L'UNION FAIT LA FORCE

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

# Les enjeux cyber, IE et PJL
# Résiliences critiques

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

FIEV
ÉQUIPER LE FUTUR DE L'AUTOMOTIVE

L'UNION FAIT LA FORCE

# SOMMAIRE

L'UNION
FAIT LA FORCE

# Hexatrust et ses missions

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L'Hexa Pres

L'UNION FAIT LA FORCE

# Qui sommes-nous ?

## Hexatrust, le groupement des champions français et européens de la cybersécurité et du cloud de confiance.

- Association de loi 1901 regroupant une centaine d'entreprises de la cybersécurité et du cloud de confiance
- Créée en 2013 par 11 entreprises
- Défendre les intérêts des acteurs du secteur auprès des pouvoirs publics et unir nos forces pour promouvoir nos solutions souveraines

**Quelques chiffres**

**+140**
membres

**+8000**
experts

**10**
milliards d'euros de chiffre d'affaires réalisés par nos membres

**Nos valeurs**

**Excellence**

**Confiance**

**Action**

**Innovation**

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

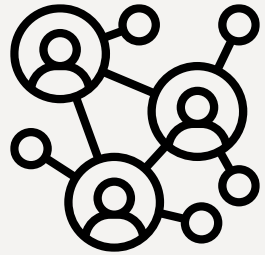
L'Hexa Pres

L'UNION FAIT LA FORCE

# Tous nos membres

**Défendent une certaine idée de la maîtrise des données, de l'indépendance technologiques et de la transparence**

**ont à cœur de promouvoir l'écosystème français et européen**



**partagent des valeurs d'entraide, d'excellence et d'innovation**

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L'Hexa Pres

L'UNION FAIT LA FORCE

# Nos missions

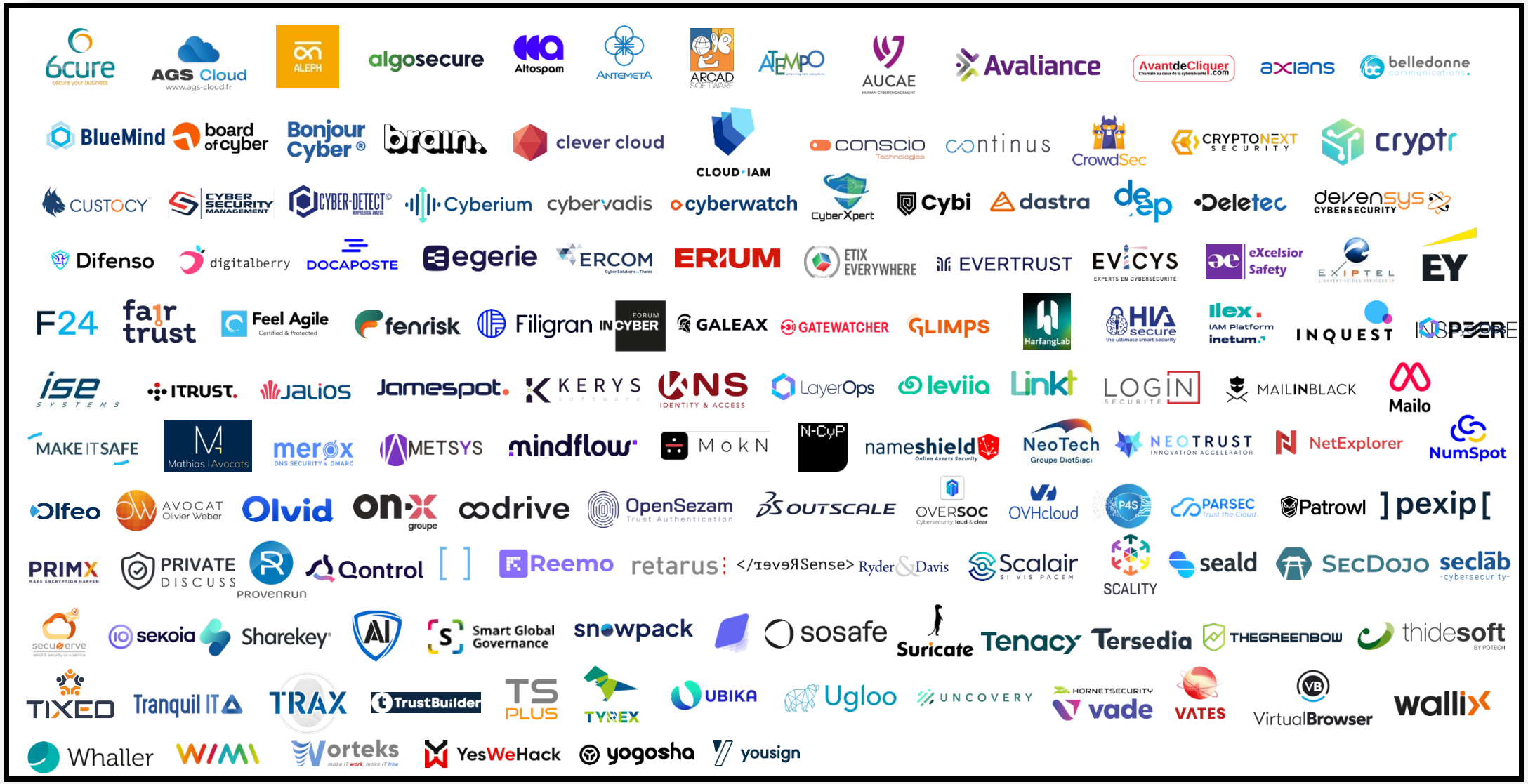
L'UNION FAIT LA FORCE


**Unis pour construire ensemble une filière engagée pour un monde numérique plus sûr, résilient et protecteur des données.**

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

# L'Hexa Pres

L'UNION FAIT LA FORCE



L'UNION
FAIT LA FORCE

# Enjeux liés à la cyber et l'IA pour vos métiers

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L'Hexa Pres

L'UNION FAIT LA FORCE

# Des cybermenaces et des motivations

Hameçonnage (phishing)

DDoS (Attaque par déni de service)

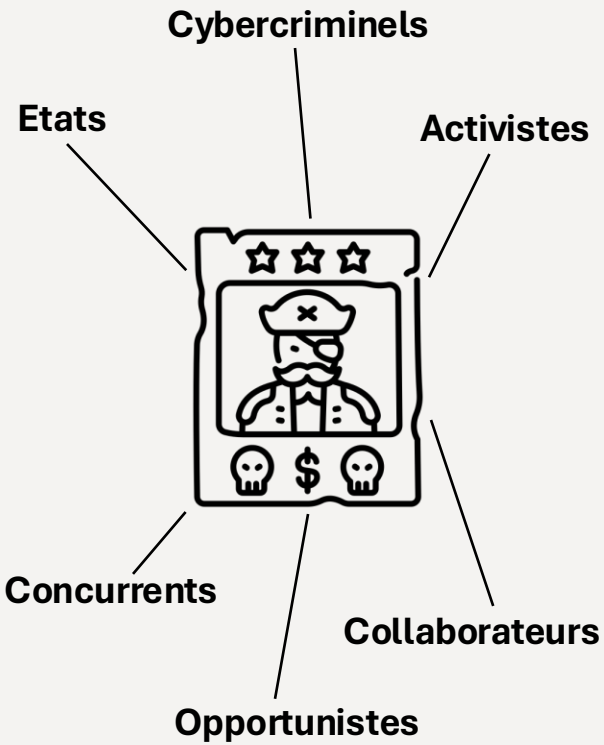
Rançongiciel (ransomware)

Défiguration du site

Attaque sur la chaine d'approvisionnement

**Le cyberattaquant – type**

n'existe pas !




**Motivations**

Cybercriminalité

Espionnage

Sabotage

Atteinte à l'image

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L'Hexa Pres

L'UNION FAIT LA FORCE

# Quelques chiffres...

**226**

attaques recensées depuis 2020

**50M$**

Cyberattaque de Continental en 2022 pour 55 millions de fichiers publiés

**3, 31Mrd$**

Marché de la cybersécurité automobile en 2023, estimation à 12,9 milliards en 2032

L'Hexa Pres

L'UNION FAIT LA FORCE

# Les risques liés au secteur industriel

## Évolution et exposition croissante

- Passage à l'industrie 4.0 interconnexion IT/OT = explosion de la surface d'attaque.
- Systèmes conçus pour l'isolement désormais connectés à Internet et aux SI d'entreprise.

## Menaces majeures

- Espionnage industriel (prépositionnement, cartographie réseau, vol de secrets de fabrication).
- Sabotage ciblé (altération des procédés de production → défauts qualité, arrêts chaîne).
- Cybercriminalité & ransomwares : la dépendance à la continuité de production = levier de pression.
- Malveillance interne & négligences : usage de clés USB, contournement de consignes, erreurs humaines.

## Vulnérabilités critiques

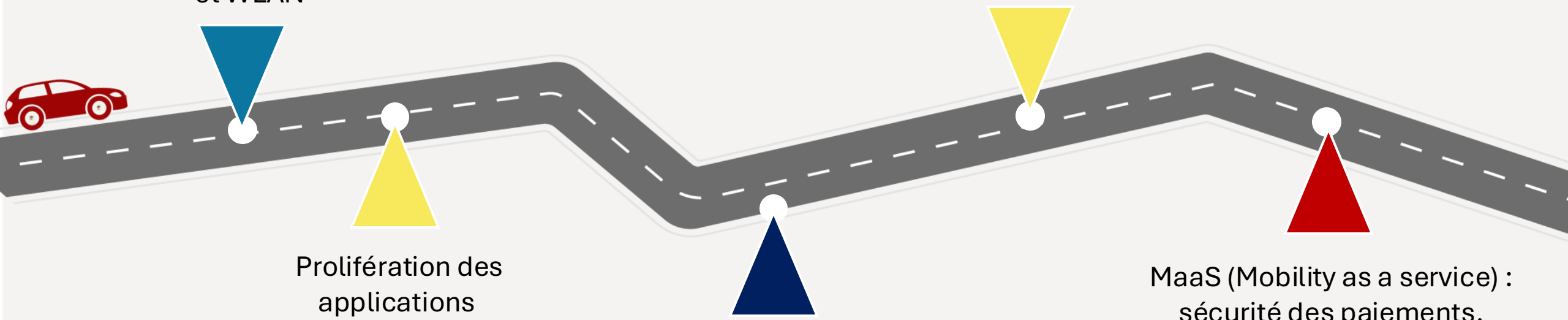
- Protocoles non sécurisés, systèmes non patchables, technologies sans fil exposées.
- Utilisation de composants IT génériques non qualifiés pour l'OT.
- Faible maturité SSI du personnel industriel (manque de formation & culture cyber).

L'Hexa Pres

L'UNION FAIT LA FORCE

# Les risques liés à la mobilité

Augmentation de la surface d'attaque via les Ordinateurs de bord et système d'assistance via les interfaces sans fil Bluetooth et WLAN



Prolifération des applications compagnons

Prise de contrôle à distance d'un véhicule autonome

Mises à jour à distance dont les mises à jour OTA et cycle de mises à jour perpétuel

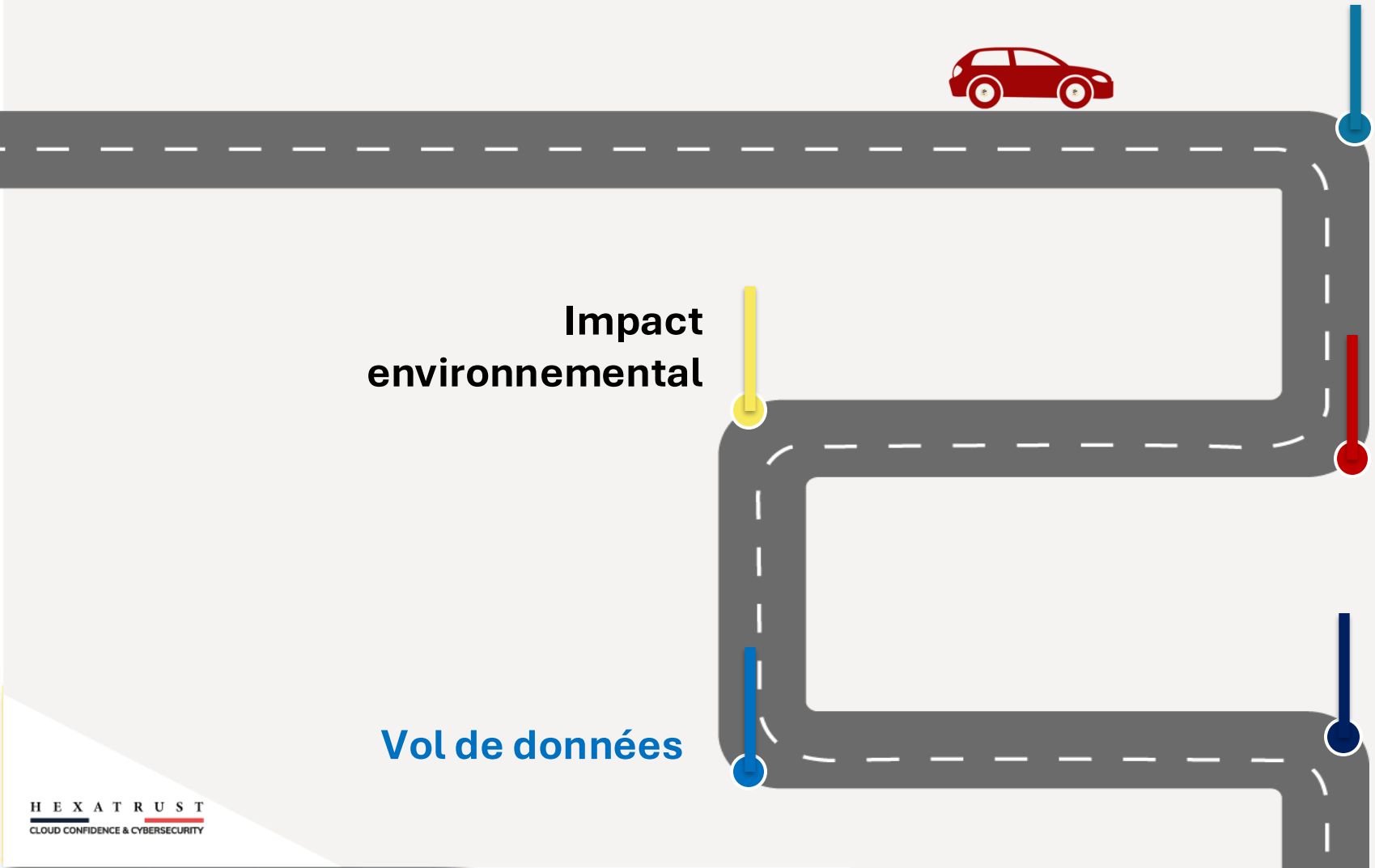
MaaS (Mobility as a service) : sécurité des paiements, facturation et protection des données personnelles

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L'Hexa Pres

L'UNION FAIT LA FORCE

# Impacts concrets pour les équipementiers automobiles



Dommages matériels/humains

Impact environnemental

Perte de chiffre d'affaires

Vol de données

Responsabilité légale / image

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

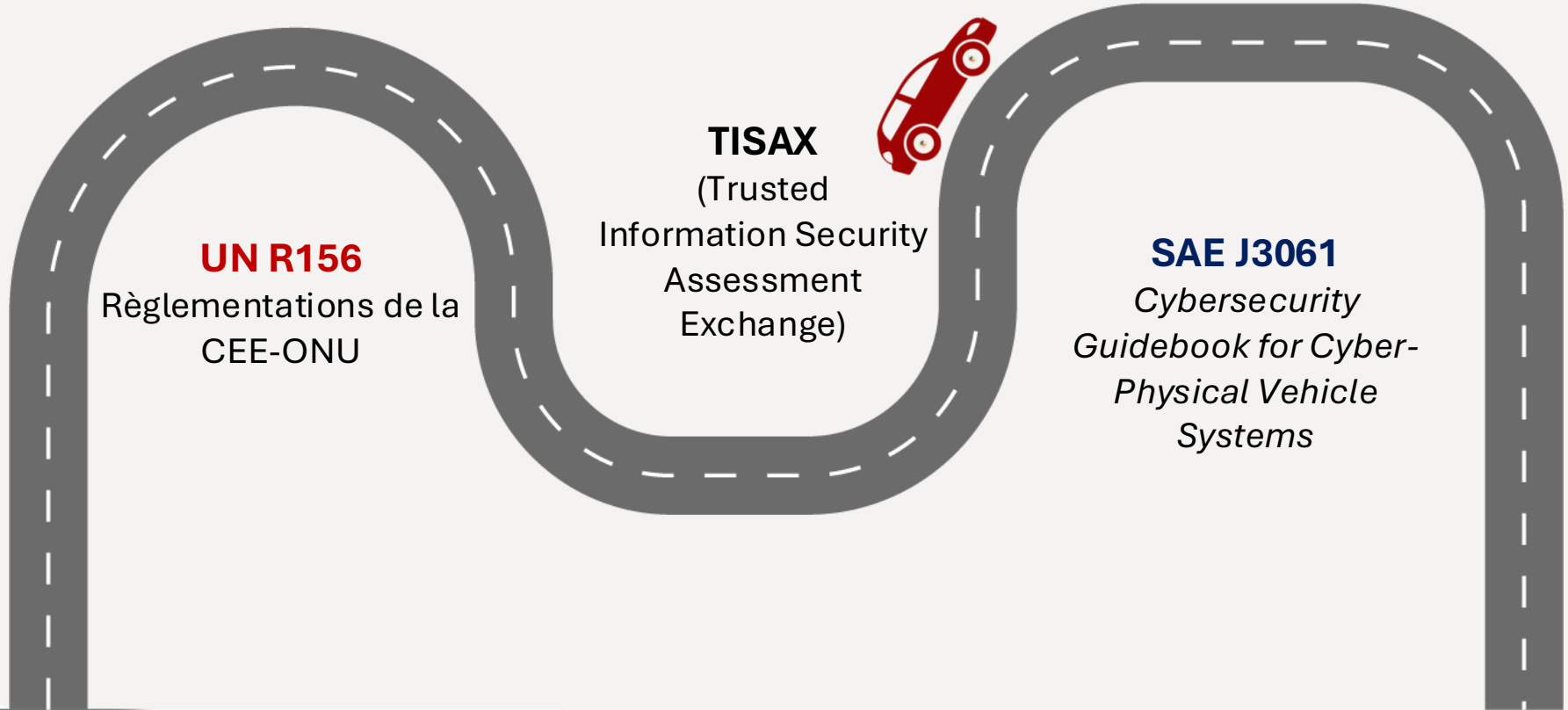
L'Hexa Pres

L'UNION FAIT LA FORCE

# L'industrie… aux multiples normes

**UN R155**
Règlementations de la CEE-ONU

**ISO/IEC 27001**
*Information Security Management Systems (ISMS)*



**ISO/SAE 21434**
*Road Vehicles – Cybersecurity Engineering*

**UN R156**
Règlementations de la CEE-ONU

**TISAX**
(Trusted Information Security Assessment Exchange)

**SAE J3061**
*Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*

**ISO 26262**
*Functional Safety*

# La cybersécurité est un sujet de gouvernance

## Effets d'une cyberattaque sur la gestion informatique

**Cyberattaque**

### Effets immédiats

- Réparation des dommages faits au SI
- Coûts engenders par les renforts
- Coût de remplacement du matériel défectueux

### 1 à 3 mois après

- Reconstruction du SI
- Changement des pratiques

### 6 mois à 3 ans après

- Impact négatif sur la réputation de l'entreprise
- Perte de confiance

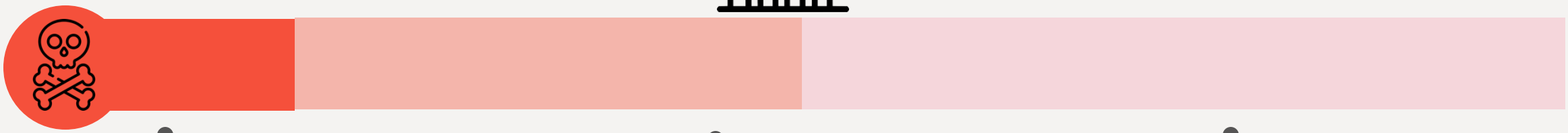
L'Hexa Pres

L'UNION FAIT LA FORCE

# La cybersécurité est un sujet de gouvernance

## Effets d'une cyberattaque sur les pertes d'exploitation

**Cyberattaque**



### Effets immédiats

- Fonctionnement de l'entreprise perturbé, voire interrompu
- Perte des données
- Perte de temps des équipes
- Opportunités manquées
- Communication compliquée avec les clients et fournisseurs

### 1 à 3 mois après

- Désorganisation de l'activité
- Coût des dédommagements

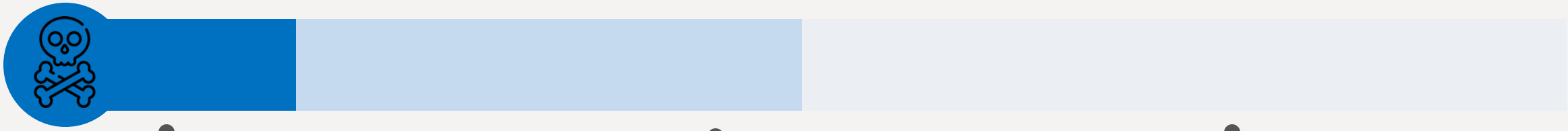
### 6 mois à 3 ans après

- Impact négatif sur la réputation de l'entreprise
- Perte de confiance

# La cybersécurité est un sujet de gouvernance

## Effets d'une cyberattaque sur les coûts juridiques

**Cyberattaque**



### Effets immédiats

- Dépôt de plainte de l'entreprise et gestion qui en découle
- Analyse des impacts juridiques possibles effectués par des professionnels

### 1 à 3 mois après

- Demande des autorités
- Audits supplémentaires

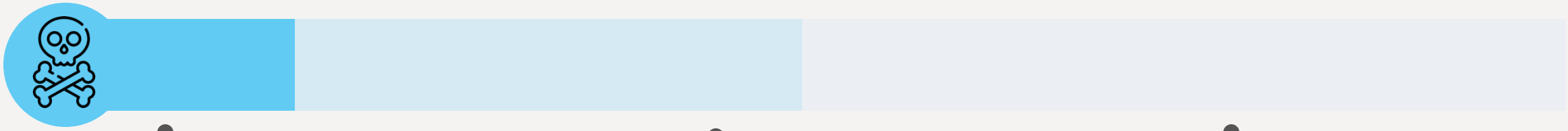
### 6 mois à 3 ans après

- Coûts liés aux conseils juridiques et aux éventuelles amendes

# La cybersécurité est un sujet de gouvernance

## Effets d'une cyberattaque sur la communication

**Cyberattaque**



### Effets immédiats

- Définition de l'attitude à adopter suite à l'attaque
- Temps dédié à répondre aux différentes interrogations

### 1 à 3 mois après

- Image de l'entreprise dégradée
- Possibilité de publication de nouveaux éléments

### 6 mois à 3 ans après

- Impact négatif sur la reputation de l'entreprise
- Perte de confiance

L'Hexa Pres

L'UNION FAIT LA FORCE

# L'IA: de nouveaux risques...

## Problèmes de Confidentialité

## Augmentation de la surface d'attaque

## Augmentation du nombre d'acteurs

À cause de ChatGPT, un avocat américain cite des arrêts... qui n'ont jamais existé

Par Paul Sugy
Le 30 mai 2023 à 14h31

SUIVRE

ChatGPT avocats New York

Lire dans l'app | Copier le lien

Écouter cet article 00:00/02:42



Le générateur de texte par intelligence artificielle ChatGPT avertit ses usagers qu'il n'est pas infaillible. *Supatman /*

Chatbot

Le chatbot IA d'un concessionnaire automobile vend un Chevrolet à 1 dollar

Par Hasina H. Mis à jour : Il y a un an 3 minutes de lecture

*L'intelligence artificielle est une technologie en constante évolution. Elle impressionne souvent par ses capacités, mais elle peut aussi commettre des erreurs, amusantes pour les internautes, mais moins plaisantes pour les entreprises. C'est ce qui s'est produit avec le chatbot d'un concessionnaire automobile californien, qui a vendu un Chevrolet à un client pour seulement 1 dollar.*

Air Canada reconnu responsable des hallucinations de son chatbot

Publié le 21 février 2024 à 07:01



Les entreprises qui intègrent à tort et à travers des chatbots pour renseigner leurs clients y réfléchiront peut-être à deux fois, après la déconfiture d'Air Canada devant les tribunaux.

En mars 2023, Air Canada inaugurait sur son site web un nouveau chatbot carburant à l'intelligence artificielle, dont le boulot était de soulager les centres d'appels de l'entreprise lors

L'Hexa Pres

L'UNION FAIT LA FORCE

# … mais aussi des opportunités

**Détection Avancée des Menaces**

**Automatisation des Réponses**

**Accessibilité et Coût**

L'Hexa Pres

L'UNION FAIT LA FORCE

# Projet de loi résilience

- Le texte devrait être **finalisé d'ici le 2ème semestre**
- Un **référentiel attendu, avec 20 mesures de sécurité**
- Une loi qui touchera **l'ensemble de la chaine de sous-traitance** ; toutes les entreprises devront monter en compétence

**Résilience des activités d'importance vitale**

- Transposition de REC
- Renforcer la résilience des infrastructures critiques

**Cybersécurité**

- Transposition de NIS2
- Mise à niveau de la cybersécurité sur un standard européen pour les entités essentielles

**Résilience opérationnelle numérique du secteur financier**

- Transposition de DORA
- Encadrement des risques par les TIC dans le secteur financier

L'Hexa Pres

L'UNION FAIT LA FORCE

# Quels sont les types d'entités concernés ?

**- Directive NIS2 -**

Intégration progressive depuis octobre 2024

Jusqu'à

**15 000**

entreprises et organisations concernées:


**Entité importante**

- Secteur 1 et
- Au moins 50 personnes ou
- ont un chiffre d'affaires et un bilan annuel supérieur à 10 millions d'euros. ;


**Entité essentielle**

- Grande taille ou taille intermédiaire
- Au moins 250 employés ou plus
- ou ont un chiffre d'affaires annuel supérieur à 50 millions d'euros et un bilan annuel supérieur à 43 millions d'euros ;

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

*Source : ANSSI*

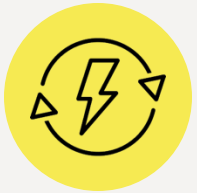
L'Hexa Pres

L'UNION FAIT LA FORCE

# Quels sont les secteurs concernés ? *

Secteur hautement critique

Autres secteurs critique



Energie

Transports

Secteur bancaire

Infrastructure des marchés financiers

Santé

Eau potable

Eaux usées

Infrastructure numérique

Gestion des services TIC

Administration

Espace

Services postaux & expédition

Gestion des déchets

Fabrication, production et distribution de produits chimiques

Production, transformation, distribution des denrées alimentaires

Fabrication * *

Recherche

Fournisseurs numériques

- En attente des codes NAF de la part de l'ANSSI

* * Dispositifs médicaux et de diagnostic in vitro; produits informatiques, électroniques et optiques ; équipements électriques ; machines et équipements; véhicules automobiles; remorques et semi-remorques ; autres matériels de transport)

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L'Hexa Pres

L'UNION FAIT LA FORCE

# Quelles obligations pour les entités concernées ?

## 1
## Le partage d'informations

Les entités seront tenues de fournir un certain nombre d'informations à l'ANSSI et de les mettre à jour.

## 2
## La gestion des risques cyber et la mise en place de mesures adaptées

Les entités devront mettre en place des mesures juridiques, techniques et organisationnelles pour gérer les risques qui menacent la sécurité de leurs réseaux et de leurs systèmes d'information.

## 3
## La déclaration d'incidents

Les entités devront signaler à l'ANSSI leurs incidents de sécurité ayant un impact important et fournir des rapports concernant l'évolution de la situation.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

# Comment avancer ?

Plusieurs leviers sont indispensables :

- **Segmenter rigoureusement** les environnements IT et OT.
- **Mettre à jour régulièrement les équipements**, en priorité ceux exposés à Internet.
- **Surveiller activement** les tentatives d'intrusion grâce à des SOC spécialisés capables d'alerter précocement.
- **Former les opérateurs industriels** aux risques cyber.
- **Adopter une approche par risque**, en se concentrant sur les vulnérabilités réellement critiques pour l'activité.

L'UNION
FAIT LA FORCE

# Les solutions Hexatrust

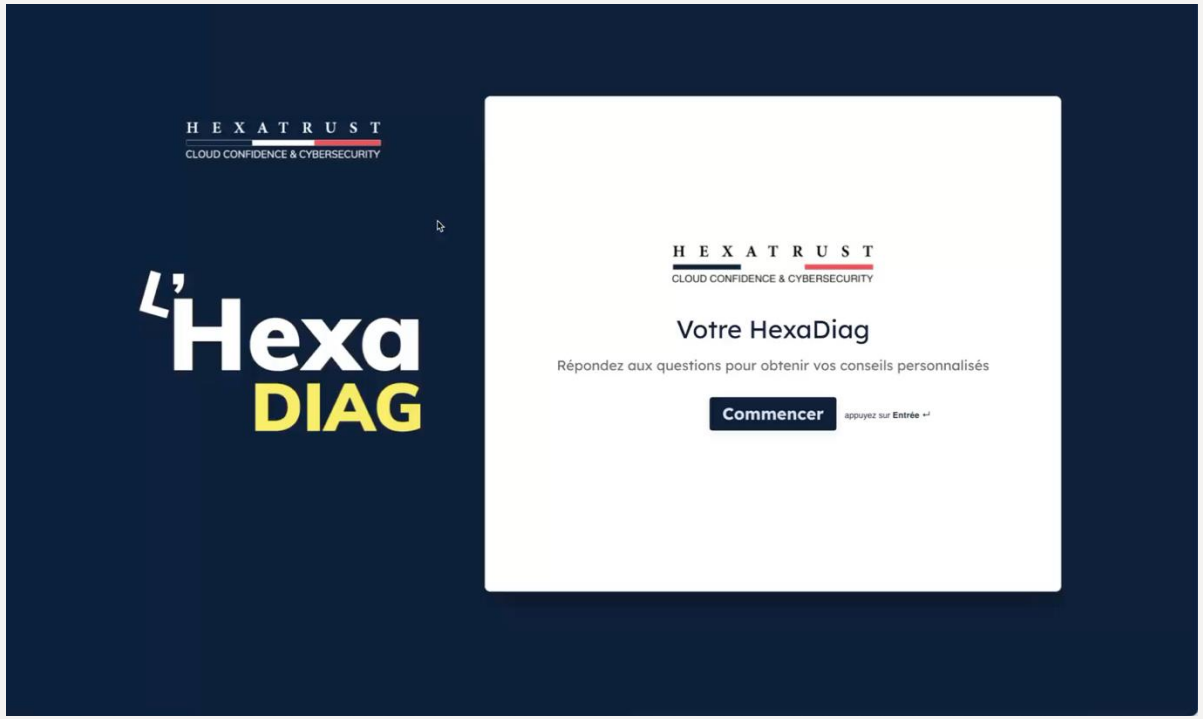
HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L'Hexa Pres

L'UNION FAIT LA FORCE

# Hexadiag

- Permettre aux dirigeants d'identifier les vulnérabilités de leurs entreprises
- Un questionnaire prenant en compte plusieurs normes et référentiels
- Une marketplace afin de se mettre aux normes avec des solutions souveraine.



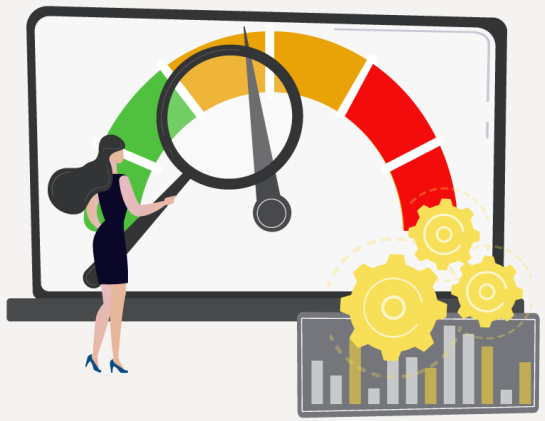

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

L'Hexa Pres

L'UNION FAIT LA FORCE

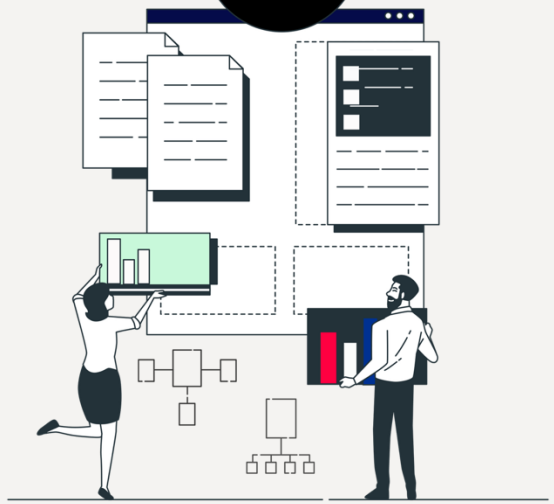
# Le fonctionnement

1



**AUTODIAGNOSTIC**
RAPIDE

2



**RAPPORT**
INSTANTANÉ

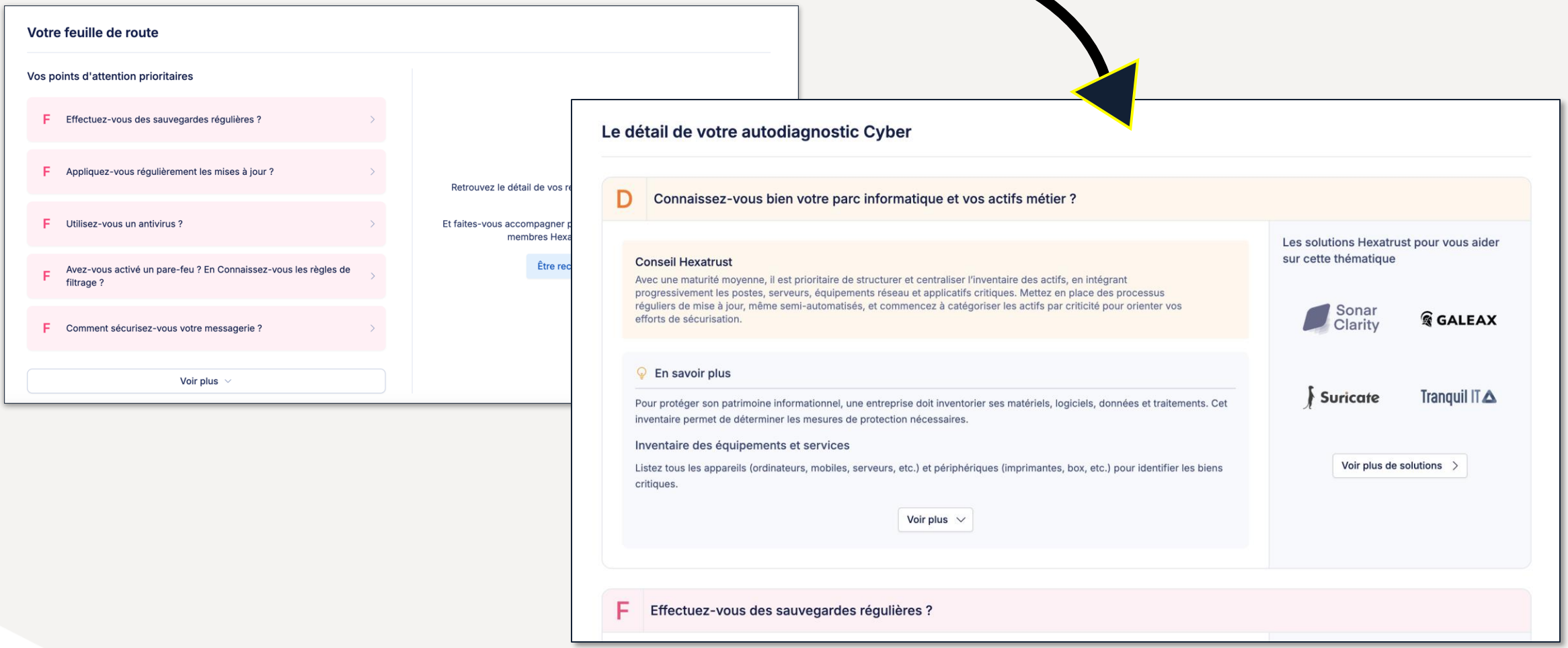
3

**ACCOMPAGNEMENT**
PERSONNALISÉ

L'Hexa Pres

L'UNION FAIT LA FORCE

# Le fonctionnement



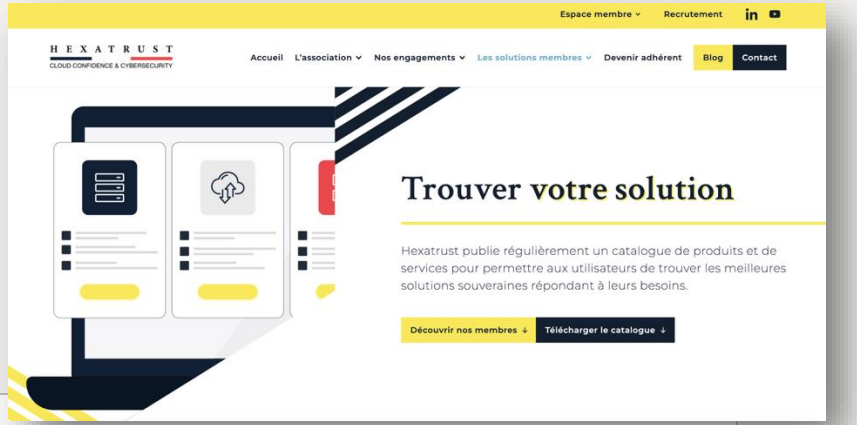

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

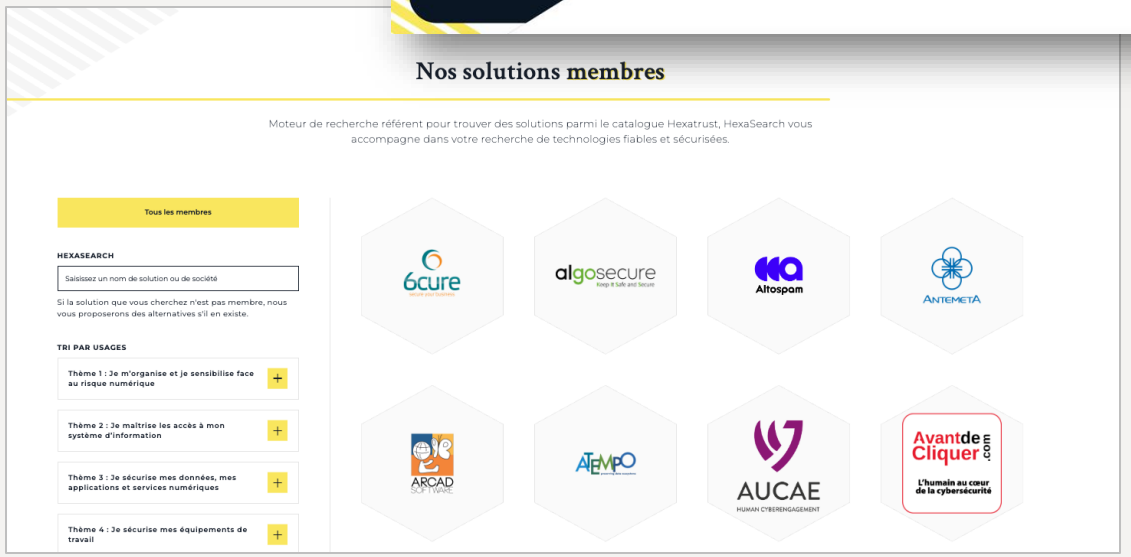
L'Hexa Pres

L'UNION FAIT LA FORCE

# L'HexaSearch

- Moteur de recherche pour trouver des solutions souveraines parmi le catalogue Hexatrust ;
- Trouver des alternatives françaises/européennes

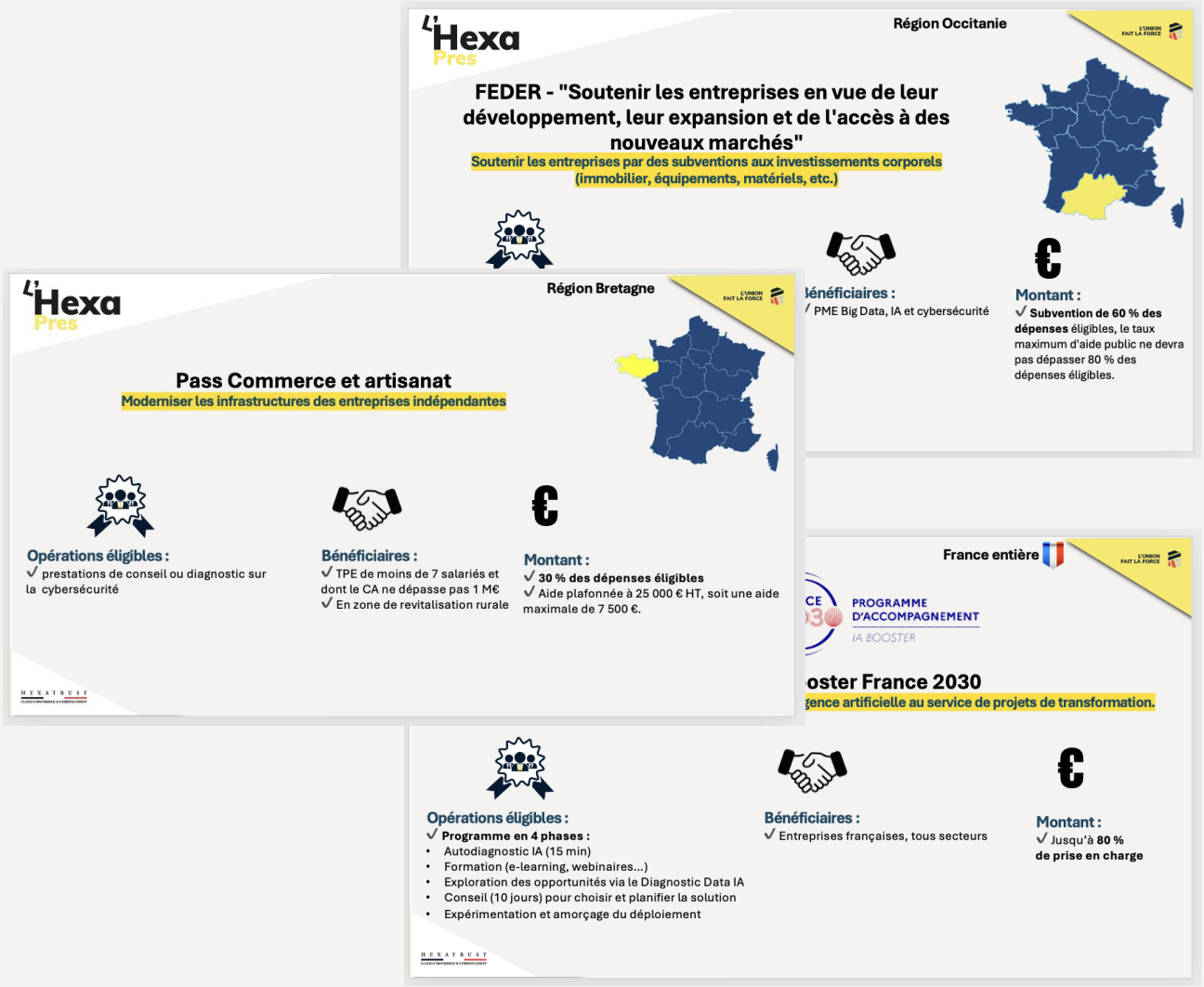



HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

# Guide d’aides Hexatrust

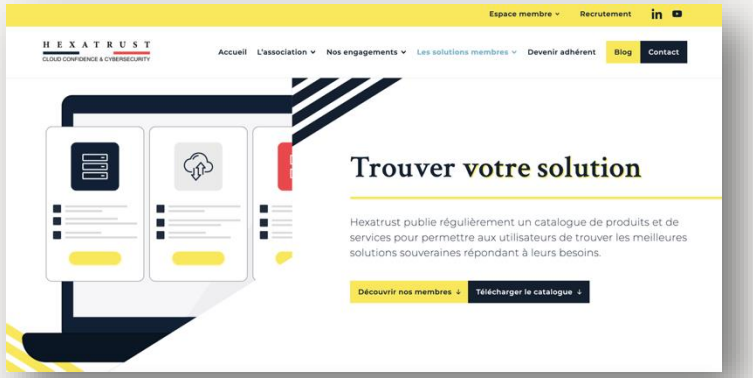
- Panorama des aides nationales et régionales financières pour renforcer sa sécurité
- Définit les opérations éligibles, les bénéficiaires, et les montants
- Tenu à jour annuellement
- Intégration des aides sur les enjeux IA



L'Hexa Pres

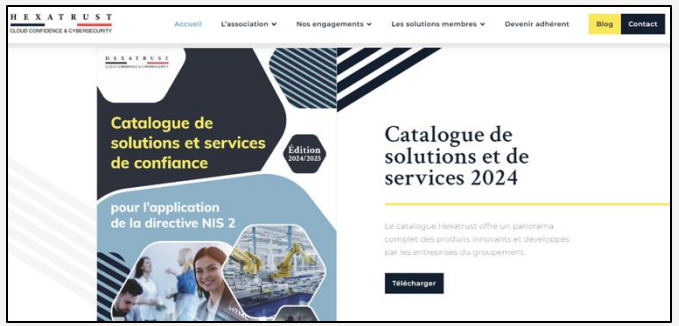
L'UNION FAIT LA FORCE

# Plus de ressources...




Trouvez le service ou le produit adapté à vos besoins grâce à notre annuaire


Améliorez votre connaissance des pratiques Zero Trust avec notre livre blanc




Découvrez nos solutions via notre catalogue de solutions à télécharger

Rendez-vous sur **www.hexatrust.com**

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

# LES UECC

- Sourcing : vitrine des solutions françaises et européennes
- Conférences, exercices de crises, workshop sur les enjeux d'aujourd'hui et de demain
- Echanges et networking


Rendez-vous sur **www.uecc-hexatrust.com**

L'UNION
FAIT LA FORCE

# Merci !

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

# Sources


9e baromètre de la cybersécurité des entreprises réalisé par le CESIN et OpinionWay.

Le Panorama de la cybermenace 2024 de l'Anssi

*Guide de l'ANSSI : La cybersécurité des systèmes industriels - méthode de Classification*

HexaDiag

HexaSearch

Les Universités d'été de la Cybersécurité et du Cloud de confiance (UECC)