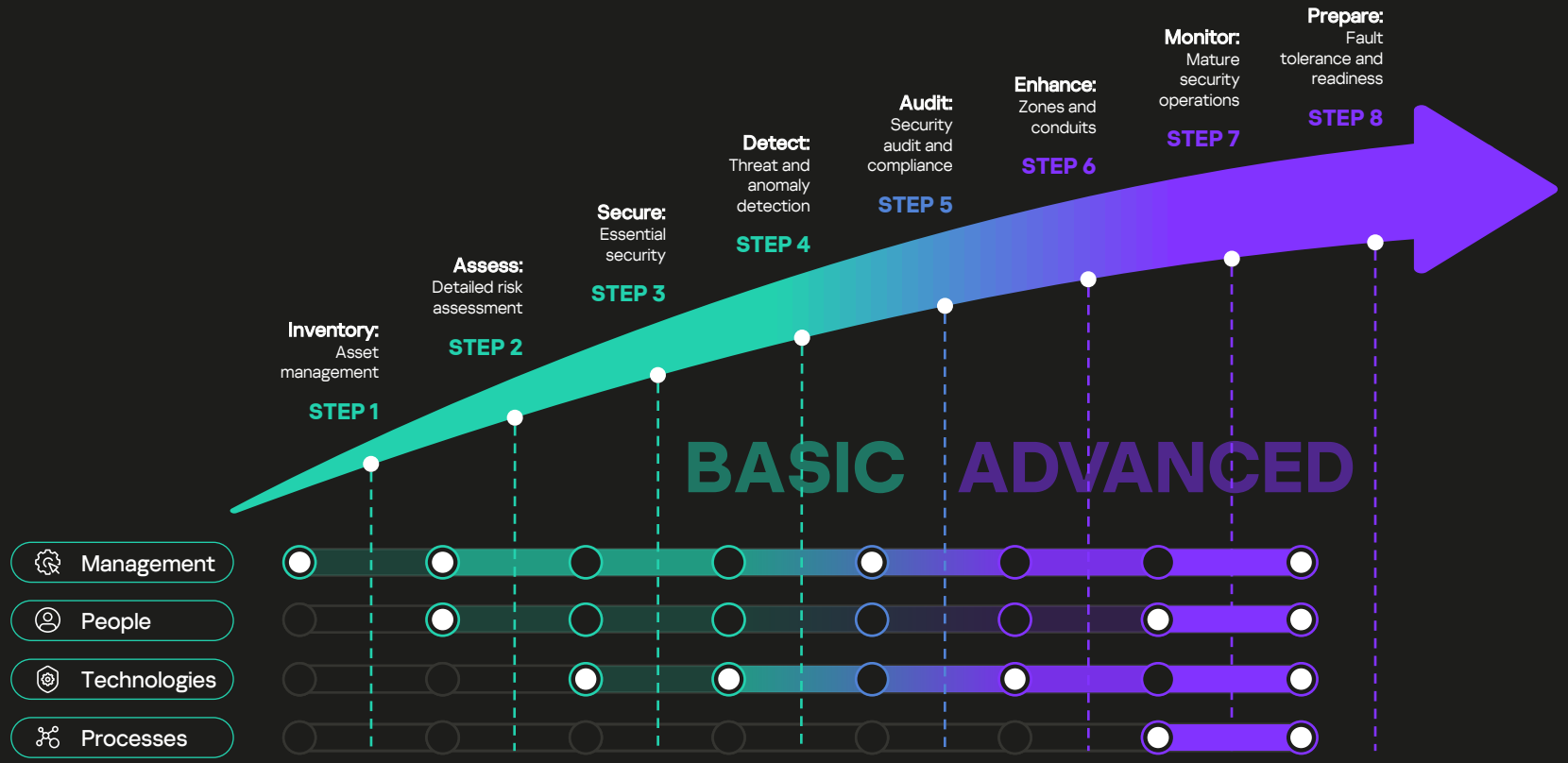
Knowledge

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

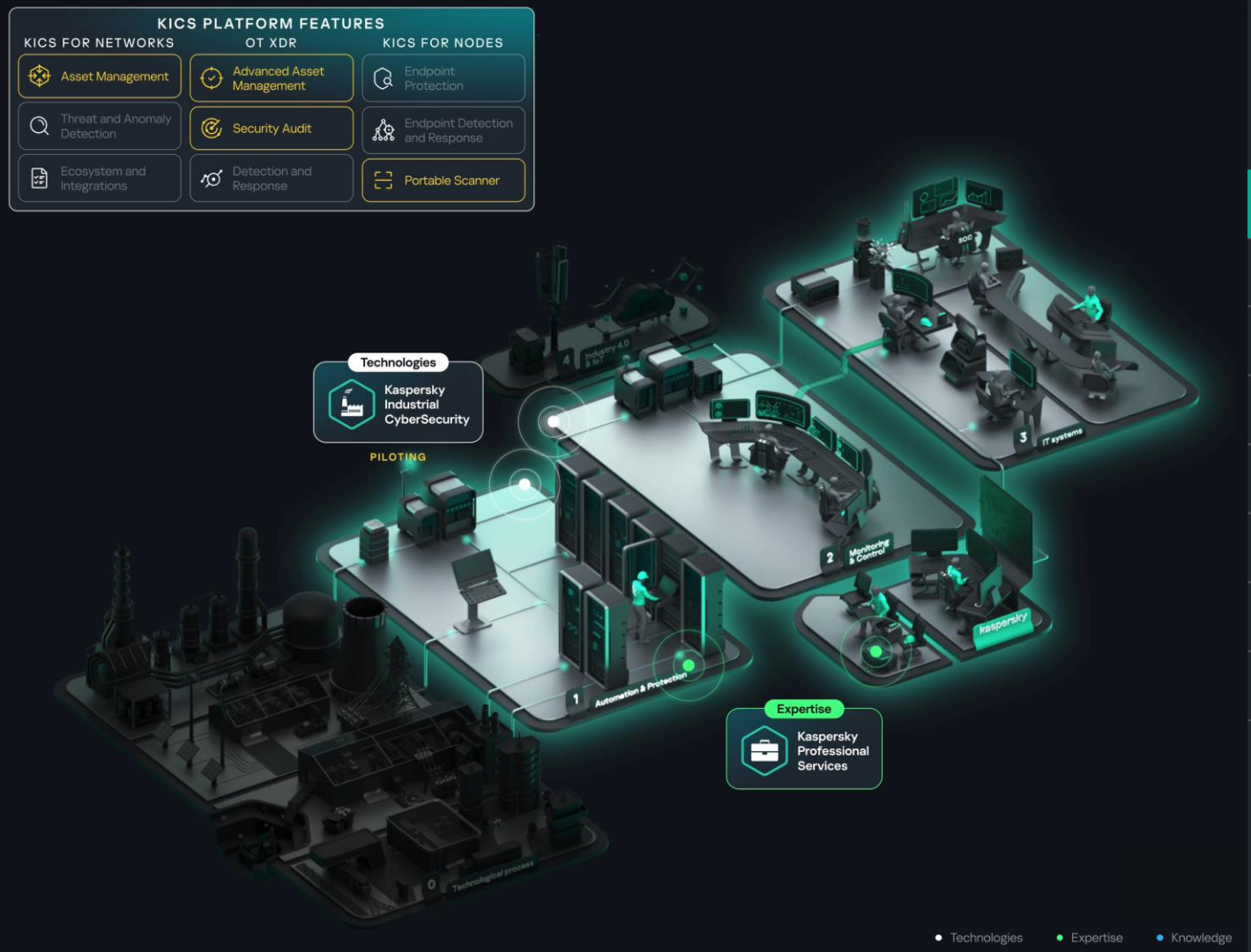


https://www.kaspersky.com/go/industrialcyberresilience

8 Bước Để Tăng Cường ATTT Cho Môi Trường OT



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



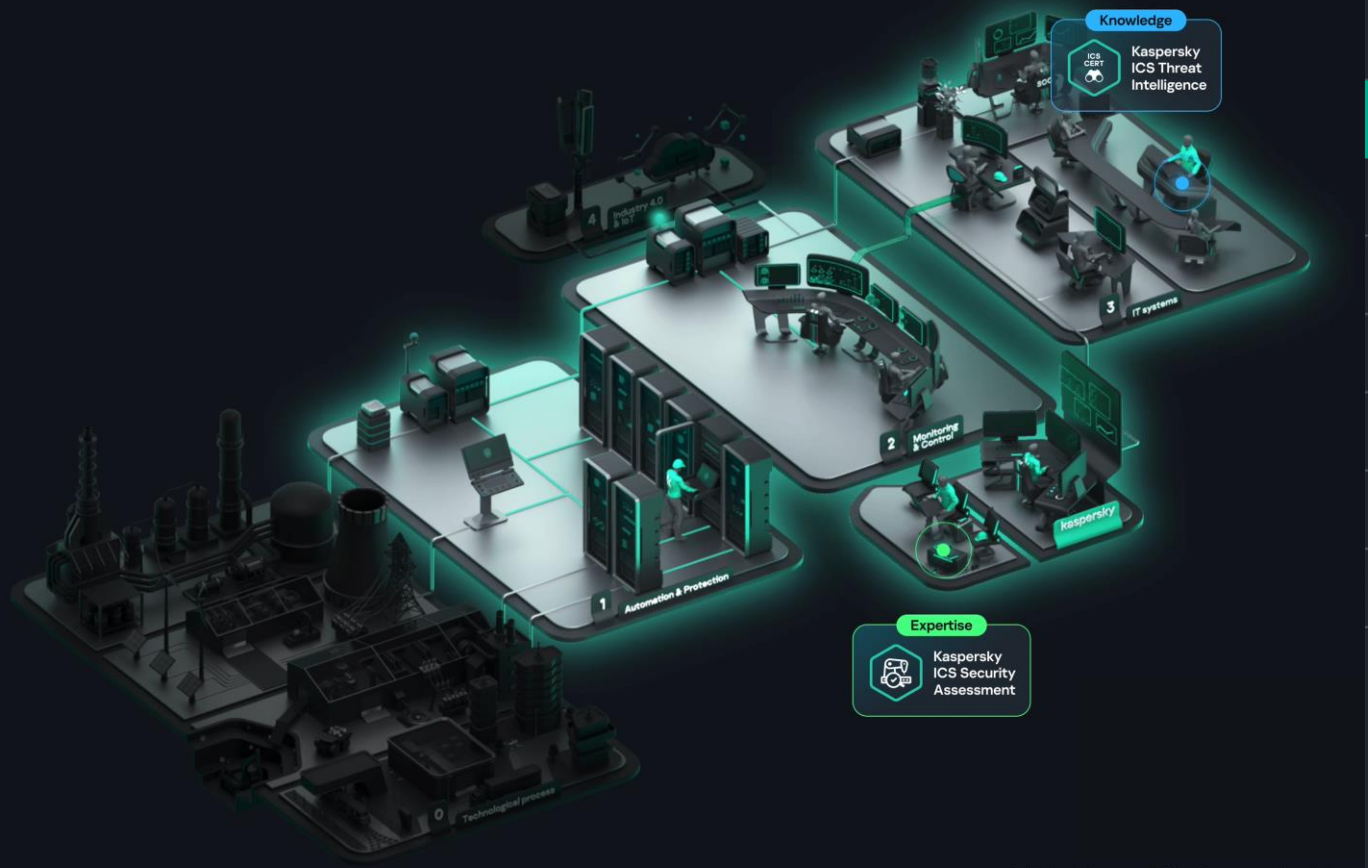
Industrial cyber resilience

8 steps to secure your enterprise

1. **Inventory: asset management**
2. 1.1 Outline objectives
3. 1.2 Prepare for discovery
4. 1.3 Use active pooling
5. 1.4 Map network
6. 1.5 Inventory
7. 1.6 Monitor continuously
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, I), p. 3
NIST SP 800-82r3	6.1.1: Asset Management
GB/T 44462.1	7.3.5.5.3: Asset Management



Industrial cyber resilience

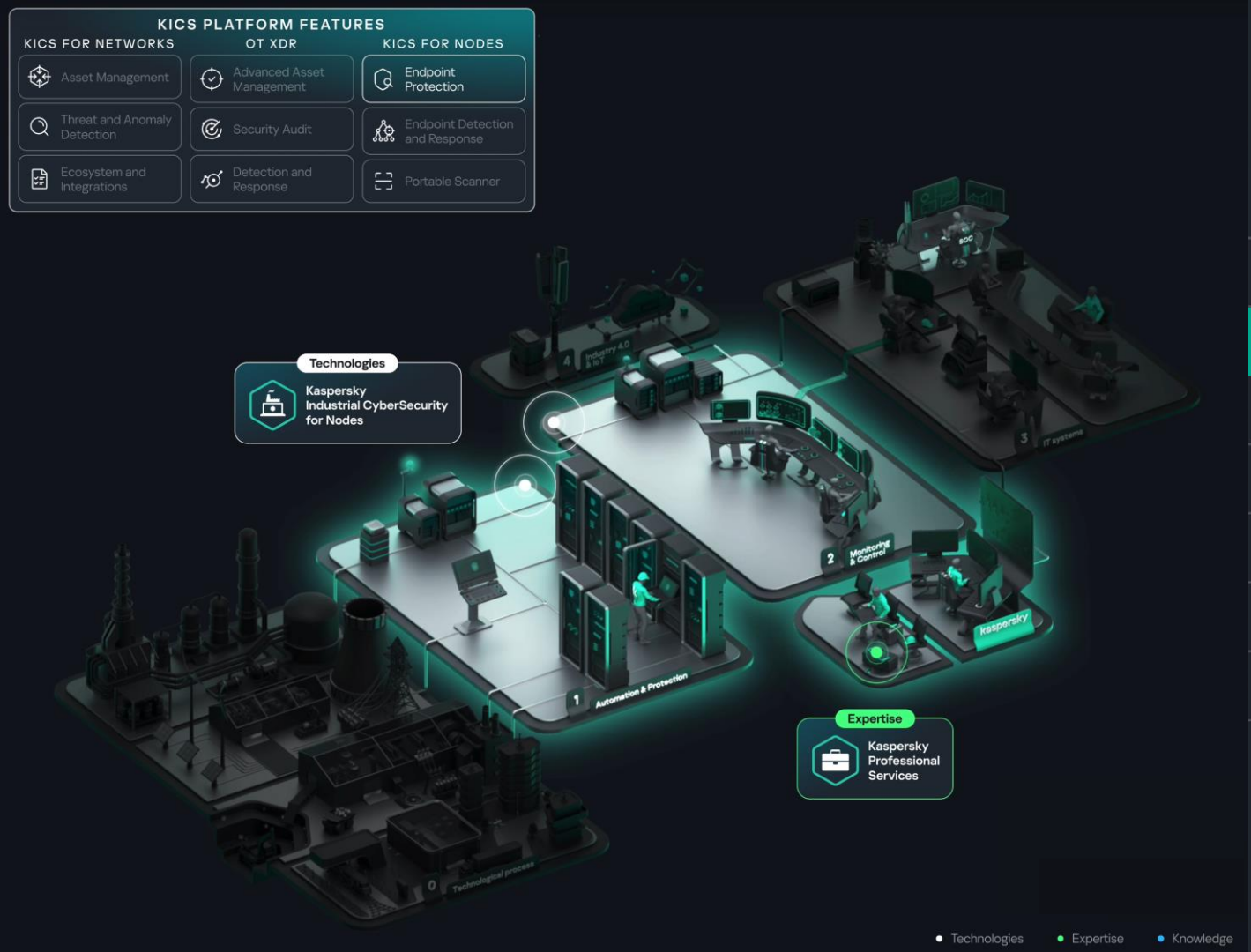
8 steps to secure your enterprise

1
2 **Assess:** detailed risk evaluations
- 2.1 Identify vulnerabilities
- 2.2 Assets threats
- 2.3 Analyze impacts
- 2.4 Risk prioritization
- 2.5 Consider compliance

3
4
5
6
7
8

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



Industrial cyber resilience

8 steps to secure your enterprise

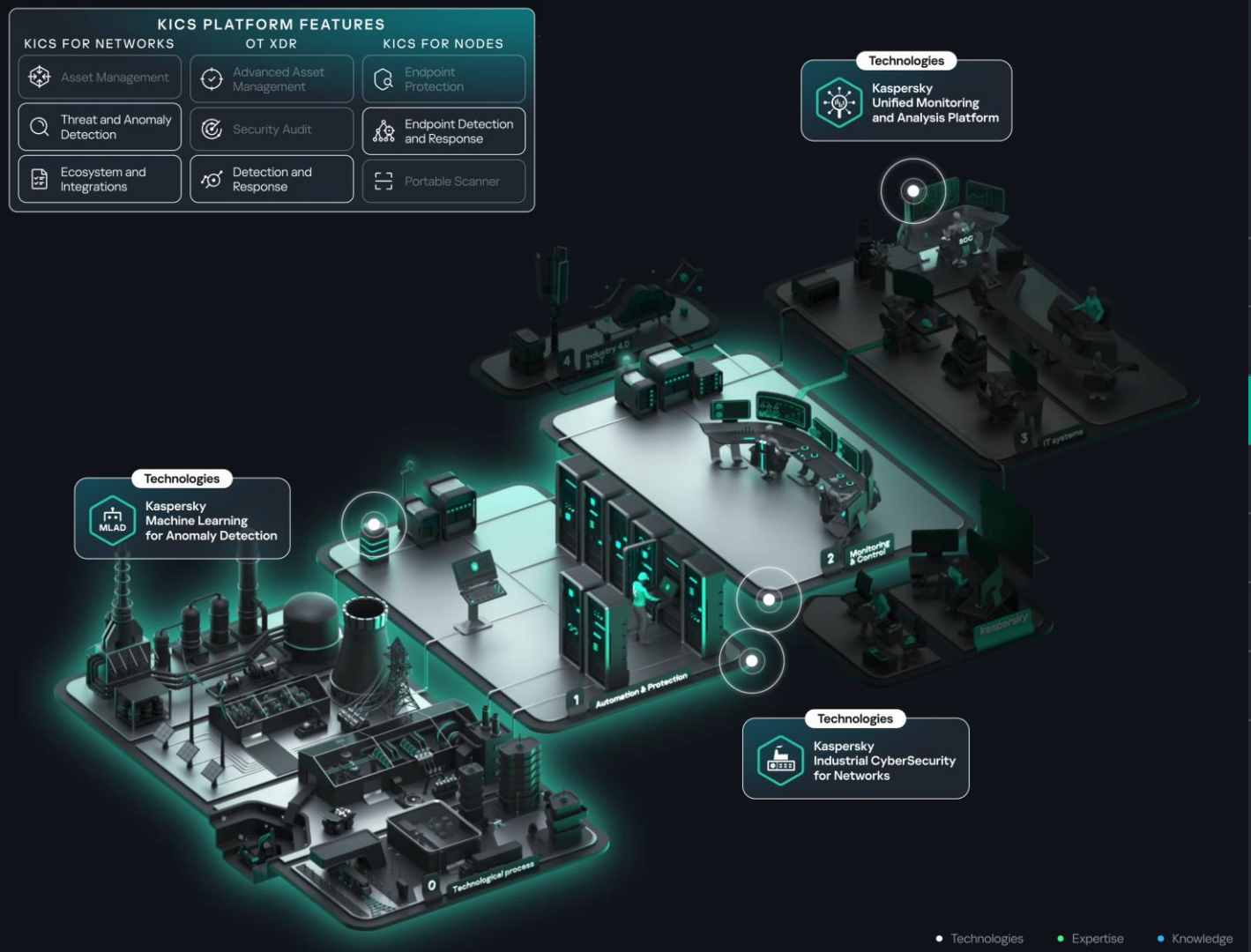
1
2
3
4
5
6
7
8

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

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

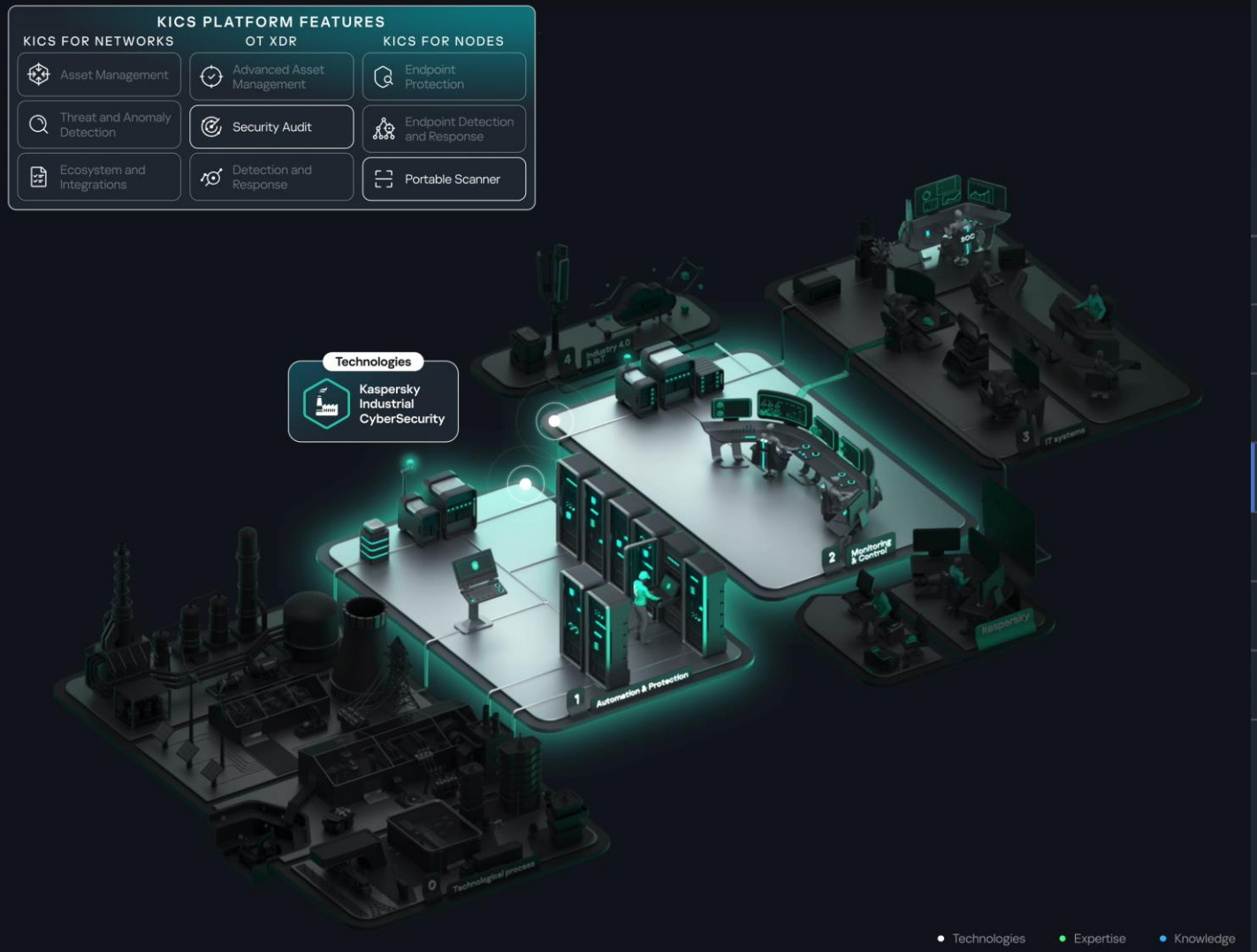
1
2
3
4
5
6
7
8

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



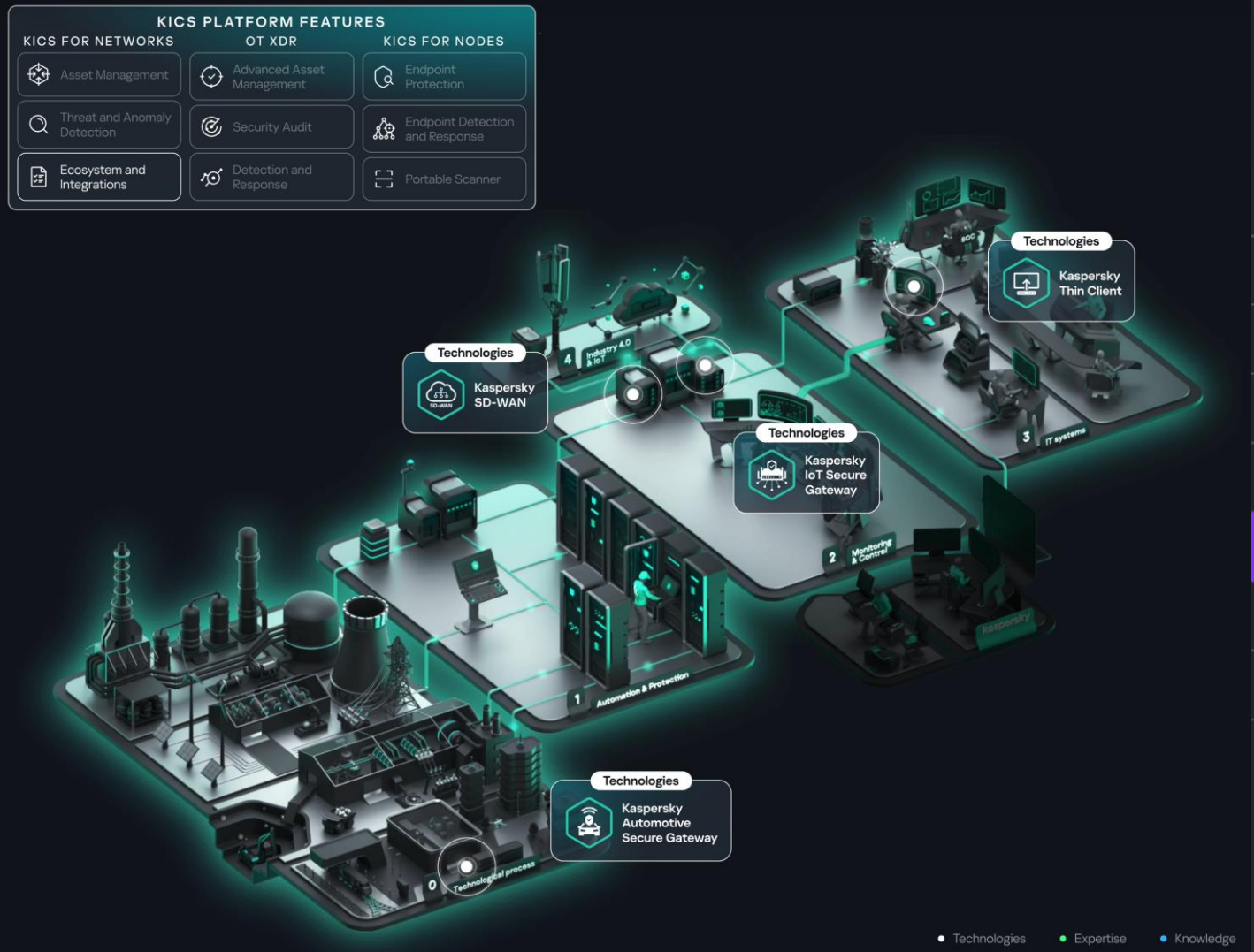
Industrial cyber resilience

8 steps to secure your enterprise

1. Audit: compliance and vuln.
2. 5.1 Identify frameworks
3. 5.2 Implement technical controls
4. 5.3 Hold risk assessment workshops
5. 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

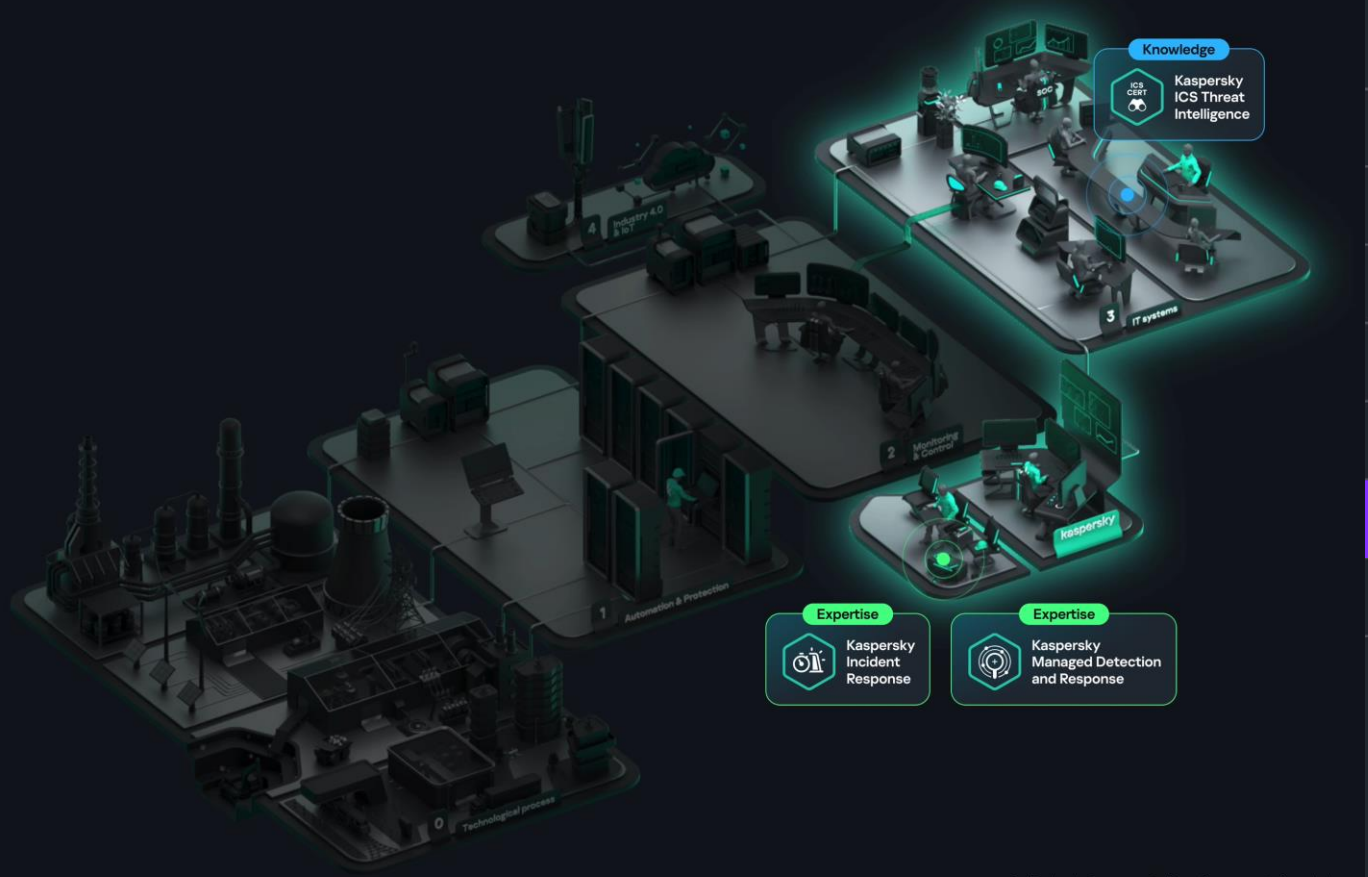
1
2
3
4
5
6
7
8

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

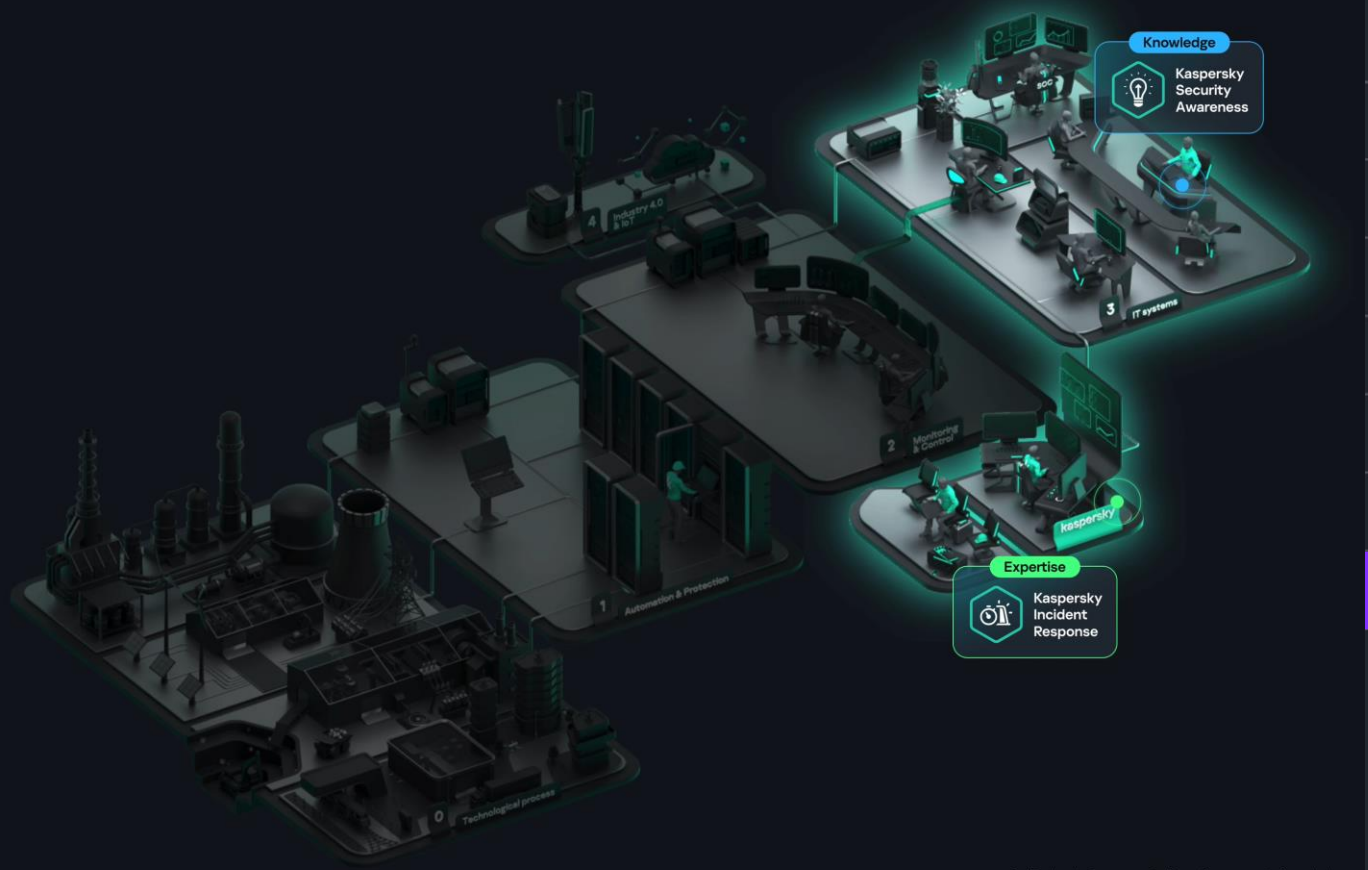
1
2
3
4
5
6
7
8

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

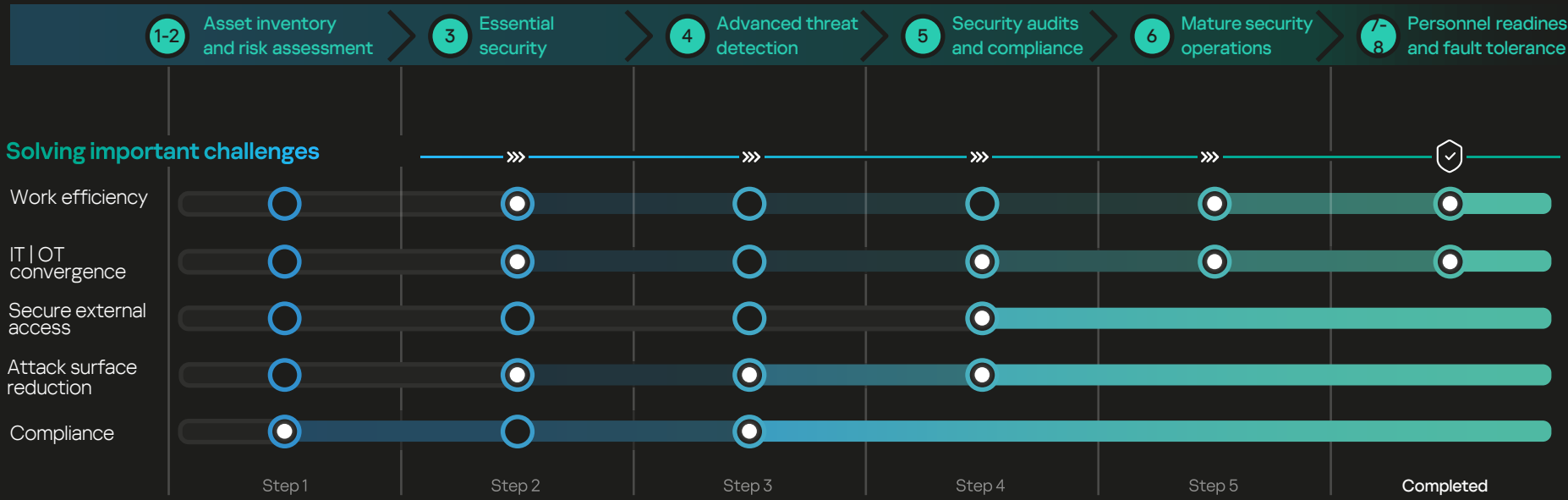
Prepare: ensure resilience

- 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

Steps to secure your industrial enterprise



Giải Pháp Đã Được Chứng Minh, Được Tin Cậy Toàn Cầu

Chúng tôi bảo vệ hơn 200.000 khách hàng doanh nghiệp trên toàn thế giới, từ các ngành nghề đa dạng, cung cấp các giải pháp bảo mật hiệu quả cho các tổ chức có quy mô và độ phức tạp khác nhau.

200
Quốc gia và vùng lãnh thổ

30+
văn phòng đại diện khu vực

Từ tầm ảnh hưởng toàn cầu đến sự phù hợp sở tại, Kaspersky mang đến sự bảo vệ đáng tin cậy mọi nơi.

Thích ứng với các ngành nghề	khách hàng Doanh nghiệp theo ngành	Các Quốc gia
Dịch vụ tài chính	~3,500	130
Chính phủ	~6,300	125
Năng lượng	~1,600	93
Sản xuất	~38,000	171
Bán lẻ	~12,700	125
Chăm sóc sức khỏe	~4,900	89

Và hơn thế nữa

Vận tải | Dầu khí | Công nghệ thông tin | Giáo dục | Viễn thông

Chuong
Tran
Presales Manager

kaspersky

www.kaspersky.com.vn

#kaspersky
#bringonthefuture