WEBINAIRE

LIVE
WEBINAR

CYBERSÉCURITÉ & COLLECTIVITÉS : LES ENJEUX & PARTAGE DE BONNES PRATIQUES

16 juin 2026

14h00 - 15h00

Animé par avangarde cyber sécurité

CDG 01

Webinar CDG01 du 16 juin 2026

Agenda

Mot d'introduction par CDG01	Les menaces Cyber	Les enjeux au sein des collectivités	Réglementation	Par où commencer ?	Echange Q&R
1'	5'	10'	10'	10'	10'

Nous vous rappelons

- Coupez vos micros
- Posez vos questions dans le chat

Introduction aux menaces Cyber

La cyber sécurité en 1 chiffre

453 200

Atteintes numériques enregistrées en 2025

(plaintes, signalements relatifs aux escroqueries, aux contenus illicites où aux usages frauduleux)

+ 87% *d'atteintes sur les 5 dernières années*

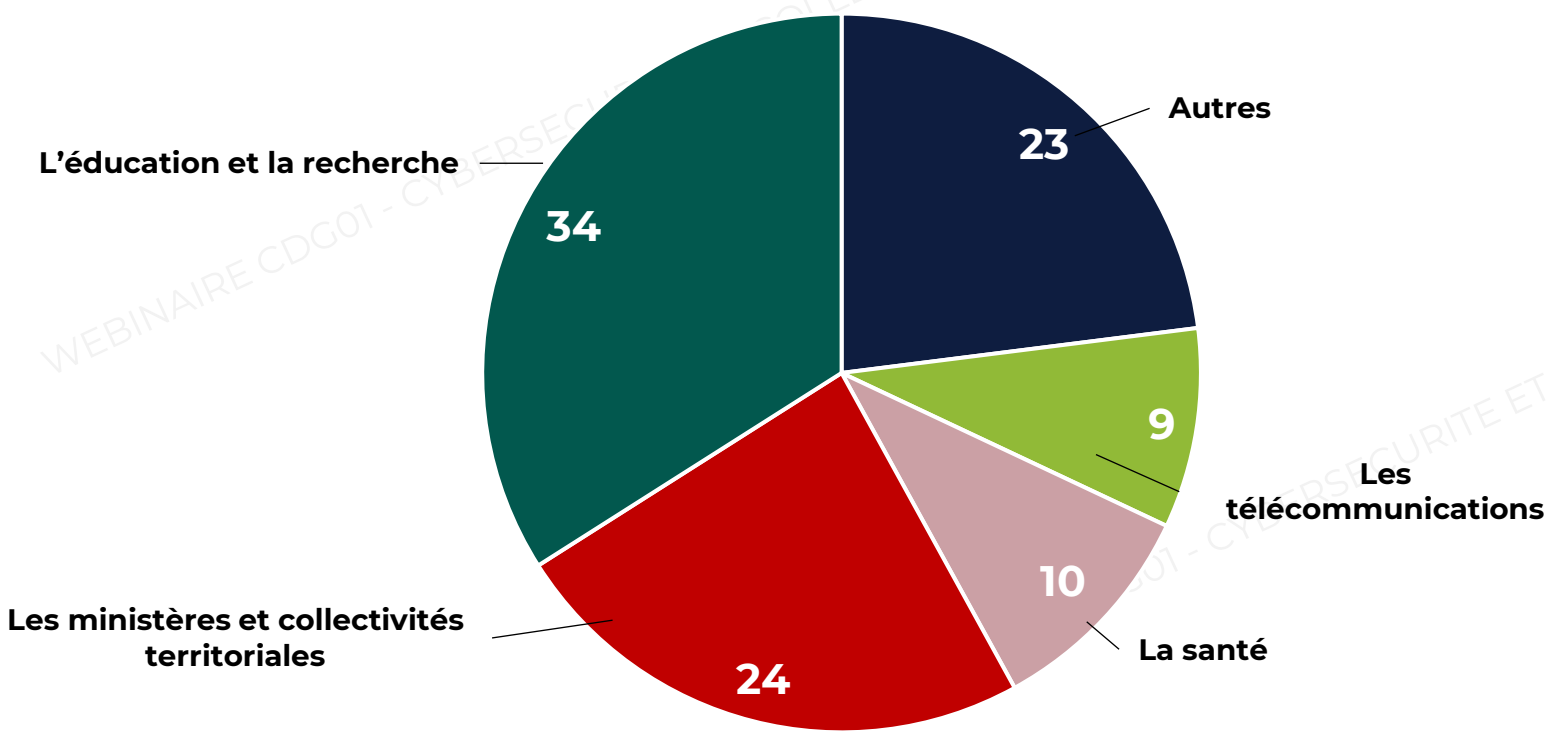
Source : « Rapport Annuel sur la cybercriminalité 2026 » de COMCYBER-MI

Des cyberattaques en hausse continue

1347 revendications et annonce de cyberattaque signalée en 2025

(vol de donnée, hacktivisme, rançongiciel)

(**+27%** par rapport à 2024)



1 / 4

Des cyberattaques ciblent les ministères et collectivités territoriales

Principaux vecteurs d’intrusions observés

Réutilisation d’identifiants compromis

Accès à distance non sécurisés

Achat d’accès initiaux auprès de courtiers spécialisés

Hameçonnage ciblé

Attaques via la chaîne d’approvisionnement

Des menaces de plus en plus industrialisées

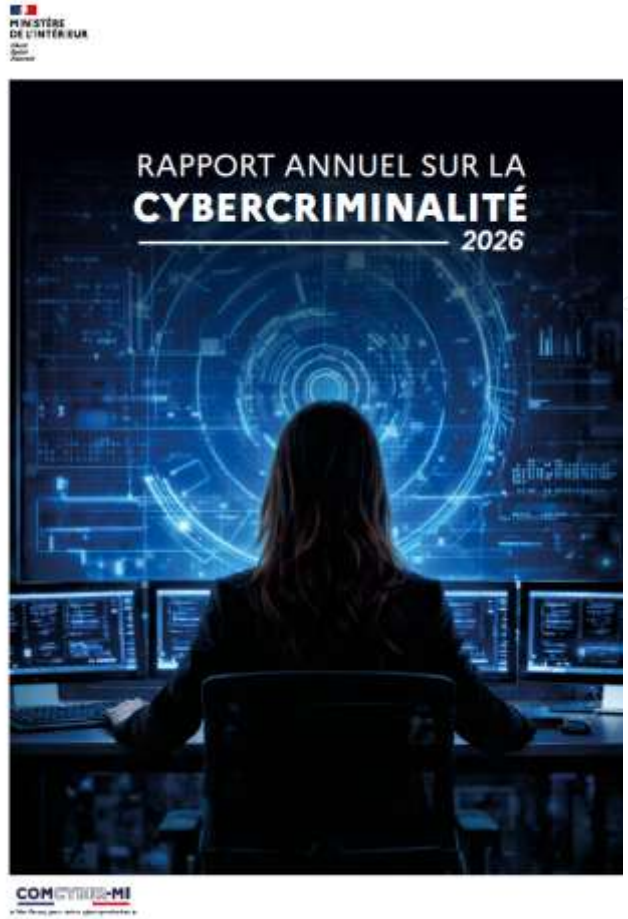
Tendance 2026

AI-as-a-Service

Opérations hameçonnage à grande échelle, *conception de logiciels malveillants, exploitation des vulnérabilités, production de contenu manipulé*

Cybercrime-as-a-Service

*Démocratisation du modèle accessible à des profils moins expérimentés, avec des exigences techniques moins élevées pour passer à l'acte (**développement des infostealers et des courtiers en accès initial**)*



Via des modes opératoires structurés…

1ere PHASE ➡ Préparation / reconnaissance-weaponisation

- *Quelle est l'actualité de l'organisme ? (vie de l'entreprise, marché gagné)*
- *Quelle est l'organisation de l'entreprise ?*
- *Quelles sont leurs situations familiales ? Leurs hobbies ?*
- *A quelle heure font-ils leurs running ? En vacances, ou en déplacement ?*
- *Quels sont les entrées/sorties de l'usine ? A quelle fréquence ?*
- *Etc…*

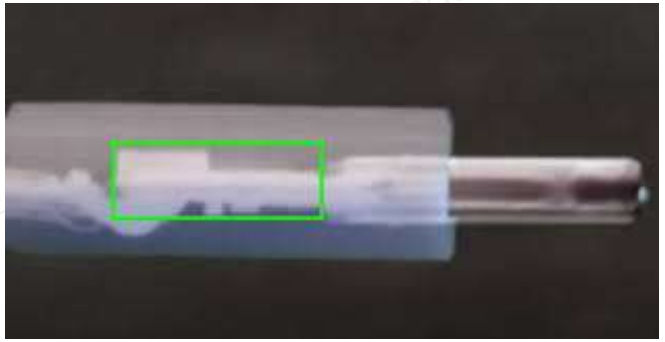
Quelques exemples

Redirection vers un site web malveillant pouvant solliciter des données à caractères personnelles

Quelques exemples

Câble utilisé pour charger la batterie d'un iPhone....

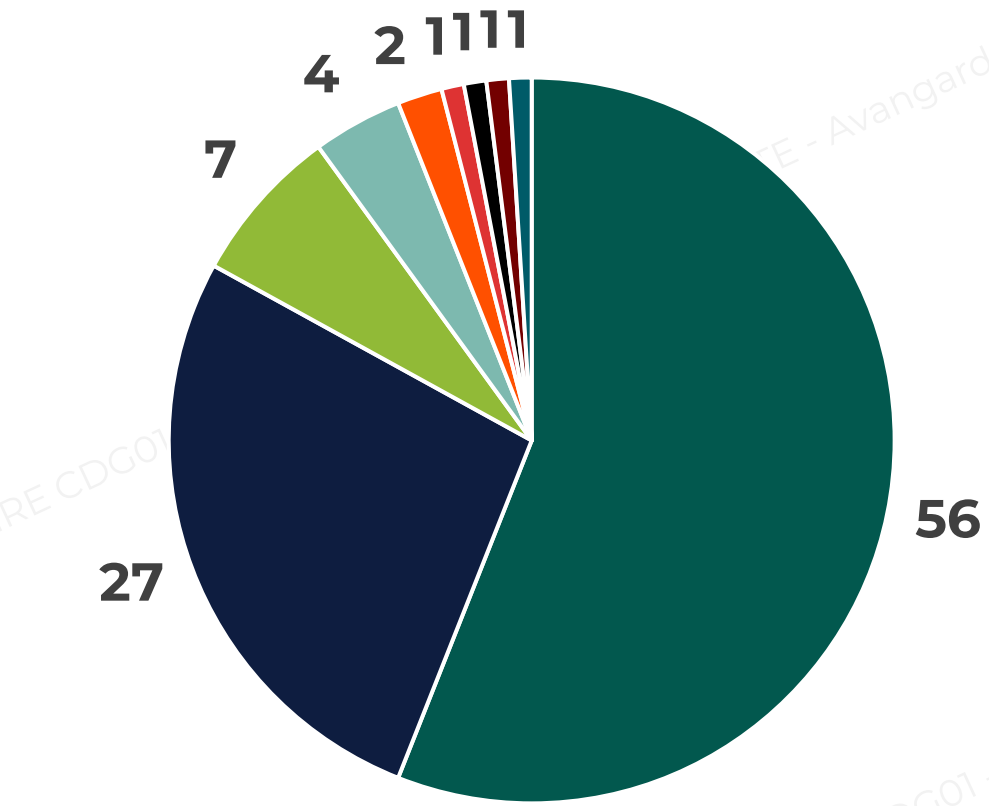
Mais aussi... pour déployer un code malveillant sur un ordinateur



Les enjeux au sein des collectivités

Focus sur l'état de la cybercriminalité dans les collectivités territoriales

Sous-catégories les plus visées par les cybercriminels dans le secteur institutionnel en 2025



1 attaque sur 2

dans le secteur institutionnel vise les collectivités

Exemples de cyberattaques récentes

Mai 2026

#Interruption du service

Méthode : attaque par rançongiciel

Impact : paralysie du SI de la municipalité et blocage des services électroniques.

Avril 2026

#Supply Chain

Méthode : Attaque par rebond depuis prestataire externe

Impact : exposition des comptes utilisateurs des services de billetterie (noms, prénoms, adresses mail et mots de passe).

Nov 2025

#Prestataire mutualisé

Méthode : Exploitation d'une faille de sécurité chez un prestataire commun à 1300 communes française qui réalisait la gestion des démarches administratives.

Impact : Fuite des données sensibles (états civils, passeport, livret de famille, RIB et justificatif de domicile).

Exemples de cyberattaques récentes

Mai 2026

#Fuite de donnée

Méthode : vol d'une base de données

Impact : Fuite des données personnelles des usagés de la médiathèque (date de naissance, ville de résidence, adresse mail, nom prénom et N téléphone).

Mai 2026

 # Fuite de donnée

Méthode : attaque par rebond depuis un prestataire externe gérant le système de billetterie et de réservation en ligne des musées municipaux

Impact : Fuite des données personnelles des usagers et suspension des services de vente en ligne

Juin 2026

#Fuite de donnée

Méthode : vol d'une base de données

Impact : Fuite des données personnelles des 15895 agents (fonction, adresse mail, nom prénom et N téléphone).L'ensemble semble correspondre à un annuaire interne ou professionnel

Les principales menaces ciblant les collectivités

3 principales cyberattaques

Attaque Ddos

Volonté de perturbation du service et de gain médiatique pour l'attaquant

Vol de donnée

Plusieurs cas de vente de données personnelles de millions de Français survenus en 2025 et relayés dans les médias

Rançongiciel

Les attaquants ont tendance à privilégier le vol et la menace de diffusion des données pour forcer les victimes à payer la rançon

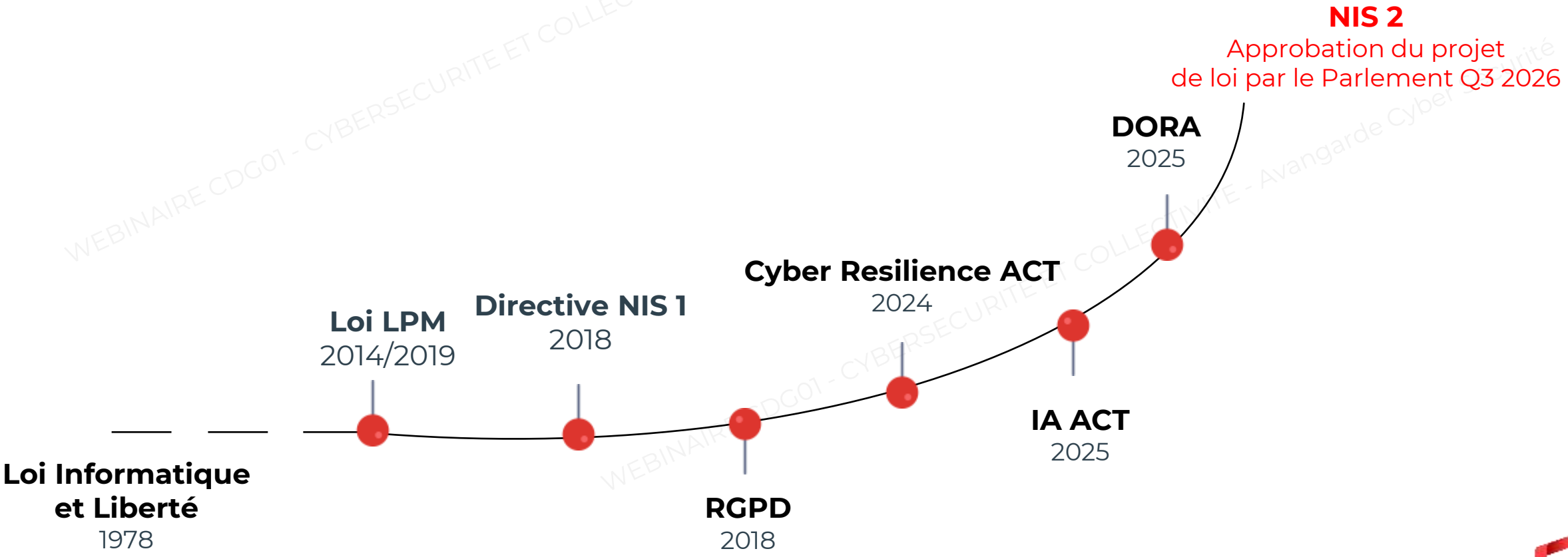
Méthodes d'intrusions en hausse :

- **Par une plateforme numérique mutualisée** tel des prestataires gérant des services essentiels pour plusieurs collectivités.

- **Par la Supply chain** - les prestataires les moins sécurisés de l'écosystème peuvent servir d'accès indirect aux systèmes de la cible finale.

Face à ces menaces…

Une prise de conscience notamment traduite à travers la législation



Règlementations liées à la cyber sécurité

#RGPD

#NIS 2

NIS 2 en quelques mots

Portée (art. 3)
18 secteurs métiers dont 11 nouveaux
Entités essentielles (EE) et importantes (EI)

Obligations
Notification à l'ANSSI

Sanction (art. 34)
en cas de violation des articles 21 ou 23

Gouvernance (art. 20)
Implication forte des organes de direction

Signalement (art. 23)
Obligation de signalement d'incident à l'ANSSI (CERT-FR)

Mesures de gestion de risques (art. 21)
Organisationnelle, techniques et opérationnelles

NIS 2 : quelles sont les exigences ?

Mesures techniques opérationnelles et organisationnelles prévues par la directive NIS 2

GOUVERNANCE	PROTECTION	DEFENSE	RESILIENCE

Le **principe de proportionnalité de NIS 2 s'applique sur les mesures de gestion des risques**.
Pour se défendre contre la menace cybercriminelle :
- 20 objectifs de sécurité (EE)
- 15 objectifs de sécurité (EI)

Les **mesures doivent être proportionnées** aux :
- Degré d'exposition aux risques
- Aux impacts d'un incident

NIS 2 : quelles sont les exigences ?

Gouvernance

- Recensement des SI
- Mise en œuvre d'un cadre de gouvernance de la sécurité numérique
- Maîtrise de l'écosystème (prestataires et fournisseurs informatiques)
- Prise en compte de la sécurité numérique dans la gestion des ressources humaines
- Maitrise des SI
- Mise en œuvre d'une approche par les risques
- Audit de la sécurité des SI

→ Objectifs spécifiques aux entités essentielles (EE)

Défense

- Identification et réaction aux incidents de sécurité
- Supervision de la sécurité des SI

→ Objectifs spécifiques aux entités essentielles (EE)

NIS 2 : quelles sont les exigences ?

Protection

- Maîtrise des accès physiques aux locaux
- Sécurisation de l'architecture des SI
- Sécurisation des accès distants aux SI
- Protection des SI contre les codes malveillants
- Gestion des identités et des accès des utilisateurs aux systèmes
- Maitrise de l'administration des SI
- Sécurisation de la configuration des ressources des SI
- Administration des SI depuis des ressources dédiées

Objectifs spécifiques aux entités essentielles (EE)

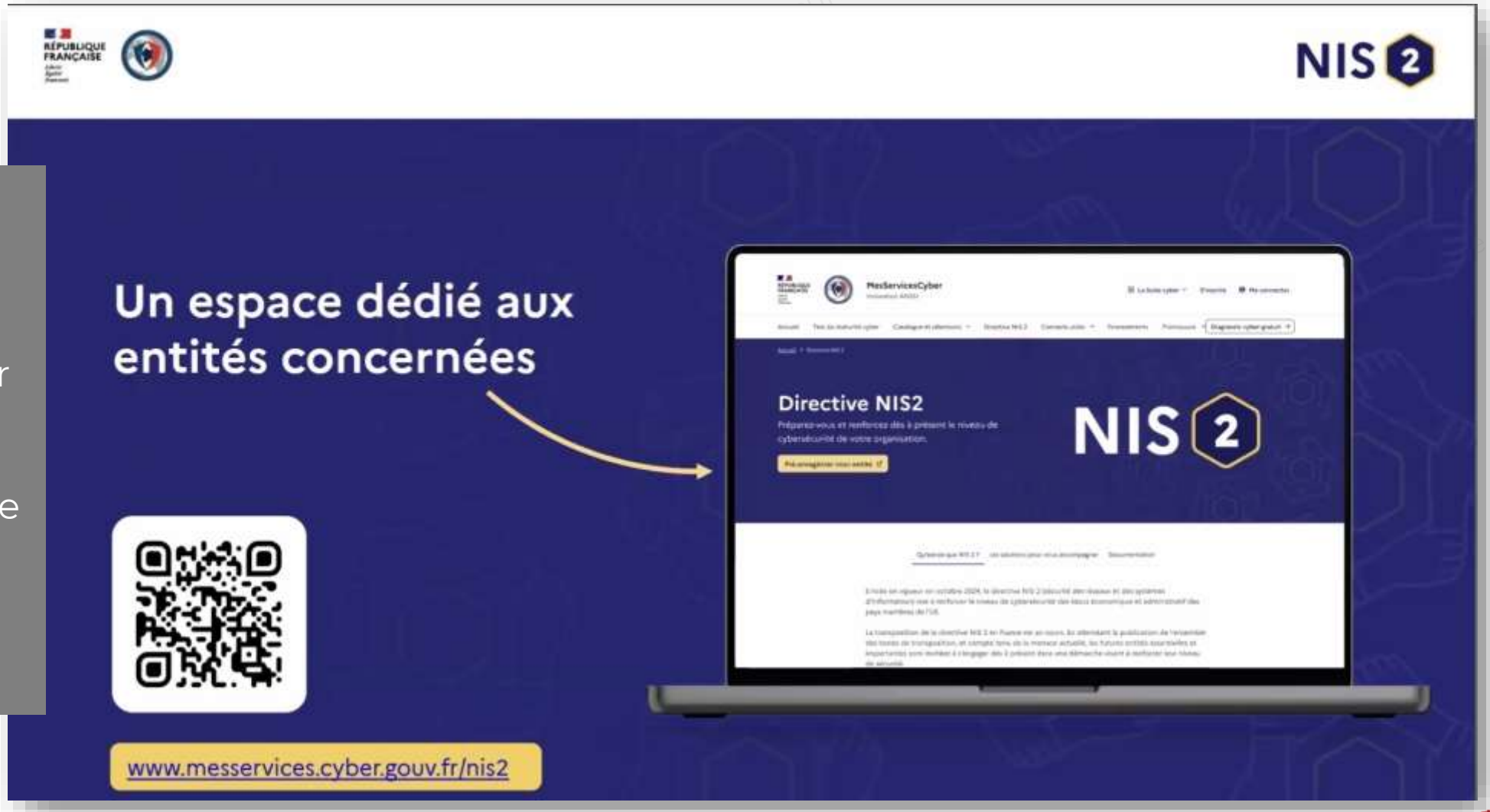
Résilience

- Continuité et reprise d'activité
- Réaction aux crises d'origine cyber
- Exercices, tests et entraînements

NIS 2 : pour en savoir plus ?

[MonEspaceNIS2 - Accueil]

Plateforme pour faciliter l'accès aux services et ressources de l'ANSSI



Ne pas oublier la réglementation RGPD

Traitements de données personnelles

Toute opération, ou ensemble d'opérations, portant sur des données personnelles, **quel que soit le procédé utilisé**

- Collecte
- Organisation
- Conservation
- Transfert
- Suppression
- Consultation
- Modification
- Diffusion

Par où commencer ?

Quelques constats récurrents

Retour d'expérience Prestataires lors de missions d'audit cyber

Sécurisation des postes de travail (i.e. clé USB, obsolescence)

Gestion des accès (i.e. mot de passe)

Sauvegardes

Documentation et gouvernance cyber (qui fait quoi ?)

Sensibilisation (direction, agents)

Supervision cyber sécurité (SOC)

Quelles sont les actions prioritaires à mener ?

Par où commencer ?

PILOTER VOS RISQUES CYBER
&
METTRE EN PLACE UNE GOUVERNANCE

AU SEIN DE VOTRE DIRECTION

01

Connaître son écosystème

Que devons-nous protéger ?
Réaliser un état des lieux
Piloter ses prestataires
Prioriser les actions urgentes

02

Sensibiliser

Impliquer…
- Les agents de la collectivité
- La direction

Par où commencer ?

METTRE EN PLACE
LES MESURES
de
PROTECTION
DEFENSE
RESILIENCE

03

Mettre en œuvre des mesures Urgentes

Quelles mesures prioriser ?

04

Se préparer à la gestion de crise cyber

Comment réagir ?
Inclure le scénario 'cyber' dans son PCS

Quelques exemples de mesures

1. **Séparez strictement vos usages** à caractère personnel de ceux à caractère professionnel
2. **Mettez régulièrement à jour** vos outils numériques
3. Protégez vos accès par une **authentification double-facteur** ou à minima par des MdP robustes
4. **Évitez les réseaux Wi-Fi publics** ou inconnus
5. **Sauvegardez régulièrement** vos données (méthode 3 – 2 – 1 – 0)
6. **Revoir les accès** des utilisateurs et administrateurs
7. **Déployer des EDR** et superviser des alertes

Anticipez vos besoins & modéliser un budget dédié Cyber sécurité

Réagir face à des atteintes numériques

04 72 40 56 56

Cyber Assistance
Auvergne-Rhône-Alpes

Disponible 24H/24 et 7J/7

Pour les collectivités, PME, ETI et associations

Offrir une assistance gratuite aux TPE, PME, ETI, collectivités et associations du territoire confrontées à une menace ou à une cyberattaque.
Cyber Assistance Auvergne-Rhône-Alpes intervient pour **protéger**, **diagnostiquer** et **accompagner** face aux cyberincidents, en coordination avec un réseau d'experts qualifiés.

Risque CYBER SECURITE -> Que retenir ?

INTEGRER RISQUE CYBER DANS L'ORGANISATION

NE PAS HESITER A S'APPUYER SUR EXPERTISE EXTERNE

COMMUNIQUER
SENSIBILISER
....
ANTICIPER

MERCI


WEBINAIRE
LIVE
WEBINAR
CYBERSÉCURITÉ & COLLECTIVITÉS :
LES ENJEUX & PARTAGE DE
BONNES PRATIQUES
16 juin 2026
14h00 - 15h00
Animé par avangarde cyber sécurité
CDG 01

avangarde cyber sécurité

Alois MICHAUD

Consultant senior Cybersécurité

Alois.michaud@avangardecyber.fr

Emmanuel PETIT

Directeur Offres & Services

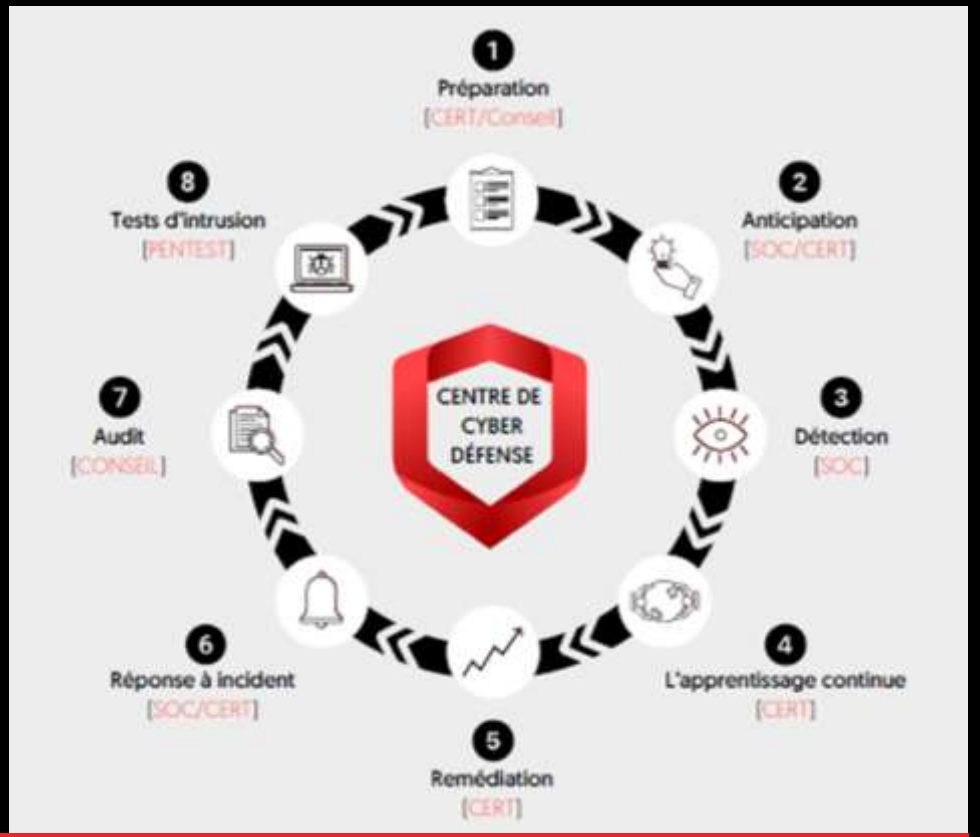
Emmanuel.petit@avangardecyber.fr

avangarde cyber sécurité

Qui sommes nous ?

Une offre Cybersécurité 360°

- Un groupe comprenant **+ de 350** personnes
- **+ de 60** collaborateurs 'cybersécurité'
- **+ de 10 ans** d'existence au sein du groupe Monaco Digital
- Qualifiée PASSI depuis + **de 6 ans** (AMSN) et depuis 2023 (ANSSI)
- **+ de 150** clients
- Une présence en **France** et à Monaco
- Des clients dans **+ de 6** pays



VISA DE SÉCURITÉ

EXPERT CYBER

CLUBEBIOS

Un seul partenaire pour une protection totale.

avangarde cyber sécurité

Qui sommes nous ?

POUR PLUS DE RENSEIGNEMENTS

Titulaire de marché ‘Cyber’ pour la région Auvergne-Rhones-Alpes

Avangarde Cyber Sécurité est titulaire d’un accord-cadre via la centrale d’achat ‘CANUT’ permettant d’apporter son expertise aux services des établissements publics.

Cet accord-cadre donne accès aux bénéficiaires de la centrale d’achat à des prestations de cybersécurité dans les domaines suivants :

- Stratégie, pilotage et exigences règlementaires,
- Pilotage global de la sécurité du système d’information et mise en œuvre d’un SMSSI,
- Prestations techniques (Audits, Tests d’intrusion, Analyses de risques…).

CANUT

Gouvernance et stratégie sécurité *(i.e. analyse risque, conformité réglementaire, pilotage projet etc.)*

Audit des écarts de sécurité *(selon guide d'hygiène de l'ANSSI)*

RSSI mutualisé

Monitorat et assistance technique

Exercice de Crise Cyber

Prestation technique de sécurité *(i.e. audit, pentest)*

avangarde cyber sécurité

Qui sommes nous ?

Avangarde Cyber Sécurité propose des services de supervision sécurité de votre SI

10
EXPERTS SOC

24/7
SURVEILLANCE

+ 900
RÈGLES DE DÉTECTION SEKOIA.IO

+150
RÈGLES DE DÉTECTION MCS

+ 150
TRACKER CTI

Un seul partenaire pour une protection totale.

avangarde cyber sécurité

avangarde cyber sécurité