SPAC
ALLIANCE

Chubb
POWERED BY APi GROUP

JOURNÉE DE LA SÉCURITÉ

STADE VÉLODROME

19 MARS 2026

1. SPAC Alliance
2. Nouvelles Menaces
3. NIS 2 / REC / CRA
4. Objectif : sécurité et conformité

1 – SPAC Alliance

FONDÉE EN 2020 – 3 MISSIONS

> INFORMER ET SENSIBILISER
> INFLUENCER ET AGIR
> NORMALISER ET CERTIFIER

NOUS RASSEMBLONS TOUT L'ECOSYSTÈME

SPAC ALLIANCE MEMBER

> INDUSTRIELS
> INTÉGRATEURS
> INSTITUTIONNELS
> FOURNISSEURS DE SERVICES

SPAC ALLIANCE CLUB

> UTILISATEURS
> INSTALLATEURS / BE
> CONSULTANTS
> JOURNALISTES

1 – Membres SPAC Alliance

SPAC
ALLIANCE

2- Évolution des Menaces

ATTAQUES CYBER

ATTAQUES PHYSIQUES

ATTAQUES HYBRIDES

« Il ne devrait plus y avoir d'écart entre sécurité physique et cybersécurité. »

ENISA Threat Landscape 2024

SPAC ALLIANCE

2- Quelques chiffres

Quelques chiffres :

9%

des attaques cyber réussies*

€€

attaques très coûteuses

X2

coûts comparés UE vs USA / Moyen Orient

*Rapport IBM sur le coût d'un vol de données 2020 - 2025

3 – Le maillage réglementaire

OBLIGATIONS
Entités publiques /privées

PRODUITS DE CONFIANCE
Fabricants, éditeurs

INNOVATION

CERTIFICATION
Schémas européens

SPAC ALLIANCE

3-NIS 2 : un nouveau paradigme

Network and Information Security 2 (10/2024)

PROTEGER PLUS

Plus d'entités concernées (EI - EE)

Implique la chaîne d'approvisionnement

PROTEGER MIEUX

Concept de sécurité de bout-en-bout

Lien entre sécurité cyber & physique

ACCOMPAGNER

Rapport d'incident rapide et obligatoire

Réseau transfrontalier CSIRT – CERT EU

SANCTIONNER

Pénalités financières

SPAC ALLIANCE

3-REC : maintient des activités vitales

Directive sur la Résilience des Entités Critiques(10/2024)

RÉSILIENCE

PROTÉGER

RÉAGIR

RÉSISTER

ATTÉNUER

ABSORBER

S'ADAPTER

SE REMETTRE

RISQUES PHYSIQUES

TERRORISME

MALVEILLANCE

CATASTROPHES NATURELLES

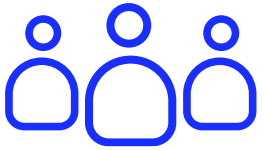
RÉCHAUFFEMENT CLIMATIQUE

"Assurer une protection physique adequate des locaux et infrastructures critiques",

ART 13.1.b

SUPERVISION

Rapport d'incident rapide et obligatoire



Audits externes cycliques & supervision

SANCTIONNER

Pénalités financières

SPAC >ALLIANCE<

3- NIS 2 / REC : qui est concerné ?

SECTEUR DE HAUTE CRITICITÉ	TYPE D'ENTITÉ			AUTRES SECTEURS CRITIQUES	TYPE D'ENTITÉ
	CRITIQUE (REC)	ESSENTIELLES CA > 50M€ EFFECTIF>250	IMPORTANTES CA < 50 M € STAFF 50 - 250		
ENERGIE	EC	EE	IE	POSTE ET DISTRIBUTION	IE
TRANSPORT	EC	EE	IE	GESTION DE DECHETS	IE
SECTEUR BANCAIRE	EC	EE	IE	FABRICATION, PRODUCTION ET DISTRIBUTION DE PRODUITS CHIMIQUES	IE
INFRASTRUCTURES DES MARCHÉ FINANCIERS	EC	EE	IE	FABRICATION, PRODUCTION ET DISTRIBUTION DE DENREES ALIMENTAIRES	IE
SANTÉ	EC	EE	IE	FABRICATIONS DIVERSES	IE
EAUX POTABLES	EC	EE	IE	FOURNISSEUR DE SERVICES NUMERIQUES	IE
EAUX RESIDUAIRES	EC	EE	IE	RECHERCHE	IE
INFRASTRUCTURES NUMERIQUES	EC	EE	IE		
ADMINISTRATIONS PUBLIQUES	EC	EE			
ESPACE	EC	EE	IE		
GESTION DES SERVICES TIC INTERENTREPRISES	EC	EE	IE		
FABRICATION, PRODUCTION ET DISTRIBUTION DE DENREES ALIMENTAIRES	EC				

EC	ENTITE CRITIQUE
EE	ENTITE ESSENTIELLE
IE	ENTITE IMPORTANTE

SPAC >ALLIANCE<

3 – Exemple : l'hôpital

Zones critiques

Zones sensibles

Zones Publiques

> Besoin de technologies de confiance adaptées et correctement déployées

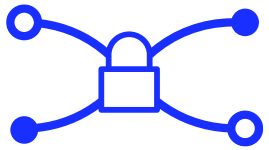
SPAC >ALLIANCE<

3 - Cyber Resilience Act

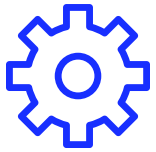
(10/2025)

CONCERNE LES PRODUITS AVEC UN ÉLÉMENT DIGITAL

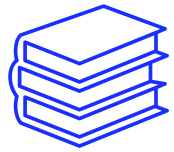
RESPONSABILITÉ DES FABRICANTS PARTAGÉE AVEC LES IMPORTATEURS ET DISTRIBUTEURS



Hardware et
Software



S'applique durant
tout le cycle de vie



41 Standards attendus
#16 : Contrôle d'accès, piloté par SPAC Alliance

Amendes : Jusqu'à 15 M€ / 2.5% du CA mondial

NON CONFORME = PAS DE MARQUAGE CE = INTERDIT SUR LE SOL EUROPEÉN

CE

SPAC
ALLIANCE

3 – NIS 2 et REC en France

Coûts d'une attaque : 5 à 10% du CA*

PME	ETI	GE
466 k€	13 M€	165 M€

Chiffres, planning et investissement

- > Passage de 500 à 15 000 entités concernées
- > Une seule loi cyber pour NIS 2 + REC + DORA
- > Investissement à prévoir : de 100/200k (EI) à 450/880K (EE)

LOI + DECRET 06/2026

Référentiel RECYF

SPAC >ALLIANCE<

**Cour des comptes – Réponse de l'état aux cybermenaces sur les SI civils – juin 25*

3 – RECYF : Référentiel Cyber France

20 objectifs de sécurité

QUOI

COMMENT

QUI

OBJECTIF DE SÉCURITÉ 6. MAITRISE DES ACCES PHYSIQUES AUX LOCAUX

RAPPEL DE L'OBJECTIF DE SECURITE

Les entités [importantes ou essentielles] mettent en place des mécanismes de contrôle d'accès et de gestion des droits d'accès ainsi que des processus de gestion des visiteurs afin de s'assurer que seules les personnes autorisées ont accès à leurs locaux et en particulier aux locaux techniques ou contenant des serveurs de données.

MOYENS ACCEPTABLES DE CONFORMITE

		ATTENDU D'UNE EI	ATTENDU D'UNE EE
6.1-EI/EE	L'entité met en place des mesures de sécurité permettant de limiter l'accès de personnes non autorisées à ses locaux, ses salles serveurs et ses locaux techniques (*par exemple : tenue d'un registre des visiteurs, badges d'accès, etc).*	Oui	Oui
6.2-EE	L'entité s'assure de la protection physique des locaux, salles serveurs et locaux techniques (*par exemple : vidéosurveillance, gardiennage, alarme*). Cette protection physique permet de prévenir, de surveiller et de réagir aux accès non autorisés à ces locaux.	Non	Oui

SPAC ALLIANCE

3 – RECYF : Référentiel Cyber France

La sécurité physique est une brique de conformité

GOUVERNANCE (#2)	GESTION RH (#4)	CONTRÔLE D'ACCÈS (#6)	CLOISONNEMENT SI (#7)	MENACES HYBRIDES (#9)

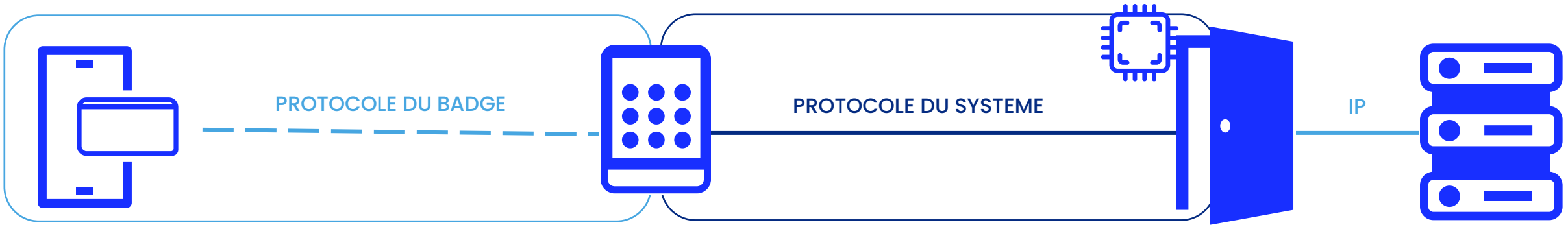
Correspondance avec d'autres référentiels

ISO 27001	ISO 27002	ISO 27005	EBIOS RISK MANAGER	Réglement d'execution 2024/2690

SPAC
>ALLIANCE<

4 – Assurer sa sécurité

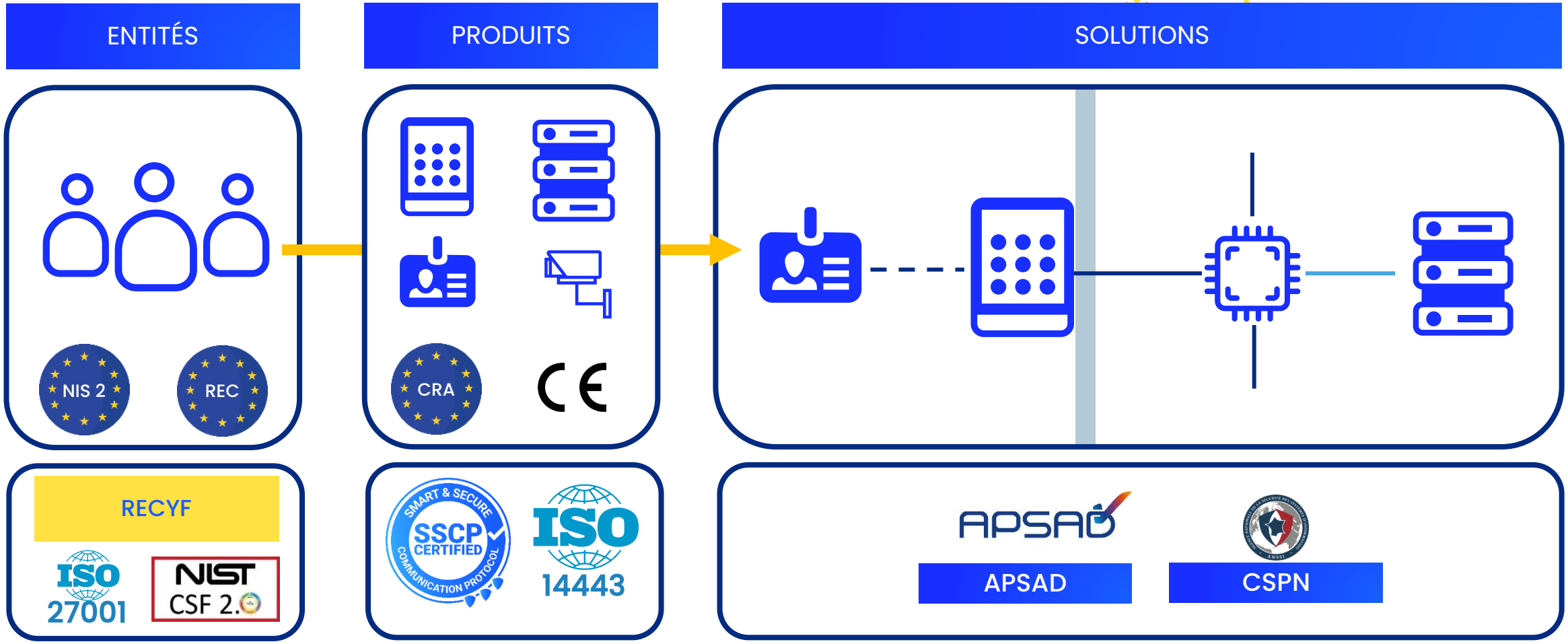
Ne pas confondre conformité et sécurité



NON SECURISE	125 KHZ	LECTEUR FRAGILE	WIEGAND – TTL – DATA CLOCK
SECURISE DE BOUT EN BOUT	13,56 MHZ ISO 14443	LECTEUR ROBUSTE	OSDP SC / SSCP

SPAC ALLIANCE

4 – Atteindre la conformité



SPAC ALLIANCE

4 – Par où commencer ?

COMPRENDRE SES BESOINS	COMPRENDRE SES OBLIGATIONS	DÉPLOYER TESTER ET MAINTENIR
ANALYSE DE RISQUE	S'IDENTIFIER / SE DÉCLARER	GOUVERNANCE DE LA SÉCURITÉ
MAPPING DES NIVEAUX DE SÉCURITÉ	MonEspaceNIS2 - Suis-je concerné ? - Pour bien débuter	PROCESS D'APPLICATION DES CORRECTIFS
CARTOGRAPHIE DES SYSTÈMES	ClubSSI - Anticiper l'enregistrement NIS 2	TEST D'INTRUSION PHYSIQUE ET CYBER
AUDIT	SE FORMER ET S'INFORMER SUR LE CADRE RÉGLEMENTAIRE	CHOIX DES PARTENAIRES

SPAC >ALLIANCE<

Conception, Expertise, Intégration et Risques métiers

APSAD ISO 27001

Maintenance

Certifications Multi-Marques

Cybersécurité

Notre approche sociotechnique :

Un sous-système social : structure organisationnelle et personnes liés au SI

Un sous-système technique: technologies (hardware, software et équipements de télécommunication).

Nos Méthodes :

EBIOS

AGILE

Chubb Delta
POWERED BY APi GROUP

DÉCOUVREZ TOUS LES SERVICES SPAC ALLIANCE :

LIBRAIRIE SPAC ALLIANCE

MINI AUDIT DE SÉCURITÉ

- GRATUIT
- ANONYME
- RAPIDE
- COMPLET

SERVICES

AUDIT DE SECURITÉ

GOUVERNANCE

ANALYSE DE BADGE

FORMATION MIFARE

REJOIGNEZ LE CLUB SPAC ALLIANCE

SPAC
ALLIANCE
CLUB

- > RENFORCEZ VOS COMPÉTENCES
- > ACCÉDEZ À TOUS NOS CONTENUS
- > TARIF SPÉCIAL SUR LES SERVICES
- > CONTACT DIRECT AVEC LES MEMBRES

Code : SPAC50

Contact

Mathieu Cyrille

+33 6 22 46 02 26

Mathieu.cyrillle@chubbfs.com

Chubb Delta
POWERED BY APi GROUP

Tibaud Estienne

+33 6 12 70 26 07

t.estienne@spac-alliance.org

SPAC
>ALLIANCE<

www.spac-alliance.org