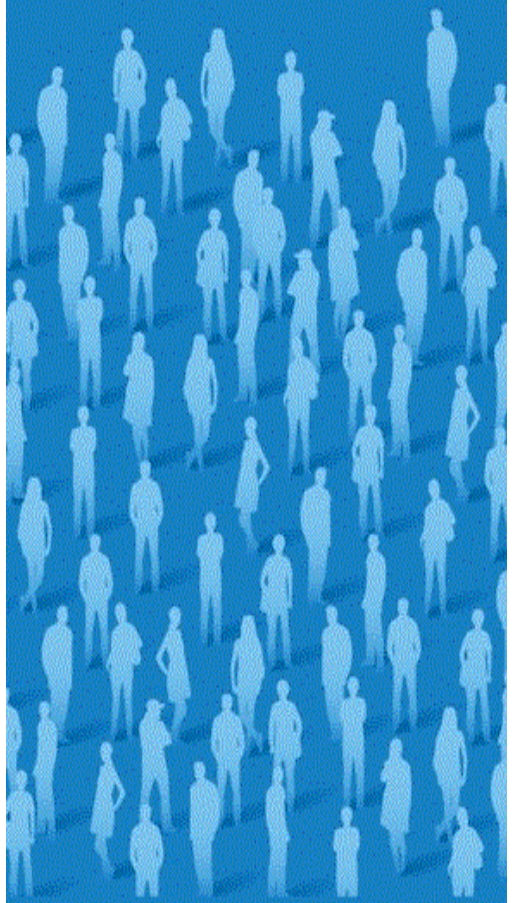
ACHAT PUBLIC ET CYBERSECURITE

du choc culturel au changement de paradigme indispensable

Sébastien TAUPIAC
Administrateur de l'APASP
Directeur de la Communication
et des Relations Publiques
e-Attestations

Pierre-Ange ZALCBERG
Avocat
chez Nemrod Avocat,
Ancien directeur juridique
adjoint de l'EFS
Nemrod
Avocat

APASP
Association Pour l'Achat dans les Services Publics
www.apasp.com



27 juin 2024

Les intervenants

Sébastien TAUPIAC
Administrateur de l'APASP
Directeur de la Communication
et des Relations Publiques

e-Attestations

Pierre-Ange ZALCBERG
Avocat
chez Nemrod Avocat,
Ancien directeur juridique
adjoint de l'EFS

Nemrod
Avocat

SOMMAIRE

Cybersécurité

1. LA SITUATION
2. LE CHOC CULTUREL
3. LES FONDAMENTAUX
4. L'EXPOSITION SPECIFIQUE DU SECTEUR PUBLIC
5. LA MOBILISATION EUROPEENNE ET NATIONALE
6. LA GESTION DU RISQUE
7. LES CONSEILS CLES POUR L'ACHETEUR PUBLIC

LA SITUATION

e-Attestations

Cyberattaques et secteur public : "la question n'est pas de savoir si cela va arriver, mais quand"

Un risque CERTAIN et non PROBABLE

2023 : toute la sphère publique

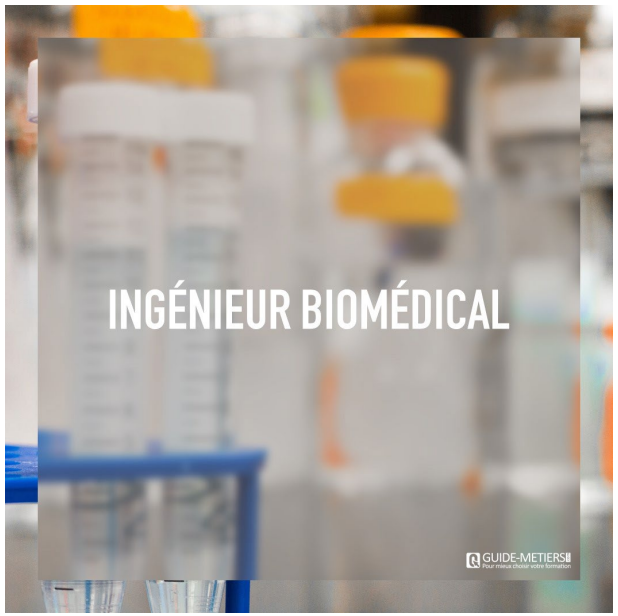
https://www.numerama.com/cyberguerre/1535532-cyberattaque-la-carte-des-villes-departements-et-hopitaux-victimes-des-hackers-en-2023.html

LE CHOC CULTUREL

Le choc des cultures – un nouveau risque

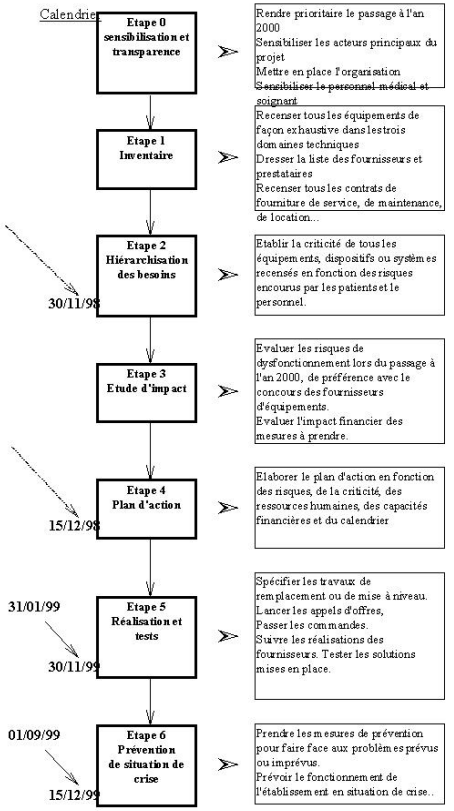
La culture de l'hygiène
La maîtrise du risque
La création des CLIN
LE RISQUE INFECTIEUX

1988…



L'ingénierie biomédicale
Le marquage CE
La matériovigilance
LE DYSFONCTIONNEMENT

1993…



LE BUG DE L'AN

2000…

Le choc des cultures – un risque pas si nouveau

NOVEMBRE

	L	M	M	J	V	S	D
							01
45	02	03	04	05	06	07	08*
46	09	10	11	12	13	14	15
47	16	17	18	19	20	21	22
48	23	24	25	26	27	28	29
49	30	31					

*Vendée Globe : départ le 8 novembre des Sables d'Olonne

2013 Révélations d'Edward Snowden

Une clé USB, un article du Guardian : ainsi s'est construite la légende du lanceur d'alerte. ***Ses révélations sur les services de renseignements américains renforceront la paranoïa et déclencheront une prise de conscience collective à l'échelle mondiale.***

L’effet de surprise et l’amplification

Un contexte réglementaire et juridique trop récent

Risque pénal faible pour les hackers mais fort pour les établissements publics

Pression limitée sur les acteurs jusqu’en 2020 (Obligations OSE, OIV, Directive NIS2)

Une absence de budget public

Des priorisations financières / crise

Le coût de l’internalisation et de l’externalisation

Un intérêt économique important pour les hackers

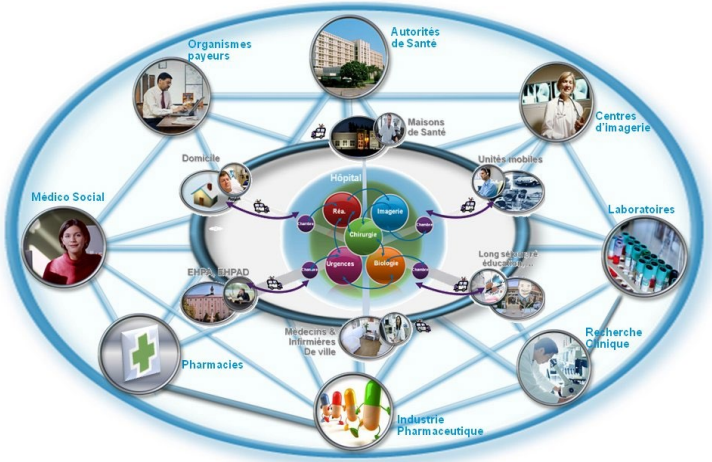
CLIN (oui)

CLINum (non)

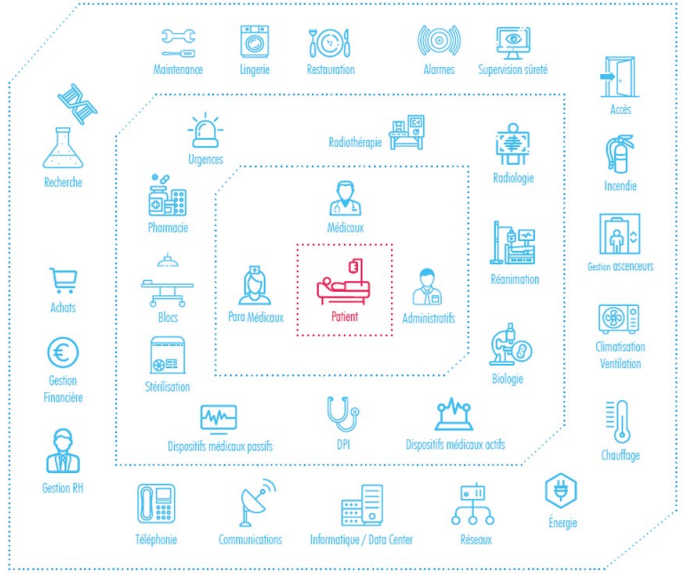
Un positionnement délicat de l’informatique et du numérique

Gouvernance

Millefeuille territorial et GHT



Santé connectée sur un territoire de Santé



Equipements connectés (point de fragilité), parcours digital, IA, SI

Digitalisation des services accélérée par la crise sanitaire

Une forte motivation des hackers

1- L'aspirant Hacker

Ce sont généralement des adolescents utilisant des techniques de piratage récupérées sur le web, par simple curiosité intellectuelle, par distraction, sans forcément prendre la mesure de leurs actes.
Ce profil d'apprenti pirate peut parfois déclencher des cyberattaques à leur insu, par simple téléchargement et exécution de scriptes, récupérés sur internet.

2- Le cracker

Il se différencie des autres hackers par ses motivations qui ne sont pas financières. Il est expérimenté et prend plaisir à pirater des systèmes d'information, uniquement pour en montrer les failles.

3- Le hacker éthique

Il met son expertise au profit de la communauté, en découvrant les failles de sécurité, auxquelles il essaye d'apporter des solutions techniques. Il n'est pas motivé par l'appât du gain.

4- Les mercenaires

Extrémiste, avec des compétences techniques très variées, il se considère comme le pirate des temps modernes. Il monnaie ses compétences et travaille généralement pour des organisations mafieuses.

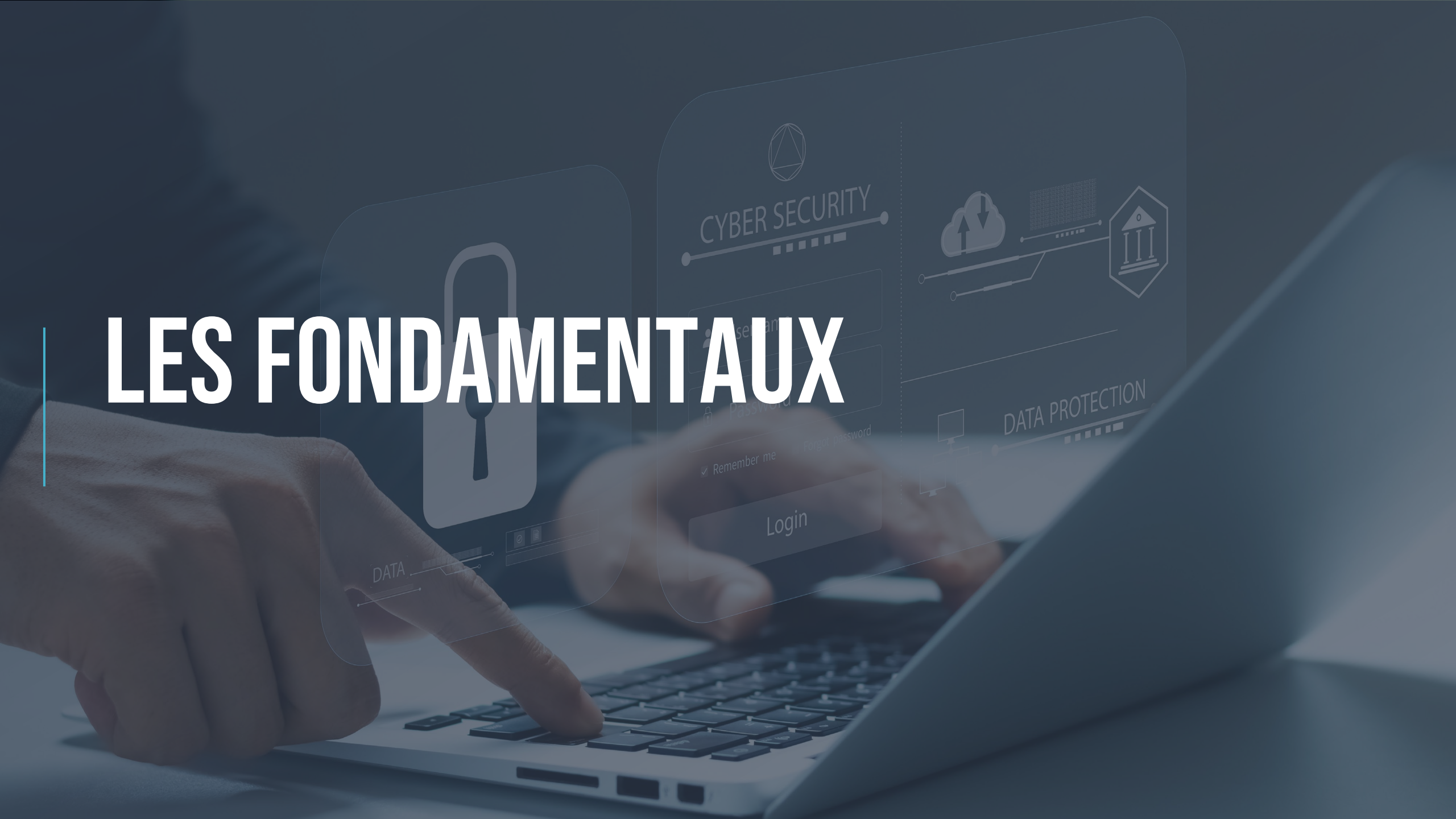
5- Le cyber espion

Expert dans l'espionnage industriel, il met son expertise et ses connaissances afin d'infiltrer les entreprises et d'en voler les données (savoir-faire industriels… brevets …). Il est expert dans l'ingénierie sociale et sait exfiltrer les données sans se faire remarquer à des fins mercantiles.

6- Les agents gouvernementaux / hacker militaires

Ce sont des hackers recrutés par des organisations gouvernementales (ANSSI, services secrets..) et services de l'armée. Ils viennent en appui sur différentes missions afin d'aider à comprendre les attaques, à les éviter. Ils sont experts dans l'analyse forensic, visant notamment à collecter les preuves d'une attaque mais travaillent également sur les cyberarmes et cyber défenses des gouvernements qui les emploient.

LES FONDAMENTAUX



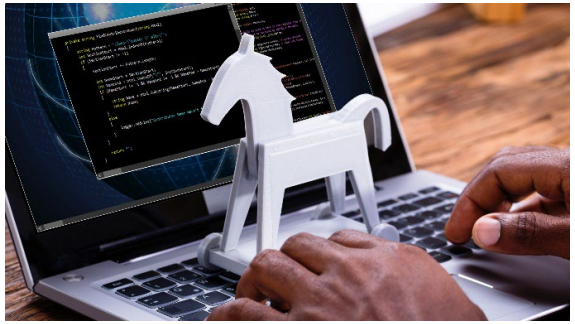
La thématique

Les attaques les plus connues du grand public sont les attaques virales. Elles ne représentent en réalité que **5 à 10 % des attaques qui sont aujourd'hui identifiées.**

Les attaques par virus sont pratiquement gérées à 100% par les Antivirus du marché **dont la quasi-totalité des professionnels de santé sont déjà équipés.**

La thématique

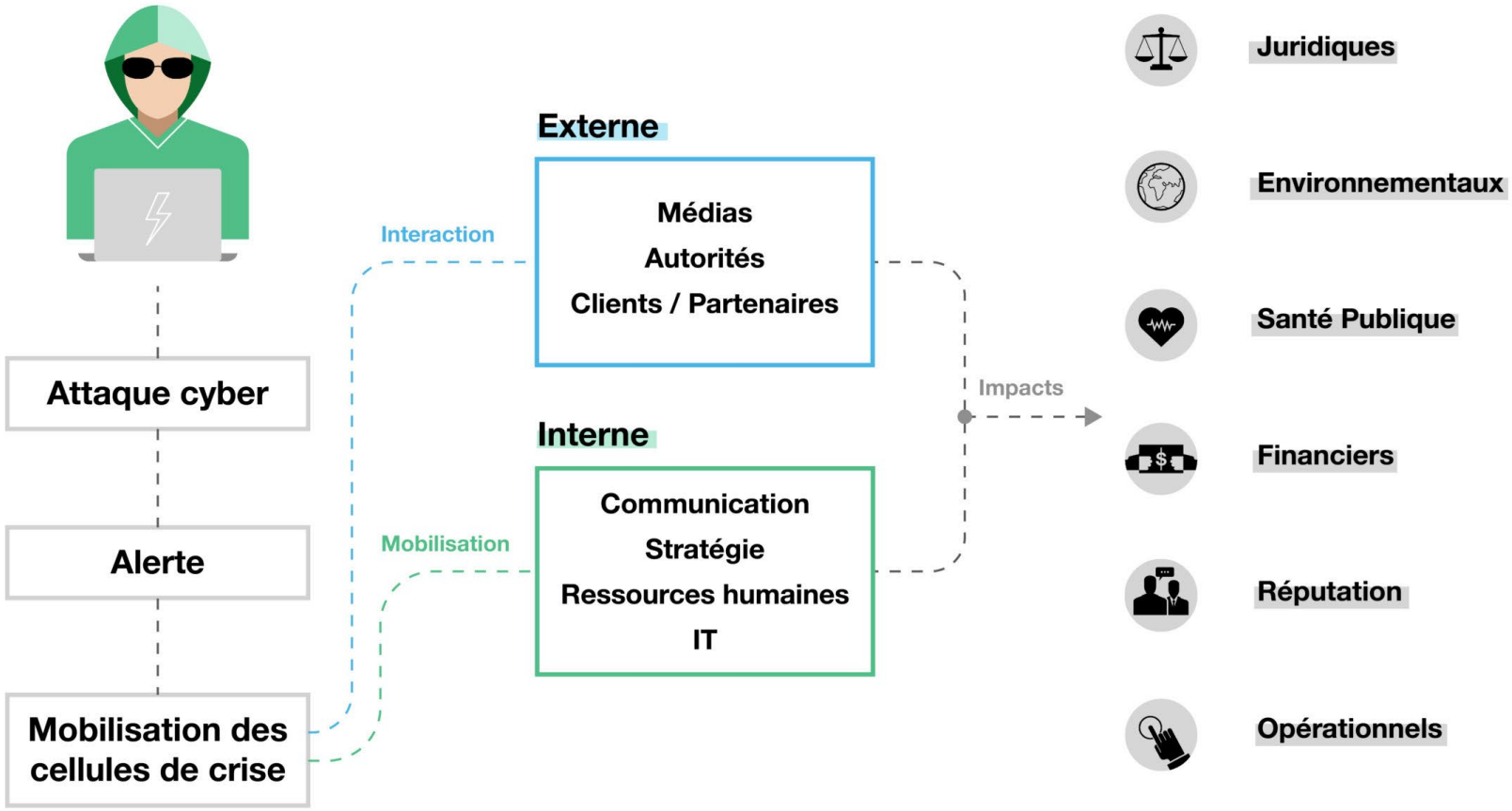
Les menaces et attaques constatées auprès des acteurs publics et des établissements associés sont aujourd'hui d'un autre ordre :



- malwares,
- phishing,
- crypto-locker,
- ransomwares,
- arnaques par spam,
- fraudes techniques,
- usurpations d'identité numérique
- … et malveillances.

Aucune solution antivirale du marché ne permet de les contrer

Le scénario type de gestion d'une cyberattaque



Exemple simplifié d'un scénario d'exercice de gestion de crise
Source : Orange Cyberdefense

Les enjeux

Réglementaire/juridique

- Responsabilité civile et pénale de l'établissement public
- Intégration de la cybersécurité au sein des processus (ex : achat, juridique, …)

Economique (coûts directs et indirects)

- Coûts assurantiels, rançons, …
- Audits, conseils, réorganisation, sensibilisation, formation, …
- Pertes d'activité (ex : secteur de la santé)
- Indemnisation des pertes/vol de données

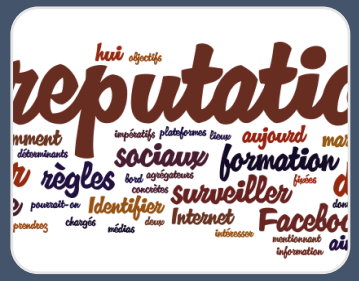
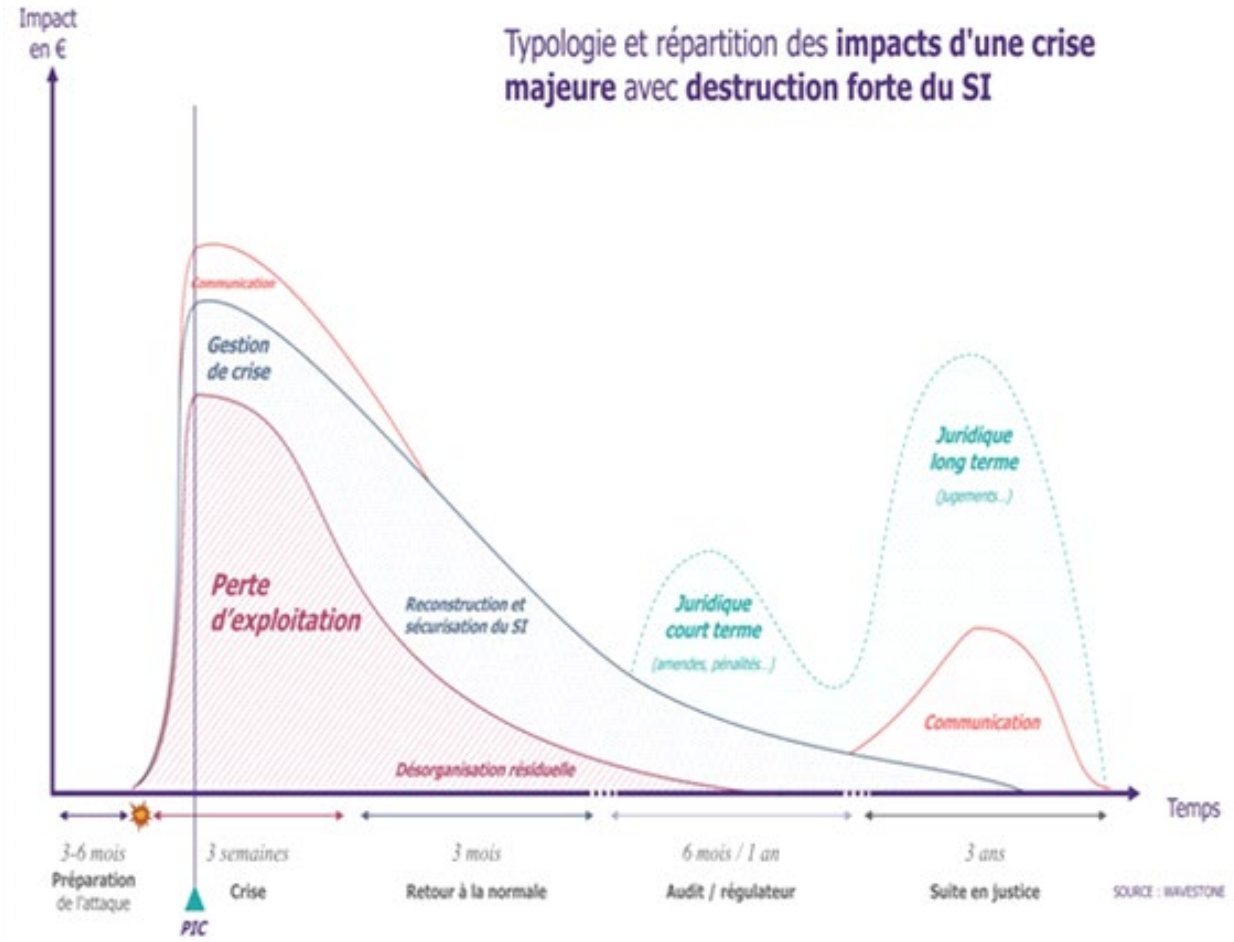


Image et réputation

- Dégradation voir arrêt des missions de service public
- Positionnement au regard des instances et acteurs institutionnels
- Perte d'attractivité vis-à-vis des usagers
- Perte d'attractivité vis-à-vis des personnels

Les coûts directs et indirects



Des exemples concrets de coûts
Secteur de la santé

Médecin libéral
20 000 €

Ehpad
30 000 €

Clinique Hôpital
160 000 €

CHR CHU
300 000 €

Par jour en coût global

61 % - Le ransomware, ou logiciel d'extorsion, est un logiciel malveillant qui prend en otage des données personnelles.

38 % - Le déni de service est une attaque qui vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs.

23% La défiguration de site web modifie l'apparence d'un site Internet. Le site n'est souvent plus utilisable, au moins partiellement, ce qui peut entraîner des pertes directes de productivité et l'extorsion de données sensibles,

18% Le vol de données personnelles est une activité prisée des pirates, celle ci peut provoquer la perte de plusieurs centaines de milliers d'euros pour un Etablissement de Santé

L'EXPOSITION SPECIFIQUE DU SECTEUR PUBLIC

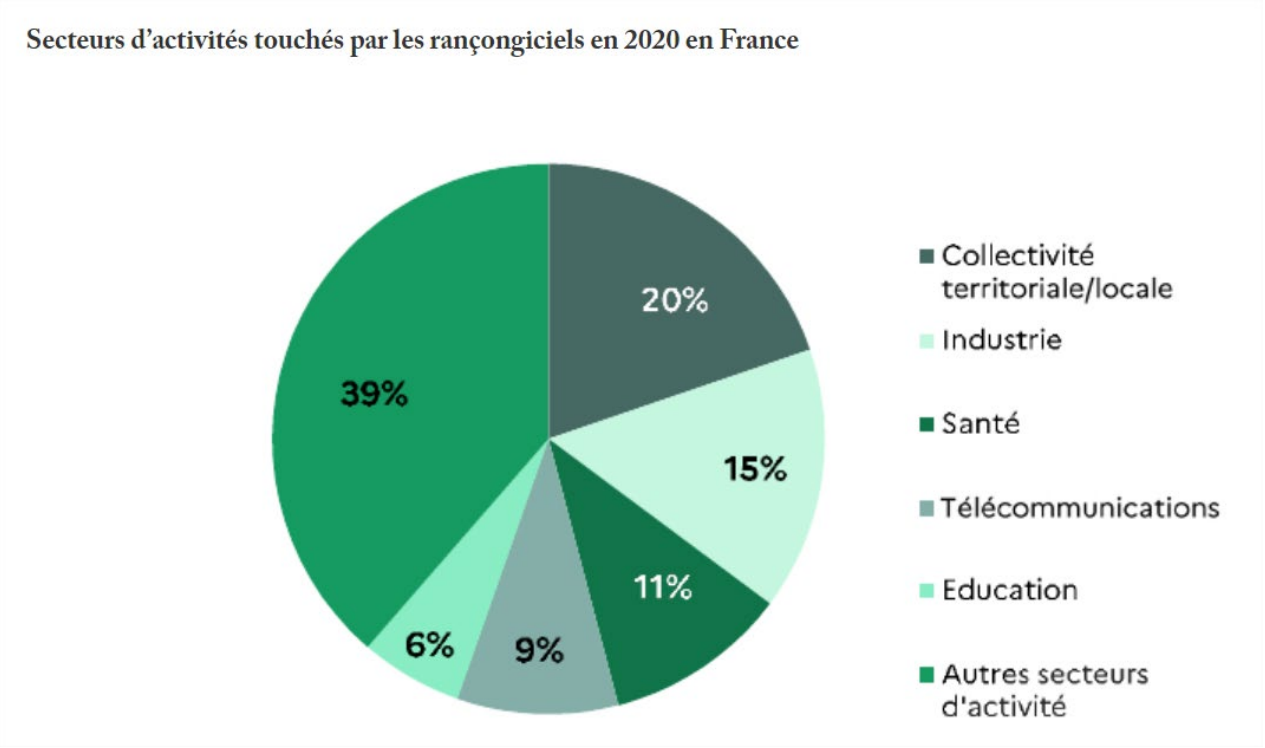
Les enjeux spécifiques à la France

Pays industrialisé
Puissance militaire mondiale et arme nucléaire
Diplomatie internationale / données sensibles
Digitalisation accélérée
Développement des réseaux hauts-débits

Industrie de pointe (Airbus, Dassault …)
Secteur de la santé (recherche clinique, …)
Référence mondiale en sciences et en mathématiques

<u>Ne pas oublier les risques internes en France</u>

- Espionnage industrielle
- Mouvements de contestation sociaux
- Enjeux de politique interne



Source : ANSSI (2020)
https://www.ssi.gouv.fr/actualite/cybersecurite-faire-face-a-la-menace-la-strategie-francaise/

L’exposition particulière du secteur public

Eclatement administratif public (GHT, communautés de communes, Métropoles, …) -> obligations digitales et fragilité des réseaux

Manque de coordination publique
Enjeux d’indépendance des collectivités
Formation et sensibilisation des agents
Regard ancien sur les compétences et l’exposition du secteur public

Secteur de la santé

- Recherche clinique et valeur associée
- Valeur d’un dossier patient
- Impact du déni de services et rançons
- Service public essentiel / vital
- Environnement clinique pensé en termes de sécurité médicale et non en termes de sécurité informatique

1. La suppression des outils informatiques et surtout des outils métiers
2. La durée de la crise (de quelques jours à plusieurs mois)
3. Les enjeux vitaux liés au patient (3 jours)
4. Des secteurs déjà fragilisés pas la crise (ex : pharmacie)
5. Un contexte en ressources humaines spécifique
6. Un haut niveau de connexion et d’interconnexion (nombreuses interfaces internes et externes)

LA MOBILISATION EUROPEENNE ET NATIONALE

Les opérateurs d’importance vitale (OIV)

Opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation

Mise en place de mesures de protection contre des actes malveillants portant atteinte à leur bon fonctionnement.

Accompagnement spécifique par l’ANSSI

<u>Les secteurs désignés (12)</u>

Alimentation

Gestion de l'eau

Santé (Une part importante des CHU)

Activités civiles de l’Etat

Activités judiciaires

Activités militaires de l’Etat

Énergie , Finances , Transports

Communications électroniques

Audiovisuel et information

Industrie , Espace et recherche

Un opérateur d'importance vitale (OIV) est, en France, une organisation identifiée par l'État comme ayant des activités indispensables à la survie de la nation ou dangereuses pour la population.

En 2016, il y en avait 249 dans 12 secteurs d'activité et 4 dominantes.

Pour des raisons de sécurité nationale, la liste des OIV n'est pas publique et il est demandé aux entreprises désignées de ne pas communiquer sur leur implication au dispositif.

Le dispositif est décrit par décret en 2006 avant d'être codifié au Code de la Défense en 2007.

Les opérateurs de service essentiel(OSE)

Opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services.

OSE désigné par arrêté du Premier ministre
Désignation et déclaration de(s) système(s) d'information Essentiel(s) (SIE) à l'ANSSI
Concerne les SIE internes ou externalisés

Les secteurs désignés
Energie / Transport / Logistique
Banque / Infrastructures de marchés financiers / Services financiers / Assurances
Social / Emploi et formation professionnelle
Santé (tous les établissements supports au GHT)
Fournitures et distribution d'eau potable
Traitement des eaux non potables
Infrastructures numériques
Éducation, Restauration

Détail des services dans le Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

DIRECTIVE NIS 2

En janvier 2023, les États membres de l'UE ont officiellement promulgué une révision de la directive 2016 sur les réseaux et les systèmes d'information (NIS). Conçue pour répondre à plusieurs cyberattaques largement médiatisées et dommageables, la Directive NIS2 renforce les exigences de sécurité, rationalise les obligations de signalement et introduit des mesures de surveillance et des exigences de mise en œuvre plus strictes.

La Directive NIS 2 élargit ses objectifs et son périmètre d'applicabilité **pour apporter davantage de protection.**
Deuxième semestre 2024 au plus tard pour la France.

A l'échelle nationale, NIS 2 s'appliquera à des milliers d'entités appartenant à plus de dix-huit secteurs qui seront désormais régulés. Environ 600 types d'entités différentes seront concernés, parmi eux des administrations de toutes tailles et des entreprises allant des PME aux groupes du CAC40.

La directive NIS 2 n'oblige pas les OSE à avoir recours à des solutions de sécurité labélisées par l'Anssi, comme c'est le cas pour les opérateurs d'importance vitale et leurs systèmes d'information vitaux (SIV). De ce point de vue, la tâche sera donc plus simple pour les OSE, qui pourront continuer à exploiter leurs solutions existantes pour leurs systèmes d'information essentiels (SIE).

Elles devront cependant le faire en respectant 23 règles précises. Et c'est là qu'il devient nécessaire de se pencher sur le texte, afin de s'assurer du bon déploiement de ces solutions on-premise, de leur bonne utilisation, et administration en toute conformité.

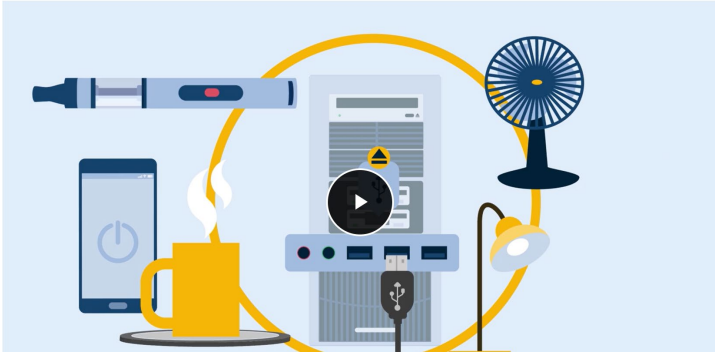
LA GESTION DU RISQUE

La culture de la gestion des risques

Appréhender la cybersécurité comme tous les autres risques
Le risque est identifié, pérenne et à forts impacts.

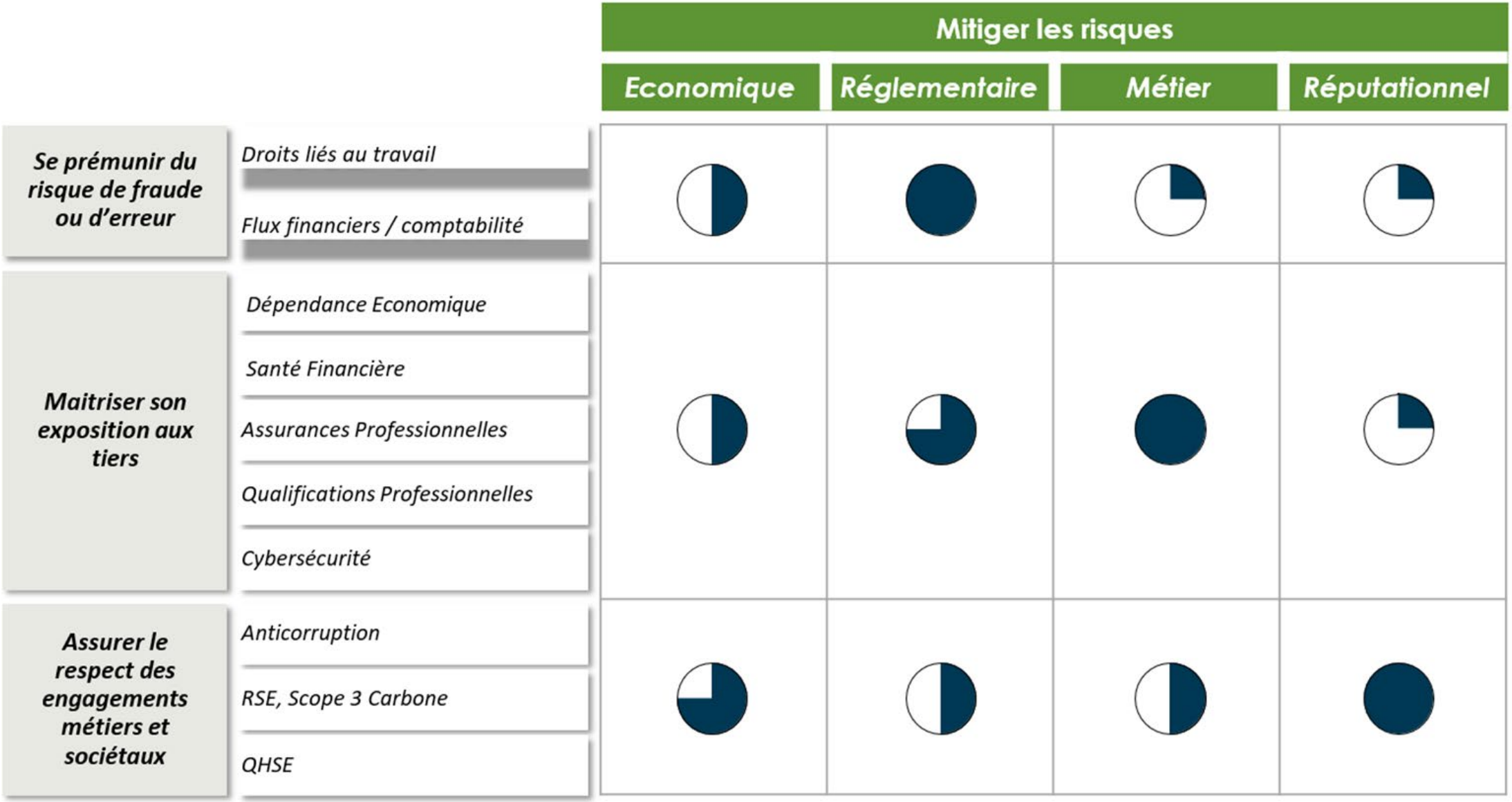
- Déploiement réglementaire et juridique
- Accompagnement économique (ressources, moyens, compétences, formation)
- Enjeu culturel (éducation, sensibilisation, prévention)

Les risques « historiques »
Alcool, drogue (campagnes de prévention)
Virus (effet Covid19)
Insécurité routière (pression réglementaire)
Tremblements de terre (sensibilisation)
Cambriolages et vols (principe de précaution et moyens techniques)
Sécurité incendie (formation obligatoire)



-> Prévention voire prédiction (avantages du digital)

L’identification des risques



La cartographie des risques

	Mineur	Modéré	Sérieux	Majeur
Très probable	Erreur au sein du DCE Rupture d'approvisionnement (fournitures de bureau)	Rupture d'approvisionnement (informatique)	Rupture de service (éditeur SI, gardiennage, bionettoyage)	Cyberattaque **Rupture d'approvisionnement (médicaments)** Travail illégal (travaux)
Probable	Erreur de publication Indisponibilité acheteur (1 semaine)	Indisponibilité acheteur (1 mois) **Non déclaration d'un sous-traitant** Non-respect des engagements contractuels	Atteinte à la probité Contrôle de l'AFA Démission de l'acheteur **Contrôle Urssaf** **Contrôle CRC**	Absence de réponse **Défaillance fournisseurs** Non-respect du RGPD Erreur de qualification (exemple : JEI, ESS) **Travail illégal (services)**
Peu probable	Règlement sur mauvais compte bancaire (500 €)	Règlement sur mauvais compte bancaire (5 k€)	Règlement sur mauvais compte bancaire (> 50 k€)	**Exclusion à tort de la commande publique d'un candidat** Travail illégal (véhicules)
Rare			**Référé précontractuel** Recours au fond	Attaque extra-terrestre

LES CONSEILS CLES POUR L'ACHETEUR PUBLIC

e-Attestations

Quels sont les impacts liés à l'achat public ?

Lorsque l'on associe cybersécurité et achat public, on pense souvent aux enjeux liés au choix d'un prestataire de cybersécurité.

Si cet angle est important, il ne doit pas faire oublier deux autres angles essentiels que sont :

- **L'intégration de la cybersécurité sur l'ensemble de ses procédures d'achat qu'elles soient de gré à gré ou formalisées ou qu'elles portent sur des marchés de fourniture, de service ou de travaux,**

- **La cybersécurisation des procédures d'achat** considérant que les données liées internes ou externes, exploitées à l'occasion de leur réalisation, présentent un caractère personnel et/ou sensible et donc intéressent des acteurs malintentionnés.

CYBERSÉCURITE DANS LE PROCESSUS ACHAT

Concrètement…

1. **Identifier la criticité du marché public au regard des enjeux SSI** : prévoit-on de sous-traiter le traitement de données personnelles, quelle est la sensibilité de ces données personnelles, quelles sont les données stratégiques susceptibles d'être partagées avec le prestataire ? comment intervient-il sur le SI de l'acheteur public ?

2. **Définir un clausier d'exigences techniques et bien choisir ses exigences SSI au regard du besoin** pour éviter les discriminations non justifiées

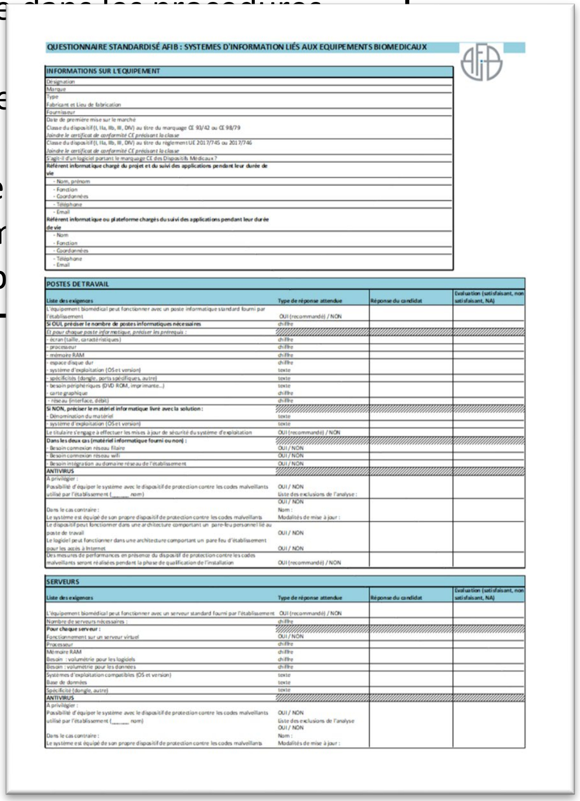
3. **La portée des exigences :** clauses contractuelles imposées à l'exécution (avec pénalités) et/ou condition de participation (certification) et/ou éléments à apprécier dans l'analyse des offres (critères, sous-critères).

Exemple de clause

Le Titulaire se conforme à la règlementation applicable en matière de protection des données, notamment personnelles ainsi qu'aux recommandations et référentiels applicables de la CNIL en matière de cybersécurité.

Le Titulaire respecte les cinq recommandations de l'AFIB en matière de sécurité numérique des équipements biomédicaux :

- Intégrer la sécurité numérique [...] d'acquisition ;
- Définir la collaboration dans le [...] santé ;
- Assurer la sécurité des équipe[...]
- Définir la criticité des équipem[...]
- Agir rapidement en cas de cyb[...]



Grands domaines d'exigences (exemples) pour un clausier utile à construire avec le RSSI

DOMAINE A EXAMINER	OBJECTIF/RESULTAT RECHERCHE
Sécurité Organisationnelle	Réponse obligatoire pour tout type de prestation. L'objectif est de savoir comment la sécurité est intégrée à l'organisation et fonctionne dans l'entreprise. De plus, l'acheteur souhaite avoir une idée des moyens mis en œuvre.
Sécurité Physique des locaux	Réponse obligatoire dans le cas où la prestation se réalisera en dehors des locaux de l'acheteur
Sécurité Informatique	Réponse obligatoire pour les prestations de développement informatique, exploitation de service ou toute autre prestation nécessitant une connexion au système d'information de l'acheteur. Les exigences de ce domaine sont valables dans le cas d'une prestation de développement pour le produit livré dans le cadre de cette prestation.
Exigences des prestations SaaS	Obligation de réponse pour toute prestation dans le Cloud de type *Software as a Service (SAAS)* sauf pour un candidat ou titulaire ayant le visa SecNumCloud et/ou "Cloud de Confiance" de l'ANSSI. Le candidat devra répondre aux exigences organisationnelle, physique, plan de continuité et plan d'assurance sécurité.
Plan de Continuité d'Activité	Obligation de réponse pour toute prestation d'exploitation et/ou de service.
Plan d'Assurance Sécurité	Obligation de réponse lors de la soumission de l'offre.

Exemples de clauses SSI

- L'exigence peut former une condition de participation à la consultation laquelle si elle n'est pas remplie exclut d'emblée les candidats potentiels :

> L'hébergement des données sur le territoire national ou européen est obligatoire. En outre, l'hébergement de certaines données doit répondre aux exigences légales et réglementaires (données à caractère personnel, données de santé, etc.).

- Il s'agit là d'une application concrète de l'article L.2112-4 CCP :

« Un acheteur public peut imposer que les moyens utilisés pour exécuter tout ou partie d'un marché, pour maintenir ou pour moderniser les produits acquis soient localisés sur le territoire des États membres de l'Union européenne afin, notamment, de prendre en compte des considérations environnementales ou sociales ou d'assurer ***la sécurité des informations*** *et des approvisionnements »*

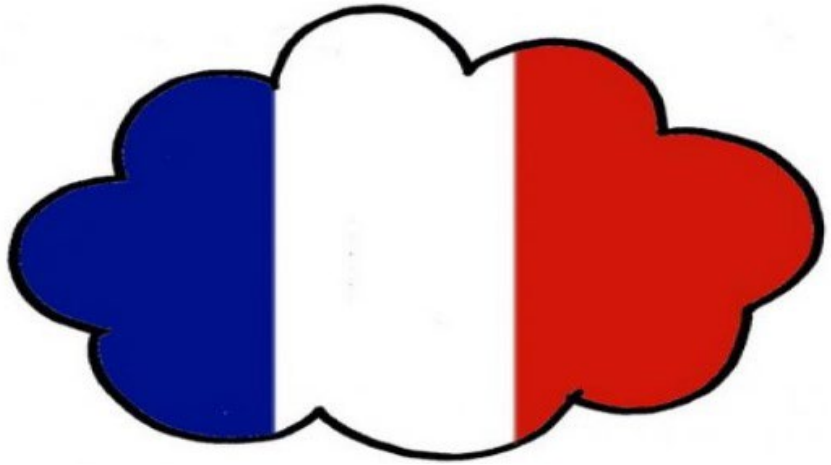
Exemples de clauses SSI

- L'exigence peut avoir la portée de clause contractuelle imposée à l'exécution au titulaire.
- Identifiée comme telle dans le CCTP, les candidats désireux de répondre à la consultation adapte leur offre et leur organisation en cas d'attribution, pour permettre l'exécution de la clause sous peine d'engager leur responsabilité contractuelle :

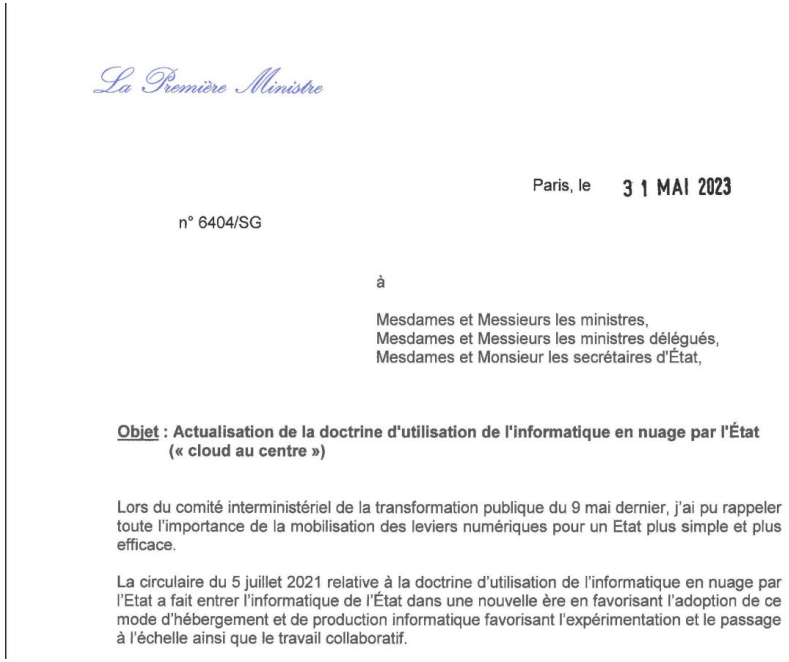
Le système d'information bénéficie d'une alimentation électrique de secours d'une autonomie minimale de 4 heures

Le point d’attention majeur … Le cloud

- Si vous avez des données sensibles à confier à un prestataire, ce dernier pourrait les faire héberger dans le cloud.
- Si ces données sont sensibles et que leur compromission serait de nature à porter atteinte à l'ordre public ou à la santé des personnes, etc. Vous ne pouvez pas ne pas vous soucier du mode d'hébergement de votre prestataire
- Si cloud US, lois US d'application extraterritoriale (FISA, cloud act).
- D'où la doctrine cloud de l'Etat et la certification "SecNumCloud" requise dès lors qu'un système d’information implique des données d’une sensibilité particulière.
- Exigence de nature à "assécher" la concurrence mais si elle est justifiée, elle doit s'imposer.



Doctrine cloud de l'Etat



La Première Ministre

Paris, le 31 MAI 2023

n° 6404/SG

à

Mesdames et Messieurs les ministres,
Mesdames et Messieurs les ministres délégués,
Mesdames et Monsieur les secrétaires d'État,

Objet : Actualisation de la doctrine d'utilisation de l'informatique en nuage par l'État (« cloud au centre »)

Lors du comité interministériel de la transformation publique du 9 mai dernier, j'ai pu rappeler toute l'importance de la mobilisation des leviers numériques pour un Etat plus simple et plus efficace.

La circulaire du 5 juillet 2021 relative à la doctrine d'utilisation de l'informatique en nuage par l'Etat a fait entrer l'informatique de l'État dans une nouvelle ère en favorisant l'adoption de ce mode d'hébergement et de production informatique favorisant l'expérimentation et le passage à l'échelle ainsi que le travail collaboratif.

Applicable à l'Etat et ses opérateurs

Recommandation R9 : un SI impliquant des données d'une sensibilité particulière dont l'hébergement se réalise dans le nuage, doit faire intervenir un opérateur certifié "SecNumCloud" et immunisée contre les lois extraeuropéennes

Qu'est-ce qu'une donnée d'une sensibilité particulière ?

Une donnée protégée par un secret légal (secret des affaires, secret de la défense nationale, etc.)

+

Dont la compromission porterait atteinte à l'ordre public, la sécurité, ou la santé des personnes, PI

Question de l'application par ricochet ?
Ex : marché de conseil prévoyant l'exploitation de données sensibles par le cabinet ?
Comment les données seront-elles traitées et hébergées ?

C’est quoi ?

« SecNumCloud » :

Certification de l’Agence nationale de sécurité des systèmes d’information (ANSSI) qualifiant les prestataires de services d’informatique en *cloud*. L’objectif est d’enrichir l’offre de prestataires de *cloud* « de confiance » à destination des entités publiques et privées souhaitant externaliser l’hébergement de leurs SI.

Immunité contre les lois extra-européennes :

L’Etat cherche à se prémunir de toute possibilité d’ingérence, en sollicitant que les choix des prestataires soient réalisés en consciente protection des lois extra-européennes. Cette exigence vise – principalement sans le nommer - le *Cloud Act US* (*Cloud Ac*t du 23 mars 2018 : *Clarifying Lawful Overseas Use of Data Act*, modification du titre 18 section 2703 du US Code), loi fédérale américaine qui étend la portée géographique des demandes des autorités américaines à pouvoir accéder aux données sur les serveurs, quelle que soit leur localisation. Quand on confie des données personnelles à un prestataire américain (ou un prestataire européen avec hébergement sur le territoire américain), on sait donc que le *Cloud Act US* peut s’appliquer.

CYBERSÉCURITE DU PROCESSUS ACHAT

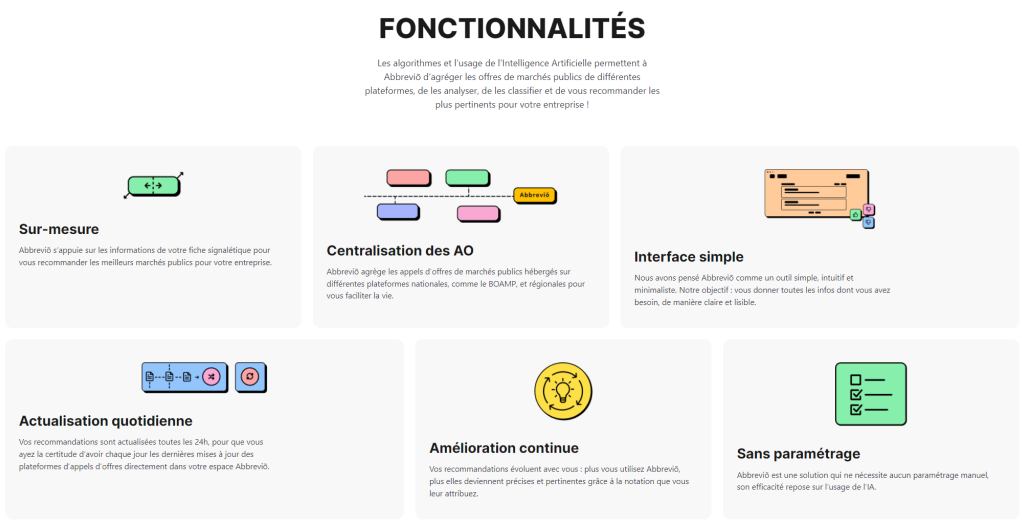
La cybersécuriation des procédures

Si la dématérialisation des procédures de marché publics s'est imposée, non sans mal, dans notre paysage de l'achat public, la digitalisation de ces processus a inévitablement engendré les risques associés.

En effet, si les acheteurs peuvent à juste titre faire confiance aux profils acheteurs disponibles sur le marché, de nombreuses zones d'ombres subsistent en amont de la publication et en aval de la contractualisation.

Si les données publiées par l'acheteur ont un caractère public, il est indispensable de préserver la liberté d'accès, la transparence et surtout l'égalité de traitement. Les risques sont par exemple les suivants :

- ✓ Accès à des éléments audio ou écrits en phase de sourcing ;
- ✓ Accès au dossier de consultation avant sa publication ;
- ✓ Accès aux réponses des candidats une fois décryptées.
- ✓ Autant de situations potentielles liées à des défauts de sécurisation des accès et des données au sein de l'établissement public sans oublier la crise qui a conduit de nombreux acheteurs à réaliser via des clés USB, disques durs externes ou pire encore des transferts via certaines plateformes, des analyses d'offres à leur domicile via un environnement informatique non sécurisé.

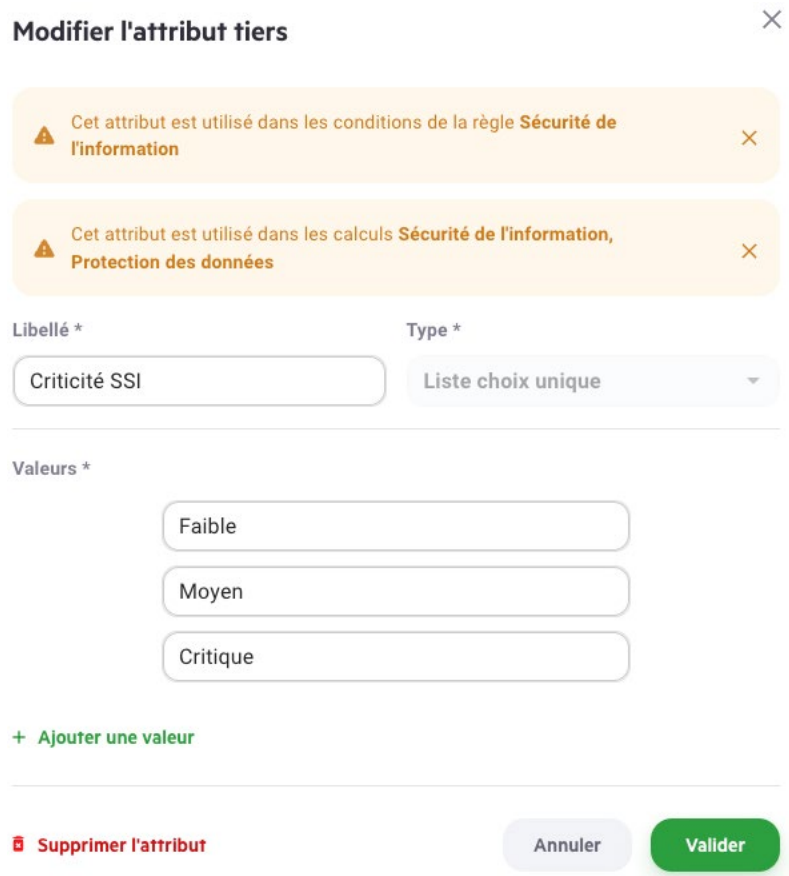


EN CONCLUSION, UNE EVALUATION CONTINUE DES RISQUES

Attribut : criticité SSI

Criticité

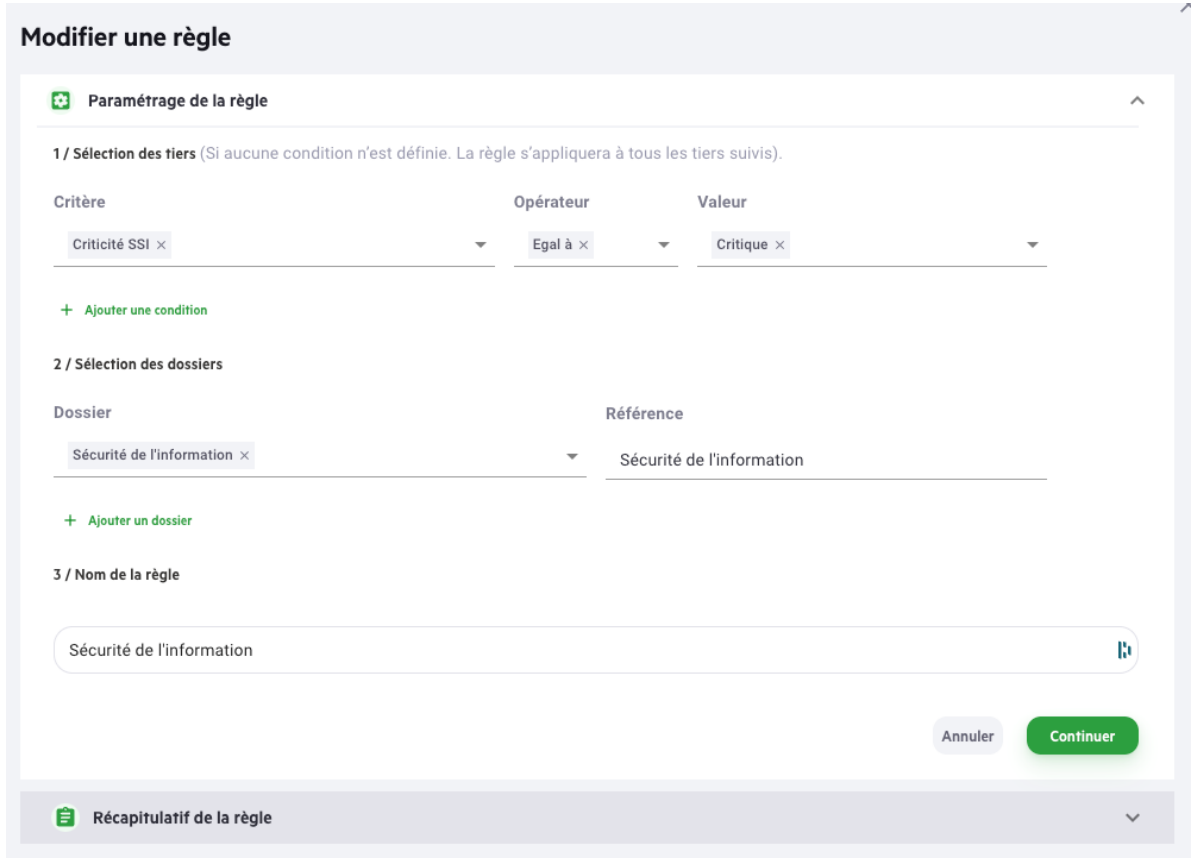
Niveau de criticité du prestataire	Critères
Niveau 1 : Faible	Le fournisseur n'est pas essentiel à l'activité d'e-attestations.com , Le fournisseur ne traite pas de données professionnelles d'e-Attestations.com et/ou de ses clients.
Niveau 2 : Moyen	Le fournisseur est important pour la réalisation des activités d'e-attestations.com mais peut facilement être remplacé par un autre. Le fournisseur traite des données personnelles de salariés e-Attestations.com et/ou de ses clients.
Niveau 3 : Critique	Le fournisseur est difficilement remplaçable, Le fournisseur traite des données personnelles de salariés e-attestations.com et/ou de ses clients susceptibles d'avoir un impact sur la vie privée des personnes concernées ou particulières. Le service qu'il délivre est indispensable pour le fonctionnement de l'activité d'e-attestations.com .

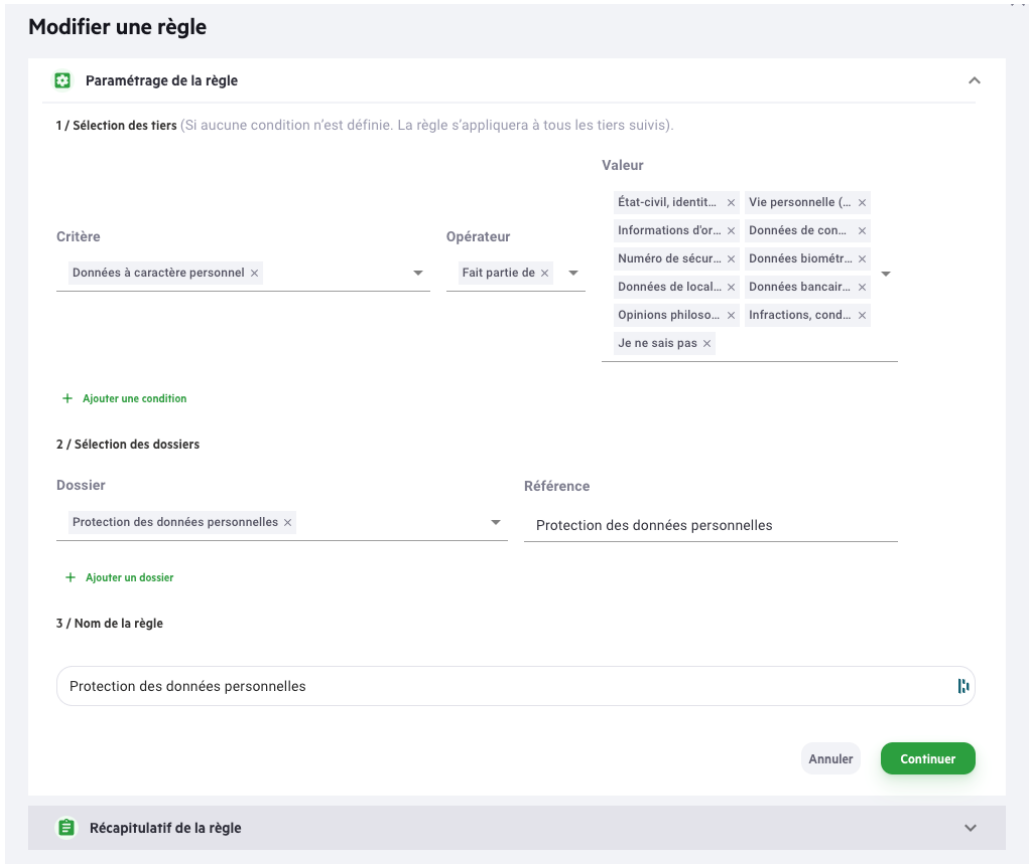


Tiers	Criticité SSI	Service demandeur	Familles d'achats	Sécurité de l'information	Protection des données	Complétude	Statut du fournisseur	Actions
ALTARES - D & B	Critique	Ventes, Produits, Communication	FOURNISSEURS DE DONNEES	OK avec réserves	Non concernée		OK	
AMAZON WEB SERVICES EMEA SARL	Critique	Technologie, Produits, Sécurité	IT PROD	OK	OK		OK	
ATLASSIAN PTY LTD	Critique	Technologie	IT PROD	OK	Non concernée		OK	
E-ATTESTATIONS.COM	Critique	Comptabilité, Sécurité	IT HORS PROD	OK	OK		OK	
SAGE	Critique	Comptabilité	IT PROD	OK avec réserves	Non concernée		OK	
YOUSIGN	Critique	Produits	IT PROD	OK avec réserves	OK		OK	
Zoho Corporation B.V.	Critique	Comptabilité, Ventes, Expérience clie...	IT HORS PROD	OK	OK		OK	

e-Attestations

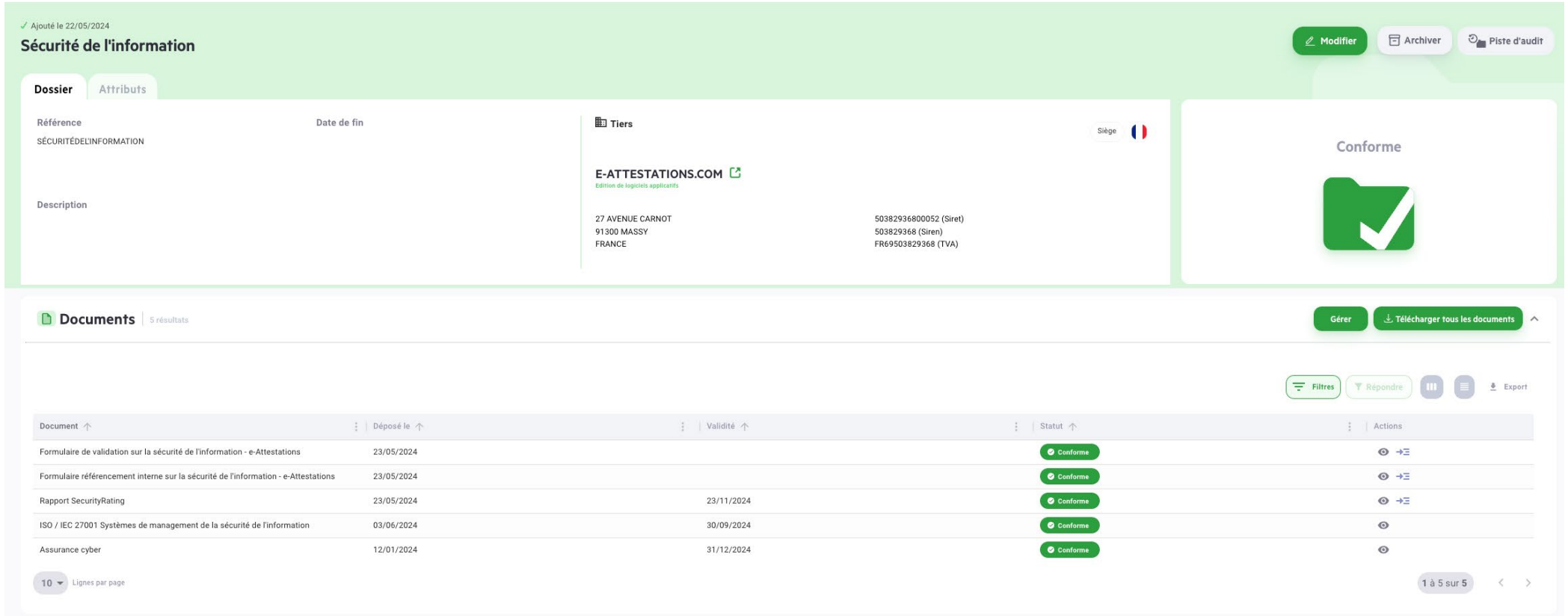
Règles : Sécurité de l’information et protection des données





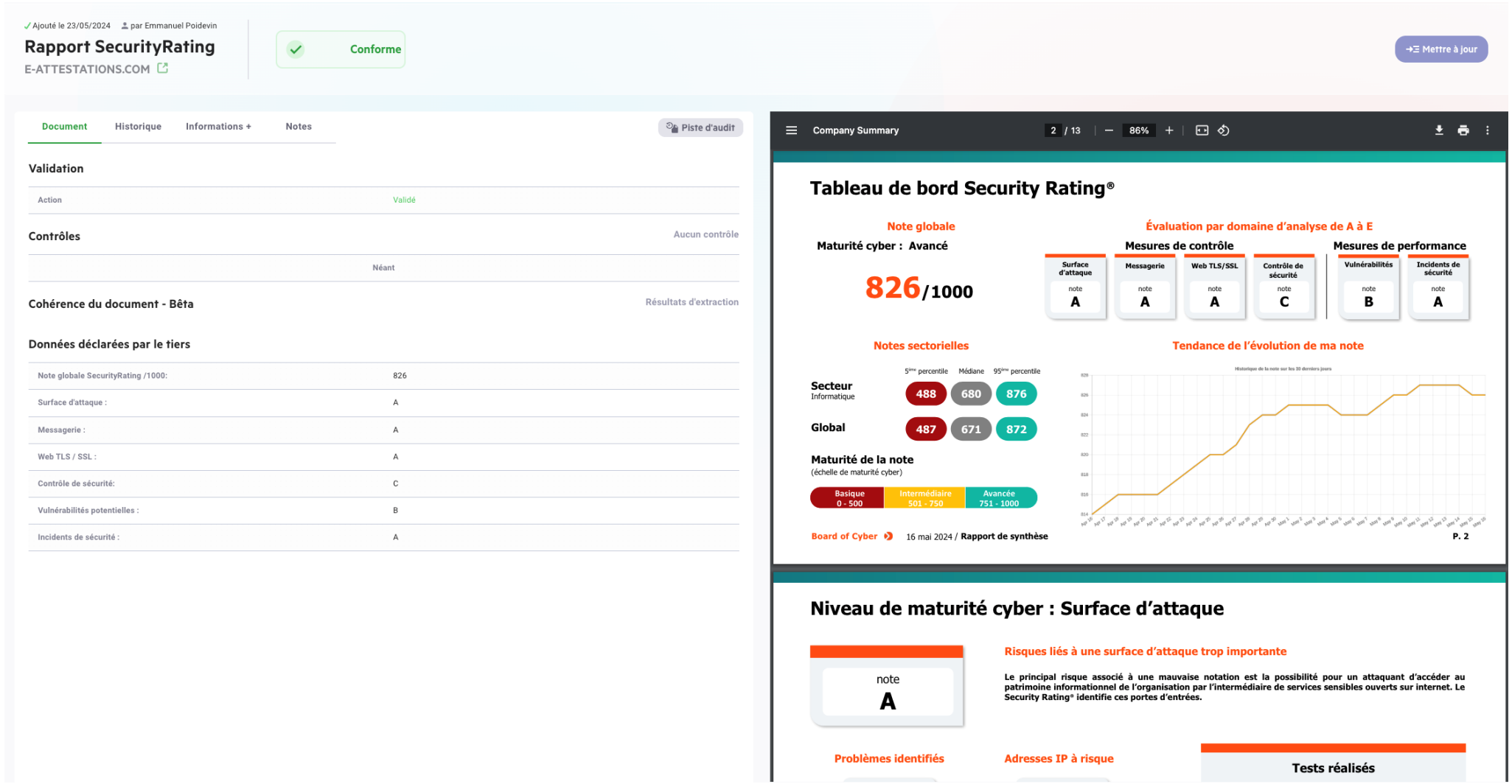
e-Attestations

Securité de l’information



e-Attestations

Score de maturité cyber : security rating



Preuves

✓ Ajouté le 03/06/2024 par Emmanuel Poidevin

ISO / IEC 27001 Systèmes de management de la sécurité de l'information

Tiers
E-ATTESTATIONS.COM
Edition de logiciels applicatifs

Conforme

Document | Historique | Informations + | Notes

Piste d'audit

Validation

Action	Validé
Commentaire	Validation automatique

Contrôles

Aucun contrôle

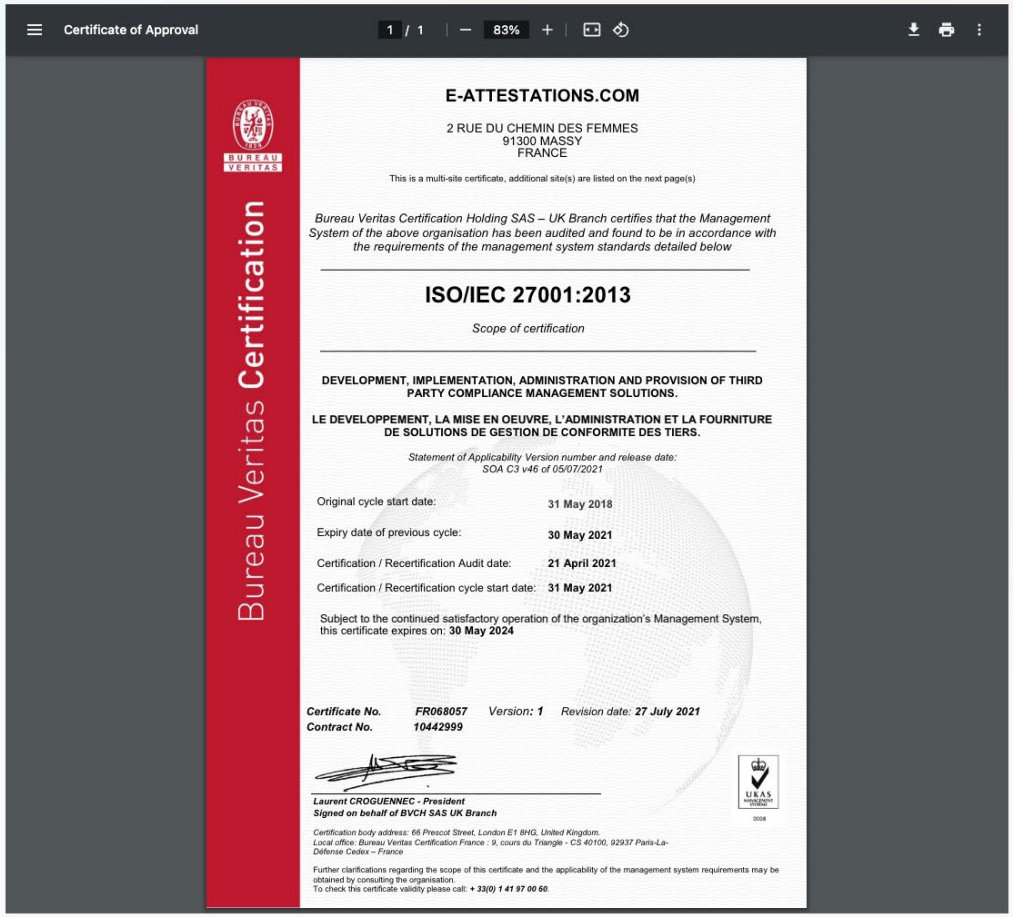
Néant

Cohérence du document - Bêta

Résultats d'extraction

Données déclarées par le tiers

Version du certificat	Element 1: 0: 2, Element 2: 0: 0, Element 3: 0: 1, Element 4: 0: 3,
Numéro de certificat	FR068057
Domaine(s) de certification	LE DEVELOPPEMENT, LA MISE EN OEUVRE, L'ADMINISTRATION ET LA FOURNITURE DE SO...
Organisme Certificateur	BUREAU VERITAS
Date d'obtention de la certification	31/05/2018



e-Attestations

Assurances

✓ Ajouté le 12/01/2024 par Pascal GUE

Assurance cyber

Tiers

E-ATTESTATIONS.COM

Edition de logiciels applicatifs

Conforme

Document | Historique | Informations + | Notes

Piste d'audit

Validation

Action	Validé

Contrôles

Aucun contrôle

Néant

Cohérence du document - Bêta

Résultats d'extraction

Données déclarées par le tiers

N°de contrat	RD00860750E
Nom de l'assureur	AIG
N°de tél de l'assureur	+33 9 69 32 15 24
Plafond de Garantie	1 500 000 €

Microsoft Word - Attestation PACK Cyber 0220... 1 / 2 89%

AIG

ATTESTATION D'ASSURANCE

PACK CYBER

contrat n° RD00860750E

Nous soussignés, **AIG EUROPE SA, Succursale pour la France, Tour CBX - 1 Passerelle des reflets, 92400 Courbevoie**, attestons que :

E-ATTESTATIONS.COM
27 Avenue Carnot Immeuble Galliléo
91300 MASSY

est assuré auprès de notre société par le contrat n° RD00860750E contre les conséquences d'atteintes à la sécurité de son réseau ou de la responsabilité civile pouvant lui incomber en raison d'atteintes aux données personnelles ou confidentielles.

Tous les termes qui apparaissent en caractères gras et en italique dans le corps du texte sont définis aux Conditions Générales..

MONTANT DES GARANTIES : 1.500.000 **EUROS** par ***période d'assurance.***

ACTIVITÉS DU SOUSCRIPTEUR ET DE SES FILIALES

CATÉGORIES D'ACTIVITÉS	DÉTAILS
Télécom et Gestion des données informatiques	Fournisseur d'accès internet, opérateur de télécommunication, infogérance, traitement de données informatiques. **À l'exclusion des hébergeurs et des fournisseurs de cloud.**

LA PRESENTE ATTESTATION EST DELIVREE POUR SERVIR ET VALOIR CE QUE DE DROIT POUR LA PERIODE DU 31/12/2023) AU 31/12/2024 A 0 HEURE ET N'IMPLIQUE QU'UNE PRESOMPTION DE GARANTIE A LA CHARGE DE L'ASSUREUR.

LA PRÉSENTE ATTESTATION NE SAURAIT ENGAGER L'ASSUREUR AU-DELÀ DES CLAUSES ET CONDITIONS DU CONTRAT AUQUEL IL CONVIENT DE TOUJOURS SE RÉFÉRER.

Adresse Postale : Service Gestion Pack AIG – Tour CBX - 1 passerelle des reflets, CS 60234, 92913 Paris La Défense Cedex
Téléphone : 09 69 32 15 24 – Courriel : gestion@packassurances.fr – Site internet : www.aig.com/fr/pack

e-Attestations

Piste d’audit

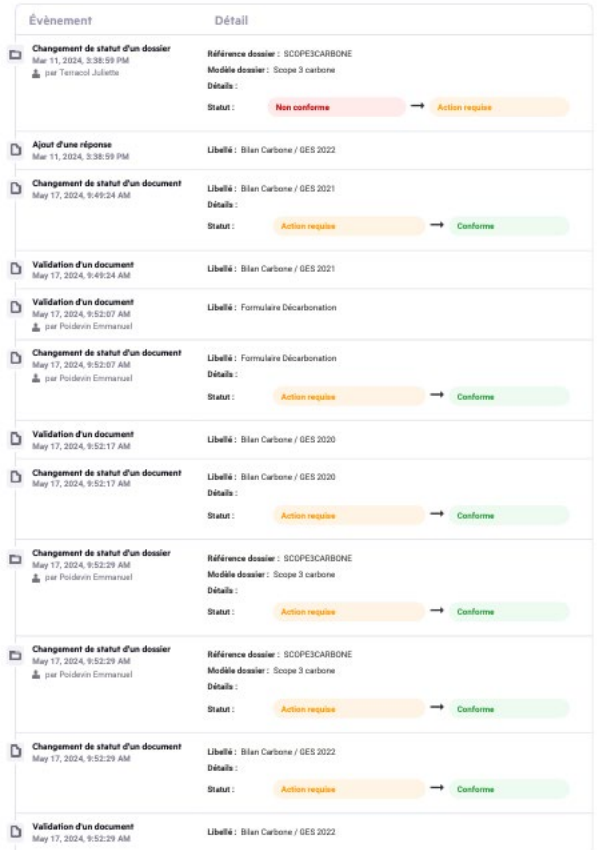
TIERS

E-ATTESTATIONS.COM

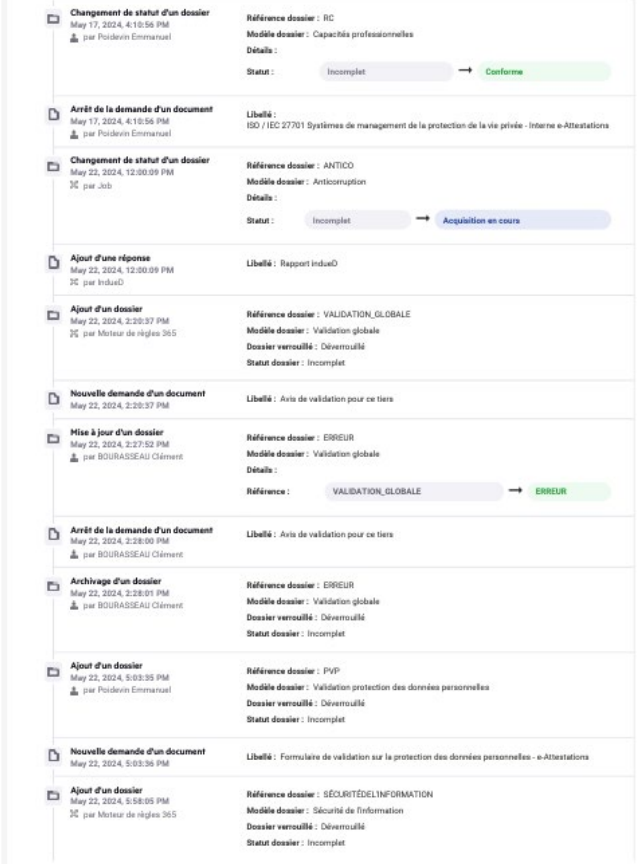
50382936800052

POWERED BY e-Attestations

PISTE D'AUDIT
03/06/2024 09:30:06



Évènement	Détail
Changement de statut d'un dossier Mar 11, 2024, 3:38:59 PM par Terracol Juliette	**Référence dossier :** SCOPE3CARBONE **Modèle dossier :** Scope 3 carbone **Détails :** **Statut :** Non conforme → Action requise
Ajout d'une réponse Mar 11, 2024, 3:38:59 PM	**Libellé :** Bilan Carbone / GES 2022
Changement de statut d'un document May 17, 2024, 9:49:24 AM	**Libellé :** Bilan Carbone / GES 2021 **Détails :** **Statut :** Action requise → Conforme
Validation d'un document May 17, 2024, 9:49:24 AM	**Libellé :** Bilan Carbone / GES 2021
Validation d'un document May 17, 2024, 9:52:07 AM par Poidevin Emmanuel	**Libellé :** Formulaire Décarbonation
Changement de statut d'un document May 17, 2024, 9:52:07 AM par Poidevin Emmanuel	**Libellé :** Formulaire Décarbonation **Détails :** **Statut :** Action requise → Conforme
Validation d'un document May 17, 2024, 9:52:17 AM	**Libellé :** Bilan Carbone / GES 2020
Changement de statut d'un document May 17, 2024, 9:52:17 AM	**Libellé :** Bilan Carbone / GES 2020 **Détails :** **Statut :** Action requise → Conforme
Changement de statut d'un dossier May 17, 2024, 9:52:29 AM par Poidevin Emmanuel	**Référence dossier :** SCOPE3CARBONE **Modèle dossier :** Scope 3 carbone **Détails :** **Statut :** Action requise → Conforme
Changement de statut d'un dossier May 17, 2024, 9:52:29 AM par Poidevin Emmanuel	**Référence dossier :** SCOPE3CARBONE **Modèle dossier :** Scope 3 carbone **Détails :** **Statut :** Action requise → Conforme
Changement de statut d'un document May 17, 2024, 9:52:29 AM	**Libellé :** Bilan Carbone / GES 2022 **Détails :** **Statut :** Action requise → Conforme
Validation d'un document May 17, 2024, 9:52:29 AM	**Libellé :** Bilan Carbone / GES 2022



Changement de statut d'un dossier May 17, 2024, 4:10:56 PM par Poidevin Emmanuel	**Référence dossier :** RC **Modèle dossier :** Capacités professionnelles **Détails :** **Statut :** Incomplet → Conforme
Arrêt de la demande d'un document May 17, 2024, 4:10:56 PM par Poidevin Emmanuel	**Libellé :** ISO / IEC 27701 Systèmes de management de la protection de la vie privée - Interne e-Attestations
Changement de statut d'un dossier May 22, 2024, 12:00:09 PM par Job	**Référence dossier :** ANTICO **Modèle dossier :** Anticorruption **Détails :** **Statut :** Incomplet → Acquisition en cours
Ajout d'une réponse May 22, 2024, 12:00:09 PM par IndueD	**Libellé :** Rapport indueD
Ajout d'un dossier May 22, 2024, 2:20:37 PM par Moteur de règles 365	**Référence dossier :** VALIDATION_GLOBALE **Modèle dossier :** Validation globale **Dossier verrouillé :** Déverouillé **Statut dossier :** Incomplet
Nouvelle demande d'un document May 22, 2024, 2:20:37 PM	**Libellé :** Avis de validation pour ce tiers
Mise à jour d'un dossier May 22, 2024, 2:27:52 PM par BOURASSEAU Clément	**Référence dossier :** ERREUR **Modèle dossier :** Validation globale **Détails :** **Référence :** VALIDATION_GLOBALE → ERREUR
Arrêt de la demande d'un document May 22, 2024, 2:28:00 PM par BOURASSEAU Clément	**Libellé :** Avis de validation pour ce tiers
Archivage d'un dossier May 22, 2024, 2:28:01 PM par BOURASSEAU Clément	**Référence dossier :** ERREUR **Modèle dossier :** Validation globale **Dossier verrouillé :** Déverouillé **Statut dossier :** Incomplet
Ajout d'un dossier May 22, 2024, 5:03:35 PM par Poidevin Emmanuel	**Référence dossier :** PVP **Modèle dossier :** Validation protection des données personnelles **Dossier verrouillé :** Déverouillé **Statut dossier :** Incomplet
Nouvelle demande d'un document May 22, 2024, 5:03:36 PM	**Libellé :** Formulaire de validation sur la protection des données personnelles - e-Attestations
Ajout d'un dossier May 22, 2024, 5:58:05 PM par Moteur de règles 365	**Référence dossier :** SÉCURITÉDEL1NFORMATION **Modèle dossier :** Sécurité de l'information **Dossier verrouillé :** Déverouillé **Statut dossier :** Incomplet

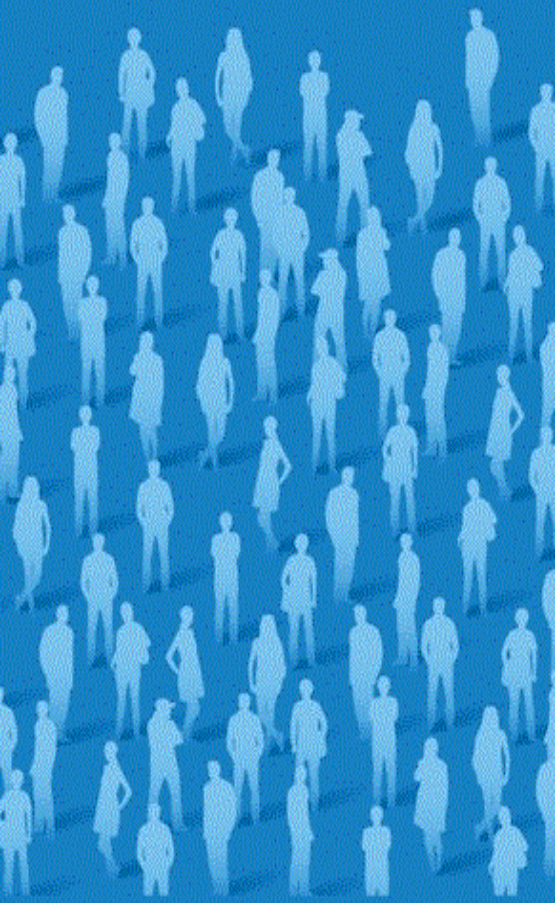
e-Attestations

MERCI

APASP

Association Pour l'Achat dans les Services Publics

www.apasp.com



Thème de notre prochaine Web Conférence

Filière textile, réindustrialisation et rôle de la commande publique

Le jeudi 19 SEPTEMBRE 2024 de 14 h 30 à 15 h 30

Animation :
Christelle DIDELOT, Directrice Générale de « Façon de faire », un collectif engagé du Fabriqué en France, durable et responsable, une nouvelle façon de faire du textile made in France
et
Sébastien TAUPIAC, expert en achat public et administrateur de l'APASP.

Programme

- La filière textile en France et le renouveau apporté par le collectif « Façon de Faire »
- La cohérence entre nouveau positionnement de la filière et objectifs des acheteurs publics (Loi Agec, Industrie verte, …)
- Comment acheter du textile « Made in France » avec le Code de la Commande Publique ?
- Cas d'usage avec les uniformes scolaires

Inscription : https://attendee.gotowebinar.com/register/4356420540551759959

L’APASP propose à ses adhérents une assistance technique marchés publics, une revue de presse, des Web formations suivies d’une journée pratique, des colloques, des séminaires, un outil de gestion « CEPHEE » pour les groupements de commandes…

Pour en savoir plus sur nos adhésions, rendez-vous sur www.apasp.com ou contactez nous au 01 42 80 93 93