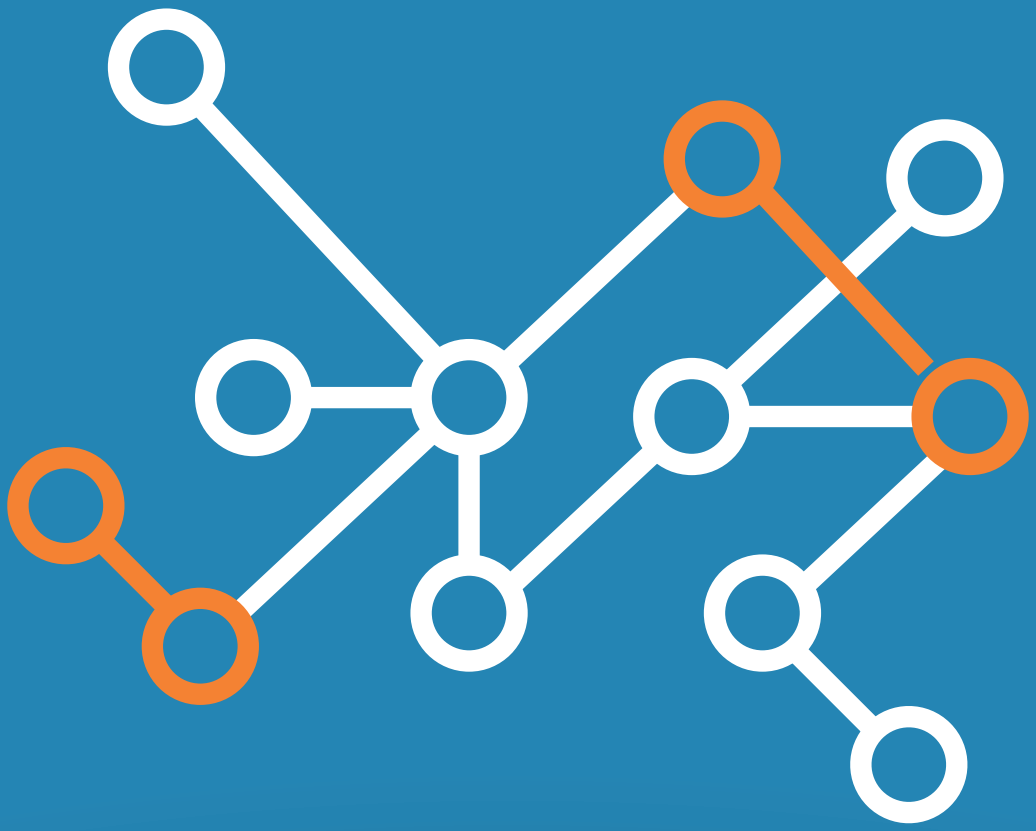

JE TESTE MA MATURITÉ CYBER.

Livret réalisé par l'Agence Smart Industry et SMART4D dans le cadre du workshop « Cybersécurité Industrielle : quels risques, quelles solutions ? ».

AGENCE SMART INDUSTRY

SMART4D®

DIGITAL AQUITAINE

Basé en Nouvelle-Aquitaine, SMART4D a pour vocation de bâtir un réseau d'experts et d'industriels sur les usages de la simulation numérique (Réalité Virtuelle et Augmentée, Simulation interactive, Modélisation scientifique, technique et industrielle).

Depuis 2017, SMART4D anime, fédère et structure, l'ensemble des acteurs du territoire néo-aquitain (start ups, PME, ETI, grands comptes et institutionnels, académiques et recherche), autour de leurs activités et besoins de développement, d'intégration et de mise en œuvre de solutions applicatives.

Les projets collaboratifs sont le moteur de l'activité de SMART4D. Ils permettent de créer une dynamique collective, en réunissant les membres, autour de thématiques communes, pour relever de nouveaux défis techniques et d'usages afin d'inventer les solutions de demain !

//////////////

Contact :

Marion **LENOIR**
Chargée de mission SMART4D

+33(0)6 24 50 70 24

mlenoir@digital-aquitaine.com

Au sein d'une entreprise, amorcer une démarche de transformation digitale peut vite s'avérer compliqué (manque de temps, de compétences…). C'est pourquoi nos consultants vous conseillent et vous accompagnent dans les différentes étapes de votre projet de Digitalisation Opérationnelle et de Sécurisation/Optimisation de vos systèmes d'information.

Notre valeur-ajoutée ? Nous vous conseillons en toute objectivité, afin de vous garantir des conseils personnalisés et adaptés pour booster les performances de vos équipes et de votre entreprise.

//////////////

Contact :

Alexandra **DESSERRE**
Présidente de l'Agence Smart Industry

+33(0)6 51 88 20 11

alexandra.desserre@agencesi.tech

Jean-Baptiste **SICAUD**
Responsable de projet SI

+33(0)6 12 94 54 60

jb.sicaud@agencesi.tech

QUESTIONNAIRE « EVALUER LE NIVEAU DE PROTECTION DANS LE MILIEU INDUSTRIEL »

Gestion des vulnérabilités et Politique de patch management

	Oui	Non
Connaissez-vous le niveau de vulnérabilité sur vos équipements industriels (ex: PDA, machine-outil, etc.) ?	☐	☐
A la publication d'une nouvelle vulnérabilité critique, pouvez-vous facilement identifier les équipements vulnérables de votre parc industriel ?	☐	☐
Votre solution de gestion des vulnérabilités est-elle capable de prioriser et de vous produire une liste des patchs critiques à appliquer ?	☐	☐
Votre solution de gestion des vulnérabilités vous permet-elle d'avoir la liste exhaustive des machines à redémarrer et des systèmes hors support ?	☐	☐
Mesurez-vous le délai moyen de correction de vos vulnérabilités critiques ?	☐	☐

Sensibilisation des collaborateurs

	Oui	Non
Réalisez-vous régulièrement des sessions de sensibilisation aux risques de Cybersécurité ?	☐	☐
Évaluez-vous périodiquement la sensibilité de vos collaborateurs via des campagnes de phishing contrôlées ?	☐	☐
Avez-vous mis à disposition de vos collaborateurs un moyen de remonter les tentatives de phishing afin de les qualifier et les quantifier ?	☐	☐
Avez-vous une charte informatique pour vos utilisateurs ?	☐	☐

Segmentation des infrastructures réseau

	Oui	Non
Existe-t-il un filtrage par firewall entre les réseaux administratif et industriel ?	☐	☐
Les logs de vos solutions de filtrage réseau sont-ils collectés et stockés à des fins d'analyse ?	☐	☐
Réalisez-vous périodiquement des audits des configurations des règles de filtrage ?	☐	☐

Sécurité des mots de passe

	Oui	Non
Réalisez-vous des audits de mot de passe ?	☐	☐
Avez-vous mis en place une politique de complexité des mots de passe forte (12 caract. + minuscule + majuscule + chiffres + caract. spéciaux) ?	☐	☐
Fournissez-vous à vos utilisateurs un gestionnaire de mots de passe ?	☐	☐
Avez-vous mis en place un gestionnaire de mot de passe pour vous ainsi que pour vos collaborateurs ?	☐	☐

Protection des postes clients et machines

	Oui	Non
Vos postes de travail sont-ils protégés par une solution antivirus ?	☐	☐
Les alertes de l'EDR ou de l'antivirus sont-elles analysées ?	☐	☐
Possédez-vous une console de gestion des mises à jour ?	☐	☐
Possédez-vous une console permettant de pousser les mises à jour critiques sur votre parc administratif et industriel ?	☐	☐
Est-ce que chaque utilisateur à un compte nominatif ?	☐	☐

Évaluer le niveau de protection externe

	Oui	Non
Avez-vous réduit l'accès à internet au strict minimum dans votre environnement de production ?	☐	☐
Vos utilisateurs ont-ils accès au SI par une solution d'accès externe ?	☐	☐
Vos prestataires ont-ils un accès à votre infrastructure ?	☐	☐
Vos accès distants sont-ils soumis à une authentification à double facteur ?	☐	☐
Êtes-vous alerté et traitez-vous en temps réel les connexions simultanées d'un utilisateur depuis plusieurs pays ?	☐	☐
Est-ce que la solution d'accès externe limite le périmètre d'accès à votre SI au strict nécessaire ?	☐	☐

Gestion des accès d'administration et des comptes à privilèges

	Oui	Non
Vos administrateurs utilisent-ils des comptes dédiés et nominatifs pour les accès aux configurations des infrastructures et des applications ?	☐	☐
Vos administrateurs utilisent-ils un modèle de Tiering pour segmenter les accès aux postes de travail / serveurs / Active Directory	☐	☐
Existe-t-il un bastion permettant de centraliser et sécuriser les logs de configuration des infrastructures et des applications ?	☐	☐
Les administrateurs informatiques sont-ils les seuls à pouvoir installer des logiciels en environnement de production ?	☐	☐

Préparer la continuité

	Oui	Non
Vos équipements industriels font-ils partie de l'Active Directory ?	☐	☐
Votre système de sauvegarde inclut-il des sauvegardes à froid (externalisé du SI) ?	☐	☐
Faites-vous régulièrement des tests de restauration de systèmes complets ?	☐	☐
Avez-vous évalué la durée de restauration de l'ensemble de votre SI et est-ce en corrélation avec les contraintes métiers ?	☐	☐

[Notes]

[Notes]

85%

des violations de la cybersécurité sont causées par une erreur humaine.

94%

94 % de tous les logiciels malveillants sont envoyés par e-mail.

Un ordinateur en sécurité est un ordinateur éteint. Et encore...

10'

Les attaques de ransomware se produisent toutes les 10 secondes.

+ 80%

Plus de 80 % des événements de cybersécurité impliquent des attaques de phishing.

1/2

Près de la moitié de toutes les cyberattaques ciblent les petites entreprises.

Vous souhaitez **contacter un intervenant ?**

- Olivier **GRALL**
  Délégué à la sécurité numérique - ANSSI

  olivier.grall@ssi.gouv.fr

- Toufik **AHMED**
  Directeur adjoint – ENSEIRB-MATMECA

  toufik.ahmed@enseirb-matmeca.fr

- Guy **FLAMENT**
  Directeur – Campus Cyber Nouvelle-Aquitaine

  directeur@campuscyber-na.fr

- Laurent **BODART**
  Vice-président – Clusir Nouvelle-Aquitaine

  lbodart@clusir-aquitaine.fr

- Jabier **MARTINEZ**
  Chercheur – Tecnalia Research & Innovation

  jabier.martinez@tecnalia.com

- Stéphane **POTIER**
  Responsable de l'offre Cybersécurité OT & IOT – Advens

  stephane.potier@advens.fr

- Steve **HERVÉ**
  Cybersecurity Senior Manager & Directeur
  agence Sud-Ouest – Atos

  steve.herve@atos.net