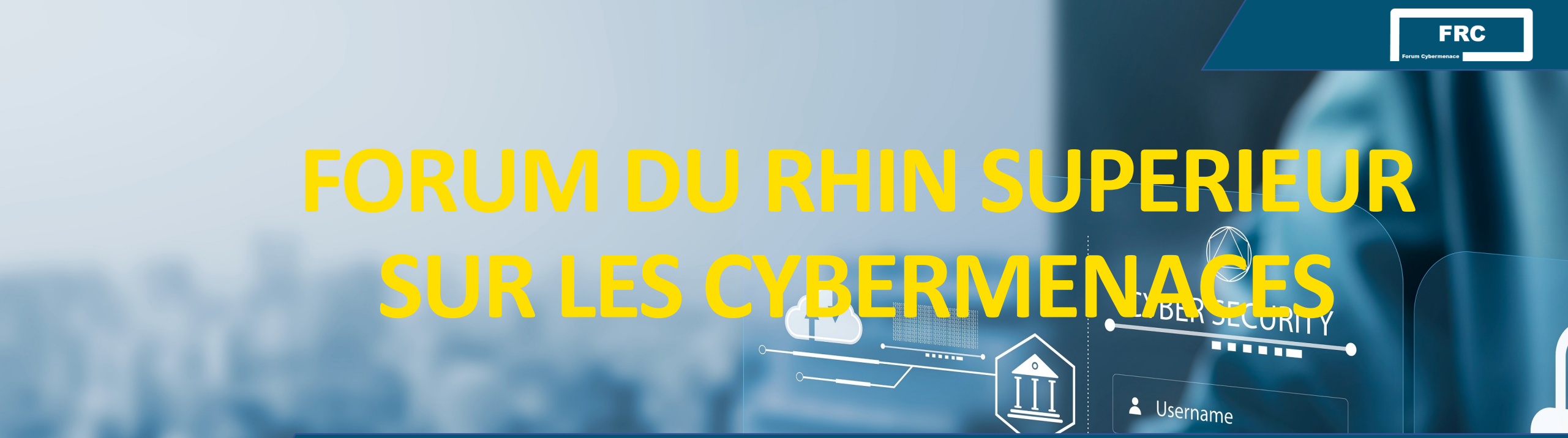
FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES



15ème FRC - INSP Strasbourg - Auditorium Michel Debré

Données hébergées et services dans les centres de données

Où seraient vos données en cas de sinistre dévastateur ?

EDITION 2022

Le Forum du Rhin supérieur sur les Cybermenaces

2017

2018

2019

2020

2021

2013

2014

2015

2016

2009

2010

2011

2012

2022

Madame Emmanuelle HAASER

Responsable veille et marketing- CCI Alsace Eurométropole

Lieutenant-colonel (RC) de la Gendarmerie Nationale

Général Jude VINOT

Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

Monsieur Jean-Luc HEIMBURGER

Président de la CCI Alsace Eurométropole

Monsieur Jean ROTTNER

Président de la Région Grand Est

Le programme du FRC 2022

DATA CENTERS : Et vos données en cas de sinistre dévastateur ?

8 NOVEMBRE 2022
auditorium de l'INSP
1 rue Sainte Marguerite à Strasbourg

FRC 15ème édition

13H00 ouverture des portes

13H30 discours d'ouverture

Général Jude VINOT - Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin
Jean-Luc HEIMBURGER - Président de la CCI Alsace Eurométropole
Jean ROTTNER - Président de la Région Grand Est
Josiane CHEVALLIER - Préfète de la Région Grand Est - Préfète du Bas-Rhin

Emmanuelle HAASER - animation - LCL (RC) Gendarmerie Nationale

14H00 conférence plénière

La résilience des systèmes d'informations et de communications, un enjeu majeur.

Général de Corps d'Armée Frédéric AUBANEL - Commandant du ST(SI)2, le Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure

14h30 table ronde # 1 : faits et témoignages

L'incendie dévastateur de centres de données à Strasbourg en 2021
Daniel GUNNER - Expert judiciaire honoraire - Anc. expert devant la CPI de La Haye - Colonel (RC) de la gendarmerie nationale

Pilotage et communication lors d'un sinistre catastrophique
Didier HEIDERICH - Président de l'Observatoire International des Crises - Président de HEIDERICH Consultants

Témoignage(s) d'organisme(s) impacté(s)

15h45 pause

16H15 Table ronde # 2 - obligations et état de l'art

L'informatique en nuage : la clarté des risques face au brouillard des responsabilités
Ludovic HAYE - Sénateur du Haut-Rhin - Colonel (RC) de la gendarmerie nationale

Assurance et rôles des parties
Michel SCHIRA - Directeur technique des Assurances de Biens et de Responsabilité au sein du Groupe ROEDERER

Audit et certification des centres de données
Jean-François BEUZE - Président Directeur général de SIFARIS Conseil en stratégies et en cybersécurité

Centres de données du futur
Fabrice COUPRIE - Président d'Advanced Mediomatrix

17h45 conférence de clôture

Général Marc WATIN-AUGOUARD
Général d'armée (2S)
Fondateur du Forum International de la Cybersécurité (FIC)
Président de l'Institut National pour la Cybersécurité et la Résilience des Territoires

18H30 cocktail

entrée libre
demande d'inscription sur
www.adhonores.alsace
formulaire en ligne

INSP
Institut national
du service public

FRC 2022 : Nos partenaires

CCI ALSACE EUROMÉTROPOLE

FRC 2022 : Nos partenaires

FRC 2022 : Nos partenaires

La Région Grand Est

FRC 2022 : Nos sponsors

FRC 2022 : Nos sponsors

BANQUE POPULAIRE
ALSACE LORRAINE CHAMPAGNE

FRC 2022 : Nos sponsors

CRCC

COMPAGNIE
REGIONALE DES
COMMISSAIRES AUX
COMPTES

COLMAR

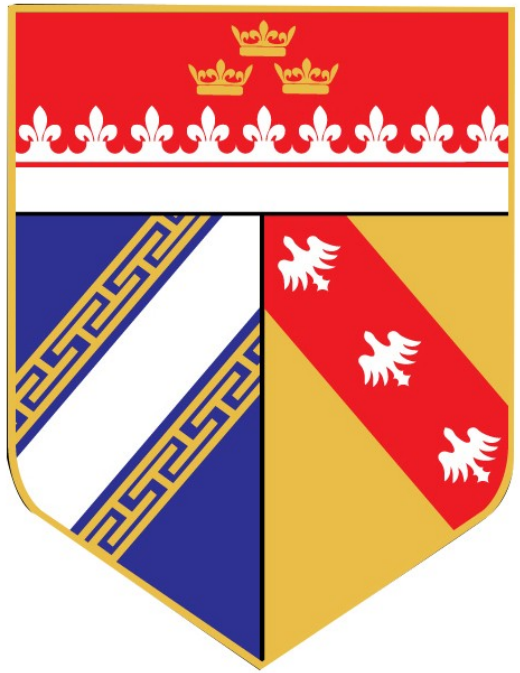
FRC 2022 : Nos sponsors

FRC 2022 : Nos sponsors

SOCIETE GENERALE

FRC 2022 : Nos sponsors

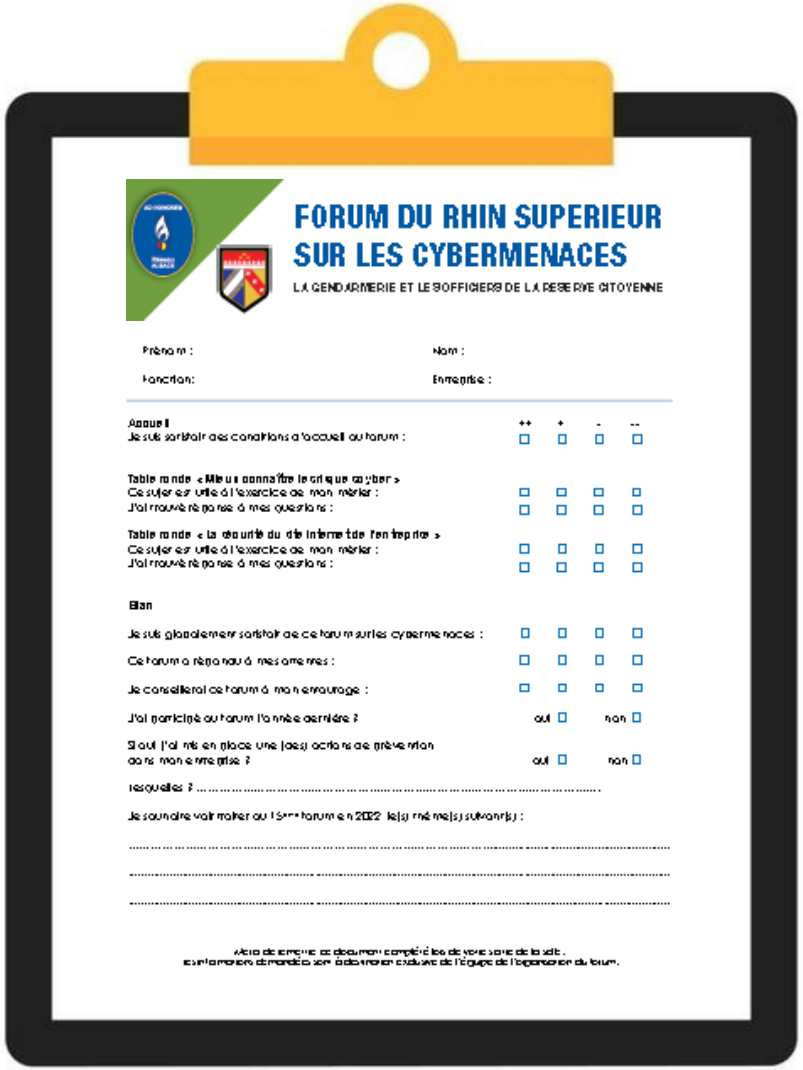
La Gendarmerie, la RCDS et Ad honores - Réseau Alsace



FRC 2022
Notre objectif : Faire connaître et partager

Progresser dans les actions à mettre en œuvre pour la sécurité des données face à un sinistre désastreux possible

FRC 2022 : Fiche d'évaluation



FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

LA GENDARMERIE ET LE SOFFICIERS DE LA RESERVE CITOYENNE

Prénom : Nom :

Fonction: Entreprise :

	++	+	-	--
Accueil				
Je suis satisfait des conditions d'accueil au forum :	☐	☐	☐	☐
Table ronde « Mieux connaître la stratégie cyber »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Table ronde « La sécurité du développement 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 souhaiterais voir traiter au 3ème forum en 2022 le(s) thème(s) suivant(s) :

.....

.....

.....

Merci de remettre ce document complété lors de votre sortie de la salle.
Il sera ensuite demandé son dépouillement exclusif de l'équipe de l'organisation du forum.

FRC 2022 : Notre fidèle dessinateur

FRC 2022 : Connexion WiFi et Internet

Connexion au réseau Wifi : WIFI_INSP

Identifiant : **cybermenaces**

Mot de passe : **k47uzCQ2**

Profil : **EVENEMENT**

N’hésitez pas à consulter notre site :
https://adhonores.alsace/

Dans le respect de la charte informatique de l'INSP

La résilience des systèmes d'information et de communications, un enjeu majeur

par le colonel Sébastien HAMEL

Conférence plénière

EDITION 2022

Plan

1- Le service des technologies et des systèmes d'information de la sécurité intérieure

2- La résilience : de quoi s'agit-il ? Un enjeu majeur...

3- La résilience - Les risques

4- La résilience : une stratégie globale… focus sur le centre de données

5- Histoire de la construction du SI des forces de sécurité intérieure

Le Service des Technologies et Systèmes d'Information de la Sécurité Intérieure

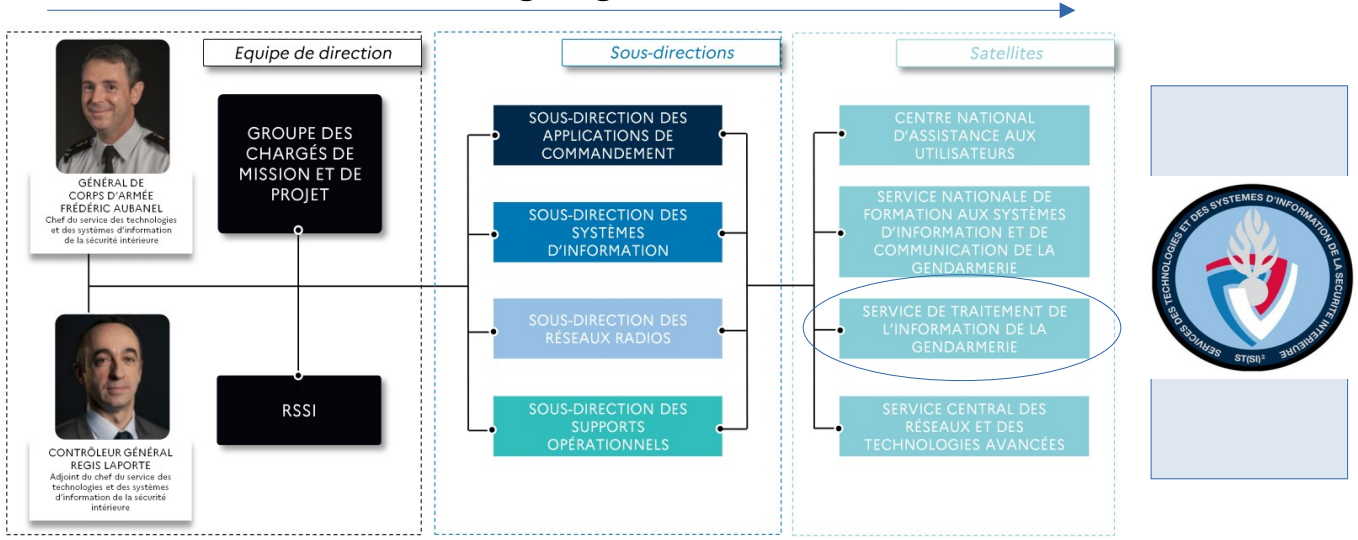
Créé en **2010** pour accroître la capacité opérationnelle des forces de sécurité intérieure sur le terrain par la fourniture d'un service adapté, sûr, efficient, **résilient** pour **LA SÉCURITÉ DES FRANÇAIS**

Maîtrises d'ouvrage et d'œuvre des systèmes opérationnels des forces de sécurité intérieure

En **2015**, maîtrise d'œuvre des réseaux RADIO, de la mobilité et de la proximité numérique (plateformes)

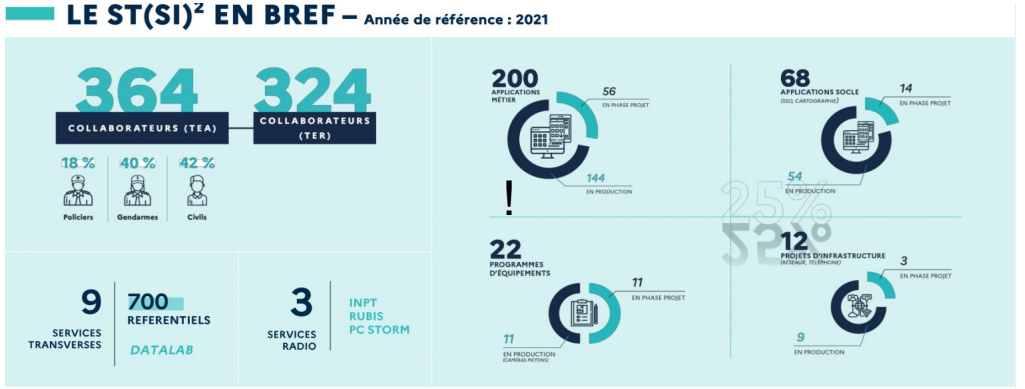
En **2023**, création de l'agence du numérique des forces de sécurité intérieure, rattachée aux 2 directeurs

Organigramme



Service du Traitement de l'Information Gendarmerie

Opère le centre de données



Clients : **250 000 gendarmes et policiers** répartis sur près de **4000 sites** géographiques - **la population** sur l'ensemble du territoire national

La résilience : de quoi s'agit-il ? Un enjeu majeur

- **La résilience** : il s'agit de la capacité d'un système informatique à **résoudre les problèmes** et à **continuer de fonctionner** en cas **d'incident, de panne, d'augmentation de charge ou de piratage** – elle doit être appréhendée de manière globale

- **Un enjeu fonctionnel majeur** : garantir aux gendarmes et policiers de terrain qu'ils pourront, **en tous lieux, tous temps et toutes circonstances, accéder aux applications métiers**, même en mode dégradé, pour garantir **la sécurité des français**
- → En effet, Quid de l'individu, contrôlé sur le territoire national, sous main des forces de l'ordre, qui pourrait se soustraire à ses obligations, parce que **les fichiers de police (personnes recherchées, antécédents judiciaires, etc) ne sont pas accessibles,** et faire ainsi peser un risque d'ordre public, voire terroriste, sur nos concitoyens ?

- **La résilience – une réflexion globale** : terminaux ↔ liaisons ↔ centre de données (applications) opéré

- **Les enjeux techniques : Maîtrise** des technologies et des coûts (souveraineté) – Principes de **modularité** (terminaux d'accès au SI – liaisons - briques socle – applications), de **cloisonnement** du SI (choix d'architecture réseau → image du sous-marin) et de **redondance** - **Sites multiples** (bascules et sauvegarde données)

La résilience - Les risques

- **Risques en fonctionnement courant** : réflexion non aboutie, défaillance interne d'un exploitant ou externe d'un partenaire ou prestataire de service (problème de conception, mauvaise implémentation, erreur humaine d'exploitation, service externe non résilient, attaque sécurité, charge indue, déni de service)
- **→ 2020 : après un arrêt, 50 % des organisations ont perdu des données** - Malgré l'évolution vers le Cloud (privé, public, hybride), parmi les entreprises, près de **deux tiers déclarent ne pas disposer d'une protection haute disponibilité et d'une reprise après sinistre** après le stockage de leurs données dans le Cloud
- **→ 2019 : pour les forces de sécurité intérieure : retour d'expérience après la coupure électrique d'août 2019**

- **Risque de catastrophe** : **naturelle** (tremblement de terre, inondation, incendie) - **attentat terroriste** (impact POST ATTENTATS 2001 !)
- **- réflexion globale sur la résilience** → focus sur le centre de données (décisions : **sites distants** A/A, **capacité humaine 24/7** rapidement projetable - statut militaire, **renforcer la technique et l'organisation** (systèmes matériels redondants, documentations), **plans de continuité et de reprise d'activité** régulièrement éprouvés
- - **sponsor / pilotage central** : Plan Global de Secours (technique / organisationnel), audits réguliers, suivi des recommandations et remédiations (CODIR / GSOP)
- - **certifications ISO** 20k (qualité de service), 27001 (organisation) et 22301 (planifier, mettre en œuvre, exploiter, surveiller, réviser, maintenir et améliorer de manière continue un système d'information) → **professionnaliser l'exploitation du centre de données et les échanges entre production, DSI, Clients**

- **Risque Cyber** : nécessite, au-delà des mécanismes de résilience et de sécurité du SI, une **posture de Vigilance & Protection → sensibilisation et surveillance**
- **→ 2020 : revenus mondiaux pour les cybercriminels : 1 522,6 milliard de dollars / an**
- **→ Coût de la cybercriminalité pour les victimes : 6 000 milliards de dollars / an (190 000 dollars / s)**
- **IMMUNITÉ Cyber Gendarmerie** : évaluer sa sécurité numérique en 10 points et prendre les mesures permettant de limiter ce risque
  - **I**nventaire, **M**ots de passe, **M**ises à jour et sauvegardes, **U**tilisateurs sensibilisés, **N**eutralisation des virus / attaques, **I**nformatique et liberté (protection des données nominatives), **T**élétravail en sécurité (Protection des portes d'accès au SI), **É**valuation régulière, **Cyber** attaques anticipées et contenues (système cloisonné)
- **Conséquences importantes** → perte voire cessation d'activité, perte de données (patrimoniales), perte financière, atteinte à l'image, etc

La résilience : une stratégie globale… focus sur le centre de données

- **Diagnostic** : Identifier **les processus métiers et les données (patrimoine)** pour lesquels continuité / reprise d'activité doivent être assurées dans les circonstances les plus défavorables (à titre d'exemple : garantir un accès aux éléments secrets, fiches techniques et documentations, etc)
- **Analyse** des risques, projets techniques à mener pour garantir la résilience, besoins matériels et en organisation, à partir des enjeux et du diagnostic (itératif - cycle d'amélioration continue)
- **Réflexion globale** : comment assurer la résilience sur l'ensemble de la chaîne : terminaux, liaisons, **focus sur le centre de données opéré**
- **Construction du SI et de ses composants** : veille technologique sur les solutions d'infrastructure, techniques de sécurité et d'organisation permettant de **garantir la résilience du SI** – **« Sécurité et vie privée dès la conception »** – dans un contexte d'ouverture des centres de données et de multiplication des risques (internes / externes)
- **Choix des Infrastructures d'environnement, Architectures de sécurité, Systèmes redondants, répliqués** (des couches basses aux plus hautes) **permettant de garantir un SI disponible, les accès et la consistance des données** patrimoniales et opérationnelles (Disponibilité – Intégrité – Confidentialité – Traçabilité / **Sauvegardes** à chaud et à froid : point d'attention sur les sauvegardes à tester régulièrement !)
- **Résilience** concerne **les bâtiments** (nombre de sites, type / structure, sûreté, protection, cloisonnement, etc), **l'environnement** (énergie, Tableau Général Basse Tension, groupes électrogènes, batteries, onduleurs, chaîne de refroidissement, etc), **les liaisons** (opérateurs et inter-sites), **les équipements réseaux et de sécurité**, **les serveurs**, **les logiciels** (scalabilité, résilience du code – développement Cloud), **les systèmes de stockage (réplication) et de sauvegarde** des données (chaudes, froides, déportées)
- **Aspects organisationnels** : Méthode - processus de mise en production / maintenance / exploitation, documentés et éprouvés - qualité - audits
- **Maîtriser les frontières** du SI : **systèmes de protection périphérique du SI** (D M Z)
- Impact **FORMATION / COMMUNICATION** interne (irriguer l'organisation d'une culture sécurité & résilience), avec les clients et partenaires (contrats de service) **avant, pendant et après l'incident / le sinistre** (retour d'expérience sur chaque incident)
- **Mécanismes de continuité et de reprise d'activité régulièrement testés** pour **limiter les impacts**

- **Exemple : la construction du SI des forces de sécurité intérieure (2000 - 2022)**

- **An 2000** : diagnostic - bug, construction empirique des premiers systèmes d'information (SILO) → perte de maîtrise et augmentation des coûts
- **Attentats de 2001 : réflexion globale – à partir d'une page blanche...**
- **Stratégie** : **Souveraineté** technique et financière – **Maîtrise** du SI, centralisé à base de technologies Web et opensource (lorsque cela répond au besoin) – **Principe de modularité** des briques techniques (socle transverse et applications) répondant à la « sécurité dès la conception » et à la résilience → Inventaire des applications, adhérences et besoins à adresser - Chefs de projets contraints par un **cadre de cohérence technique & le comité des applications** pour **renforcer la cohérence globale et la résilience** du poste de travail jusqu'au centre de données (via les liaisons)
- **Un socle technique central solide sur 2 sites distants** (**architecture efficiente et redondante** des réseaux (cloisonnés) sécurisés, de la gestion des identités & des annuaires, des systèmes d'authentification, des DNS, des PROXY, des systèmes de gestion des traces (obligation juridique), des échanges de données inter-applicatifs (source de données unique consolidée et pas d'adhérences entre applications : utilisation des API)
- **Réseau intranet sécurisé chiffré étendu** jusqu'au plus bas niveau (3500 unités) avec **Garantie de Temps de Rétablissement** - secours bas débit « RUBIS » pour les communications opérationnelles et interrogations fichiers (enjeu institutionnel majeur)
- **Terminaux maîtrisés** : **fixes banalisés** utilisables par tout utilisateur, en tout lieu, dans toutes les unités (plan de continuité d'activité) - **mobiles** depuis 2015 - **portable** depuis tout point d'accès internet en 2020, pour accéder au SI et aux applications métiers – Capacité de pilotage / intervention depuis le central sur les terminaux

Conclusion – le Cloud et les risques associés → tables rondes

La résilience des systèmes d'information et de communications, un enjeu majeur pour le service des technologies et des systèmes d'information de la sécurité intérieure pour assurer la sécurité des français.

Avec l'émergence des technologies et services du Cloud, il est primordial de **catégoriser** les processus métiers, les applications et les données à répartir entre hébergement traditionnel et hébergement de type cloud (privé – hybride ou public) en veillant à **conserver la maîtrise** des éléments de sécurité, systèmes transverses du socle, des applications et données qui représentent le patrimoine des forces de sécurité intérieure.

Cela passe par une **réflexion globale préalable**, l'identification des **systèmes et données d'importance vitale, des risques** qu'ils soient techniques (objet de la table ronde n°1) ou juridiques (objet de la table ronde n°2) et des scenarii (projets) pour les traiter avant que le sinistre n'arrive.

Tout doit être mis en œuvre pour qu'**en cas de sinistre**, vous puissiez **reprendre vos activités essentielles** sur un **centre de données disponible**, bâtiment ou mobile (container), avec des **données consistantes**, par des **personnels « drillés »** à la continuité / reprise d'activité, disposant de leur base de connaissance pour l'exploitation !

FRC
Forum Cybermenace

Daniel GUINIER
Thierry FUSALBA

Table ronde 1: Faits et témoignages

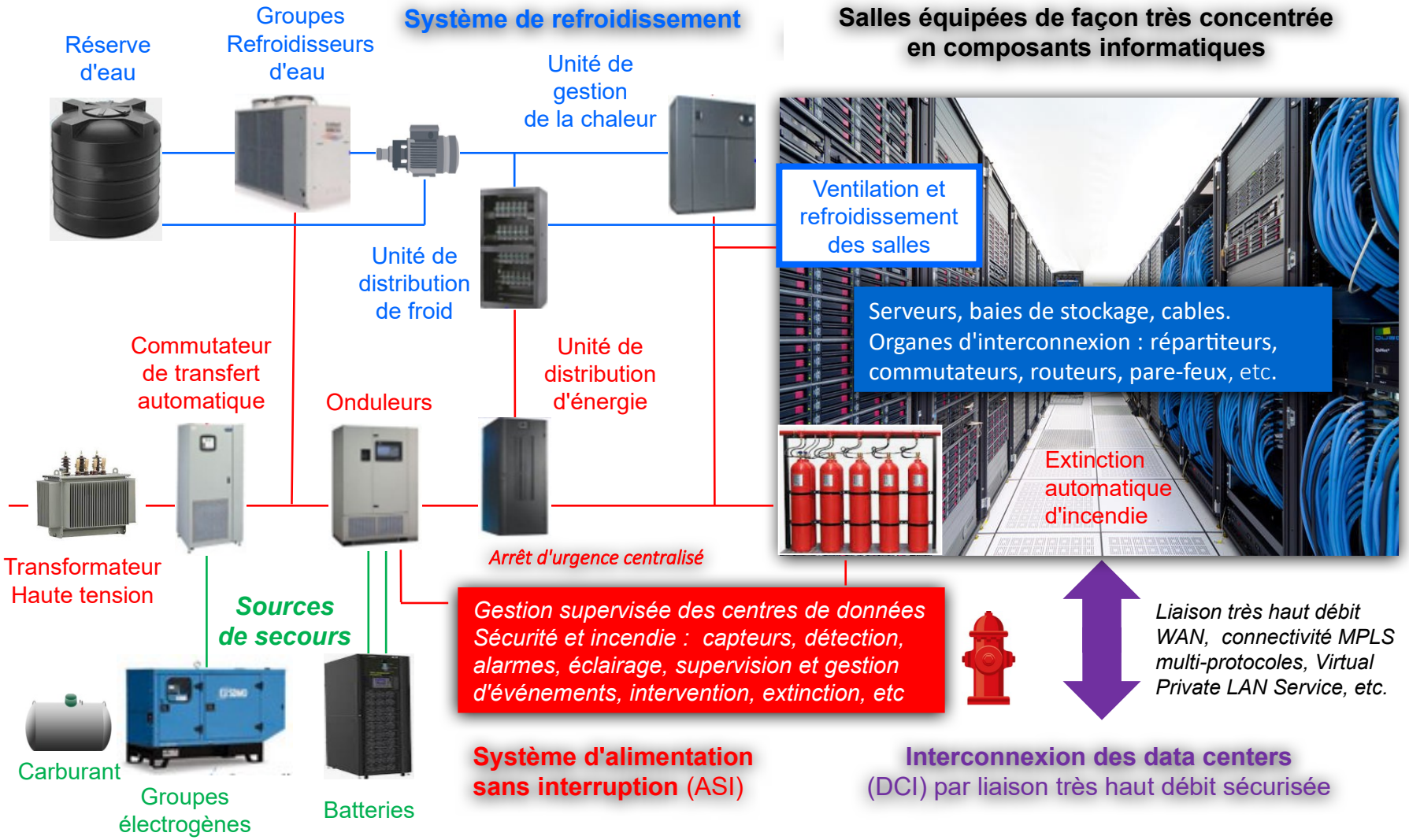
EDITION 2022

L'incendie dévastateur de centres de données à Strasbourg en 2021

par Daniel GUINIER

EDITION 2022

Constituants d'un centre de données



Contenus et contenants d'une salle

Patrimoine informationnel immatériel des clients et de l'opérateur

Patrimoine technologique matériel chez l'opérateur du CdD

"Données" au sens large constituées d'actifs de type et de criticité variés

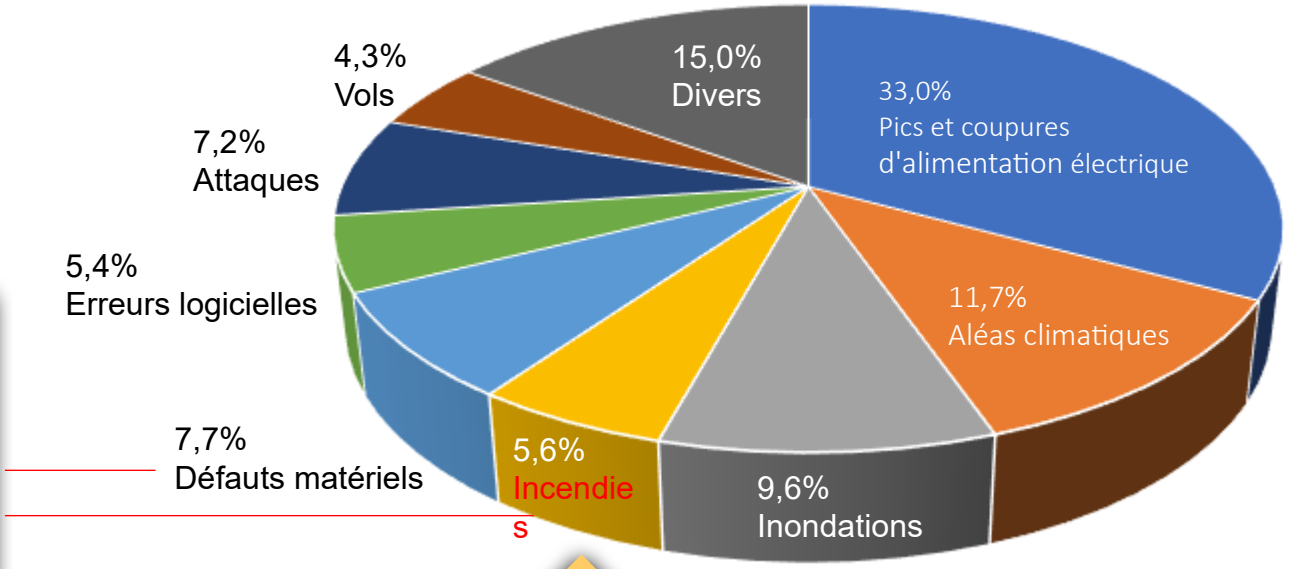
Actifs d'information, actifs logiciels
actifs de fonctionnalités-middleware,
et l'ensemble sauvegardé en autre lieu

Equipements pour la détection, l'analyse, le suivi d'anomalies et les actions immédiates : température, ventilation, humidité, eau, alimentation électrique, caméras, équipements de sécurité physique et logique, et **incendie** : présence d'étincelles, de flammes ou de fumées, extinction automatique par gaz inerte, etc.

Un CdD doit présenter les garanties d'un environnement contrôlé avec des moyens d'urgence et redondants et une sécurité globale liée à l'ensemble du site, sans oublier **les actifs humains et la prise en compte des alentours.**

Risques internes … et de proximité

Exemples cités par Scaleway concernant ses centres de données en France :
Risques internes : Au cours des 10 dernières années : **4 explosions d'onduleurs**, et à **un feu batterie** en 2019.
Risques d'incendie et d'explosion à proximité : En 2013 une entreprise spécialisée dans le recyclage de papier, en 2019, une autre, spécialisée dans le traitement de produits chimiques, ceci à quelques mètres des installations.



Impact important

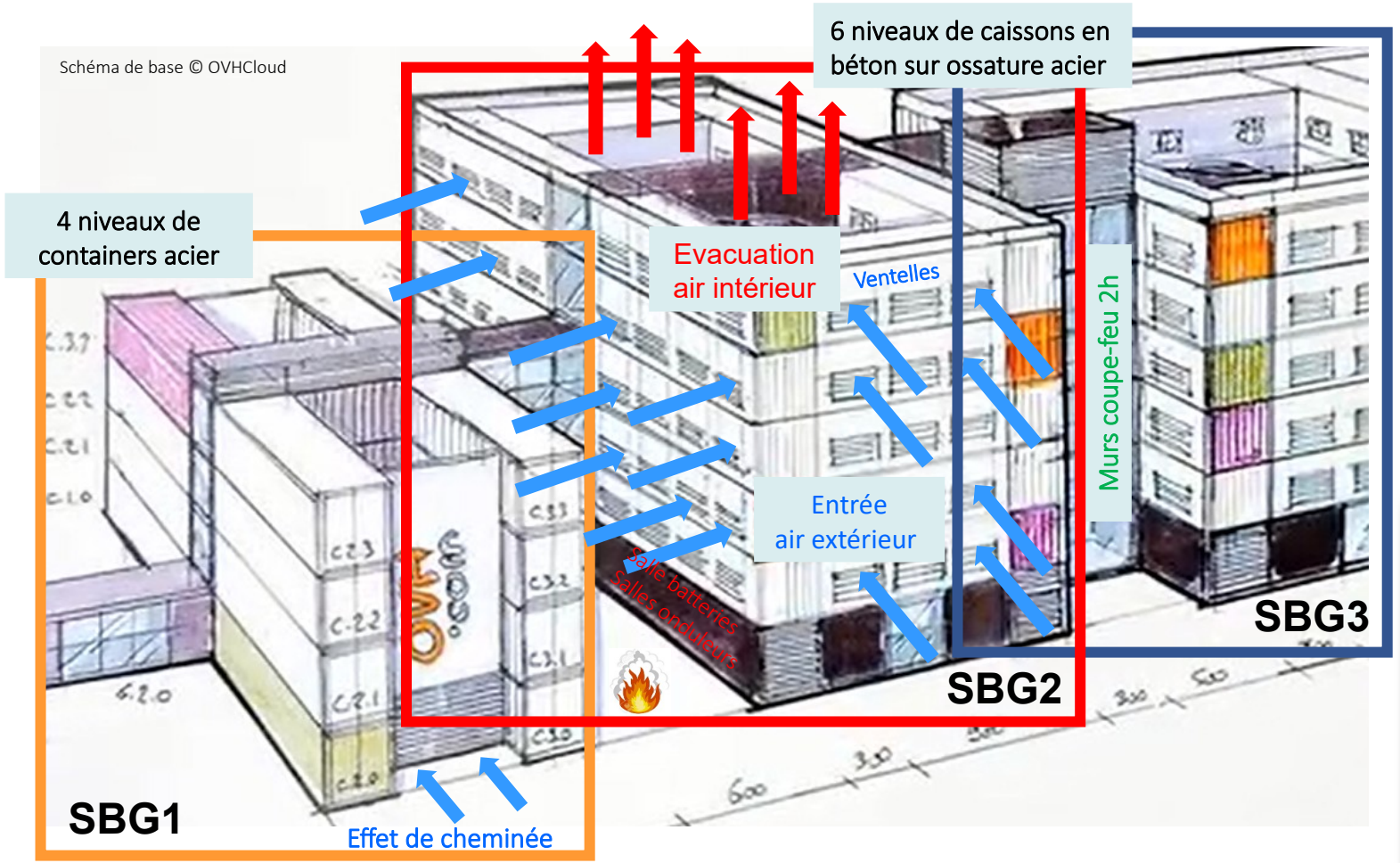
Source : Global Security

Les courts-circuits, les **onduleurs** et les **batteries** représentent les **sources de risques d'incendie les plus courantes**.

31 cas d'incendie de centres de données ont été déclarés de 2003 à 2021, avec un temps d'arrêt moyen de 17,5 heures, *sans refléter la réalité au vu de clauses de non-divulgation et de craintes sur la réputation*.

Source : https://www.lebigdata.fr/incendie-data-center-dossier-complet

Conception modulaire des centres de données d'OVHCloud Strasbourg



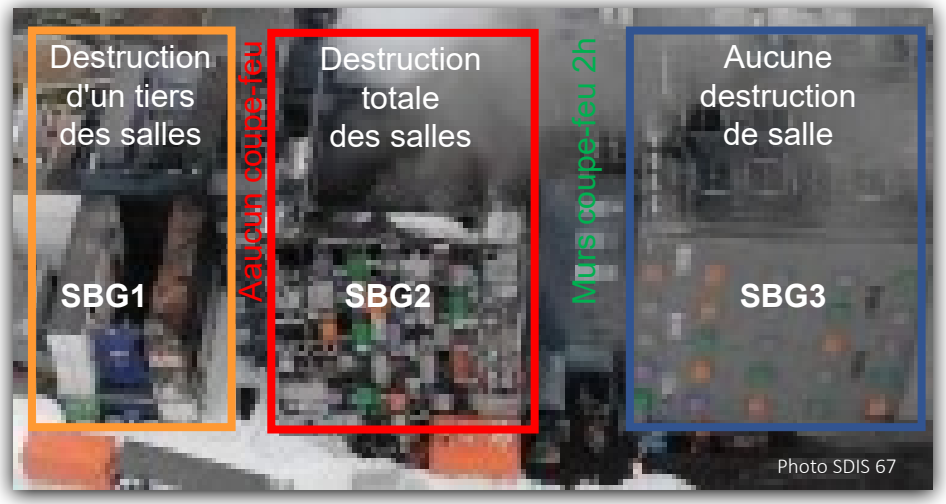
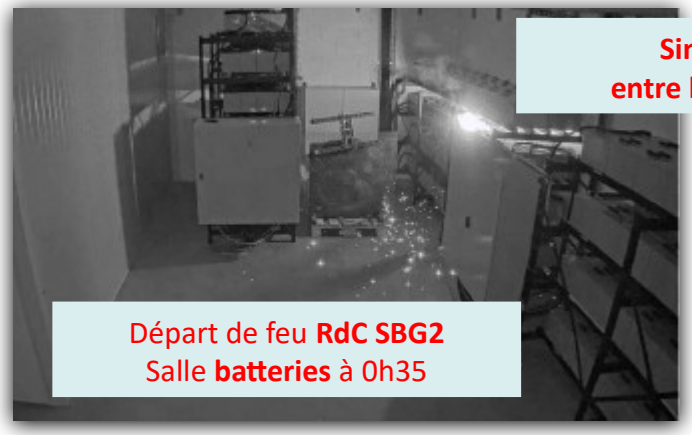


Photo : Sapeurs-pompiers du Bas-Rhin

Etat après l'incendie

Origine et poursuite de l'incendie

Source : vidéosurveillance OVHcloud



Départ de feu **RdC SBG2**
Salle **batteries** à 0h35

Simultanéité et lien entre les deux événements

Départ de feu **RdC SBG2**
Salle **onduleur** 2 à 0h35

La veille au matin, intervention technique sur un des onduleurs, avec changement de composants et remise en fonctionnement dans l'après-midi.

Photos : Sapeurs-pompiers du Bas-Rhin

Un problème électrique est visible simultanément dans deux salles différentes du rez-de-chaussée de SBG2, au niveau d'un onduleur et des batteries qui lui sont reliées.

Chronologie de l'incendie du 10 mars 2021

FRC
Forum Cybermenace

Départs de feu coïncidents
RdC de **SBG2**
Salle onduleur 2 et
Salle des batteries

Alerte incendie provenant de détecteurs et alarmes

Appel SER
(Strasbourg Electricité Réseaux)

00:52

Début d'intervention de SER

01:27

Alim. de SBG2 coupée

01:50

Permanence de courant électrique

02:14

03:28

Coupure effective de l'alimentation du site

01:49

Appel SDIS67

Appel

Bateau pompe EUROPA

02:58 **Arrivée**

Coupure des énergies de secours

00:35 **00:37** **00:39** **00:42** **00:59** **01:13** **01:28**

SBG2

SBG1
SBG3
SBG4

03:42

Tweet d'Octave Klaba, président d'OVHCloud, annonçant un incident majeur

Arrivée du personnel d'OVHCloud **sur le lieu**

Mise en sécurité et **Evacuation de SBG2**

Fumée noire
Propagation rapide du feu

Début d'intervention des sapeurs-pompiers

Concernant SBG2
Dégâts très importants

SBG2 totalement embrasé et propagation du feu sur SBG1

04:09

L'incendie présentait toujours une menace pour les autres centres de données du site

Maîtrise de l'incendie avec quelques foyers résiduels **06:45**
Contrôle total de l'incendie **10:02**
Fin d'intervention sans aucun blessé à déplorer **18:13**

EDITION 2022

Reprise de feu le 19 mars **18:50** Intervention du SDIS67 et arrêt des services du site pour mise en sécurité

Répercussions directes immédiates et mesures prises

10 mars

En France
Plus de 18% des adresses IP attribuées à OVHCloud ne répondaient plus

Datastore, VPS, VPS Backup Services, Public Cloud Archive, etc.

Certaines sauvegardes

3,6 millions de sites Web de 464 000 noms de domaine

Indisponibles temporairement pour la plupart

Parmi les plus touchés : 184 000 sites Web de 59 600 noms de domaine .fr

Etablissement du plan de redémarrage provisoire

Estimation attendue entre 19 mars 22 mars

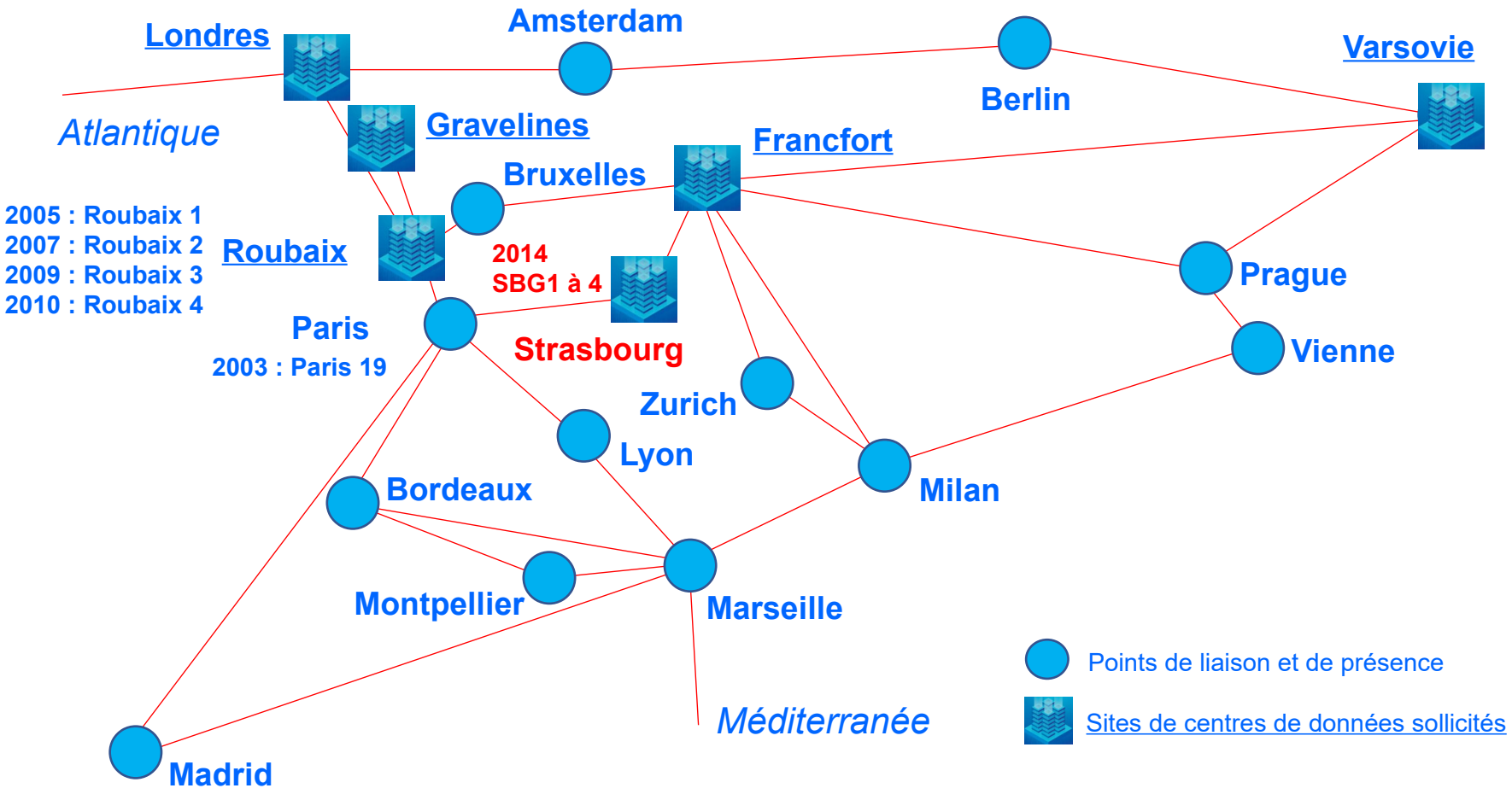
- **pour SBG1 et SBG3 : redémarrage progressif des services** - acheminement de 10 000 serveurs.
- **pour SBG2 totalement détruit : substitution** par des infrastructures d'autres centres d'OVHCloud : *Roubaix, Gravelines, Francfort, Varsovie et Londres*
- **pour SBG4 : mise en sécurité** pour être **en partie opérationnel le 15 mars**

Mise en cause du plan de redémarrage prévu suite à un nouvel incident le 19 mars

- **pour SBG1 : renoncement au redémarrage**
- **migration physique des infrastructures** pour une **reprise totale des services avant le 31 mars**

Des centaines d'entreprises, de villes, d'associations, de clubs sportifs, de médias, de partis politiques, etc., ont été impactés. Sans aucune sauvegarde ou réplication par ailleurs leurs données seraient définitivement perdues.

Sites d'OVHCloud sollicités



Le réseau européen d'OVHCloud est en mesure d'offrir des moyens de secours, de réplication et de sauvegarde distants non soumis au même risque, de façon préférable à un seul *"data-bunker"*.

Conclusion et perspectives

- **De façon générale**, il n'est pas vu :
  - **De gestion adéquate des *"données"*** clairement identifiées dans le cadre d'un **plan de sauvegarde et de géo-réplication**, formalisant les services et responsabilités réciproques.
  - **De véritable PRA/PCA** testé pour gérer une catastrophe ou un sinistre désastreux où les lieux sont dévastés, **dépassant la seule reprise des infrastructures informatiques**.

- **La sécurité des centres de données constitue un défi majeur** exigeant **une stratégie globale** pour s'opposer aux menaces **logiques et physiques**
  - **Par une sécurité "*by-design*"** bâtie dès la phase de conception et tout au long du cycle de vie, identifiant les vulnérabilités et les menaces, pour réduire les risques et la surface d'attaque.
  - **Par une défense en profondeur** assurée par des lignes coordonnées et indépendantes pour que la sécurité repose sur un ensemble cohérent de mesures techniques et non techniques, comme des procédures, plutôt que sur l'illusion de disposer d'un *"data-bunker"*.

Cet incendie n'est pas un incident majeur mais bien une situation qui relève d'un sinistre majeur associé à un lieu de forte concentration technologique.

Bibliographie sélective

BEA-RI : Rapport d'enquête sur l'incendie au sein du centre de stockage de données OVH situé à Strasbourg (67) le 10 mars 2021. Bureau d'enquêtes et d'analyses sur les risques industriels, mai 2022, 43 p.

CST (2020) : Guide sur la défense en profondeur pour les services fondés sur l'infonuagique ITSP.50.104, mai, GdC/CST-CSE, 49 p.

France Datacenter : La sécurité-incendie dans les datacenters. Livre blanc, 2019, 62 p.

Guinier D. : Catastrophe et management - Plans d'urgence et continuité des systèmes d'information. Masson, 1995, 344 p.

Guinier D. : L'informatique en nuages ou *"cloud computing"*, un enjeu pour l'entreprise et un défi pour la sécurité. Conférence plénière. 3ème forum FRC, ENA Strasbourg, 25 novembre 2010.

Guinier D. : Protection des données : Caractéristiques et planification des sauvegardes, 9ème forum FRC, ENA Strasbourg, 8 novembre 2016.

Guinier D. : Cyberattaques et catastrophes : de l'imposture et autres causes à la sidération des entreprises. *Expertises,* n° 418, novembre 2016, pp. 371-376.

Guinier D. : La part humaine déterminante face aux crises majeures. Revue de la Gendarmerie nationale, n° 268, pp. 155-161, janv. 2021.

Guinier D. : L'hébergement des données : un sujet brûlant... Retour sur les convictions et le risque d'indisponibilité. *Expertises,* n°468, mai 2021, pp. 200-204.

Guinier D. : Résilience et management de la continuité d'activité. Tribune publiée par le Cercle K2, 5 pages, publié le 10 juin 2021.

Pilotage et communication lors d'un sinistre catastrophique

par le colonel (r) Thierry FUSALBA

EDITION 2022

Spécificités de la Communication des crises cyber-data

- 3 aspects complémentaires : la destruction de données (accident), les attaques réputationnelles (fake news, désinformation), la criminalité (hameçonnage, rançons…) = *une politique de prévention globale*
- Des acteurs multiples aux attentes et intérêts parfois contradictoires = *fixer des priorités & faire des choix*
- Absence des 3 V (vilains, victimes, visuels) + la grande technicité = *peu d'intérêts des audiences donc des journalistes*

La gestion de crise ne se résume donc plus au pilotage mais :

Prévention (veille, détection) **+ pilotage** (réaction, solution) **+ exploitation** (cicatrisation, correction)

La problématique d'une réponse adaptée pour OVH

1 / La nature du sinistre :

- Facteur aggravant 1 : mise en cause de l'entreprise pour défaut de sécurité
- Facteur aggravant 2 : *bis repetita non placent (nuit 10/3 et 19/3)*
- Facteur aggravant 3 : ampleur sinistre (1 centre détruit et un endommagé) = interruption services et pertes données pour des milliers entreprises et services publics

2 / La nature de l'activité :

- Facteur complexifiant 1 : sensibilité des données vs. Transparence
- Facteur complexifiant 2 : service H24/7 = priorité au redémarrage
- Facteur complexifiant 3 : spécificités techniques vs « vulgarisation »

Principes d’une COM2Crise lors d’un sinistre Cyber

Faut-il communiquer et vers qui ?

- 99% des cas, oui
- L’interne (par sécurité), les autorités (CNIL, Préfecture, clients…), les assurances
- Et les médias ?

Faut-il tout dire ?

- Selon les audiences
- Selon son niveau de connaissance
- Selon sa situation

Et les médias ?

- Oui, mais pas tout
- Oui, mais pas tout de suite
- Oui, mais pas tous

UNIQUE C4

« Préparez-vous au pire, avec les meilleurs »

Understand	Analyse de l'environnement et des acteurs	
Name	Bornage de la crise & des possibilités d'action	
Identify	Identification des stratégies adverses (ME) et des scénarios d'évolution	
Qualify & Quantify	Recherche des modes d'actions (MA) possibles	
Unify	Confrontation MA/ME et choix d'une stratégie	
Experiment & Exploit	Mise et œuvre MA choisi et conduite vers la sortie de crise	

UNIQUE C4

Thierry FUSALBA, Col (r)
Fondateur, directeur
www.agencec4.com

FRC
Forum Cybermenace

Témoignage(s) d'organisme(s) impacté(s)

EDITION 2022

Pause – 30 minutes

FRC
Forum Cybermenace

Ludovic HAYE
Michel SCHIRA
Jean-François BEUZE
Fabrice COUPRIE

Table ronde 2 : Obligations et état de l'art

EDITION 2022

L’informatique en nuage : la clarté des risque face au brouillard des responsabilités

par le sénateur Ludovic HAYE

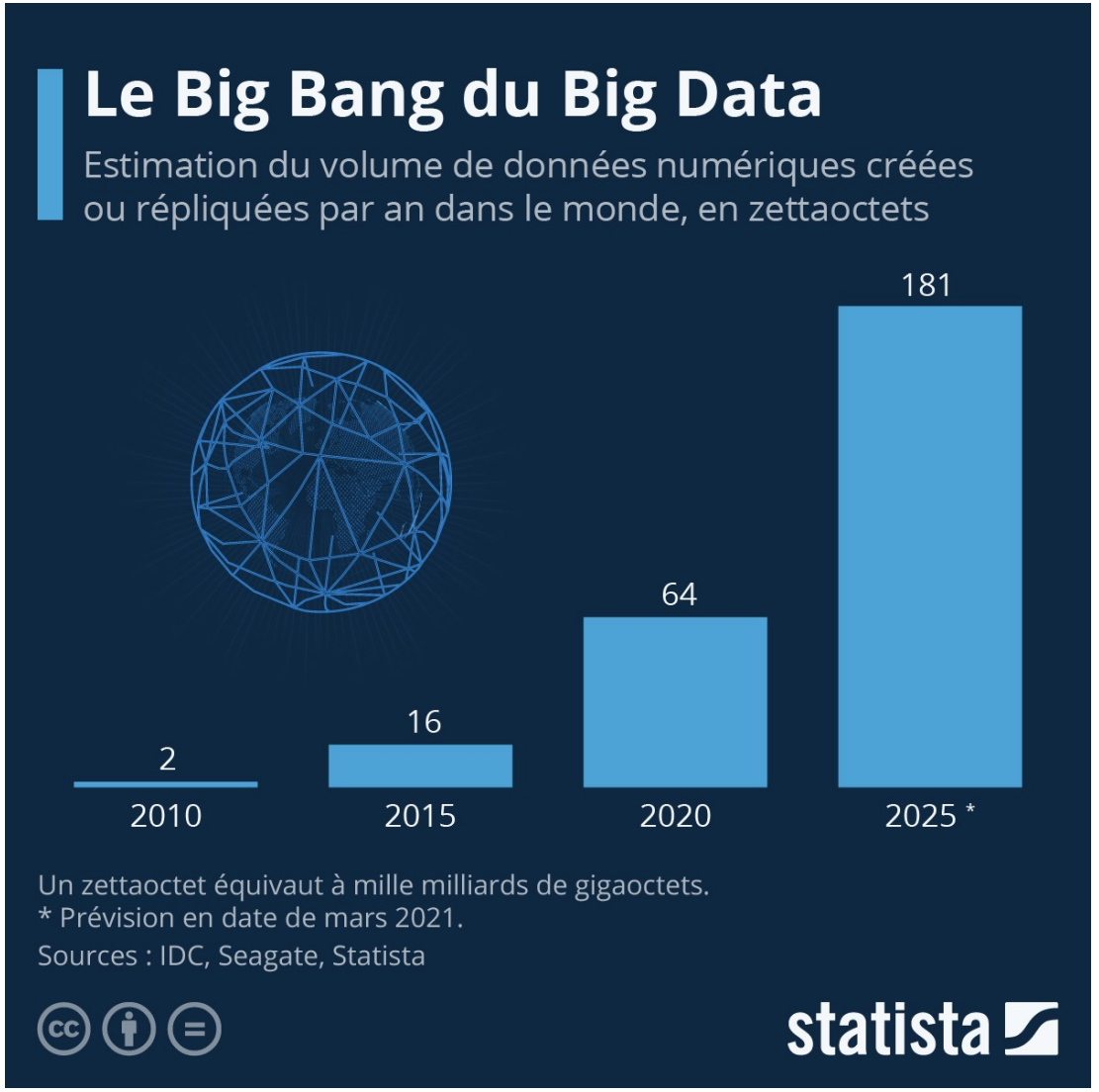
EDITION 2022

Le cloud et le Big Data : une 4ème révolution industrielle

L'utilisation du cloud et des data-centers est devenue inévitable :

- Augmentation exponentielle des données que l'Humanité produit
- Activités croissantes qui nécessitent beaucoup de données (streaming, IA, objets connectés…)

90% des entreprises européennes utilisent le cloud computing en 2022



1. Les risques physiques

- Accidents liés au fonctionnement du data-center (forte émission de chaleur, fort besoin en eau pour climatiser, panne électrique)
- Obsolescence du matériel (l'usage intensif accélère l'usure des composants)
- Sabotages (intrusions ; destruction du matériel ; coupure des câbles de fibre reliant les usagers ; vol de données)

Incendie d'un data-center d'OVHCloud à Strasbourg (mars 2021)

Pertes :
- *3,6 millions de site web*
- *464.000 noms de domaine*

Environ 16.000 clients impactés

Crédit photo : zdnet.fr

2. Les risques logiques

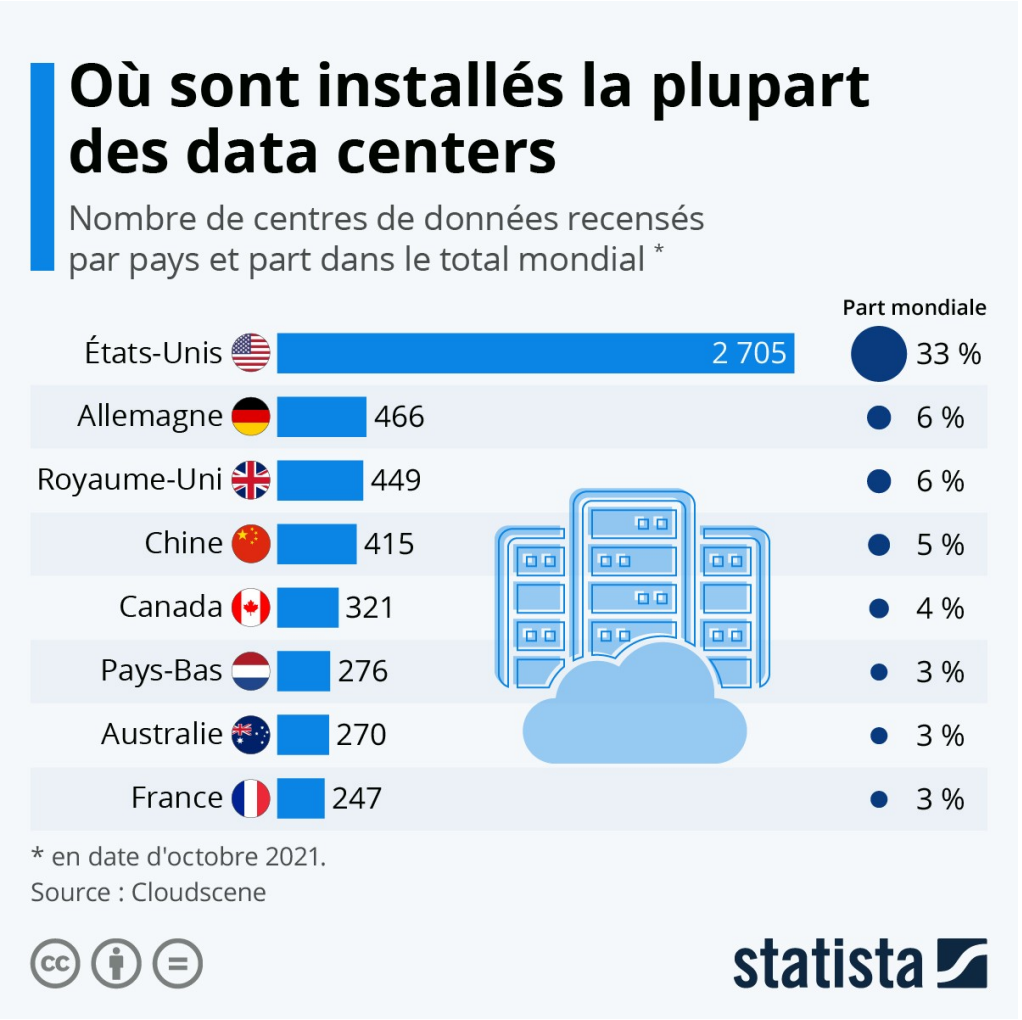
- Obsolescence des logiciels permettant l'exploitation du data-center (surtout pour la majorité des clients utilisant un SaaS)
- Cyberattaques (usurpation des comptes administrateur ; DDoS ; ransomware ; manipulation des tables de routage pour saboter le trafic)

3. Les risques légaux

Le cloud est in-fine un endroit physique, avec un emplacement géographique et qui suit les lois du sol.

Les lois auxquelles sont soumises les données stockées dépendent :

- Du pays où se trouve le data-center (difficile de le savoir car le stockage des données n'est pas linéaire)
- Des pays par lesquels transitent les données (où passent les câbles)
- De l'origine des composants matériels des infrastructures (extra-territorialité du droit américain)



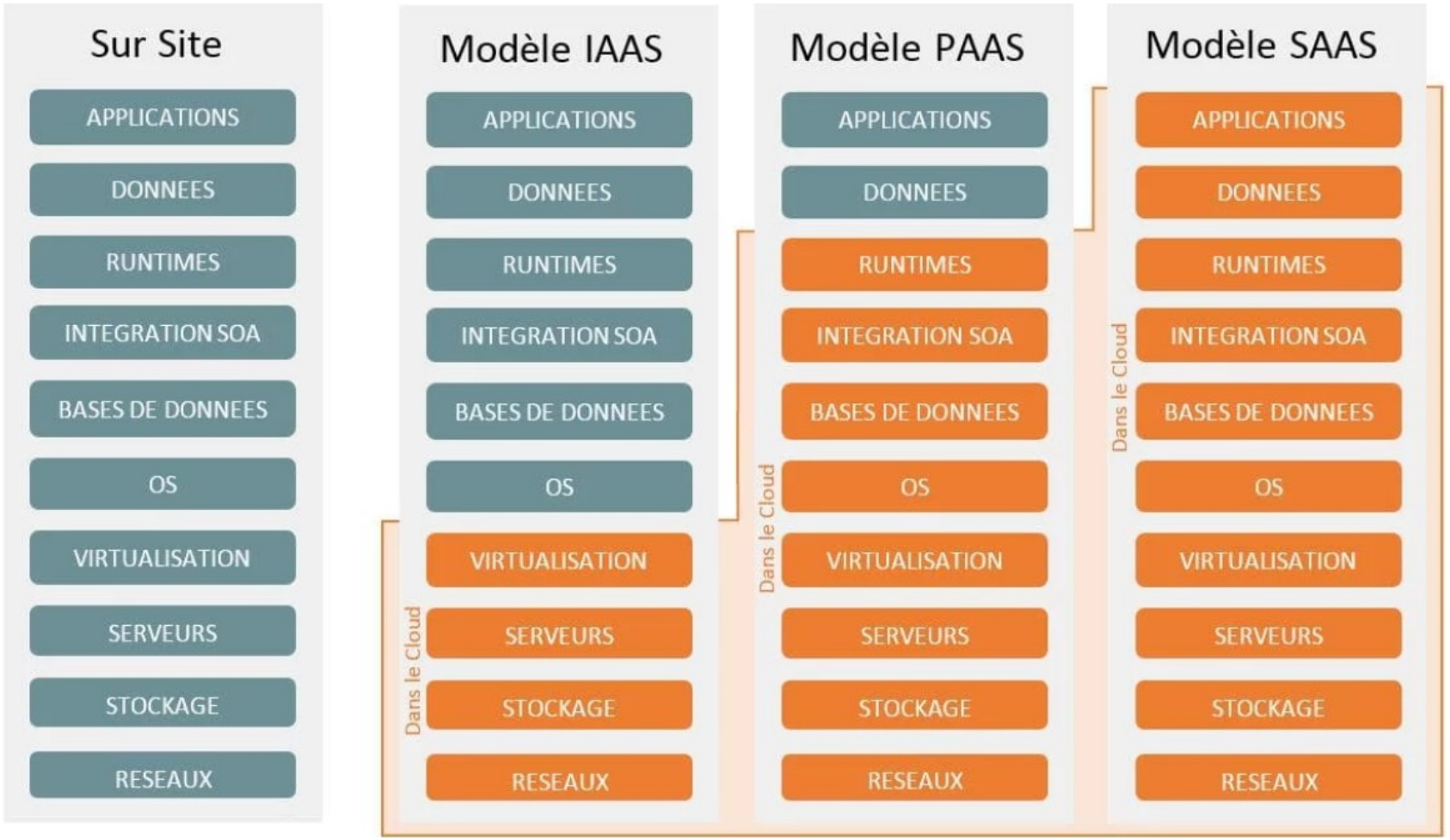
4. Les risques contractuels

Rappel : cloud = modèle où le client consomme des ressources informatiques (espace de stockage, puissance de calcul, serveurs) **sans en posséder l'infrastructure technique**.

Donc, le client passe de la maitrise d'une infrastructure à la maitrise d'un processus. **Le contrat devient donc l'outil fondamental** pour :

- Définir les droits et devoirs de tous les acteurs de la virtualisation
- Définir des options de redondance et la continuité de service (choix du client)
- Définir les responsabilités en cas de litige

LE BROUILLARD DES RESPONSABILITES



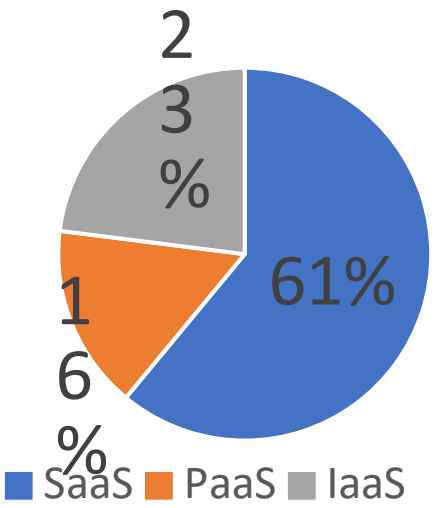
IaaS : Infrastructure as a Service = sous-traitance des infrastructures matérielles
PaaS : Platform as a Service = sous-traitance du matériel + des applications d'exploitation (middleware)
SaaS : Software as a Service = formule « all inclusive » des services cloud

Fournisseur : met à disposition des infrastructures (disponibilité).
Le reste relève d'options et de formules (IAAS, PAAS, SAAS) auxquelles le client **choisit ou non** de souscrire.

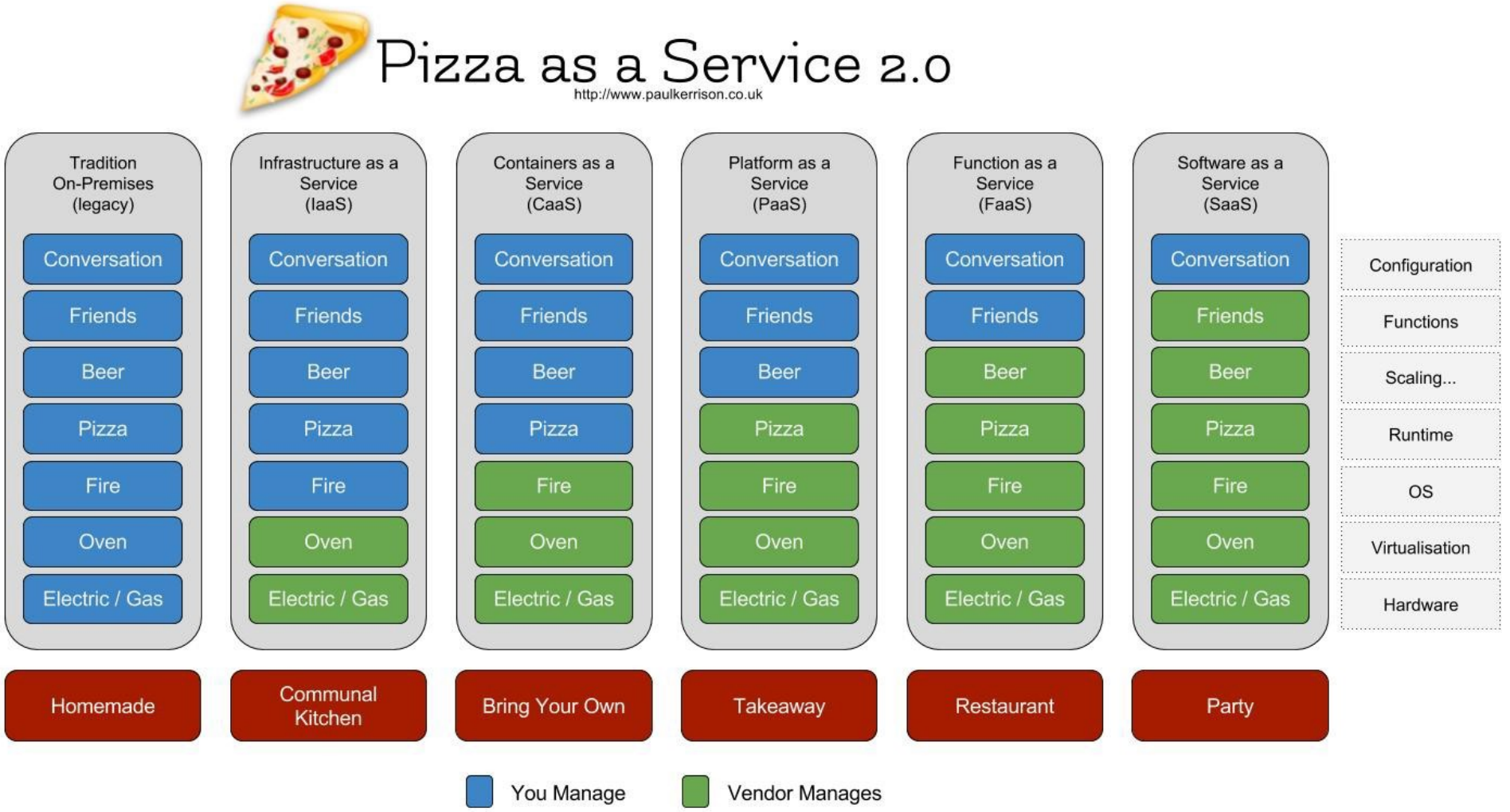
Leurre du cloud dans l'imaginaire des clients qui font le raccourci « C'est dans le cloud, donc c'est redondé et c'est sécurisé ». **Tout a un prix.**

Plus le client délègue, plus il accepte d'exposer ses données et activités.

Services les plus utilisés par les entreprises européennes en 2021



Plus on délègue, plus on perd le contrôle sur ses données



Le partage des responsabilités en cas de pertes de données : qui est responsable ?

La responsabilité de l'hébergeur dépend de **trois facteurs** :

1. **La nature du sinistre** : s'agit-il d'un « cas de force majeur » ? (art L-1218 du Code Civil : événement qui échappe au contrôle du débiteur, ne pouvant être raisonnablement prévu, extérieur à la volonté des parties)

2. **Les clauses du contrat** : Le contrat de base délègue la responsabilité au client. Celui-ci doit lui-même choisir le type de redondance qu'il souhaite mettre en œuvre (sauvegarde, plan de continuité etc.)

3. **La nature des données perdues** : s'il s'agit de données personnelles, la RGPD s'applique. Sinon, il faut se reporter au contrat.

Les responsabilités environnementales

Les data-centers sont des infrastructures très coûteuses en ressources. Leur accroissement doit nous interpeller sur les conséquences environnementales et les responsabilités des acteurs du cloud.

- Forte consommation électrique : 76,8 TWh* en 2020 (16% de la conso française annuelle) : dont la moitié pour le refroidissement
- Forte consommation en eau (pour la climatisation)
- Forte consommation en composants matériels et électroniques (métaux rares notamment)

→ Comment répartir ce type de responsabilité entre les hébergeurs et les clients ?

→ Qui doit assumer les coûts environnementaux de l'essor du cloud computing ?

**Source : rapport Commission européenne 2020*

CONCLUSION

- Les risques qu'entraine le modèle du cloud sont bien connus par les hébergeurs et doivent l'être par les clients
- Les responsabilités des acteurs face à ces risques sont bien moins clairs et suscitent des débats
- Pour le client, le recours à un service cloud peut donner l'illusion d'une simplification du travail et d'une déresponsabilisation de sa part : en réalité, tout dépend du contrat qu'il a choisit
- Lorsqu'on parle des responsabilités, on évoque toujours les considérations premières du client (sécurité des données, continuité de son activité *etc*.). En revanche : on ne prend jamais en compte les conséquences environnementales du recours à ce modèle

Assurance et rôle des parties : avant, pendan
suite à un sinistre catastrophique

par Michel SCHIRA

EDITION 2022

Plan de l’intervention

La clarification des contrats d’assurance sur l’étendue des garanties

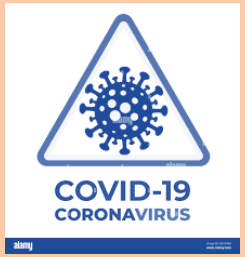
Les principaux contrats d’assurance en lien avec les données



L’intervention de l’assureur et le rôle du client

La clarification des contrats d'assurance

Une vague d'avenants de remédiation consécutive à la crise sanitaire



La réaffirmation du caractère incorporel des données, programmes informatiques et serveurs virtuels

Les principaux contrats d'assurance en lien avec les données

Le contrat d'assurance Dommages aux Biens (= les dommages subis par l'assuré)

Le contrat d'assurance Responsabilité Civile (= les dommages causés aux tiers)

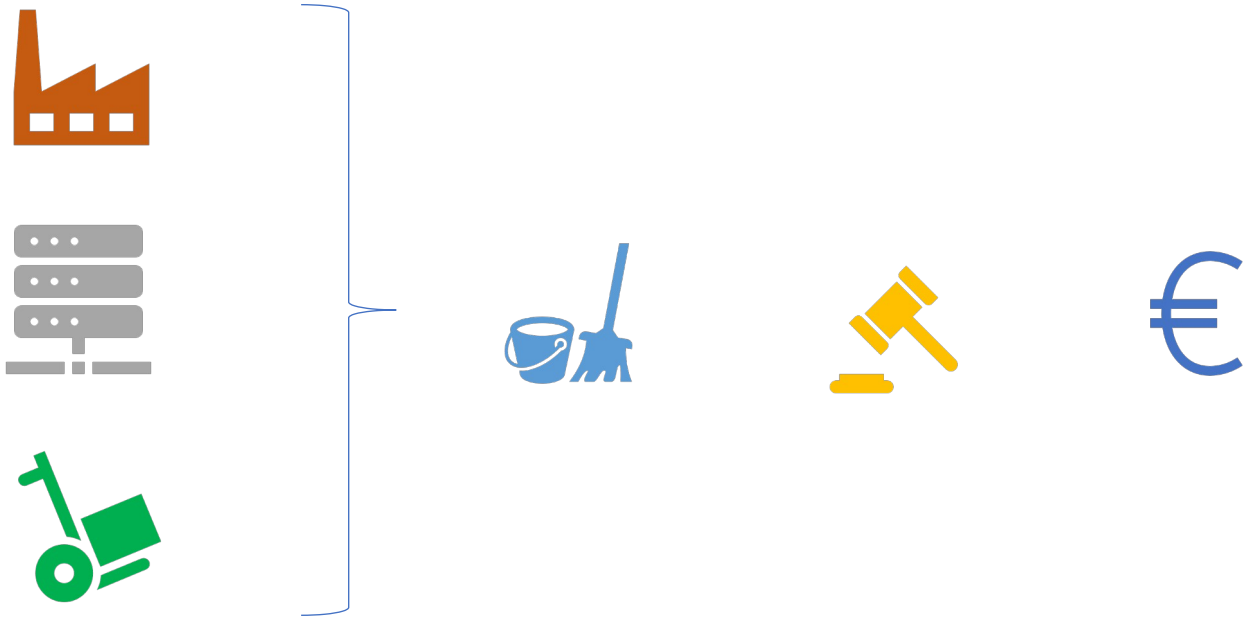
Le contrat d'assurance Cyber

Le contrat d'assurance Dommages aux Biens

(= les dommages subis par l'assuré)

Garantir les dommages matériels, subis par les biens assurés et résultant d'un événement garanti ainsi que :

- les frais et pertes consécutifs aux dits dommages matériels,
- Les responsabilités consécutives aux dits dommages matériels,
- les pertes d'exploitation consécutives aux dits dommages matériels.

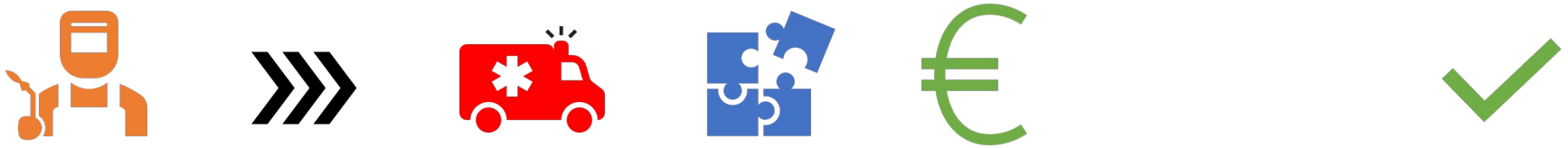


Focus Cyber

Le contrat d’assurance Responsabilité Civile

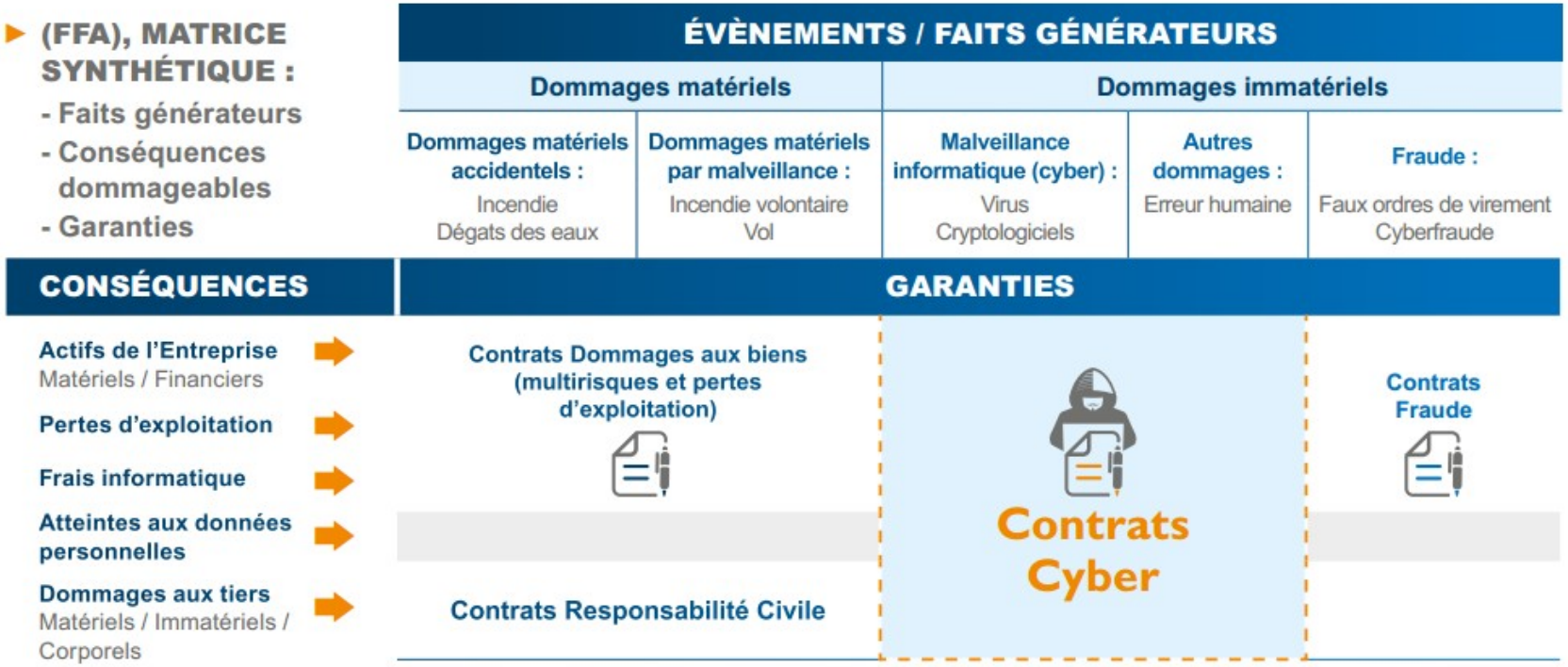
(= les dommages causés aux tiers)

Garantir les frais de défense et les conséquences pécuniaires (dommages-intérêts) de la responsabilité de l’assuré en raison des dommages corporels, matériels et immatériels (pécuniaires) causés aux tiers à l’occasion des activités assurées.



Le contrat d'assurance Cyber

Offrir des prestations d'assistance, garantir les frais et pertes (volet « Dommage ») et des conséquences pécuniaires en raison de dommages causés aux tiers (volet « Responsabilité Civile ») en cas d'atteinte aux données ou au système d'information.



Le rôle des parties

L'assureur — Le courtier — Le client

1 En amont : la souscription

2 En cours de contrat

3 Lors du sinistre

Le rôle des parties

1 En amont : la souscription

Identification et quantification des risques

Echanges, visite de risque et questionnaires

Contrat d’assurance adapté

Evolutions dans le temps

Le rôle des parties

2 En cours de contrat

Rencontres et échanges réguliers

Adaptation des contrats : investissements, nouvelles activités, etc.

Flux financiers : encaissement des primes, paiement des sinistres courants

Le rôle des parties

3 Lors du sinistre

Le client

L’assureur

Le courtier

Conclusion

- La toujours nécessaire référence aux textes des contrats
- L’évolution du marché de l’assurance sur la thématique « Cyber »
- L’assureur partenaire et le courtier garant de la relation tripartite

Audit et certification des centres de données

par Jean-François BEUZE

EDITION 2022

Audits et certifications

Le choix d'un Data Center est un acte stratégique qui exige une préparation minutieuse ou de contrôle des services proposés.

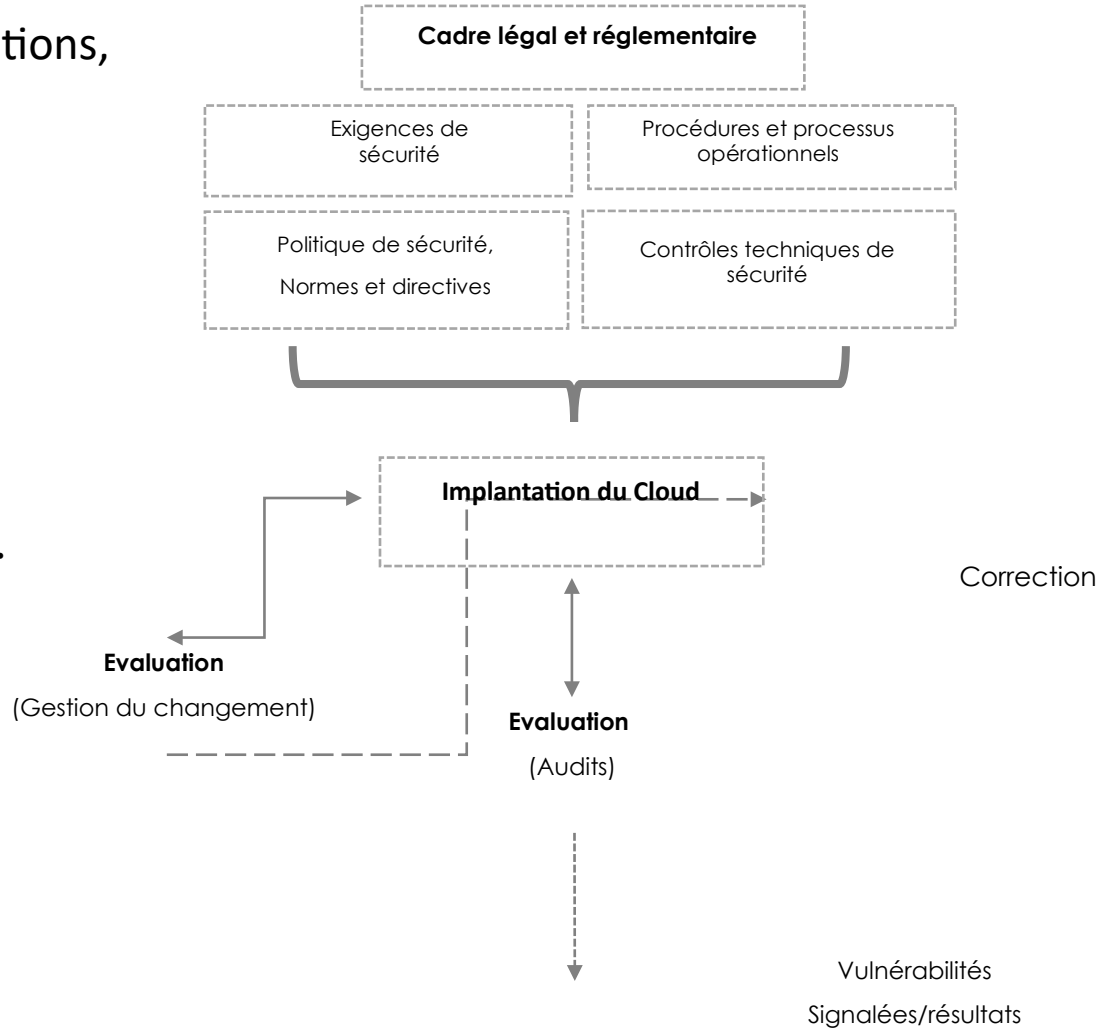
Le contractant, au-delà de l'identification de certification ou de lancement d'audit, se doit d'identifier au minimum le niveau de sécurité du service proposé.

Il s'agira notamment de s'assurer qu'aucune contrainte réglementaire n'interdit pas le recours à certains types de Data Center.

Audits et certifications

Avant même de parler d'un audit ou de vérifier les certifications, vous devez avoir le réflexe de définir en amont :

- les exigences réglementaires ;
- les exigences techniques de sécurité ;
- l'évaluation de la sécurité d'un service ;
- sa mise en œuvre et en mode exploitation ;
- la correction des vulnérabilités et les contrôles de sécurité.



Audits et certifications

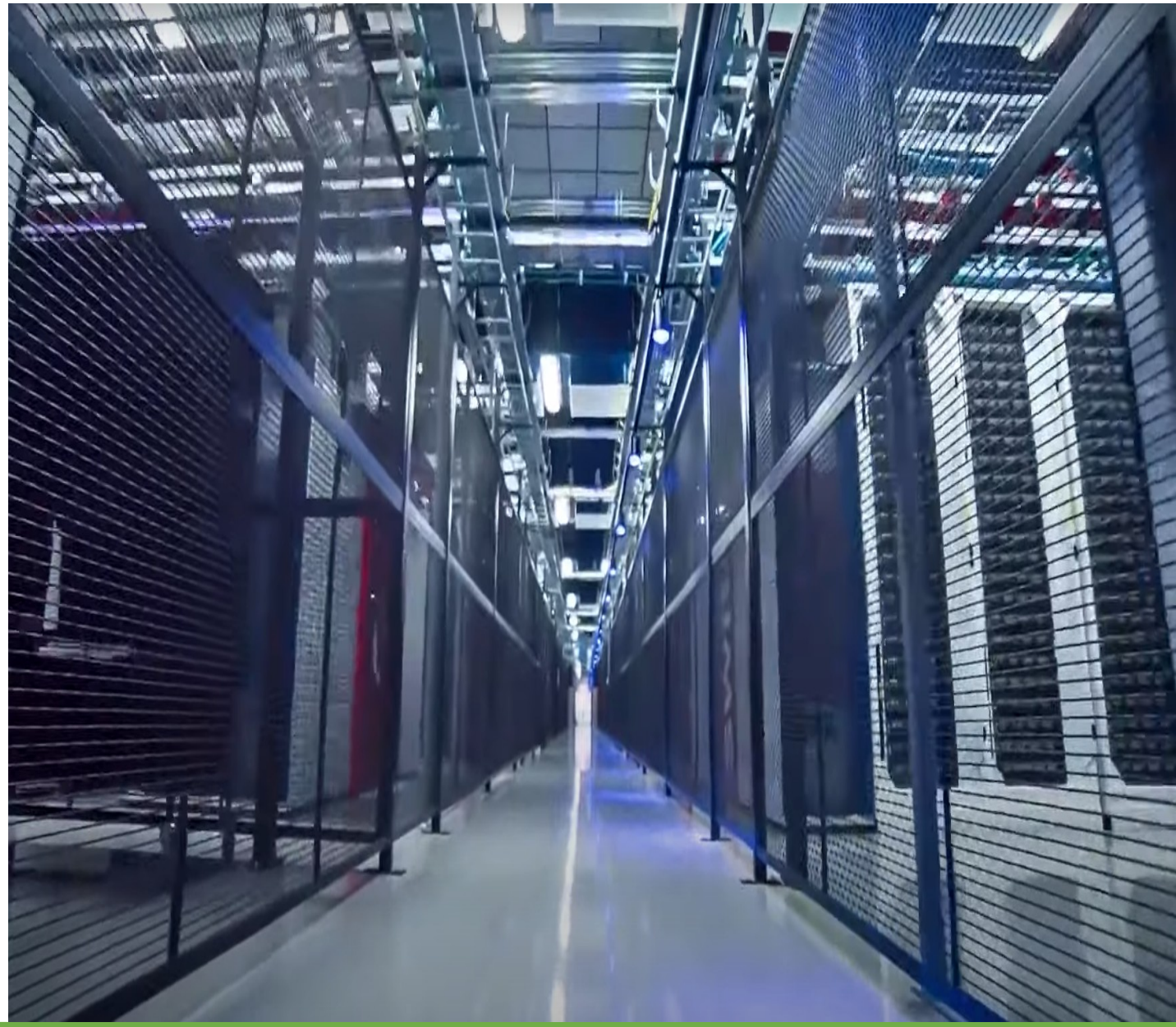
La démarche de qualifier les exigences de sécurité dans le cadre d'audits et/ou de certifications permet de garantir un haut niveau de qualité de service.

Il convient ainsi de prévoir, tout au long du contrat, la possibilité de ***vérifier l'effectivité des garanties*** en matière de protection des données (audits de sécurité, visite des installations, certifications à jour, etc.).

Audits

Les Data Centers sont tenus d'assurer un suivi permanent de leur niveau de maîtrise des risques et du respect des politiques et règles de sécurité applicables sur le périmètre de leur prestation, y compris auprès de leurs propres sous-traitants.

Les risques sont nombreux pour les contractants et de différents types (liés à la gestion, aux finances, à l'interopérabilité, à la conformité légale et réglementaire, à la sécurité, au maintien de la résilience, etc.).



Audits

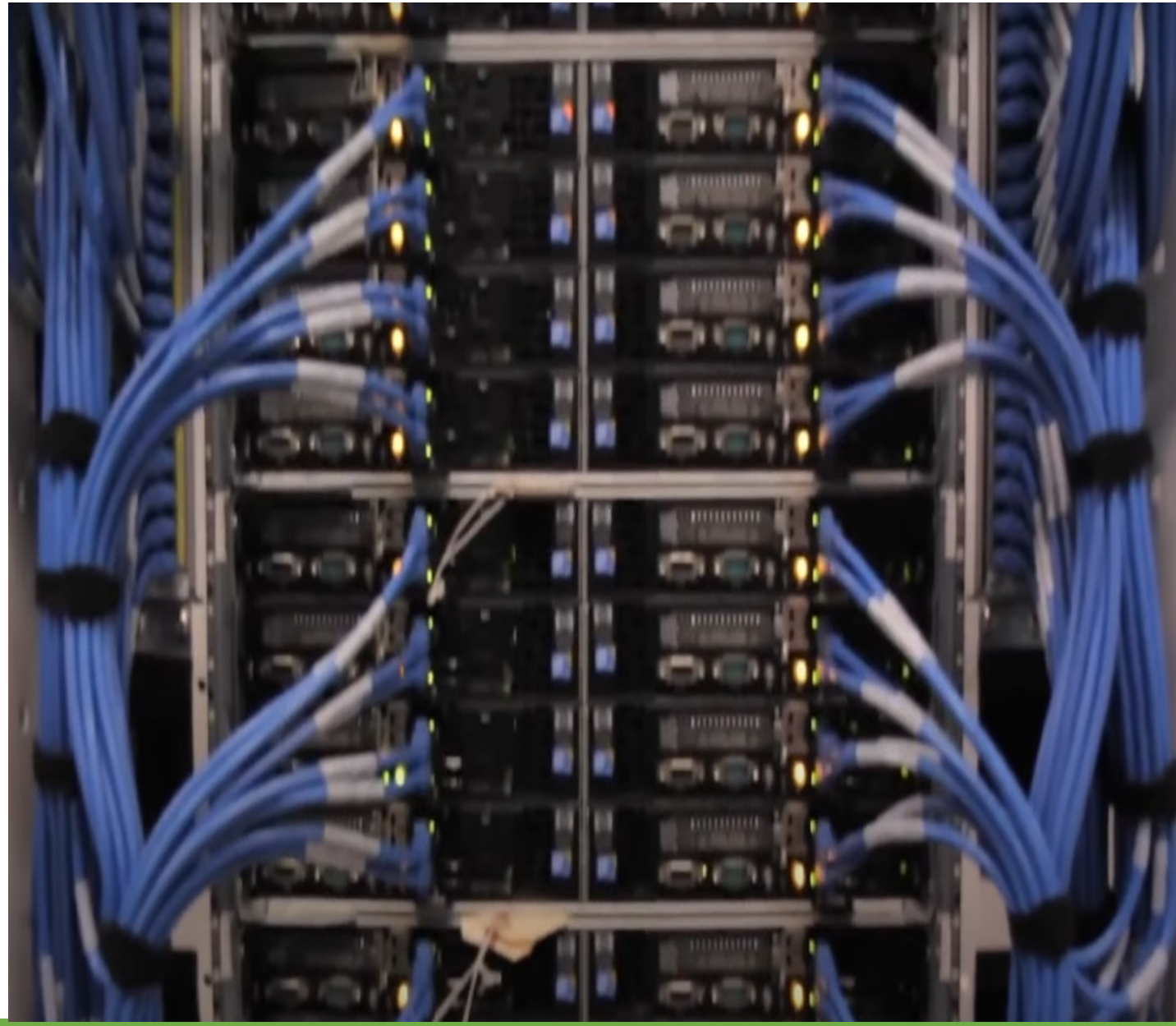
Les Data Centers doivent répondre aux différents enjeux liés à la Sûreté, la Cybersécurité, la résilience et la protection du patrimoine informationnel de ses clients.

- la certification ISO 27001 examine à la loupe tous les aspects des activités d'hébergement du Data Center.
    - Nous parlerons ici : des infrastructures physiques, l'organisation des sites et la gestion des accès, ainsi que les compétences des personnels.
    - Mais aussi : des modes de communication et d'exploitation ainsi que les systèmes de sauvegarde ou de reprise d'activité, en cas d'incidents.

Audits

Les évaluations de sécurité doivent porter sur l'engagement du Data Center :

- à respecter les exigences de sécurité ;
- à fournir toute pièce nécessaire à l'évaluation de la sécurité du service qu'il fournit ;
- à accepter un audit de sécurité diligenté par un tier ;
- à identifier ses sous-traitants assurant l'hébergement du service et des données ;



Certifications

Certifications :

- ISO/IEC 27001, 27017 et 27018 ;
- ISO/IEC 27701 pour la protection des données personnelles ;
- ANSSI SecNumCloud ;
- HDS (hébergement de données de santé) ;
- PCI DSS ;
- ISO 9001 : Management de la qualité ;
- ISO 14001 : Management de l'environnement ;
- ISO 50001 : Management de l'énergie.

Nous parlerons ici que de certifications et non de conformité à un règlement ou à un évaluateur (Ex RGPD ou EBA)

Certifications

Les Data Centers sont généralement classifiés selon 4 niveaux, en fonction de leur niveau d'équipements et de leur niveau de disponibilité.

La certification TIER est attribuée par l'institut Up Time.

Tiers 1 : dispose d'équipements non redondés et de réseaux d'approvisionnement uniques.

Tiers 2 : Les équipements critiques sont redondés afin de réduire les interruptions de service. Le taux de disponibilité monte ainsi à 99,75 % (environ 22 h d'arrêt cumulé par an).

Certifications

Tiers 3 : Tous les équipements du *Data Center* sont redondés pour éviter tout arrêt de fonctionnement durant les opérations de maintenance. Le taux de disponibilité est de 99,98 %.

Tiers 3+ : Par rapport au TIER 3, le *Data Center* dispose de réseaux d'alimentation électrique et de refroidissement doublés.

Tiers 4 : L'infrastructure est intégralement redondée. Ce niveau offre la garantie la plus forte, avec un taux de disponibilité de plus de 99,99 % (moins de 24 minutes d'arrêt cumulé annuel). RTE étant le seul distributeur national d'électricité à haute tension sur le territoire français.

Certifications

Il est nécessaire de vérifier les engagements suivants du Data Center :

- la détention de certifications de sécurité en cours de validité ;

- Le respect des exigences renforcées de localisation géographique du service et la sous-traitance ;

Les contractants devront privilégier alors qu'ils bénéficient de certifications ou de qualifications reconnues, en cours de validité de type ISO.

La confiance n'exclut pas le contrôle

Centres de données du futur

par Fabrice COUPRIE

EDITION 2022

France Datacenter & Advanced MédioMatrix

- Fédérateur des acteurs du datacenter en France.
- Advanced MédioMatrix certifié Tier III Facility.
- L'éco-responsabilité, la souveraineté, la sécurité et la performance.

Comment les datacenters feront-ils face aux transformations de demain ?

Une infrastructure essentielle

- Lieu de stockage et de traitement de toutes les données numériques.
- Maintien des services numériques.
- Bon fonctionnement informatique.
- Garantie la sécurité des données.

Données multipliées par 3 d’ici 2025

ECO-RESPONSABILITES

ADVANCED MEDIOMATRIX

LE **MADE IN FRANCE** ET **MADE IN EUROPE** PRIVILÉGIÉS

RECYCLAGE DE LA CHALEUR DÉGAGÉE PAR LES SERVEURS

#GREEN IT

LA PRODUCTION PHOTOVOLTAÏQUE GRÂCE À L'INSTALLATION DE **PANNEAUX SOLAIRES**

RÉCUPÉRATION DES EAUX DE PLUIE

UN PUE INFÉRIEUR À **1,3**

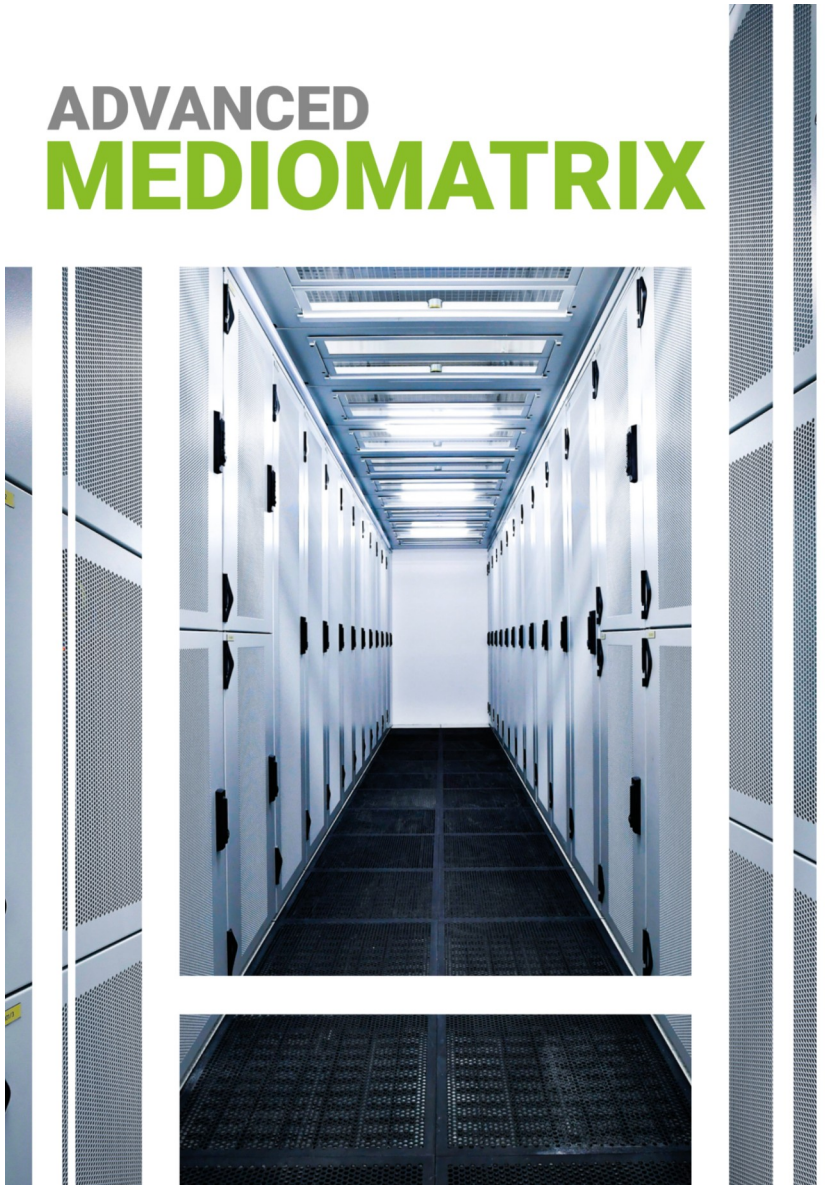
CERTIFIÉ **ISO 14001** Management environnemental

UNE CONSOMMATION D'ÉNERGIE **100% VERTE**

LE DATACENTER EST REFROIDI À **90%** DU TEMPS EN FREECOOLING DIRECT

Souveraineté numérique

- Contexte géopolitique et croissance exponentielle des données numériques.
- Importance de la gouvernance des systèmes d'information.
- Régir la sécurité des données par les lois françaises et européennes.
- Volonté d'une généralisation du statut d'infrastructure critique.
- France Datacenter promeut l'hébergement de données en France.



Conclusion

Les enjeux de demain :

- Assurer un développement numérique durable et éco-responsable.
- Réduire son empreinte carbone.
- Offrir une sérénité aux acteurs et utilisateurs du numérique.
- Garantir une conformité de stockage des données
- Mutualisation des salles informatiques : efficiente & économique.
- Répondre aux besoins futurs.

FRC
Forum Cybermenace

FRC
Forum Cybermenace

EDITION 2022

Conférence de clôture

par le général d'armée (2s) Marc WATIN-AUGOUARD

EDITION 2022

Conclusion du 15ème FRC

par le général Jude VINOT
Commandant le Groupement de Gendarmerie Départementale du Bas-Rhin

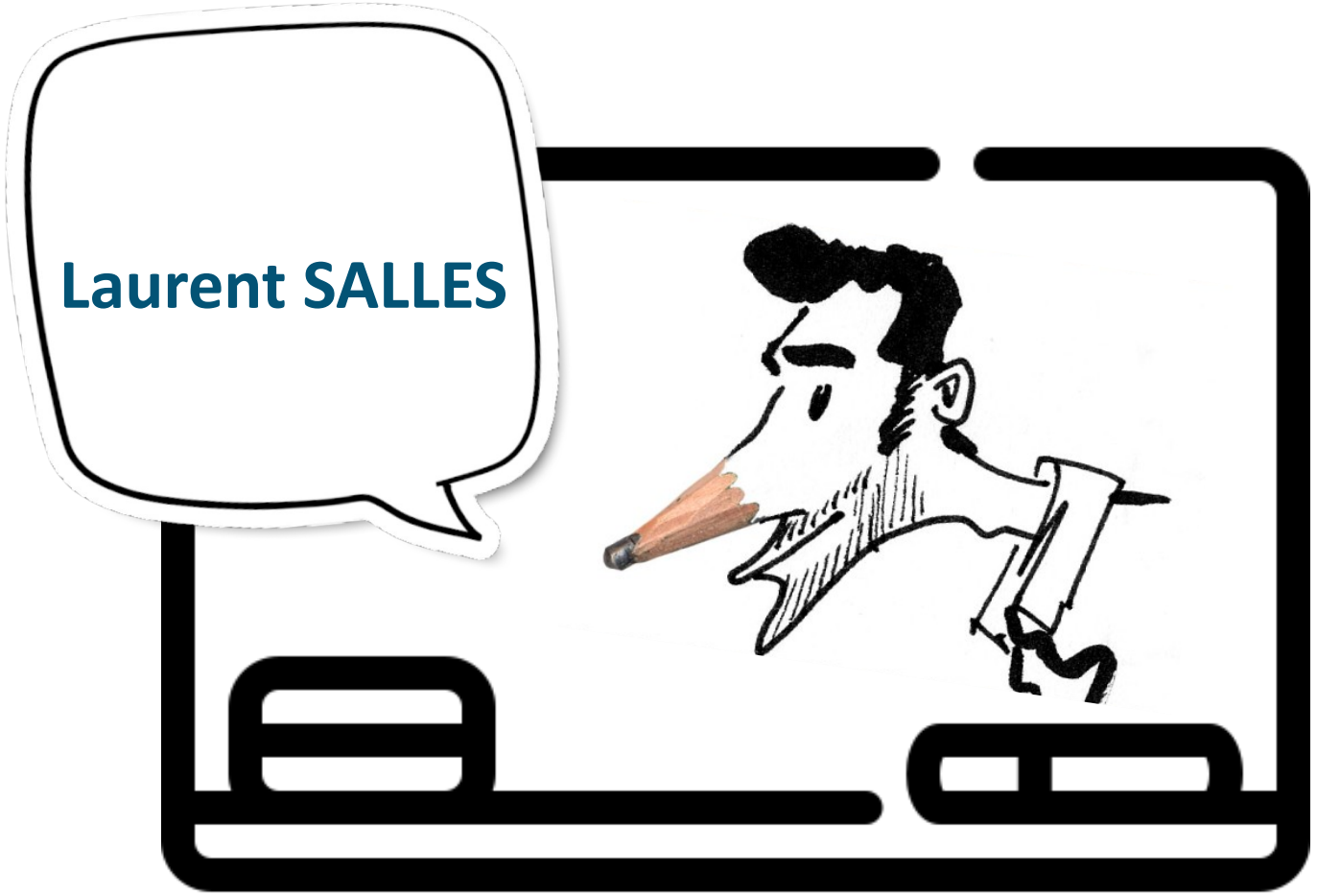
par Gilbert GOZLAN
Président de l'association Ad honores – Réseau Alsace

FRC 2022 - Remerciements

L'équipe d'organisation

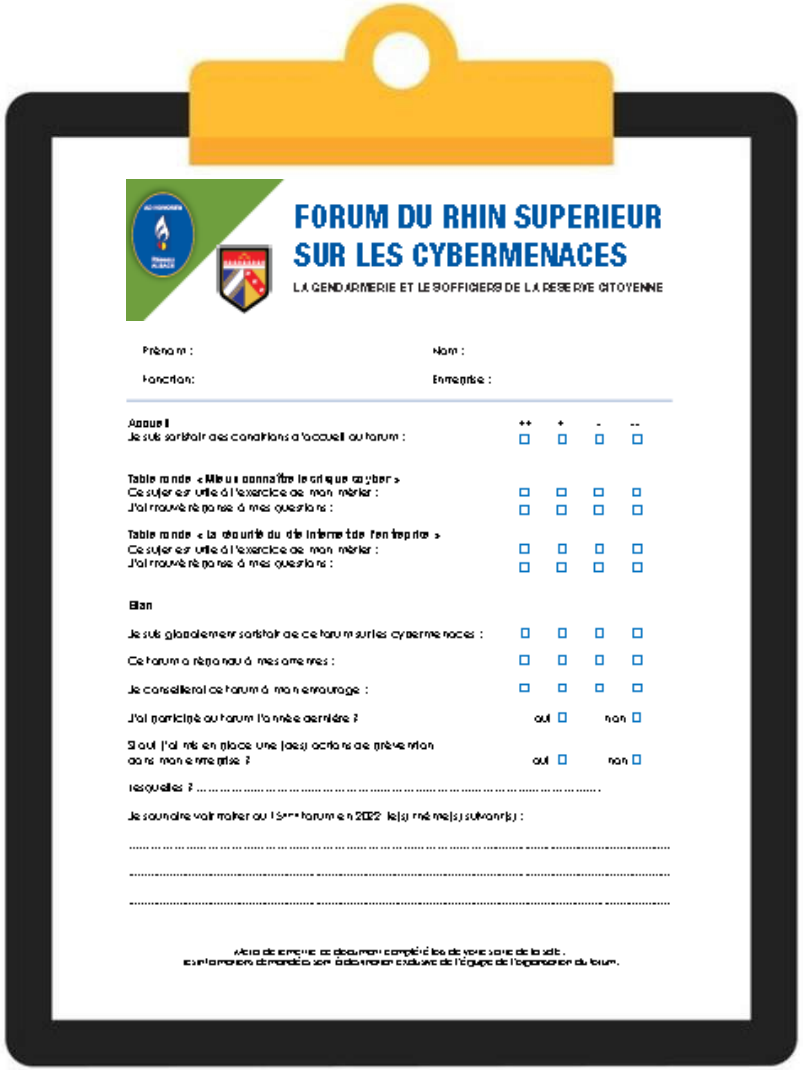
Christophe CHARLY
Sébastien DUPENT
Daniel GUINIER
Emmanuelle HAASER
Ludovic HAYE
Hervé HUMBERT
Isabelle HUCK
Sophie MARTIN
Didier SCHERRER
Jonathan WEBER
Lcl Jean-Marc PETON
Adj Eléna VALLEJO
Mdl Vanessa URBAN
Adj (RO) Pierre MEYER

FRC 2022 - Remerciements



FRC 2022 - Remerciements

FRC 2022 : Fiche d'évaluation



FORUM DU RHIN SUPERIEUR SUR LES CYBERMENACES

LA GENDARMERIE ET LE SOFFICIERS DE LA RESERVE CITOYENNE

Prénom : Nom :

Fonction: Entreprise :

	++	+	-	--
Accueil				
Je suis satisfait des conditions d'accueil au forum :	☐	☐	☐	☐
Table ronde « Mieux connaître la stratégie cyber »				
Ce sujet est utile à l'exercice de mon métier :	☐	☐	☐	☐
J'ai trouvé réponse à mes questions :	☐	☐	☐	☐
Table ronde « La sécurité du développement 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 souhaiterais voir traiter au 3ème forum en 2022 le(s) thème(s) suivant(s) :

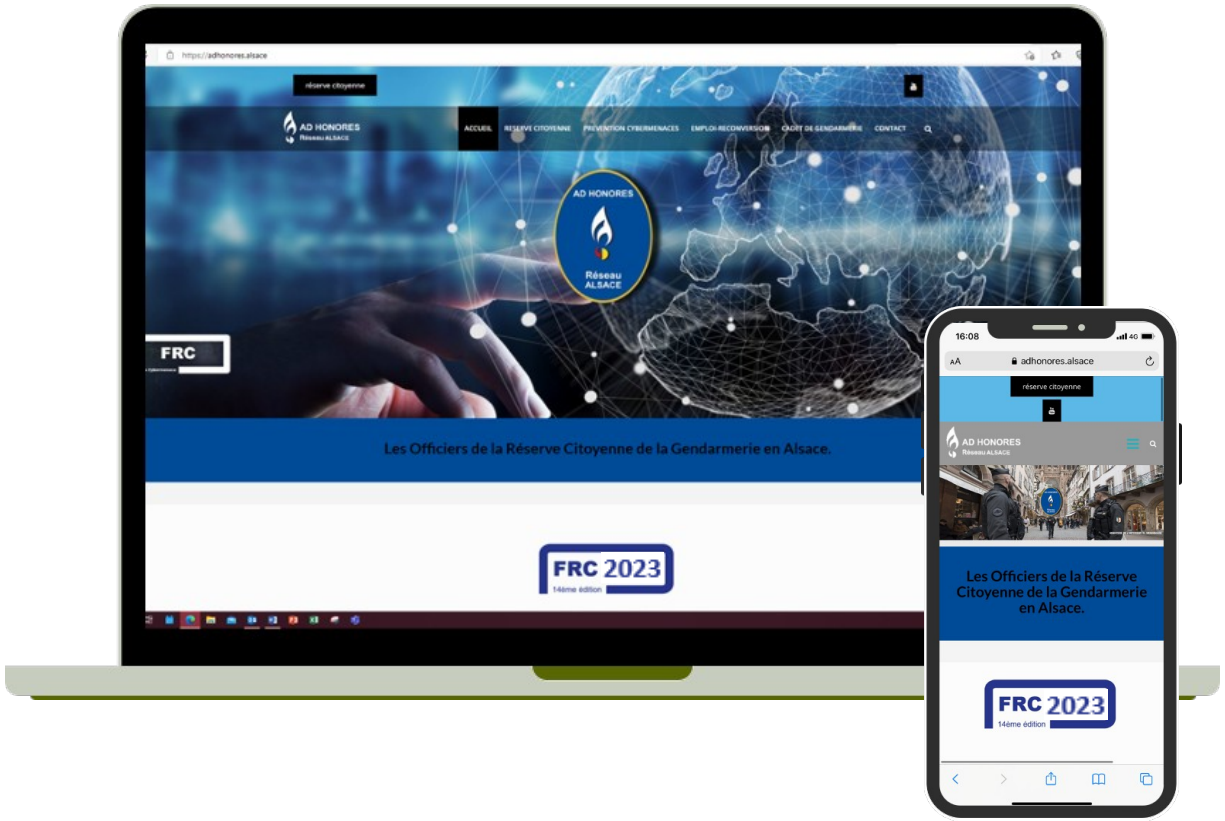
.....

.....

.....

Merci de remettre ce document complété lors de votre sortie de la salle.
Il sera ensuite demandé son dépôt exclusif de l'équipe de l'organisation du forum.

16 ème FRC - 7 novembre 2023



https://adhonores.alsace/


FIC
Forum International
de la Cybersécurité
5, 6 et 7 avril
Lille Grand Palais
europe.forum-fic.com

La Gendarmerie Nationale recrute :

12 000 personnes dans 300 métiers

Informations et renseignements :

Centre d'informations et de recrutement de Strasbourg

www.lagendarmerierecrute.fr

Gendarmerie nationale UNE MÊME FLAMME NOUS ANIME.