FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES


2009


2010


2011


2012


2013


2014


2015


2016


2017

2018

FRC
www.frc.alsace


12ème FORUM DU RHIN SUPÉRIEUR
SUR LES CYBERMENACES
LA GENDARMERIE & LES OFFICIERS DE LA RÉSERVE CITOYENNE
MIEUX CONNAÎTRE LES RISQUES
POUR MIEUX LES PRÉVENIR
PROGRAMME
FRC 2019
12ème édition
WWW.FRC.ALSACE
@CYBERMENACES

FRC 2019 : ANIMATION

Monsieur Gilbert GOZLAN

Directeur Délégué Sécurité - La Poste Nord & Est
Président de l'association AD Honores Réseau Alsace
Colonel (RC) de la gendarmerie nationale

FRC 2019 : DISCOURS D ’OUVERTURE

Monsieur Thierry ROGELET

Directeur de l’enseignement et de la recherche
Représentant de Monsieur GIRARD Directeur de l’ENA

FRC 2019 : DISCOURS D ’OUVERTURE

Général Marc CLERC

Commandant Adjoint de la région de gendarmerie Grand Est,
Commandant le groupement de gendarmerie départementale du Bas-Rhin

FRC 2019 : DISCOURS D ’OUVERTURE

Monsieur Jean-Luc HEIMBURGER

Président CCI Alsace Eurométropole

FRC 2019 : PROGRAMME

MIEUX CONNAITRE LES RISQUES POUR MIEUX LES PREVENIR

13h00 — ACCUEIL DES PARTICIPANTS

13h30 — DISCOURS D'OUVERTURE

Colonel Marc CLERC
Commandant adjoint de la région de gendarmerie du Grand Est.
Commandant le groupement de gendarmerie départementale du Bas-Rhin.

Monsieur Jean-Luc HEIMBURGER
Président de la CCI Alsace Eurométropole.

Monsieur Jean-Luc MARX
Préfet du Bas-Rhin.
Préfet de la région Grand Est.

■ Animation
Monsieur Gilbert GOZLAN
Directeur Délégué Sécurité - la Poste Nord & Est.
Président de l'association AD HONORES Réseau Alsace.
Colonel (RC) de la gendarmerie nationale.

14h00 — CONFERENCES PLENIÈRES

PANORAMA DES RISQUES CYBER

Colonel Philippe BAUDOIN
Officier Adjoint du Commandement de la région de gendarmerie du Grand Est - Zone de Défense et de Sécurité Est.
Ancien Conseiller au Ministère de l'Intérieur à la Mission de Lutte contre les Cybermenaces.

PROSPECTIVES ET ENJEUX

Général d'armée (2S) Marc WATIN-AUGOUARD
Ancien inspecteur général des armées-gendarmerie,
Directeur du Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN).

15h00 — TABLE RONDE #1

MIEUX CONNAITRE LES RISQUES CYBER

La cyber assurance, le risque perçu par l'assureur.
Monsieur Michel SCHIRRA
Directeur technique des assurances de biens et de responsabilité du Groupe ROEDERER.

La chasse aux vulnérabilités : le Bug Bounty.
Monsieur Jean Bernard YATA
RSSI du Groupe FM Logistic.

Evaluer ses risques : la méthode EBIOS.
Monsieur Michel ROCHELET
Référent ANSSI Région Grand-Est.

16h00 — PAUSE

16h30

DÉMONSTRATION OPÉRATIONNELLE :

Peut-on encore faire confiance aux images ?
Messieurs Kevin OUAHMAD et Gauthier WAGNER
Etudiants de l'Ecole Nationale Supérieur d'Ingénieurs Sud Alsace (ENSISA), à l'Université de Haute Alsace (UHA).

17h00 — TABLE RONDE #2

LA SECURITE DU SITE INTERNET DE L'ENTREPRISE

Le cambriolage numérique : actualisation.
Lieutenant Olivier BROGGI
Commandant la division délinquance, économique, financière et numérique de la Section de Recherches de Strasbourg.

Adjudant Elena VALLEJO
Enquêtrice délinquance financière de la Section de Recherches de Strasbourg.

Les enjeux des PME en matière de sécurisation des paiements électroniques.
Monsieur Eric WIES
Chef d'escadron (RC) de la gendarmerie nationale.
Ingénieur réseau INSEE.

L'hébergement du site : le cloud public.
Monsieur Thomas VIERLING
Directeur de LPB Conseil.

18h00 — CONCLUSION DE LA JOURNÉE

Colonel Marc CLERC et Monsieur Gilbert GOZLAN

18h30 — COCKTAIL

Salle de conférence de l'ENA

FRC 2019 : NOS PARTENAIRES

FRC 2019 : NOS PARTENAIRES

CCI ALSACE EUROMÉTROPOLE

FRC 2019 : NOS PARTENAIRES

FRC 2019 : NOS PARTENAIRES

CLUSIR EST

FRC 2019 : NOS PARTENAIRES

FRC 2019 : NOS SPONSORS

Atheo

INGENIERIE | HUMAN INSIDE

FRC 2019 : NOS SPONSORS

BANQUE POPULAIRE
ALSACE LORRAINE CHAMPAGNE

FRC 2019 : NOS SPONSORS

CRCC
COMPAGNIE REGIONALE DES COMMISSAIRES AUX COMPTES
COLMAR

Partenaire de la marque Alsace

FRC 2019 : NOS SPONSORS

LCR

LES CONSTRUCTEURS REUNIS

FRC 2019 : NOS SPONSORS

SOCIETE GENERALE

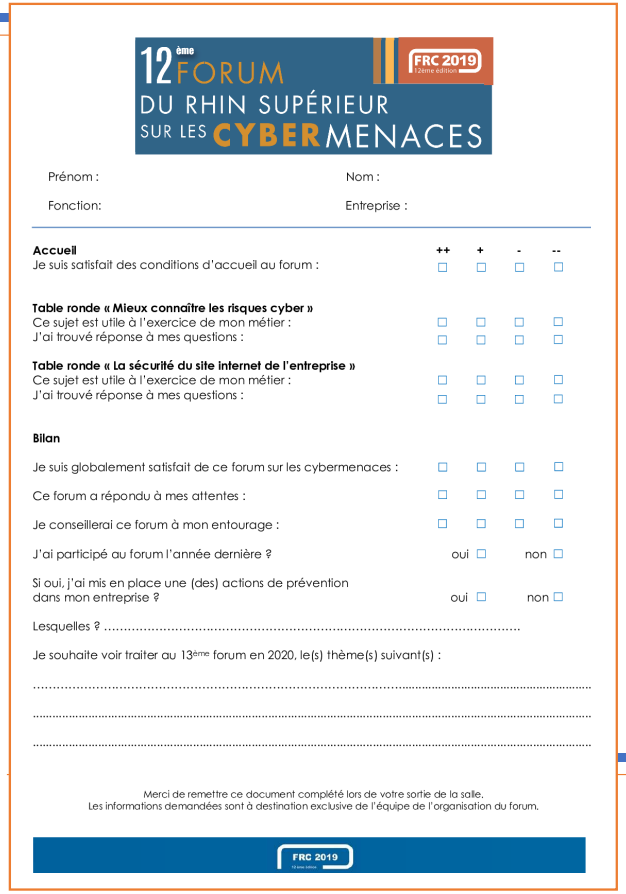
La Gendarmerie, la RC & AD Honores

FRC 2019 : NOTRE OBJECTIF

Connaître et partager les enjeux

Adopter et faire adopter les bons comportements et les bonnes actions à mettre en œuvre

FRC 2019 : QUESTIONNAIRE



12ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

FRC 2019 12ème édition

Prénom : Nom :

Fonction: Entreprise :

	++	+	-	--
Accueil				
Je suis satisfait des conditions d'accueil au forum :	☐	☐	☐	☐
Table ronde « Mieux connaître les risques cyber »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Table ronde « La sécurité du site internet de l'entreprise »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Bilan				
Je suis globalement satisfait de ce forum sur les cybermenaces :	☐	☐	☐	☐
Ce forum a répondu à mes attentes :	☐	☐	☐	☐
Je conseillerai ce forum à mon entourage :	☐	☐	☐	☐

J'ai participé au forum l'année dernière ? oui ☐ non ☐

Si oui, j'ai mis en place une (des) actions de prévention dans mon entreprise ? oui ☐ non ☐

Lesquelles ? .....

Je souhaite voir traiter au 13ème forum en 2020, le(s) thème(s) suivant(s) :

.....

.....

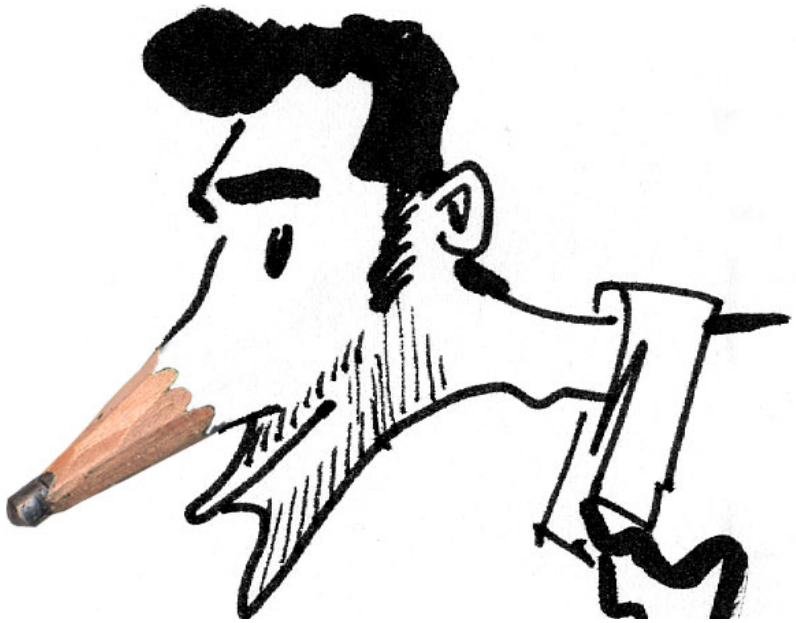
.....

Merci de remettre ce document complété lors de votre sortie de la salle.
Les informations demandées sont à destination exclusive de l'équipe de l'organisation du forum.

FRC 2019

FRC 2019 : NOTRE DESSINATEUR

Laurent SALLES



Code wifi : Identifiant cyber

Mot de passe

mRd74hD6

Nom cyber

Profil EVENEMENT

N’hésitez pas à consulter notre site :

www.frc.alsace

Et nous rejoindre sur Twitter :

@cybermenaces #FRC2019

FRC 2019 : Conférence Plénière

Panorama des Risques cyber

Colonel Philippe BAUDOIN

Officier Adjoint du Commandement de la Région de Gendarmerie Grand-Est – Zone de défense et de Sécurité Est

Ancien Conseiller au Ministère de l'Intérieur à la Mission de Lutte contre les Cybermenaces

Rapport sur l'état de la menace lié au numérique

3ème édition établie par l'ensemble des services du ministère de l'Intérieur, sous la coordination de la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC)

- Qui ce document concerne-t-il ? De quoi parle-t-il ?
  - Les enjeux stratégiques
    - Enjeux sociétaux, économiques, juridiques, technologiques et de coopération
  - Les usages et phénomènes constatés
    - Usages & vecteurs de diffusion des attaques cyber
    - Attaques contre les systèmes d'information & utilisation d'Internet à des fins criminelles
    - Perception de la menace
  - Les actions du ministère de l'Intérieur
  - A quels défis faut-il se préparer ?

- Quelle période couvre-t-il ? Comment a-t-il été réalisé ?
- Quelle est la volumétrie des menaces liées au numérique ?
- Où consulter/télécharger ce rapport

https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019 ou site de la documentation française (rapports publics)

Etat de la menace lié au numérique

Les enjeux stratégiques

Enjeux sociétaux :

- Poser des règles de fonctionnement claires et équilibrées pour accompagner la transformation numérique
- Lutte contre les contenus illicites et terroristes ;
- Relations avec les plateformes numériques

Enjeux économiques: menaces insidieuses pour toutes entités

- Ciblage « supply chain » (prestataires fournisseurs consultants)
- Se protéger : dispositif prévention & gestion des risques
- Développement marché des de cybersécurité - assurances
- Contre-ingérence économique
  - La concomitance entre attaque informatique et faits plus traditionnels n'est pas rare
  - Être très attentif lorsque l'entreprise affronte un moment clé de son fonctionnement

Etat de la menace lié au numérique

Les enjeux stratégiques

Enjeux juridiques et normatifs :

- Effets RGPD, LPM 2019-2025
- Loi programmation Justice (enquêtes sous pseudonyme…)
- Projets de loi : contenus haineux

Enjeux technologiques :

- Anonymisation / Chiffrement

Enjeux de coopération :

- À l'international : Afrique
- En interne : rôle du Parquet F1 de TGI de Paris

Etat de la menace lié au numérique

Les usages et phénomènes constatés

Usages :

- *Smartphones*/plateformes multi-usages :
  - App malveillantes ou fausses, mAPT
- Objets connectés, 5G → facteurs de vulnérabilité

Phénomènes :

- Ingénierie sociale sociale / *Typosquatting*
- *Cybercrime* as a service

Etat de la menace lié au numérique

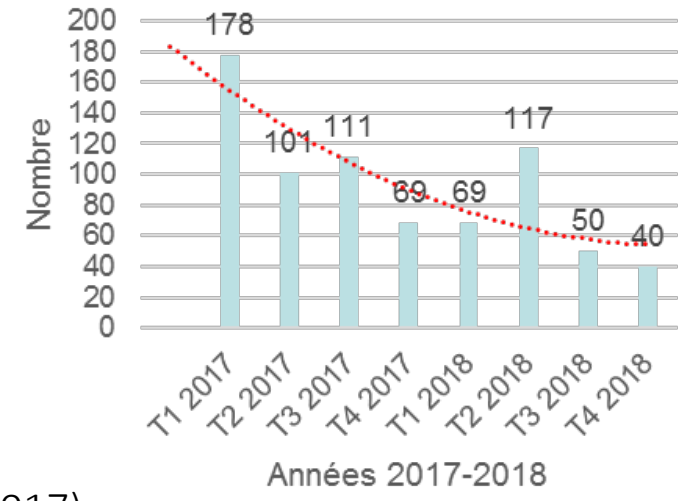
Les usages et phénomènes constatés

Phénomènes :

- Ingénierie sociale sociale / *Typosquatting*
- *Cybercrime* as a service
- Attaques sur les systèmes d'information :
  - Attaques ciblées – *spear phishing*
  - Vol de données : ex. « Rex Mundi »
  - Dénis de service (hacktivistes…)
  - Défiguration
- Délinquance liée aux cryptoactifs

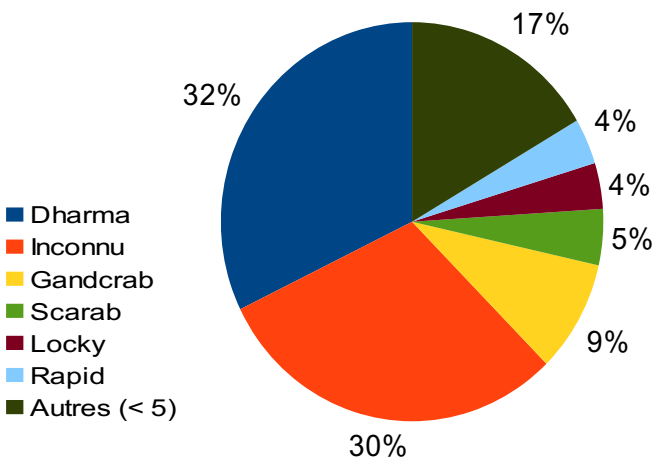
→ phénomène du *cryptojacking* (depuis fin 2017)

Défigurations – Source ANSSI



Etat de la menace lié au numérique

Les usages et phénomènes constatés



Occurrence des cryptolockers : Analyse des plaintes pour rançongiciel GN-C3N-01/19

Phénomènes :

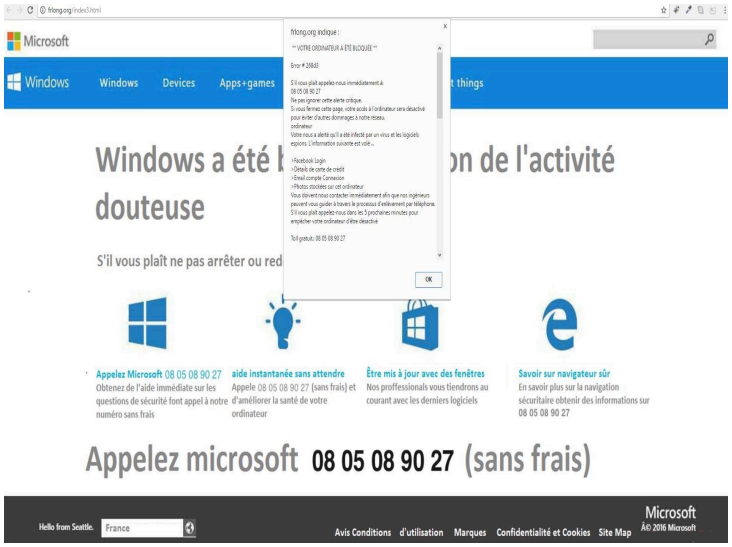
- Rançongiciels (*principale menace*) :
  - Après 2017 (*Wannacry*, *Notpetya*), ces attaques persistent
  - Toutefois **changement de stratégie** des cybercriminels : autrefois indiscriminées, les attaques par rançongiciel semblent davantage **cibler les grandes entreprises ayant la capacité de payer des rançons très élevées** (ex. Altran, Fleury Michon, …)
  - Mais aussi les hôpitaux et les collectivités territoriales
  - Souches : PyLocky (déchiffreur STSI²) … Ryuk, LockerGoga…
  - Peu de plaintes… Signalements
- Marchés criminels en ligne – Darknets, environnement en pleine évolution :
  - Après *Alphabay* et *Hansa Market*, une opération française avec la « Main Noire »

Etat de la menace lié au numérique

Les usages et phénomènes constatés

L'utilisation d'Internet à des fins criminelles :

- Les escroqueries:
  - Faux ordres de virements internationaux (FOVI) : en net recul
  - Faux investissements sur le FOREX ou au placements indexés sur les cryptomonnaies
  - Faux supports techniques : essor en 2018 et arrestations
  - Autres : RGPD, *Scam Romance,* chantage à la webcam prétendument piratée (*Sextorsion*)



Etat de la menace lié au numérique

Les usages et phénomènes constatés

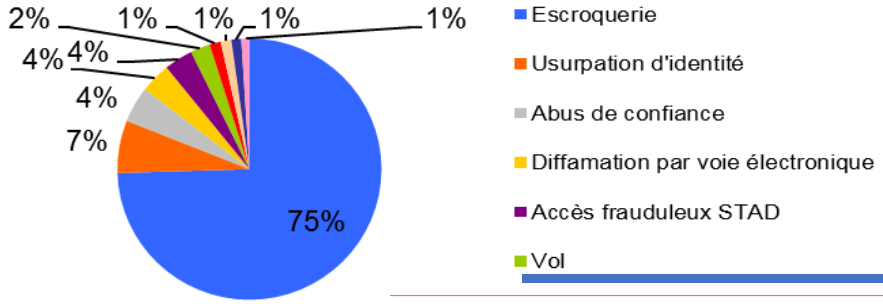
L'utilisation d'Internet à des fins criminelles :

- Les escroqueries
- La lutte contre la fraude à la carte bancaire:
  - attaques de distributeurs par la technique dite du « *jackpotting* »
- La lutte contre la pédopornographie et l'exploitation sexuelle de mineurs en ligne :
  - Lutte contre le «live streaming» et le «grooming» (enq. sous pseudo.)
  - Arrestation d'un administrateur français du plus ancien forum pédopornographique du darknet

Etat de la menace lié au numérique

Les usages et phénomènes constatés

- Perception de la menace :
  - Atteintes aux STAD : 9.970 infractions enregistrées en 2018 par les services (plaintes) – Non représentatif du phénomène
  - Harcèlement en ligne : x 2 entre 2016 et 2018 (627)
  - Infractions à la loi Informatique et Libertés, stable en 2016 et 2017, est en hausse en 2018 (+14%), année du RGPD.
  - Vision statistique des infractions constatées (Gendarmerie)



- Plateforme PERCEVAL:
  - accessible en ligne, via service-public.fr, vise à recueillir et analyser le contentieux massif des **usages frauduleux de carte bancaire**

Etat de la menace lié au numérique

Les actions du ministère de l'intérieur

- Prévention :
  - Permis Internet 2 Millions d' élèves
  - Sensibilisation économique – DGSI (74 000 auditeurs)
  - Nomination d'un délégué à la protection des données au MI
- Investigation :
  - Capacité à bien accueillir les victimes
  - Schéma général organisation : réseau territorial piloté en central
  - DGSI : au sein de la DT, un département cyber et STNCJ
- Innovation :
  - Les **partenariats public-privé** (Groupe de contact permanent, Comité stratégique de filière industries de sécurité…)
  - La transformation numérique : Plateforme de signalement des violences sexuelles et sexistes, Brigade numérique de la G.N. …

L'appréhension des **phénomènes de masse** : THESEE (escroq. en ligne)

Aide à la remédiation : GIP ACYMA *cybermalveillance* - implication du MI

Etat de la menace lié au numérique

À quels défis faut-il se préparer ?

Sur les réponses :

- Souveraineté numérique et maîtrise des technologies clés
- Prise de conscience du risque cyber: citoyens, entreprises, collectivités locales
- Esprit du continuum de sécurité : « personne ne laisse sa porte ouverte »
- Dépôt de plainte : démarche positive et vertueuse pour tous,

(reconnaissance de la victime et préjudice, renseignement criminel cyber, prévention ciblée) a minima signalement

- Prévention sur les territoires

Sur les publics :

- Grands évènements = surface d'attaque (JO 2024…)
- Protection des espaces intelligents : défi en raison des diversité des organisations, de l'hétérogénéité des niveaux de sécurité…

L'Etat ne peut faire seul, les entreprises non plus, établir la confiance et construire ensemble

Questions ?


CYBERMENACES
COMMENT PROTÉGER
VOTRE ENTREPRISE ?
TIONALE - SCÈNE CYBERCRIME - GENDAR
GENDARMERIE NATIONALE - SCÈNE CYBERCRIM
Retrouvez-nous
sur les réseaux sociaux
Twitter® : @Gendarmerie
Facebook® : gendarmerienationale
Instagram® : www.instagram.com/gendarmerie_nationale_officiel/
www.gendarmerie.interieur.gouv.fr
MINISTÈRE
DE
L'INTÉRIEUR

FRC 2019 : Conférence Plénière

Prospectives et enjeux

Marc WATIN-AUGOUARD
Général d'armée (2S)

Ancien inspecteur des armées-gendarmerie
Directeur du Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN)

FRC 2019 : Table ronde #1

Mieux connaître les risques cyber

Table ronde #1 : Mieux connaître les risques cyber

Monsieur Michel SCHIRRA

Directeur technique des assurances de biens et de responsabilité du Groupe ROEDERER

Monsieur Jean-Bernard YATA

RSSI du Groupe FM Logistic

Monsieur Michel ROCHELET

Référent ANSSI Région Grand-Est

Mieux connaître les risques cyber

Monsieur Michel SCHIRRA

La cyber assurance,
le risque perçu par l'assureur

Sommaire

- Une préoccupation partagée
- Un risque spécifique à plus d'un titre
- Le contrat d'assurance Cyber
- Comment les assureurs appréhendent-ils le risque ?
- Pour quel coût ?

Risque

Une préoccupation partagée

1. Les entreprises

"Les entreprises françaises sont de plus en plus préoccupées par la fréquence et la gravité croissante des incidents cyber, les plaçant ainsi pour la première fois en tête du Top 10 du classement des risques en France" - *(Corinne Cipière, CEO d'AGCS France)* :

CLASSEMENT 2019	POURCENTAGE	CLASSEMENT 2018
1 - Incidents cyber	41 %	2 (46) %
2 - Interruptions d'activités	40 %	1 (47) %
3 - Incendie, explosion	29 %	= (21 %)
4 - Catastrophes naturelles	28 %	= (21 %)
5 - Évolutions législatives et réglementaires	26 %	4 (21 %)
6 - Évolutions de marchés	18 %	= (18 %)
7 - Nouvelles technologies	18 %	8 (14) %
8 - Atteinte à la réputation	12 %	9 (13) %
9 - Défaillances de qualité	12 %	7 (16) %
10 - Vol, fraude et corruption	10 %	9 (13) %

Participants = 86 - Réponses = 106 - Les chiffres représentent un pourcentage de toutes les réponses. Plus d'un risque et d'une industrie pouvaient être sélectionnés. Les chiffres ne totalisent pas 100 % car 3 risques pouvaient être sélectionnés - *Source : Allianz Global Corporate & Specialty.*

2. Les assureurs

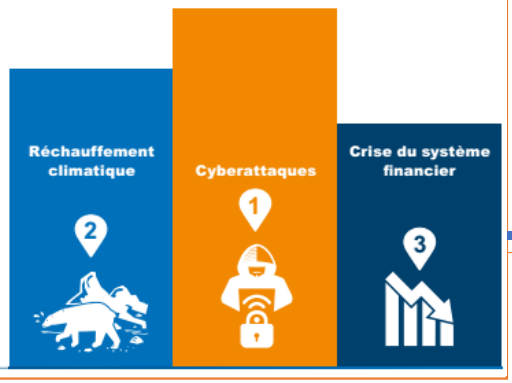
"Quand on regarde l'évolution des risques entre 2018 et 2019, les risques technologiques restent les plus élevés. Le risque cyber, en particulier, reste le Ier risque selon les assureurs et les réassureurs français"

- Bernard Spitz,
Président de la Fédération française de l'assurance (FFA)

Fédération Française de l'Assurance

Source : FFA - Février 2019

BAROMÈTRE 2019 DES RISQUES ÉMERGENTS POUR L'ASSURANCE - Risques à horizon 5 ans %



Risque

Un risque spécifique à plus d'un titre

Des produits dédiés à la couverture du risque cyber ont été développés depuis près de vingt ans aux États-Unis, et depuis moins de dix ans en France.

Aujourd'hui, le marché mondial de l'assurance cyber est estimé entre 3 et 3,5 milliards d'USD. Le marché américain capte 85 à 90 % de ces primes. L'Europe, elle, ne représente encore que 5 à 9 % de ce marché, soit un montant maximum de 255 millions d'euros (300 millions de dollars) de primes, sur lesquels la France ne représente que 40 millions d'euros.
En France, et plus largement en Europe, le marché de l'assurance cyber demeure embryonnaire.

C'est donc une formidable opportunité pour les assureurs, en même temps qu'un immense défi.

Risque

Et, pour les assureurs, spécifique à plus d'un titre

1ère difficulté : la capacité du marché de l'assurance

Pour qu'un risque soit assurable, il faut que les pertes anticipées soient inférieures à la capacité disponible des assureurs pour les couvrir.

Le coût global maximal des incidents cyber est demeuré jusqu'à présent très inférieur à celui d'autres grands risques et de nombreuses catastrophes naturelles en particulier : le coût global de l'ouragan Katrina de 2005, par exemple, a été estimé à plus de 80 Mds d'USD 2016, dont environ 40 Mds étaient assurés.

Lloyd's of London a présenté le scénario d'attentat de grande ampleur qu'elle envisage le plus probable dans sa dernière étude sur les cyber-risques : l'attaque d'un prestataire de cloud. Lloyd's en estime les pertes dans une fourchette allant de 15 à121 milliards d'USD, pour une moyenne évaluée à 53 milliards d'USD.

Risque

Et, pour les assureurs, spécifique à plus d'un titre

2ème difficulté : l'interdépendance

L'interdépendance des systèmes informatiques et des acteurs économiques multiplie les probabilités de propagation de certains types d'incidents cyber.

Exemple : le logiciel malveillant NotPetya, qui s'est servi de la procédure de mise à jour d'un logiciel de comptabilité ukrainien pour infecter diverses cibles en Ukraine, dont l'aéroport de Kiev ainsi que le système de surveillance des radiations de la centrale nucléaire de Tchernobyl, avant de contaminer la Russie, le Royaume-Uni, la Norvège, les Pays-Bas ou la France, le 27 juin 2017, seulement cinq heures après la première détection du virus.

La suprématie de certains systèmes d'exploitation (comme Microsoft Windows) rend de nombreux ordinateurs/systèmes vulnérables au même incident.

Risque

Et, pour les assureurs, spécifique à plus d'un titre

3ème difficulté : la faiblesse des données statistiques

Pour être assurables, les pertes associées à un risque donné doivent être estimées et modélisées grâce à l'analyse de séries historiques d'événements passés.

4ème difficulté : la difficulté de l'évaluation des enjeux

On peut mesurer les coûts directs (coût de restauration des données ou du système d'information) et les coûts induits (pertes d'exploitation) mais comment mesurer les impacts indirects ou d'image ?

Risque

Et, pour les assureurs, spécifique à plus d'un titre

5ème difficulté : la difficile analyse du risque

Une couverture optimale supposerait une expertise cyber pointue de la part de l'assureur et une fine connaissance de l'entreprise cliente.
Or, force est de constater que ni l'une ni l'autre ne sont toujours présente.

Les entreprises peuvent aussi être réticentes à partager des informations parfois sensibles, stratégiques ou confidentielles.

Risque

Et, pour les assureurs, spécifique à plus d'un titre

Le positionnement de son transfert s'inscrit en marge de garanties existantes :

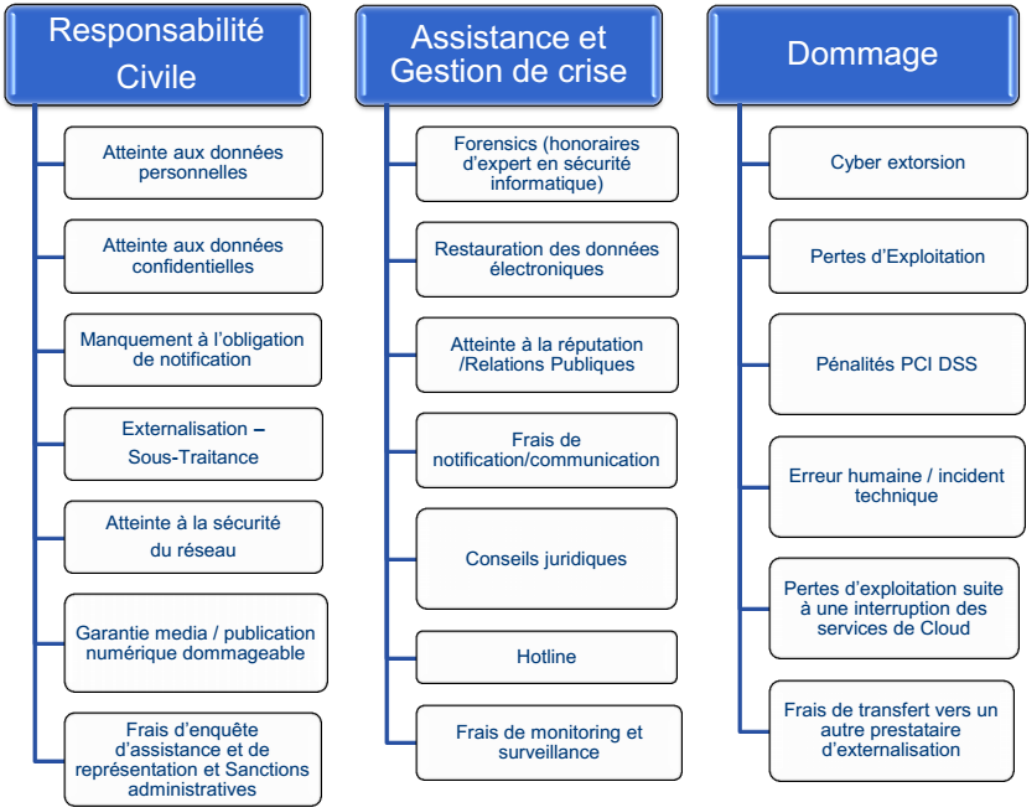
- **(FFA), MATRICE SYNTHÉTIQUE :**
  - Faits générateurs
  - Conséquences dommageables
  - Garanties

CONSÉQUENCES	ÉVÈNEMENTS / FAITS GÉNÉRATEURS				
	Dommages matériels		Dommages immatériels		
	Dommages matériels accidentels : Incendie, Dégats des eaux	Dommages matériels par malveillance : Incendie volontaire, Vol	Malveillance informatique (cyber) : Virus, Cryptologiciels	Autres dommages : Erreur humaine	Fraude : Faux ordres de virement, Cyberfraude
	GARANTIES				
Actifs de l'Entreprise (Matériels / Financiers)	Contrats Dommages aux biens (multirisques et pertes d'exploitation)		Contrats Cyber		Contrats Fraude
Pertes d'exploitation					
Frais informatique					
Atteintes aux données personnelles					
Dommages aux tiers (Matériels / Immatériels / Corporels)	Contrats Responsabilité Civile				

Le contrat d'assurance Cyber

Assurance

Les contrats d'assurance « Cyber » sont des contrats multirisques : ils offrent des couvertures de dommages (frais et pertes subis) et de responsabilité civile (dommages immatériels aux tiers), et des services de gestion de crise.



Comment les assureurs appréhendent-ils ce risque ?

Évaluer le risque

Et bien ... pas forcément de manière très fine ...

Pour des entreprises qui ont déjà une certaine taille (CA jusqu'à 50 M€), la souscription d'une offre Cyber peut se réaliser en quelques clics.

Il faut alors renseigner quelques données :

- Le Chiffre d'Affaires (avec le distinguo Usa/Canada) ;
- Le secteur d'activité (ou le code « Naf ») ;
- La nature et le volume des données personnelles détenues (pour certains) ;
- Le montant de garantie recherchée (pour certains) ;
- et, ... c'est tout !

A partir de là, vous pouvez obtenir une couverture allant de 50 000 € à plusieurs millions d'euros.

Pour des risques hors de ce périmètre, présentant une exposition au risque plus sensible {en raison notamment du nombre de données traitées ou leur valeur marchandes}, l'analyse va se faire au travers d'un questionnaire détaillé voire d'un audit préalable par un ingénieur spécialisé.

Évaluer le risque

Comment les assureurs appréhendent-ils ce risque ?

Les critères d'éligibilité prédéterminés :

Disposer de logiciels antivirus, anti-malware et pare feu et procéder à une mise à jour régulière de l'ensemble des dispositifs informatiques, des serveurs et réseaux, notamment pour les mises à jour de sécurité conformément aux recommandations des fournisseurs informatiques.

Disposer de procédures de sauvegarde hebdomadaire sur des équipements déconnectés et/ou externalisés

Disposer de procédures de restauration des données

Ne pas exercer les activités suivantes :

- toute activité de production audiovisuelle et musicale ;
- tout site Internet de réseau social ;
- toute activité liée aux institutions financières[1] ;
- toute vente d'armes, de drogues, de substances et produits illicites ;
- toute communication ou diffusion d'informations ou d'images à caractère érotique et pornographique ;
- tout site Internet à caractère religieux, politique et idéologique ;
- tout service de rencontres amicales, sentimentales et sexuelles ;
- toute activité de jeux et paris ; toute activité contraire aux bonnes mœurs

Exemple : Pack Cyber de la Compagnie AIG

Pour quel coût ?

Le coût

Exemple : tableau à lecture directe de la Compagnie CHUBB

Activités classiques hors institutions Financières, prestataires de services de paiement, sociétés informatiques, établissements de santé ou de soins, sociétés d'enchères en ligne, sociétés de Jeux et paris en ligne, sociétés de vente en ligne, administrations, collectivités locales ou territoriales, sociétés du secteur énergétique (y compris Pétrole/gaz), sociétés du secteur de l'hôtellerie et de la restauration, sociétés de commerce de détail.

Chiffre d'affaires annuel en Millions d'euros	Limite d'engagement toutes garanties confondues par période d'assurance					
	100.000€	250.000€	500.000€	1.000.000 €	2.000.000€	3.000.000€
Jusqu'à 2,5 M€	654 €	927 €	1 472 €	2 235 €		
entre 2,5M€ et 5 M€		1 145 €	1 799 €	2 671 €	3 434 €	
entre 5M€ et 10 M€		1 472 €	2 289 €	3 597 €	4 687 €	5 832 €
entre 10M€ et 25 M€			3 107 €	4 851 €	6 540 €	8 775 €
entre 25M€ et 50 M€				6 540 €	9 156 €	12 263 €

Franchises Générales	1.000 €	1.500 €	2.000 €	2.500 €	3.500 €	5.000 €
Perte d'exploitation	12h	12h	12h	12h	12h	12h
Frais d'assistance à incidents (dont coach)	0	0	0	0	0	0

Les primes mentionnées sont des primes annuelles et s'entendent TTC (taxe d'assurance comprise).

Mieux connaître les risques cyber

Monsieur Jean Bernard YATA

La chasse aux vulnérabilités :
Le Bug Bounty

FM Logistic in short

A family company privately owned

2019

52 YEARS

180 LOCATIONS

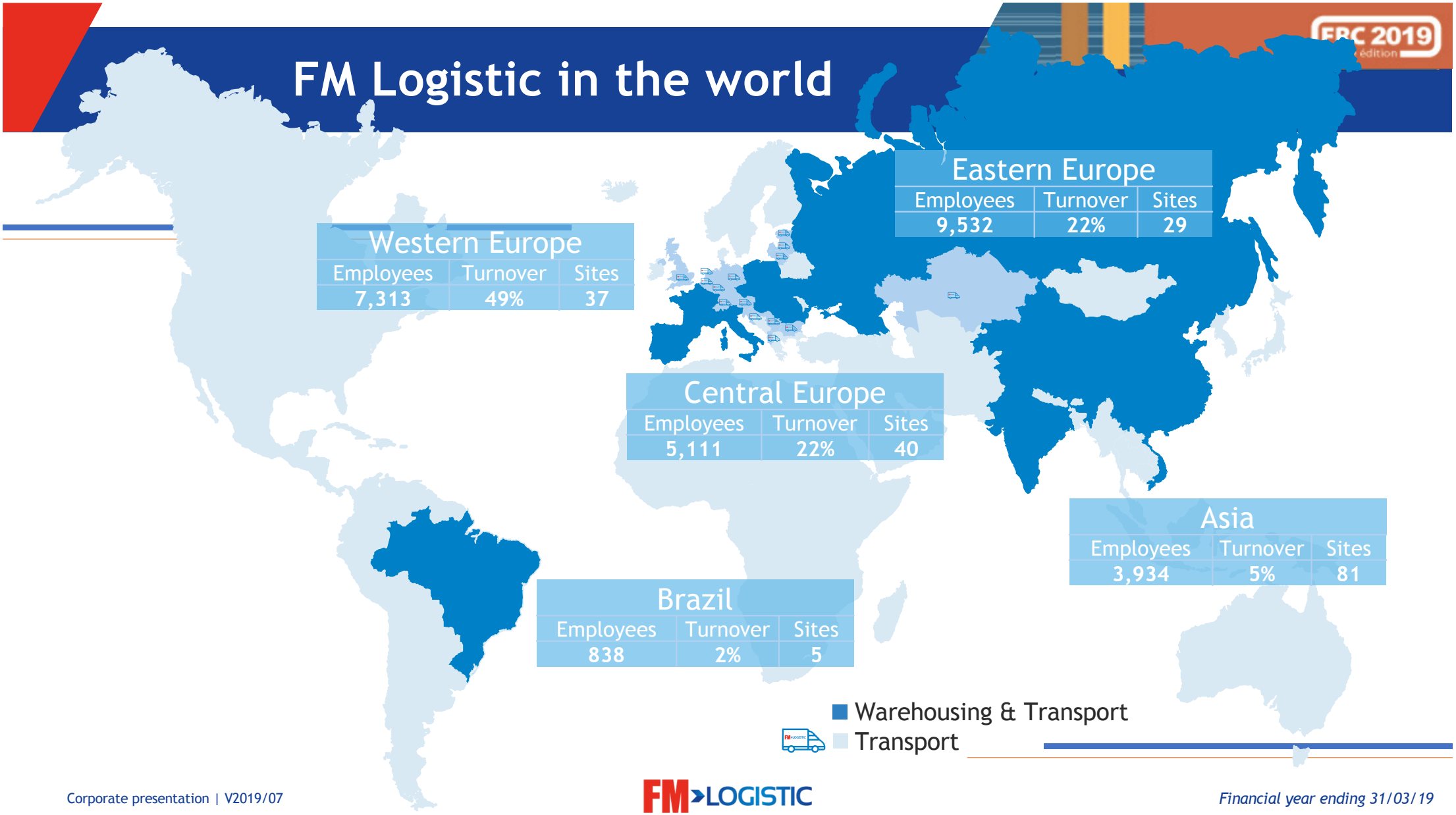
3.9 MILLION SQM

14 COUNTRIES

27,200 EMPLOYEES
(average FTE's)

1,31 MILLION €

FM Logistic in the world



Western Europe

Employees	Turnover	Sites
7,313	49%	37

Eastern Europe

Employees	Turnover	Sites
9,532	22%	29

Central Europe

Employees	Turnover	Sites
5,111	22%	40

Asia

Employees	Turnover	Sites
3,934	5%	81

Brazil

Employees	Turnover	Sites
838	2%	5

Warehousing & Transport

Transport

Audits Classiques Versus Bug Bounty

FRC 2019
12ème édition

1

Besoin en audit

- **Audit classique**
  - Site web, messagerie
  - Annuaires internes, flux d'authentification en clair
  - Mots de passe

  - **Industrialisé**
  - **Méthodologie mature**
  - **Idéal pour une compréhension de la surface d'attaque**
  - **Coût fixe**

- **Bug Bounty**
  - Applications spécifiques
  - Technologies rares
  - Expertise approfondie

  - **Communauté mondiale de chercheurs**
  - **Modèle d'audit agile & évolutif**
  - **Exhaustivité des tests**
  - **Echelle de rémunération des failles selon vos critères**

Les Plateformes de Bug Bounty

2

Avantages Bénéfices

- **Simples**
  - Définition du périmètre
  - Tests éligibles
  - Tests qualifiants

- **Economiques**
  - Optimisation du budget selon programme
  - Grille des primes

- **Efficaces**
  - Maximum de compétences mobilisées
  - Diversité des tests réalisés
  - Expertises rares accessibles

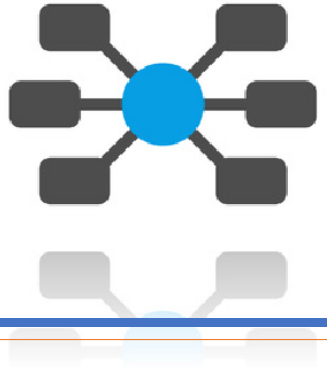
- **Sécurisées**
  - Campagnes publiques ou privées
  - Plateformes souveraines
  - Restriction des participants (cooptation, mise en relation)

Les Plateformes de Bug Bounty

3

Dans le monde

- **Européennes**
  - YOGOSHA (FR)
  - BOUNTY FACTORY (Yes We Hack) (FR)
  - ZEROCOPTER (NL)
- **Américaines**
  - HACKERONE
  - BUGCROWD
  - COBALT
- **Autres**
  - INTIGRITY
  - CYBER ARMY (ID°
  - BUGBOUNTY (JP)



Mieux connaître les risques cyber

Monsieur Michel Rochelet

Evaluer ses risques : la méthode EBIOS

LA CYBERSÉCURITÉ
Méthode d'analyse de risque EBIOS RM

Michel ROCHELET

Délégué de l'ANSSI
pour la région Grand Est
michel.rochelet@ssi.gouv.fr

EBIOS RISK MANAGER

Expression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité

Carte d'identité de la méthode EBIOS Risk Manager

CIBLE

Risk managers

RSSI

Chefs de projet

DG de PME

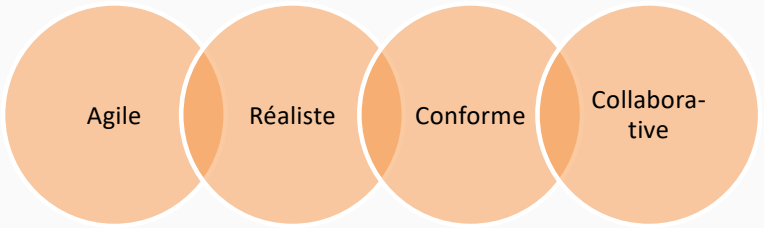
VISION

*Offrir une compréhension partagée **des risques cyber** entre les décideurs et les opérationnels*

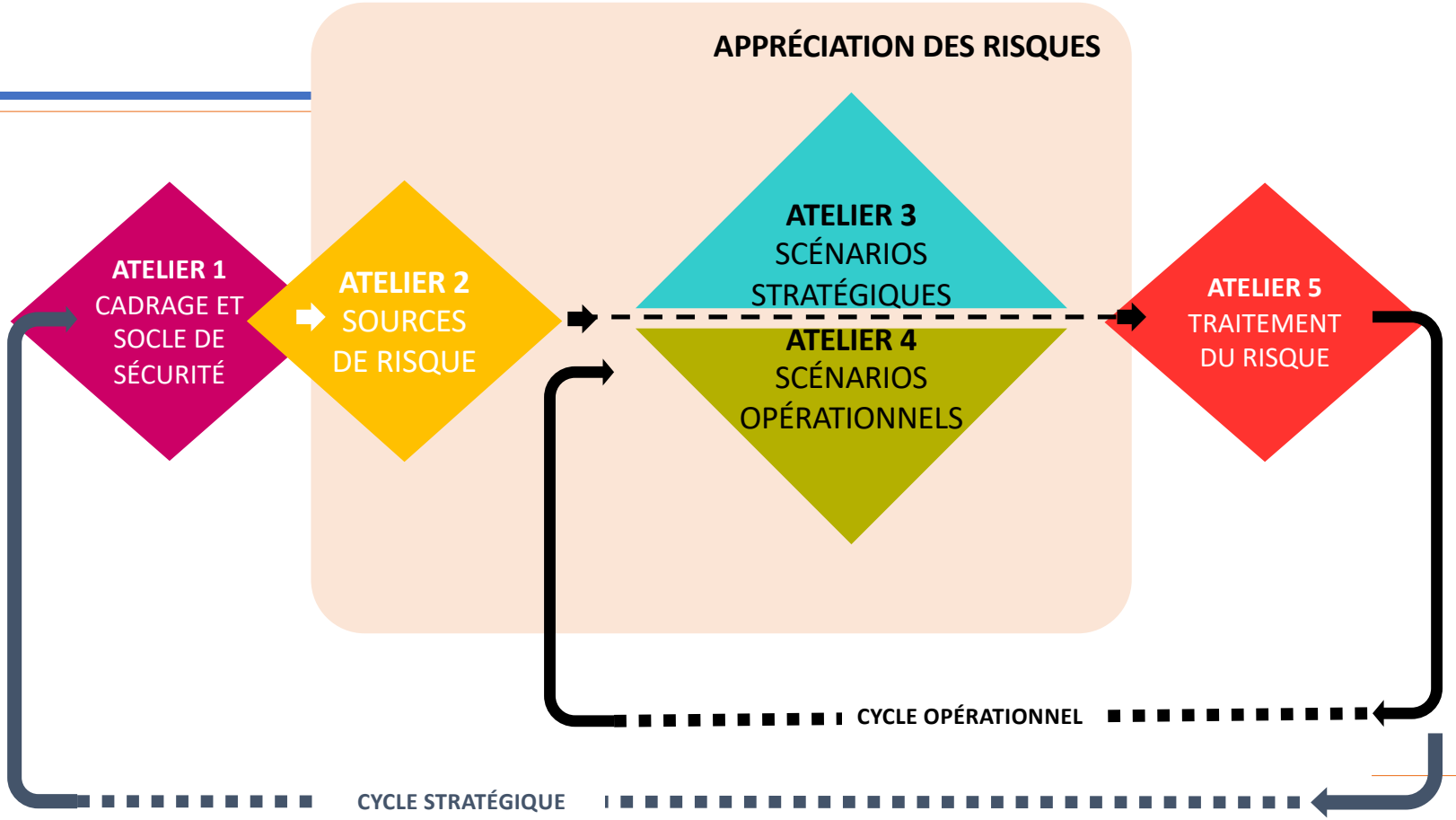
INNOVATION

- Prise en compte de l'écosystème des parties prenantes du SI de l'entreprise
- Pertinence des scénarios d'attaques (rapport efficacité/coût, du point de vue de l'attaquant)

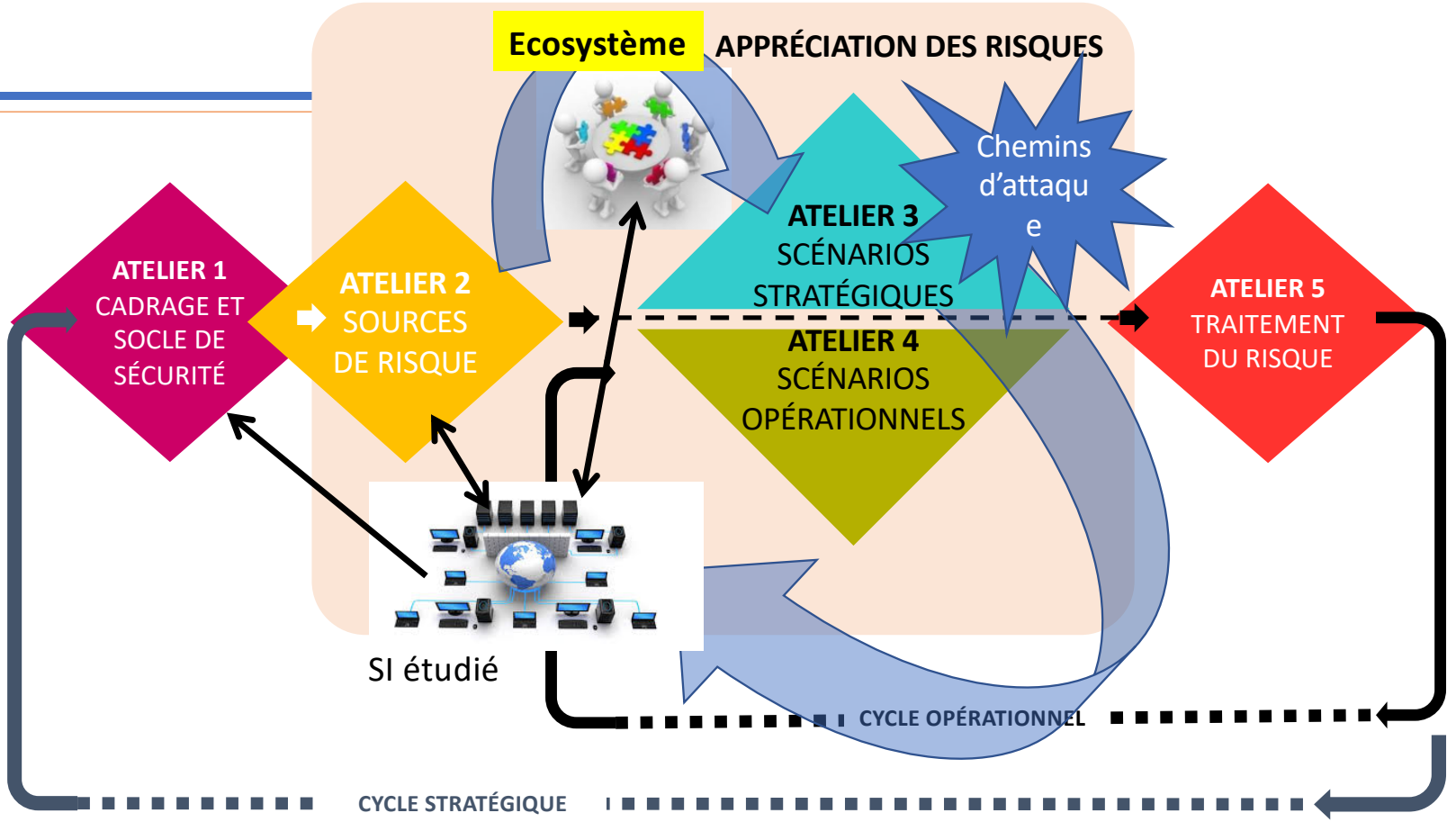
VALEURS



EBIOS RM : méthode itérative / 5 ateliers



EBIOS RM : méthode itérative / 5 ateliers



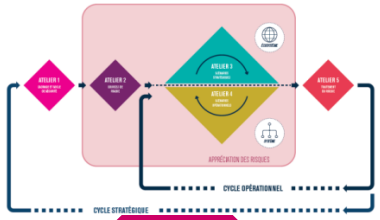
Cas fictif

SOCIÉTÉ DE BIOTECHNOLOGIE FABRIQUANT DES VACCINS

- Estimation d'un niveau de maturité faible en matière de sécurité du numérique
- Sensibilisation basique à la sécurité du numérique à la prise de poste des salariés
- Existence d'une charte informatique

Atelier 1 : cadrage et socle de sécurité

OBJECTIF : Définir le cadre de l'étude et du projet, son périmètre métier et technique



ATELIER 1
CADRAGE ET SOCLE DE SÉCURITÉ

ÉLÉMENTS EN SORTIE :

- Éléments de cadrage de l'étude : participants, planning…
- **Périmètre métier et technique** : missions, valeurs métier, biens supports
- **Événements redoutés** et leur niveau de gravité
- Socle de sécurité : liste des référentiels applicables, état d'application, identification des écarts

PARTICIPANTS : Direction, Métiers, RSSI, DSI

Définir le périmètre métier et technique

A1

MISSION	IDENTIFIER ET FABRIQUER DES VACCINS				
DÉNOMINATION DE LA VALEUR MÉTIER	**Recherche & développement (R&D)**			**Fabriquer des vaccins**	**Traçabilité et contrôle**
NATURE DE LA VALEUR MÉTIER *(PROCESSUS OU INFORMATION)*	Processus			Processus	Information
DESCRIPTION	Activité de recherche et développement des vaccins nécessitant : • l'identification des antigènes ; • la production des antigènes (vaccin vivant atténué, inactivé, sous-unité) : fermentation (récolte), purification, inactivation, filtration, stockage ; • l'évaluation préclinique ; • le développement clinique.			Activité consistant à réaliser : • le remplissage de seringues (stérilisation, remplissage) ; • le conditionnement (étiquetage et emballage).	Informations permettant d'assurer le contrôle qualité et la libération de lot (exemples : antigène, répartition aseptique, conditionnement, libération finale…)
ENTITÉ OU PERSONNE RESPONSABLE *(INTERNE/EXTERNE)*	Pharmacien			Responsable production	Responsable qualité
DÉNOMINATION DU/DES BIENS SUPPORTS ASSOCIÉS	Serveurs bureautiques (internes)	Serveurs bureautiques (externes)	Systèmes de production des antigènes	Systèmes de production	Serveurs bureautiques (internes)
DESCRIPTION	Serveurs bureautiques permettant de stocker l'ensemble des données de R&D	Serveurs bureautiques permettant de stocker une partie des données de R&D	Ensemble de machines et équipements informatiques permettant de produire des antigènes	Ensemble de machines et équipements informatiques permettant de fabriquer des vaccins à grande échelle	Serveurs bureautiques permettant de stocker l'ensemble des données relatives à la traçabilité et au contrôle, pour les différents processus
ENTITÉ OU PERSONNE RESPONSABLE *(INTERNE/EXTERNE)*	DSI	Laboratoires	Laboratoires	DSI + Fournisseurs de matériel	DSI

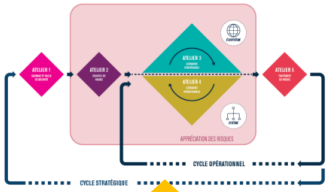
Identifier les événements redoutés

A1

VALEUR MÉTIER	ÉVÉNEMENT REDOUTÉ	IMPACTS	GRAVITÉ
R&D	Altération des informations d'études et recherches aboutissant à une formule de vaccin erronée	• Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts juridiques	3
	Fuite des informations d'études et recherches de l'entreprise	• Impacts sur le patrimoine intellectuel • Impacts financiers	3
	Perte ou destruction des informations d'études et recherches	• Impacts sur les missions et services de l'organisme • Impacts sur les coûts de développement • Impacts sur le patrimoine intellectuel	2
	Interruption des phases de tests des vaccins pendant plus d'une semaine	• Impacts sur les missions et services de l'organisme • Impacts financiers	2
Fabriquer des vaccins	Interruption de la production ou de la distribution de vaccins pendant plus d'une semaine pendant un pic d'épidémie	• Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts financiers	4
	Fuite du savoir-faire de l'entreprise concernant le processus de fabrication des vaccins et de leurs tests qualité	• Impacts financiers	2
Traçabilité et contrôle	Altération des résultats des contrôles qualité aboutissant à une non-conformité sanitaire	• Impacts sur la sécurité ou la santé des personnes • Impacts sur l'image et la confiance • Impacts juridiques	4

Atelier 2 : sources de risque

OBJECTIF : identifier les Sources de Risque (SR) ➔ Qui ?
et leurs objectifs Visés (OV) ➔ Pour faire quoi ?



ÉLÉMENTS EN ENTRÉE :

- Valeurs métier **(atelier 1)**
- Événements redoutés **(atelier 1)**

ATELIER 2
SOURCES
DE RISQUE

ÉLÉMENTS EN SORTIE :

- Liste des couples SR/OV
- Représentation des SR/OV sous la forme d'une cartographie

PARTICIPANTS : Métiers, RSSI, Direction (validation des résultats de l'atelier)

Évaluer les couples SR/OV et sélectionner les plus pertinents

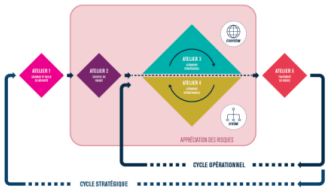
A2

SOURCES DE RISQUE (SR)	OBJECTIFS VISÉS (OV)	MOTIVATION	RESSOURCES	PERTINENCE
Concurrent	Voler des informations	Fortement motivé	Ressources importantes	Très pertinent
Hacktiviste	Saboter la mpagne nationale de ccination	Assez motivé	Ressources significatives	Plutôt pertinent
Hacktiviste	Divulguer informations sur les te animaliers	Peu motivé	Ressources significatives	Moyennement pertinent
Cyber-terroriste	Altérer la co position des vaccins à des fi e bioterrorisme	Peu motivé	Ressources limitées	Peu pertinent

Événement redouté/R&D : fuite des informations d'études et recherches de l'entreprise – Gravité : 3

Atelier 3 : scénarios stratégiques

OBJECTIF : Identifier les **parties prenantes** critiques de l'écosystème et construire des scénarios de risque de haut niveau (scénarios stratégiques)



ÉLÉMENTS EN ENTRÉE :

- Missions et valeurs métier **(atelier 1)**
- Événements redoutés et leur gravité **(atelier 1)**
- Sources de risque et objectifs visés **(atelier 2)**

ATELIER 3
SCÉNARIOS STRATÉGIQUES

ÉLÉMENTS EN SORTIE :

- Cartographie de menace de l'écosystème
- Scénarios stratégiques
- Mesures de sécurité retenues pour l'écosystème

PARTICIPANTS : Métiers, Architectes fonctionnels, Juristes, RSSI

Cartographie de menace de l'écosystème
- Parties prenantes -

A3

C1 – ÉTABLISSEMENTS DE SANTÉ

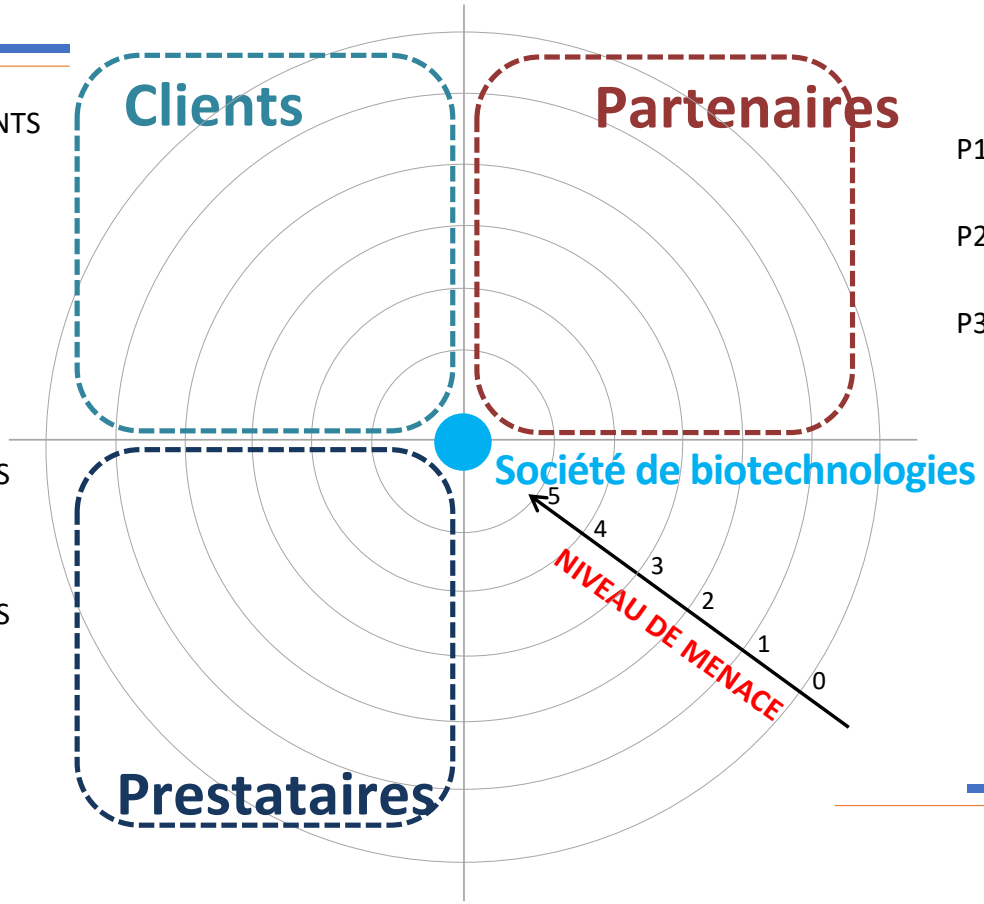
C2 – PHARMACIES

C3 – GROSSISTES RÉPARTITEURS

F1 – FOURNISSEURS INDUSTRIELS CHIMISTES

F2 – FOURNISSEURS DE MATÉRIEL

F3 – PRESTATAIRE INFORMATIQUE



P1 – UNIVERSITÉS

P2 – RÉGULATEURS

P3 – LABORATOIRES

Cartographie de menace de l'écosystème

A3

Pour chaque **partie prenante**, évaluer 4 critères :

EXPOSITION

Dépendance
La relation avec cette partie prenante est-elle vitale pour mon activité ?

Pénétration
Dans quelle mesure la partie prenante accède-t-elle à mes ressources internes ?

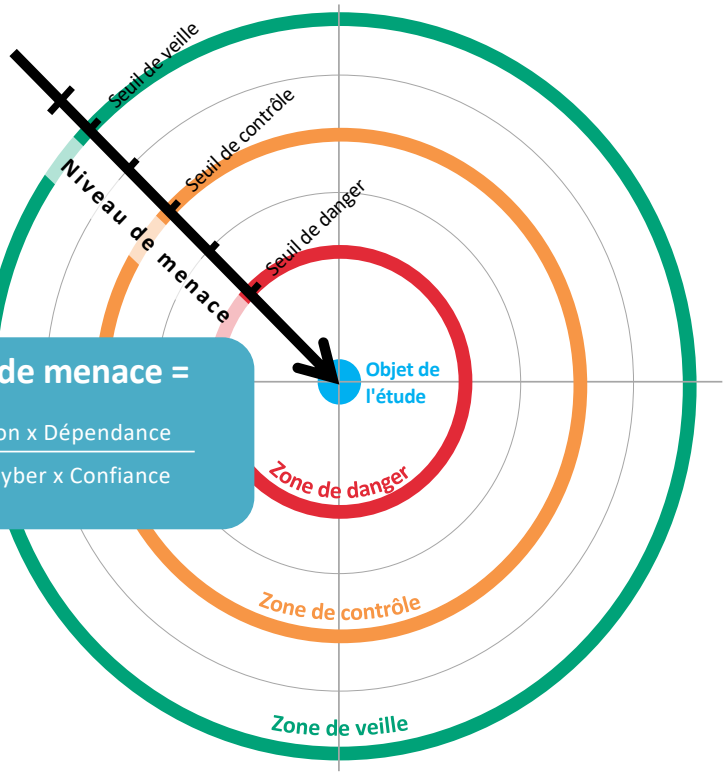
FIABILITE CYBER

Maturité cyber
Quelles sont les capacités de la partie prenante en matière de sécurité ?

Confiance
Est-ce que les intentions ou les intérêts de la partie prenante peuvent m'être contraires ?

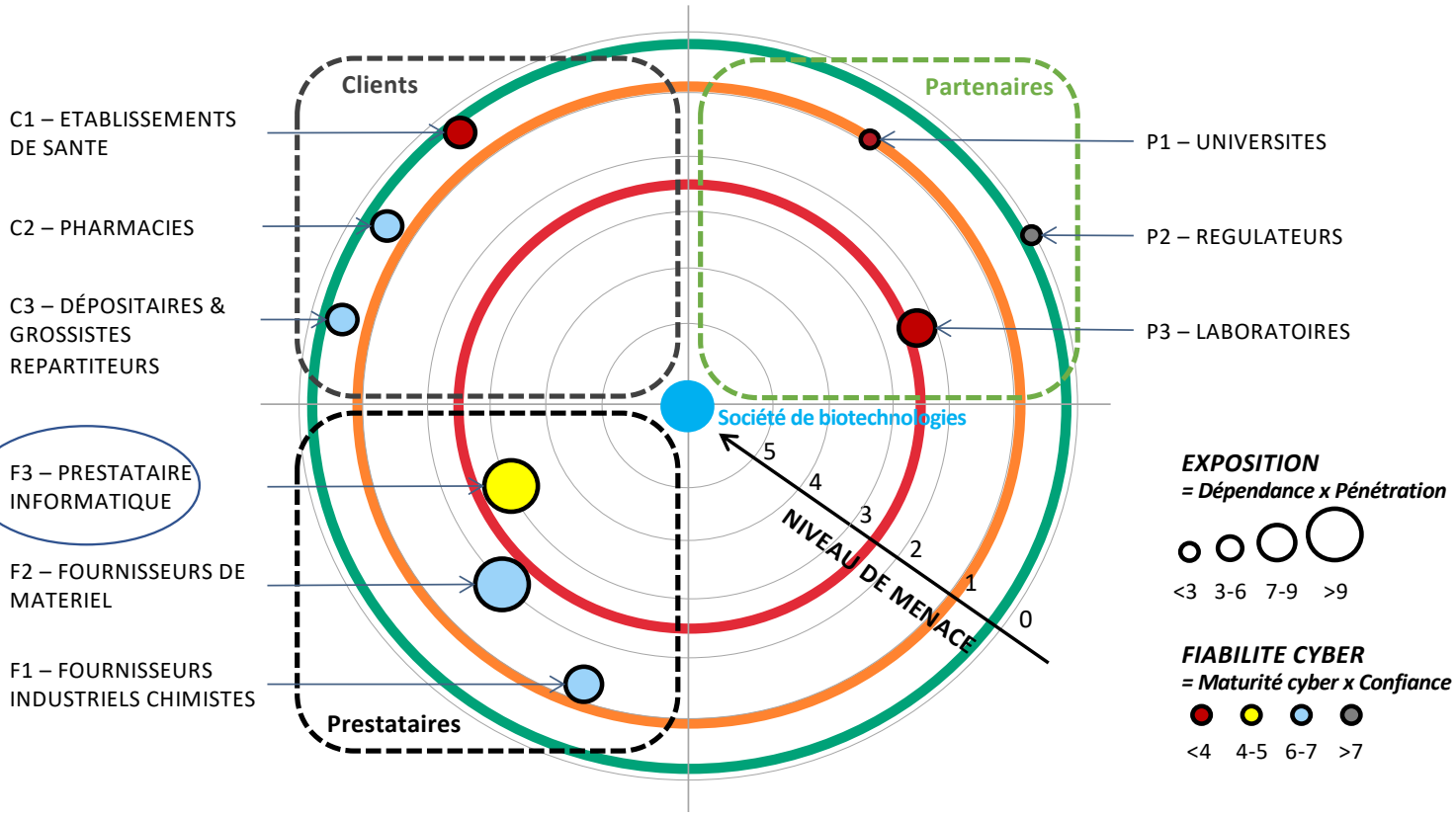
Niveau de menace =

$$\frac{\text{Pénétration x Dépendance}}{\text{Maturité cyber x Confiance}}$$



A3

Cartographie de menace de l'écosystème



Zone de veille

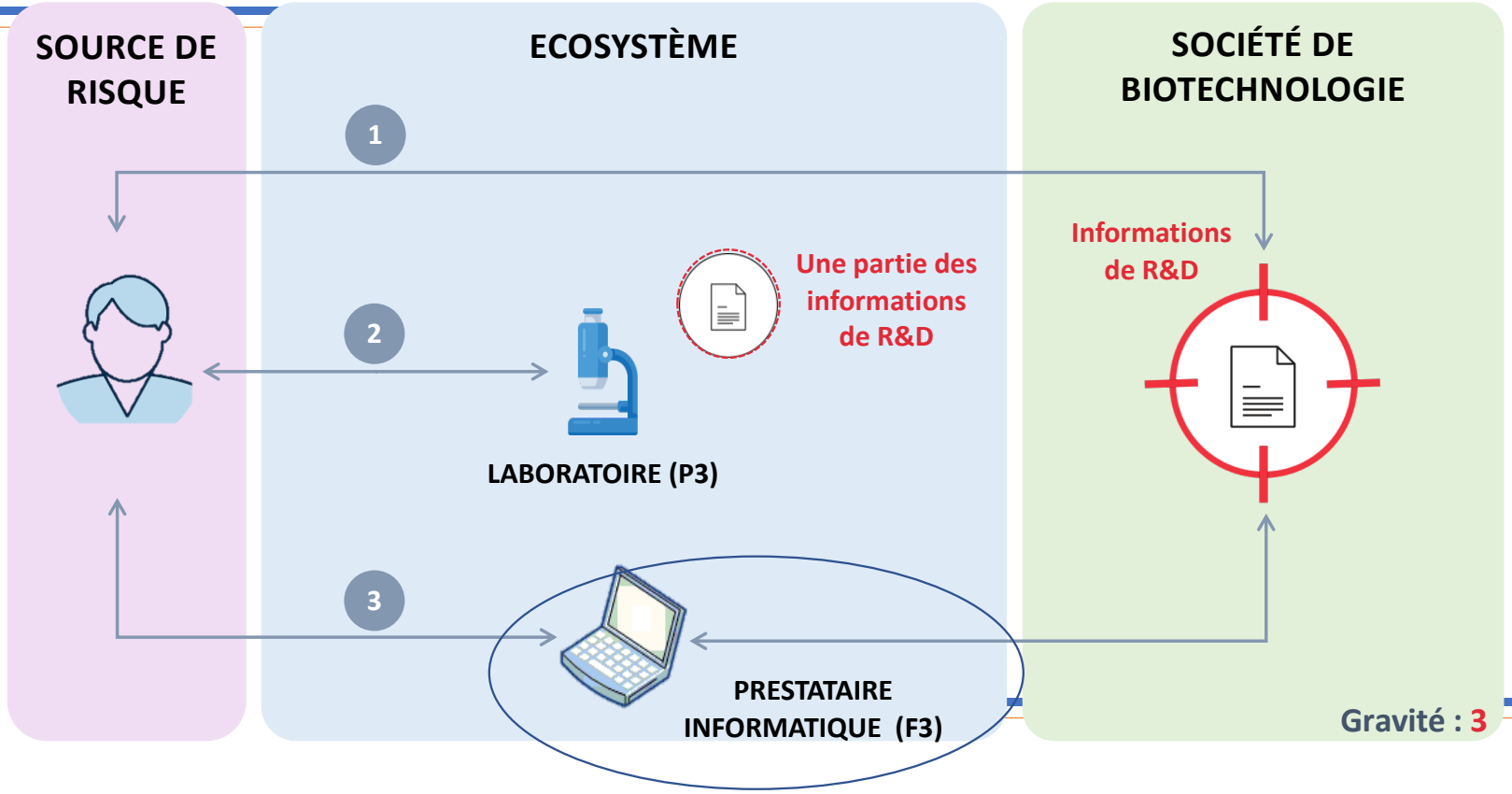
Zone de contrôle

Zone de danger

Élaborer des scénarios stratégiques

A3

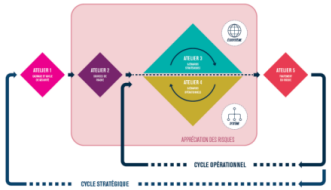
A2 **Source de risque :** Concurrent **Objectif visé :** Voler des informations



Un scénario stratégique constitué de 3 chemins d'attaque

Atelier 4 : scénarios opérationnels

OBJECTIF : Construire les scénarios opérationnels schématisant les modes opératoires techniques qui seront mis en œuvre par les sources de risque



ÉLÉMENTS EN ENTRÉE :

- Missions, valeurs métier, biens supports **(atelier 1)**
- Socle de sécurité **(atelier 1)**
- SR et OV **(atelier 2)**
- Scénarios stratégiques **(atelier 3)**

ATELIER 4
SCÉNARIOS OPÉRATIONNELS

ÉLÉMENTS EN SORTIE :

- **Un scénario opérationnel par chemin d'attaque**
- Évaluation de la vraisemblance des scénarios opérationnels

PARTICIPANTS : RSSI, DSI, Architectes SI

Élaborer les scénarios opérationnels

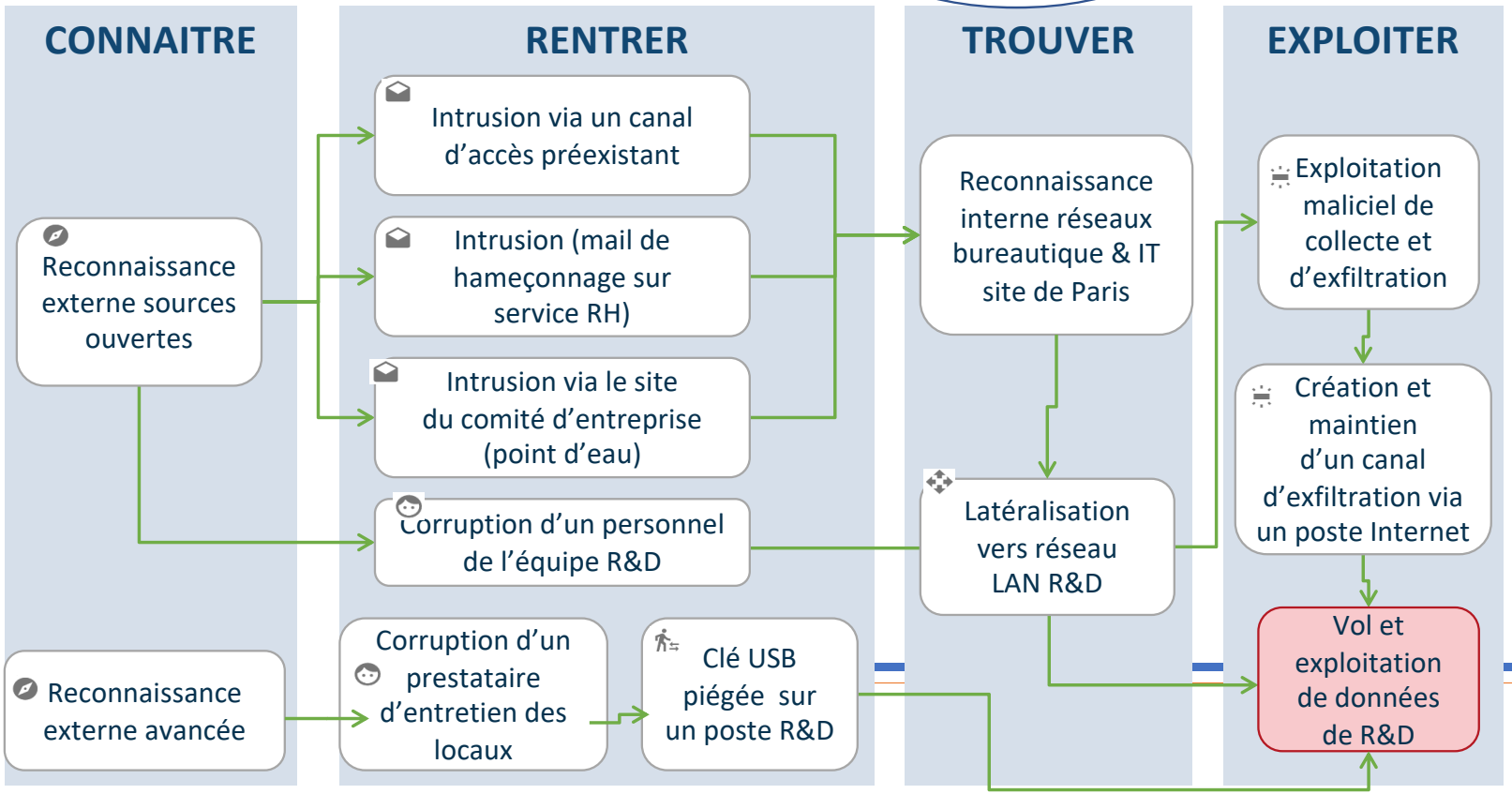
A4

A3

Scénario stratégique : un concurrent vole des informations de R&D

Chemin d'attaque : n°1 – attaque directe

Gravité : 3

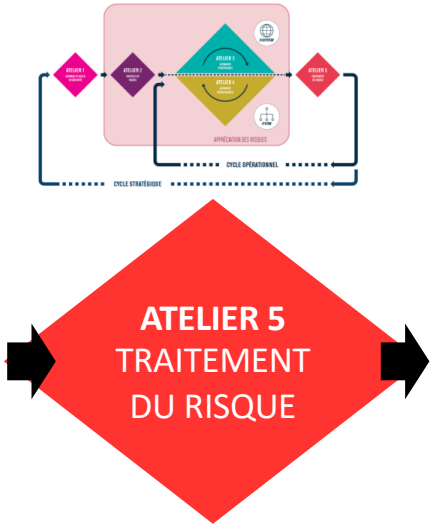


Atelier 5 : traitement du risque

OBJECTIF : Définir une stratégie de traitement du risque et identifier les risques résiduels

ÉLÉMENTS EN ENTRÉE :

- Socle de sécurité **(atelier 1)**
- Mesures de sécurité portant sur l'écosystème **(atelier 3)**
- Scénarios stratégiques **(atelier 3)**
- Scénarios opérationnels **(atelier 4)**



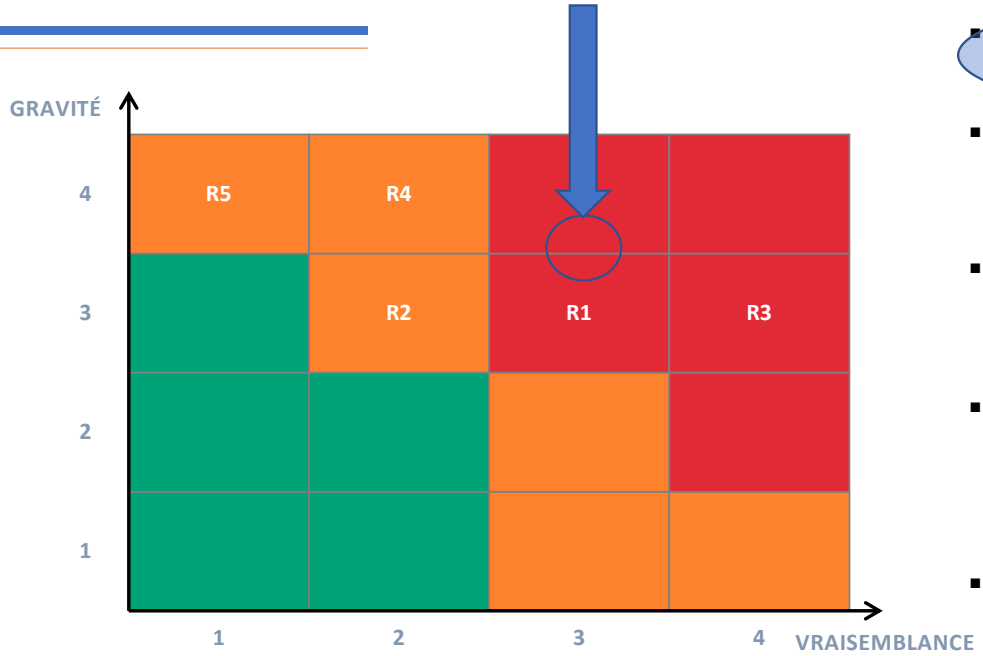
ÉLÉMENTS EN SORTIE :

- Stratégie de traitement du risque
- Plan d'amélioration continue de la sécurité (PACS)
- Synthèse des risques résiduels
- Cadre du suivi des risques

PARTICIPANTS : Direction, Métiers, RSSI, DSI

A5

Scénario de risques



Scénarios de risques :

- **R1** : Un concurrent vole des informations de R&D grâce à un canal d'exfiltration direct
- **R2** : Un concurrent vole des informations de R&D en exfiltrant celles détenues par le laboratoire
- **R3** : Un concurrent vole des informations de R&D grâce à un canal d'exfiltration via le prestataire informatique
- **R4** : Un hacktiviste provoque un arrêt de la production des vaccins en compromettant l'équipement de maintenance du fournisseur de matériel
- **R5** : Un hacktiviste perturbe la distribution de vaccins en modifiant leur étiquetage

La représentation de la stratégie de traitement doit permettre de comparer les risques les uns par rapport aux autres et être compréhensible par l'ensemble des participants

A5

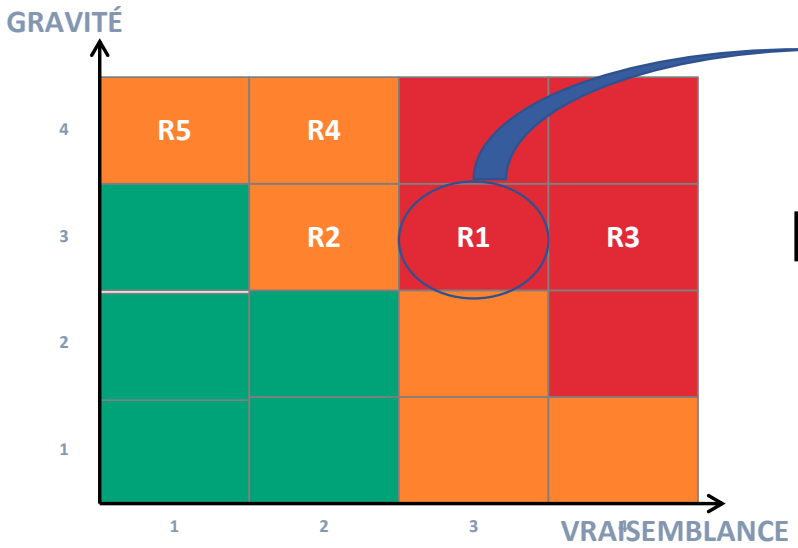
Définir les mesures de sécurité dans un Plan d'Amélioration Continue de la Sécurité (PACS)

Mesure de sécurité	Scénarios de risques associés	Responsable	Freins et difficultés de mise en œuvre	Coût/Complexité	Échéance	Statut
GOUVERNANCE						
Sensibilisation renforcée au hameçonnage par un prestataire spécialisé	R1	RSSI	Validation de la hiérarchie obligatoire	+	Juin 2019	En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	R1, R5	RSSI		++	Mars 2019	A lancer
Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les prestataires et laboratoires	R2, R3, R4	Équipe juridique	Effectué au fil de l'eau à la renégociation des contrats	++	Juin 2020	En cours
Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire ou un laboratoire	R2, R3, R4	RSSI / Équipe juridique		++	Juin 2019	A lancer
Audit de sécurité organisationnel des prestataires et laboratoires clés. Mise en place et suivi des plans d'action consécutifs	R2, R3, R4	RSSI	Acceptation de la démarche par les prestataires et laboratoires	++	Juin 2019	A lancer
Limitation des données transmises au laboratoire au juste besoin	R2	Équipe R&D		+	Mars 2019	Terminé
PROTECTION						
Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement)	R1, R3	DSI		+++	Septembre 2019	En cours
Renforcement du contrôle d'accès physique au bureau R&D	R1	Équipe sûreté		++	Mars 2019	Terminé
Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site	R4	DSI		++	Septembre 2019	A lancer

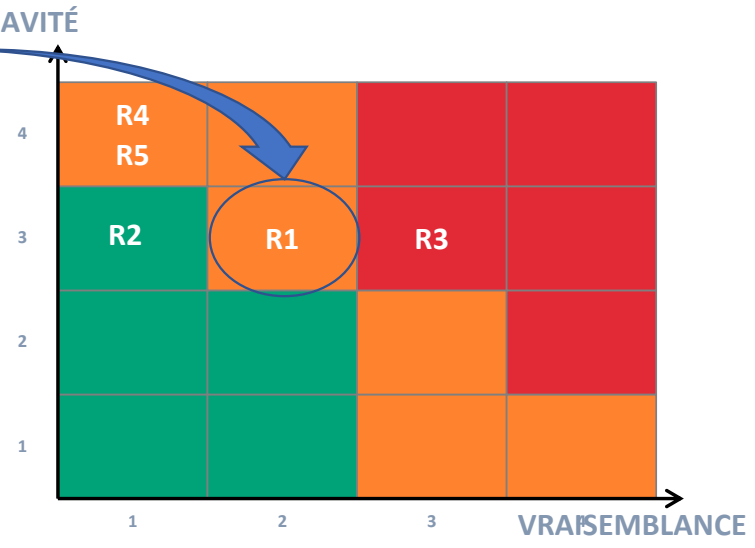
A5

Gérer les risques résiduels

Cartographie du risque initial (avant traitement)



Cartographie du risque résiduel (après application du PACS)



Au terme de l'analyse, les risques résiduels sont acceptés formellement par la direction

Mettre en place le cadre de suivi des risques

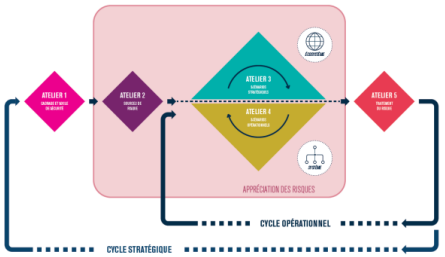
A5

Mettre en place un comité de pilotage pour le suivi des risques

MESURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN ŒUVRE	COÛT / COMPLEXITÉ	ÉCHÉANCE	STATUT
GOUVERNANCE						
Sensibilisation renforcée au hameçonnage par un prestataire spécialisé	R1	RSSI	Validation du CHSCT indispensable	+	6 mois	En cours
Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique par un PASSI	R1, R5	RSSI		++	3 mois	À lancer
Intégration d'une clause de garantie d'un niveau de sécurité satisfaisant dans les contrats avec les prestataires et laboratoires	R2, R3, R4	Équipe juridique	Effectué au fil de l'eau à la renégociation des contrats	++	18 mois	En cours
Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire ou un laboratoire	R2, R3, R4	RSSI / Équipe juridique		++	6 mois	À lancer
Audit de sécurité organisationnel des prestataires et laboratoires clés. Mise en place et suivi des plans d'action consécutifs	R2, R3, R4	RSSI	Acceptation de la démarche par les prestataires et laboratoires	++	6 mois	À lancer
Limitation des données transmises aux laboratoires au juste besoin	R2	Équipe R&D		+	3 mois	Terminé
PROTECTION						
Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement)	R1, R3	DSI		+++	9 mois	En cours
Renforcement du contrôle d'accès physique au bureau R&D	R1	Équipe sûreté		++	3 mois	Terminé
Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site	R4	DSI		++	9 mois	À lancer

Suivi de l'avancement du PACS

Suivi des indicateurs de maintien en condition de sécurité (MCS)



Suivi des mises à jour de l'étude des risques selon les cycles stratégique et opérationnel

SOLUTIONS LOGICIELLES CONFORMES EBIOS RISK MANAGER

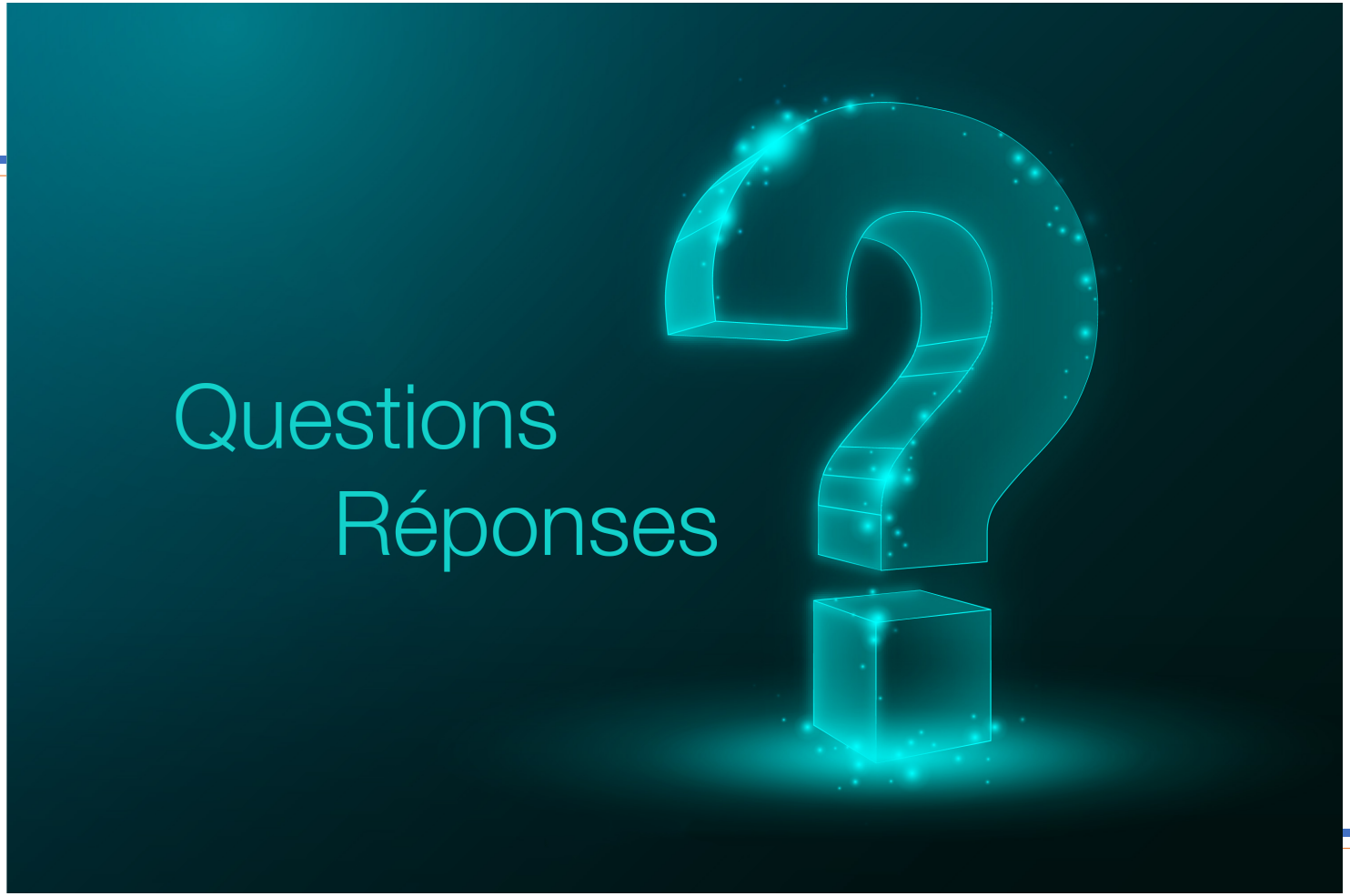
SOLUTIONS LOGICIELLES EBIOS RISK MANAGER LABELLISÉES

Prestataire	Nom de la solution logicielle labellisée	Version
ALLATEC Parc Ceres Rue Ferdinand Buisson 53810 CHANGE https://www.riskoversee.com	Agile Risk Manager	1.0
EGERIE Software 44 boulevard de Strasbourg 83000 Toulon http://www.egerie-software.com	EGERIE Risk Manager	3.0

SOLUTIONS LOGICIELLES EBIOS RISK MANAGER EN COURS DE LABELLISATION

Seuls apparaissent les projets de labellisation que les éditeurs ont accepté de rendre publiques. En cas de suspension du projet, celui-ci est retiré de la liste.

Prestataire	Nom de la solution logicielle en cours de labellisation	Version
ADACIS Sarl 5 Ferreau Sud, 33230 Bayas http://www.adacis.net	ARIMES	1.0
APSYS ZAC du Grand Noble 37, avenue Escadrille Normandie Niemen 31700 BLAGNAC https://www.apsys-airbus.com	Fence	3.0
IBM France 17 avenue de l'Europe 92275 Bois Colombes Cedex	IBM OpenPages GRC Platform	8.0


Questions
Réponses


Pause !

DÉMONSTRATION OPÉRATIONNELLE

DeepFake - Your face isn’t yours anymore

Monsieur Kevin OUAHMAD
Monsieur Gauthier WAGNER

Peut-on encore faire confiance aux images ?

Plan de présentation

Voici ce que vous découvrirez au cours de cette brève présentation :

1. Le deep Learning en 1 min
   - Bref historique
   - Un aperçu du fonctionnement
2. Le DeepFake, une arme dangereuse
   - Une vraisemblance redoutable
   - Un clonage de voix pour encore plus de dégâts
3. Comment se protéger
   - Des défauts visibles
   - Un réseau de neurones capable de les détecter

01

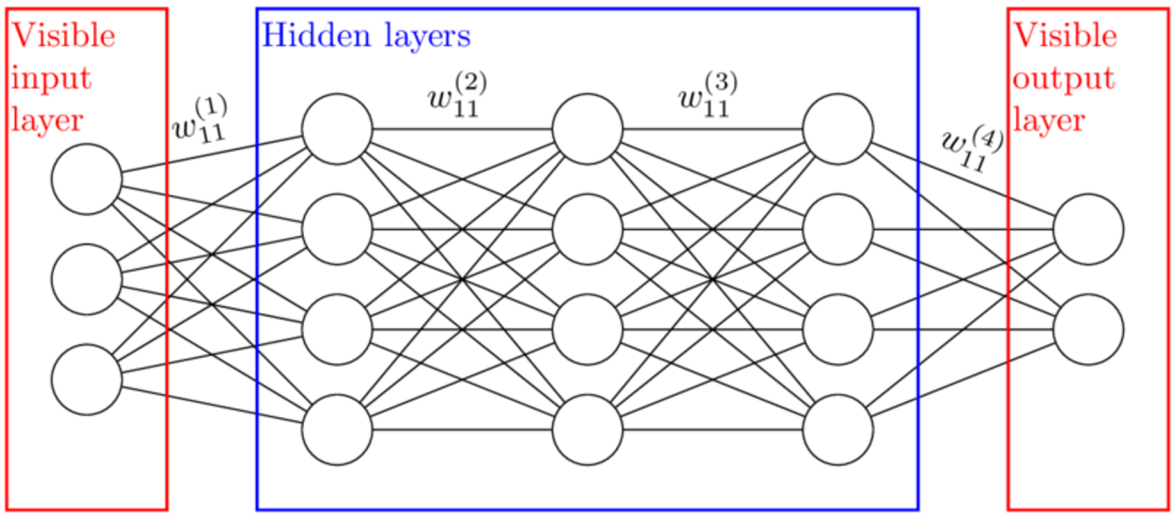
Le Deep Learning

Une technologie qui pourrait marquer l'histoire

Une merveilleuse histoire de temps

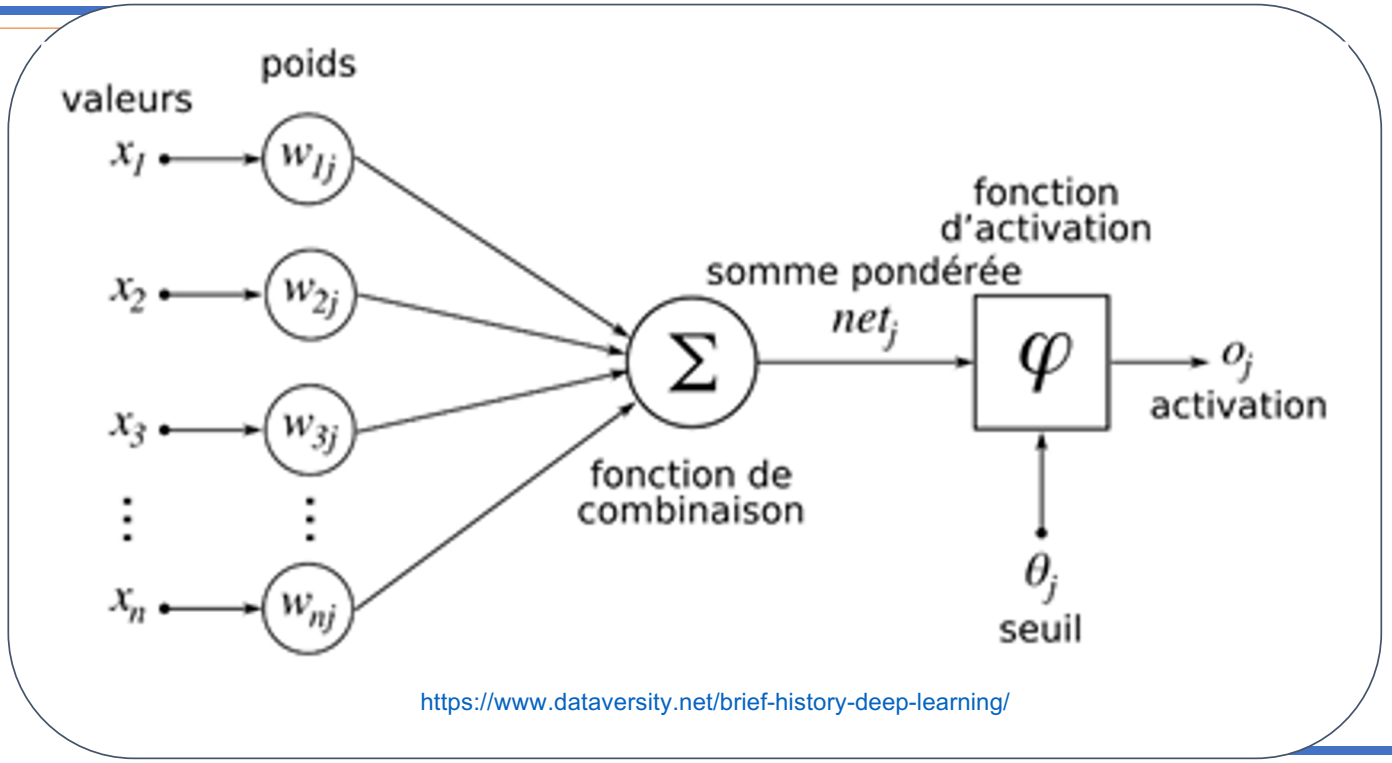
- **1943.** 1er modèle de calcul basé sur les réseaux de neurones
- **1960.** Arrivée de la *Backpropagation*
- **1999.** Développement des 1ers GPU
- **2012.** L'avènement grâce à ImageNet
- **2019.** Un investissement incroyable

Modèle d'un réseau de neurones profond



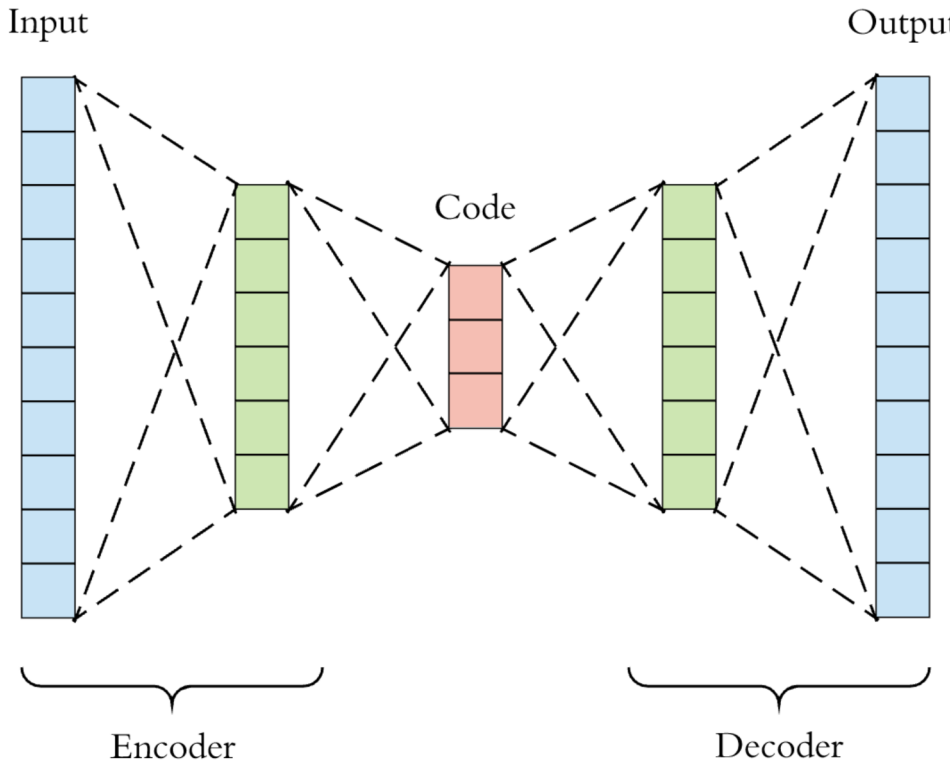
https://www.researchgate.net/figure/An-example-of-a-deep-learning-neural-network-with-3-hidden-layers-For-a-Boltzmann_fig6_286513346

Modèle d'un réseau de neurones profond



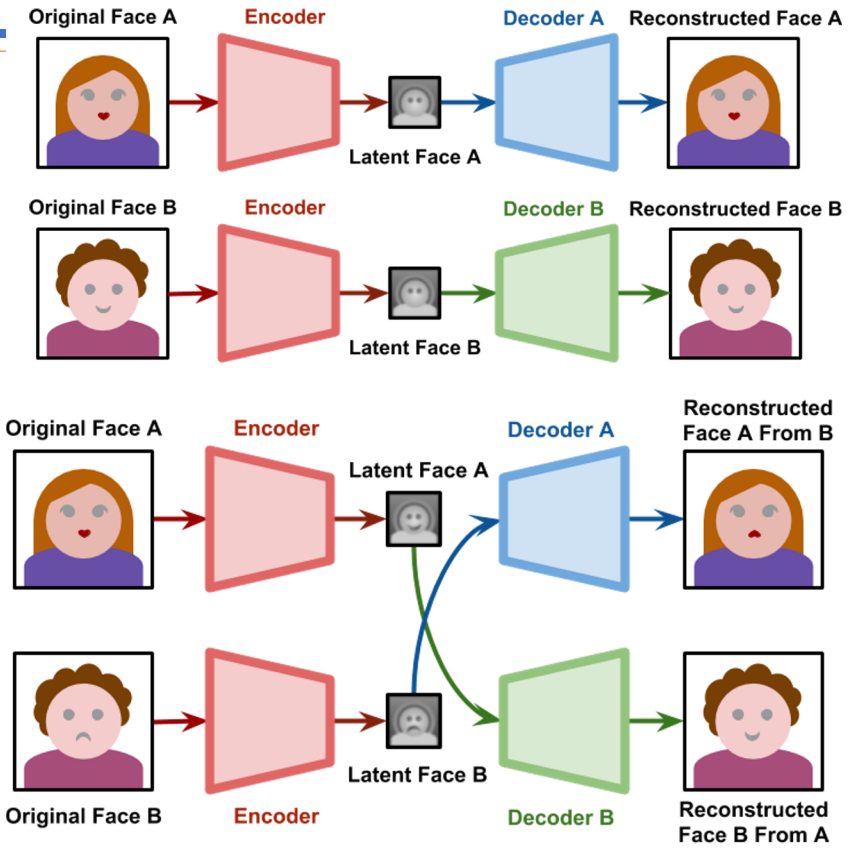
https://www.dataversity.net/brief-history-deep-learning/

Les AutoEncoders pour le DeepFake



https://towardsdatascience.com/generating-images-with-autoencoders-77fd3a8dd368

Les AutoEncoders pour le DeepFake



De manière générale

Pour le DeepFake

https://www.alanzucconi.com/2018/03/14/understanding-the-technology-behind-deepfakes/

02

Entre de bonnes mains

Le DeepFake fait des ravages

Un travail de professionnel

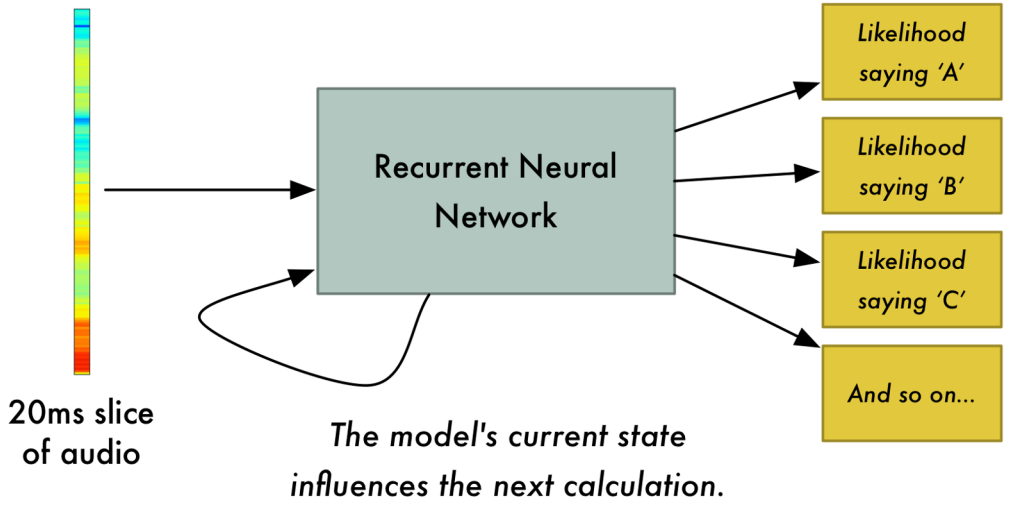
DeepFake
En temps réel

Il est possible de réaliser du DeepFake en temps réel

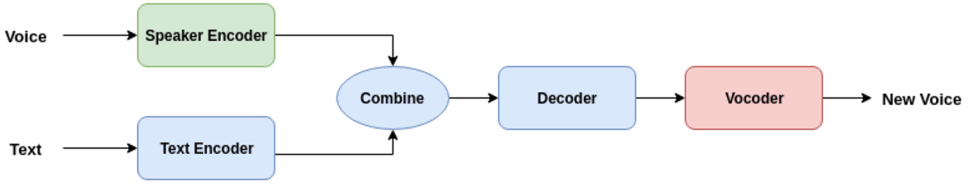
Associé à un réseau de neurones pour le clonage de voix, le résultat est redoutable

https://www.youtube.com/watch?v=gLoI9hAX9dw

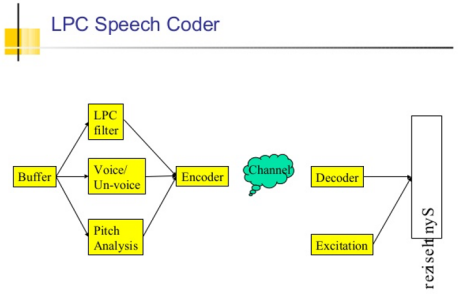
Deep Voice



https://medium.com/@ageitgey/machine-learning-is-fun-part-6-how-to-do-speech-recognition-with-deep-learning-28293c162f7a



https://towardsdatascience.com/you-can-now-speak-using-someone-elses-voice-with-deep-learning-8be24368fa2b



3 réseaux de neurones parmi tant d'autres

25

https://www.slideshare.net/HemarajaNayakaS/speech-encoding-techniques

03

Comment se protéger

DeepFakes.. Attrapez les tous !

Un combat sans répit

Création de Deepfakes

Détection de Deepfakes

https://pixabay.com/photos/chess-game-play-king-black-knight-2551751/

Un combat sans répit

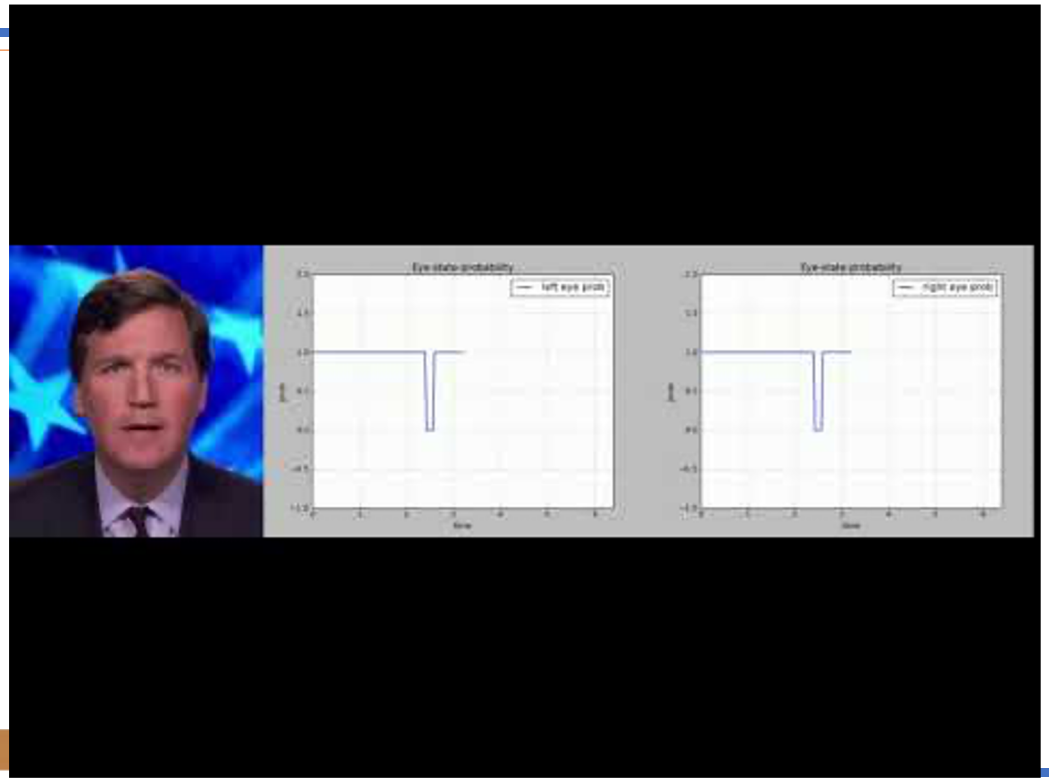
Chercher les défauts

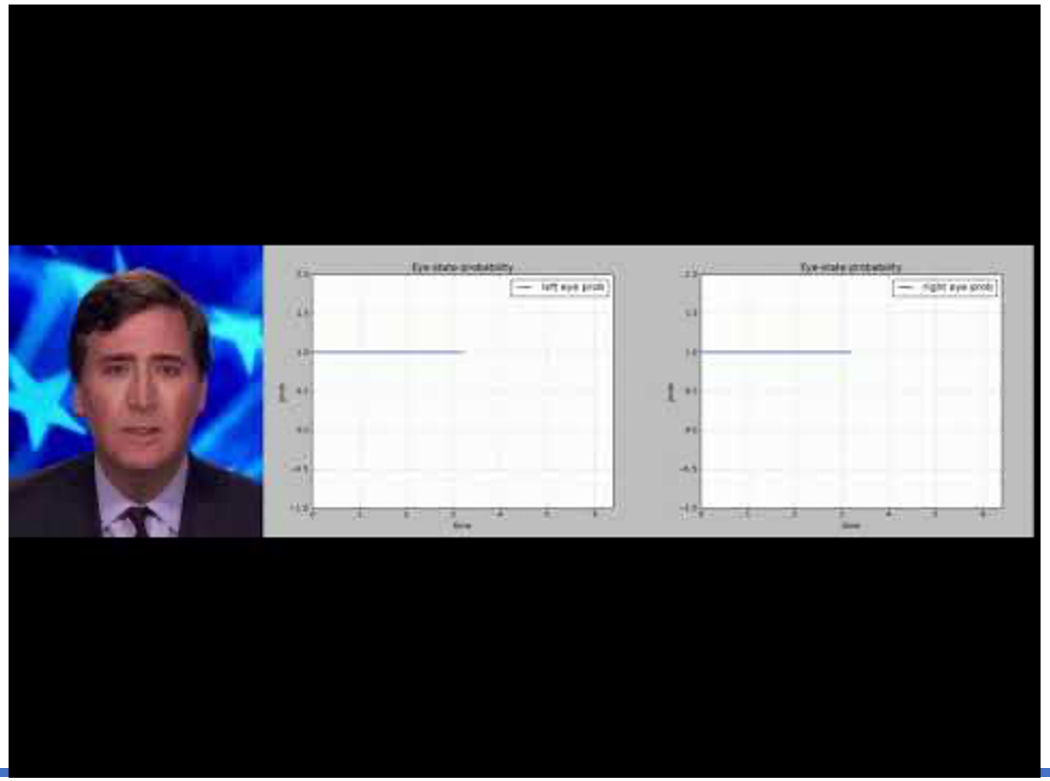
- Incohérences flagrantes
- Problèmes de luminosité / d'ombres
- Petits détails du visage

Combattre le feu par le feu

- Un réseau de neurones pour les détecter en un clin d'œil

Une IA pour les détecter tous





https://phys.org/news/2018-08-deepfake-videos-eye.html

Conclusion

Un danger dont il faut se méfier

Merci

Avez-vous des questions?

kevin.ouahmad@uha.fr
gauthier.wagner@uha.fr
ENSISA

Sources

- https://en.wikipedia.org/wiki/Deep_learning
- http://www.ensisa.uha.fr/
- http://www.uha.fr/
- https://github.com/iperov/DeepFaceLab

FRC 2019 : Table ronde #2

La sécurité du site internet de l'entreprise

Table ronde #2 : La sécurité du site internet de l'entreprise

Adjudant Elena VALLEJO

Enquêtrice délinquance financière de la Section de Recherches de Strasbourg

Lieutenant Olivier BROGGI

Commandant la division délinquance économique, financière et numérique de la Section de Recherches de Strasbourg

Monsieur Eric Wies

Ingénieur réseau INSEE. Chef d'escadron (RC) de la gendarmerie nationale

Monsieur Thomas VIERLING

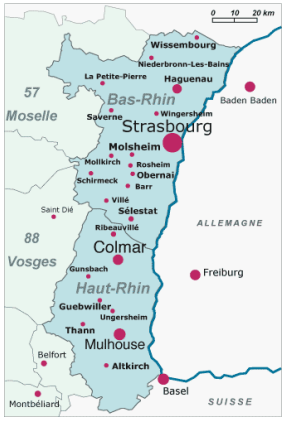
Directeur de LPB Conseil

La sécurité du site internet de l'entreprise

Adjudant Elena VALLEJO
Lieutenant Olivier BROGGI

Le cambriolage numérique : actualisation.

Présentation



Présentation de la DDEFN SR STRASBOURG

◊

Les différents aspects du cambriolage numérique

◊

Le constat Alsacien

◊

Les contres mesures ou moyens simples de prévention

Section de Recherches
De STRASBOURG

D.D.E.F.N
(Division de lutte contre la délinquance Économique, Financière et Numérique

DDEFN SR Strasbourg

5 enquêteurs DEFI
Qualifiés CNTECH – ESP

1 enquêteur NTECH
Qualifiée DEFI 1

Délinquance financière

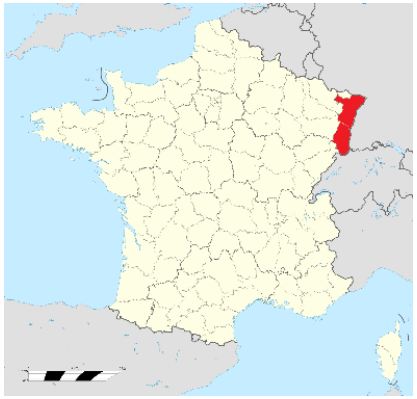
Cyber-criminalité

Criminalité organisée internationale

Cambriolage numérique

- Escroqueries à l'investissement (crypto-monnaies, terres rares, produits de consommation, produits d'épargne...)
- FOREX (faux trading,...;)
- FOVI (faux ordres de virements) faux président, faux fournisseur, changement de compte....)
- Rançongiciel
- Faux Support technique
- Mailing scams (RGPD, ADAP, VAT,...)
- Typosquating
- Physhing

Le cambriolage numérique en ALSACE



- En 2018 (constat Gendarmerie)
- Victimes : tout type d'entreprises
- Tous domaines d'activités (agriculture, commerce, industrie...)
- FOVI, faux investissements, ransonware, contrôle à distance,...
- **12 faits recensés pour un préjudice de 1,3 million d'euros.**

Focus modus operandi

FOVI

- par compromission de boites mail (faux président)
- par contrôle à distance (usurpation opérateur de maintenance de la banque)

RANÇONGICIELS

- faille de sécurité exploitée, chiffrement et effacement de logs
- pièce jointe (wanacry)

FAUX INVESTISSEMENT

Les contres mesures

<u>AU NIVEAU DES ENTREPRISES :</u>

Matériel : Maximisation du niveau de sécurité, sauvegardes
Humain : Formation / Protocoles de vérification

<u>AU NIVEAU DES FORCES DE L'ORDRE</u>

FOVI : blocage des fonds, coopération internationale et CRI
RANÇONGICIELS : blockchain – identification – déchiffrement

Chaîne d'action de la SR à l'EC3 (ACYMA - NoMoreRansom)

La sécurité du site internet de l'entreprise

Monsieur Eric WIES

Les enjeux des PME en matière de sécurisation des paiements électroniques

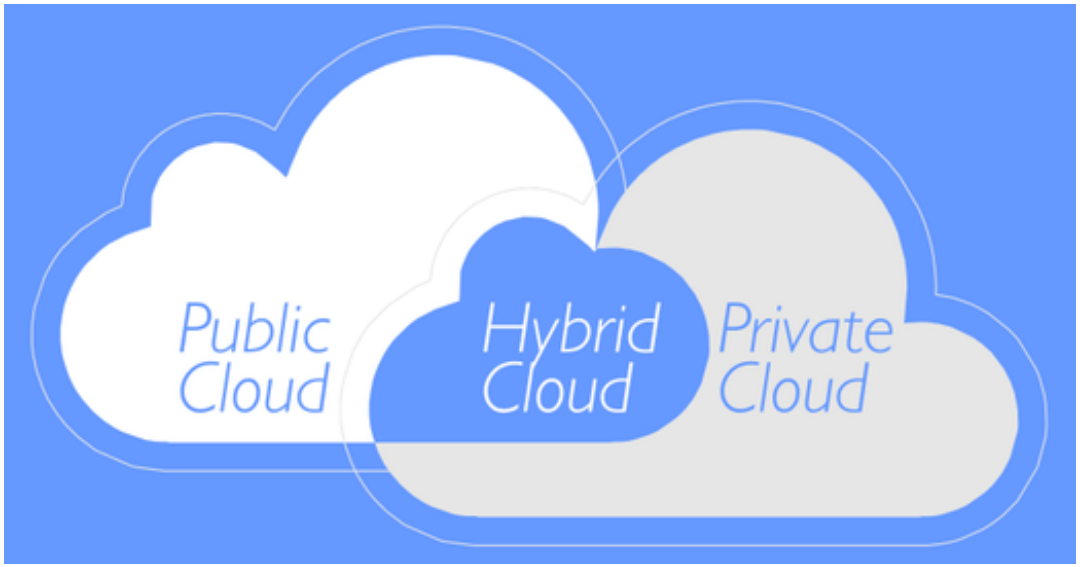
Auto-héberger son SI
Ne pas céder aux sirènes et aux chimères

Hébergement vs Cloud

- Héberger son SI
  - C’est has-been
  - C’est cher
  - C’est pas souple
  - Faut toujours prévoir plus !
- Le cloud
  - C’est l’avenir
  - C’est modulable
  - On paie ce que l’on consomme

Le cloud hybride ?

- On peut allier les 2 technologies ?
- Et passer de l'une à l'autre ?
  - Suivant les besoins ?
  - Suivant les applications
- Quid de la sécurité ?
  - Entre applis et données
  - Entre les différents fournisseurs



Mais les fuites de données se multiplient

01net.com

Rechercher un produit, un logiciel, une vidéo ... | Codes Promo | Services

VIDÉOS ACTUALITÉS TESTS ASTUCES TELECHARGER.COM JEUX VIDÉO BONS PLAN

Produits Applis, Logiciels Jeux Technos Sécurité Buzz, société Télécoms Culture, médias Politique, Droits Science, recherche

01net › Actualités › Sécurité

En France, plus de 2,6 millions d'images médicales en libre accès sur Internet

17/09/2019 à 19h03

Siècle DIGITAL

TECHNOLOGIE

Royaume-Uni : les données biométriques d'un million de personnes ont été exposées

Facile de changer un mot de passe, plus compliqué de modifier ses empreintes digitales...

Fuite de données : 7,7 millions de clients d'un laboratoire d'analyse US touchés

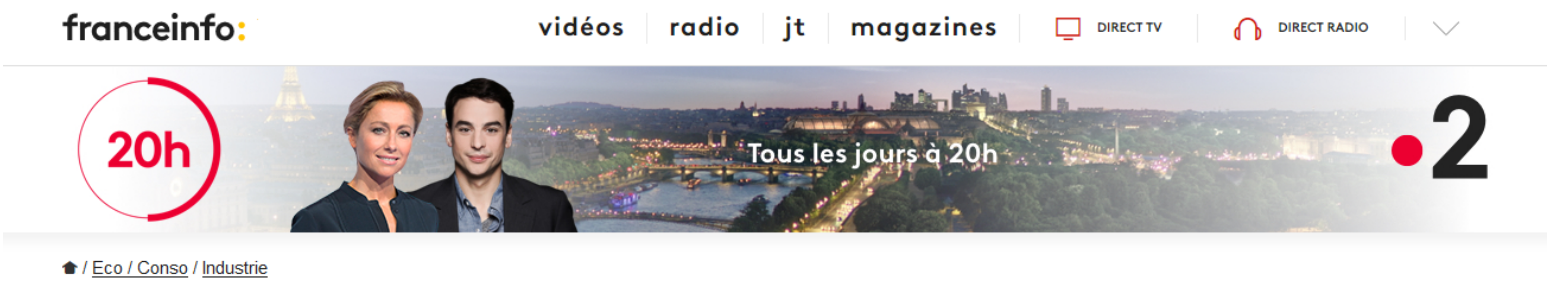
Heureusement il y a le cloud souverain !

Vraiment ?


LEMONDE INFORMATIQUE
ACTUALITÉS
DOSSIERS
ÉVÉNEMENTS
SERVICES
LIVRES-BLANCS
PARTENAIRES
En ce moment :
SILICON VALLEY
LMI IT TOUR
ASSISES DE LA SÉCURITÉ
TOUTE L'ACTUALITÉ / CLOUD / IAAS
Cloudwatt : arrêt définitif de service en février 2020
Dominique Filippone , publié le 31 Juillet 2019

Le syndrome EDF

- On sous traite le SI, On fait faire par d'autre
- On perd peut à peut le savoir faire
- On perd le contrôle



EPR de Flamanville : symbole de la perte du savoir-faire français ?

Alexandra Bensaid explique sur le plateau du 20 Heures que les mésaventures de l'EPR de Flamanville (Manche) illustrent non pas une faillite technologique, mais une perte de savoir-faire technique.

Pourquoi auto héberger son SI

- Ce n'est pas que les applications et les données

- Mais tout l'éco système numérique
  - DNS, Mails
  - Fournisseur d'accès et les liens physiques

- Et protéger chaque couche, chaque élément

- Garder le contrôle, le savoir, et le savoir-faire sur
  - Ce que l'on manipule
  - Comment on le manipule

Un peu d'imagination

- Imaginons un entreprise
  - Qui dispose des identités de tous les individus d'un pays
  - Qui dispose de la liste électorale
- On peut vraiment mettre toutes ces données
  - Chez un fournisseur externe ?
  - Dans un cloud ?
- Quel serait le risque pour la démocratie ?
- Bien sur cette entreprise … existe !

Insee
Institut national de la statistique et des études économiques
Mesurer pour comprendre

La sécurité du site internet de l'entreprise

Monsieur Thomas VIERLING

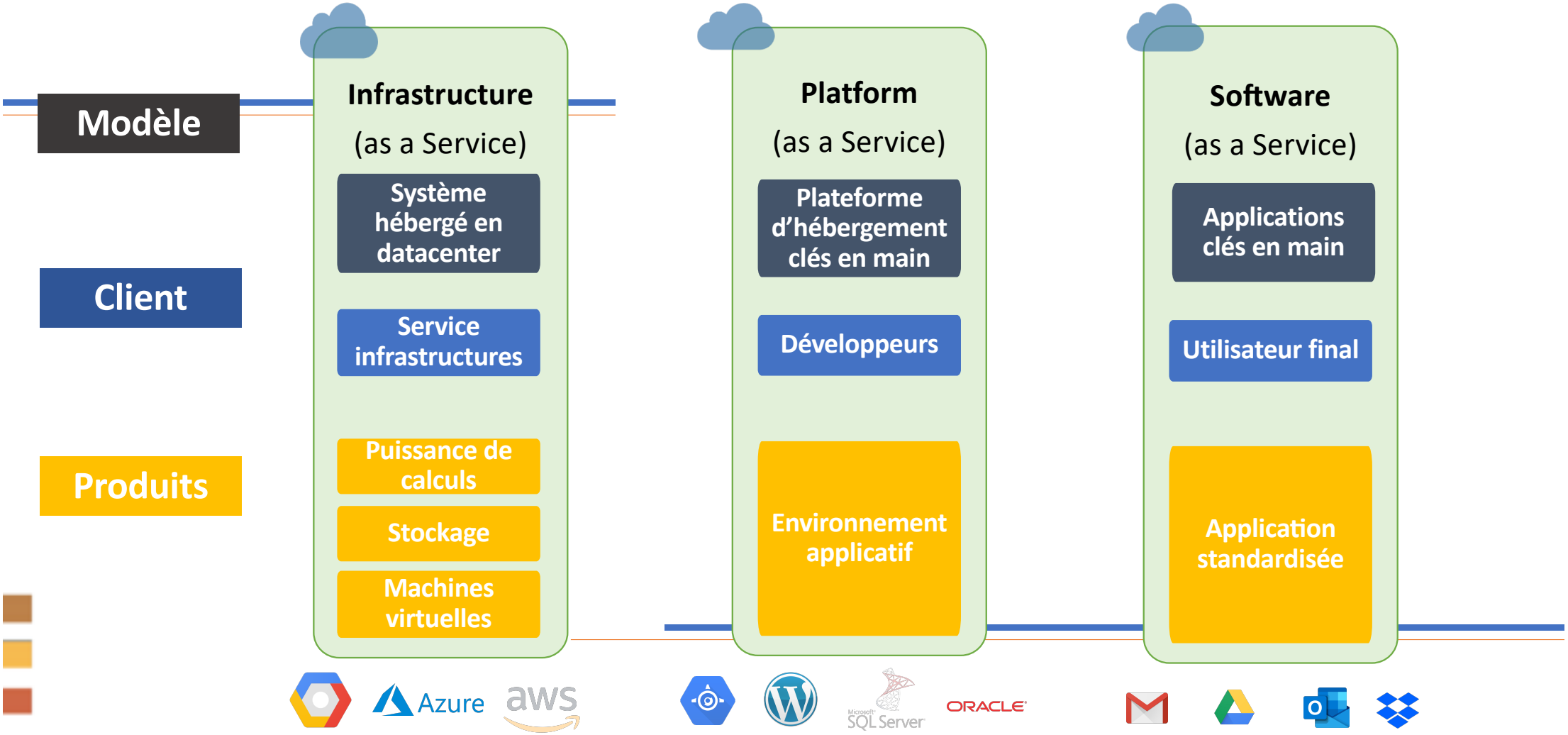
L'hébergement du site : le cloud public.

La sécurité des plateformes Cloud pour les PME/PMI

AGENDA

1. Les différents services Cloud
2. Quelles questions se poser en termes de sécurité ?
3. Est-il possible d'échapper au Cloud ? Quelles règles mettre en place ?

1. Les différents services du Cloud et cas d'usages



1. Les différents services du Cloud et cas d'usages

Responsabilités	On-Premise	IaaS	PaaS	SaaS
Informations et données	Responsabilité de l'entreprise			
Postes de travail				
Gestion des identités et accès				
Annuaire technique, comptes utilisateurs			Responsabilité partagée	Responsabilité partagée
Applications (Développements, etc…)			Responsabilité partagée	
Contrôle des accès au réseau (Parefeu, enregistrement de logs…)			Responsabilité partagée	
Systèmes d'exploitations (mises à jours, maintenance…)				
Equipements physiques (serveurs, disques durs…)				
Réseaux physiques (routeurs, switchs…)				
Centre d'hébergement (salles serveurs, protections électriques, climatisation…)				Responsabilité de l'éditeur

2. Quelles questions se poser en termes de sécurité ?

La sécurisation des données

Evaluer les risques :

- Pertes
- Accès illégitimes
- Altérations

Comprendre les impacts :

- Pertes financières
- Défaillance légale
- Image de l'entreprise

Prendre des mesures, mais quelles sont vos responsabilités ?

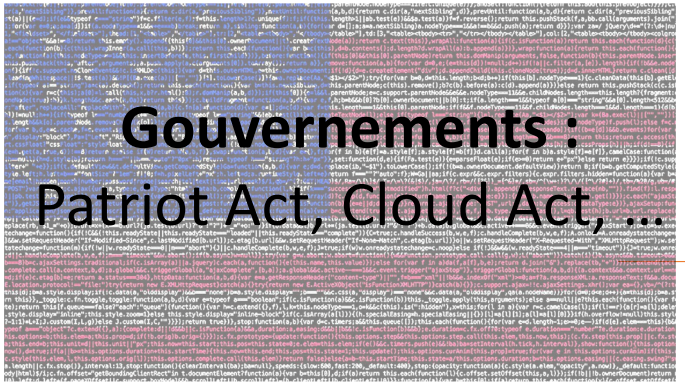
2. Quelles questions se poser en termes de sécurité ?

Certifications et conformités du prestataire

Management :
ISO 2700X, SOC X …

Géographiques :
RGPD, Privacy Shield, …

Secteurs :
Hébergeurs de Données de Santé, Autorité des Marchés Financiers, …



Gouvernements :
Patriot Act, Cloud Act, …

3. Est-il possible d'échapper au Cloud ?

- Nouveau modèle économique
- Mêmes acteurs
- Rôle de la DSI dans l'Entreprise
- Shadow IT …

Quelles alternatives ?

3. Principaux axes de réflexion sécurité / architecture Cloud

1. Gestion des identités
2. Définition du niveau d'engagement
3. Propriété des données
4. Intégration avec le SI
5. Traçabilité des actions
6. Auditabilité

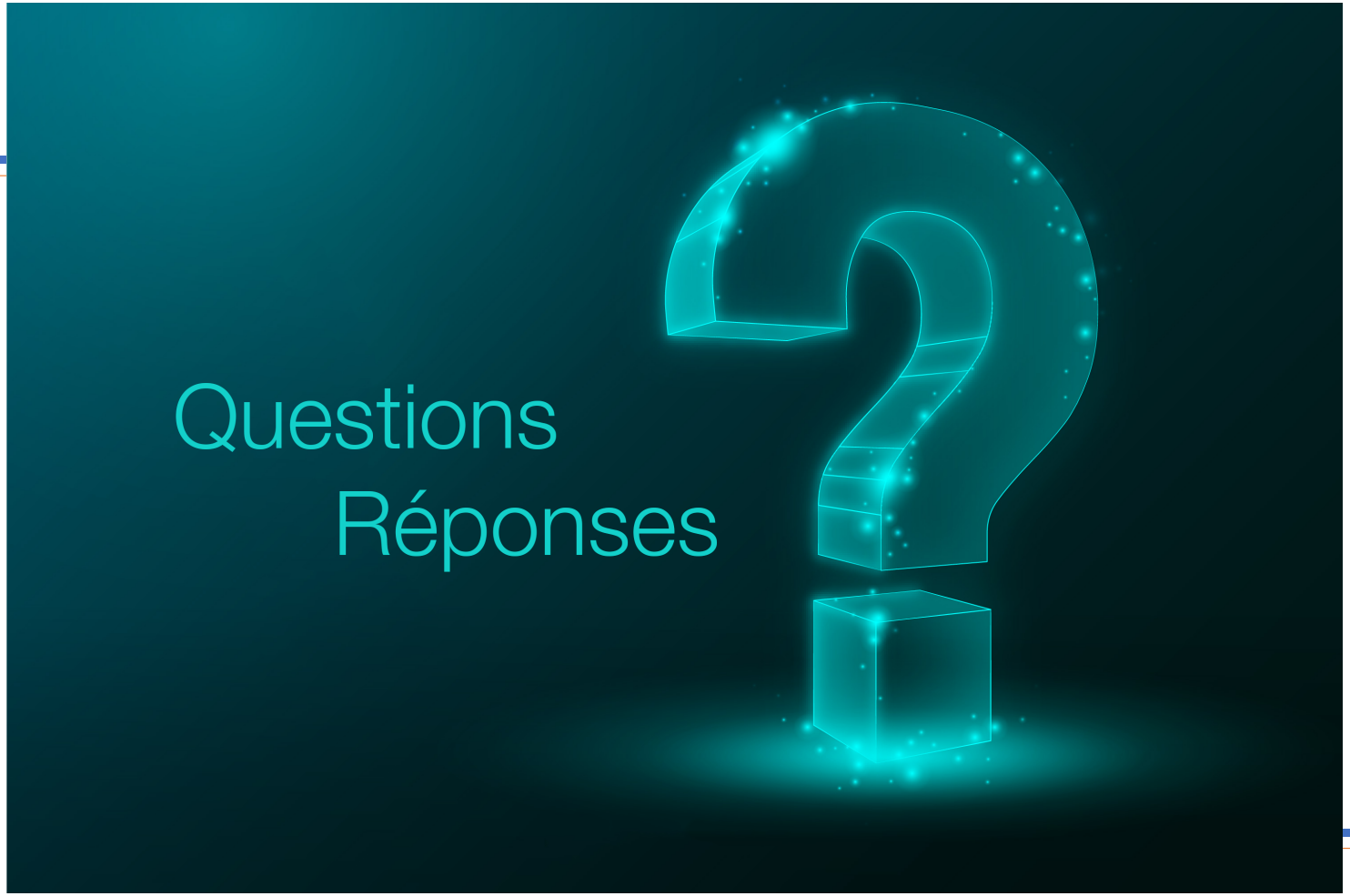
VOTRE CONTACT

Thomas VIERLING

Directeur & Consultant Sénior

tvierling@lpb-conseil.com

+33 (0)6 07 17 28 77


Questions
Réponses

La Gendarmerie, la RC & AD Honores

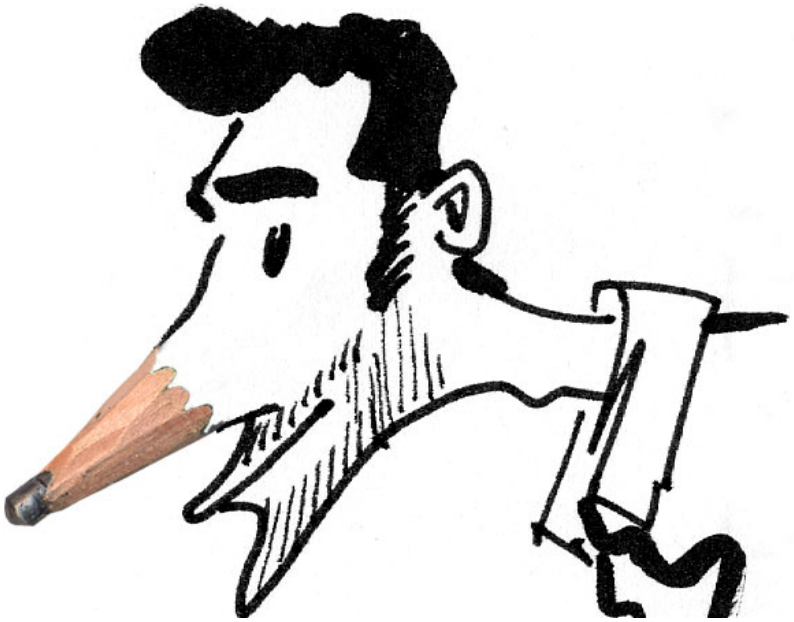
FRC 2019 : REMERCIEMENTS

L'équipe d'organisation

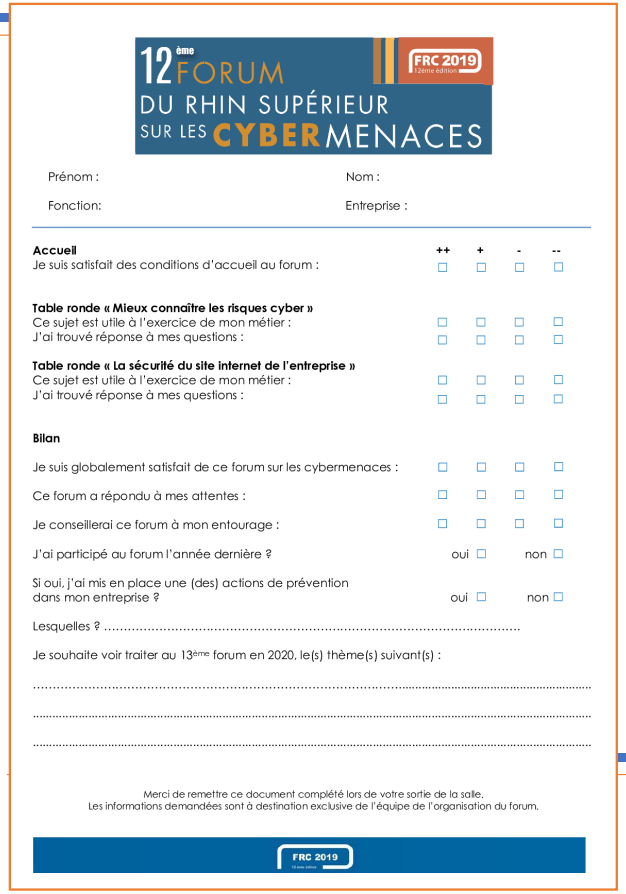
Emmanuelle HAASER
Isabelle HUCK
Johan MOREAU
Jonathan WEBER
Didier SCHERRER
Hervé HUMBERT
Daniel GUINIER
LCL. Jean-Michel ROBINET
Col. Didier LIMET
Adj. Pierre MEYER
Elony GONÇALVES

FRC 2019 : REMERCIEMENTS

Laurent SALLES



FRC 2019 : Fiche d'évaluation



12ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

FRC 2019 12ème édition

Prénom : Nom :

Fonction: Entreprise :

	++	+	-	--
Accueil				
Je suis satisfait des conditions d'accueil au forum :	☐	☐	☐	☐
Table ronde « Mieux connaître les risques cyber »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Table ronde « La sécurité du site internet de l'entreprise »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Bilan				
Je suis globalement satisfait de ce forum sur les cybermenaces :	☐	☐	☐	☐
Ce forum a répondu à mes attentes :	☐	☐	☐	☐
Je conseillerai ce forum à mon entourage :	☐	☐	☐	☐

J'ai participé au forum l'année dernière ? oui ☐ non ☐

Si oui, j'ai mis en place une (des) actions de prévention dans mon entreprise ? oui ☐ non ☐

Lesquelles ? .....

Je souhaite voir traiter au 13ème forum en 2020, le(s) thème(s) suivant(s) :

.....

.....

.....

Merci de remettre ce document complété lors de votre sortie de la salle.
Les informations demandées sont à destination exclusive de l'équipe de l'organisation du forum.

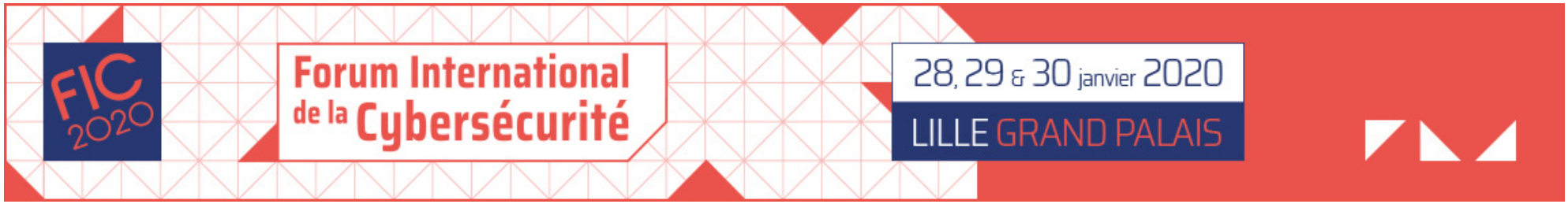
FRC 2019

FRC

Notre site : www.frc.alsace

Notre Twitter : @cybermenaces

NOS PROCHAINS RENDEZ-VOUS



NOS PROCHAINS RENDEZ-VOUS

Le 19 mars 2020

NOS PROCHAINS RENDEZ-VOUS

Au printemps 2020

NOS PROCHAINS RENDEZ-VOUS

13

FRC 2020
13 ème édition

Le 03 novembre 2020