Siemens and the secrets of Stuxnet

Industrial Cyber Security

SIEMENS

Agenda

Overview

SIEMENS

Stuxnet

SIEMENS

Lesson Learned 1

SIEMENS

Lesson Learned 2

SIEMENS

Lessons Learned 3

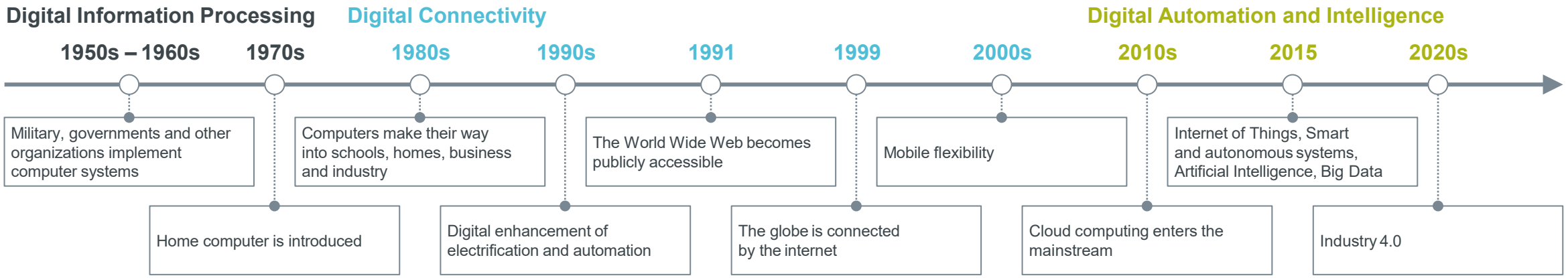
SIEMENS

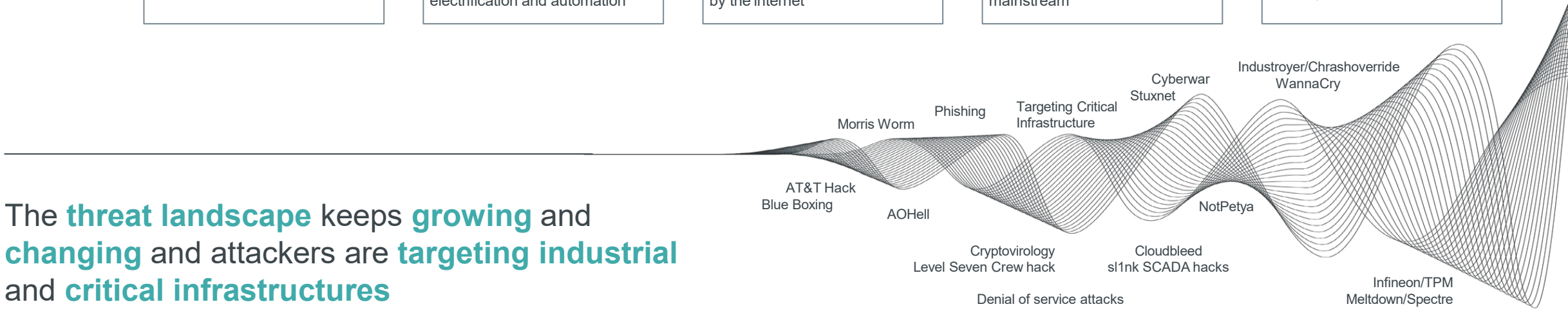
SIEMENS

Overview

SIEMENS

Evolution of the cyber threat landscape





The **threat landscape** keeps **growing** and **changing** and attackers are **targeting industrial** and **critical infrastructures**

DF CS SD SCP PSS

SIEMENS

Stuxnet

SIEMENS

Stuxnet: Targeted Trojan against specific Plant Configuration

Trojan Analysis

- High sophistication of propagation and infection mechanisms:
  - 4 zero-day exploits within the Microsoft Windows operating system
  - Theft of 2 different valid certificates
  - 60000 lines of code
- Implementation of the Trojan required
  - in-depth expertise of SIMATIC programming and
  - insider knowledge of specific plant details

Impact

Infected general PCs	>10000
Infected PCs with SIMATIC automation software installed	24
Number of damaged plants known to Siemens	0

Source: Süddeutsche Zeitung Online, 22.9.2010

SIEMENS

Lesson Learned 1

SIEMENS

Lessons Learned 1:
Have a process for vulnerability handling!

We expect them…

- Party Researchers
- Government Test Labs
- Security Standards
- Siemens System Test

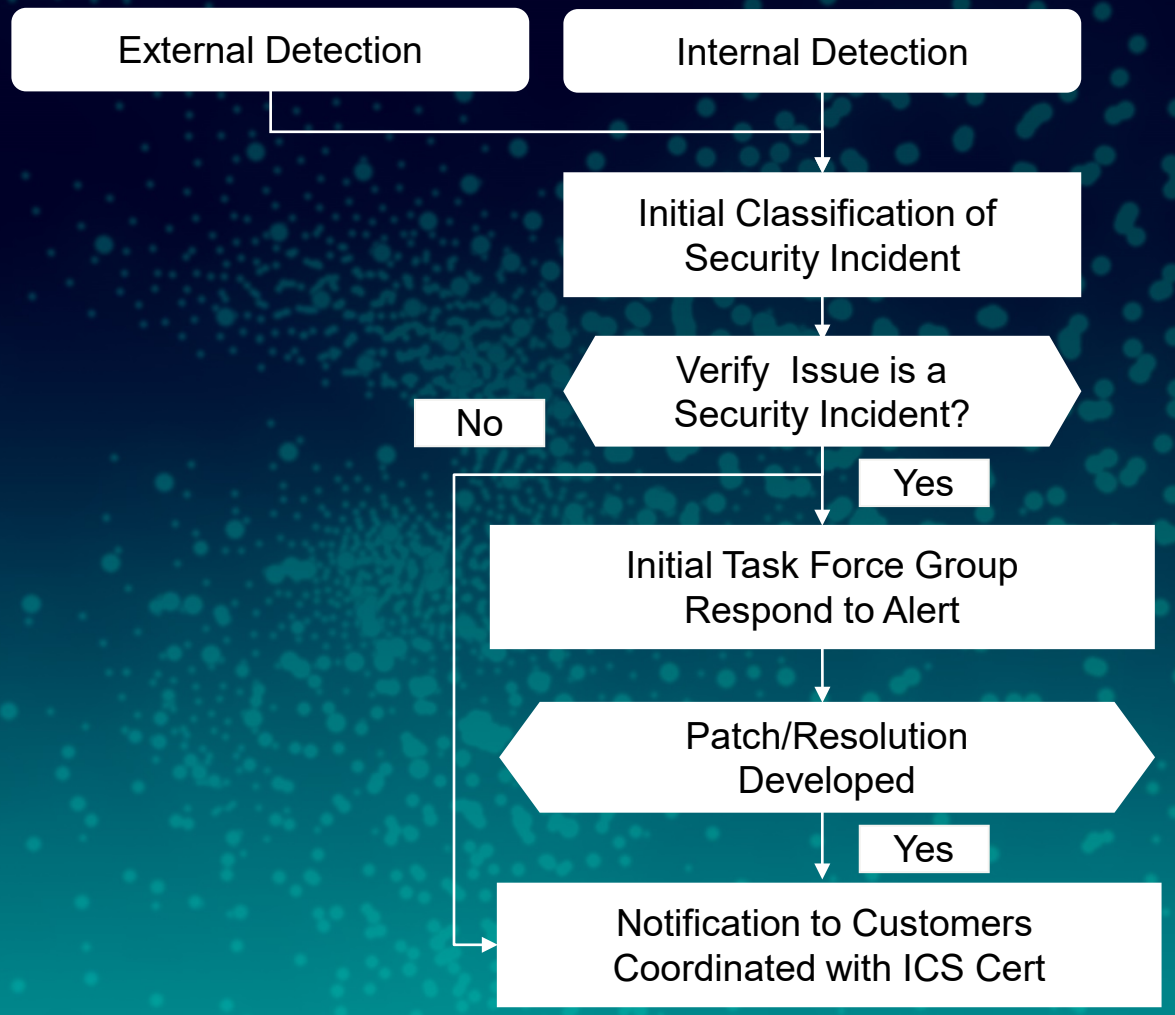
We plan for them…

- Have made changes in our processes
- Are making changes in our products

Siemens is working to avoid them…

- Initial Design
- System Test
- Security Test Lab

We will support our customers!

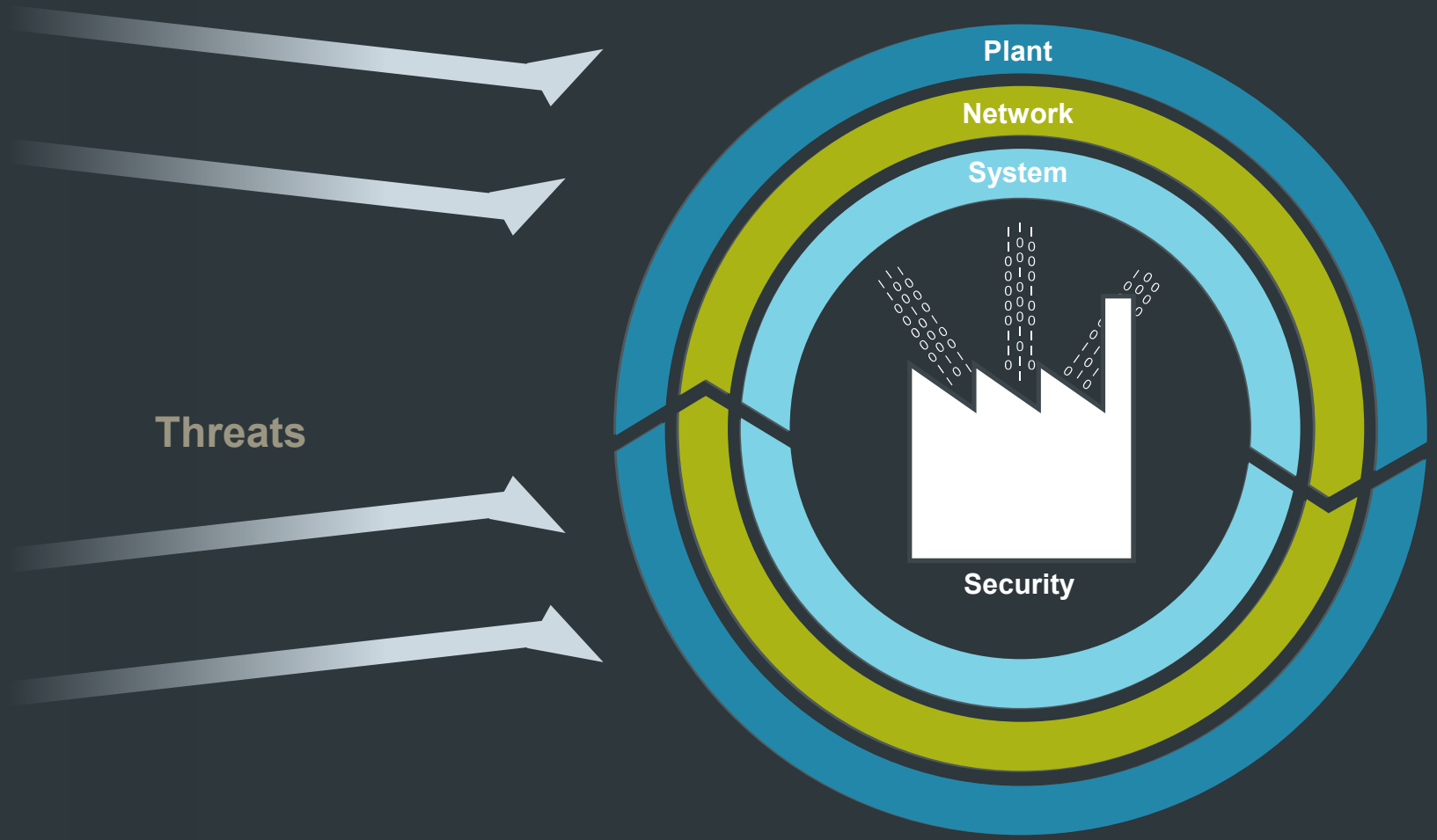


SIEMENS

Lesson Learned 2

SIEMENS

Lessons Learned 2:
Take a leading standard and apply it!
Defense-in-Depth-Concept based on IEC-62443



Plant security

- Physical access protection
- Processes and guidelines
- Holistic security monitoring

Network security

- Cell protection
- Perimeter protection
- Firewalls and VPN

System integrity

- System hardening
- Patch management
- Detection of attacks
- Authentication and access protection

Holistic Security Concept takes security on the next level - A holistic approach for IT and OT

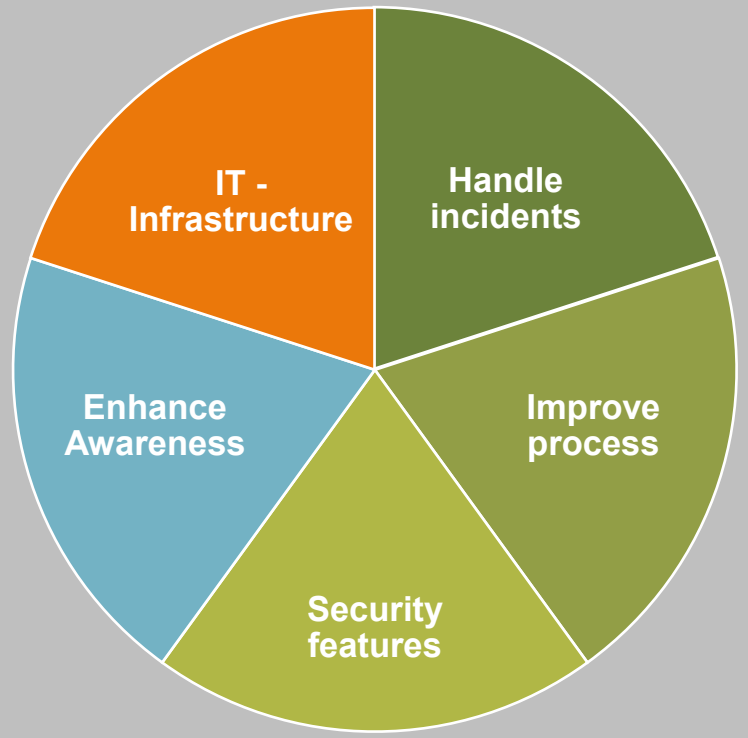
HSC answers key questions for security in business

“What in my business do I need to protect?”
Identification of the critical business assets is a core component of the concept

“Which level of security do I need?”
Security level drives requirements, in alignment with IEC 62443, to protect against attacks

“How do I protect the specific assets?”
Standards based security solutions are applied to protect and monitor the critical assets

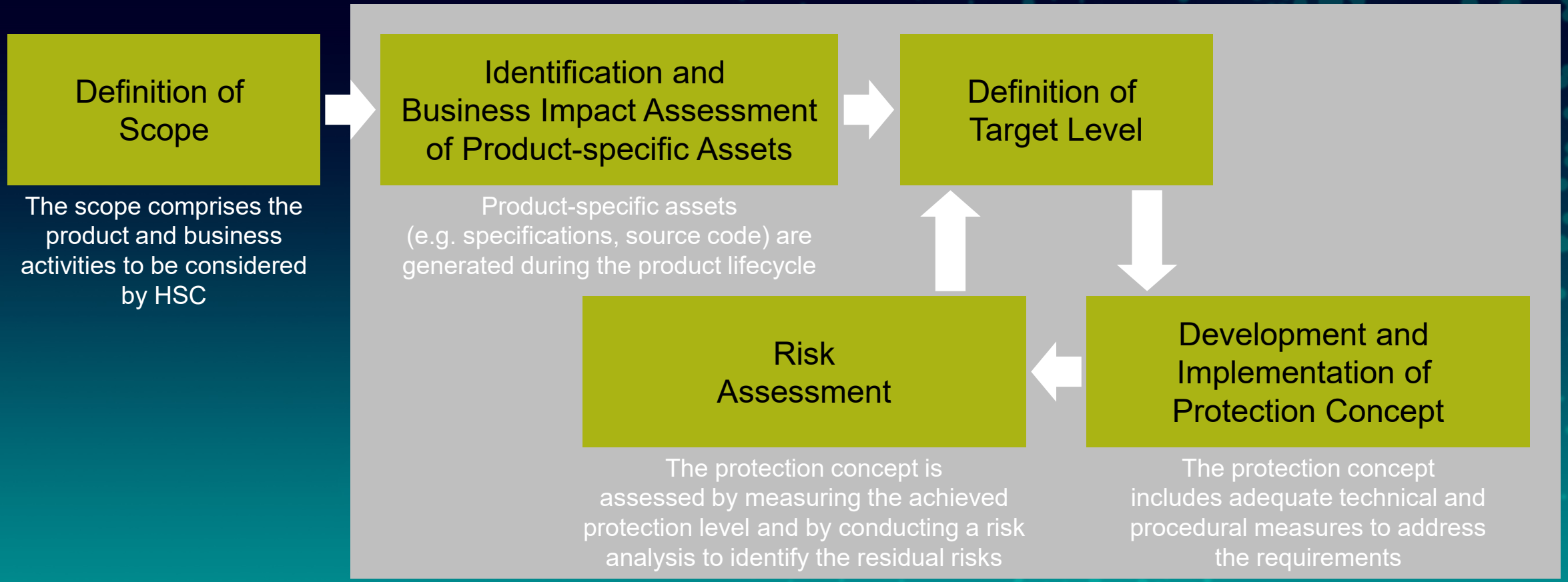
HSC addresses 5 levers including the IT



SIEMENS

General Workflow for the Protection of Product-specific Assets

IEC62443/ISO27001 Based Method



SIEMENS

Protection Levels are the key criteria and cover security functionalities and processes

Security process

- Based on IEC 62443-2-4 and ISO27001
- Maturity Level 1 - 4

Protection Level (PL)

Security functions

- Based on IEC 62443-3-3
- Security Level 1 - 4

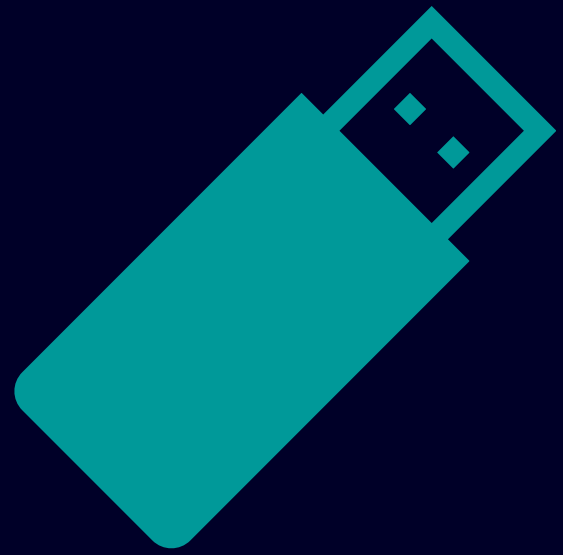
SIEMENS

Selected HSC security measures from PL 1 to PL 4

	Secure Physical Access	Organize Security	Secure Solution Design	Secure Operations	Secure Lifecycle management
PL 4	Revolving doors with card reader and PIN; Video Surveillance and/or IRIS Scanner at door	Dual approval for critical actions	Firewalls with Fail Close (e.g. Next Generation Firewall) …	…. Monitoring of all device activities	Online security functionality verification …
+					
PL 3	Revolving doors with card reader	… No Email, No WWW, etc. in Secure Cell …	… 2 PCs (Secure Cell/outside) …	… … Monitoring of all human interactions	Automated backup / recovery … Remote access with cRSP or equivalent
+					
PL 2	Doors with card reader	Persons responsible for security within own organization … Mandatory security education	Physical network segmentation or equivalent (e.g. SCALANCE) …	… Continuous monitoring (e.g. SIEM)	Backup verification Remote access restriction (e.g. need to connect principle)
+					
PL 1	Locked building/doors with keys	Awareness training (e.g. Operator Awareness Training) Mandatory rules on USB sticks (e.g. Whitelisting)	Network **segmentation** Firewall protection (e.g. SCALANCE S) …	… Security logging on all systems	Backup / recovery system

SIEMENS

Lessons Learned 3

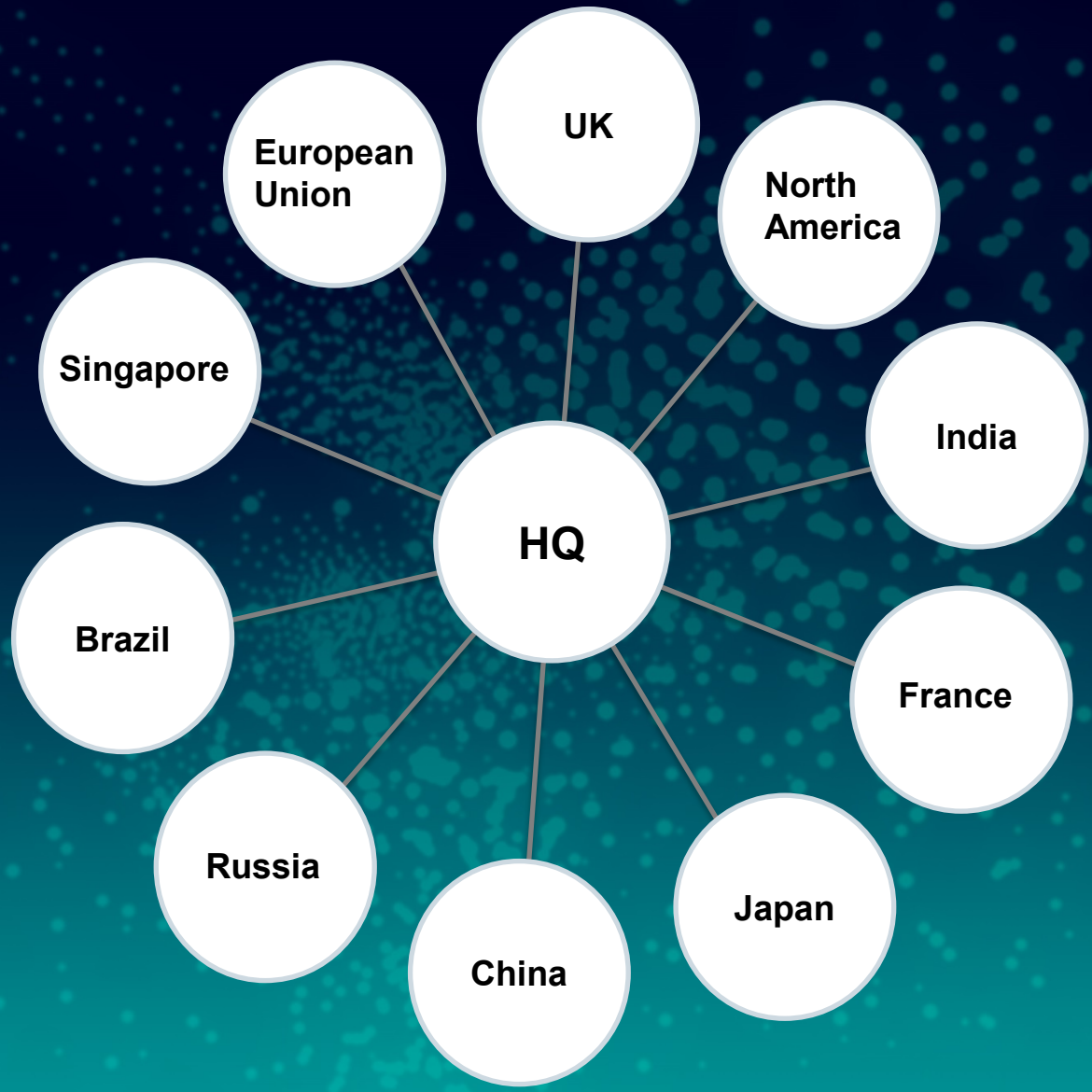


SIEMENS

Lessons Learned 3: Build a Security Network

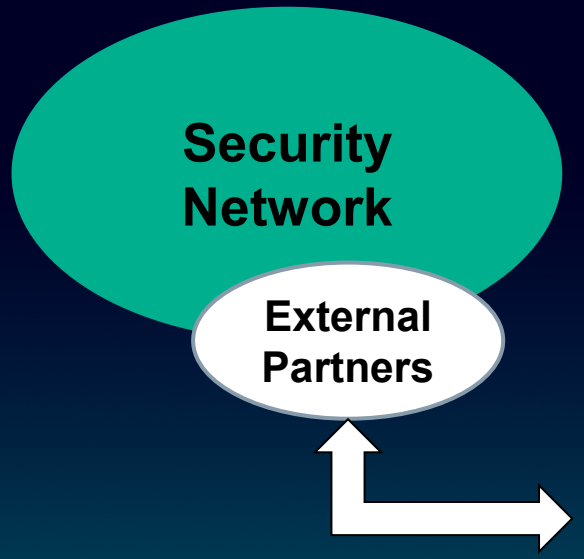
Tasks of the Security Hubs

- Setup of Security Network
- Worldwide Incident handling
- Setup of Alerts and remedies
- Cooperation with …
  - Local CERT
  - Governmental Departments
  - Standardization & Regulations
- Handling of Import/Export Issues



SIEMENS

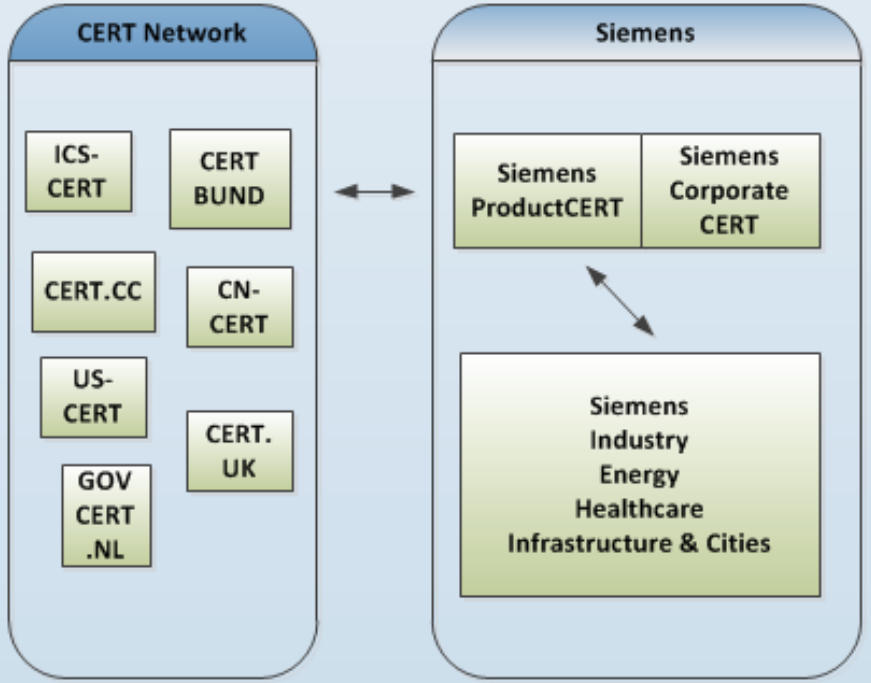
Industrial Security
Cooperation with governmental organizations



The organizational background of the CERT organizations

- The first CERT was founded in 1988
- Several hundred CERT organizations for governmental and private sector worldwide
- Trusted information exchange via the international organization “FIRST”
- Expected rules of cooperation are defined in the operational framework of FIRST
- Siemens has a ProductCERT

CERT cooperation



SIEMENS

The Outcome

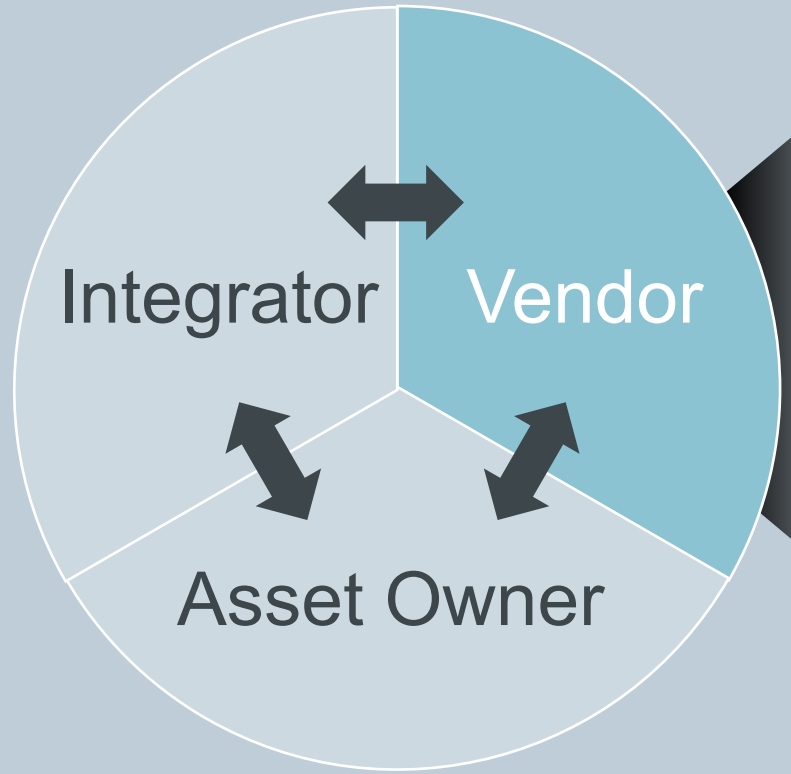
Industrial Security
Granted Certificates

• **ACHILLES certification**	• **IEC 62443**	• **ANSSI certification (CSPN)**
• Protection against DoS attacks • Defined behavior in case of attack • Improved Availability	• Certification of “Secure Product Development Lifecycle” for Division DF and PD based on IEC 62443-4-1 for 34 Sites since 2016	• First security level certification (CSPN – Certification de Sécurité de Premier Niveau)

SIEMENS

Industrial Security - Certification based on IEC 62443-4-1, 4-2 and 3-3 of development processes for industrial products of Siemens

Stakeholders according to IEC 62443



SIEMENS	TÜV SÜD Industrial IT Security – Secure Product Development Lifecycle
Security by design	✓
Security verification and validation testing	✓
Security update management	✓

SIEMENS

Industrial Security
Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity.

SIEMENS