# CENTRE RESSOURCES RÉGIONAL CYBER (C2RC)

MISSIONS ET ACTIVITÉS AUPRÈS DES PME DE LA RÉGION SUD PACA

T.JARDIN@C2RCSUD.ORG

C2RC
Centre Ressources Régional Cyber

# L'état des lieux

- **Les grandes entreprises investissent massivement dans la protection de leur infrastructure et de leurs données**
  - *Security Operation Center* (SOC), *Security Information & Event management (SIEM), Computer emergency response team (CERT),…*
- **L'état  et l'Europe ont lancés des programmes de sécurisation des infrastructures vitales**
  - Opérateur d'Importance Vitale (OIV) dans le cadre de la LPM pour la France
  - Opérateur de service essentiel (OSE) dans le cadre de la directive NIS (*Network and Information Security*) pour l'Europe.
- **Le citoyen, la TPE peuvent aujourd'hui accéder au service de en cas de cyberattaque**

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

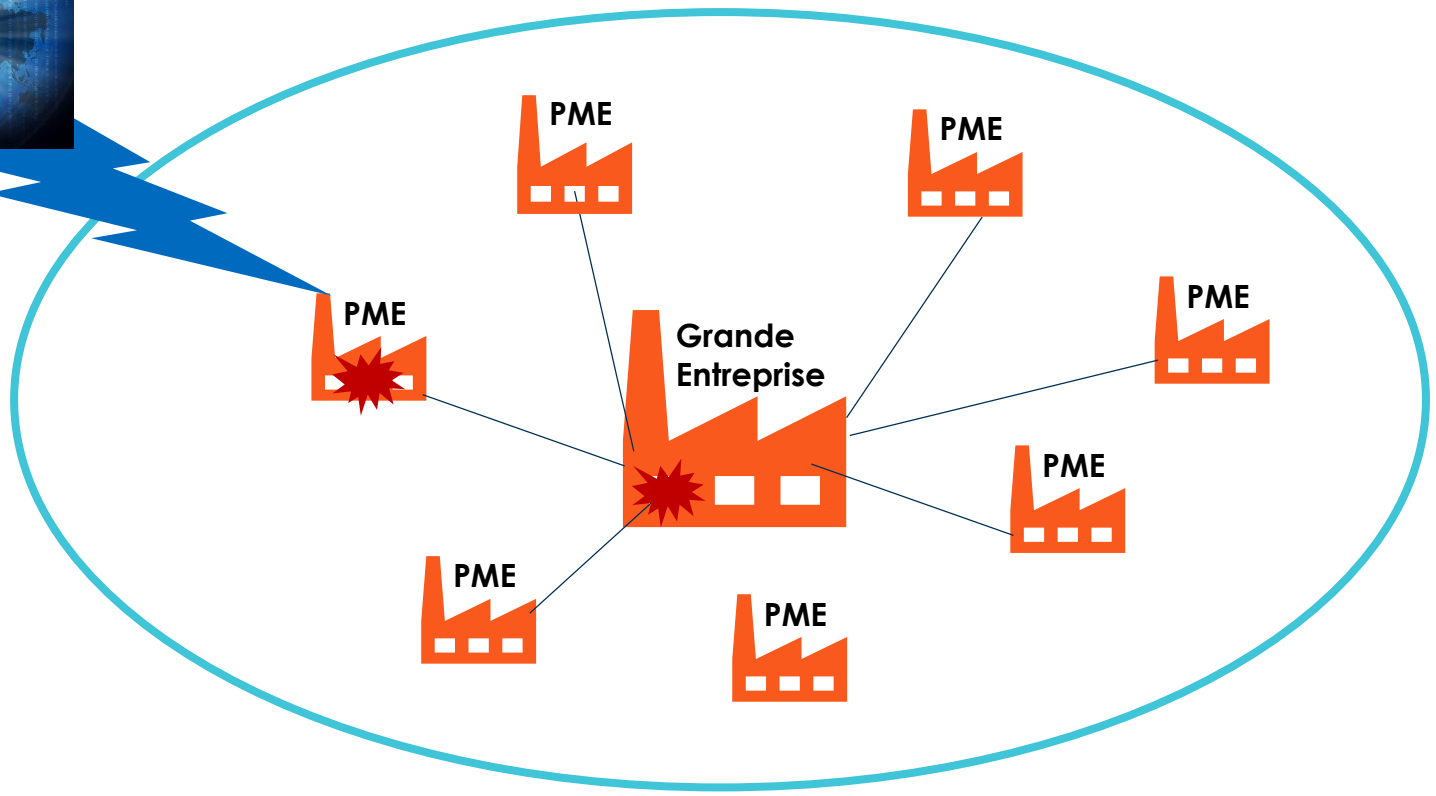
  - Service de questions/réponses qui apportent une réponse à une situation simple.



C2RC
Centre Ressources Régional Cyber

# Quand la vulnérabilité des PME impacte les grandes entreprises

- Quand la *supply chain* d'une grande entreprise est touché par une cyberattaque, c'est tout l'écosystème et notamment le donneur d'ordre qui peut être atteint.






C2RC
Centre Ressources Régional Cyber

# Situation actuelle

## Quid des PME /ETI et des collectivités locales ?

- Trop petites structures pour disposer des services de l'ANSSI qui ne peut être partout;
- Ne dispose pas des moyens financiers des grandes entreprises pour assurer sa propre protection;
- Problématique plus complexe que le particulier ou les TPE qui nécessite l'intervention d'un opérateur afin de qualifier l'incident.

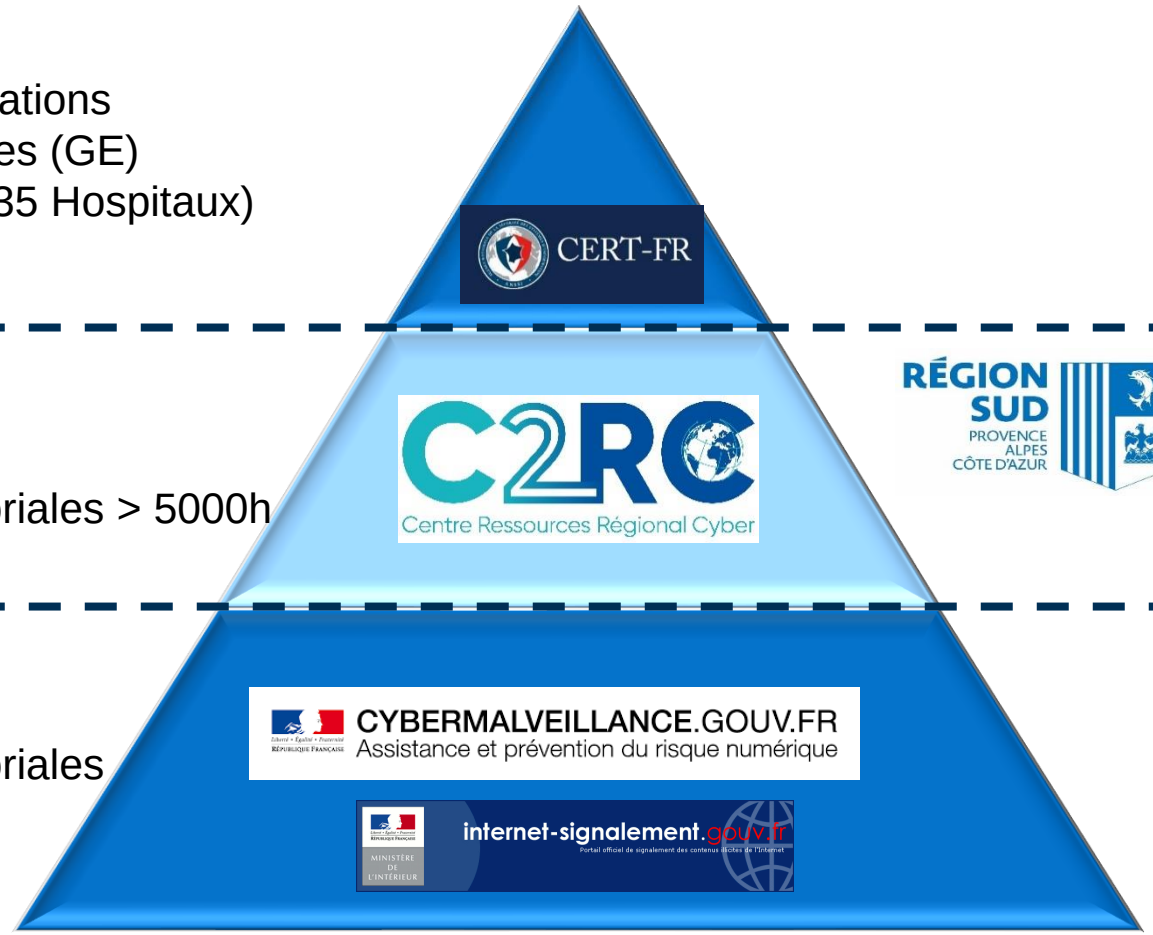
## 18 Février 2021 : Annonce du volet cybersécurité du plan France Relance

Par ailleurs, pour développer une protection autonome et efficace sur le long terme des entités publiques, un programme d'incubation à la création de centres régionaux de réponse d'urgence aux incidents cyber (CSIRT) est développé par l'ANSSI, en partenariat avec les régions.

# Positionnement

- Grandes Administrations
- Grandes Entreprises (GE)
- OIV / OSE( dont 135 Hospitaux)
- Métropoles

- ANSSI
- CERT/CSIRT grands groupe
- CERT/CSIRT sectoriels




- ETI
- PME
- Collectivités Territoriales > 5000h

- CERT/CSIRT Régionaux

- TPE
- Collectivités Territoriales
- Particuliers

- Cybermalveillance
- Pharos



C2RC
Centre Ressources Régional Cyber

# Missions

- **Assurer une veille** à partir de l'écosystème sécurité informatique régional et national sur les menaces et les vulnérabilités.
- **Sensibiliser** les entreprises de la région de manière permanente en relayant par mail les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité.
- **Alerter** par mail les entreprises à partir d'un maillage des organismes en charge de cybersécurité et des remontées d'informations des entreprises sur des menaces et vulnérabilités.
- **Accompagner** les entreprises  victimes d'un incident informatique et les orienter vers des prestataires en sécurité informatique, référencés de la région.



- Le C2RC assure <u>gratuitement</u> les services d'alerte et de réponse à l'incident pour l'ensemble des entreprises de la région
- <u>Une inscription préalable</u> aux services du C2RC est nécessaire afin de disposer des services d'assistance.



C2RC
Centre Ressources Régional Cyber

# Pourquoi le C2RC est unique

- **1er Centre Régional de réponse à incident en construction en France**
  - Structuration suivant les standards internationaux en Computer Emergency Response Team (CERT / CSIRT)
  - Intégration en cible au réseau de confiance et d'échanges ( ANSSI, Cybermalveillance, IntercertFR)

SIM3 Model & References

- **Proximité régionale**
  - Le C2RC est basé dans la même région que les entreprises inscrites
  - Connecté aux acteurs économiques de la région (pôles de compétitivité, collectivités territoriales, associations professionnelles)
  - En liaison avec les forces de police et les services régionaux de l'Etat

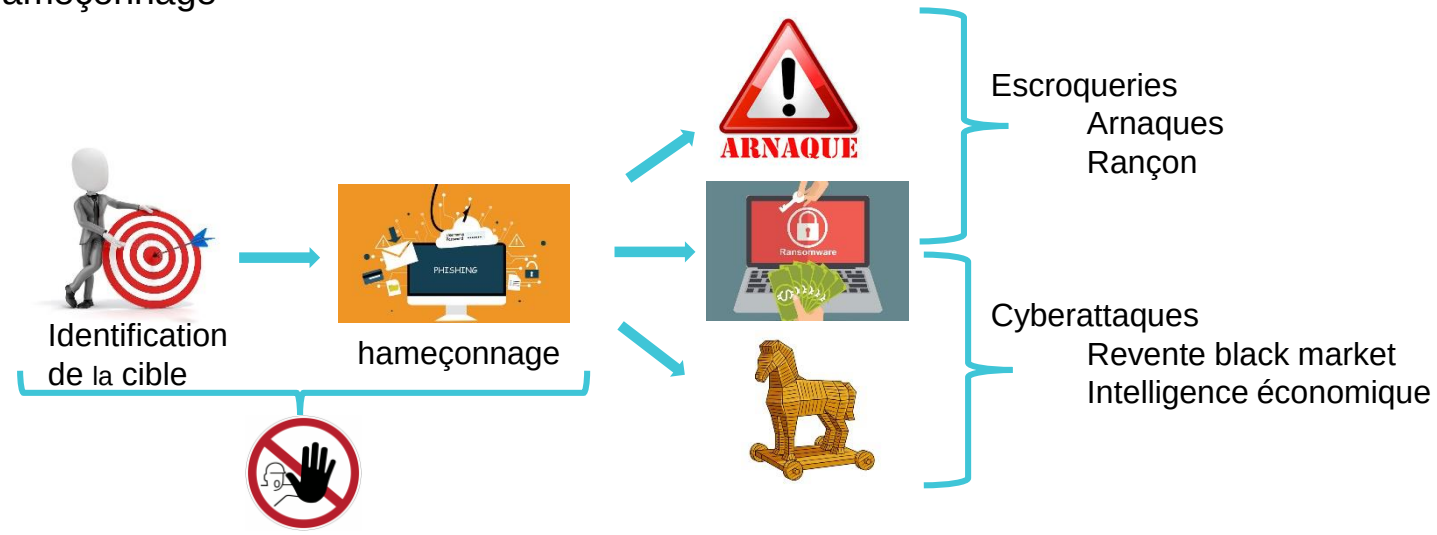
- **Accompagnement des entreprises**
  - Inscription obligatoire afin de disposer d'un premier aperçu du Système d'Information de l'entreprise
  - Emission d'information, recommandations et d'alertes vers ses inscrits en flux continu
  - Assistance « humaine » et personnelle en cas d'incident et suivi de la résolution


C2RC
Centre Ressources Régional Cyber

# Pourquoi le C2RC est unique

- **Développement économique dans le domaine de la cybersécurité**
  - Mise en avant des prestataires régionaux en cybersécurité possédant des labélisations de confiance
  - Intégration de la cybersécurité dans les programmes d'assistance aux startup de la région
  - Participation au renforcement de la sécurisation des sous-traitants des grands donneurs d'ordre.

- **Privilégier l'anticipation à la réaction.**
  - Assister par une sensibilisation continue des entreprises à :
    - Réduire son exposition à l'ingénierie sociale
    - Contrer le phishing/hameçonnage



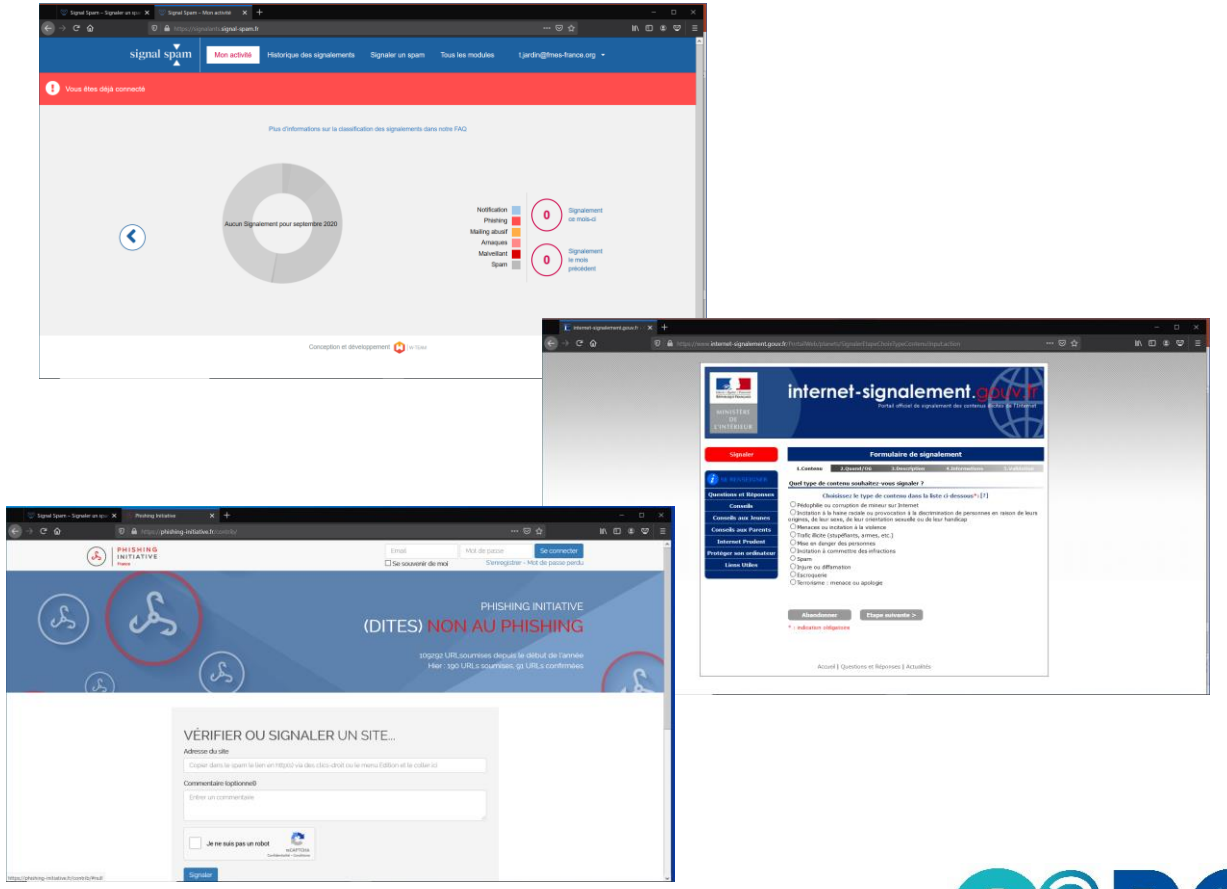
# Pourquoi le C2RC est unique

## Signalement systématique

- Incitation des entreprises au dépôt de plainte et/ou déclaration sur Pharos
- Signalement des mails suspicieux aux plates-formes nationales

## Assistance intelligente

- Limitation des impacts sur le système d'information, liés à la cyberattaque
- préservation des preuves numériques afin d'enquêtes
- Communication de coordonnées de prestataires informatique et/ou juridique en fonction de la situation






Centre Ressources Régional Cyber

# Gestion des inscriptions

**Référencement Prestataires**

① Demande d'inscription via WEB

② Vérification des services couverts

- *Localisation*
- *Taille*
- *certifications*

Affichage sur le site WEB

**Base des prestataires**

**Inscription TPE / PME / ETI**

Demande d'inscription via WEB

①

Demande d'inscription via acteurs régionaux

② Inscription Entreprise

- *Localisation*
- *Nomination correspondant C2RC*
- *Questionnaire sur le Système d'information*

**www.c2rcsud.org**

**Zone public**

**Zone privé**

Description générale du Système d'information (interne, externe, mixte) ③

**Base des Inscrits**



C2RC Centre Ressources Régional Cyber

# Service de Veille et d'Alerte

**Veille sur les menaces et les vulnérabilités**

CERT-FR

SEKOIA

Collecte informations sites officiels (.gouv.fr) ①

Collecte informations blogs, autres

② Analyse de l'information

- *Identification priorité*
- *Recherche des sources et croisement de l'information*
- *Traduction en termes compréhensibles*

**www.c2rcsud.org**

**Base d'Information**

③ Publication Site Web

**Zone public**

**Zone privé**

**Base des Inscrits**

④ Service d'alerte Mail, Newslettter

**Entreprise**

C2RC Centre Ressources Régional Cyber

# Service de gestion des incidents

Entreprise

Résolution cas simple

① Signalement incident par mail / téléphone

Base des Inscrits

② Analyse de l'incident niveau 1

Négociation et éventuellement résolution cas complexe

③ Analyse de l'incident Niveau 2

Gendarmerie nationale

POLICE NATIONALE

④ Signalement

Base d'information

⑤ REX de l'incident

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Collecte des informations de traitement de l'incident

Base des prestataires

④ Mise en relation avec des prestataires

Prestataires

Activités en cible

C2RC
Centre Ressources Régional Cyber

# Centre Opérations


Outillage
Et procédures

Analyse
vulnérabilités

**Poste Analyste**

**Bac à Sable**

---

**Coordinateur Cyber**

**Vigie**

**Régulateur**

Veille

- Veille
- Alerte

Escalade

- Pilotage
- Gestion es incidents

Niveau 2

- Gestion des incidents

Niveau 1

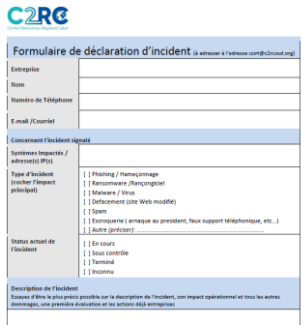
Mise à Jour

Alerte

Demande

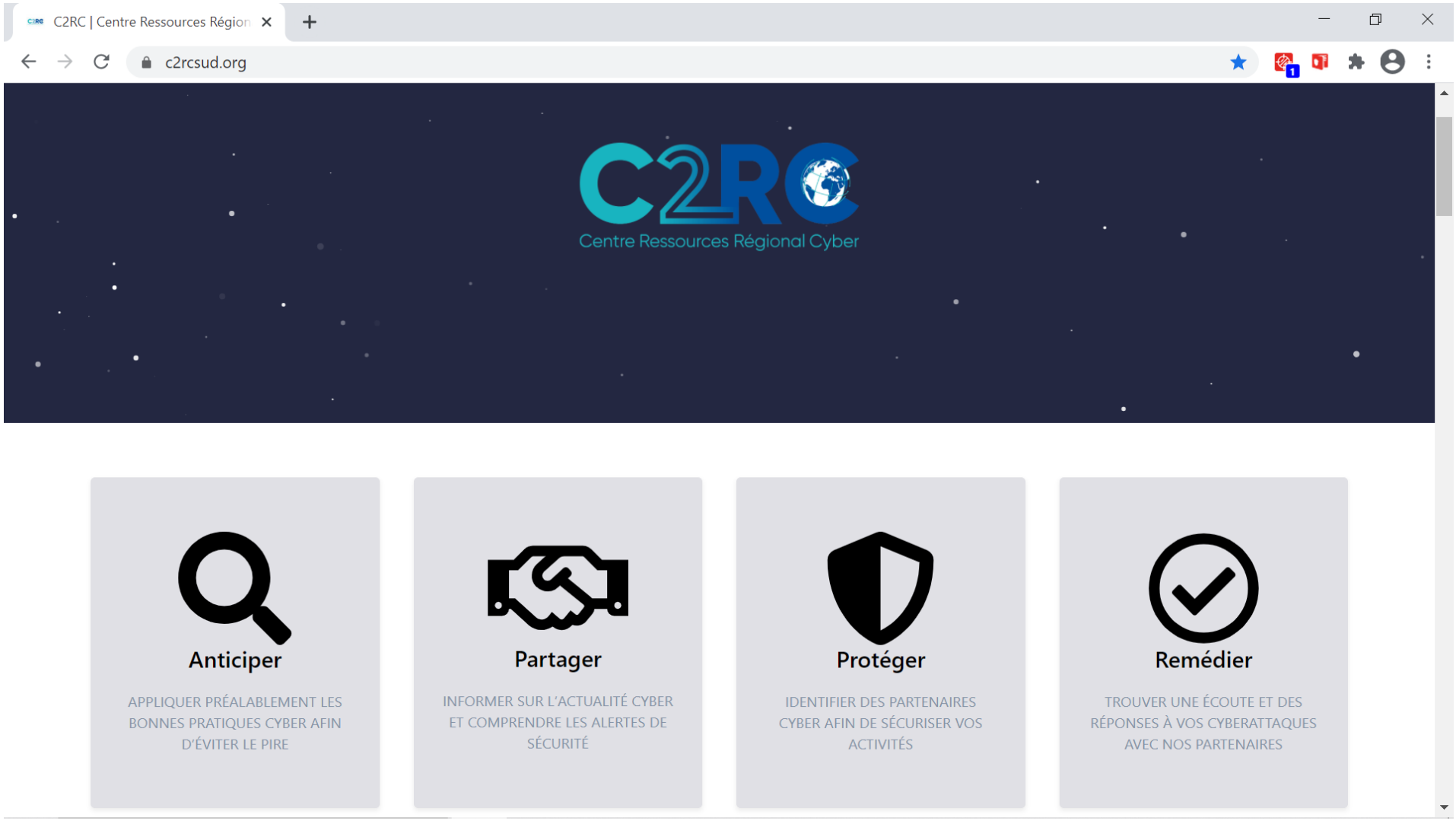
**C2rcsud.org**

**PME**


C2RC
Formulaire de déclaration d'incident

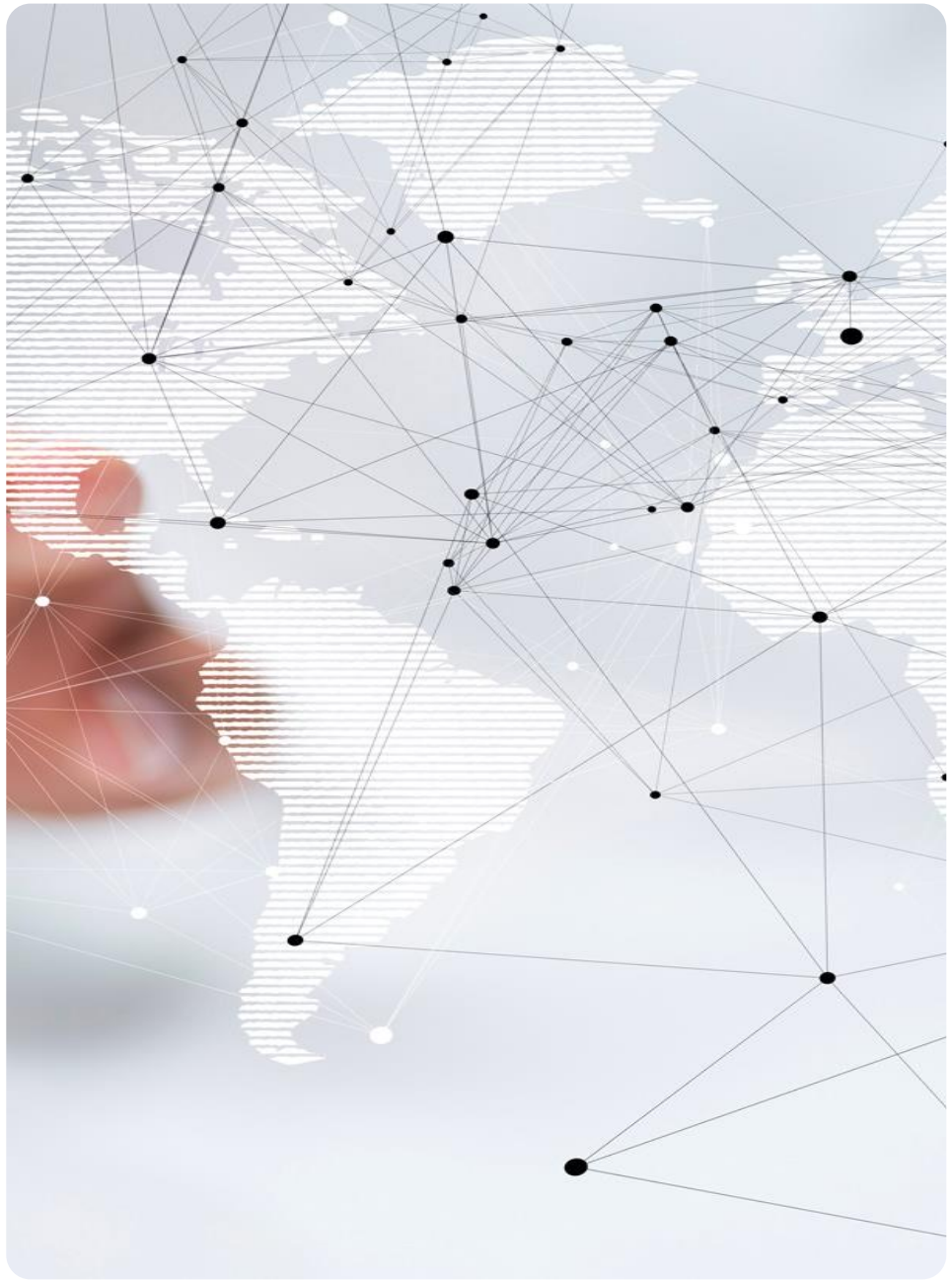
Centre Ressources Régional Cyber

# Le site Web : c2rcsud.org






C2RC
Centre Ressources Régional Cyber



# Questions ?