

**Découvrez la
directive NIS 2 et
passez à l'action !**

NIS 

Introduction

A propos de l'ANSSI

- Créeée en 2009, l'**Agence nationale de la sécurité des systèmes d'information** (ANSSI) est l'**autorité nationale en matière de cybersécurité et de cyberdéfense** en France.
- Placée auprès du secrétaire général de la défense et de la sécurité nationale (SGDSN) l'ANSSI appartient aux services du Premier ministre.
- Son action pour la protection de la Nation face aux cyberattaques se traduit en cinq grandes missions : **défendre, connaître, partager, accompagner, réguler.**



Partout en Europe, la menace cyber élevée

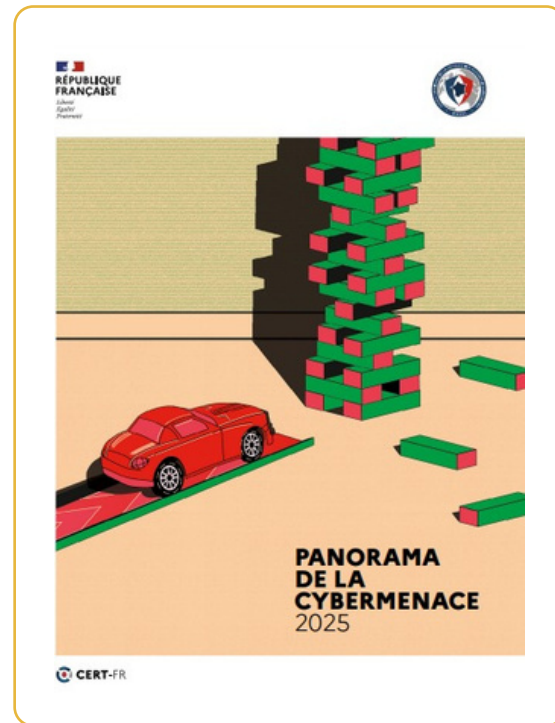
L'ensemble du tissu économique et social est ciblé :

1. De manière opportuniste et indifférenciée.
2. Notamment les secteurs critiques.
3. En particulier les PME et les collectivités territoriales.

La menace se maintient à un niveau élevé :

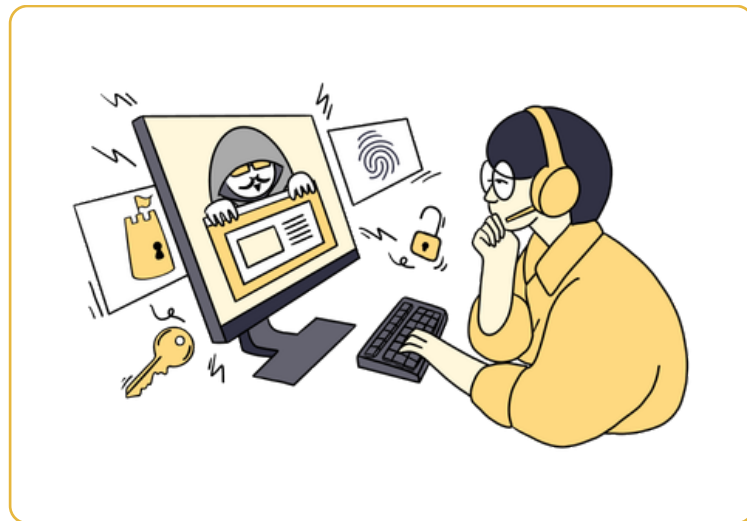
- Entre 2020 et 2025, un doublement du nombre d'attaques ;
- En 2025, 1366 incidents ont été portés à la connaissance de l'ANSSI (1361 en 2024), après des années de croissance.

Les **impacts de ces attaques peuvent être très graves**, en matière de continuité d'activité, financière, juridique ou réputationnelle.



Pourquoi tant d'attaquants parviennent à leurs fins ?

- 1.Des mesures de sécurité simples non mises en œuvre** (sensibilisation, sauvegardes, mauvaise configuration des équipements et logiciels, gestion des identités, etc.).
- 2.Des vulnérabilités techniques non corrigées, exploitées par les attaquants :** +50% des cyberattaques en 2024 exploitent des vulnérabilités d'équipements de sécurité « en bordure » (ex. Pare-feux, VPN, etc.).
- 3.Un défaut de supervision des incidents de sécurité.**



Mais la maturité des organisations reste faible !



● Insuffisant	1557 16%
● Émergent	3393 35%
● Intermédiaire	2708 28%
● Confirmé	1706 18%
● Optimal	250 3%

Baromètre de la maturité cyber

France, 23/03/2026

Source : messervices.cyber.gouv.fr

Quelle est la maturité
cyber de mon
organisation ?



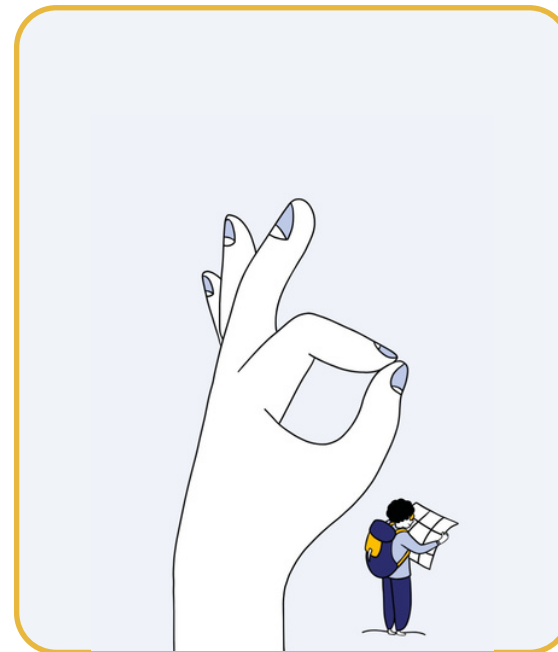
Je fais le test en 3mn !

Le test de maturité cyber évalue le positionnement global d'une organisation sur les enjeux de cybersécurité. Il ne s'agit pas d'un test de maturité vis-à-vis de la directive NIS2.

La directive NIS2

En 2016, la première directive NIS a été adoptée

- Elle constitue la première initiative européenne en matière de cybersécurité ;
- Son objectif : Garantir la continuité des activités économiques critiques en cas de cyberattaque ;
- Sa méthode : Imposer un socle minimal de cybersécurité à un certain nombre d'acteurs critiques, les opérateurs de service essentiel (OSE) et les fournisseurs de services numériques (FSN) ;
- Sa cible : 16 secteurs avaient été identifiés (énergie, transports, banques, santé, infrastructures numériques, etc.) ;
- Depuis 2016, 263 OSE ont été désignés en France.



NIS 2 : un changement de paradigme par rapport à NIS 1 pour faire face à une menace devenue systémique

Constat	D'une menace principalement ciblée à une menace également opportuniste
Cible	Touche l'ensemble du tissu économique, en particulier les petites structures (PME/ETI, collectivités territoriales, associations, etc.)
Changement d'échelle	De quelques centaines d'entités désignées à plus de 25 000 entités majoritairement régulées selon une logique de seuil
Niveau d'exigence	Un niveau de sécurité imposé et adapté à la maturité et au profil de l'entité
Sanctions	Sanctions administratives proportionnées au type d'entité et à la gravité des manquements

2 catégories d'entités assujetties

Pour garantir une proportionnalité de traitement, la directive NIS 2 distingue 2 catégories d'entités assujetties :

EE

Entités essentielles

Généralement des structures déjà sensibilisées ou confrontées à la menace cyber et déjà régulées.

EI

Entités importantes

Généralement des organisations moins matures et avec peu de ressources à consacrer à la cybersécurité.

**Mon organisation
est-elle concernée
par la directive NIS2
?**



Je fais le test !

Pour les entreprises, 17 secteurs sont concernés dans 2 catégories

Secteurs hautement critiques

- Administrations publiques
- Eaux potables
- Eaux non potables
- Énergies
- Espace
- Gestion des services Technologies de l'information et de la Communication (interentreprises)
- Infrastructures des marchés financiers
- Infrastructures numériques
- Santé
- Secteur bancaire
- Transport

Autres secteurs critiques

- Fabrication, production et distribution de produits chimiques
- Fournisseurs numériques
- Gestion des déchets
- Industries manufacturières
- Production, transformation et distribution de denrées alimentaires
- Recherche
- Services postaux et d'expédition

ETI et grandes
entreprises

Entités essentielles (EE)

Entités importantes (EI)

Moyennes
entreprises

Entités importantes (EI)

Micro et petites
entreprises

Entités non assujetties

Pour les administrations et les collectivités territoriales

Etat

Inclus comme EE ou EI selon les cas
à l'exception de celles exerçant des activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi

Région

Incluses comme EE

Echelon local

Incluses comme EE Inclus selon une logique de proportionnalité avec :

- Une approche par seuil pour certaines collectivités (fixé par la loi) ; et
- Une approche par « activités exercées » afin de viser celles relevant de **secteurs hautement critiques et critiques**

3 obligations principales pour les EE et EI



Enregistrer son organisation auprès de l'autorité nationale compétente. En France, l'ANSSI.

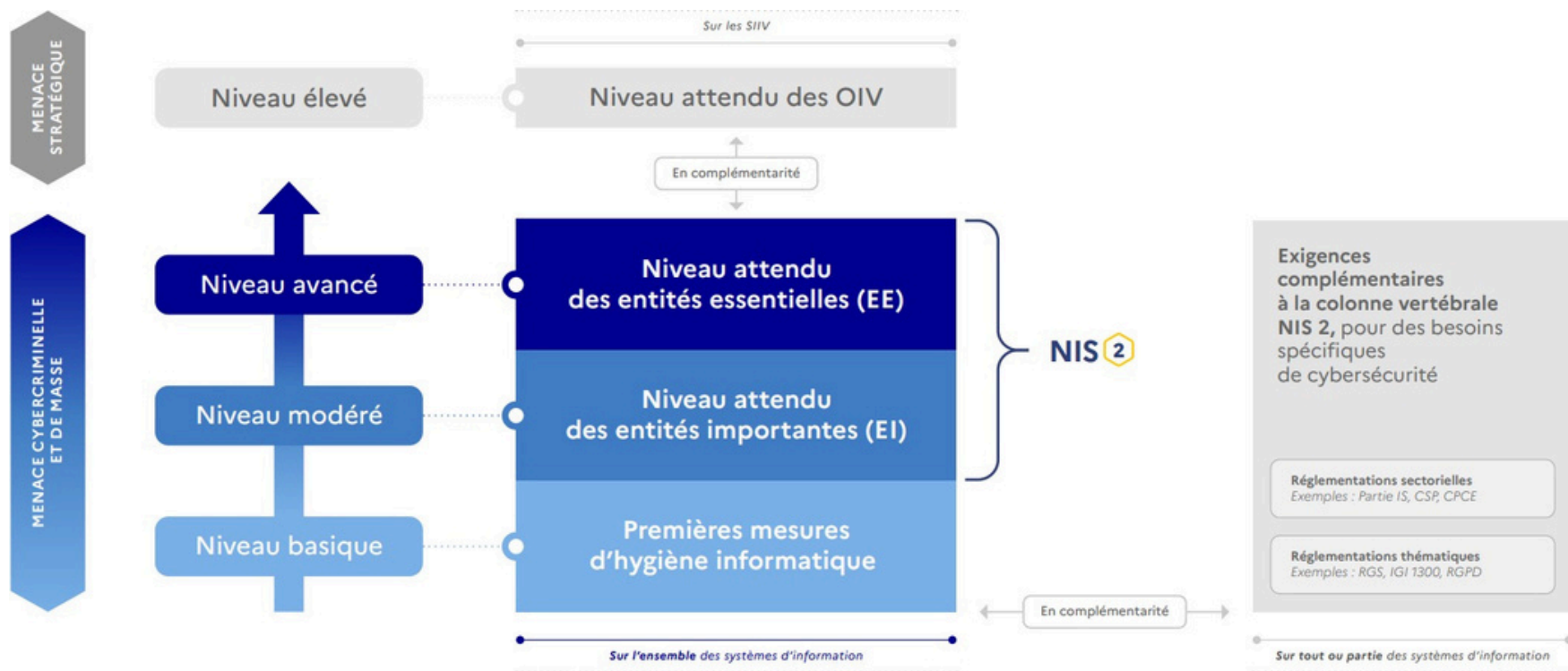


Mettre en œuvre des mesures de gestion des risques, par le respect des objectifs de sécurité fixés par la transposition de la directive NIS 2.



Notifier ses incidents importants et ses vulnérabilités critiques à l'ANSSI.

NIS 2 : colonne vertébrale du cadre réglementaire de cybersécurité



Des contrôles susceptibles de conduire à des sanctions

L'ANSSI travaille à l'intégration d'un rôle de supervision avec possibilité de mener des contrôles, d'instruire une procédure en cas de soupçons de manquement et de prononcer des mesures d'exécution.

Les mesures d'exécution comme les sanctions seront proportionnées à la gravité du manquement et prendront en compte le comportement de l'entité.

Une commission des sanctions indépendante sera instituée pour prononcer les sanctions :

EE

Entités essentielles

Jusqu'à 10 millions d'euros
ou 2 % du chiffre d'affaires
annuel mondial.

EI

Entités importantes

Jusqu'à 7 millions d'euros
ou 1,4 % du chiffre
d'affaires annuel mondial

Embarquez avec NIS2 grâce à un espace dédié !



www.messervices.cyber.gouv.fr/nis2





S'informer sur la directive



La directive, les secteurs concernés, les obligations, la FAQ.

FAQ MonEspaceNIS2 Bêta

Aller sur MonEspaceNIS2

Comment pouvons-nous vous aider ?

Rechercher sur le centre d'aide...

Cette FAQ est évolutive et est enrichie progressivement. Certaines questions-réponses dépendent de l'issue du débat parlementaire et des consultations sur les textes réglementaires, dans le cadre du processus de transposition. Les questions-réponses de cette FAQ seront mises à jour en conséquence.

Toutes les catégories

Introduction

Les clés pour comprendre la directive NIS2

Transposition nationale

Toutes les informations concernant l'organisation de la transposition nationale

Périmètre des entités

Comprendre quelles entités seront assujetties à la directive NIS2

Accompagnement de l'ANSSI

Les actions mises en place par l'ANSSI pour accompagner les entités régulées

messervices.cyber.gouv.fr/nis2



Vérifier son éligibilité



Un test pour permettre à une entité de vérifier si elle est concernée

Mon entité est-elle concernée ?

Déterminez si votre entité est régulée par la directive NIS 2

Pour bien débiter

Ce test permet de cerner si votre entité sera concernée par la directive NIS 2, et ce dès 2024. Nous le tiendrons à jour au fil des précisions apportées par la transposition en droit français.

Si votre entité appartient à un groupe d'entreprises aux activités variées, ce test peut être réalisé pour chaque entreprise filiale, ou pour le groupe si celui-ci mène une activité économique.



messervices.cyber.gouv.fr/nis2

✓ Enregistrer son organisation auprès de l'ANSSI



Un accès facilité au service de pré-enregistrement

NIS 2 : Pré-enregistrer mon entité **BETA**

Anticiper l'obligation d'enregistrement

La directive européenne NIS 2 permet d'élever le niveau de cybersécurité des entités essentielles et entités importantes par l'application de règles harmonisées et simplifiées.

Dans le cadre de sa mise en œuvre, et dans l'attente de l'entrée en vigueur de l'obligation d'enregistrement qui interviendra avec la publication des textes réglementaires, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) met à disposition des entités un service de pré-enregistrement pour leur permettre d'anticiper cette étape.

Le pré-enregistrement constitue la première brique de l'entrée en vigueur de NIS 2 et un premier pas pour les entités dans le respect de leurs obligations.



Pourquoi pré-enregistrer mon entité ?

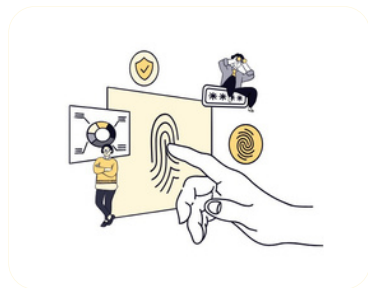
Comment s'assurer que mon entité est concernée ?

Qui peut pré-enregistrer puis enregistrer mon entité ?

Comment procéder au pré-enregistrement de mon entité ?



Réduire ses risques cyber



Le Référentiel Cyber France (ReCyF) applicable à NIS2

Exigence NIS 2	Correspondance	Référence ISO 27001/27002	Observations
SI SE Objectif de sécurité 1: Recensement des systèmes d'information / Recensement des SI / 1.3.4.1EE L'entité liste l'ensemble de ses activités et services, y compris les activités et services qui ne correspondent pas aux critères pour lesquels l'entité est devenue une entité importante ou essentielle (par exemple : une entité essentielle au titre d'une activité exploitation d'un oléoduc liste, en plus des activités et services participant à l'exploitation de l'oléoduc, tous les autres activités et services qu'elle fournit). Pour chaque entrée de cette liste, l'entité : - identifie un responsable de l'activité ou du service (par exemple le chef de service auquel est rattachée l'activité ou le service, un directeur métier, la direction générale, etc.) ; - liste les systèmes d'information les supportant.	MOYENNE	→ 27002-2022-5.9 Inventaire des informations et autres actifs associés	Afin de valider la mesure du référentiel NIS2, la recommandation ISO doit être complétée par un travail de d'inventaire des activités et services de l'entité.
SI SE Objectif de sécurité 1: Recensement des systèmes d'information / Recensement des SI / 1.3.4.1EE L'entité précise dans la liste prévue au (a) les systèmes d'information qui ne sont exposés à aucun des risques mentionnés à l'alinéa 2 de l'objectif de sécurité. L'entité renseigne les justifications de ces choix.	MOYENNE	→ 27001-2022-6.1.2 Appréciation des risques de sécurité de l'information → 27002-2022-5.9 Inventaire des informations et autres actifs associés	L'appréciation des risques effectuée dans le cadre des mesures ISO peut être réutilisée pour identifier les SI n'étant exposés à aucun des risques mentionnés à l'alinéa 2 de l'objectif de sécurité 1.
SI SE Objectif de sécurité 1: Recensement des systèmes d'information / Recensement des SI / 1.3.4.1EE L'entité valide et réexamine annuellement, ou en tant que de besoin notamment en cas de mise en service d'un nouveau système d'information, la liste prévue au (a)	FAIBLE / NULLE		
SI SE Objectif de sécurité 2: Mise en œuvre d'un cadre de gouvernance de la sécurité numérique Rôles et responsabilités / 2.A3.4.1EE Le dirigeant exécutif de l'entité est responsable de la sécurité numérique au sein de son entité et en particulier du suivi de la conformité des systèmes d'information aux présentes mesures.	ÉLEVÉE	→ 27001-2022-5.1 Leadership et engagement → 27002-2022-5.4 Responsabilité de la direction → 27002-2022-5.31 Exigences légales, statutaires, réglementaires et contractuelles	Il convient d'explicitier la responsabilité du dirigeant exécutif.

Le référentiel des exigences de sécurité (ReCyF) de l'ANSSI et **un outil de comparaison** avec d'autres référentiels.

messervices.cyber.gouv.fr/nis2



A tout instant, signaler un incident de sécurité à l'ANSSI



Un accès simplifié au formulaire de déclaration et de demande d'assistance du CERT-FR

RÉPUBLIQUE
FRANÇAISE
*Liberté
Égalité
Fraternité*

Club SSI

[Inscription](#)
[FAQ](#)
[EN](#)

Faire une déclaration au CERT-FR

Déclaration réglementaire, déclaration d'incidents ou demande d'assistance, accédez aux formulaires vous permettant de notifier le CERT-FR.

Déclaration d'incident sur votre système d'information

Le CERT-FR peut vous accompagner dans la gestion d'un incident de sécurité. Remplissez ce formulaire pour solliciter notre assistance ou remplir vos obligations de déclaration FSN, OSE ou OIV. Attention, les informations transmises ne doivent pas être de niveau Diffusion Restreinte ou classifiées.

* Champ obligatoire

Étape 1 / 5

Entité concernée par l'incident

* Nom de l'organisme victime

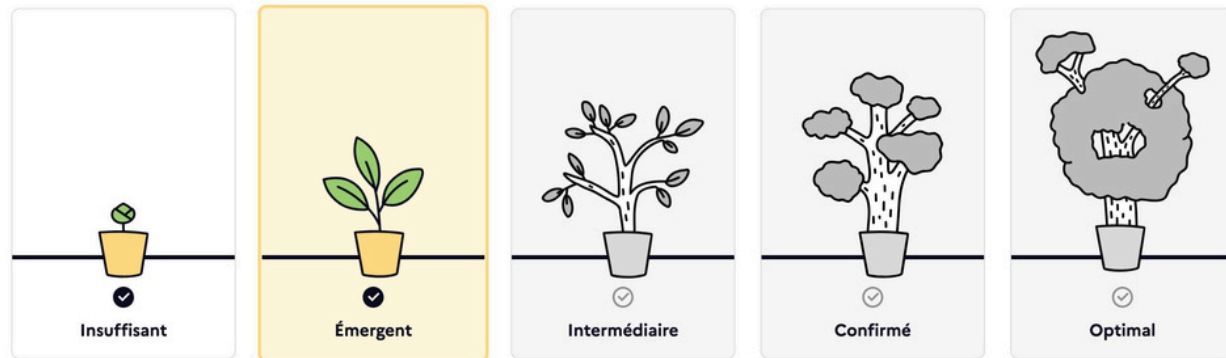
Recherche automatique des informations issues de la base Sirene* en utilisant l'API <https://recherche-entreprises.api.gouv.fr/>

**D'autres solutions pour
aider toutes les
organisations publiques et
privées**



Un test de maturité cyber (3mn)

Seul ou en groupe, pour évaluer le positionnement global d'une organisation sur les enjeux cyber.



messervices.cyber.gouv.fr

Le test de maturité cyber évalue le positionnement global d'une organisation sur les enjeux de cybersécurité. Il ne s'agit pas d'un test de maturité vis-à-vis de la directive NIS2.

**Quelle est la maturité
cyber de mon
organisation ?**



Je fais le test en 3mn !

Le diagnostic cyberdépart (1h)

Un 1er diagnostic cyber gratuit, adapté aux organisations qui souhaitent agir mais ne savent pas par où commencer.

- **Gratuit**
- **Rapide** (1h)
- **En visio ou présentiel**
- **Accompagné** par un Aidant cyber bénévole.



+5 400

Organisations déjà
accompagnées



92% sont satisfaites

Un catalogue d'outils, services, guides de l'ANSSI à explorer

CRISE CYBER



Rançongiciels

Attaques par rançongiciels, tous concernés.

ANSSI →

Service



Conseil Technique

Poser une question technique

ANSSI →

Outil



EBIOS Risk Manager

Réaliser une analyse de risque

ANSSI ↗

CRISE CYBER



Crise cyber

Organiser un exercice de gestion de crise cyber

ANSSI →

messervices.cyber.gouv.fr

Les contacts cyber utiles et prestataires labellisés



Les **contacts nationaux, régionaux et sectoriels.**



Les **prestataires qualifiés et labellisés.**

messervices.cyber.gouv.fr

Les financements cyber à jour



PRESTATIONS DE CONSEIL APPUI À L'INVESTISSEMENT

Cyber PME

PME ETI

BPI France



FORMATION

Pass Cyber formation

TPE PME

CCI des Hauts-de-France



APPUI À L'INVESTISSEMENT

Mon bouclier cyber expert

PME

Région Sud Provence-Alpes-Côte d'Azur



PRESTATIONS DE CONSEIL

Accompagnement CYBIAH

PME

Union européenne



AUDITS

Pass Cyber conseil

PME

Région Hauts-de-France



PRESTATIONS DE CONSEIL

Mon bouclier cyber essentiel

PME

Région Sud Provence-Alpes-Côte d'Azur

