

SPAC
>ALLIANCE<

Chubb
POWERED BY **API GROUP**

JOURNÉE DE LA SÉCURITÉ

STADE PIERRE MAUROY

06 OCTOBRE 2026

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

1 – SPAC Alliance

3 MISSIONS DEPUIS 2020

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

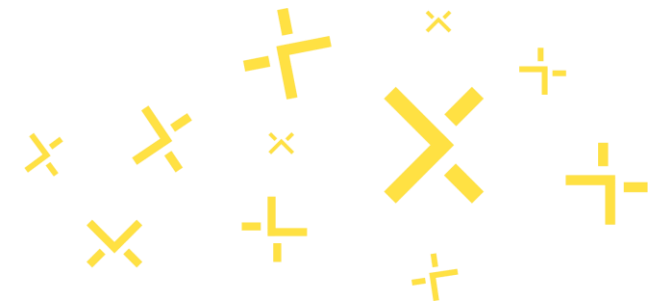
NOUS RASSEMBLONS TOUT L'ECOSYSTEME



- > INDUSTRIELS
- > INTEGRATEURS
- > INSTITUTIONNELS
- > FOURNISSEURS DE SERVICES



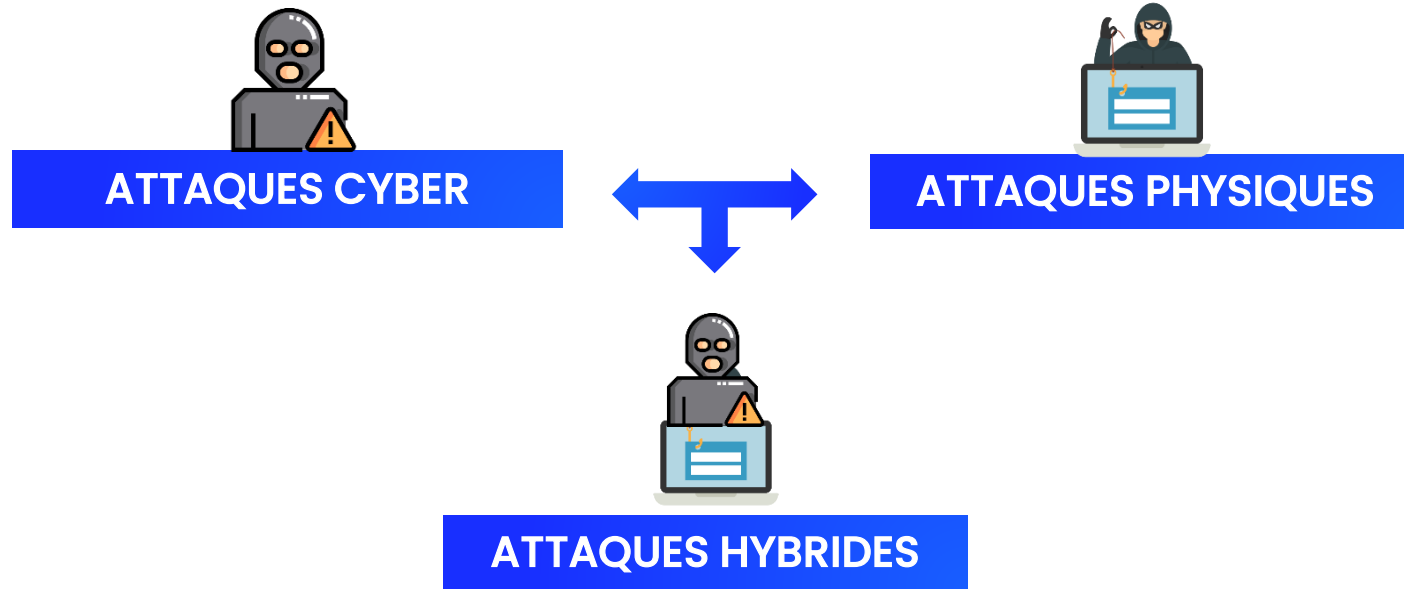
- > UTILISATEURS
- > INSTALLATEURS / BE
- > CONSULTANTS
- > JOURNALISTES



1 – Membres SPAC Alliance



2- Nouvelles Menaces



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

ENISA Threat Landscape 2024



2- Attaques hybrides

Quelques chiffres :

9%

**des attaques
cyber réussies***

30%

**des données sont
volées sur site***

€€

**attaques très
coûteuses**

X2

**coûts comparés
UE vs USA / Moyen Orient**



3 – Le maillage réglementaire



OBLIGATIONS
Entités publiques /privées



PRODUITS DE CONFIANCE
Fabricants, éditeurs



INNOVATION

CERTIFICATION
Schémas européens



3-NIS 2 : un nouveau paradigme

Network and Information Security 2 (10/2024)

PROTEGER PLUS



Plus d'entités
concernées (EI - EE)



Responsabilité collective et
transfrontalière

PROTEGER MIEUX



Concept de sécurité
de bout-en-bout

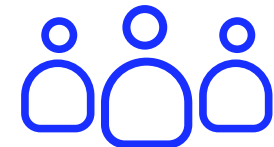


Lien sécurité cyber
& physique

ACCOMPAGNER



Rapport d'incident
rapide et obligatoire



Réseau transfrontalier
CSIRT - CERT EU



SANCTIONNER

Pénalités financières

3-REC : maintien 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

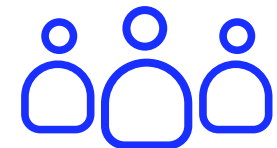
“Assurer une protection physique
adequate des locaux et infrastructures
critiques”,

ART 13.1.b

SUPERVISION



Rapport d'incident
rapide et obligatoire



Audits externes
cycliques &
supervision



SANCTIONNER
Pénalités financières

3 – NIS 2 et REC en France

Chiffres, planning et investissement

- > Passage de 500 à 18 000 entités concernées
- > Une seule loi cyber pour NIS 2 + REC + DORA
- > Investissement à prévoir : de 100/200k (EI) à 450/880K (EE)



LOI + DECRET FIN 2026

Référentiel ReCyF

NORMES SPECIFIQUES

Coûts d'une attaque : 5 à 10% du CA*

PME
466 k€

ETI
13 M€

GE
165 M€

3 – Exemple : l'hôpital



> Besoin de technologies de confiance adaptées et correctement déployées

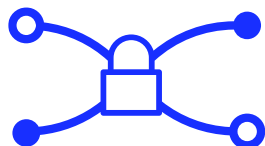
3 – Cyber Resilience Act



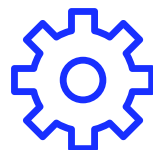
(10/2025)

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



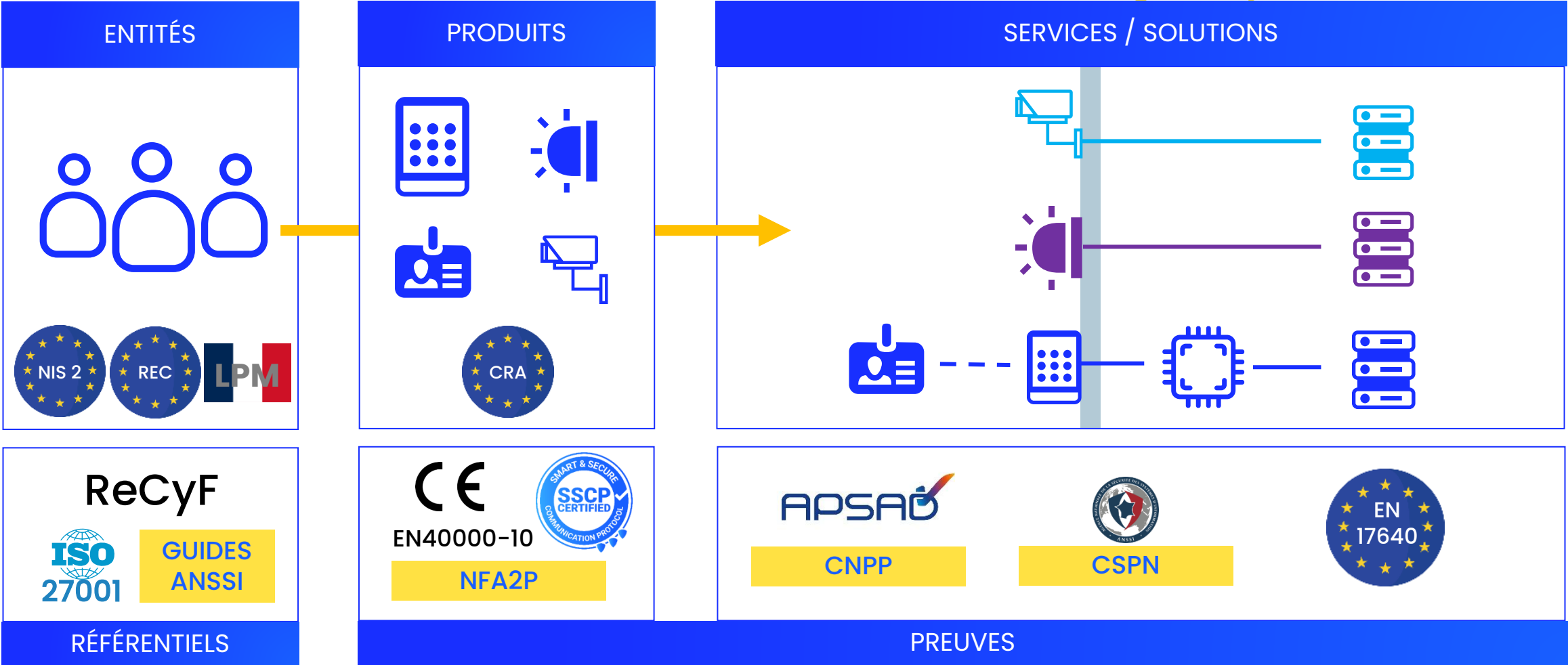
41 Normes harmonisées
EN 40000-10, initiée par SPAC Alliance

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

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



4 – Viser la conformité



4 – ReCyF : Référentiel Cyber France

20 OBJECTIFS

SÉCURITÉ PHYSIQUE
& CYBERSÉCURITÉ



MOYENS ACCEPTABLES
DE CONFORMITÉ



DOCUMENTATION ET
PREUVES

EXEMPLE

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 (<i>par exemple : tenue d'un registre des visiteurs, badges d'accès, etc</i>).	Oui	Oui
6.2-EE	L'entité s'assure de la protection physique des locaux, salles serveurs et locaux techniques (<i>par exemple : vidéosurveillance, gardiennage, alarme</i>). Cette protection physique permet de prévenir, de surveiller et de réagir aux accès non autorisés à ces locaux.	Non	Oui

4 – ReCyF et sécurité physique

OBJECTIFS 6 : MAÎTRISE DES ACCÈS PHYSIQUES AUX LOCAUX

6.1 : Limiter les accès non autorisés aux locaux

6.2 : Protéger physiquement, prévenir, surveiller, réagir

6.3 : Attribuer les droits d'accès en fonction des besoins nécessaires

6.4 : S'assurer que l'accès des visiteurs soit dûment autorisé

AUTRES OBJECTIFS LIÉS À LA SÉCURITÉ PHYSIQUE

Objectif 2 :
Chiffrement des données

Objectif 2 :
Application des correctifs et mises à jour

Objectif 4 :
Gestion des visiteurs, des arrivées et départs

Objectif 10 :
Changer les éléments secrets par défaut



Logique identique pour l'ISO 27001 / 27002

4 – Guide ANSSI GTB / GTC



BONNES PRATIQUES

MAÎTRISER LES ACCÈS AUX ÉQUIPEMENTS TECHNIQUES

SÉCURISER CHAQUE ÉQUIPEMENT

SÉCURISER CHAQUE COMMUNICATION

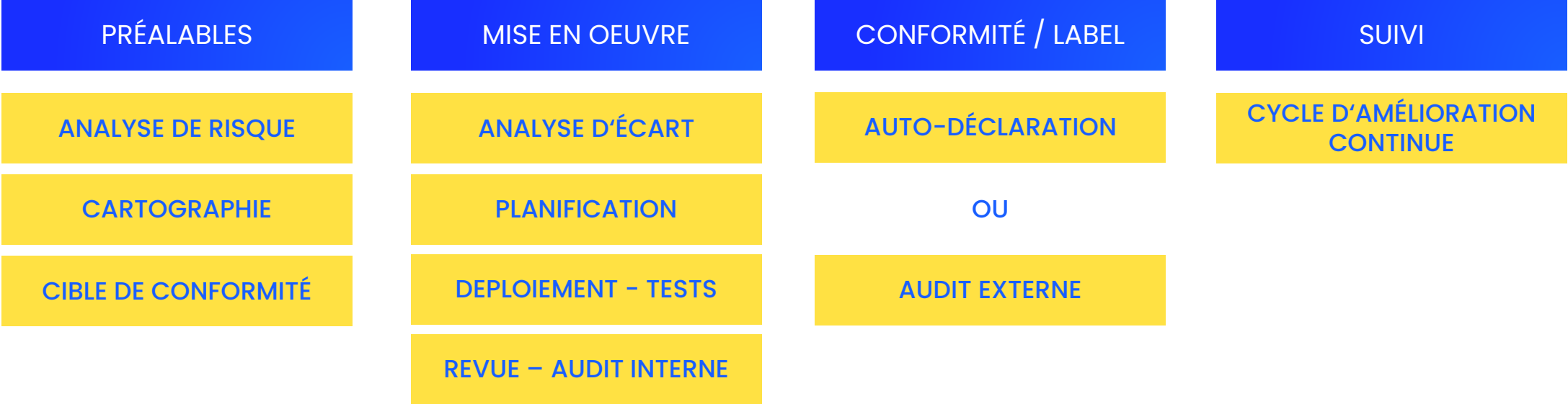
CCTP

PRÉCISION DES FONCTIONS / NIVEAUX DE SÉCURITÉ

DURÉE ET CONDITIONS D'ASSISTANCE ET DE SUPPORT

PREUVES (CERTIFICATIONS, DOCUMENTATION...)

4 – La démarche conformité



DÉCOUVREZ TOUS LES SERVICES SPAC ALLIANCE :

➤ **LIBRAIRIE SPAC ALLIANCE**

➤ **MINI AUDIT DE SÉCURITÉ**

GRATUIT

ANONYME

RAPIDE

COMPLET

➤ **SERVICES**



AUDIT DE SECURITÉ



GOVERNANCE



ANALYSE DE
BADGE



FORMATION
MIGRATION

REJOIGNEZ LE CLUB SPAC ALLIANCE



➤ RENFORCEZ VOS COMPÉTENCES

➤ ACCÉDEZ À TOUS NOS CONTENUS

➤ TARIF SPÉCIAL SUR LES SERVICES

➤ UN AN OFFERT AVEC LE CODE **CHUBB**

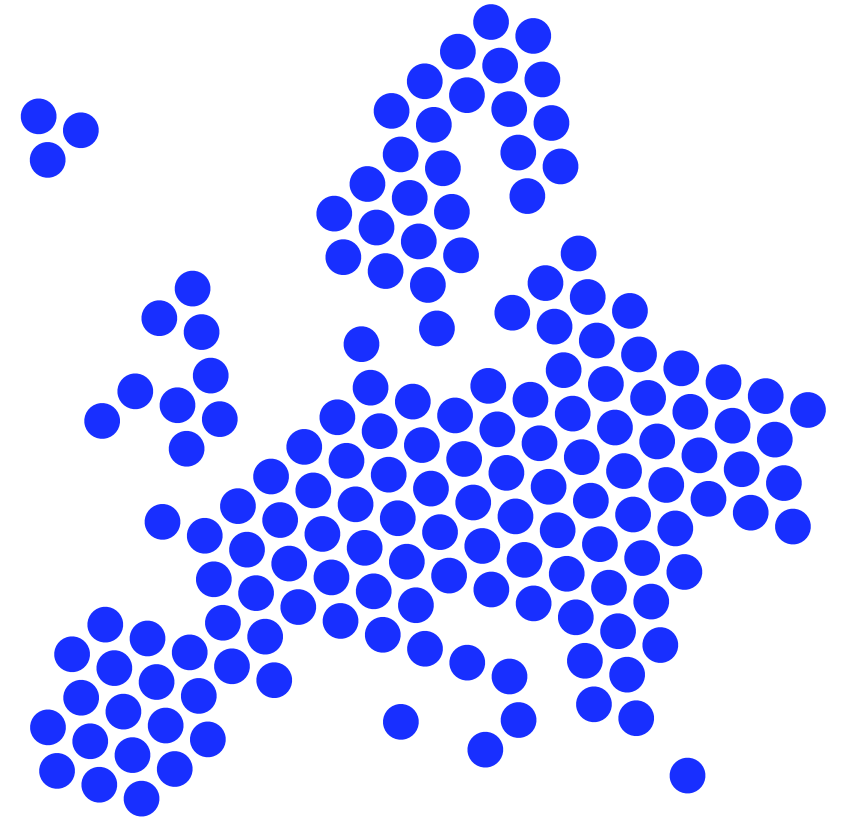


Contact

Tibaud Estienne

+33 6 12 70 26 07

t.estienne@spac-alliance.org



www.spac-alliance.org