Cybersécurité des systèmes industriels Siemens, 10 ans déjà…

CyberCercle, 10 Décembre 2020

SIEMENS

Table of contents
Index / Agenda

SIEMENS

La cyber, un enjeu majeur dans la digitalisation de l'économie

Traitement numérique de l'information

1950s – 1960s
Mise en place des premiers ordinateurs par les gouvernements, les militaires et quelques grandes organisations

1970s
Lancement de l'ordinateur personnel

Connectivité numérique

1980s
Les ordinateurs arrivent dans les écoles, entreprises, usines et chez les particuliers

1990s
Amélioration numérique de l'électrification et de l'automatisation

1999
Le monde entier se connecte à internet

1991
Internet (World Wide Web) disponible au public

Automatisation numérique

2010s
Développement de l'usage du cloud computing

2000s
Développement de l'usage mobile

2020s
Internet des objets (IoT), Systèmes autonomes et intelligents, Intelligence artificielle, Big Data

2020s
Industrie 4.0

SIEMENS

Cybersécurité: des menaces réelles
Tous les domaines touchés

SIEMENS
Ingenuity for life

Des cibles variées : systèmes IT (web) / systèmes OT (industrie) / IoT (objets) – aucunes limites

Les *VICES* de l'espèce humaine : *Vénal, Idéologie, Compromission, Ego, Sabotage*…

SIEMENS

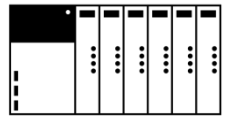
On explique depuis plusieurs années, à raison, que les attaques se déplacent

IT

Système d'information utilisé pour la communication d'entreprise

OT (ICS, DCS)

Systèmes opérationnels utilisés au niveau de l'usine



Automation hardware

Power Meters

DCS / HMI screens

Field Devices

- Focus traditionnel pour les investissements cyber
- Les systèmes sont remplacés tous les 3 – 5 ans
- Assets connus / Bien compris
- Les pirates volent les données
- Tolérance pour le basculement ou le délai

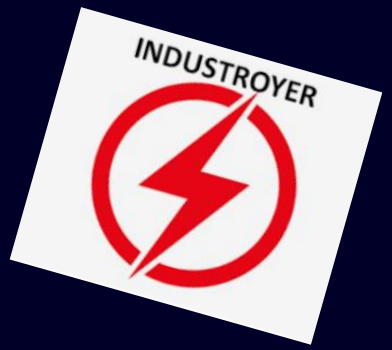
- Souvent ignoré – maturité faible en cyber
- Legacy systems de plus de 20 – 30 ans
- Beaucoup d'assets inconnus / pas très bien compris
- Les attaquants perturbent / détruisent / retardent l'alimentation
- La **disponibilité** est **critique**

Domaine de Siemens - Expertise approfondie du domaine

De l'IT vers l'OT

SIEMENS

Alors que plus exactement elles profitent de la convergence IT-OT



SIEMENS

Stuxnet, premier “exemple” connu d’un virus spécifiquement conçu pour attaquer les systèmes industriels

Un niveau de sophistication et de maturité étonnant des attaquants: aussi élevé en OT qu’en IT…

- Découvert à l’été 2010…origine sans doute étatique
- Complexité inhabituelle, souvent décrit comme cyberarme: utilisation de failles 0-day Windows (.lnk), capacité à détecter puis reprogrammer les automates ciblés (accélération jusqu’à explosion des rotors d’aluminium des centrifugeuses) et de cacher le tout à la supervision
- 100.000 systèmes affectés dont 65.000 en Iran (au 29/09/2010), dont site de Natanz (centrale de Bouchehr…)
- Hypothèse: aurait été conçu par la NSA en collaboration avec l’unité militaire israélienne 8200, opération « Olympique Games » initiée sous l’administration Bush et continué sous celle d’Obama
- But: s’attaquer aux centrifugeuses iraniennes d’enrichissement d’uranium (1000 centrifugeuses hs)
- Bref…Stuxnet a transformé un risque théorique connu depuis longtemps en réalité technique…

SIEMENS

A cause de… STUXNET … finalement, grâce à !!!

Certification Achilles

Holistic Security Concept

Certification IEC62443

Gamme S7-1500

Qualification ANSSI

Maintien en Qualification ANSSI

ProductCERT

Qualifié

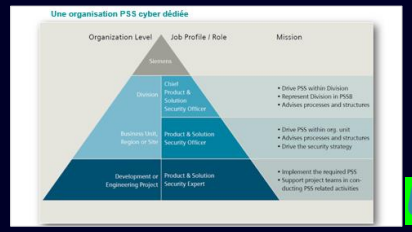
CSPN

S7-1518 & XM408 les 1ers lauréats

Les services cyber

Les 3 derniers lauréats, nos automates redondants !

Une organisation dédiée



2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020…

SIEMENS

Aucun autre automate redondant n'est qualifié par l'ANSSI… mais hormis Siemens, aucun autre automate n'a décroché la qualification à ce jour !

Discours ANSSI pratique:

- "Vous êtes OIV, vous DEVEZ declarer vos SIIV et les HOMOLOGUER, au sens LPM du terme"
- "Nous vous recommandons d'acheter du matériel qualifié ANSSI"
- "Qualifié ANSSI = pré-homologué !"
- "Pour les PLC, SIEMENS sont les seuls, prenez des S7-1500 !"

Liste des matériels qualifies pour les ICS

Tixeo - Tixeo Secure Video Conferencing						
11.5.2.0	24/03/2020	31/12/2020	Elémentaire		✓	912
Protection des systèmes industriels						
Codra Ingénierie Informatique - Panorama Suite						
Panorama E2	26/03/2020	26/03/2023	Elémentaire		✓	919
Siemens - Automates programmables gamme SIMATIC S7-1500						
2.6	25/04/2019	25/04/2022	Elémentaire		✓	1716
2.1.0	09/11/2017	09/11/2020	Elémentaire			5479
Stormshield - Stormshield Network Security - Pare-feu Industriel SNi40						
2.7.4	09/10/2018	09/12/2021	Elémentaire		✓	16934
Protection du poste de travail						
Ministère des armées - Acid Cryptofiler						
7.1.5.x	07/12/2017	07/12/2022	Standard	Diffusion Restreinte	✓	6143

ICS

1 suite logicielle

1 gamme complète de 21 PLC

1 matériel

SIEMENS

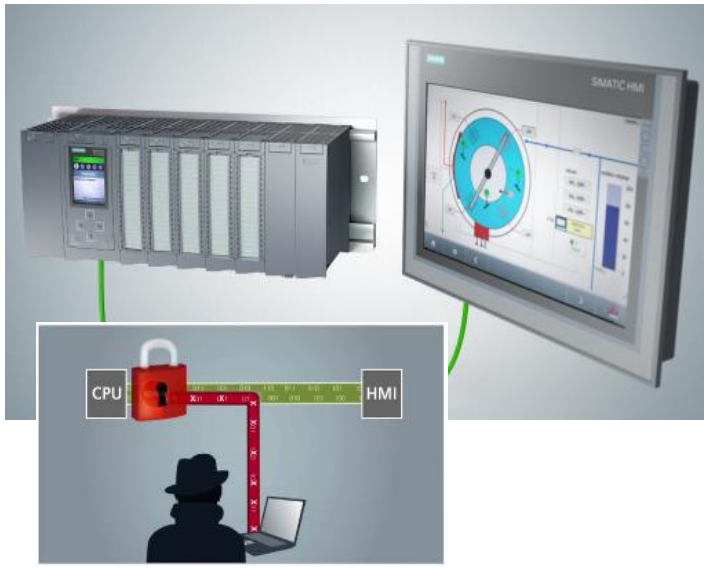
STORMSHIELD

SIEMENS

La qualification, concrètement, comment se traduit-elle “sur le terrain” ?

Security Integrated

Fonctions de sécurité évaluées
Gestion des entrées malformées
Stockage sécurisé des données utilisateur
Authentification sécurisée à l'interface d'administration
Politique d'accès
Signature du firmware
Intégrité et authentification du programme utilisateur
Authenticité et intégrité des commandes du mode de fonctionnement
Communications sécurisées
Fonction(s) de sécurité non évaluées
Néant
Restriction(s) d'usage
Non



Chiffrement

Protection physique

Authentification

Signature crypto

Cloisonnement

Protection anti-rejeu

SIEMENS

Et l'aventure continue, encore et encore…

Simatic S7-1518

Certifié et Qualifié (Avril 2016)

Scalance XM400

Certifié (Juin 2016)

Les versions qualifiées du produit peuvent être identifiées avec les informations ci-dessous.

Référence du produit	Type
6ES7518-4AP00-0AB0	CPU 1518-4 PN/DP
6ES7518-4FP00-0AB0	CPU 1518F-4 PN/DP
6ES7517-3AP00-0AB0	CPU 1517-3 PN/DP
6ES7517-3FP00-0AB0	CPU 1517F-3PN/DP
6ES7516-3FN01-0AB0	CPU 1516F-3 PN/DP
6ES7516-3AN01-0AB0	CPU 1516-3 PN/DP
6ES7516-2PN00-0AB0	ET 200pro:CPU 1516PRO-2 PN
6ES7516-2GN00-0AB0	ET 200pro:CPU 1516pro F-2 PN
6ES7515-2FM01-0AB0	CPU 1515F-2 PN
6ES7515-2AM01-0AB0	CPU 1515-2 PN
6ES7513-1FL01-0AB0	CPU 1513F-1 PN
6ES7513-1AL01-0AB0	CPU 1513-1 PN
6ES7512-1SK01-0AB0	CPU 1512SP-1 PN
6ES7512-1SK01-0AB0	CPU 1512SP-1 PN
6ES7511-1FK01-0AB0	CPU 1511F-1 PN
6ES7511-1AK01-0AB0	CPU 1511-1 PN
6ES7510-1SJ01-0AB0	CPU 1510SP F-1 PN
6ES7510-1DJ01-0AB0	CPU 1510SP-1 PN

SIEMENS

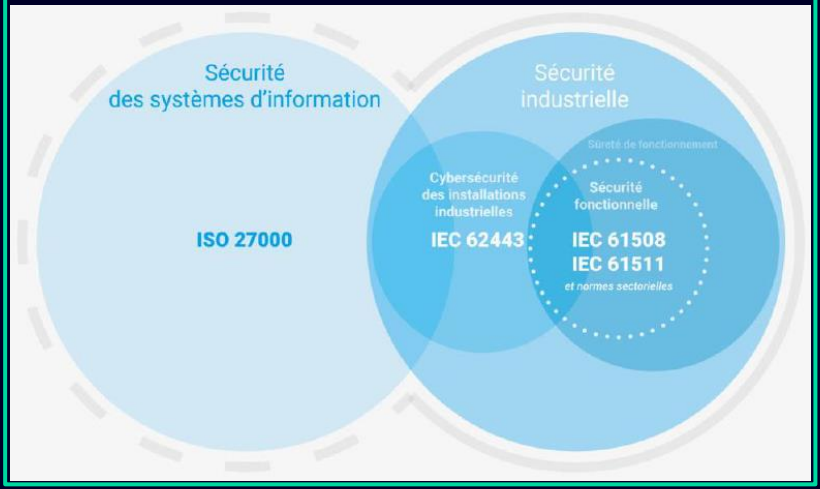
L’alliance de la cybersécurité et de la sûreté

La dualité “security-safety”

- Parfois antagoniste (défiab !)
- Parfois collaborative
- Une frontière perméable

Au service d’un objectif commun:

- La disponibilité !
- Demande d’apprivoiser le temps



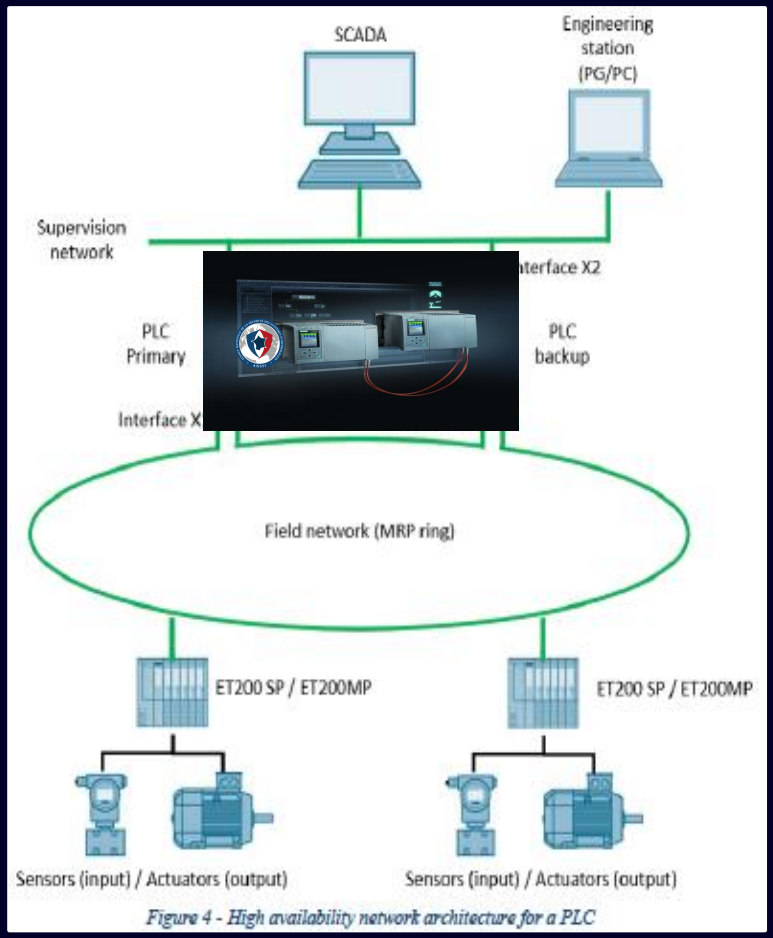


Figure 4 - High availability network architecture for a PLC

SIEMENS

ProductCERT SIEMENS: un process IH & VH dédié à nos produits… mais pas que !

La publication de vulnérabilités: une communication nécessaire

- Il n'est pas inné de dévoiler ses vulnérabilités et d'afficher ses faiblesses

ubuntu®

Adobe

Microsoft

- Le traitement de ces vulnérabilités, dans ses produits mais aussi dans les COTS embarqués… impose un travail de coopération, donc de communication (maîtrisée: prise de conscience et anticipation !!!)…et de confiance !

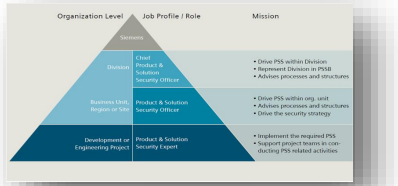
- De plus, nous ne pouvons faire confiance à celui qui est invulnérable…

…car il ment !

SIEMENS

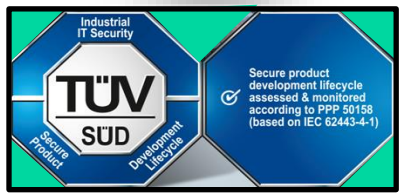
La cyber chez Siemens, c'est… un partenaire de confiance!

Siemens a su faire évoluer son organisation en fonction des enjeux de la cybersécurité des systèmes industriels: Product and Solution Security office



Siemens 1er industriel disposant en France d'un commutateur certifié (XM-400) et d'une gamme complète d'automates qualifiés par l'ANSSI (S7-1500) incluant les dernières CPU redondantes

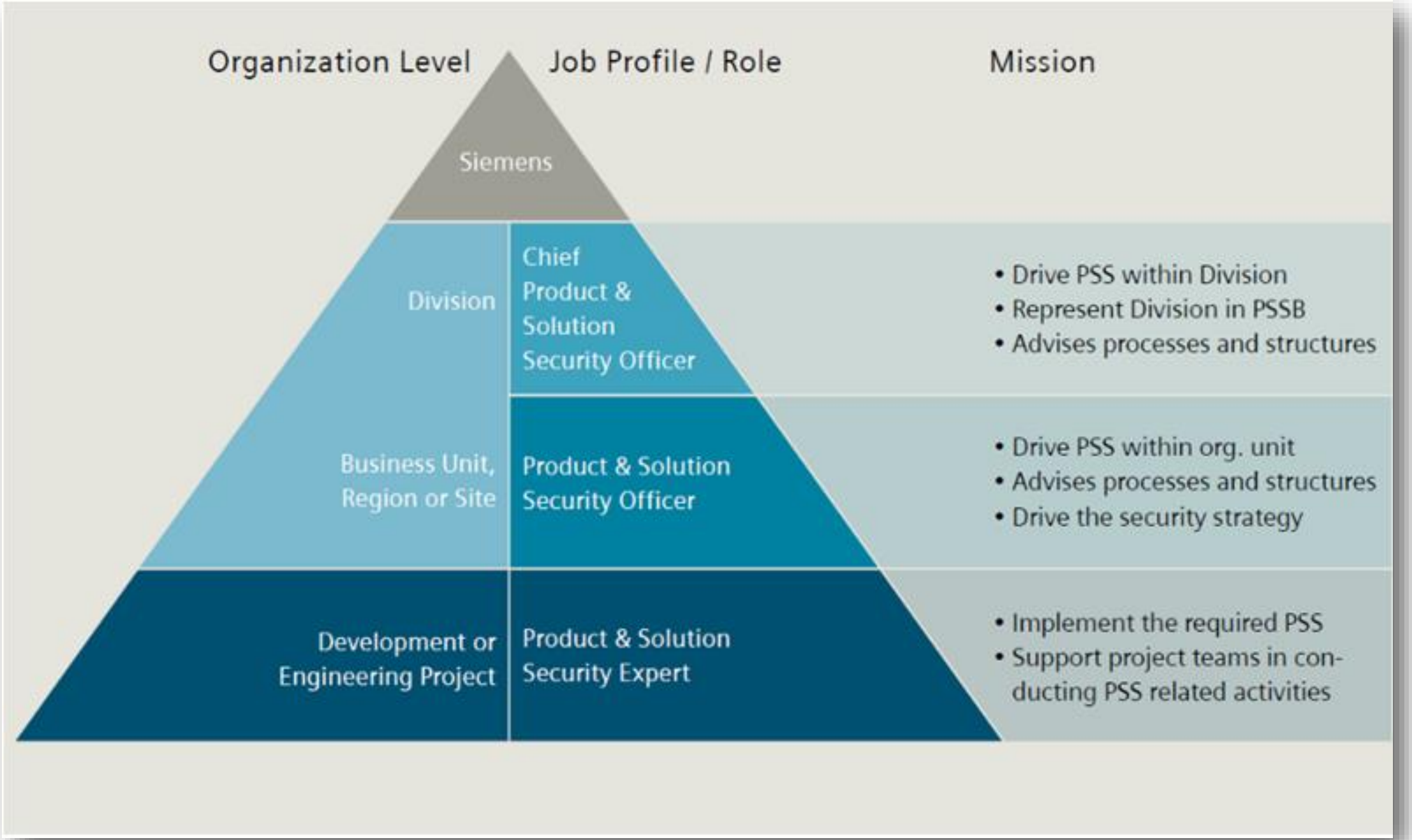
Siemens 1er industriel dont l'intégration de la sécurité dans les phases du cycle de vie du développement des produits est certifié sur la base de la norme internationale IEC 62443



Siemens vous accompagne dans la sécurisation de vos systèmes industriels au travers de services personnalisés

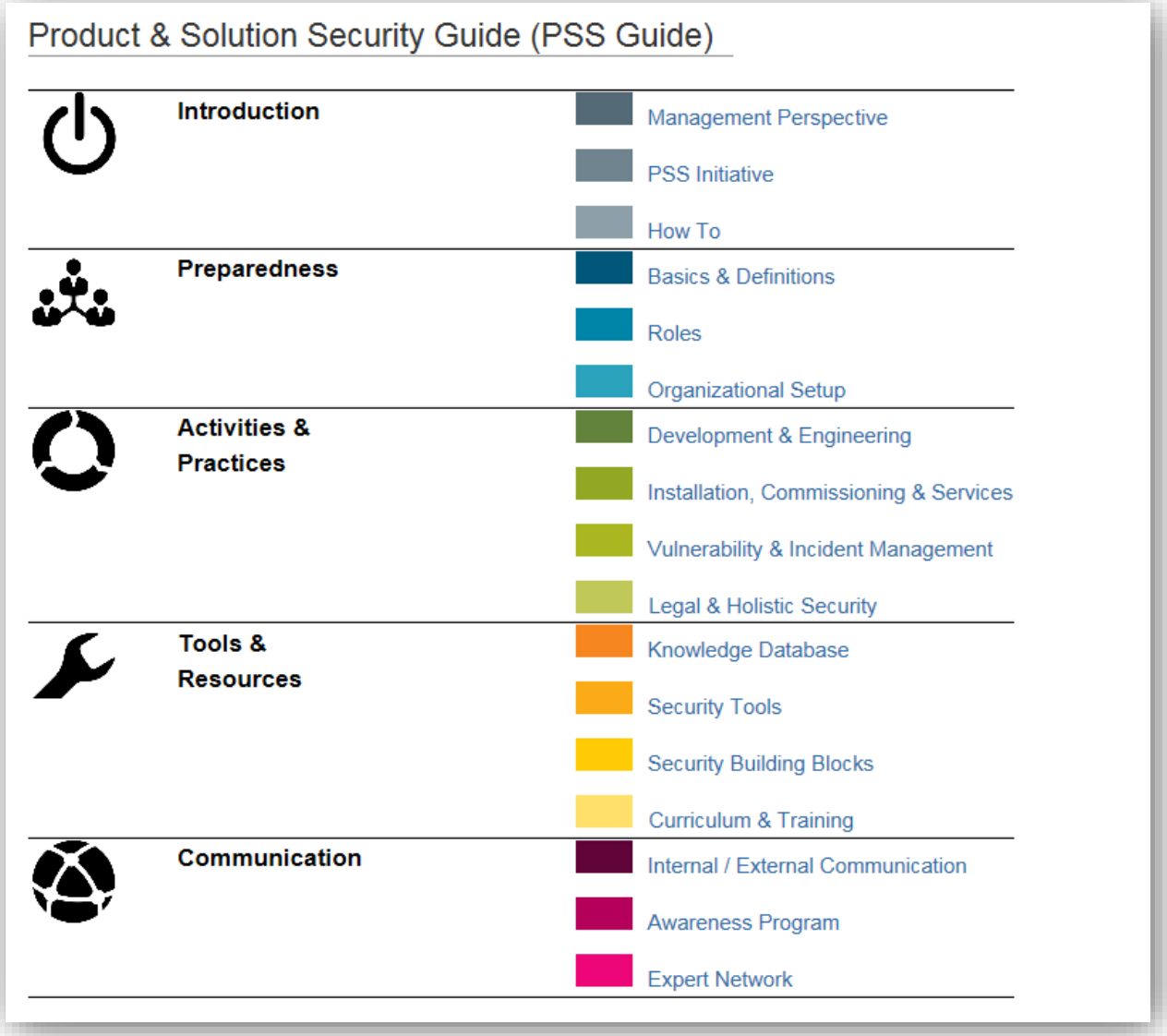
SIEMENS

Une organisation PSS cyber dédiée



Sécurité industrielle
Une organisation pour gérer tous les aspects de la sécurité industrielle

Un guide de référence pour l'ensemble des divisions



Certifications : Achilles (Wurldtech)
1er équipementier avec la certification Achilles Niv 2 depuis 2012

CPU certifiées

LOGO!

S7- 300 PN/DP

S7- 400 PN/DP

S7- 1500 PN/DP

S7- 1200

S7- 400 HF CPU V6.0

S7- 410-5H

CPs certifiés

CP343-1 Advanced

CP443-1 Advanced

CP1543-1

CP1628

Station DP certifiées

ET200 PN/DP CPUs

Pare-feu certifiés

SCALANCE S602, S612, S623, S627-2M

+ Protection contre les attaques DoS

+ Comportement défini en cas d'attaque

- **Disponibilité accrue**
- **Protection de la pile IP**

ProductCERT : Computer Emergency Response Team
Un CERT dédié aux produits

SIEMENS
Ingenuity for life

Contact | Global | English

Products & Services | Market-specific Solutions | Company

Search for ...

Products & Services > Services > CERT Services

Siemens ProductCERT and Siemens CERT

The central expert teams for immediate

SIEMENS

Search Security Advisories

Subscribe to Security Advisories

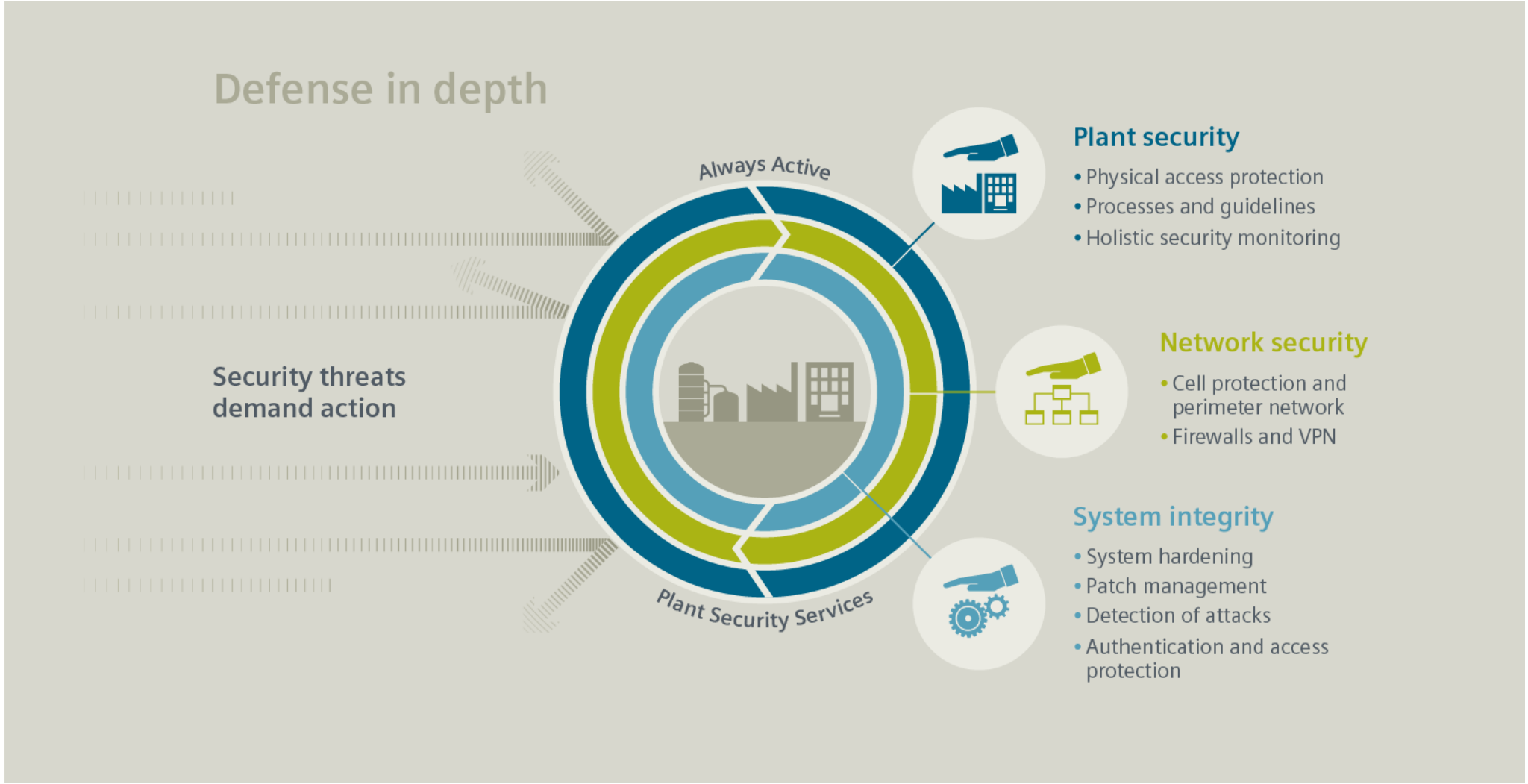
Search (SSA-ID, CVE-ID, Title, Products, Sector, Tags)

Filter by Date | Reset

ID	CVSS Score	Document Title	Info	Version	Last Update	Download
SSA-100232	8.6	Denial-of-Service vulnerability in SCALANCE X switches		V1.0	2019-08-13	PDF TXT
SSA-121293	7.2	Code Upload Vulnerability in SIMATIC WinCC and SIMATIC PCS 7		V1.1	2019-08-13	PDF TXT
SSA-232418	5.3	Vulnerabilities in SIMATIC S7-1200 and SIMATIC S7-1500 CPU families		V1.0	2019-08-13	PDF TXT
SSA-530931	7.5	Denial-of-Service in Webserver of Industrial Products		V1.0	2019-08-13	PDF TXT
SSA-616472	6.5	ZombieLoad and Microarchitectural Data Sampling Vulnerabilities in Industrial Products		V1.1	2019-08-13	PDF TXT
SSA-671286	6.6	Multiple Vulnerabilities in SCALANCE Products		V1.0	2019-08-13	PDF TXT
SSA-697412	9.1	Multiple Vulnerabilities in SIMATIC WinCC, SIMATIC WinCC Runtime, SIMATIC PCS 7, SIMATIC TIA Portal		V1.2	2019-08-13	PDF TXT

Suivez-nous sur Twitter ou via notre flux RSS

Sécurité industrielle
La défense en profondeur (Holistic Security Concept)



Des process de fabrication des produits sécurisés… eux-mêmes sécurisés et certifiés !

1er constructeur certifié sur la base de l'IEC 62443-4-1

Près de 30 sites de développement certifiés sur la base de l' IEC 62443-4-1

pcs 7 1er SNCC certifié IEC 62443-3-3 / IEC 62443-4-1

1ere solution de sous-station électrique certifiée IEC 62443-3-3 / IEC 62443-4-1

Et bien d'autres (WinCC OA…) !

SIEMENS

Certification de Sécurité de Premier Niveau (CSPN)
Printemps 2016 – les deux 1er lauréats des systèmes industriels

Simatic S7-1518

Certifié et Qualifié (Avril 2016)

Scalance XM400

Certifié (Juin 2016)

Recommandation d'achat par l'état
SIMATIC S7-1500; Une gamme complète qualifiée

Famille Simatic S7-1500

Une vingtaine de référence qualifiées depuis 2017 et le maintien en qualification décroché auprès de l'ANSSI début mai 2019 (encore une première !)

Seule la qualification vaut recommandation à l'achat par l'ANSSI pour les administrations et les opérateurs d'importance vitale OIV dont ils ont en charge la protection

Des services personnalisés pour vous accompagner à sécuriser vos installations

SIEMENS
Ingenuity for life*

Au service de la sécurisation de vos installations

Evaluation de la sécurité

Evaluation du statut de sécurité actuel d'un environnement industriel

- Check de la sécurité Industrielle
- Evaluation IEC 62443
- Evaluation ISO 27001
- Evaluation des Risques & Vulnérabilités
- Consulting sur la Sécurité Industrielle
- Scanning Services
- Cartographie de l'architecture industrielle
- Classification

Implémentation de la sécurité

Diminution des risques à travers l'implémentation de mesures de sécurité

- Formations et sensibilisation à la Cybersécurité des Systèmes Industriels
- Pare Feux Nouvelle Génération
- Liste Blanche
- Anti Virus
- Sauvegarde et Restauration
- Station de décontamination et blocage applicatif des ports USB

Gestion de la sécurité

Une sécurité complète à travers des services de gestion

- Détection des anomalies
- Supervision de la Sécurité Industrielle
- Gestion des Incidents à distance
- Gestion des Vulnérabilités Industrielles
- Gestion des Patchs
- Package de services pour la sécurité des SIMATIC