Les actions et initiatives de Siemens

SIEMENS

Un sujet nouveau

La cybersécurité

Que fait Siemens en la matière ?

Rétrospective

SIEMENS

1998 Création du CERT Siemens pour la protection des infrastructures IT internes du groupe.

2004 Création du laboratoire de sécurité pour WinCC et PCS7.

2005 Naissance de la gamme Scalance S (firewall et modules VPN)
Publication du premier guide de mise en sécurité des systèmes PCS7 et WinCC.

2006 Sécurisation des installations de production.

2008 Intégration dans les roadmap produits de fonctions de sécurité.

2010 Apparition du malware Stuxnet.

Rétrospective

SIEMENS

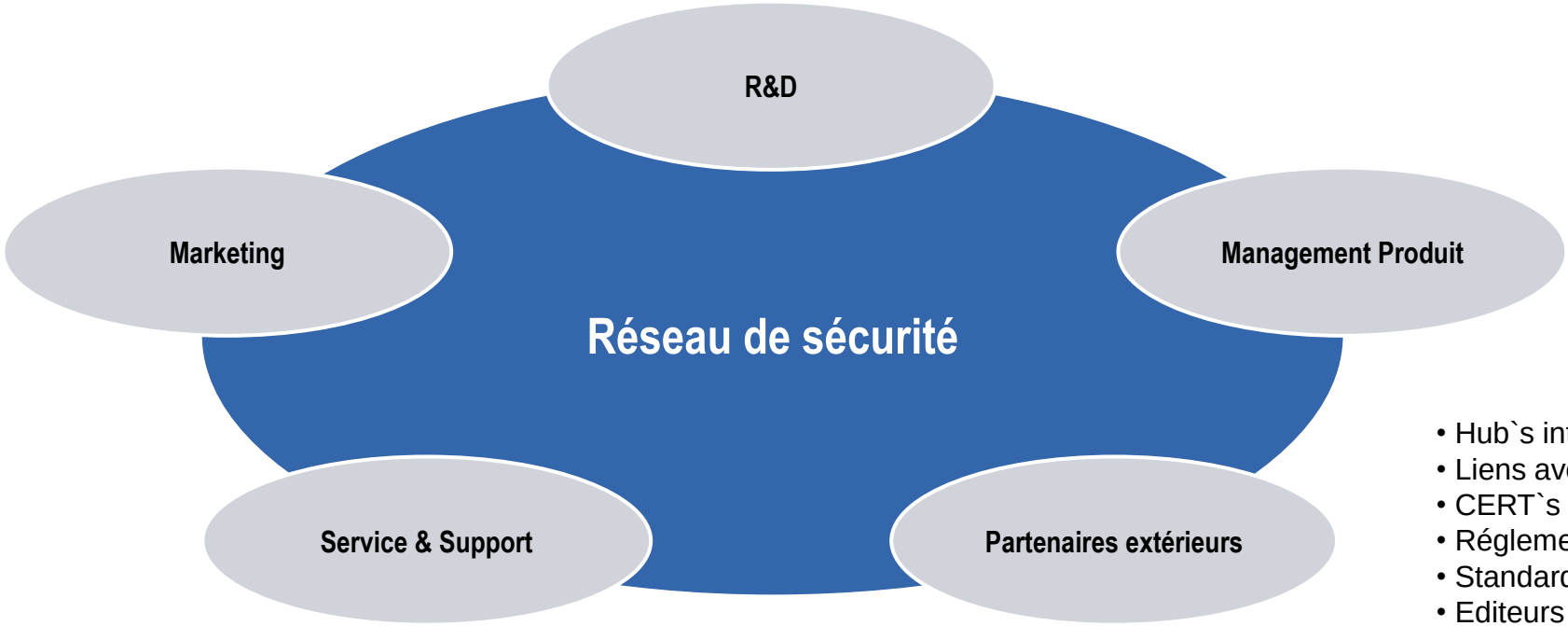
2010 (4 semaines) Mise à disposition par Microsoft, Siemens et différents éditeurs de logiciels d'antivirus, d'une première solution de détection et d'élimination de ce malware.

2011 Lancement du projet "Industrial Security".

2012 Implémentation de fonctions de sécurité dans une large gamme de produits.

2013 Lancement du S7-1500 avec fonctions de sécurités intégrées.

Sécurité industrielle
Le réseau de sécurité du secteur Industry



- Hub`s internationaux
- Liens avec organismes étatiques
- CERT`s
- Réglementation Import / Export
- Standardisation & Normalisation
- Editeurs de logiciels de sécurité
- Réseau de sécurité des éditeurs logiciels OEM`s

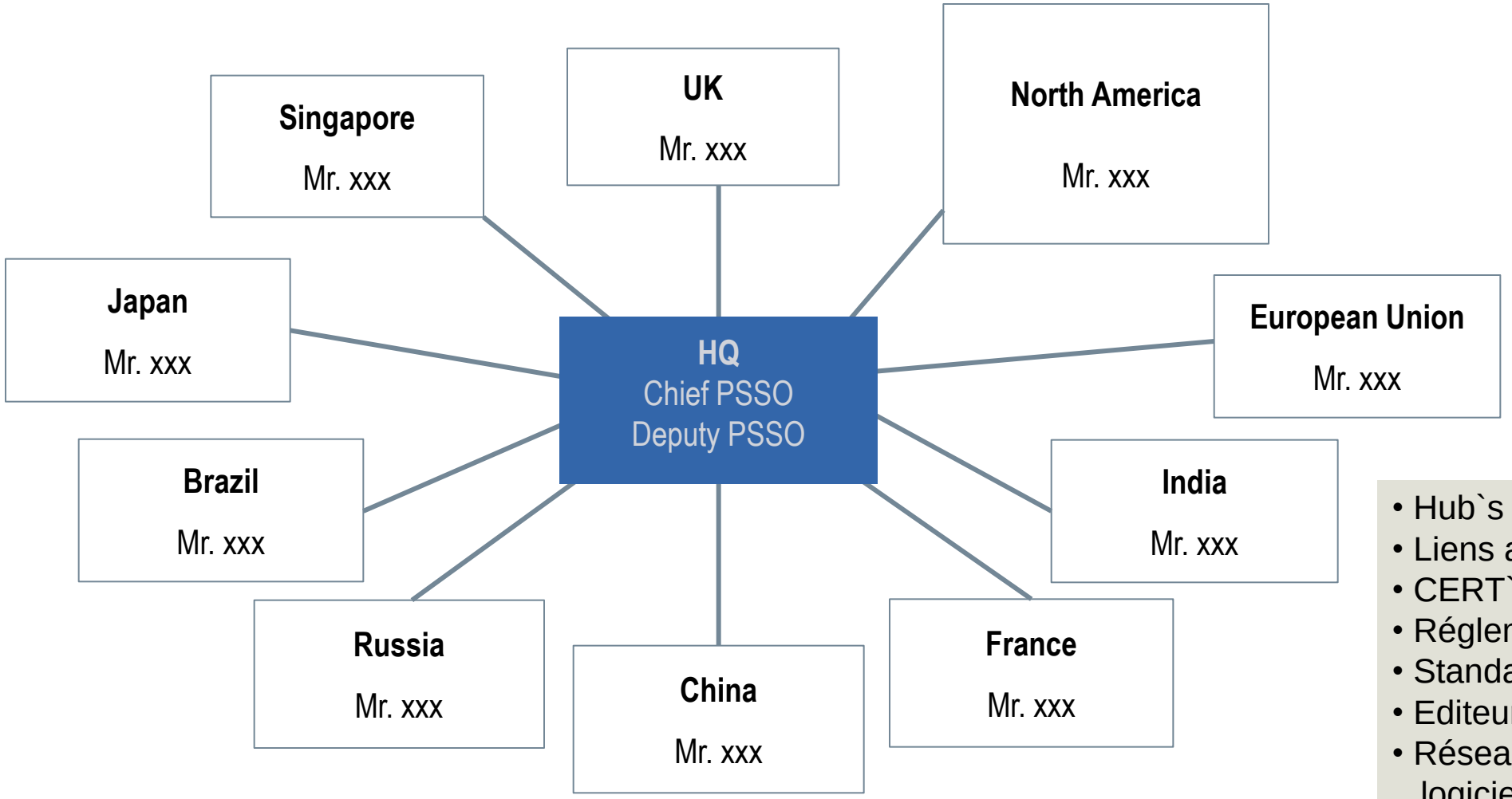
Mise en place d'un réseau de sécurité pour …
…réagir rapidement en cas de situation de crise
…piloter et coordonner tous les sujets relevant de la sécurité

Changements interne au groupe

SIEMENS

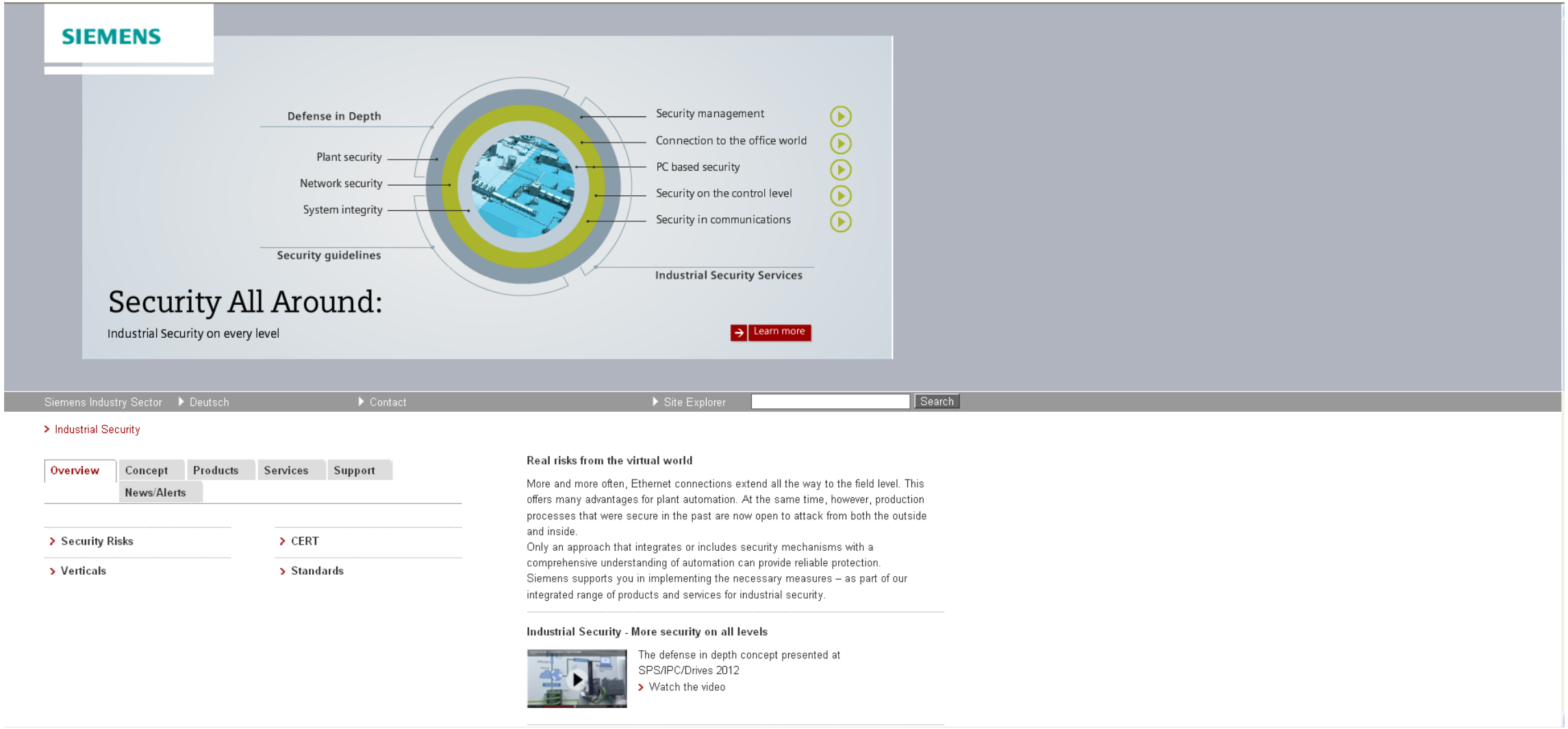
System Test	▪ IP Hardening ▪ Durcissements des tests de robustesse
Process d'escalade et de réaction en cas d'incident	▪ Process d'escalade et de réaction définis et fonctionnels
Nouveaux postes	▪ Product Security Officer et Security Expert
Modifications des Process	▪ Guide de codage, analyse statique de code, etc. pour la R&D ▪ Mise en place d'une politique de gestion du risque dans le cycle de vie produit.
Standards & Regulations	▪ Forte coopération avec les organismes de standardisation ▪ Certifications Achilles Niveau 2 …
Sensibilisation et renforcements des connaissances	▪ Workshops, formation en ligne obligatoires, conférences, présentations ▪ Formations spécifiques pour les développeurs

Sécurité industrielle
Un réseau international

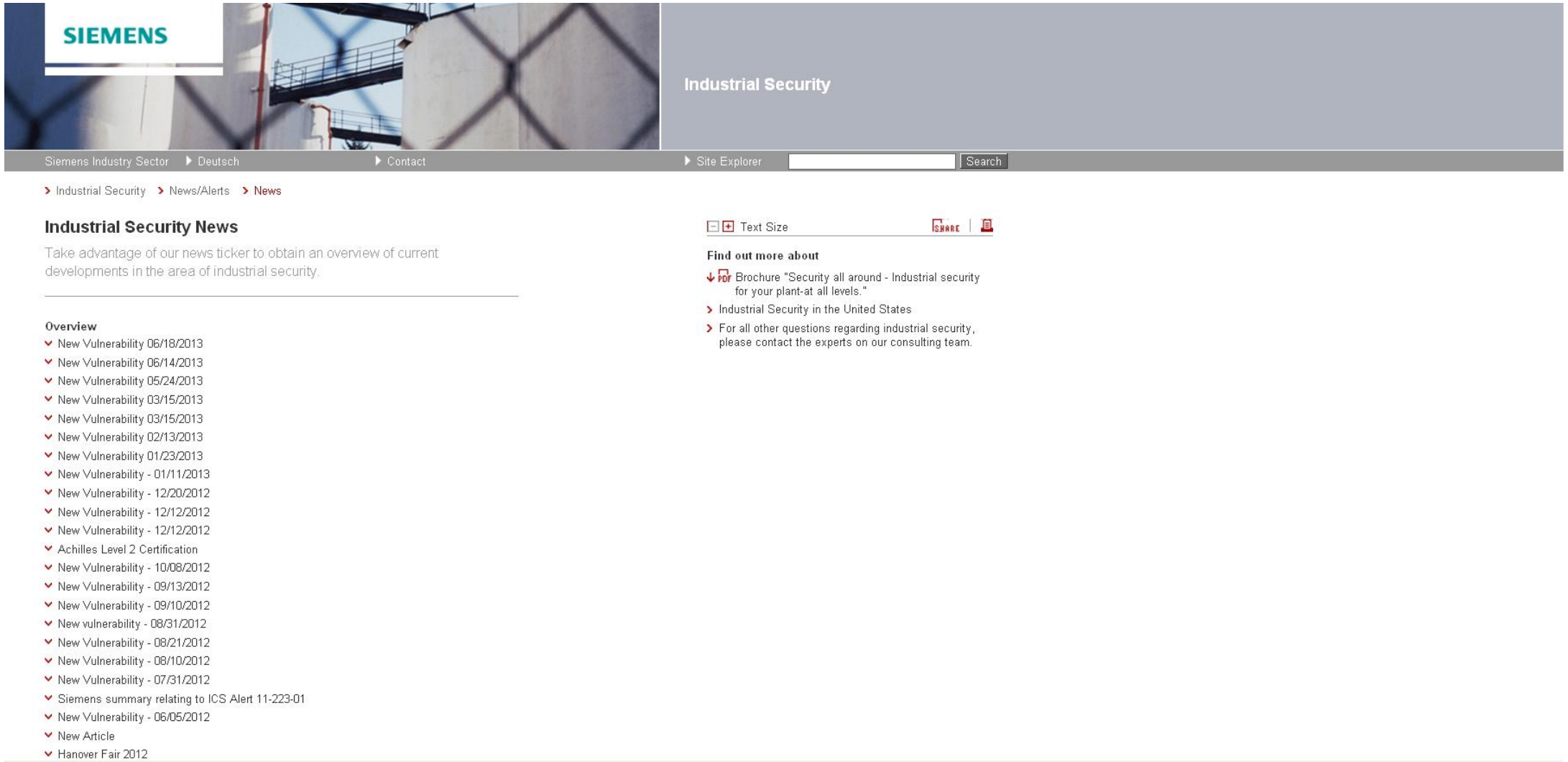


- Hub`s internationaux
- Liens avec organismes étatiques
- CERT`s
- Réglementation Import / Export
- Standardisation & Normalisation
- Editeurs de logiciels de sécurité
- Réseau de sécurité des éditeurs logiciels OEM`s

Création d'un site Internet sur la cybersécurité industrielle ouvert à tous



Création d'un site Internet sur la cybersécurité industrielle ouvert à tous

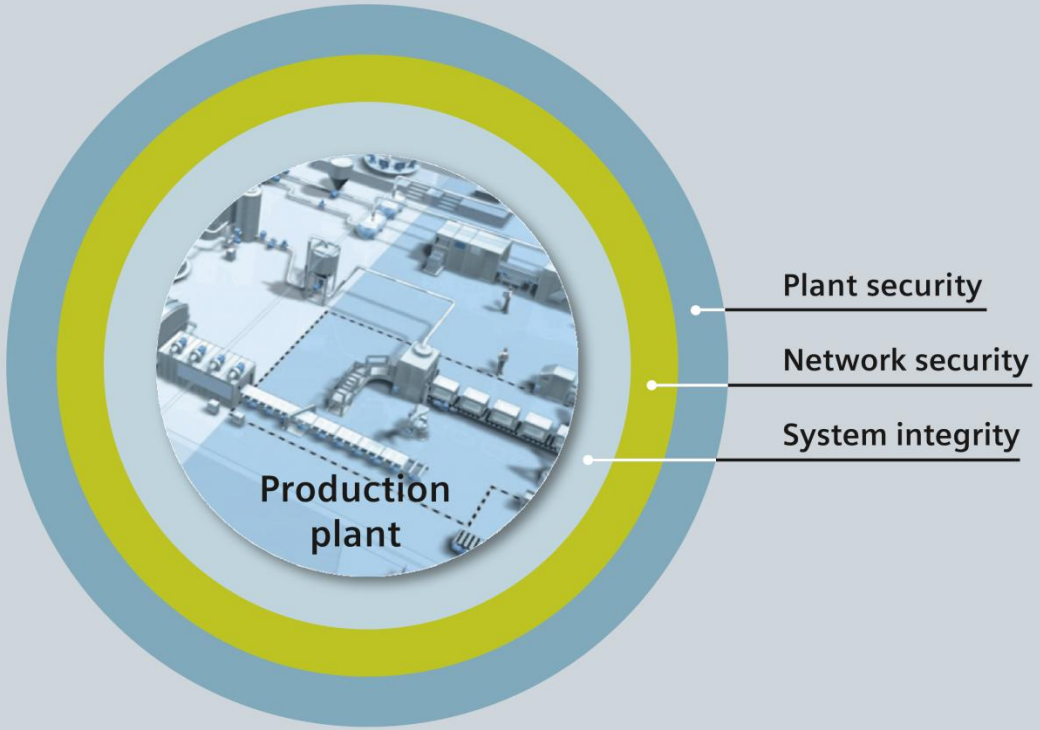


Création d'un site Internet sur la cybersécurité industrielle ouvert à tous

Security concept for the protection of industrial plants
This whitepaper gives an overview of Industrial Security. It describes the threats and risks to which industrial automation networks are exposed and presents concepts for minimizing these risks and achieving adequate protection from an economic standpoint.
In addition, it also gives an insight into what direction the situation will take as it develops based on current trends and what security mechanisms will also be able to be used in industrial environments in the future.
Download PDF

White papers
- Operational Guidelines
- ARC white paper cyber security
- Security for S7-controller
- Security white paper PC-based
- ARC whitepaper on Industrial Security in PCS 7
- SIMATIC PCS 7 / WinCC Security concept - White paper

Cybersécurité des systèmes Industriels
Le concept de défense en profondeur



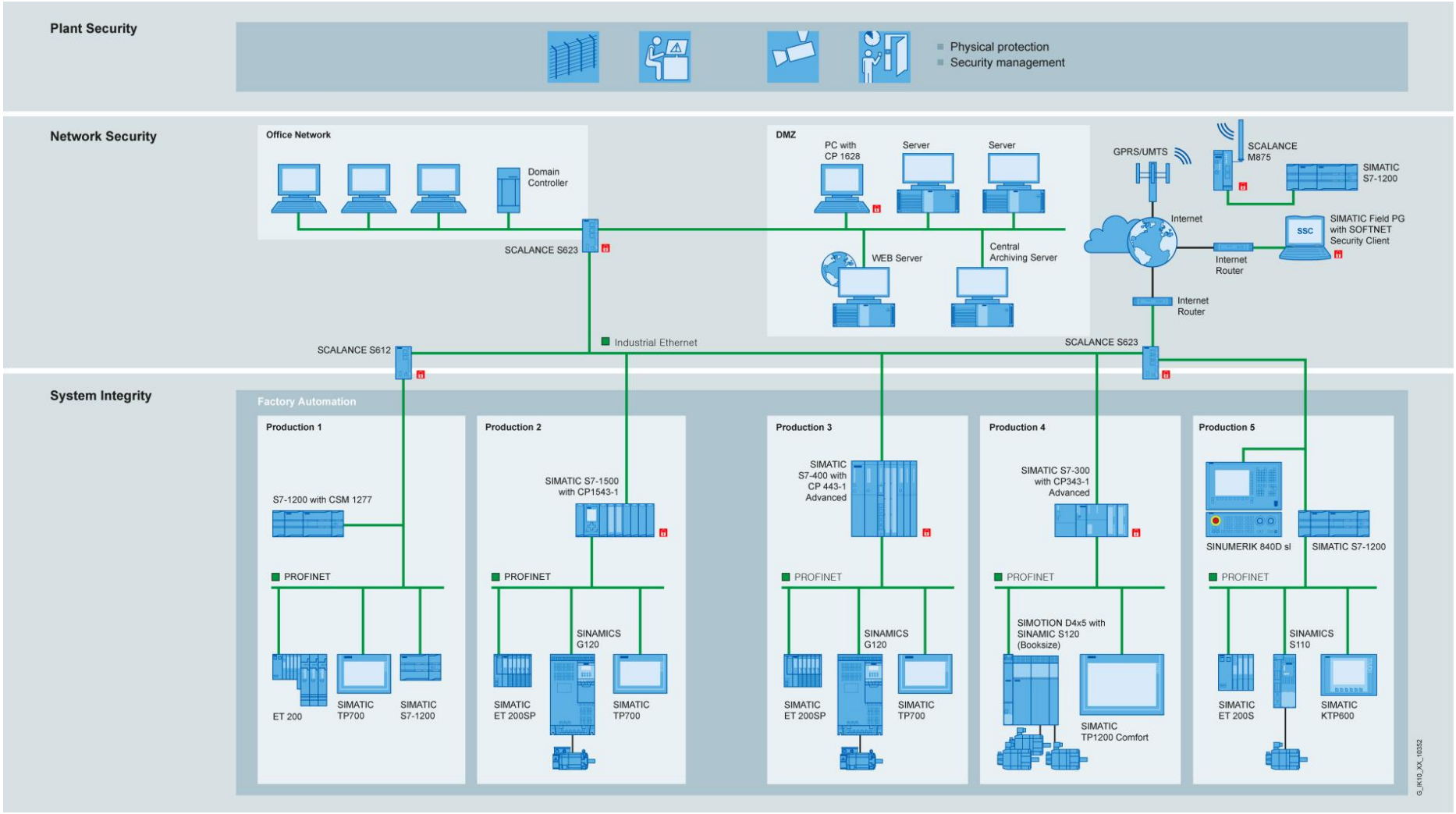
Sécurité Site
- Contrôle d'accès pour éviter les intrusions
- Protection physique des zones sensibles

Sécurité réseau
- Séparation des réseaux bureautique et des réseaux de production
- Segmentation des réseaux de production

Intégrité du système
- Antivirus et logiciel de whitelisting
- Maintenance et mise à jour logiciel
- Authentification des utilisateurs
- Mécanismes de protection d'accès intégrés aux équipements lorsque que cela est possible

Dans un contexte industriel les solutions de sécurité doivent prendre en compte tous les niveaux de protection.

Cybersécurité des systèmes Industriels
Architecture type



SIEMENS

Besoin Client

Protection réseau et segmentation

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable
- Mise en place **d'accès distant sûr**:
- Télémaintenance

Notre solution

SCALANCE S Modules de sécurité:

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NAT/NAPT (translation d'adresse)
- Fonction router (PPPoE, DDNS)
- S623 port additionnel (DMZ)
- Redondance de firewall

SCALANCE S
602/612/623

SIEMENS

Besoin Client

Protection réseau et segmentation

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable
- Mise en place **d'accès distant sûr**:
- Télémaintenance

Notre solution

SCALANCE M:

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NAT/NAPT (translation d'adresse)
- Router pour accès mobile (GPRS, UMTS et même LTE)
- Routeur d'accès ADSL
- Routeur d'accès SHDSL

SCALANCE M

Besoin Client

Protection et segmentation réseau sans ajout de composant supplémentaire

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable

Notre solution

CP 343-1/ CP 443-1 Advanced

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NAT/NAPT (translation d'adresse)
- HTTPs (pages HTML chiffrées SSL)
- FTPs (Transfert de fichiers sécurisé)
- NTP(secure) (Transfert sécurisé

de la date et l'heure avec authentification)

- SNMP V3

CP 343-1 Advanced
CP 443-1 Advanced

Cybersécurité des systèmes Industriels
CP1543-1

SIEMENS

Besoin Client

Protection et segmentation réseau sans ajout de composant supplémentaire

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable

Notre solution

CP 1543-1

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NAT/NAPT (translation d'adresse)
- HTTPs (pages HTML chiffrées SSL)
- FTPs (Transfert de fichiers sécurisé)
- NTP(secure) (Transfert sécurisé de la date et l'heure avec authentification)
- SNMP V3

CP 1543-1

* as of V12 SP1

Cybersécurité des systèmes Industriels
CP 1628

SIEMENS

Besoin Client

Protection des stations de développement et des postes opérateurs

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable

Notre solution

CP 1628

- Stateful Inspection Firewall
- VPN (chiffrement des données)
- NTP(secure) (Transfert sécurisé de la date et l'heure avec authentification)
- SNMP V3

CP 1628

Cybersécurité des systèmes Industriels
SOFTNET Security Client

SIEMENS

Besoin Client

Accès sécurisé pour stations de développement et les PC de télémaintenance

Protection contre:

- Espionnage
- Manipulation Données
- Accès indésirable

Notre solution

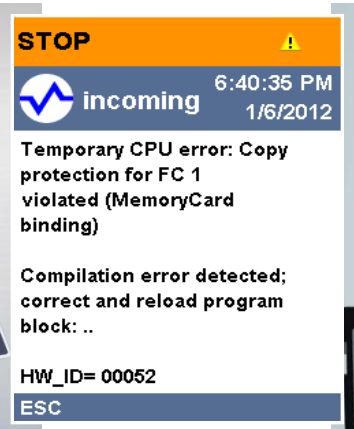
SOFTNET Security Client

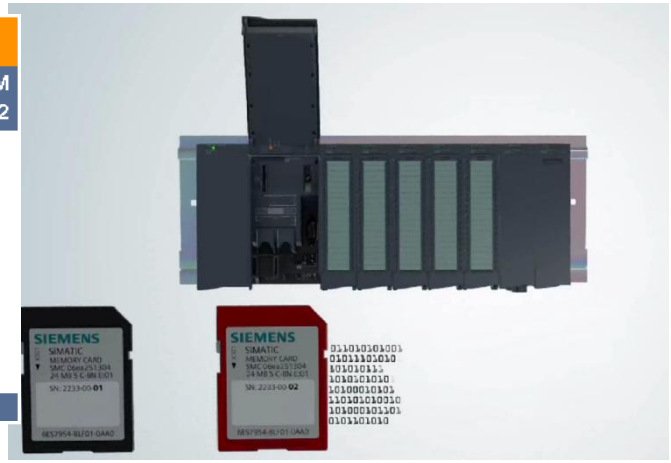
- VPN (chiffrement des données)

SOFTNET
Security Client

Cybersécurité des systèmes Industriels
SIMATIC S7-1500 et TIA Portal

SIEMENS





- Protection de la propriété intellectuelle et des investissements
- Protection contre la copie des programmes applicatifs
- Protection avancée contre les modifications de projet non autorisées
- Protection contre les manipulations non autorisées

Cybersécurité des systèmes Industriels
Antivirus et whitelisting

SIEMENS

Besoin Client

Détection et prévention des Virus, Worms et chevaux de Troyes

Protection contre:

- Code malicieux
- Manipulation de code

Notre solution

Antivirus et whitelisting

- Nos solutions sont testées avec

de grands éditeurs de logiciel d'Antivirus

TREND MICRO

symantec.

McAfee virusscan

Change Control
McAfee Embedded Security
Application Control

Nouveaux produits
Fonctions de sécurité intégrées

	SCALANCE S family	SCALANCE M875	CP 343-1 Adv/ CP 443-1 Adv	S7-1200 CPU 2) S7-1500 CPU	CP1543-1	CP 1628	SOFTNET Security Client
Configurable copy protection				•			
Access protection (authentication)				•			
Extended access protection (Firewall)	•	•	•		•	•	
Virtual Private Network with IPSec	•	•	•		• 1)	•	•
Manipulation protection (communication, configuration)	•	•	•	•	•	•	•

G_IK10_XX_10347

• applies

1) VPN (V12 SP1 or higher)

2) Firmware V4.0 (V12 SP1 or higher)

Cybersécurité des systèmes Industriels

Premier équipementier avec la certification Achilles Niveau 2 depuis 2012

API certifiés Achilles Niveau 2

S7-1500 PN/DP
S7- 300 PN/DP
S7- 400 PN/DP
ET 200S CPU

CP certifiés Achilles Niveau 2

CP 343-1 Advanced
CP 443-1 Advanced
CP 1628
CP 1543-1

+ Protection contre DoS
+ Comportement prédéfinit en cas d'attaque
➔**Disponibilité accrue**
➔**Protection IP**
➔ **Standard International**

Merci de votre attention!

SIEMENS

Jean-Christophe MATHIEU

Product and Solution Security Officer

Secteur Industry