How Siemens is working with cybersecurity

Morten Kromann, Siemens A/S

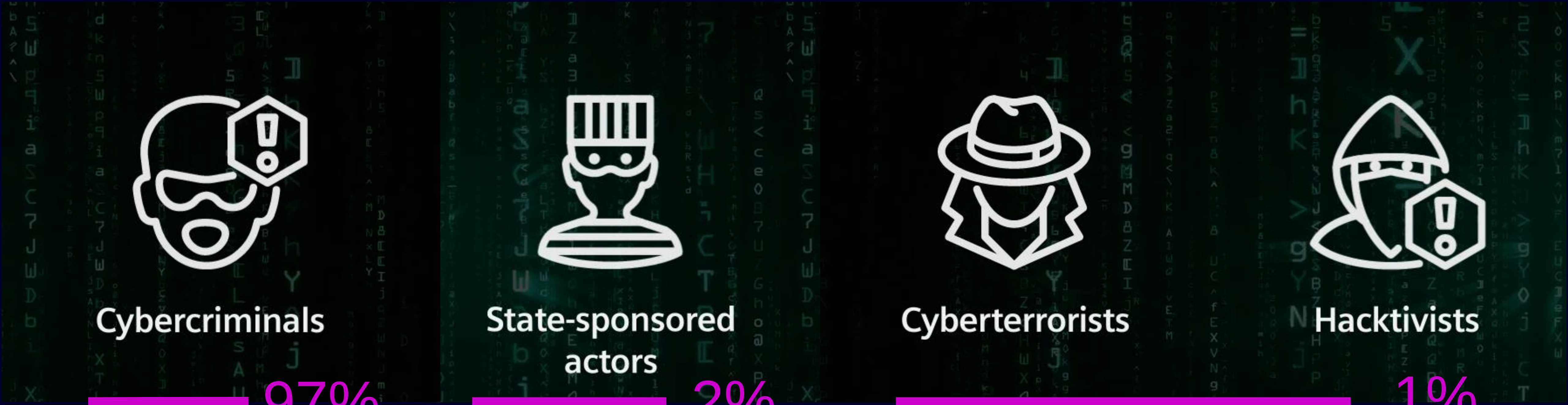
SIEMENS

Why do we do

What we do?

SIEMENS

Manufacturing has been the n.1 target of cybercrime in 2022



97% 2% 1% of all attacks

IBM X-Force 2022

Top target

Manufacturing

Attack type

1. **Ransomware**
2. Server access
3. Data theft

Attack vector

47%	**-**	**Vulnerability exploit**
40%	-	Phishing
3%	-	Removable media

SIEMENS

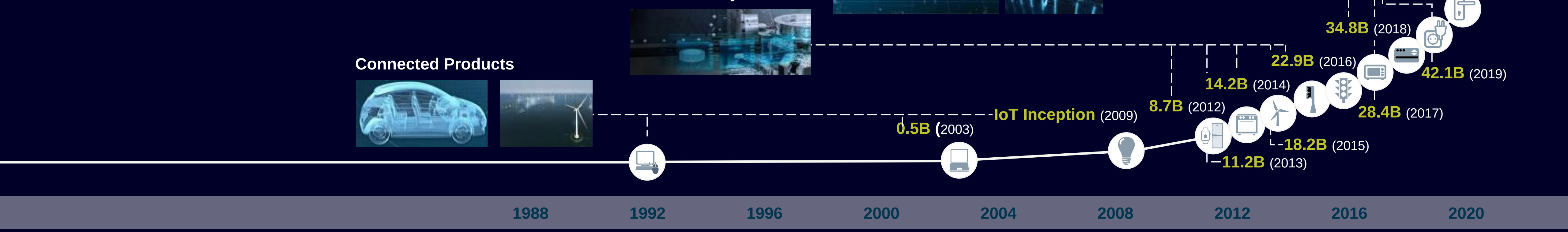
Taking cyber threats **seriously**

With **> 30 million** automated systems, > 75 million contracted smart meters and **> one million** Cloud connected products in the field”

Digitalization creates: Visible opportunities & Invisible threats

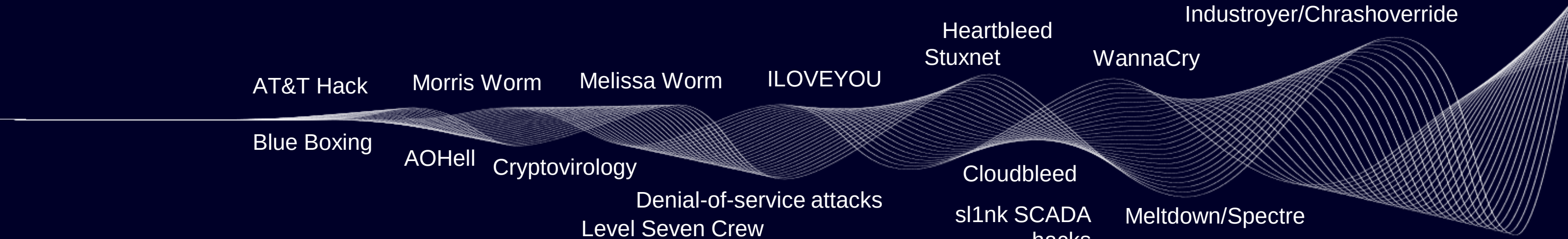
Opportunities

Billions of devices are being connected by the Internet of Things, and are the backbone of our infrastructure and economy



… and risks

Exposure to malicious cyber attacks is also growing dramatically, putting our lives and the stability of our society at risk



Stuxnet

SIEMENS

Charter of Trust

We sign for cybersecurity!
We sign the Charter of Trust.

SIEMENS AES AIRBUS Allianz AtoS CISCO DAIMLER DELL Technologies

enel IBM Munich Security Conference Münchner Sicherheitskonferenz MSC NXP SGS T · · TOTAL TÜV SÜD

SIEMENS

NATO Cooperative Cyber Defense Centre of Excellence

LOCKED SHIELDS

More info: https://ccdcoe.org/exercises/locked-shields/

How do we do

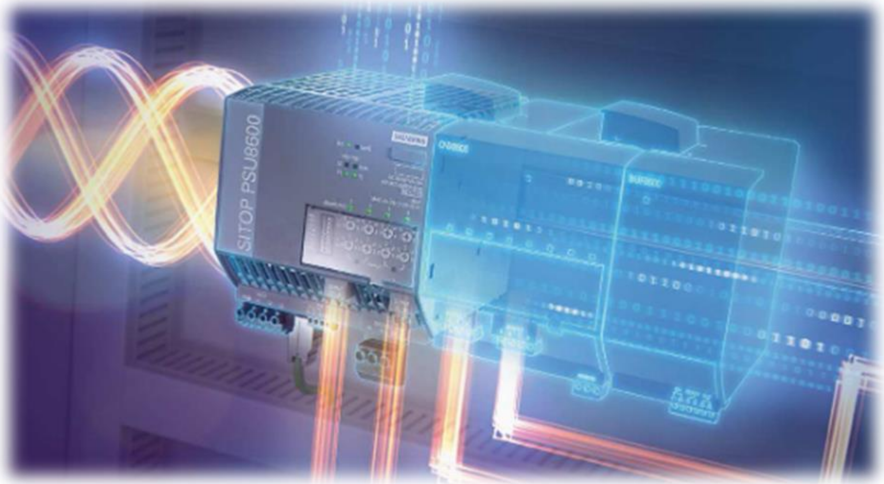
What we do?

SIEMENS

Secure products and production

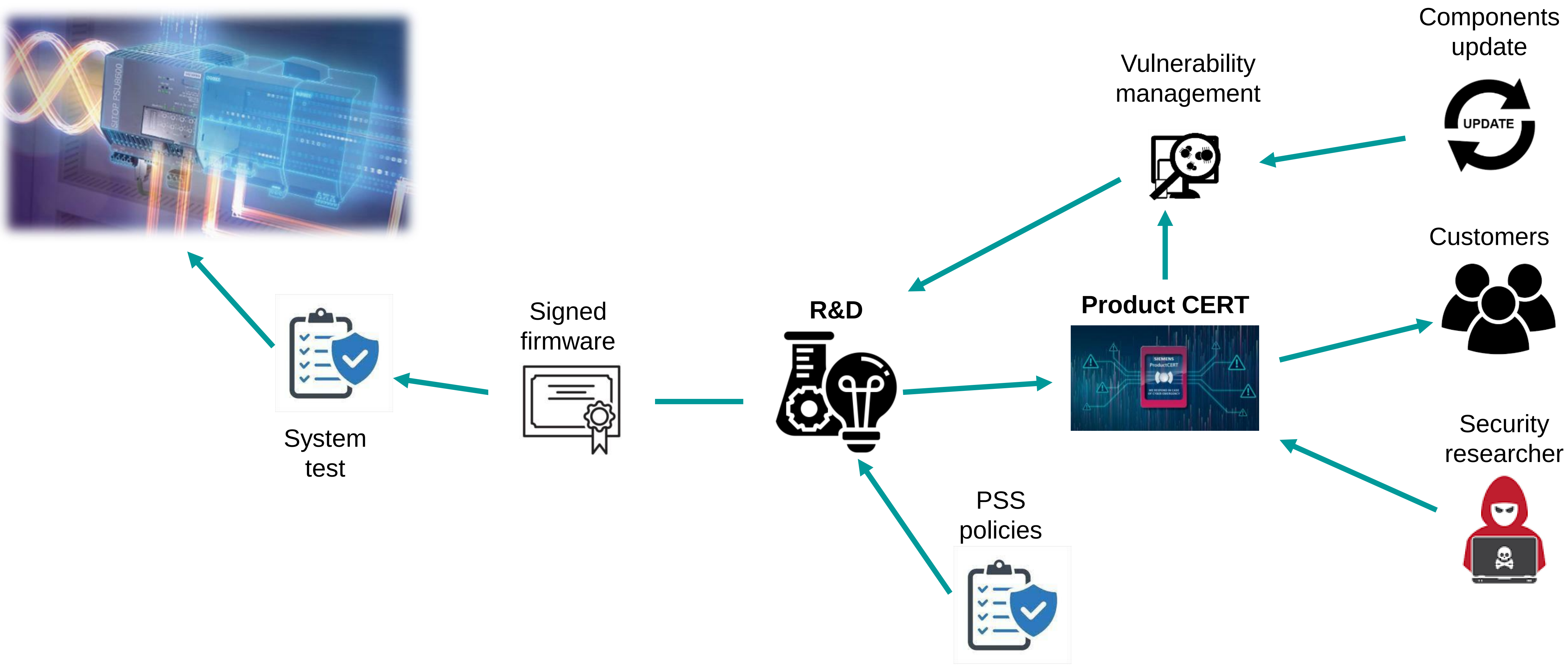
ISO27001

NIS 2 prepared
IEC62443 + addons



IEC62443 + addons

Secure products



Components update

Vulnerability management

Customers

Security researcher

Product CERT

R&D

PSS policies

Signed firmware

System test

Secure production: internal program adopts step-wise approach based on IEC 62443 standard

Key take-away: No one-size fits all solution

Achievements

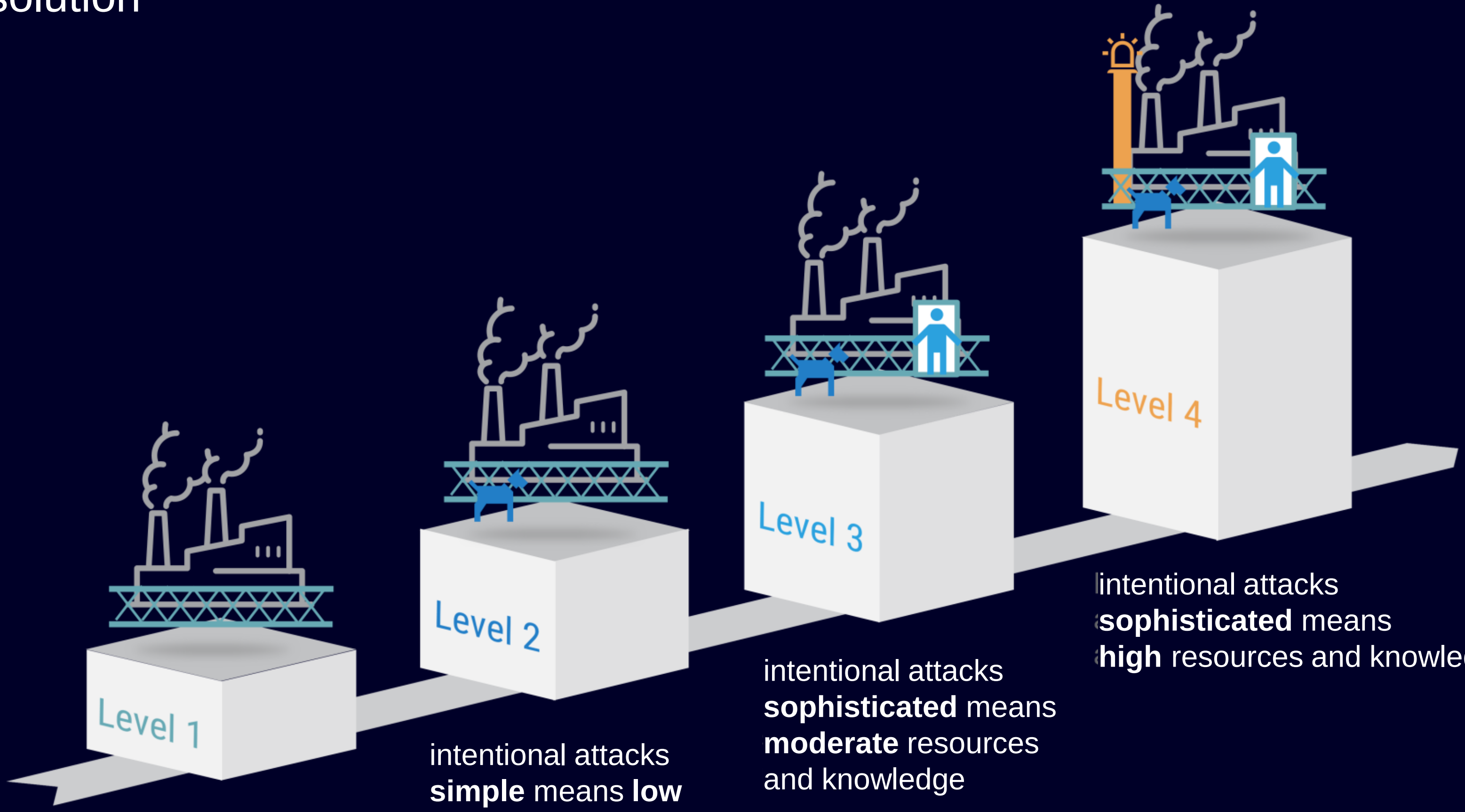
OT security blueprints

IEC 62443

OT asset Inventory

Awareness & Training

Service & technology standardization



accidental errors

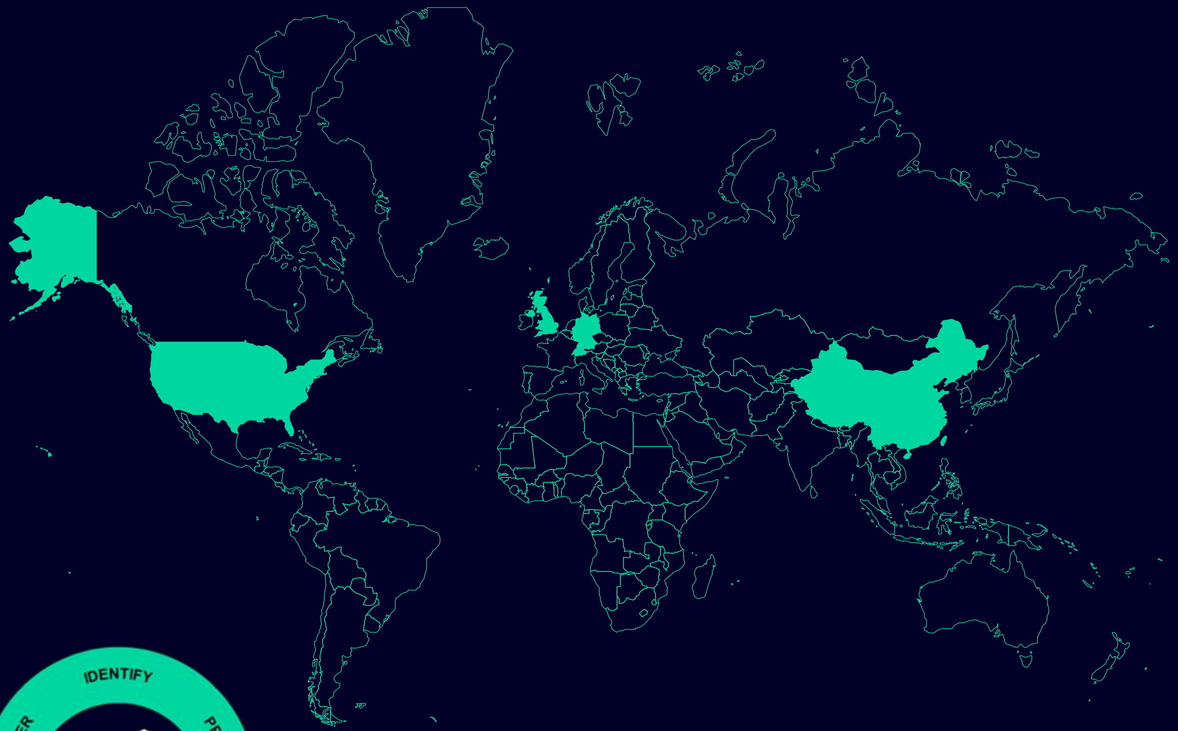
intentional attacks
simple means **low** resources
and knowledge

intentional attacks
sophisticated means
moderate resources
and knowledge

intentional attacks
sophisticated means
high resources and knowledge

SIEMENS

Asset Inventory and Network Segmentation program based on OT consulting know-how and scalable scanning solution



14+ scanned factories worldwide (e.g. CH, CN, DE, UK, US)

300+ subnetworks scanned in total across all factories

11,000+ devices identified from a wide range of OT vendors

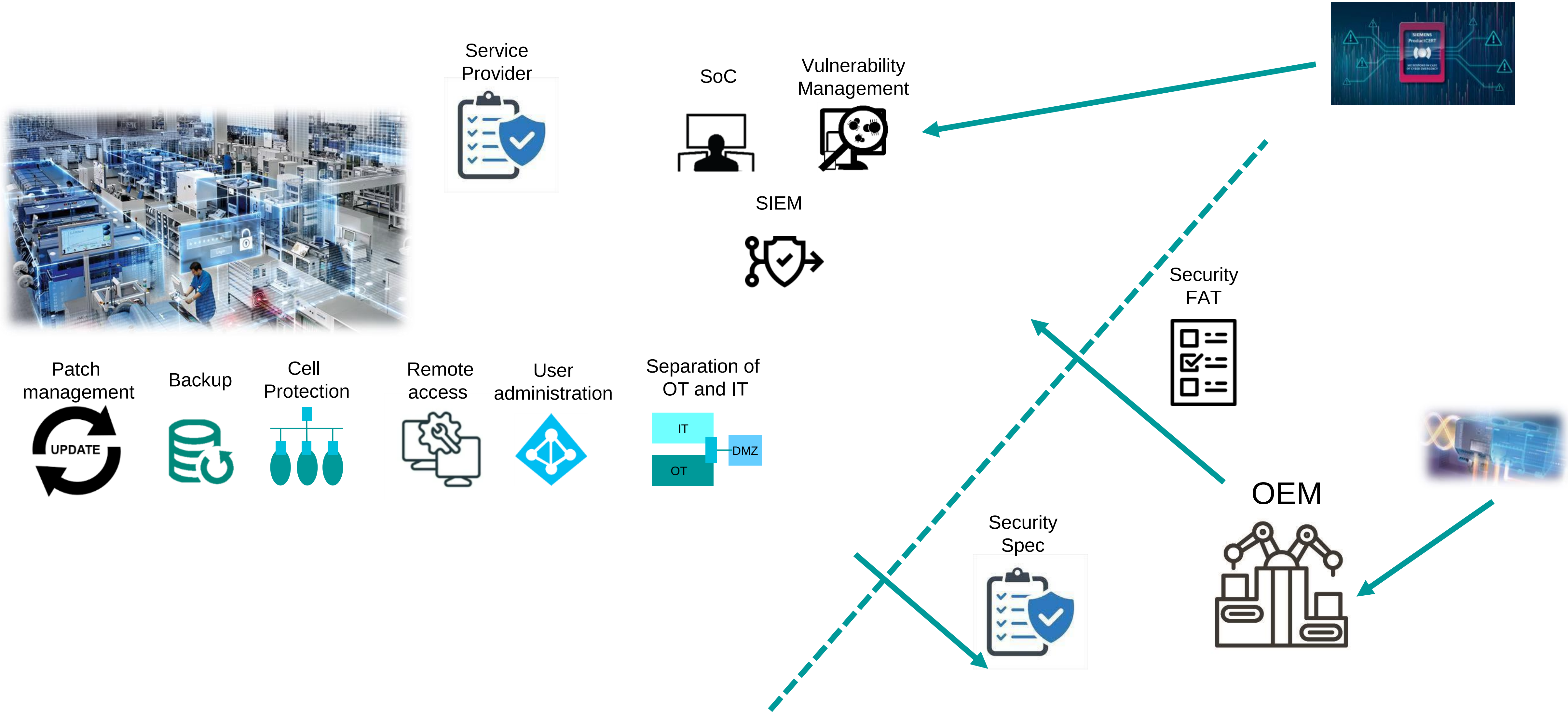
0 outages caused by our scanning activities

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
Cybersecurity

OT Security Consulting

SiESTA Siemens Extensible Testing Application

Secure production



Service Provider

SoC

Vulnerability Management

SIEM

Patch management

Backup

Cell Protection

Remote access

User administration

Separation of OT and IT

Security FAT

OEM

Security Spec

Contact

Morten Kromann
Security Expert
Siemens A/S
Bredskifte Alle 15
8210 Århus
Denmark

Phone +45 20 37 35 08

E-mail morten.kromann@siemens.com

SIEMENS