“Ciberseguridad y conectividad”

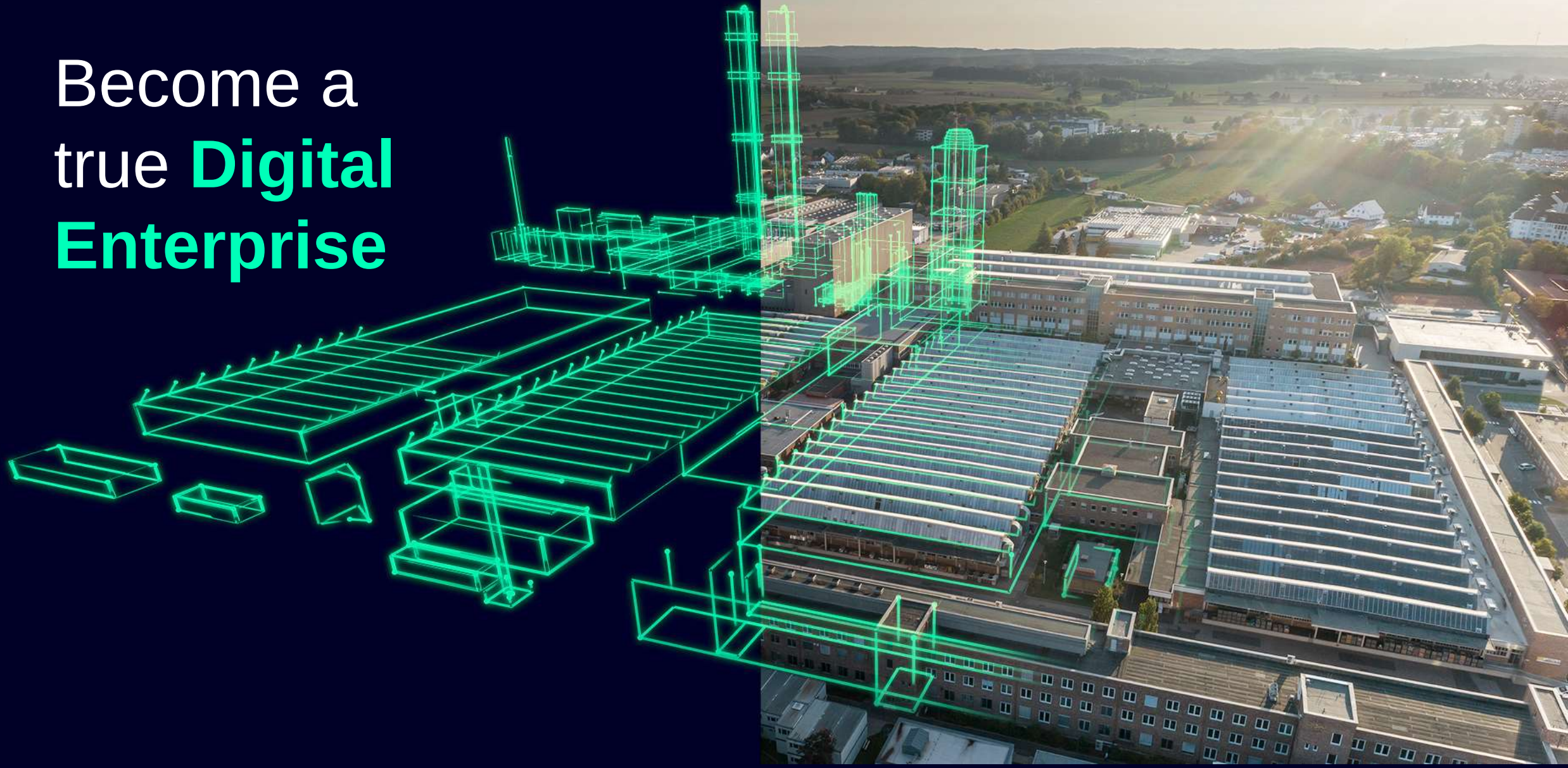
Pedro Romero Sánchez

27º Congreso de Calidad en la Automoción 4.0

Barcelona, 20 y 21 de abril de 2023

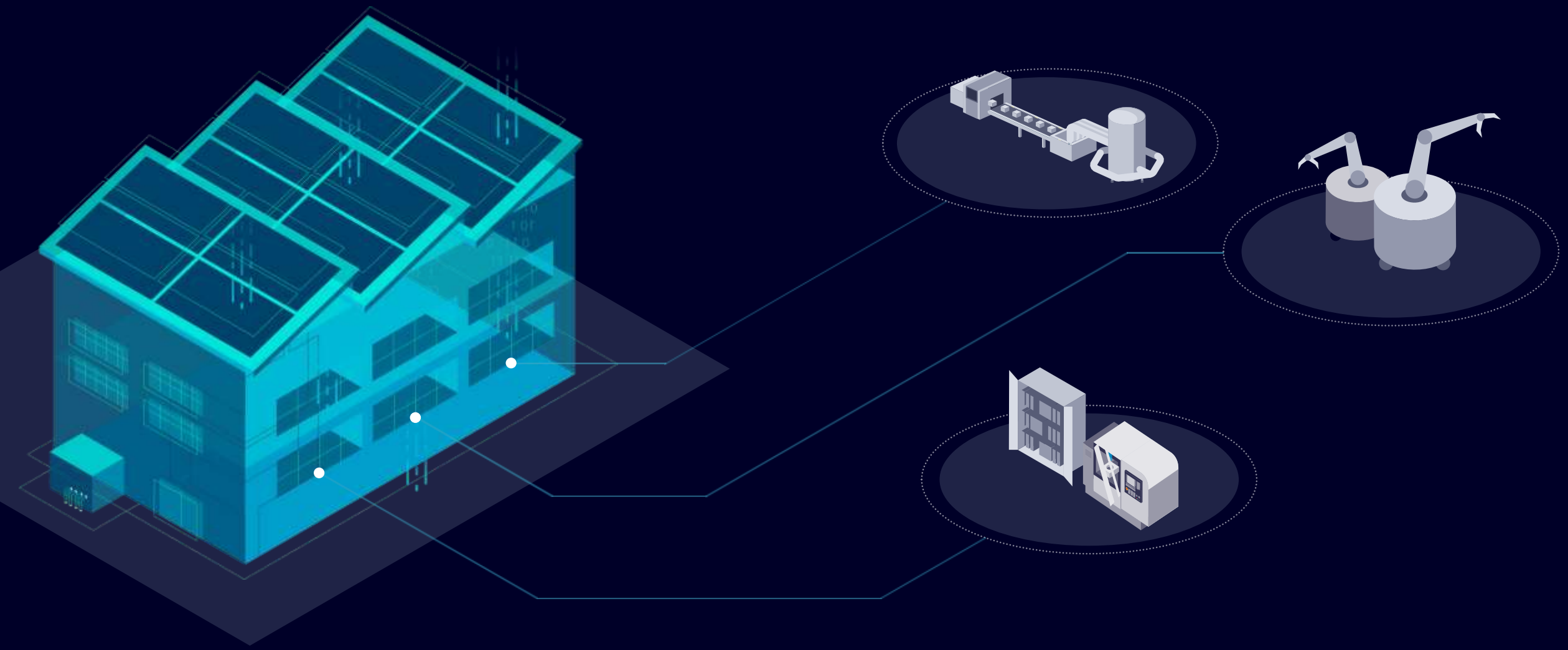
SIEMENS

Become a true **Digital Enterprise**



SIEMENS

Yesterday we had islands of communication



SIEMENS

Today everything is **connected ...**

SIEMENS

… and **at risk**

SIEMENS

Challenges and drivers
Most critical threats to industrial control systems

Industrial Control System Security Top 10 Threats and Countermeasures1	Trend, 2019
Infiltration of Malware via Removable Media and External Hardware	→
Malware Infection via Internet and Intranet	↑
Human Error Sabotage	→
Compromising of Extranet and Cloud Components	↗
Social Engineering and Phishing	→
(D)Dos Attacks	→
Control Components Connected to the Internet	↗
Intrusion via Remote Access	↗
Technical Malfunctions and Force Majeure	→
Soft- and hardware vulnerabilities in the supply chain	↑

1 Source © BSI Publications on Cyber Security | Industrial Control System Security 2022

"The manufacturing industry is often the target of cyberattacks because (traditionally, at least) this industry was highly fragmented, with individual facilities each using different IT infrastructures and multiple disjointed systems... cybercriminals continue to exploit these holes."

– Peter Fretty, IndustryWeek

SIEMENS

Why cybersecurity matters for automotive executives?

From Q4 2019 to Q1 2020, **there was a 156% increase in ransomware attacks in the manufacturing sector**. Deployment of ransomware – altering or shutting down an OT, IT or other computer system with malware until money is paid to the hacker – is just one tactic in the expanding world of cybercrime.

"Just one cyberhack can cost an automaker **$1.1 billion**. The cost for the industry as a whole could reach $24 billion by 2023."

– GlobalTradeMag

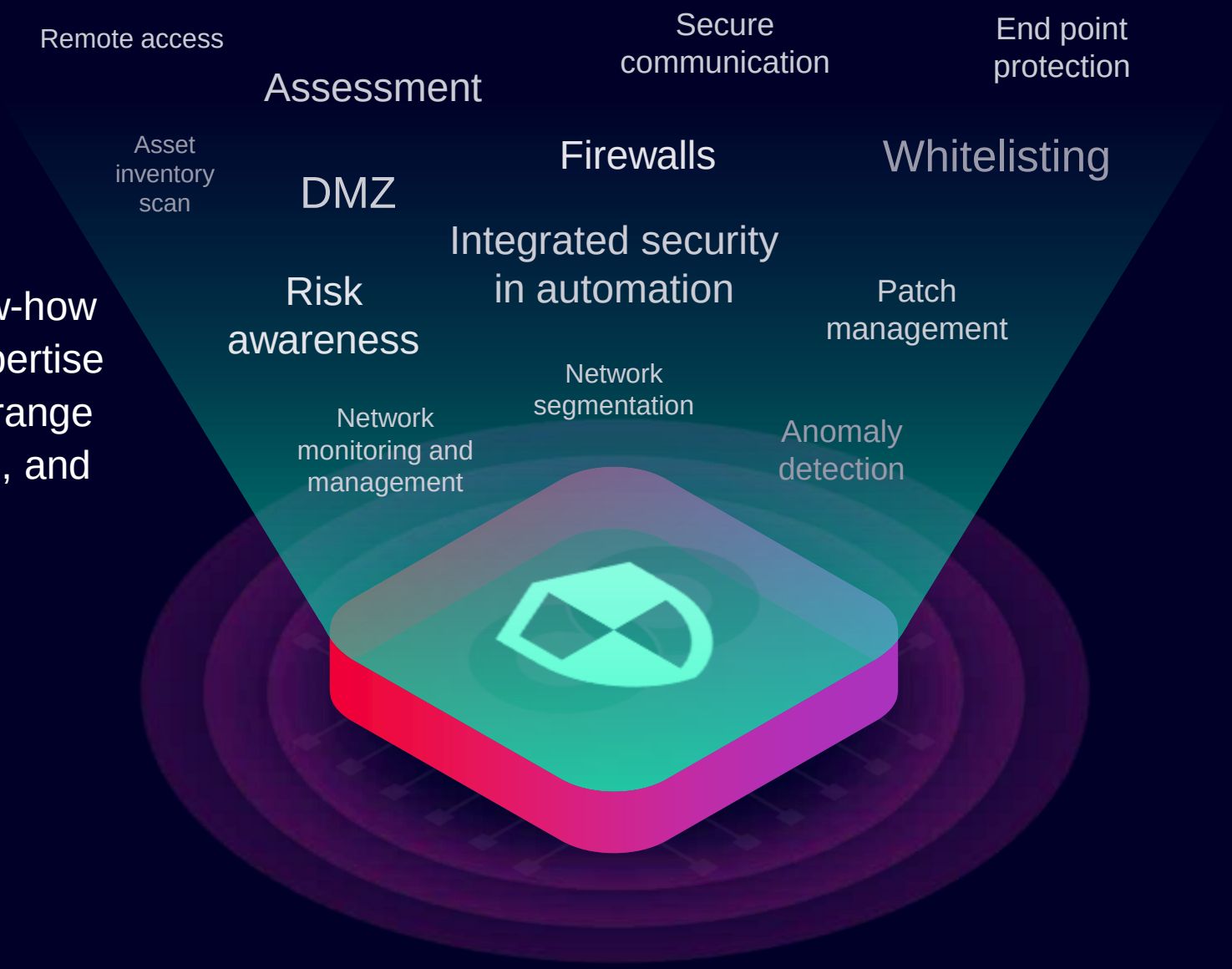
"Gartner predicts that by 2025, **40% of boards of directors** will employ a dedicated cybersecurity committee overseen by a qualified board member."

– Security Magazine

SIEMENS

Complete Cybersecurity for Industry offering

In-depth domain know-how and cybersecurity expertise combined in a broad range of hardware, software, and services for industrial security.



SIEMENS

OT is at the intersection of multiple challenges

01 **Digitalization**

Need for all types of data, in real-time
(LEAN, Predictive Maintenance, etc.)

02 **Knowledge gaps**

Lack of OT networking and
cybersecurity knowledge and experience

03 **Multiplying adversaries**

Proliferation of cyber-threat actors
(insider, external, criminal, nation-state, script kiddies)

04 **Sophisticated malware infrastructure**

Advancement in malware tools and services
(AI, cloud-based tools, etc.)

Legislation is underway in many parts of the world

CIRCIA and **SEC** regulations **in US** will change how companies address cybercrime
Focus is on: reporting, disclosure criteria and transparency

Source: McKinsey, 2022

Tightening cybersecurity obligations across **Europe** - the **NIS2** directive
Focus is on: new rules, more sectors included

Source: European Parliament, 2023

Key changes in data privacy and cyber security laws across **Southeast Asia** in 2022

Source: Herbert Smith Freehills, 2022

SIEMENS

“

The Industrial Internet of Things (IIoT) would be inconceivable without cybersecurity.“

– Roland Busch, Siemens

SIEMENS

Thank You!

SIEMENS