EGERIE
INTEGRATED CYBERRISK MANAGEMENT

Avec EGERIE, les risques n'ont plus rien d'effrayant

www.egerie.eu

EGERIE
INTEGRATED CYBERRISK MANAGEMENT

APPROCHE DE LA CYBERSÉCURITÉ PAR L'ANALYSE DES RISQUES CYBER

Les Lundis de la Cybersécurité

14/06/2021

En partenariat avec :

MEDEF Hauts-de-France

Université de Paris

WWW.EGERIE.EU

CYBERSÉCURITÉ : UN SUJET STRATÉGIQUE

Les cyberattaques augmentent régulièrement en termes de fréquence, d'intelligence et d'impact sur les activités et la visibilité des entreprises.

> It takes 20 years to build a reputation and less than 5 minutes to ruin it. Let's think about that and you'll see your business differently " Warren Buffet.

Plan de relance :

1 milliard €

pour renforcer la filière cybersécurité

Source : Stratégie nationale de cybersécurité

En France, les attaques criminelles visant des OIV

x4 entre 2019 et 2020

Source : ANSSI

5200 milliards $

Coût de la cybercriminalité pour l'économie mondiale entre 2020 et 2025.

Source : ONU

En 2020 11% des attaques visaient des établissements de santé

Source : ANSSI

VOS ENJEUX CYBER

EGERIE
INTEGRATED CYBERRISK MANAGEMENT

Comment obtenir et communiquer une image claire de la posture de risque cyber de mon entreprise ?

Comment puis-je m ’assurer que la cybersécurité est une préoccupation de l’entreprise ?

Comment sensibiliser les décideurs et leur permettre de prendre les meilleures décisions budgétaires pour concilier cybersécurité et ROI ?

Comment gagner un temps précieux sur mes analyses de risques cyber ?

Comment vérifier que ma politique de cybersécurité est appliquée efficacement dans toute mon entreprise ?

Comment évaluer, gérer et surveiller des menaces en constante évolution ?

Comment anticiper les impacts d’une éventuelle cyberattaque ?

Comment mesurer l’efficacité de mes mesures de traitement du risque ?

LA PROBLÉMATIQUE ACTUELLE

- Une surface d'attaque qui croît proportionnellement à une digitalisation globale de plus en plus large et quasi anarchique.

- Le pilotage de la cyber reste encore majoritairement effectué par l'expertise et la technologie poussées par une innovation marketing et technologique débridée …

  - EDR, XDR, SOAR, ABAS, SAST, DAST, ….

… mais les attaques sont de plus en plus nombreuses et fructueuses.

COMMENT DÉCIDER?

Nouvelles vulnérabilités

Nouveaux risques

KPI & KRI

Gap Analysis

Quel plan de traitement ? Quelle priorité ?

PAR L'EXEMPLE

- https://tvmag.lefigaro.fr/le-scan-tele/insolite/2015/04/10/28009-20150410ARTFIG00214-les-mots-de-passe-de-tv5-monde-devoiles-sur-france-2.php

- **9 mai 2015 16h47: Un serveur de TV5Monde avait été piraté il y a quinze jours**

  - L'Agence nationale de sécurité des systèmes d'information (Anssi) avait prévenu la chaîne d'une utilisation frauduleuse d'un de ses serveurs, non protégé. «L'agence a récupéré le serveur qui avait été utilisé pour des actes malveillants. Depuis, on cherchait un prestataire pour un audit de sécurité sur ce point», a indiqué Jean-Pierre Verines, le directeur informatique de TV5Monde. Il a précisé disposer d'un «firewall» quasi neuf – «notre système de sécurité est plutôt situé dans la moyenne haute de ce qui peut se faire». (Source 20Minutes)


LE FIGARO.fr télé avec TV

Programme TV | Grille TNT | Miss France 2021 | Séries | People | Télé-réalité

Programme TV > Actu télé

Les mots de passe de TV5 Monde dévoilés sur France 2

Par Sarah Lecoeuvre | Mis à jour le 10/04/2015 à 18:27 / Publié le 10/04/2015 à 16:29

7 commentaires

LE SCAN TÉLÉ / VIDÉO - Peu après la cyberattaque, les téléspectateurs du *13 Heures* de la *Deux* ont pu apercevoir les codes liés aux réseaux sociaux de la chaîne francophone.

Pas très malin. Jeudi, les chaînes de télévision ont consacré une large page au piratage de l'antenne et des réseaux sociaux de TV5 Monde. France 2 a fait de même dans ses journaux télévisés. Mais, un détail semble avoir échappé aux équipes de rédaction du service public.

Alors que l'un des journalistes de TV5 Monde est interrogé par les équipes de France 2,

PILOTAGE PAR LE RISQUE

- Conformité n’est pas sécurité!

- L’analyse de risque **en continu** doit permettre d’évaluer régulièrement la posture de sécurité en fonction des changements environnants
  - Avancement des projets internes
  - Evolution de la menace
  - Evolution des vulnérabilités

- L’analyse de risque doit être au cœur du Programme Cyber pour donner de la visibilité aux organes décisionnaires

Pour quoi faire?

- OIV Industriel

- Nouvelle vulnérabilité découverte par l'ANSSI
  - Ancienne version de Windows
  - Communication aux OIV

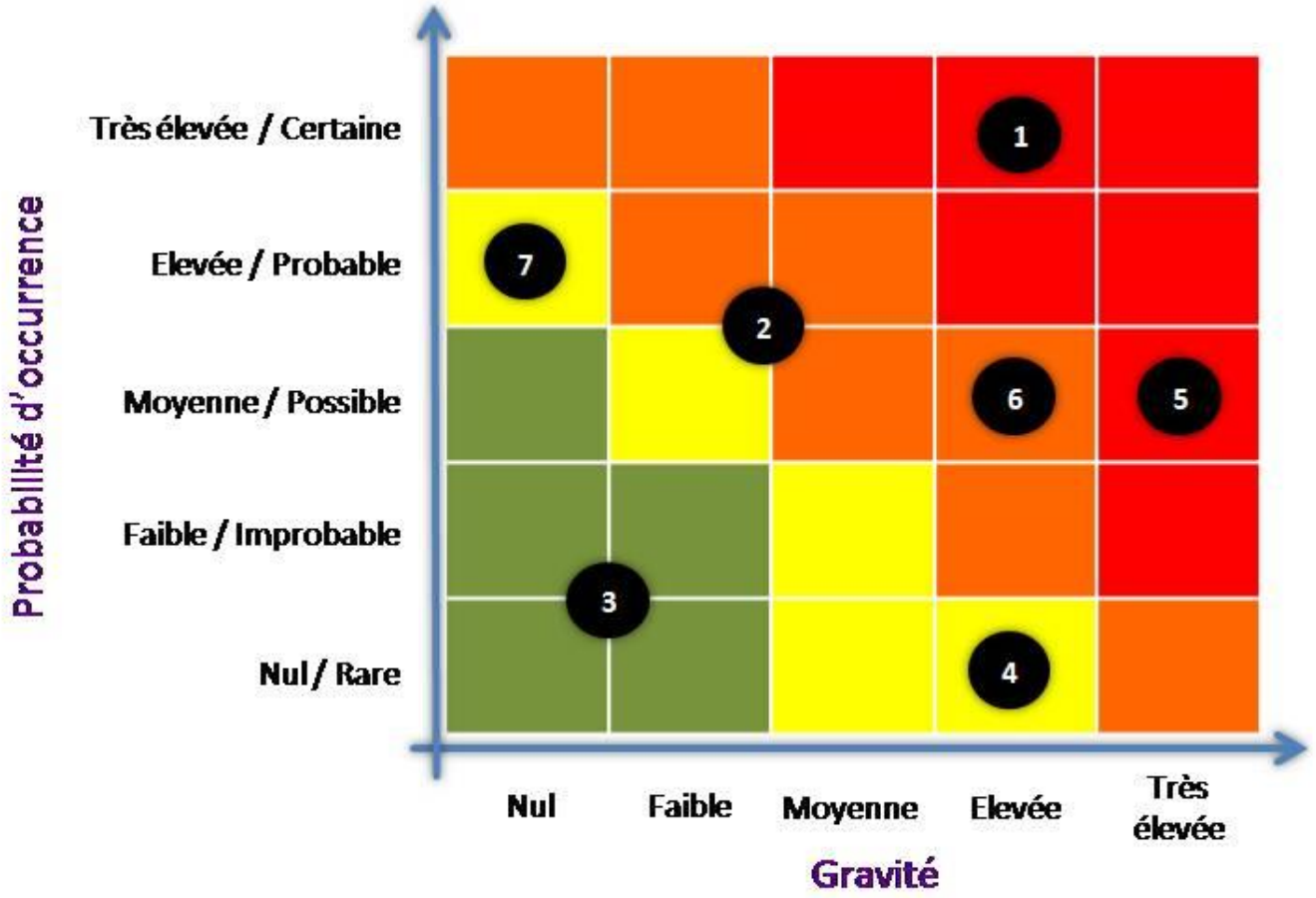
- Permettre de décider sur le plan de traitement

Pour quoi faire?

- 2017: Not Petya
  - Attaques utilisant une vulnérabilité connue

- De nombreuses entreprises industrielles touchées
  - Pourquoi leurs systèmes n'étaient-ils pas patchés donc vulnérables?
  - Divergence entre les métiers et la DSI
  - Impossibilité de prendre une décision basée sur des éléments tangibles:
    - Quel sera l'impact si je prends ne traite pas ce risque

Cartographier les risques



Catégorisation et évaluation des impacts

- impacts sur les missions et services de l'organisation
- impacts humains, matériels ou environnementaux
- impacts sur la gouvernance
- impacts financiers
- impacts juridiques
- impacts sur l'image et la confiance.

Evaluation de l'impact

NIVEAU DE L'ÉCHELLE	DÉFINITION
G5 – CATASTROPHIQUE	**Conséquences sectorielles ou régaliennes au-delà de l'organisation.** Écosystème(s) sectoriel(s) impacté(s) de façon importante, avec des conséquences éventuellement durables. Et/ou : difficulté pour l'État, voire incapacité, d'assurer une fonction régalienne ou une de ses missions d'importance vitale. Et/ou : impacts critiques sur la sécurité des personnes et des biens (crise sanitaire, pollution environnementale majeure, destruction d'infrastructures essentielles, etc.).
G4 – CRITIQUE	**Conséquences désastreuses pour l'organisation avec d'éventuels impacts sur l'écosystème.** Incapacité pour l'organisation d'assurer la totalité ou une partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. L'organisation ne surmontera vraisemblablement pas la situation (sa survie est menacée), les secteurs d'activité ou étatiques dans lesquels elle opère seront susceptibles d'être légèrement impactés, sans conséquences durables.
G3 – GRAVE	**Conséquences importantes pour l'organisation.** Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. L'organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans impact sectoriel ou étatique.
G2 – SIGNIFICATIVE	**Conséquences significatives mais limitées pour l'organisation.** Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. L'organisation surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 – MINEURE	**Conséquences négligeables pour l'organisation.** Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. L'organisation surmontera la situation sans trop de difficultés (consommation des marges).

Mesurer

- Evaluer le risque

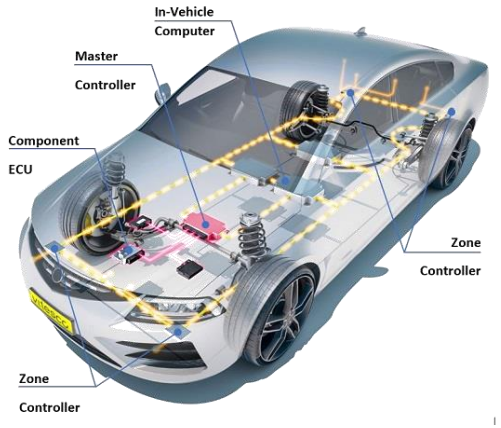
Score de risque sur un bien = (**Menace** + **Vulnérabilités**) x **Valeur du bien**
Menace = Evaluation de la Menace x Probabilité d' Ocurrence x Impact
Vulnérabilités = Sévérité des Vulnérabilités

- Quantifier: exemple méthode FAIRE

	Minimum	Average	Mode	Maximum
Primary				
Loss Events/Year	0.05	0.17	0.14	0.43
Loss Magnitude	$70,805	$393,005	$441,760	$784,037
Secondary				
Loss Events/Year	0.02	0.07	0.05	0.17
Loss Magnitude	$248,815	$3,689,381	$1,102,702	$17,564,462
Total Loss Exposure	$28,319	$316,229	$172,200	$1,908,713

Normes et méthodologies

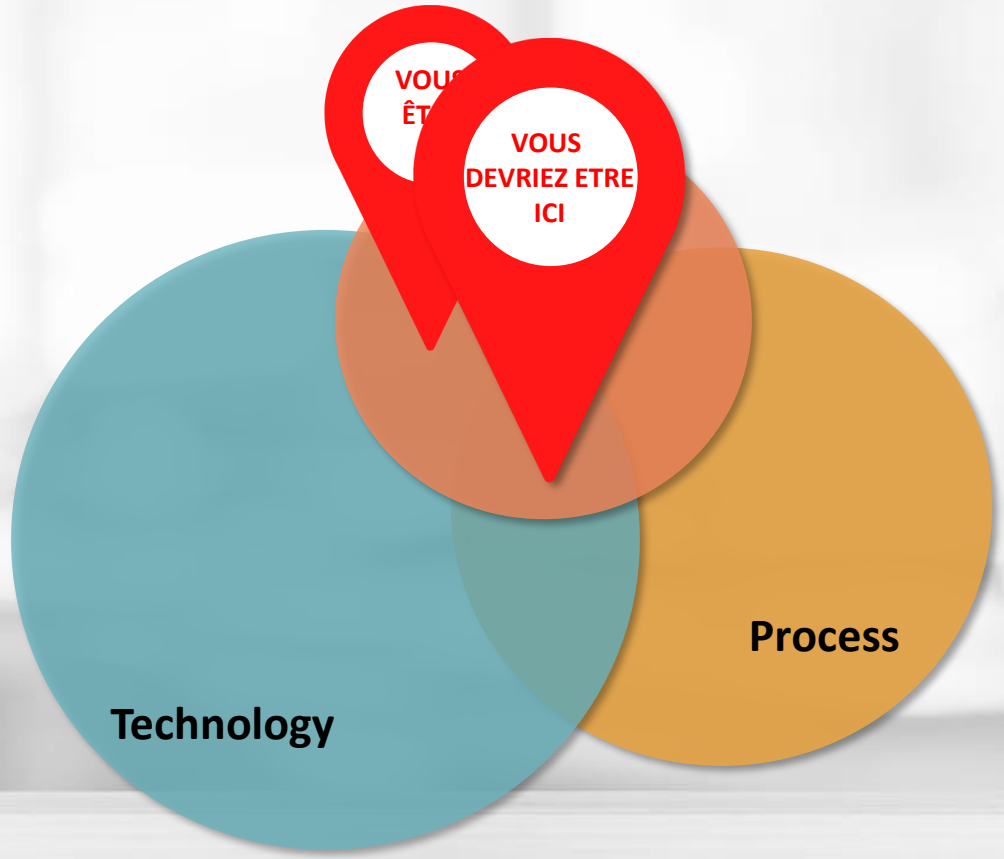
EBIOS RISK MANAGER



ISO 21434

International Organization for Standardization
ISO 27005 Risk Manager

LA NÉCESSITÉ D'UN CYBER PROGRAMME POUR ….



…. ANTICIPER LE RISQUE CYBER!

EGERIE
INTEGRATED CYBERRISK MANAGEMENT

RÉALISER DES ANALYSES DE RISQUES CYBER

Bénéficiez de la meilleure technologie pour réaliser et industrialiser vos analyses de risques

INTÉGRER LA CYBERSÉCURITÉ DANS LES PROJETS

Évaluez la cyber-criticité d'un projet afin d'adapter les mesures dans vos analyses de risques et suivre leur mise en œuvre dans le temps

ÉVALUER LA SÉCURITÉ DE SES SOUS-TRAITANTS ET FOURNISSEURS

Évaluez la posture de cybersécurité de vos sous-traitants et fournisseurs pour garantir la sécurité

MESURER LE NIVEAU D'APPLICATION DES MESURES DE CYBERSÉCURITÉ

Mesurez le déploiement de votre stratégie de cybersécurité et assurer la conformité

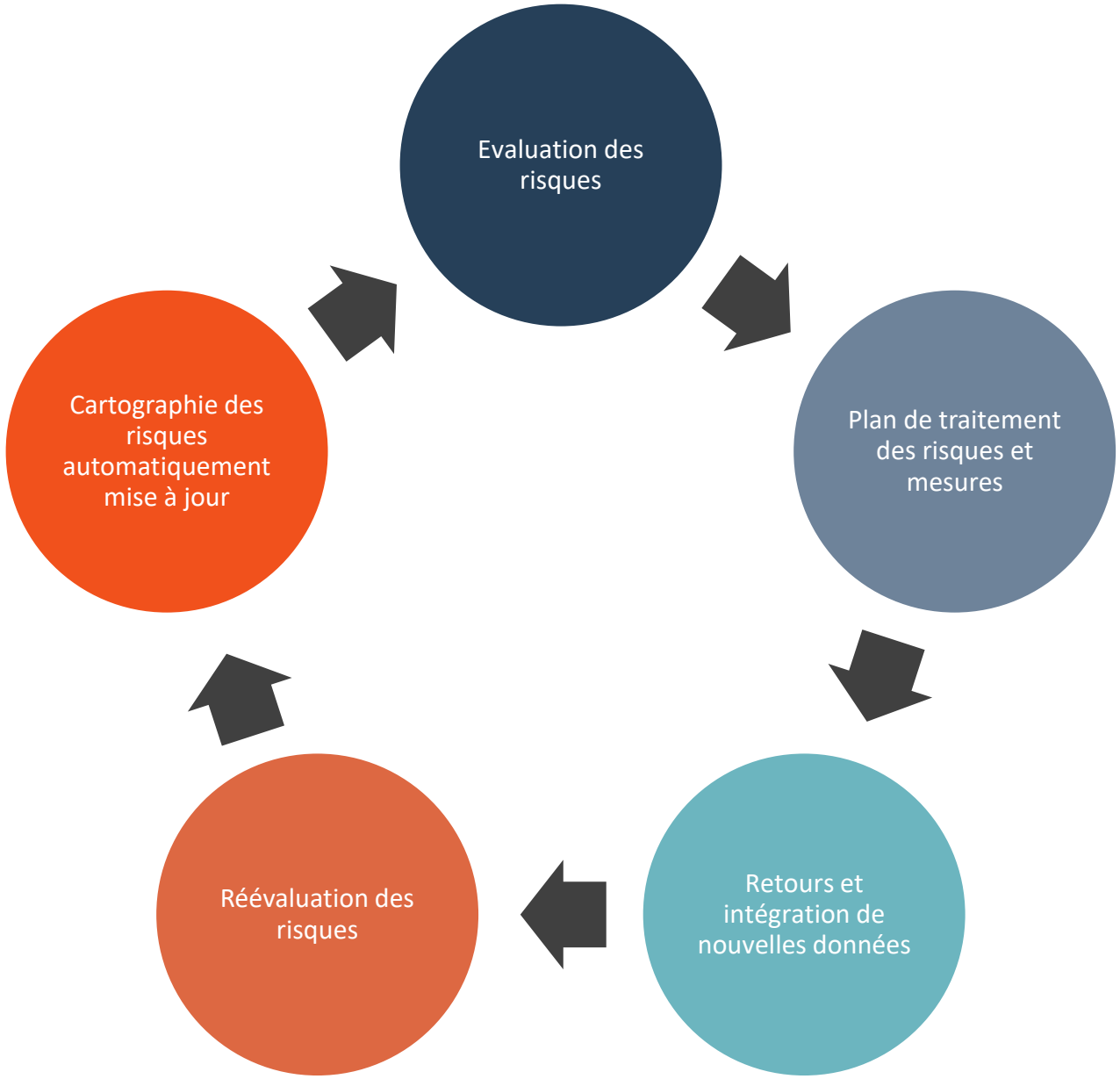
ÉVALUER LA MATURITÉ CYBER DES VEHICULES AUTONOMES ET CONNECTÉS

Évaluez la cybersécurité de véhicules entiers ou de composants connectés pour assurer la sécurité des automobilistes

GOUVERNER LA CYBERSÉCURITÉ ET LA SÉCURITÉ INDUSTRIELLE

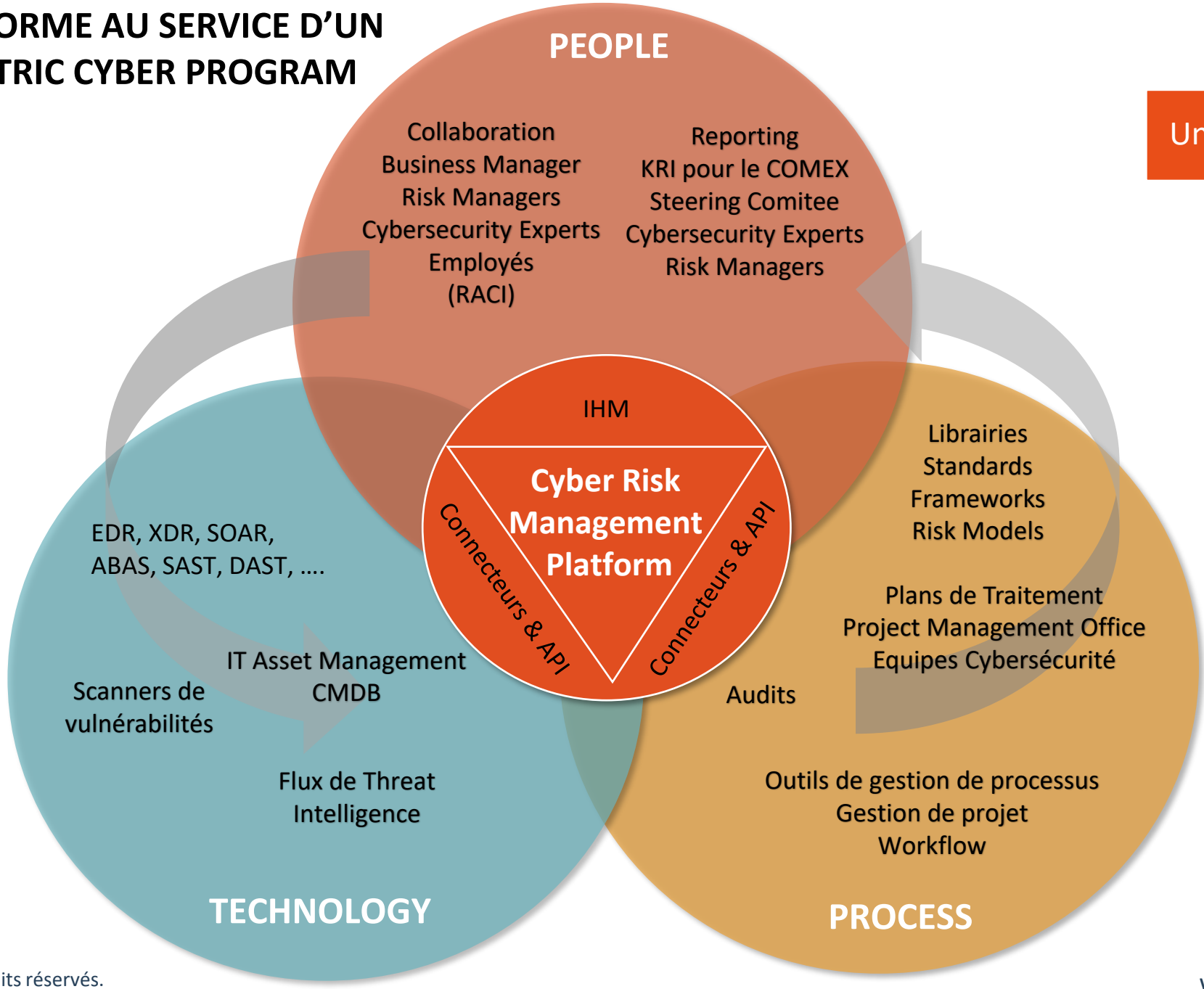
Évaluez les risques et les points faibles de vos sites industriels de production, obtenir de la visibilité sur votre niveau de maturité cyber et de sécurité et atteindre une gouvernance globale des risques

UN CERCLE VERTUEUX POUR SOUTENIR VOTRE STRATÉGIE DE CYBERSÉCURITÉ

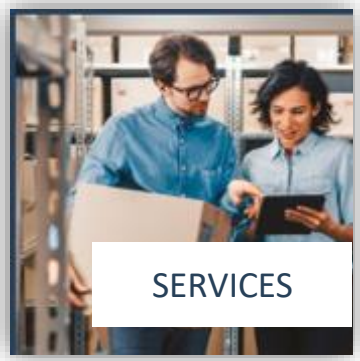


UNE PLATEFORME AU SERVICE D'UN PEOPLE CENTRIC CYBER PROGRAM

Une vision à 360 degrés



GOUVERNANCE DES RISQUES CYBER : UN DÉFI À RELEVER ENSEMBLE



EGERIE LAURÉATE DU GRAND DÉFI CYBERSÉCURITÉ

- Stratégie cyber portée au + haut niveau de l'Etat
  - Porté par le Secrétariat Général Pour l'Investissement
  - Rendre nos systèmes durablement résilients aux cyber-attaques
  - Garantir la maîtrise des technologies critiques par des acteurs français de confiance
  - Accélérer le développement de la filière

- Projet EGERIE de production d'analyses de risques dynamiques permettant un véritable pilotage en continu de la cybersécurité

- Proposer des analyses de risques cyber contextualisées
  - Permet d'élargir la surface des risques pris en compte et leur précision
  - Concaténation de différentes sources techniques

« Investir dans le développement de technologies de rupture et en favorisant l'émergence accélérée d'acteurs leaders dans leur domaine et pouvant prétendre à une envergure mondiale »

« C'est une innovation majeure qui permettra aux utilisateurs de gagner un temps précieux et un niveau de précision inégalé pour le pilotage de la performance de leur cybersécurité »

EGERIE : UNE SOCIÉTÉ VISIONNAIRE, EUROPÉENNE ET ENGAGÉE

+120 clients
Grands comptes du CAC40 et institutionnels en France et en Europe

+20 ans d'expertise
de la cybersécurité et de l'analyse de risques

+40%
CA **investi en R&D**

Une **plateforme logicielle collaborative** et agile permettant d'optimiser les analyses de risques

Un réseau de partenaires
en France et à l'international au cœur de notre stratégie

2 mentions **Gartner**
« Magic Quadrant for IT Risk Management » et « Vendor to Watch »

EGERIE **lauréate** du « **Grand Défi Cybersécurité** »

+350 consultants et experts
formés et certifies sur nos solutions

LA PLATEFORME LOGICIELLE EGERIE

- Une technologie d'**anticipation** des cyber menaces **collaborative**, **dynamique** et **automatisée**
- Permet d'**industrialiser** le **pilotage des risques cyber** et maîtriser sa **stratégie de sécurité**
- L'ADN d'EGERIE repose sur une stratégie de **communauté** et de **partage** d'expérience, de **référentiels** normatifs et réglementaires et de **bibliothèques**
- L'outillage EGERIE aide à la **conformité réglementaire et** permet aux **directions métiers** de devenir de **véritables acteurs de leur sécurité**
- On-boarding + rapide grâce à des **ambassadeurs** de l'**écosystème**

« En faisant le choix de partager, avec votre communauté, les informations produites au format EGERIE, vous devenez acteur de la meilleure stratégie de cybersécurité pour votre métier »

L'aspect centralisateur, multi-utilisateurs et multi-méthodologies de la plateforme permet de capitaliser sur les analyses réalisées et les données obtenues

EGERIE Risk Manager est la 1ère solution labellisée EBIOS Risk Manager par l'ANSSI

EGERIE
INTEGRATED CYBERRISK MANAGEMENT

EGERIE

INTEGRATED CYBERRISK MANAGEMENT

EGERIE TOULON

Siège social :
44 boulevard de Strasbourg – 83000 Toulon – France
Tél. : +33 (0)4 94 63 81 09
contact@egerie.eu

EGERIE PARIS

49 avenue d'Iéna – 75016 Paris – France
contact@egerie.eu

EGERIE LONDRES

sales@egerie.uk

www.egerie.eu