

WEBINAR

La cybersécurité en milieu industriel

Faire face
à un
contexte
tendu

Sensibiliser
tout le
monde !!!

Protéger
son SI des
menaces
cyber

SPACE AERO / SSG : Jérôme CARRASCO (Formateur), Jennifer NKIDIKA (Formatrice), François LAGAUDE (Responsable Formation)

Mardi 13 décembre 2022



150 entreprises membres

1000 projets accompagnés

L'association qui vous accompagne vers l'Excellence Industrielle

7000 stagiaires formés

37 formations expertes

BEST QUALITY

BEST DELIVERY TIME

COMPETITIVITY

SPACE Academy

"Turn our expertise into your performance"

OPÉRATEUR DE SERVICES
DE CONFIANCE

Qualifications ANSSI

Conformité réglementaire

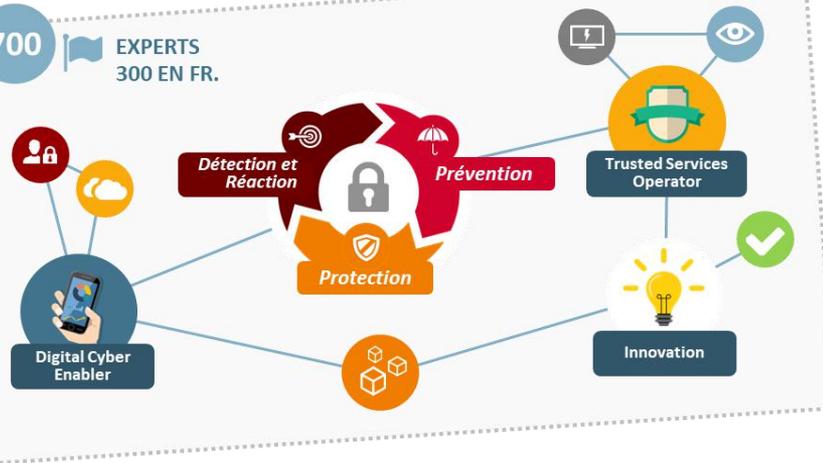
PARTENAIRE CYBER DE CONFIANCE,
ACCÉLÉRATEUR DE LA
TRANSFORMATION DIGITALE

FACILITATEUR
DU NUMÉRIQUE

Continuité digitale
Applications & Données



700 EXPERTS
300 EN FR.



NOTRE ADN



INNOVATION



FLEXIBILITÉ





Pourquoi de la cybersécurité
dans le monde industriel ?

Faire face à un contexte !

L'industrie face aux cyber attaques



UKRAINE BLACK-OUT

- Développé par les États-Unis et Israël
- Conçu pour permettre les Black Energy à une centrale électrique dans l'ouest de l'Ukraine
- 80 000 foyers sans électricité en hiver

ARAMCO

2016-2017

- 30 000 ordinateurs portables dont 2000 serveurs **PETYA NOT PETYA** une journée
- Perturbation des activités
- Les rançons touchent plus de 2000 entreprises

GERMAN STEEL MILL

2015

- Plus de 200 millions d'euros d'impact pour Saint-Martin Laussier des opérateurs ferroviaires (SNCF), des centrales nucléaires à Tricastin... correctement fermé, ce qui a entraîné une attaque "massive" par la suite

WANNACRY

L'industrie face aux cyber attaques

**Jean-Jacques Latour, responsable de
l'expertise en cybersécurité de la plate-forme
gouvernementale [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)**

- **« 91 % des organisations françaises ont été la cible d'au moins une cyberattaque au cours des douze derniers mois et 65 % d'entre elles ont même été ciblées à plusieurs reprises. »**

LE CONTEXTE DE LA CYBERSECURITE INDUSTRIELLE

ENJEUX SPÉCIFIQUES ET LES FREINS



Enjeux corporatifs

- Viabilité de l'entreprise
- Rentabilité



Enjeux IS

- Disponibilité – Intégrité – Confidentialité - Traçabilité
- Digitalisation
- Hyper-connectivité
- Harmonisation & rationalisation

Enjeux de production

- Sécurité (Personnes, Qualité)
- Engagements commerciaux
- Productivité



- *Manque d'alignement entre le métier de l'IT et de l'industrie*
- *Héritage du « Legacy »*
- *Manque de connaissance du « legacy »*
- *Manque de sensibilisation à la Cybersécurité*
- *Accélération de la digitalisation*
- *Complexité de la maintenance de l'IT/OT*

60%

des PME/PMI impactées par une cyberattaque mettent la clé sous la porte sous 6 mois.

www.CCI.fr, 2021

En général sur 1178 dirigeants interviewés pendant une enquête :

- 29% y consacrent un budget
- 34% ont une assurance en cas d'attaque
- 16% sont des TPE
- 39% savent que leur niveau cyber est insuffisant

- 50% des attaques de logiciels malveillants proviennent du courrier électronique
- Les logiciels malveillants ciblant les mobiles ont augmenté de 54 % en 2018
- 99,9 % des logiciels malveillants mobiles se trouvent dans les boutiques d'applications tierces



Quels sont les premiers
gestes essentiels ?

Sensibiliser tout le monde !!!

Oh oh! ...



Environ **82%** des incidents de cybersécurité ont pour origine une **ERREUR HUMAINE**.

Votre collaborateur peut devenir votre meilleur atout !



Notre équipe accompagne vos **COLLABORATEURS** afin qu'ils deviennent
LA PREMIÈRE LIGNE DE DÉFENSE face aux cyberattaques



SENSIBILISER



ACCOMPAGNER
LE CHANGEMENT



PARTAGER &
PROMOUVOIR



Jour 1

Matin : Sensibilisation et bonnes pratiques

Sensibilisation générale aux bonnes pratiques, afin de prévenir les incidents de Cyber Sécurité dans un contexte industriel:

- Les Menaces
- Les Impacts
- Les Bonnes Pratiques

Co-construction d'une Charte de Sécurité

Après-midi : Protection des systèmes industriels

Evolution des enjeux de Sécurité: hier, aujourd'hui, demain

Typologies de Cyber-Attaques sur les Systèmes Industriels

Etudes de cas:

- Déroulement de l'attaque
- Impacts et conséquences
- Solutions de prévention ou de réaction

Cartographie des principales solutions de protection

> Contexte

Dans un contexte où les cyber menaces sont de plus en plus fréquentes, et ciblent de plus en plus spécifiquement le domaine industriel, former les collaborateurs de votre entreprise aux bonnes pratiques et aux approches de protection est aujourd'hui un enjeu incontournable.

En sensibilisant vos employés aux risques Cyber, à ses conséquences ainsi qu'aux moyens de protection, vous les dotez des connaissances de base nécessaires afin d'intégrer la Cyber Sécurité au sein de leurs activités quotidiennes.

Ce faisant, vous protégez à la fois vos employés eux mêmes, les actifs de votre entreprise (protection de la donnée, continuité de service, etc.) et vos clients (prévention de rupture de la Supply Chain ou de la propagation d'une attaque).

Formation sélectionnée par le GIFAS pour le projet Performance Industrie du Futur.

> Objectifs

Le stagiaire une fois formé sera en mesure de :

- Mesurer les conséquences d'une Cyberattaque en milieu industriel
- Mettre en place les bonnes pratiques afin de se protéger et de protéger l'entreprise
- Appréhender les fondamentaux de la Cyber Sécurité en milieu industriel

> Public

- Le personnel impliqué dans le cycle de vie des Systèmes Industriels (Direction, production, qualité, logistique, achats/appros, planification...)

> Prérequis

Aucun



Méthodes Pédagogiques

La formation est interactive et ludique. Les participants sont répartis en équipes. Des activités jalonnent les différents concepts et font gagner des points aux équipes. L'esprit de compétition, toujours bienveillant, génère une dynamique participative, une cohésion et favorise la communication au sein des équipes. L'implication active des stagiaires favorise l'ancrage des messages et bonnes pratiques.

Méthodes d'évaluation

Test d'entrée et test de sortie permettant une évaluation des compétences acquises.



Nos Experts

L'animation est intégralement assurée par des consultants ayant une expertise pratique de la Cybersécurité en milieu industriel

Modalités

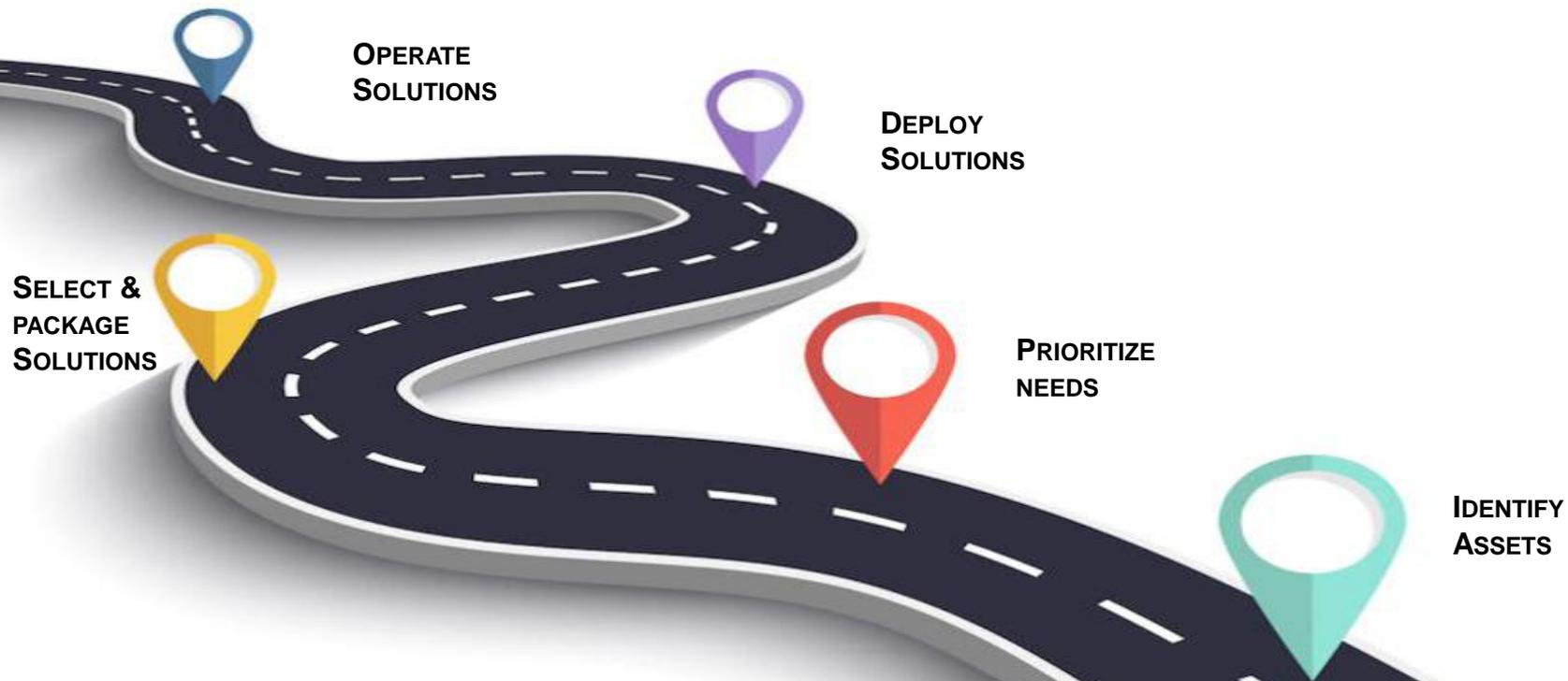
Inscription et délai : Bulletin d'inscription à compléter et à nous retourner au plus tard une semaine avant le démarrage

Accès Personnes Handicapées : nous contacter pour déterminer l'aménagement à mettre en place.



Protéger son système de production de manière efficace

La cybersécurité, un long chemin! Mais nécessaire !



Protéger son système d'information des cyber menaces en milieu industriel

Approches de prévention, de détection

C'EST QUOI UN SOC ?
OPERATE CYBER SOLUTIONS



Performance & value Cockpit



Follow the SUN Support

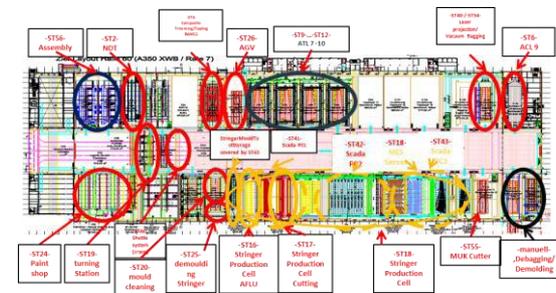
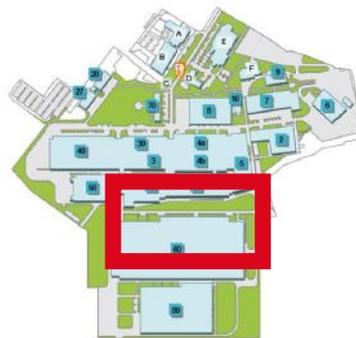
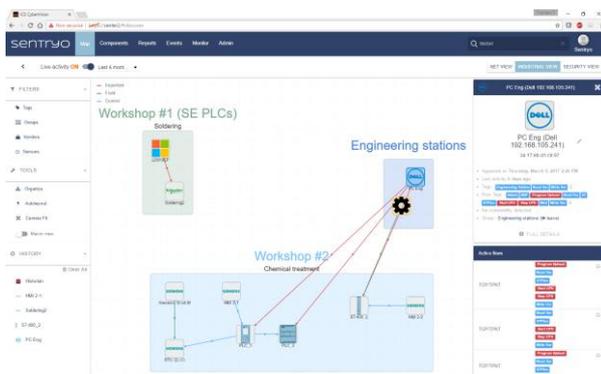


Maximiser la performance et la valeur livrée

Protéger son système d'information des cyber menaces en milieu industriel

- Réponse pour la Cybersécurité industrielle

DISSECTION D'UNE ATTAQUE UN INVENTAIRE À JOUR

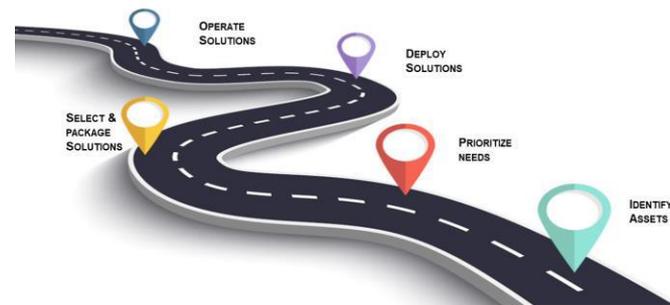


Industrial CMBD: Inventaire & géolocalisation des actifs industriels

Protéger son système d'information des cyber menaces en milieu industriel

Réponse pour la Cybersécurité industrielle

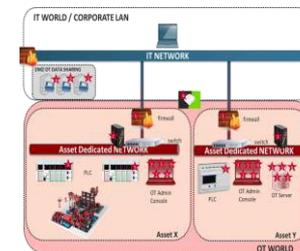
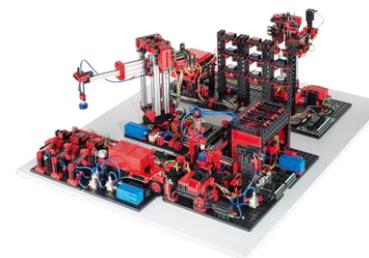
**RÉVISIONS DES ÉQUIPEMENTS ACTUELLEMENT
EN PLACE
SÉLECTION DE SOLUTIONS
SAUVEGARDES**



Exemple de catalogue de solutions industrielles



Revoir l'environnement réseau



Choisir le cadre d'évaluation approprié

Protéger son système d'information des cyber menaces en milieu industriel



Coût



Qualité



Délai



Organisation



Jour 1 : Connaître les menaces, les stratégies de sécurisation et la mise en place d'une démarche de prévention et protection

- Définition de l'industrie 4.0 et de ses objectifs
- Présentation des différents domaines de l'I4.0
- Présentation des différentes technologies utilisées eg : ERP, MES, GMAO,...
- Présentation de la stratégie de transformation digitale à l'échelle d'une entreprise
- Présentation de la stratégie de transformation digitale à l'échelle d'une usine
- Démonstration d'outils et d'applications connectés

Jour 2 : Approches de prévention, de détection et de réponse pour la Cybersécurité industrielle

- Sensibilisation à la sécurité
- Identification et gestion des assets et des risques
- Protection, détection et réaction
- Gestion des vulnérabilités
- Conclusion
- Continuité de services
- Reprise d'activités
- Déploiement des solutions de sécurité dans le domaine industriel
- Exercice: mise en place de solutions Cybersécurité
- Correction de l'exercice
- Conclusion et debrief

Contexte

La connaissance des différentes normes dans le domaine de la cybersécurité industrielle devient de nos jours importante et primordiale, si on souhaite se protéger au mieux des attaques qui sévissent aujourd'hui dans le domaine. Surtout dans un contexte où plus de 60% de sociétés qui ont été victimes d'une cyber attaque ferment leur porte dans l'année qui suit. La pro activité reste le maillon fort de la cybersécurité.

Objectifs

Le stagiaire une fois formé sera en mesure de :

- Connaître les outils d'analyse de risque
- Maîtriser les normes à respecter dans son environnement (Cyber indus)
- Concevoir et jouer un PCA et un PRA

Public

- Responsable informatique ou en collaboration avec une infogérance
- Responsable des consignes de sécurité internes à une entreprise (HSCT ou équivalent)
- Direction générale des PME ou PMI

Prérequis

- Connaissances en infrastructures informatiques

Matériel

Aucun



Méthodes Pédagogiques

Approche théorique illustrée par des exemples vécus. Un support récapitulatif est remis à l'issue de la séquence 2

Méthodes d'évaluation

Test d'entrée et test de sortie permettant une évaluation des compétences acquises.



Nos Experts

L'animation est intégralement assurée par des consultants ayant une expertise pratique de la Cybersécurité en milieu industriel.

Modalités

Inscription et délai : Bulletin d'inscription à compléter et à nous retourner au plus tard une semaine avant le démarrage.
Accès Personnes Handicapées : nous contacter pour déterminer l'aménagement à mettre en place.



Des questions ?

7. Contacts

Etudions ensemble votre projet formation



François LAGAUE
Responsable Service Formation
francois.lagaude@space-aero.org
06.12.78.66.03

[Télécharger le guide de la formation](#)



The screenshot shows the website for the 'Fondamentaux Cybersécurité industrielle' course. The header includes the SPACE logo and 'SPACE Academy' with a navigation menu: Accueil, Formations, Qui sommes-nous?, Actualités, Contact, Clients et Partenaires. The main heading is 'Fondamentaux Cybersécurité industrielle' with a subtitle 'Fondamentaux Cybersécurité industrielle : risques, enjeux et bonnes pratiques'. The course details are as follows:

- Formation**
- TARIF :**
INTER : Nous consulter
INTRA : Nous consulter
- DURÉE :**
7 heures
- GROUPE :**
De 8 à 15 personnes
- FICHE PROGRAMME :**
Téléchargez le programme détaillé de la formation.
- OBIECTIFS :**
La stagiaire une fois formé sera en mesure de :
 - Mesurer les conséquences d'une Cyber-attaque en milieu industriel,
 - Acquérir les bonnes pratiques afin de se protéger et protéger l'entreprise,
 - Appréhender les fondamentaux de la Cyber Sécurité en milieu industrielle.
- PRÉREQUIS :**
Pas de pré-requis.
- CONTENU :**
Matin : Sensibilisation et bonnes pratiques.
Après-midi : Protection des systèmes industriels.

A green arrow points to the 'TÉLÉCHARGER' button under the 'FICHE PROGRAMME' section.



Rediffusion du Webinar bientôt disponible sur

<https://www.space-aero.org/fr/actualites/>

Merci pour votre participation



Merci pour votre attention!

www.space-aero.org