Chuyển đổi số trong ngành dầu khí

Cơ hội và rủi ro về an toàn thông tin

Phuc Nguyen – Cybersec Sales Manager
Softline VN

26 tỷ VND

là chi phí vận hành mà nhà máy Dung Quất tiết kiệm được mỗi năm
nhờ chuyển đổi số trong giai đoạn 2020 - 2025
Theo báo cáo của BSR - 2025

- Tinh chỉnh bộ điều khiển và triển khai hệ thống điều khiển đa biến
- Cải tiến hệ thống quản lý sản xuất
- Bảo dưỡng hiện hữu theo định hướng thông minh và tích hợp
- Hệ thống báo cáo quản trị trực quan
- Công tác sản xuất, bảo dưỡng, thương mại, nhân sự, công việc theo thời gian thực

Từ giàn khoan đến doanh nghiệp

Hành trình số hóa toàn diện

Remote operations -
Vận hành từ xa

Asset Reliability -
Quản trị thiết bị

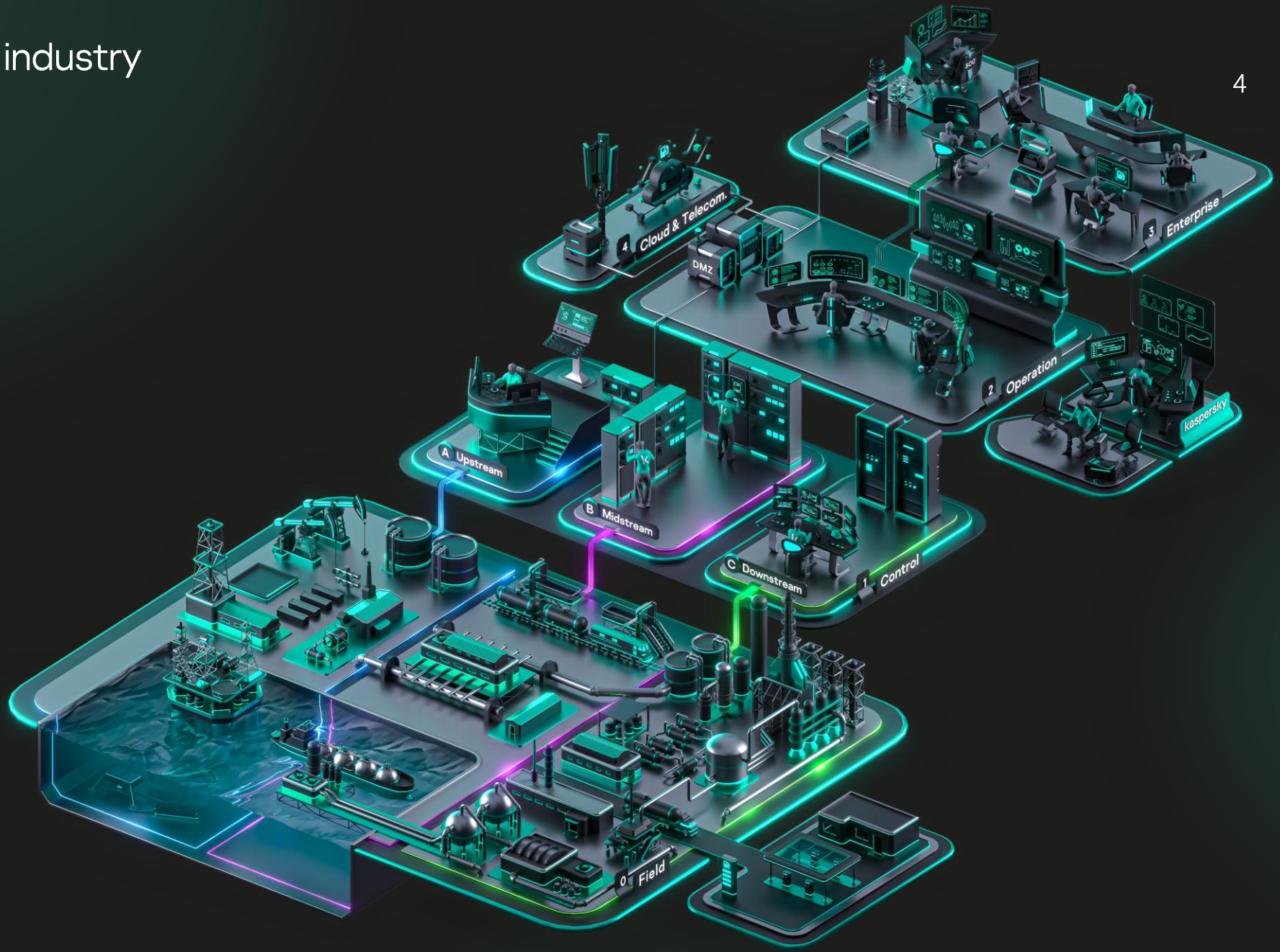
Production Optimization –
Tối ưu sản xuất

Safety & Risk Management -
Quản trị rủi ro

Supply Chain & Logistics -
Chuỗi cung ứng và hậu cần

Enterprise Data Integration -
Tích hợp dữ liệu doanh nghiệp

Digitalization in the oil and gas industry



Digitalization in the oil and gas industry

Operation

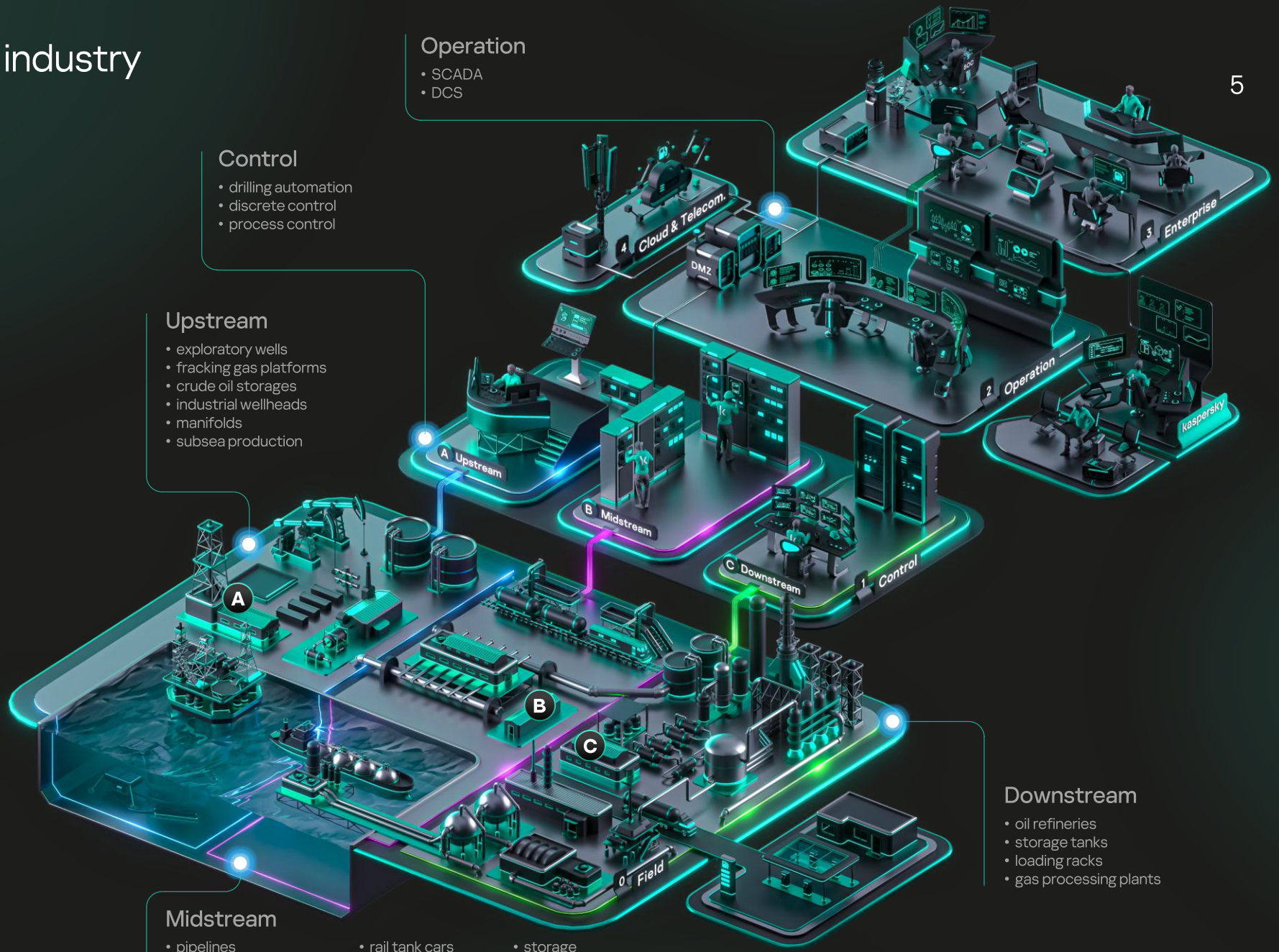
- SCADA
- DCS

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

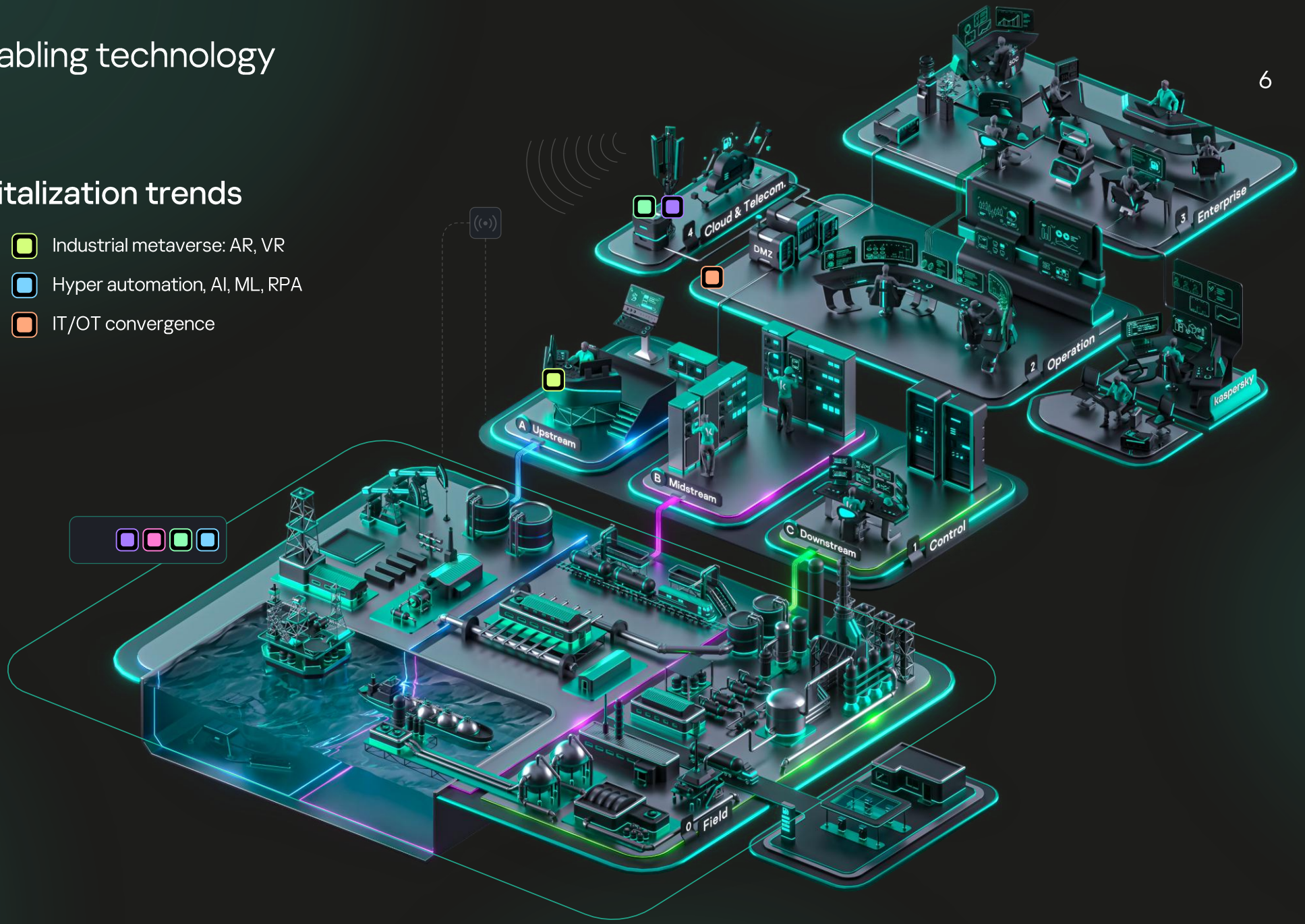
Midstream

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

Cybersecurity as an enabling technology

Color legend of digitalization trends

- IIoT & Cloud
- Digital twins
- Robotization and 5G
- Industrial metaverse: AR, VR
- Hyper automation, AI, ML, RPA
- IT/OT convergence



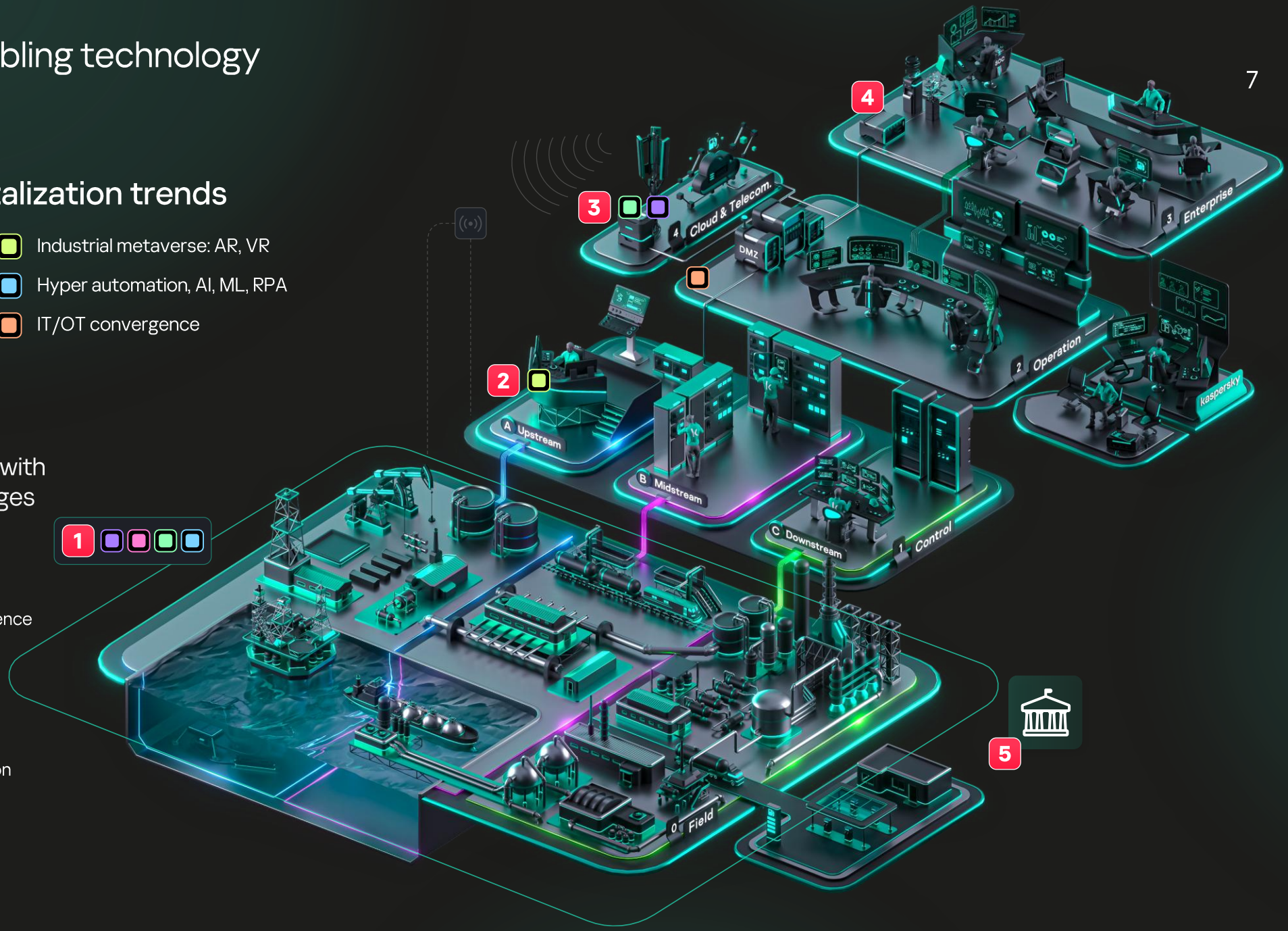
Cybersecurity as an enabling technology

Color legend of digitalization trends

- IIoT & 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 oil & gas industry goes hand in hand with security issues and challenges

1. Attack surface expansion
2. Legacy infrastructure and out-of-control IT/OT convergence
3. External access to OT infrastructure
4. Personnel deficit
5. Critical infrastructure protection regulations



Click on item 1-5 to continue

SƠ ĐỒ DIỄN BIẾN VỤ TẤN CÔNG RANSOMWARE COLONIAL PIPELINE (MỸ - 2021)

Hậu quả: Tê liệt 45% nhiên liệu bờ Đông | **Nguyên nhân chính:** Sụp đổ 3 trụ cột Zero Trust (Theo Mandiant)

1 GIAI ĐOẠN 1: XÂM NHẬP (Secure Access Sụp đổ)

CHỢ ĐEN DỮ LIỆU

Hacker mua mật khẩu bị rò rỉ

VPN CŨ (NHÂN VIÊN ĐÃ NGHỈ)

Tài khoản không bật MFA

ĐI THẲNG QUA CỔNG BẢO MẬT BIÊN

2 GIAI ĐOẠN 2: DI CHUYỂN & CHUẨN BỊ (Visibility Sụp đổ)

TUỒN DỮ LIỆU RA NGOÀI

HỆ THỐNG MẠNG NỘI BỘ

Hacker di chuyển tự do (Lateral Movement)

Nén và đánh cắp dữ liệu nhạy cảm

KẾT NỐI ĐIỀU KHIỂN (C2)

GIÁM SÁT THẤT BẠI:
SIEM/SOC 'MÙ', không phát hiện hành vi bất thường của tài khoản VPN chết.

BIỂU ĐỒ DIỄN BIẾN

3 GIAI ĐOẠN 3: TẤN CÔNG ĐIỂM YẾU (Privilege Account Sụp đổ)

ADMIN PRIVILEGE

IT SYSTEM

KHÓA VAN VẬT LÝ

DÒ QUÉT ĐẶC QUYỀN

Hệ thống quản lý lỏng lẻo

CHIẾM QUYỀN QUẢN TRỊ (ADMIN)

MÃ HÓA MÁY CHỦ TÍNH TIỀN/KẾ TOÁN

TẤN CÔNG RANSOMWARE (IT)

IT

IT

CẮT ĐỨT KẾT NỐI

OT

ĐIỀU KHIỂN ĐƯỜNG ỐNG

PHẢN ỨNG THỤ ĐỘNG:
Sợ mã độc lây từ IT sang OT –> Khóa van vật lý –>
TÊ LIỆT ĐƯỜNG ỐNG DẦU

SƠ ĐỒ CHUỖI TẤN CÔNG RANSOMWARE KÉP

XÂM NHẬP BAN ĐẦU

Hacker

KHAI THÁC LỖ HỔNG THIẾT BỊ NGOẠI VI

VPN

Vulnerability

Khai thác các lỗ hổng chưa được vá (Unpatched Vulnerabilities) trên Tường lửa, thiết bị VPN.

GỬI EMAIL GIẢ MẠO (PHISHING)

Email lừa đảo chứa mã độc đính kèm hoặc link. Lấy cắp Cookie và Mật khẩu hệ thống.

MÁY TÍNH VĂN PHÒNG BỊ NHIỄM

DỊCH CHUYỂN NGANG & NẰM VÙNG

Time Clocks

"Nằm vùng" vài tuần đến vài tháng để thu thập thông tin và dò quét mạng IT.

Quét mạng

"Nằm vùng" vài tuần đến vài tháng để thu thập thông tin và dò quét mạng IT.

HỆ THỐNG MÁY CHỦ MỤC TIÊU

Máy chủ Hóa đơn điện tử

ERP

Cơ sở dữ liệu Khách hàng

HỆ THỐNG MÁY CHỦ MỤC TIÊU

VÔ HIỆU HÓA PHÒNG THỦ

Backup

XÓA/MÃ HÓA SAO LƯU

Vô hiệu hóa hoặc mã hóa dữ liệu Backup để ép doanh nghiệp trả tiền chuộc.

TẮT PHẦN MỀM DIỆT VIRUS

TÁC ĐỘNG & TỐNG TIỀN KÉP

LOCKED

EDP

MÃ HÓA HÀNG LOẠT (MASS ENCRYPTION)

Mã hóa hàng trăm máy chủ, đổi đuôi file, đòi tiền chuộc.

TỐNG TIỀN KÉP

KHÔI PHỤC DỮ LIỆU

RÒ RỈ DỮ LIỆU

Ransom Note

Yêu cầu chuộc để giải mã file VÀ để ngăn rò rỉ thông tin đánh cắp.

Các giai đoạn tấn công và giải pháp kiểm soát

Giai đoạn tấn công	Mô tả	Lớp kiểm soát	Giải pháp
Xâm nhập ban đầu	• Khai thác truy cập từ xa / nhà thầu / bên thứ ba • Xâm nhập thông qua tài khoản hoặc kết nối hợp lệ	Quản lý danh tính và truy cập đặc quyền, xác thực đa lớp, kiểm soát truy cập từ xa	IAM, PAM, MFA, Biometric
Nằm vùng, leo thang đặc quyền & di chuyển ngang	• Kẻ tấn công đã vào được hệ thống • Âm thầm khảo sát hệ thống để tìm lỗ hổng và mở rộng phạm vi kiểm soát	• Giám sát và phát hiện hành vi bất thường • Quản lý và kiểm soát tài khoản đặc quyền	XDR, PAM
Đánh cắp dữ liệu	• Dữ liệu địa chất, trữ lượng, kế hoạch khai thác và tài liệu vận hành trọng yếu • Thông tin đấu thầu, hợp đồng và dữ liệu thương mại nhạy cảm • Mối đe dọa nội bộ	• Giám sát dữ liệu nhạy cảm • Giám sát hành vi người dùng	DLP, Risk Monitor
Triển khai ransomware	Mã hóa máy chủ, máy trạm, dữ liệu nhạy cảm gây gián đoạn hoạt động	Bảo vệ Endpoint và Server	EDR
Phá hoại vận hành	Can thiệp trái phép vào hệ thống điều khiển, logic vận hành hoặc tham số quy trình	Bảo vệ hệ thống điều khiển ICS/OT	ICS/OT Security
Điều tra sau sự cố	Can thiệp trái phép vào hệ thống điều khiển, logic vận hành hoặc tham số quy trình	Pháp y số	Risk Monitor

3 Lớp Kiểm soát An ninh Mạng cốt lõi

Identity-Centric Security

Bảo mật danh tính

- Quản lý danh tính và truy cập đặc quyền (IAM/PAM)
- Xác thực đa lớp (MFA), sinh trắc học
- Phát hiện và ngăn chặn nguy cơ chiếm đoạt hoặc lạm dụng tài khoản

Data-Centric Security

Bảo mật dữ liệu

- Bảo vệ dữ liệu nhạy cảm (DLP)
- Phân quyền truy cập và kiểm soát sử dụng dữ liệu
- Phát hiện và ngăn chặn hành vi sử dụng dữ liệu bất thường

Infrastructure Security

Bảo mật hạ tầng

- Giám sát và hiển thị đầy đủ trạng thái an ninh của hệ thống
- Phát hiện sớm các hành vi xâm nhập và bất thường
- Hạn chế phạm vi ảnh hưởng khi sự cố xảy ra

Softline Group

Investment and technology holding company with over 30 years of experience and a broad regional presence in Russia, Kazakhstan, Uzbekistan, Vietnam, Indonesia, and the UAE.

Cornerstone of Digital Transformation

25+	> 5000	> 100 000	Full range of
Companies in the Group	Manufacturers	Customers	Services and solutions

Leading IT Company in Russia

30+	30+	~1.3B USD	> 11100
Representative offices in 6 countries	Years on IT-market	Turnover in 2024	Employees

Axidian

Identity-Centric Security

Your Trusted Partner for Identity Security Solutions

Axidian Access

Quản trị danh tính và quyền truy cập

- Xác thực tập trung và đơn giản hóa truy cập (SSO)
- Xác thực đa lớp, sinh trắc học
- Kiểm soát truy cập dựa trên ngữ cảnh
- Tự động hóa vòng đời tài khoản

Axidian Privilege

Kiểm soát tài khoản đặc quyền

- Quản lý và lưu trữ tập trung mật khẩu đặc quyền
- Kiểm soát và phê duyệt quyền truy cập tạm thời
- Kiểm soát hành vi trong phiên làm việc
- Ngăn chặn rủi ro và thực thi lệnh cấm thời gian thực

Axidian Shield

Giám sát và ngăn chặn chiếm đoạt danh tính số

- Kiểm toán và phát hiện lỗ hổng trong cấu trúc hệ thống User Directory
- Giám sát và phát hiện hành vi gian lận sau xác thực
- Ngăn chặn các kỹ thuật tấn công / giả mạo danh tính

SEARCHINFORM

INFORMATION SECURITY

SearchInform DLP

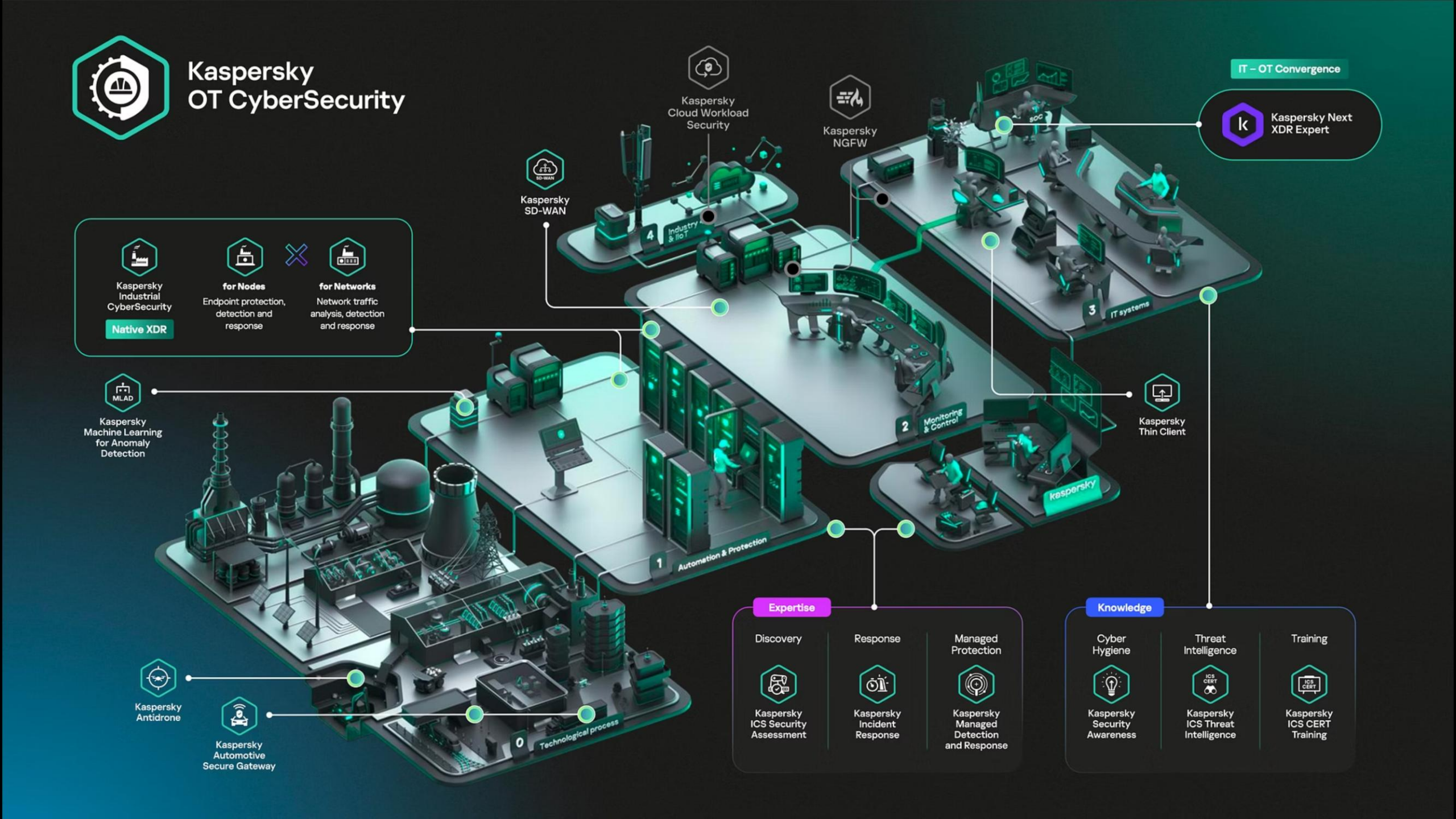
Ngăn chặn thất thoát dữ liệu

- Kiểm sát toàn diện các kênh truyền tải dữ liệu
- Nhận diện dữ liệu nhạy cảm bằng công nghệ phân tích nội dung sâu
- Thực thi chính sách bảo vệ dữ liệu tự động

SearchInform RiskMonitor

Giám sát và ngăn chặn chiếm đoạt dữ liệu

- Phân tích và nhận diện hành vi truy cập dữ liệu bất thường trong hệ thống bằng AI
- Ngăn chặn hành vi chiếm đoạt dữ liệu
- Ghi vết toàn bộ quá trình tương tác dữ liệu để phục công tác điều tra và pháp y số


Kaspersky
OT CyberSecurity
Kaspersky
Cloud Workload
Security
Kaspersky
NGFW
IT – OT Convergence
Kaspersky Next
XDR Expert
Kaspersky
SD-WAN
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
4 Industry & IIoT
3 IT systems
2 Monitoring & Control
1 Automation & Protection
0 Technological process
Expertise
Discovery
Kaspersky
ICS Security
Assessment
Response
Kaspersky
Incident
Response
Managed
Protection
Kaspersky
Managed
Detection
and Response
Knowledge
Cyber
Hygiene
Kaspersky
Security
Awareness
Threat
Intelligence
Kaspersky
ICS Threat
Intelligence
Training
Kaspersky
ICS CERT
Training

OT XDR Platform

Advanced asset management

- Extended host monitoring
- Hardware and apps. inventory
- Blind area coverage (spanless mode)

Extended Detection and Response

- Single host-network incidents
- Investigation graph
- Alert enrichment
- Manual response actions
- Network access restriction

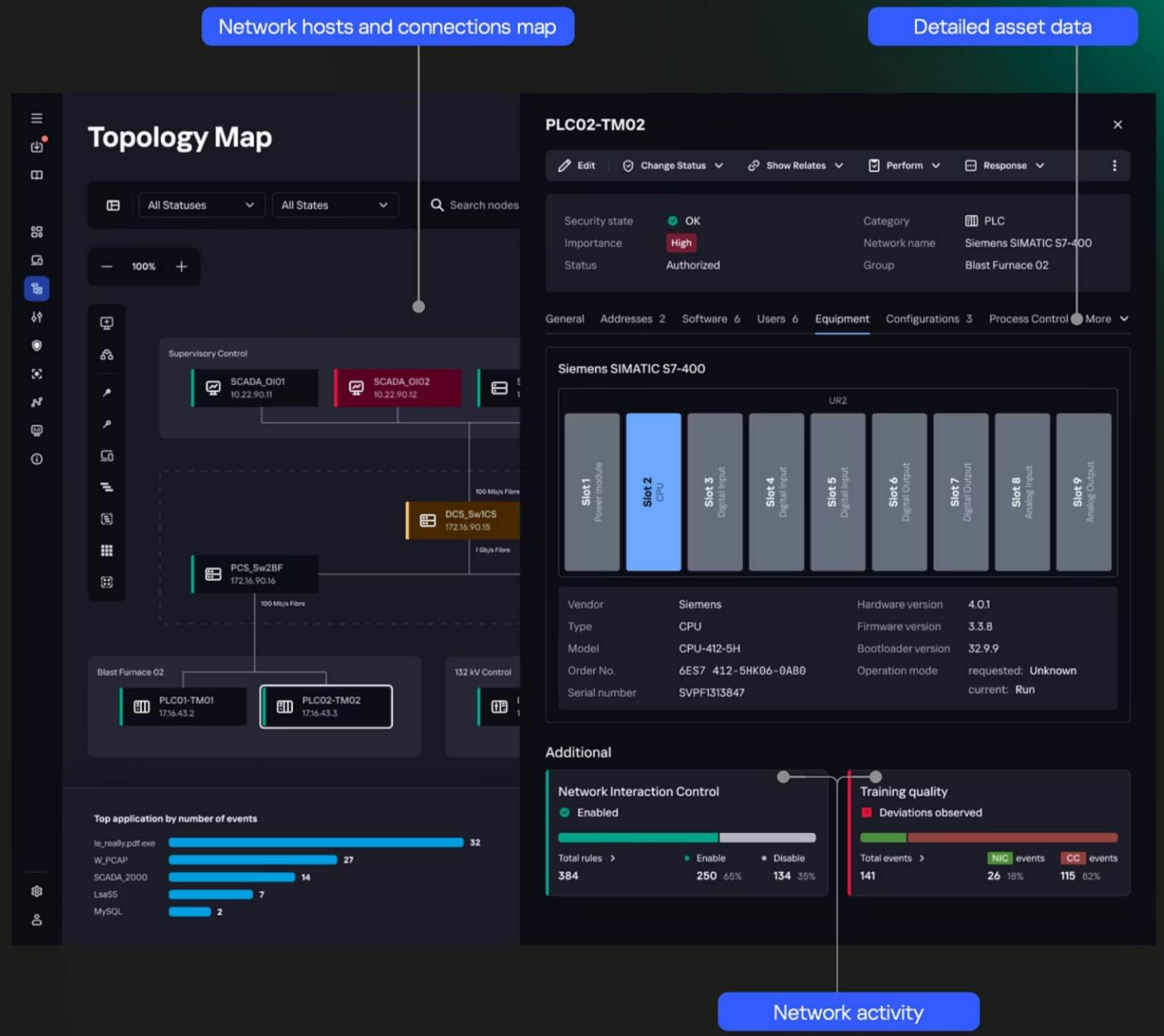
Security audit

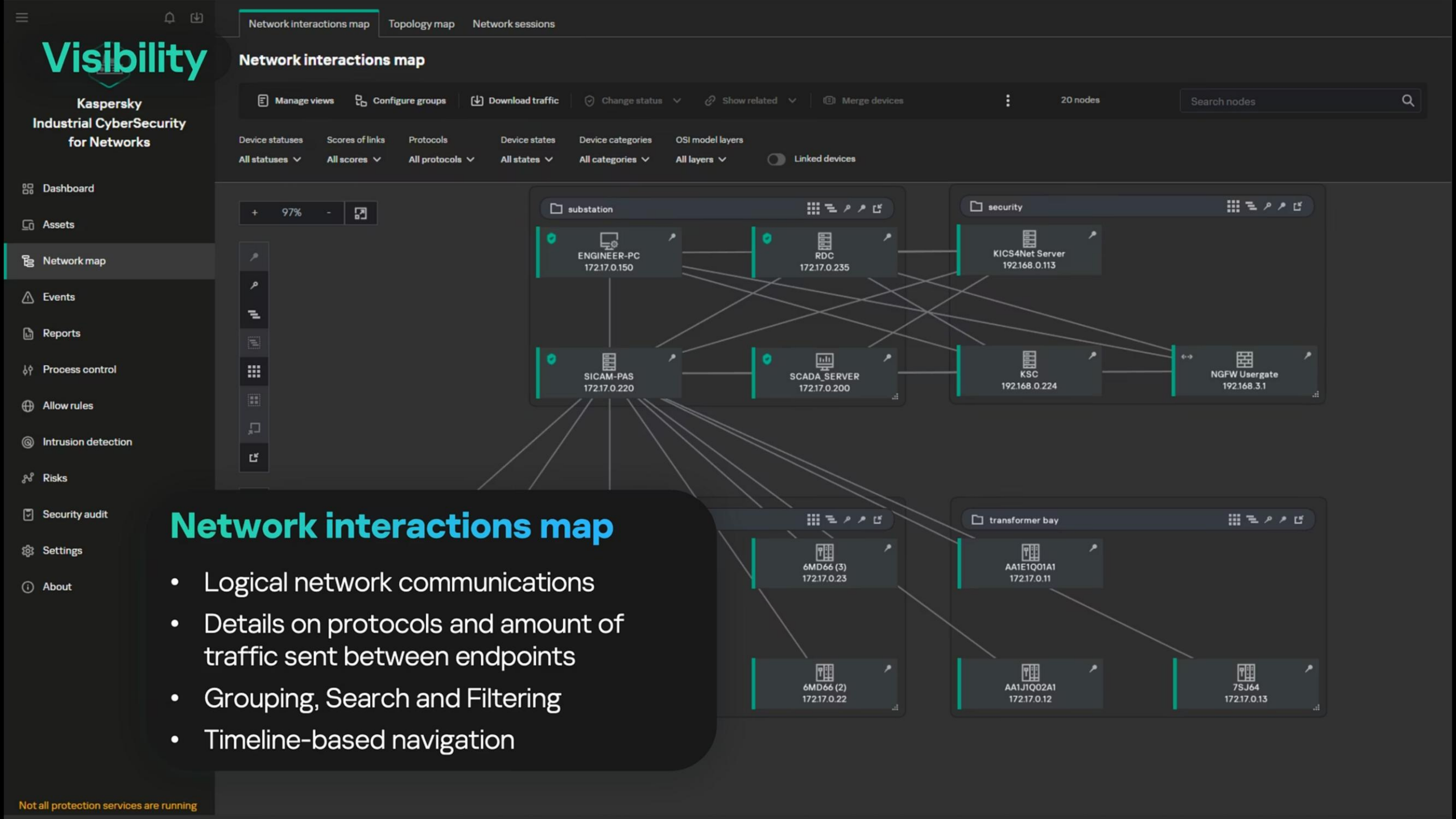
- Vulnerability scan
- Compliance audit
- Configuration change monitoring

Advanced asset management

- Extended host monitoring
- Hardware and apps inventory
- Blind area coverage (spanless mode)

Get complete infrastructure visibility: network data flows, hosts activity, hardware inventory and software/firmware versions




Visibility
Kaspersky Industrial CyberSecurity for Networks
Network interactions map
Topology map
Network sessions
Network interactions map
Manage views
Configure groups
Download traffic
Change status
Show related
Merge devices
20 nodes
Search nodes
Device statuses
All statuses
Scores of links
All scores
Protocols
All protocols
Device states
All states
Device categories
All categories
OSI model layers
All layers
Linked devices
Dashboard
Assets
Network map
Events
Reports
Process control
Allow rules
Intrusion detection
Risks
Security audit
Settings
About
97%
substation
ENGINEER-PC
172.17.0.150
RDC
172.17.0.235
SICAM-PAS
172.17.0.220
SCADA_SERVER
172.17.0.200
security
KICS4Net Server
192.168.0.113
KSC
192.168.0.224
NGFW Usergate
192.168.3.1
6MD66 (3)
172.17.0.23
6MD66 (2)
172.17.0.22
transformer bay
AA1E1Q01A1
172.17.0.11
AA1J1Q02A1
172.17.0.12
7SJ64
172.17.0.13
Network interactions map
Logical network communications
Details on protocols and amount of traffic sent between endpoints
Grouping, Search and Filtering
Timeline-based navigation
Not all protection services are running

Detection & Response

Kaspersky Industrial CyberSecurity for Networks

- Dashboard
- Assets
- Network map
- Events
- Reports
- Process control
- Allow rules
- Intrusion detection
- Risks
- Security audit
- Settings
- About

Not all protection services are running

Connection Server: Server

kics
Administrator

Events and incidents | Response actions

Export | Change status | Show related

963 New events | 0 Events in progress | Scores 0 — 10

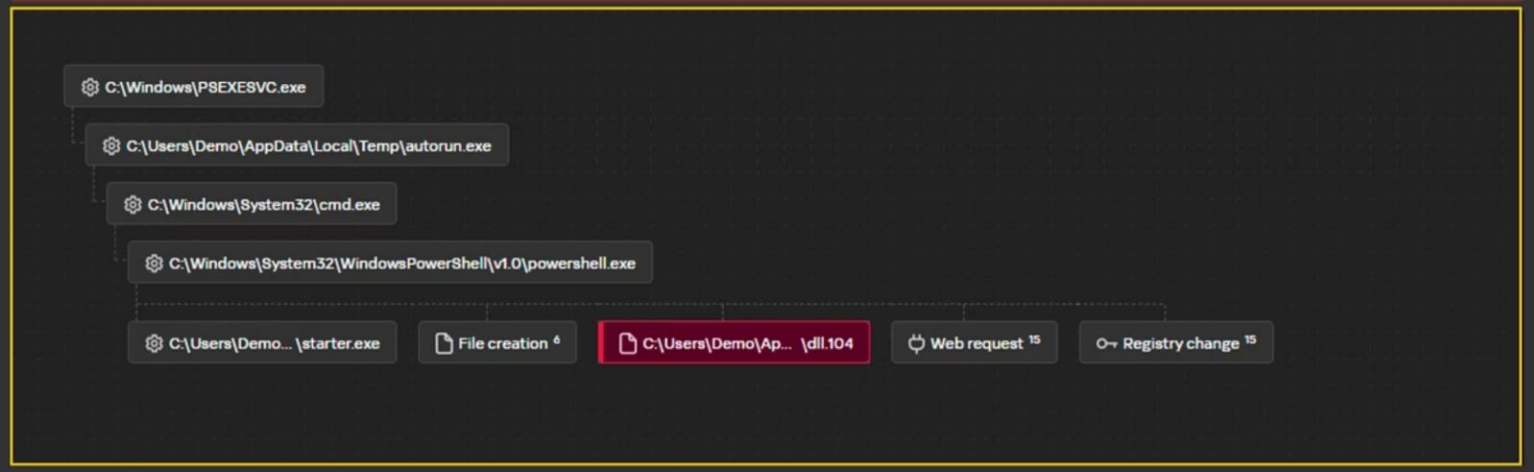
Last seen	Title
2023-11-13 20:53:35...	Signs of malware activit
2023-11-13 20:54:55...	Suspicious activity (
2023-11-13 20:53:34...	Launch of an unauth
2023-11-13 20:53:48...	Infected or probably i
2023-11-13 20:53:35...	Infected or probably i
2023-11-13 20:53:26...	Received new informatio
2023-11-13 20:53:26...	Use of remote access s
2023-11-13 20:54:03...	Unauthorized network
2023-11-13 20:53:26...	Unauthorized network
2023-11-13 20:53:09...	Suspicious activity (MIT
2023-11-13 20:53:08...	Launch of an unauthori
2023-11-13 20:53:06...	Unauthorized network int
2023-11-13 20:53:06...	Rule from the awp set (sy
2023-11-13 20:53:06...	Use of remote access s
2023-11-13 20:52:42...	Unauthorized network int
2023-11-13 20:52:22...	Unauthorized network int
2023-11-13 20:50:32...	Signs of attack (MITRE:

8.6 **Infected or probably infected object was detected**

Change status | Show related | Threat response | Create allow rule | Download traffic | Copy details | Export

Event Info | Activity event graph | All activity events

Detection processing status: Object not processed: Application is running in Report only mode



Detection information

File

Date and time	2023-11-13 20:53:37
Name	C:\Users\Demo\AppData\Local\Temp\Industroyer_104_kit\104.dll
Size	134 KB
MD5 hash	66c67ebf254f29bf925a8ae6a3163a1c
SHA256 hash	b60f097b12087f2d809d4df945a9fe2e372fbae67a0e483237a2ced9d99b27e5
Created	2023-11-13 20:53:37
Changed	2023-11-13 20:53:37
Attributes	Archive
Signed by the organization	—
Trusted digital signature	No
Creator	NT AUTHORITY\S
Time zone identifier	Computer

EDR-related endpoint activity graph

Kaspersky Industrial CyberSecurity

All-encompassing situational awareness and risk exposure control for critical infrastructure

Proven

Over 200 compatible systems from 50+ vendors: tested and proven

Schneider Electric · SIEMENS · GE · YOKOGAWA · Honeywell · B&R · Baker Hughes · EMERSON

Certified

KICS and its core technologies are under industry-leading audits: IEC 62443-4-1, ISO 27001, SOC2 type 2, GB 42250-2022 .

IEC · AICPA SOC · ISO

Recognized

Since 2013, Kaspersky products have participated in 1022 independent tests and reviews, earning 771 first place results and 871 top-three finishes

Q&A