



Ineo Cyber Sécurité
Notre énergie au service de votre sécurité

Space's Industrial Control Systems Security 3rd Edition

CyberCheck

comment évaluer rapidement le niveau de sécurité de mes sites industriels ?

02 décembre 2019



Ineo Cyber Sécurité au cœur des 24 BUs ENGIE



160 000 collaborateurs | 5 continents | 61 Mds € de CA

BUs France

Elengy
Storengy
Grdf
GRTgaz
France BtoC
France Réseau
France Energies Renouvelables

France BtoB

BUs Europe

BUs Internationales

BUs Globales

49%

Conception, installation
et maintenance



51%

Services
énergétiques



42 500
collaborateurs
1^{er} recruteur d'ENGIE



7,7
milliards d'euros
de CA fin 2018



900
implantations
locales

4 ENTITÉS

ENGIE Axima

ENGIE Cofely

ENGIE Ineo

ENDEL ENGIE



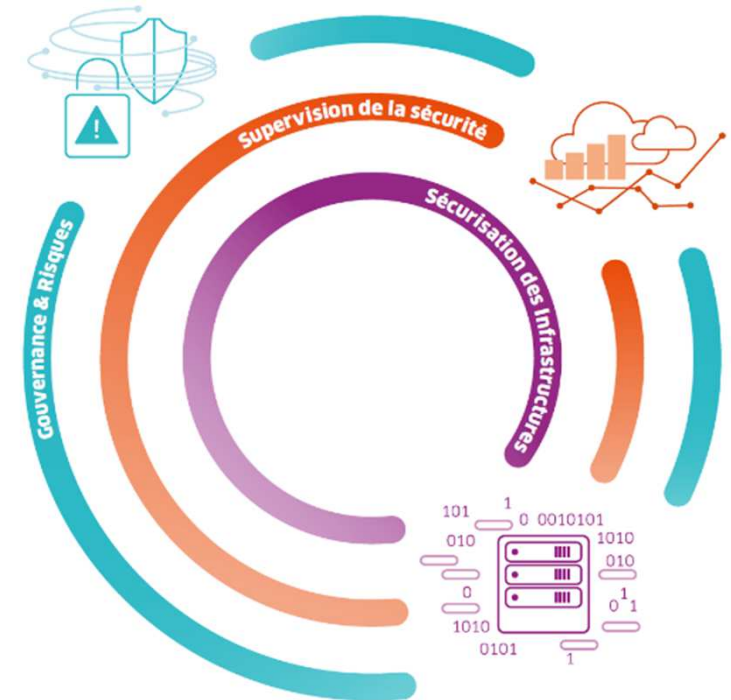
Ineo Cyber Sécurité

Qui sommes-nous ?

- ✗ Le centre de compétences Cyber de la BU France BtoB d'ENGIE
- ✗ Une équipe de 20 ingénieurs et experts
- ✗ PASSI (qualification ANSSI en cours)

Que proposons-nous ?

- ✗ Une démarche globale de la sécurité des systèmes d'information
- ✗ Une intervention sur l'ensemble de la chaîne de valeur :
 - ✗ Gouvernance & Risque
 - ✗ Supervision de la Sécurité
 - ✗ Sécurisation des Infrastructures



Les compétences Ineo Cyber Sécurité

GOVERNANCE & RISQUES

- ✕ Analyse et suivi des risques
- ✕ Organisation de la sécurité
- ✕ Conseil et accompagnement
- ✕ Conseil pour la prise en compte réglementaire (PDIS, I1901, LPM, PSSI-E...)
- ✕ Audit et contrôle
- ✕ Sensibilisation
- ✕ Homologation

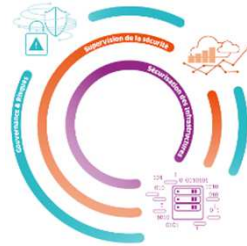
SUPERVISION DE LA SÉCURITÉ

- ✕ Mise en place d'un service SOC externe Cyberprotect
- ✕ Définition du périmètre métier à placer sous surveillance
- ✕ Accompagnement dans la définition des événements à collecter
- ✕ Définition des processus pour la réponse à incidents
- ✕ Conseil et support IBM Resilient pour la réponse à incidents
- ✕ Maintien en Condition de Sécurité

SÉCURISATION DES INFRASTRUCTURES

- ✕ Conception d'architecture sécurisée (infrastructures de transport, de télécommunications et d'énergie, smart building, smart city, ...)
- ✕ Étude comparative de produits de sécurité (IAM, pare feu, IDS, IPS, End Point Security, SIEM, ...)
- ✕ Déploiement de solution de sécurité (proxy, environnement durci, pare feu, protection des données, SIEM, ...)

Nos Offres Packagées



Services

- 01. Analyse et suivi des risques
- 02. Audits
 - SSI Industriels *CyberCheck / Security Expedition* **sentryo**
 - SSI IT *Audit de Configuration, Pentests, etc.*
- 03. Homologation
 - Développement / process réseau de DR et DR SF
 - Dossier d'homologation
- 04. CISO as a Service
- 05. Accompagnement SSI Projet



Solutions

- 06. SOC externe Cyberprotect
- 07. Campagnes de Phishing by Cyberprotect
- 08. MCS – Maintien en Condition de Sécurité
- 09. Antivirus / EDR
- 10. IBM Resilient IBM Security
- 11.

Gouvernance & Sécurisation des Annuaire (AD)

Ineo Cyber Sécurité

Exemples de projets 2018 - 2019



PZVP RSSI – RSI - Homologation SIIV
Ineo Digital



Préfecture de police

La préfecture de police, au service du public de l'agglomération parisienne

Groupe Casino – Accompagnement à la mise en place de PingCastle Enterprise dans un environnement multi-domaines, sécurisation et gouvernance de l'AD



Ministère des Armées – Dossier d'Homologation, MCS,
Accompagnement SSI
Ineo Atlantique, Ineo Centre & Ineo Défense

- **DGA** – Direction Générale de l'Armement

- **SID** - Service d'Infrastructure de la Défense



Ineo Cyber Sécurité

Présence aux événements

#SMARTINDUSTRIES2018

Partager Tweet



SMART INDUSTRIES, UN ÉVÉNEMENT UNIQUE DÉDIÉ À L'USINE DU FUTUR



les assises

de la sécurité et des systèmes d'information

✕ Évènements Groupe ENGIE

- **Cyber Security Days** du 23 au 25 Septembre 2019
- **Salon Smart Industries** du 27 au 30 mars 2018 à Villepinte Fortissimo Industrie du Futur
- **Innovations Camp Ineo** en régions

✕ Évènements majeurs de la Cybersécurité

- **FIC 2018**
 - Retex d'audits de sécurité de SI Industriels sur le modèle 3S : Sensibiliser, Sécuriser, Superviser
- **Les Assises 2019**
 - Atelier 2019 : REX "Sécurisation de l'AD avec PingCastle dans un environnement multi-domaines" le jeudi 10/10/19 à 17h.
 - Participation aux événements networking en amont de l'évènement
 - Le Cercle de la SSI

SOMMAIRE

Partie 1

Rappel sur les principales questions de sécurité ICS

Partie 2

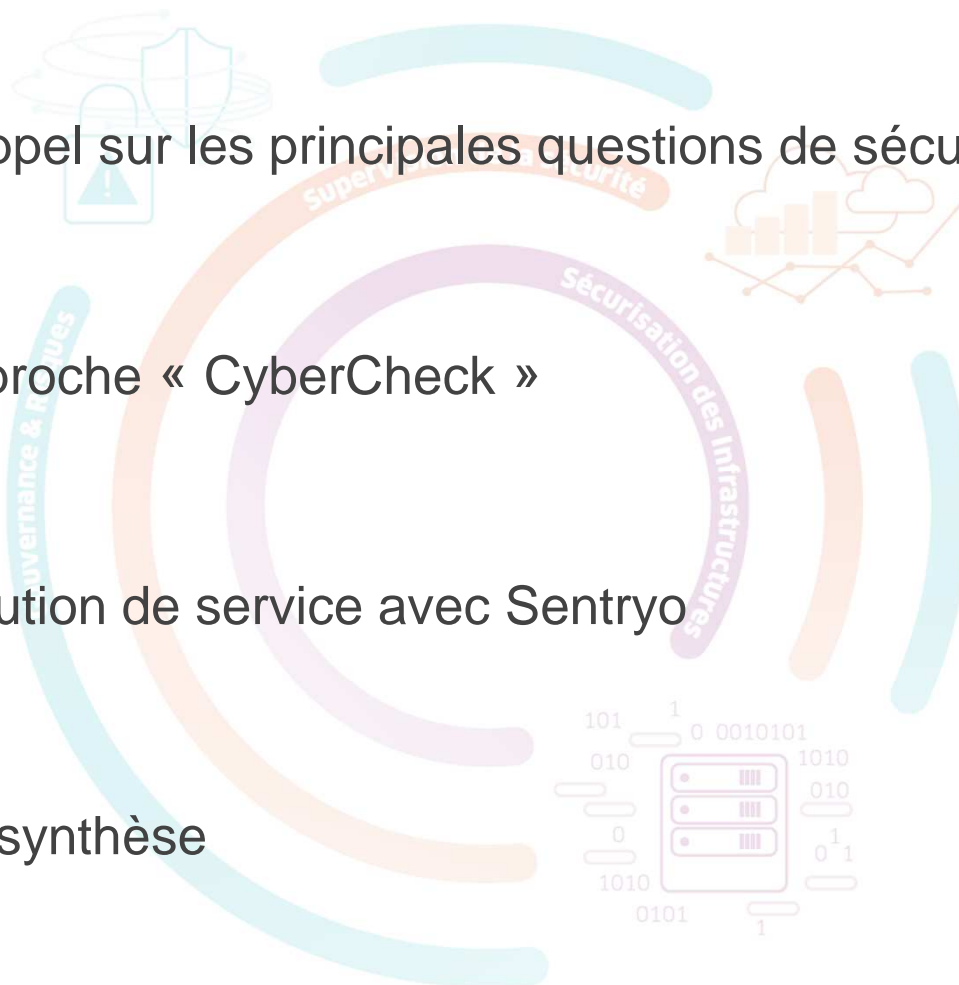
Approche « CyberCheck »

Partie 3

Solution de service avec Sentryo

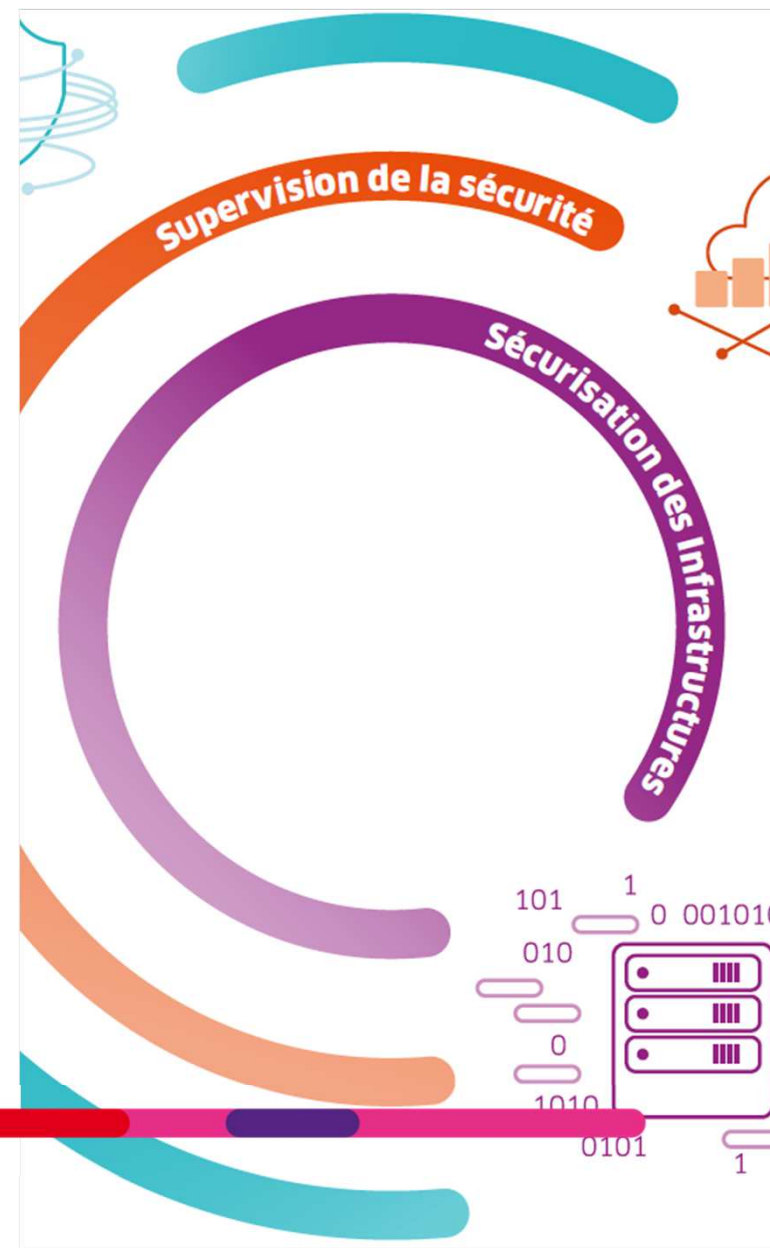
Partie 4

En synthèse

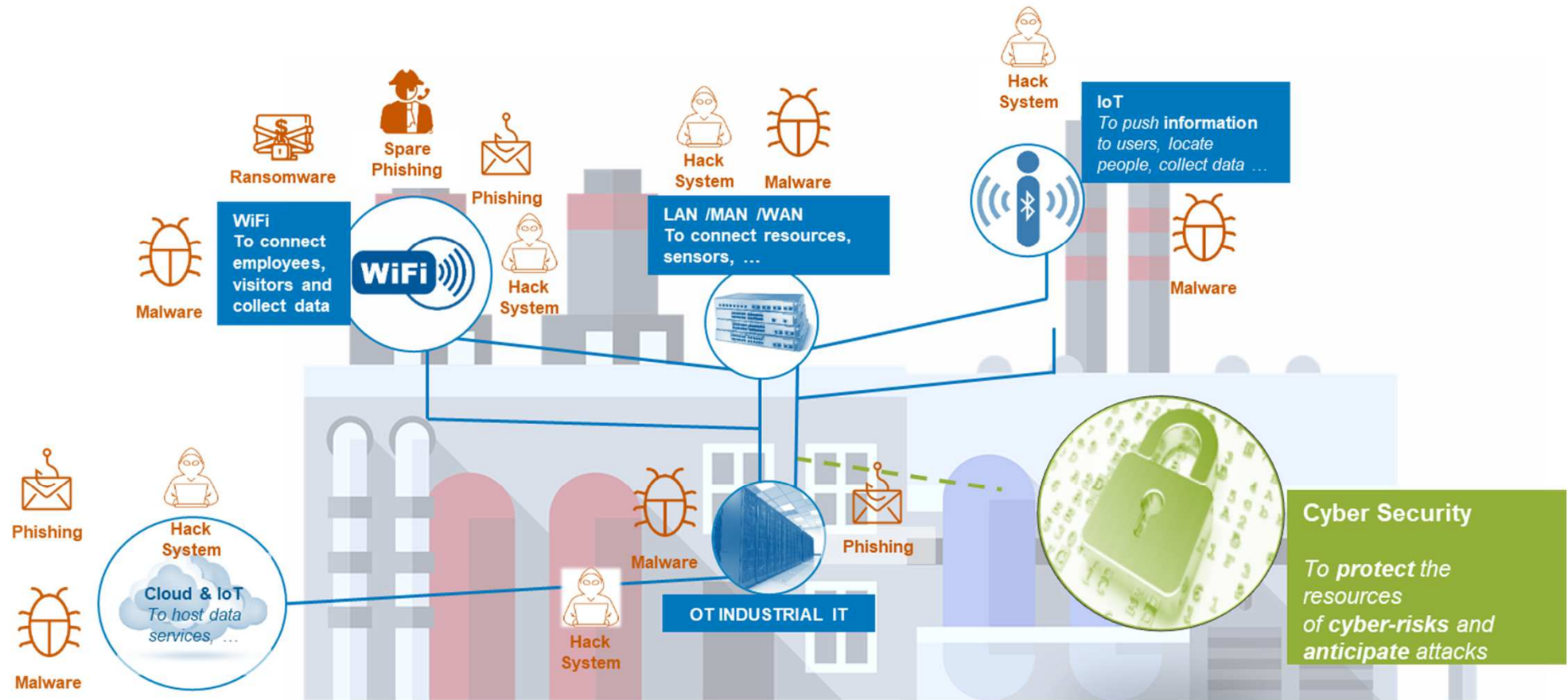


01

Rappel sur les principales questions de sécurité ICS

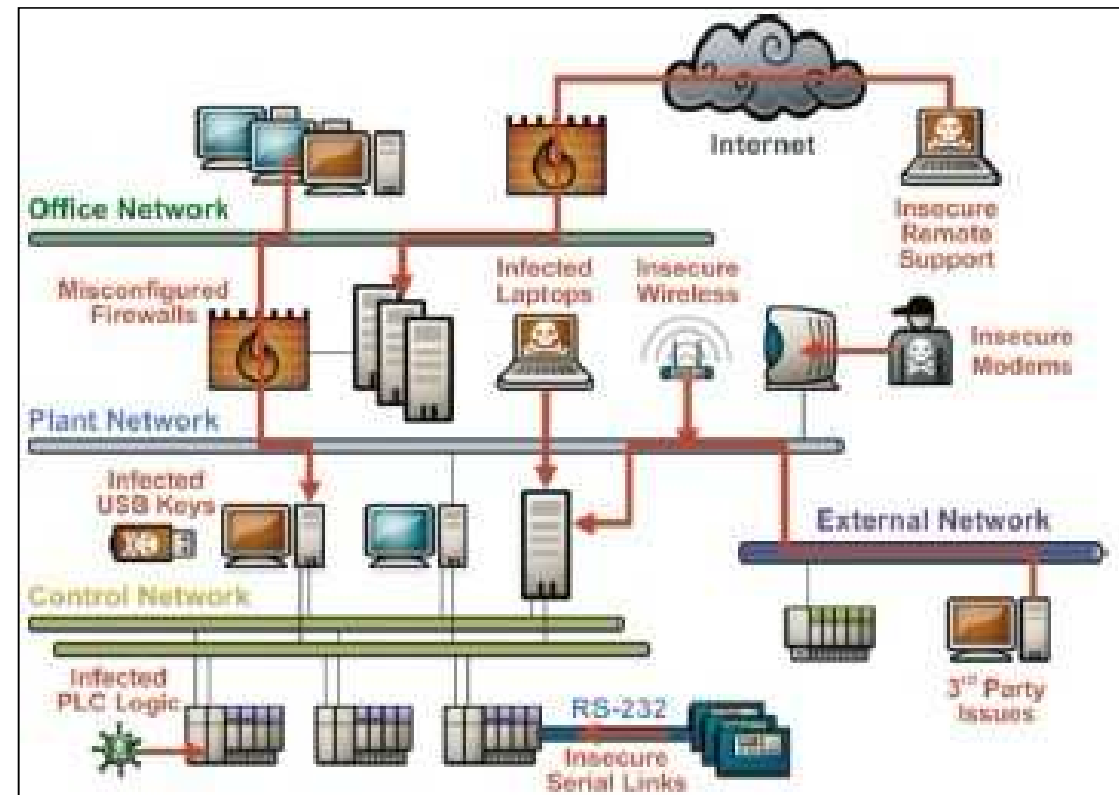


« Vulnerability by Design », le concept



Qu'est-ce que le "Vulnerability by Design"?

- › Les SI industriels ne sont pas sécurisés par défaut et sont donc plus vulnérables que les SI de gestion.
- › **Risque accru d'attaque en raison du besoin d'interconnexion des réseaux (industrie 4.0)**
- › Le SI industriel est devenu de plus en plus communicatif, ce qui augmente le risque d'exposition des équipements aux attaques.



Les 5 principaux facteurs d'attaque



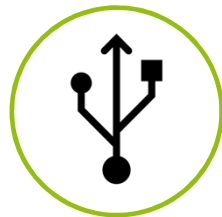
Réseaux



Equipements
sur site



Cloud /
Data Center



Clé USB



BYOD

Cas externe – WannaCry : Attaque Virale (Renault 2017)

Motivation des attaquants :

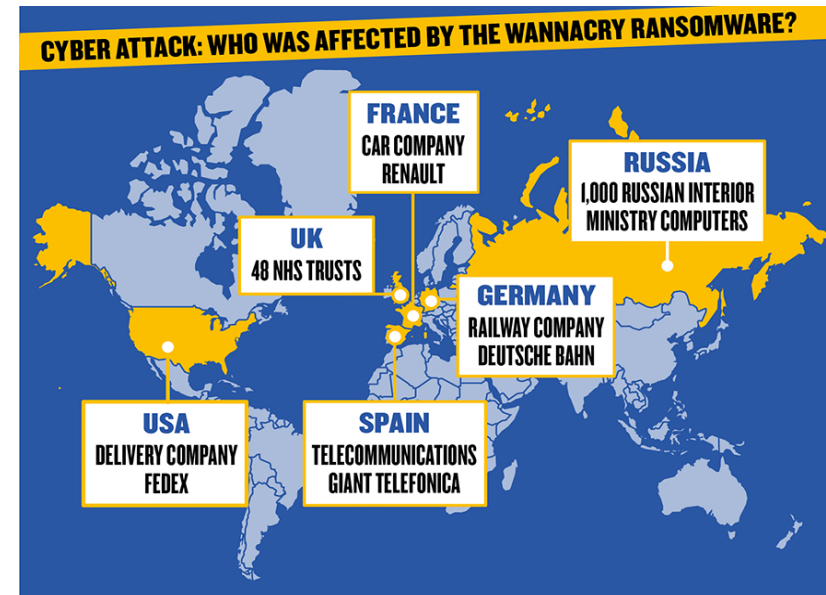
- › Déstabilisation

Vulnérabilités :

- › OS (Operating System) Windows non à jour
- › Manque de Maintien en Condition de Sécurité

Effets / impacts:

- › Blocage des ordinateurs et serveurs de l'entreprise
- › Chute massive de la production sur les sites manufacturiers

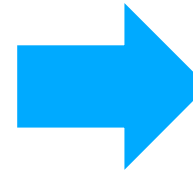


Cas d'usage – Infection SCADA par “SMB Double Pulsar”



Vulnérabilités :

- RETEX d'une réponse à incident pour SIEMENS ICS
- › Poste de travail sous la responsabilité de SIEMENS
- › Seul SIEMENS est capable de d'effectuer des actions correctives sur les machines SIEMENS
- › SIEMENS approuve seulement les solutions de sécurité spécifique
- › Faible capacité de sécurité pour SIEMENS



**3 mois pour nettoyer
les postes de travail ICS**

Remise en état :

Dernières Actions	Résultat
SIEMENS a installé Trend Micro Antivirus (solution autorisé) et performé le full SCAN SIEMENS a corrigé les OS contre la vulnérabilité à double pulsar MS17-010	Pas de malware trouvé par Trend Micro Antivirus
Surveillance GSOC de l'appareil SIEMENS	Plusieurs machines avec Symantec AV signalent toujours des attaques de SIEMENS Machine.
Le client a installé solution AV et effectue un scan complet de la machine SIEMENS.	Virus trouvé et éradiqué

Cas d'usage – Infection Système Industriel par StuxNet

Vers informatique découvert en 2010

- › APT ayant pour but de reprogrammer les API
- › Camouffle les actions exécutés
- › Déstabilisation de la production lié aux centrifugeuses Iraniennes

Points d'entrées

- › Utilise 4 Zero Day dans Windows
- › Vise les systèmes SCADA
- › Utilise des mots de passes par défaut présent dans les logiciels

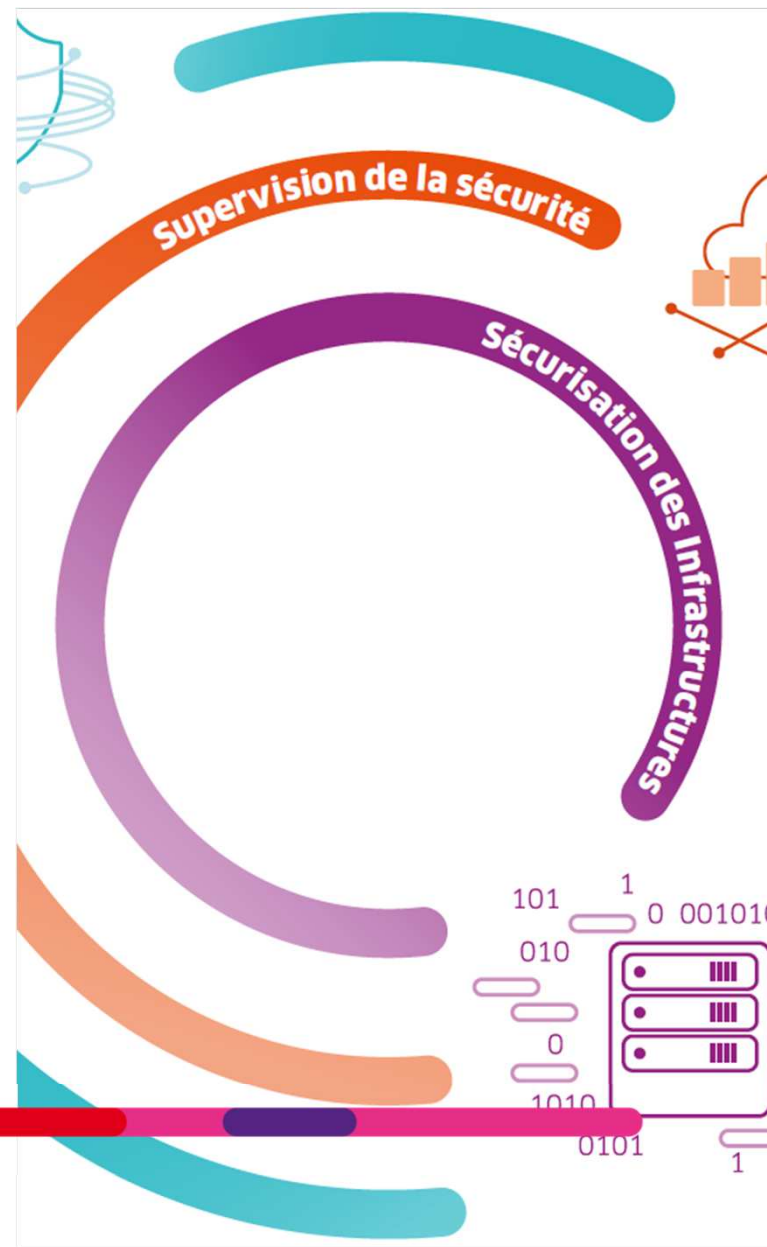
Le programme nucléaire iranien

-  Centrale nucléaire
-  Centrale en construction
-  Réacteur de recherche
-  Site d'enrichissement d'uranium
-  Yellowcake
-  Mine d'uranium



02

Approche CyberCheck



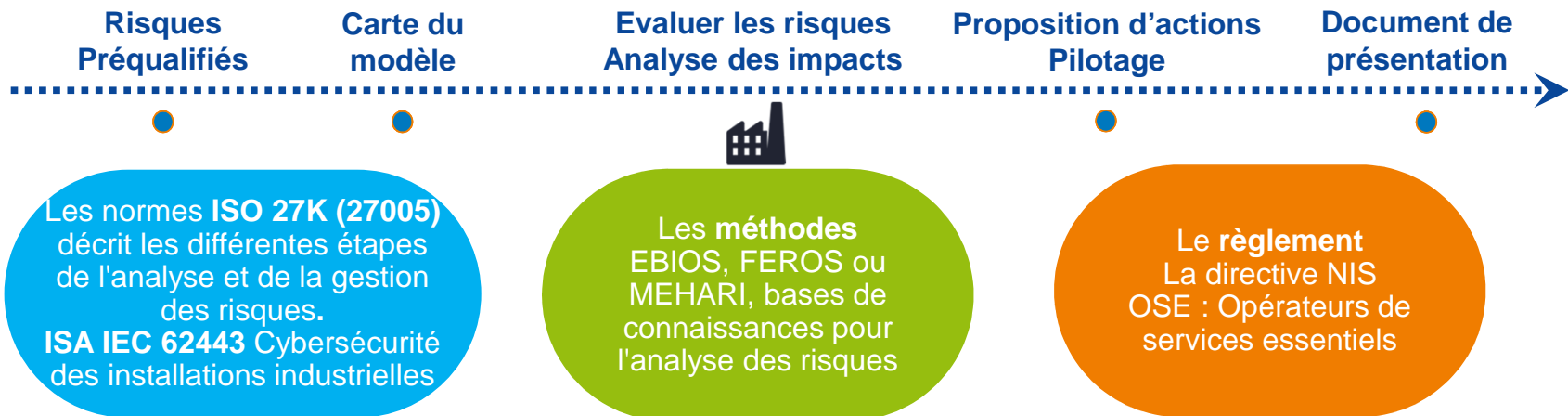
Quelle approche pour gérer les risques ?

Evaluation régulière à 360° de la maturité des sites

Évaluation des **risques** et de
l'impact des actifs



Conformité au Règlement PSSI
/ Cote et recommandations



“Security Expedition”, la genèse : 2017

Demande client :



- **Évaluer** le niveau de sécurité pour tous les sites industriels gérés par Engie.

- Action :

- › **Audit de la sécurité** pour s'assurer que le site est bien protégé s'il est accessible de l'extérieur (par Internet) - la réalisation de tests d'intrusion.
- › **Une « Security Expedition" par site** pour valider si l'architecture ICS respecte les standards ENGIE (Framework ICS 2.0)



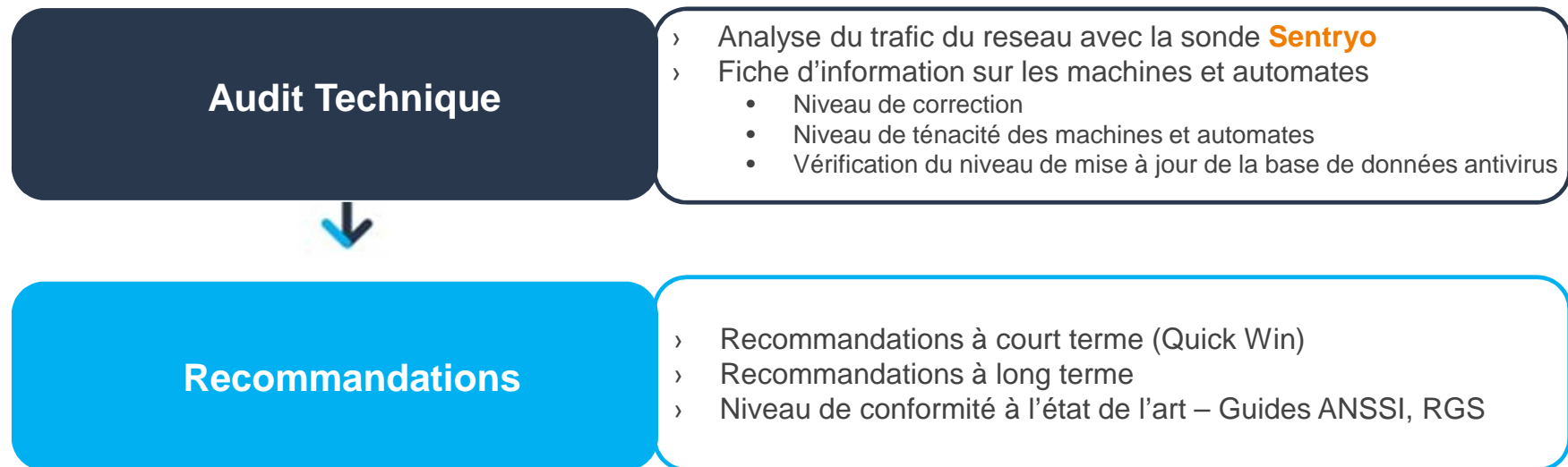
7 sites dans ce périmètre

- › 2 en France
- › 4 en Italie
- › 1 en Allemagne

Qu'est-ce que l'offre "CyberCheck"?

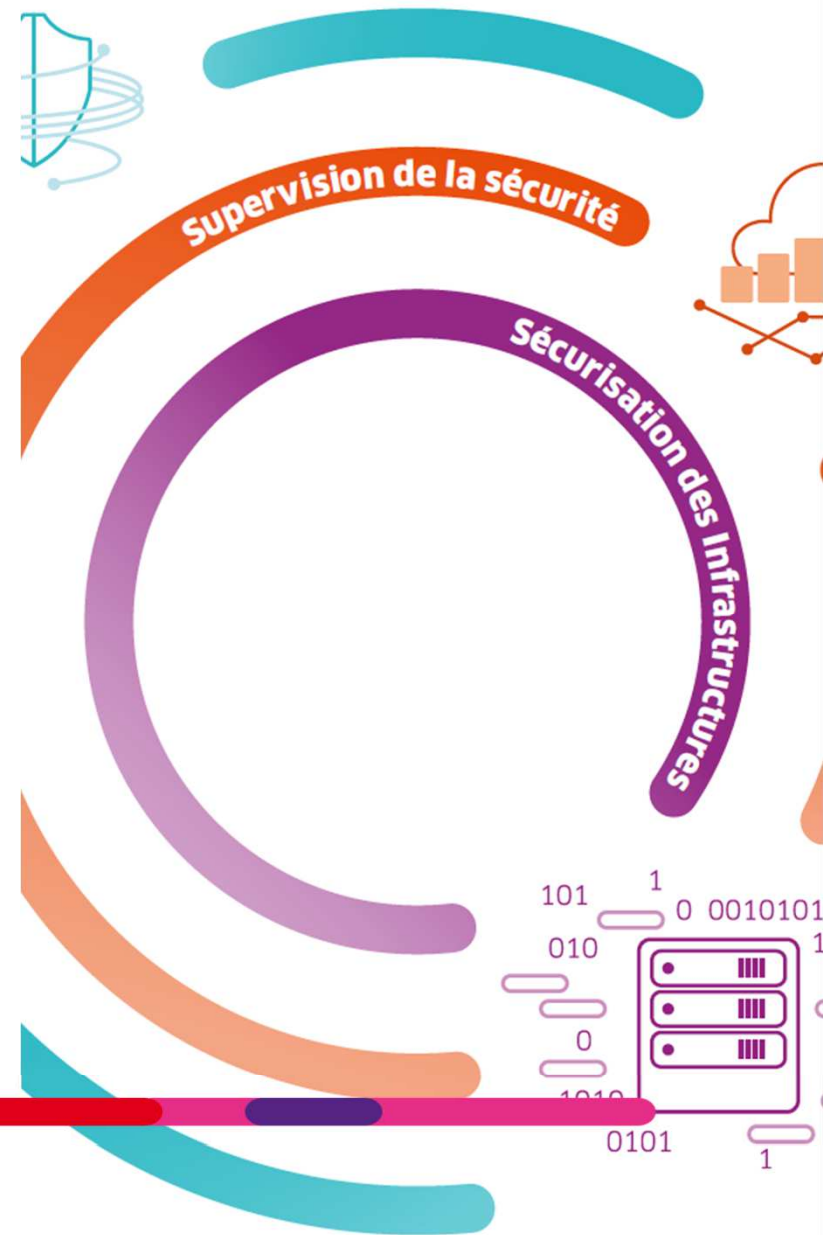
Approche basée sur :

- › Des audits de configurations
- › Une analyse du trafic des réseaux industriels via la sonde **Sentryo**.



03

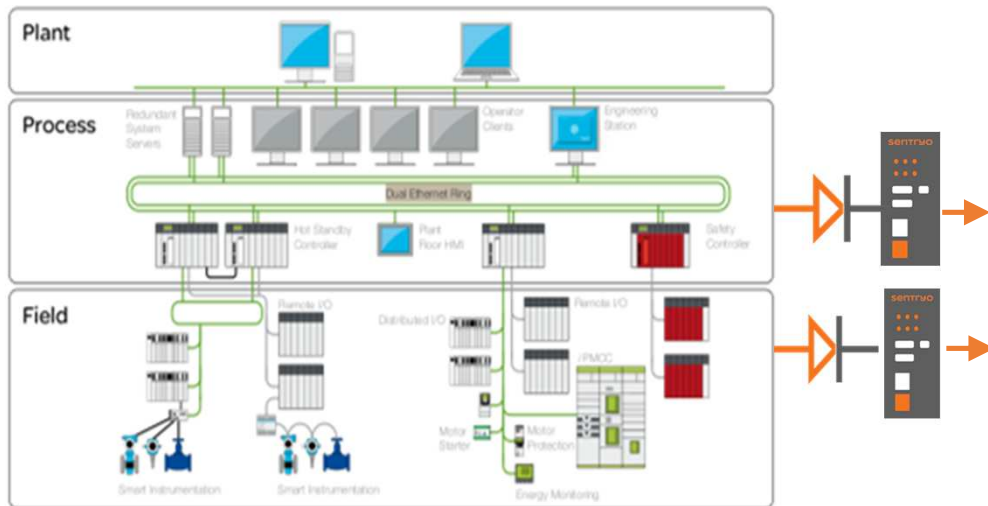
Solution de service Sentryo



Comment Sentryo « ICS CyberVision » fonctionne ?

1

Des sondes 100% passives analysent les protocoles industriels pour extraire les métadonnées (DPI - Deep Packet Inspection)



COLLECTER

■ Inventaire

- Composants, Modules
- Firmware

■ Réseau

- Metadata
- Statistiques

■ Contrôle Process

- Messages système
- Programmes
- Clés de registre

Avantages : Stockage de toutes les données collectées dans la base de données du CyberVision Center

Comment Sentryo « ICS CyberVision » fonctionne ?

1

Des sondes 100% passives analysent les protocoles industriels pour extraire les métadonnées (DPI - Deep Packet Inspection)

Beaucoup de protocoles gérés

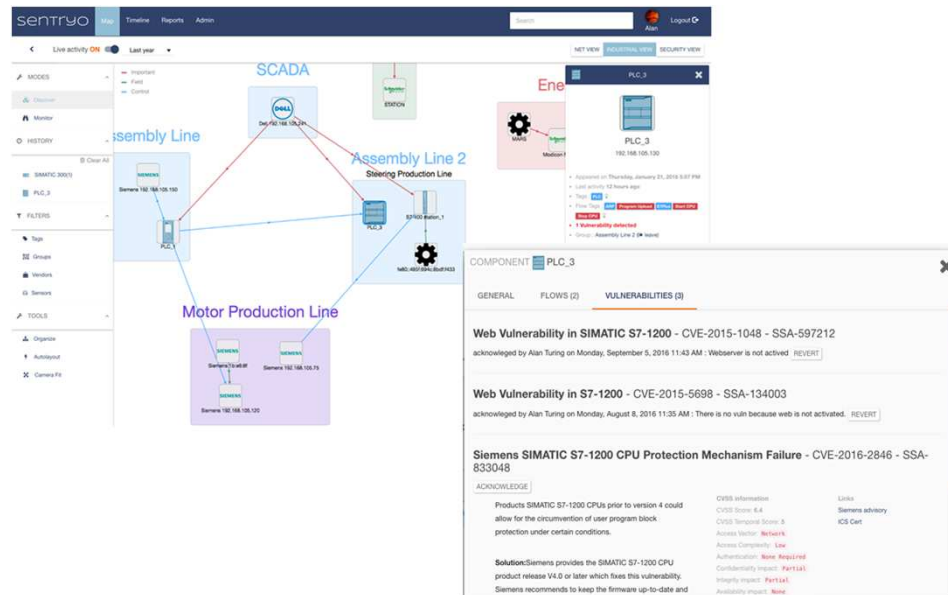
- **SIEMENS** (S7 / S7+ / Profinet)
- **SHEIDER ELECTRIC** (ModBus TCP / UNI-TE / UMAS / M580)
- **ROCKWELL** (Ethernet IP, CIP)
- **PHOENIX CONTACT** (Phoenix Contact)
- **CODESYS BASED** (Codesys protocol stack)
- **MITSUBISHI** (SLMP, CC-Link, Melsoft, RFTP)
- **OMRON** (FINS protocol)
- **FOXBORO** (DCS)
- **HONEYWELL** (Experion PKS / Safety Manager)
- **YOKOGAWA** (CENTUM VP)

- Et d'autres encore, comme **BACNET** et **Ethercat**

Comment Sentryo « ICS CyberVision » fonctionne ?

2

CyberVision Center combine les données collectées pour créer des comportements « réseau et process », les met en corrélation avec les flux de *Threat Intelligence* et interagit avec l'automaticien d'OT pour ajouter un contexte métier.

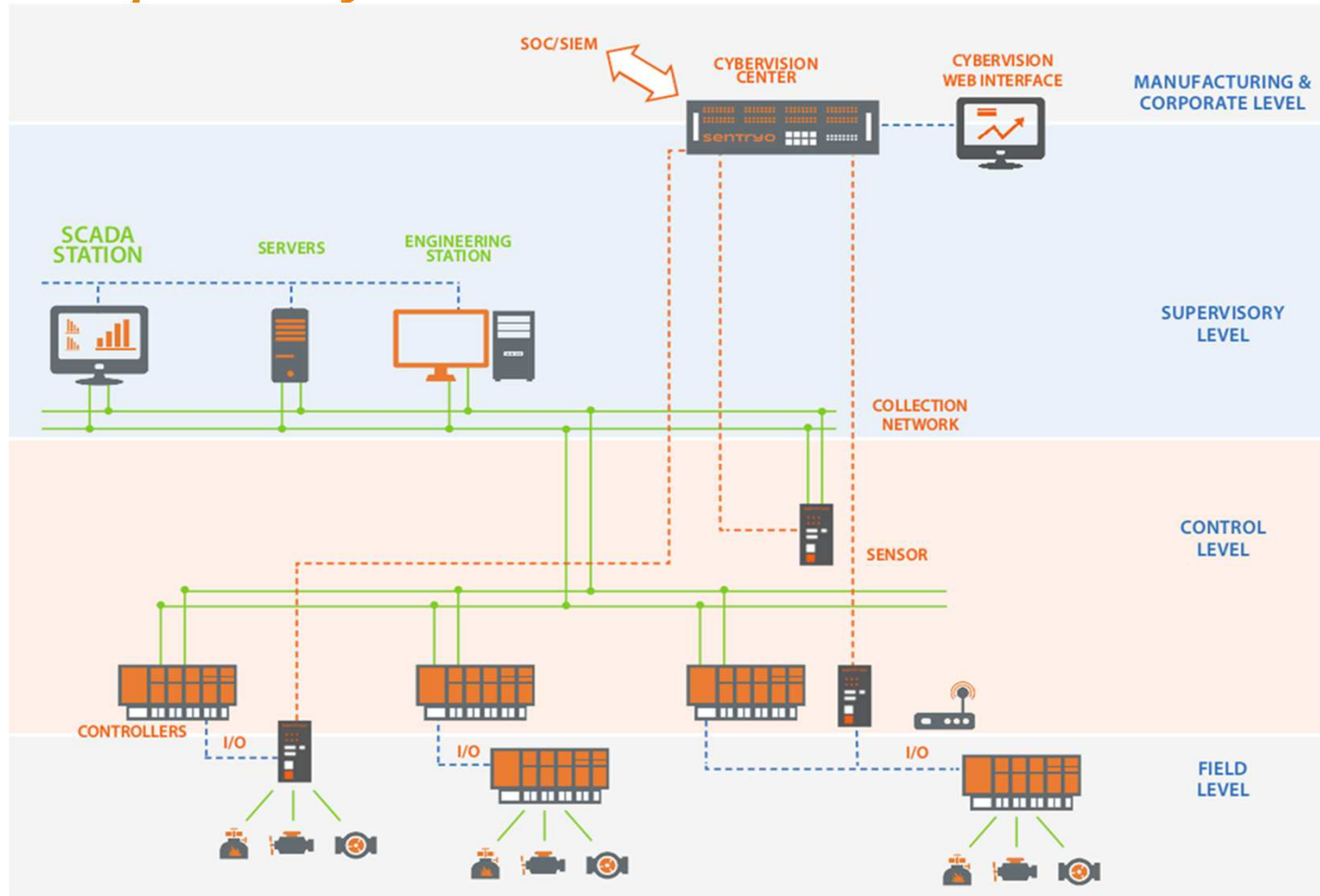


CARTOGRAPHIE

- Inventaire dynamique des équipements
- Carte des flux
- Gestion de la vulnérabilité

Avantages : Fournir une connaissance détaillée de la situation et outiller les équipes techniques pour réduire la surface d'attaque

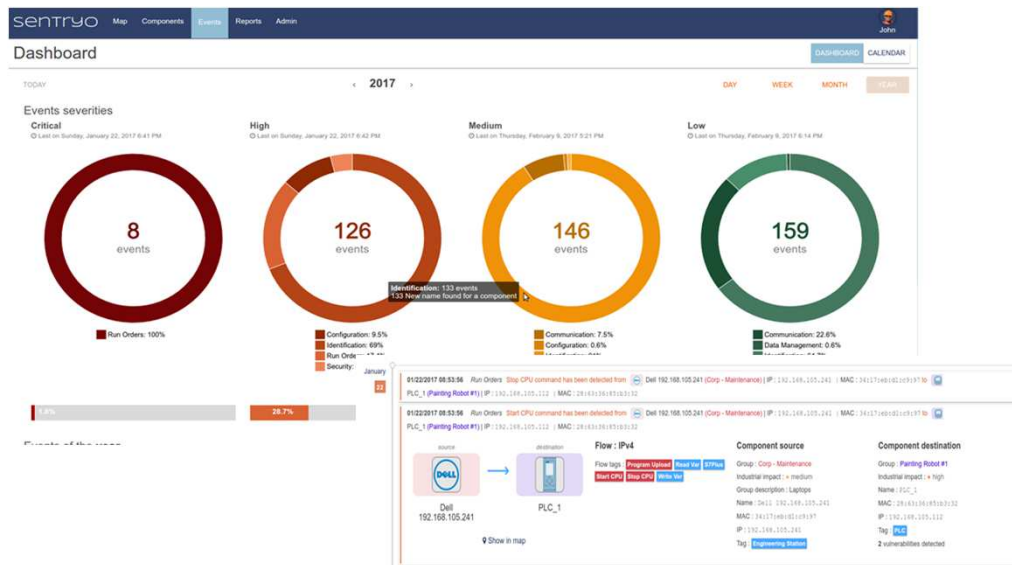
Architecture basique Sentryo



Comment Sentryo « ICS CyberVision » fonctionne ?

3

Les événements sont générés et enregistrés dans une base de données, puis contextualisés et présentés dans une vue détaillée. Les ingénieurs OT contrôlent la configuration de l'équipement et les événements clés à l'aide d'un tableau de bord.



CONTROLLER

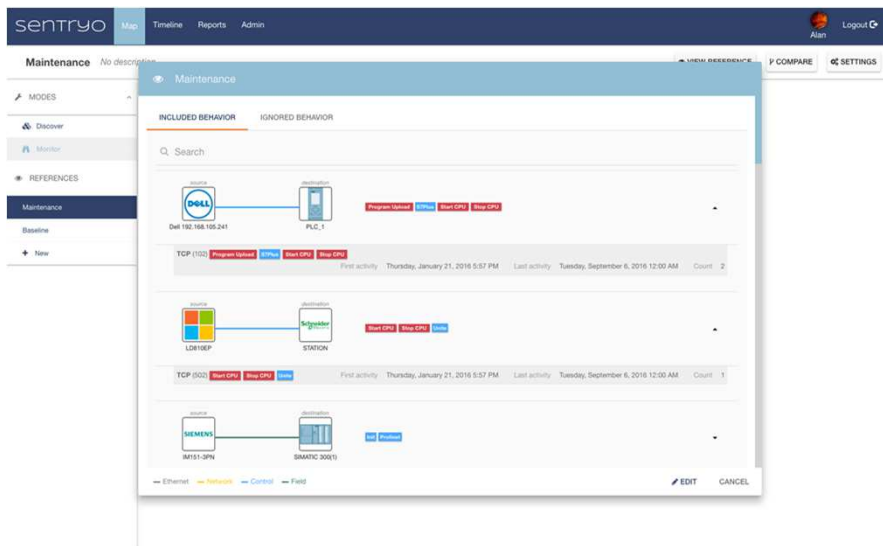
- Niveau de gravité personnalisables
- Enregistrement automatique des événements
- Tableaux de bord

Avantages : maintenir l'intégrité des systèmes industriels avec un effectif réduit

Comment Sentryo « ICS CyberVision » fonctionne ?

4

Les ingénieurs de contrôle créent des états de configuration à partir d'un ensemble de comportements. Les experts en cybersécurité ajoutent les comportements malveillants connus (IoC) via les API. ICS CyberVision utilise l'apprentissage automatique pour classer les comportements et améliorer continuellement la précision de détection.



ALERTER

- Surveiller les changements et détecter les anomalies
- Identifier les activités de piraterie
- Afficher les alertes dans une vue personnalisée

Avantages : Identifier les comportements malveillants et promouvoir la collaboration EO & IT

CyberCheck Sentryo : un 1er niveau de contrôle des actifs industriels

Sentryo a mis en place un laboratoire de recherche sur la cybersécurité industrielle pour fournir des informations précises sur les menaces. En exploitant ces flux, les partenaires et les clients sont en mesure de détecter les intrusions avant qu'elles n'aient causé de graves dommages.

Service client

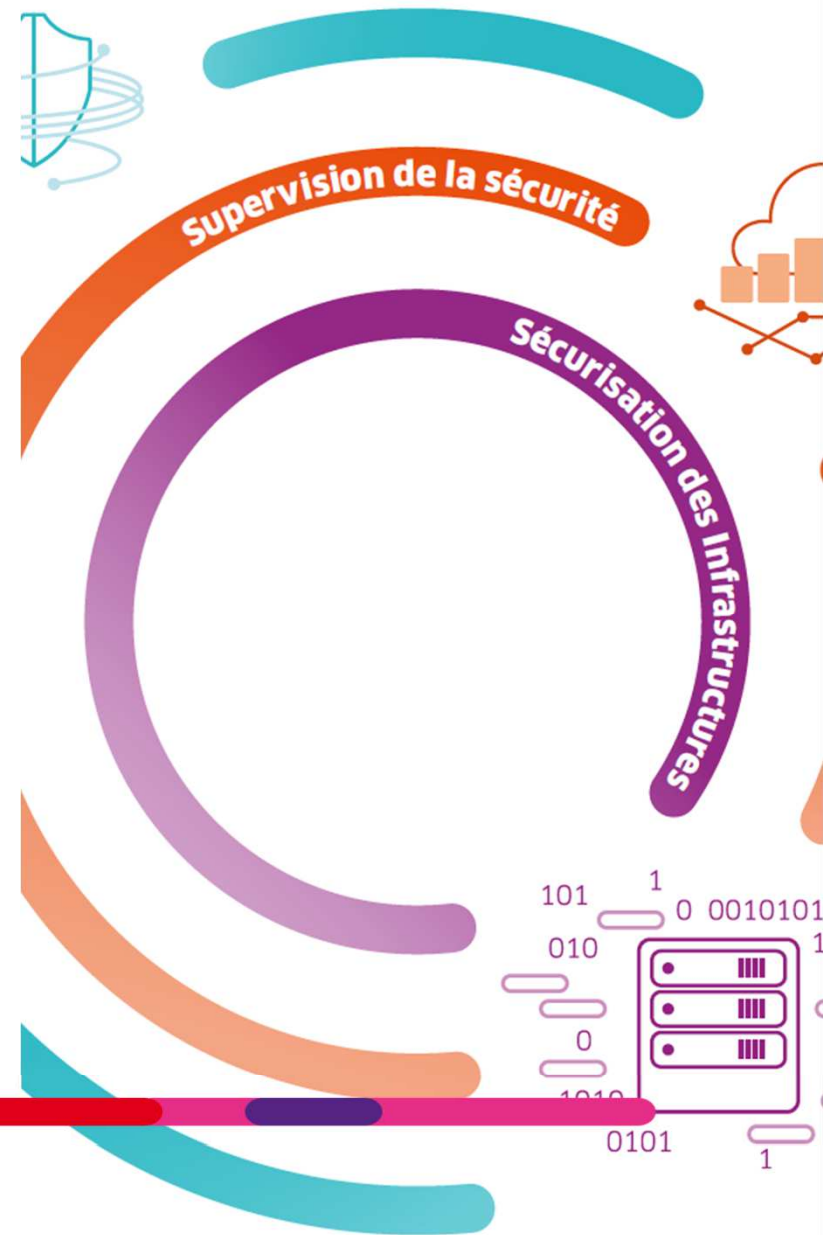
- Rapport de menaces (ex : Virus industriel tel que PLC Blaster)
- Analyse approfondie des attaques (ex : Stuxnet, Ukraine Power Plant)
- Base des vulnérabilités
- Indicateurs de compromis (ex : C2 IPs)
- Consignes de sécurité

Activité Laboratoire

- Co-publication avec ISA
- Surveillance et étude des menaces (analyse approfondie des attaques)
- Connexion avec les CERT Internationaux
- Participation à des conférences et publications sur la cybersécurité : IAEA, S4
- Projets de recherche (IoT, PLC stations)
- Conception d'un algorithme avancé de cyberdéfense

04

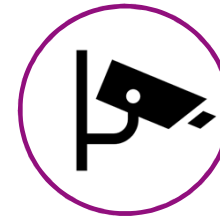
En synthèse



Ce que l'on retient de l'approche "CyberCheck" Ineo CS avec Sentryo



Coût maîtrisé

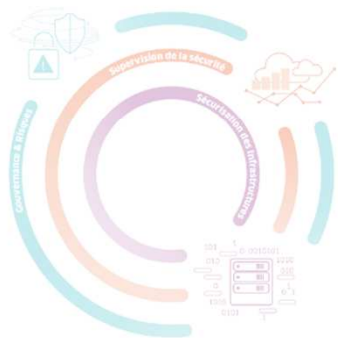


1^{er} niveau de
contrôle des actifs
industriels
(*cartographie*)



Rapport d'audit
clair

Ineo Cyber Sécurité



Notre énergie au service de votre sécurité
Confiez-nous la cybersécurité de votre activité et concentrez-vous sur votre cœur de métier



Francesco VIGLIANISI
Responsable Commercial
Ineo Cyber Sécurité
francesco.viglianisi@engie.com
Mob. +33 7 84 42 05 11

Siège : T1 Engie - 1 place Samuel Champlain
92930 Paris la Défense
Bureaux : Tour Ewater, 86 rue Henri Farman
92130 Issy-Les-Moulineaux
Email : contact.ineocybersecurite@engie.com

engie-ineo.fr