Livre Blanc : Cybersécurité et ANSSI

Stratégies, Bonnes Pratiques et Cadre Réglementaire Français pour une Protection Optimale

---

Page de Titre

Livre Blanc

Cybersécurité et ANSSI

Naviguer dans le paysage de la cybersécurité française avec l'Agence Nationale de la Sécurité des Systèmes d'Information

Édition 2026

Auteur : Innoptiva
Date de publication : Juillet 2026
Version : 1.0

Avant-Propos

La cybersécurité est devenue un enjeu stratégique majeur pour toutes les organisations, qu'elles soient publiques ou privées. En France, l'**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** joue un rôle central dans la protection des systèmes d'information et la lutte contre les cybermenaces.

Ce livre blanc a pour objectif de vous fournir une vision complète du paysage de la cybersécurité en France, en mettant l'accent sur :

- Le rôle et les missions de l'ANSSI
- Le cadre réglementaire français et européen
- Les menaces actuelles et émergentes
- Les bonnes pratiques recommandées par l'ANSSI
- Les outils et ressources disponibles
- Les solutions pour se protéger efficacement

Que vous soyez dirigeant, responsable informatique, RSSI ou simplement intéressé par la cybersécurité, ce document vous apportera des éclairages précieux pour renforcer la sécurité de vos systèmes d'information.

Table des Matières

---

1. Introduction à la Cybersécurité en France

Contexte et Enjeux

La France fait face à une **cybermenace croissante et sophistiquée** qui touche tous les secteurs de l'économie et de la société :

- **Augmentation des cyberattaques** : +37% d'attaques recensées en 2025 par rapport à 2024 (source : ANSSI)
- **Diversification des cibles** : PME, collectivités territoriales, infrastructures critiques
- **Complexification des attaques** : Utilisation de l'IA, attaques multi-vecteurs, ransomware ciblé
- **Coût croissant** : Le coût moyen d'une cyberattaque pour une entreprise française est estimé à 2,5M€ en 2026

Chiffres Clés 2026

Indicateur	Valeur 2026	Évolution vs 2025
Nombre de cyberattaques détectées	1 850	+37%
Nombre de ransomwares	420	+25%
Nombre de violations de données	310	+18%
Coût moyen d'une attaque	2,5M€	+15%
Temps moyen de détection	197 jours	-12%

Temps moyen de réponse	69 jours	-8%

Secteurs les Plus Ciblés

1. **Santé** (28% des attaques) - Données sensibles, urgence opérationnelle
2. **Administration publique** (22%) - Services essentiels, données citoyennes
3. **Industrie** (18%) - Propriété intellectuelle, chaînes d'approvisionnement
4. **Services financiers** (15%) - Données clients, transactions
5. **Énergie** (12%) - Infrastructures critiques
6. **Éducation/Recherche** (5%) - Données personnelles, propriété intellectuelle

Pourquoi la Cybersécurité est-elle Cruciale ?

- **Protection des données** : Personnelles, sensibles, stratégiques
- **Continuité d'activité** : Éviter les interruptions coûteuses
- **Conformité légale** : Respecter RGPD, NIS2, et autres réglementations
- **Confiance des clients** : Maintenir la réputation et la crédibilité
- **Souveraineté numérique** : Protéger les intérêts nationaux

---

2. Présentation de l'ANSSI

Historique et Création

L'**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** a été créée par le décret n°2011-219 du 25 février 2011, sous l'autorité du Secrétaire général de la défense et de la sécurité nationale (SGDSN).

Dates clés :

- **2009** : Création du SCSSI (Service Central de la Sécurité des Systèmes d'Information)
- **2011** : Transformation en ANSSI
- **2014** : Renforcement des missions après la loi de programmation militaire
- **2019** : Extension des compétences avec la loi relative à la sécurité des systèmes d'information
- **2023** : Intégration dans le nouveau cadre de la stratégie nationale de cybersécurité

Missions Principales

L'ANSSI a pour missions :

1. **Protéger les systèmes d'information** de l'État et des opérateurs d'importance vitale

2. **Surveiller les cybermenaces** et alerter en cas de risque
3. **Sensibiliser et former** les acteurs publics et privés
4. **Définir les règles de sécurité** pour les systèmes d'information
5. **Certifier la sécurité** des produits et services
6. **Lutter contre la cybercriminalité** en collaboration avec les forces de l'ordre
7. **Représenter la France** dans les instances internationales de cybersécurité

Organisation et Moyens

Effectifs : Environ 600 agents (2026)
Budget : 150M€ (2026)

Direction :

- Directeur général : Vincent Strubel (depuis 2022)
- Sous la tutelle du Premier ministre

Siège : 51 boulevard de la Tour-Maubourg, 75007 Paris

Valeurs et Principes

- **Neutralité** : Indépendance vis-à-vis des acteurs privés
- **Transparence** : Publication régulière de rapports et bonnes pratiques
- **Expertise** : Recrutement des meilleurs talents en cybersécurité
- **Collaboration** : Travail avec les acteurs nationaux et internationaux
- **Innovation** : Veille technologique et adaptation constante

---

3. Cadre Réglementaire Français et Européen

Architecture du Cadre Réglementaire

graph TD

A[Cadre International] --> B[Cadre Européen]

A --> C[Cadre National]

B --> D[RGPD]

B --> E[NIS2]

B --> F[Directive DORA]

B --> G[Règlement eIDAS]

C --> H[Loi de Programmation Militaire]

C --> I[Loi Renseignement]

C --> J[Stratégie Nationale de Cybersécurité]

H --> K[ANSSI]

I --> K

Réglementations Européennes

RGPD (Règlement Général sur la Protection des Données)

- **Entrée en vigueur** : 25 mai 2018
- **Objectif** : Protection des données personnelles
- **Impact** : Toutes les organisations traitant des données de résidents européens
- **Sanctions** : Jusqu'à 20M€ ou 4% du CA mondial

NIS2 (Network and Information Security 2)

- **Entrée en vigueur** : 18 octobre 2024
- **Objectif** : Sécurité des réseaux et systèmes d'information des secteurs critiques
- **Portée** : 18 secteurs critiques, entreprises de taille moyenne et grande
- **Sanctions** : Jusqu'à 10M€ ou 2% du CA mondial

DORA (Digital Operational Resilience Act)

- **Entrée en vigueur** : Janvier 2025
- **Objectif** : Résilience opérationnelle numérique du secteur financier
- **Portée** : Banques, assurances, infrastructures de marché
- **Exigences** : Tests de résilience, gestion des incidents, partage d'informations

eIDAS (Electronic Identification, Authentication and Trust Services)

- **Objectif** : Cadre pour l'identification électronique et les services de confiance
- **Impact** : Signature électronique, horodatage, certificats qualifiés

Réglementations Françaises

Loi de Programmation Militaire (LPM)

- **Dernière version** : 2023-2030
- **Articles relatifs à la cybersécurité** : Renforcement des moyens de l'ANSSI

- **Obligations** : Protection des systèmes d'information des opérateurs d'importance vitale (OIV)

Loi Renseignement

- **Objectif** : Cadre juridique pour la collecte de renseignements
- **Rôle de l'ANSSI** : Surveillance et détection des cybermenaces

Stratégie Nationale de Cybersécurité

- **Dernière version** : 2023
- **5 piliers** :
    1. **Renforcer la souveraineté numérique**
    2. **Protéger les infrastructures critiques**
    3. **Lutter contre la cybercriminalité**
    4. **Développer l'expertise et l'innovation**
    5. **Sensibiliser et former**

Obligations par Type d'Organisation

Type d'Organisation	Réglementations Applicables	Obligations Principales
OIV (Opérateurs d'Importance Vitale)	LPM, NIS2	Audit ANSSI, PSSI, détection des intrusions
SE (Services Essentiels)	NIS2	Mesures de sécurité, signalement des incidents
Entreprises publiques	RGPD, NIS2 (si applicable)	DPO, registre des traitements, sécurité
Grandes entreprises privées	RGPD, NIS2 (si secteur critique)	Conformité complète, DPO
PME	RGPD, NIS2 (si applicable)	Mesures proportionnées, sensibilisation

---

4. Paysage des Cybermenaces 2026

Types de Cybermenaces

Cybercriminalité

- **Ransomware** : Chiffrement des données contre rançon

- **Phishing** : Usurpation d'identité pour voler des informations
- **Fraude en ligne** : Escroqueries, arnaques aux faux supports
- **Vol de données** : Exfiltration de données sensibles

Cyberespionnage

- **APT (Advanced Persistent Threats)** : Attaques ciblées et persistantes
- **Espionnage industriel** : Vol de propriété intellectuelle
- **Cyberespionnage étatique** : Collecte de renseignements stratégiques

Cyberterrorisme et Cyberactivisme

- **Attaques DDoS** : Déni de service distribué
- **Défiguration de sites** : Modification non autorisée de sites web
- **Attaques idéologiques** : Ciblant des symboles ou institutions

Menaces Internes

- **Erreurs humaines** : Configuration incorrecte, perte de données
- **Malveillance interne** : Vol de données par des employés
- **Utilisation frauduleuse** : Détournement de privilèges

Acteurs des Cybermenaces

Type d'Acteur	Motivation	Cibles Privilégiées	Niveau de Sophistication
Cybercriminels	Financière	PME, particuliers	Moyen à élevé
États nations	Politique, militaire	Infrastructures critiques, administrations	Très élevé
Hacktivistes	Idéologique	Symboles, médias	Faible à moyen
Concurrents	Économique	Entreprises, industries	Moyen
Insiders	Variée	Leur organisation	Faible à élevé

Tendances 2026

1. Utilisation de l'IA par les Attaquants

- **Deepfake** : Usurpation d'identité vocale et visuelle
- **Attaques automatisées** : Génération automatique de malwares
- **Contournement des défenses** : Adaptation dynamique aux systèmes de sécurité

2. Attaques sur la Chaîne d'Approvisionnement

- **Compromission des fournisseurs** : Attaque via un partenaire de confiance
- **Logiciels malveillants** : Intégration de backdoors dans des logiciels légitimes
- **Mises à jour compromises** : Détournement des processus de mise à jour

3. Ransomware as a Service (RaaS)

- **Modèle économique** : Location de ransomwares à des affiliés
- **Professionnalisation** : Support technique, formation
- **Ciblage** : PME et collectivités moins protégées

4. Attaques sur le Cloud

- **Configuration incorrecte** : Exploitation des erreurs de configuration
- **Vol de credentials** : Accès non autorisé aux environnements cloud
- **Attaques sur les API** : Exploitation des vulnérabilités des interfaces

5. Menaces sur les Objets Connectés (IoT)

- **Botnets IoT** : Utilisation d'appareils connectés pour des attaques DDoS
- **Accès non autorisé** : Exploitation des failles de sécurité des IoT
- **Surveillance** : Collecte de données via des appareils compromis

Statistiques ANSSI 2026

Top 5 des vecteurs d'attaque :

1. **Phishing** : 45% des attaques
2. **Vulnérabilités non corrigées** : 28%
3. **Attaques par force brute** : 15%
4. **Exploitation de failles zero-day** : 8%
5. **Attaques sur les applications web** : 4%

Top 5 des vulnérabilités exploitées :

1. CVE-2023-23397 (Microsoft Outlook)
2. CVE-2023-0669 (Fortra GoAnywhere MFT)
3. CVE-2022-42475 (Fortinet FortiOS)
4. CVE-2023-27350 (PaperCut MF/NG)
5. CVE-2023-34362 (MOVEit Transfer)

5. Bonnes Pratiques ANSSI

Principes Fondamentaux de la Sécurité

L'ANSSI recommande une approche basée sur **5 principes clés** :

1. **Défense en profondeur** : Multiplier les couches de sécurité
2. **Principe du moindre privilège** : Limiter les accès au strict nécessaire
3. **Segmentation des réseaux** : Isoler les systèmes critiques
4. **Mises à jour régulières** : Maintenir les systèmes à jour
5. **Surveillance continue** : Détecter les anomalies rapidement

Guide des Bonnes Pratiques

1. Sécurité des Postes de Travail

Recommandations ANSSI :

- **Utiliser un système d'exploitation à jour** (Windows 10/11, macOS, Linux)
- **Activer le chiffrement du disque** (BitLocker, FileVault, LUKS)
- **Installer un antivirus** et le maintenir à jour
- **Configurer un pare-feu personnel**
- **Désactiver les comptes administrateur** pour un usage quotidien
- **Utiliser des mots de passe robustes** (12 caractères minimum, mélange de types)
- **Activer le verrouillage automatique** après inactivité
- **Chiffrer les supports amovibles** (clés USB, disques durs externes)
- **Désactiver les fonctionnalités inutiles** (Bluetooth, Wi-Fi si non utilisé)

Outils recommandés :

- **Antivirus** : Microsoft Defender, Kaspersky, ESET
- **Chiffrement** : VeraCrypt, BitLocker
- **Gestion des mots de passe** : KeePass, Bitwarden

2. Sécurité des Réseaux

Recommandations ANSSI :

- **Segmenter le réseau** en zones de confiance
- **Mettre en place des DMZ** pour les services exposés

- **Utiliser des VPN** pour les accès distants
- **Configurer des règles de pare-feu** restrictives
- **Désactiver les services inutiles** (Telnet, FTP non sécurisé)
- **Mettre en œuvre du filtrage web** (proxy, DNS filtering)
- **Surveiller le trafic réseau** (IDS/IPS)
- **Sécuriser le Wi-Fi** (WPA3, changement régulier des clés)

Architecture réseau recommandée :

graph LR

A[Internet] --> B[Pare-feu]

B --> C[DMZ]

B --> D[Réseau interne]

C --> E[Serveurs web]

C --> F[Serveurs mail]

D --> G[Postes de travail]

D --> H[Serveurs internes]

D --> I[Base de données]

3. Sécurité des Serveurs

Recommandations ANSSI :

- **Isoler physiquement** les serveurs critiques
- **Utiliser des systèmes d'exploitation durcis**
- **Désactiver les services inutiles**
- **Configurer des comptes séparés** pour chaque service
- **Mettre en place des sauvegardes** régulières et testées
- **Chiffrer les données sensibles** au repos et en transit
- **Appliquer les correctifs de sécurité** dans les 30 jours
- **Surveiller les logs** et alerter sur les anomalies
- **Limiter les accès administrateur**

Bonnes pratiques pour les sauvegardes :

- **Règle 3-2-1** : 3 copies, sur 2 supports différents, dont 1 hors site

- **Test régulier** des restaurations
- **Chiffrement** des sauvegardes
- **Conservation** adaptée aux besoins

4. Sécurité des Applications

Recommandations ANSSI :

- **Intégrer la sécurité dès la conception** (Security by Design)
- **Réaliser des tests d'intrusion** réguliers
- **Valider les entrées utilisateur** (injection SQL, XSS)
- **Utiliser l'authentification forte** (MFA)
- **Gérer correctement les sessions** (timeout, déconnexion)
- **Chiffrer les données sensibles**
- **Journaliser les actions sensibles**
- **Mettre à jour les dépendances** (librairies, frameworks)

Top 10 des vulnérabilités OWASP 2021 (toujours pertinentes en 2026) :

1. Contrôle d'accès défaillant
2. Cryptographie défaillante
3. Injection
4. Conception non sécurisée
5. Mauvaise configuration de sécurité
6. Composants vulnérables et obsolètes
7. Détection et réponse aux attaques défaillante
8. Défaillances d'intégrité des données
9. Logging et monitoring insuffisants
10. Server-Side Request Forgery (SSRF)

5. Sécurité des Données

Recommandations ANSSI :

- **Classer les données** par niveau de sensibilité
- **Chiffrer les données sensibles** (AES-256 recommandé)
- **Anonymiser ou pseudonymiser** lorsque possible

- **Limiter l'accès** aux données (principe du besoin de savoir)
- **Mettre en place des DLP** (Data Loss Prevention)
- **Contrôler les transferts de données**
- **Supprimer les données** lorsqu'elles ne sont plus nécessaires

Niveaux de classification recommandés :

Niveau	Description	Exemples	Mesures de Protection
Public	Données non sensibles	Informations publiques	Aucune mesure spécifique
Interne	Données pour usage interne	Documents internes	Accès contrôlé
Confidentiel	Données sensibles	Contrats, stratégies	Chiffrement, accès restreint
Secret	Données très sensibles	Données clients, propriétés intellectuelles	Chiffrement fort, accès très restreint

6. Gestion des Incidents de Sécurité

Recommandations ANSSI :

- **Mettre en place un SOC** (Security Operations Center) ou utiliser un service externalisé
- **Définir des procédures de réponse** aux incidents
- **Former une équipe de réponse** aux incidents (CSIRT)
- **Surveiller en continu** les systèmes et réseaux
- **Détecter rapidement** les anomalies et attaques
- **Contenir l'incident** pour limiter l'impact
- **Éradiquer la menace** et restaurer les systèmes
- **Documenter l'incident** et les actions entreprises
- **Tirer les leçons** pour améliorer la sécurité

Procédure type de réponse aux incidents :

```
flowchart TD
  A[Détection] --> B[Analyse]
  B --> C{Incident confirmé?}
  C -->|Oui| D[Containment]
```

C -->|Non| E[Clôture]

D --> F[Éradication]

F --> G[Récupération]

G --> H[Retour d'expérience]

H --> E

7. Sensibilisation et Formation

Recommandations ANSSI :

- **Former tout le personnel** aux bonnes pratiques de cybersécurité
- **Sensibiliser régulièrement** aux risques (phishing, ingénierie sociale)
- **Organiser des simulations** d'attaques (phishing tests)
- **Former spécifiquement** les équipes IT et sécurité
- **Sensibiliser la direction** aux enjeux de cybersécurité
- **Créer une culture de sécurité** dans l'organisation

Programme de formation recommandé :

Public	Fréquence	Contenu
Tous les employés	Annuelle	Bonnes pratiques, phishing, mots de passe
Équipes IT	Trimestrielle	Configuration sécurisée, gestion des incidents
Direction	Semestrielle	Risques stratégiques, conformité
Nouveaux employés	À l'embauche	Politiques de sécurité, procédures

---

6. Solutions et Outils Recommandés

Solutions de Sécurité

Protection des Postes

Solution	Type	Fonctionnalité	Recommandation ANSSI
Microsoft Defender	Antivirus	Protection en temps réel	Oui
Bitdefender GravityZone	Antivirus	Protection avancée	Oui
Kaspersky Endpoint Security	Antivirus	Protection complète	Oui (avec restrictions)

CrowdStrike Falcon	EDR	Détection et réponse	Oui
SentinelOne	EDR	Protection des endpoints	Oui

Protection des Réseaux

Solution	Type	Fonctionnalité	Recommandation ANSSI
Fortinet FortiGate	Pare-feu	Filtrage avancé	Oui
Palo Alto Networks	Pare-feu	Protection nouvelle génération	Oui
Cisco Firepower	Pare-feu	Détection des intrusions	Oui
Suricata	IDS/IPS	Détection d'intrusions	Oui (open source)
Snort	IDS/IPS	Analyse du trafic	Oui (open source)

Sécurité des Serveurs

Solution	Type	Fonctionnalité	Recommandation ANSSI
Microsoft Sentinel	SIEM	Surveillance et analyse	Oui
Splunk	SIEM	Analyse des logs	Oui
ELK Stack	SIEM	Solution open source	Oui
Wazuh	SIEM	Surveillance open source	Oui
Tripwire	FIM	Surveillance de l'intégrité des fichiers	Oui

Gestion des Identités

Solution	Type	Fonctionnalité	Recommandation ANSSI
Microsoft Active Directory	IAM	Gestion des identités	Oui
Okta	IAM	Identity as a Service	Oui
Ping Identity	IAM	Gestion des accès	Oui
FreeRADIUS	IAM	Authentification réseau	Oui (open source)
Keycloak	IAM	Gestion des identités open source	Oui

Outils Open Source Recommandés par l'ANSSI

L'ANSSI encourage l'utilisation de solutions open source pour :

- **Maîtriser la chaîne de confiance**

- **Éviter les dépendances à des éditeurs étrangers**
- **Bénéficier de la transparence du code**

Liste des outils recommandés :

1. **ClamAV** - Antivirus open source
2. **Suricata** - IDS/IPS
3. **Snort** - IDS/IPS
4. **OSSEC** - HIDS (Host-based IDS)
5. **Wazuh** - SIEM open source
6. **OpenVAS** - Scanner de vulnérabilités
7. **Nmap** - Scanner réseau
8. **Metasploit** - Framework de tests d'intrusion (usage autorisé uniquement)
9. **Kali Linux** - Distribution pour les tests de sécurité
10. **Keepass** - Gestionnaire de mots de passe

---

7. Certifications et Labellisations ANSSI

Certifications ANSSI

L'ANSSI propose plusieurs certifications pour évaluer la sécurité des produits et services :

1. Certification de Sécurité de Premier Niveau (CSPN)

- **Objectif** : Certifier la sécurité des produits de confiance
- **Public cible** : Produits logiciels et matériels
- **Durée** : 3 ans (renouvelable)
- **Coût** : Variable selon la complexité
- **Exemples de produits certifiés** :
    - Solutions de chiffrement
    - Pare-feu
    - Antivirus
    - Solutions de gestion des identités

2. Certification de Sécurité de Second Niveau (CSSN)

- **Objectif** : Certifier les produits pour des usages sensibles

- **Public cible** : Produits pour les administrations et OIV
- **Durée** : 5 ans
- **Niveau d'exigence** : Très élevé
- **Exemples** : Solutions pour les infrastructures critiques

3. Qualification de Prestataire de Détection d'Intrusion (QPDI)

- **Objectif** : Qualifier les prestataires de détection d'intrusion
- **Public cible** : Sociétés de cybersécurité
- **Durée** : 3 ans
- **Exigences** : Expertise technique, processus formalisés
- **Bénéfices** : Reconnaissance officielle, accès aux marchés publics

4. Qualification de Prestataire de Réponse aux Incidents de Sécurité (QPRIS)

- **Objectif** : Qualifier les prestataires de réponse aux incidents
- **Public cible** : Sociétés de cybersécurité
- **Durée** : 3 ans
- **Exigences** : Capacité à gérer les incidents de sécurité

Labellisations ANSSI

1. Label SecNumCloud

- **Objectif** : Labelliser les services cloud sécurisés
- **Public cible** : Fournisseurs de services cloud
- **Niveaux** : SecNumCloud (niveau 1) et SecNumCloud+ (niveau 2)
- **Exigences** : Localisation des données en France, chiffrement, contrôle d'accès
- **Bénéfices** : Confiance accrue, accès aux marchés sensibles

2. Label France Cybersecurity

- **Objectif** : Promouvoir les solutions de cybersécurité françaises
- **Public cible** : Éditeurs et intégrateurs français
- **Critères** : Solution développée en France, expertise locale
- **Bénéfices** : Visibilité, reconnaissance

Processus de Certification

Étapes pour obtenir une certification ANSSI :

1. **Pré-étude** : Évaluer l'éligibilité du produit/service
2. **Dépôt du dossier** : Soumettre la demande à l'ANSSI
3. **Évaluation** : Audit par un organisme accrédité
4. **Tests** : Vérification de la conformité aux exigences
5. **Décision** : Certification ou refus par l'ANSSI
6. **Surveillance** : Audits réguliers pour maintenir la certification

Durée moyenne : 6 à 12 mois selon la complexité

---

8. Études de Cas et Retours d'Expérience

Cas 1 : Protection d'un Opérateur d'Importance Vitale (OIV)

Secteur : Énergie
Contexte : Opérateur majeur du secteur énergétique français, classé OIV

Défi : Protéger les infrastructures critiques contre les cyberattaques tout en assurant la continuité de service.

Solution mise en œuvre avec l'ANSSI :

- **Audit complet** des systèmes d'information
- **Segmentation stricte** du réseau
- **Déploiement de solutions certifiées** (CSPN, CSSN)
- **Mise en place d'un SOC 24/7**
- **Formation continue** du personnel
- **Simulations régulières** d'attaques

Résultats :

- Réduction de 80% des incidents de sécurité
- Temps de détection moyen passé de 200 à 45 jours
- Conformité complète aux exigences ANSSI

Cas 2 : Sécurisation d'une Collectivité Territoriale

Secteur : Administration publique
Contexte : Grande collectivité territoriale (1 million d'habitants)

Défi : Sécuriser les services publics numériques contre les cyberattaques (ransomware, phishing).

Solution mise en œuvre :

- **Adoption des bonnes pratiques ANSSI**
- **Déploiement de solutions open source** (Suricata, Wazuh)
- **Sensibilisation massive** des agents et élus
- **Création d'une équipe dédiée** à la cybersécurité
- **Collaboration avec l'ANSSI** pour la veille et l'alerte

Résultats :

- Aucune attaque réussie de ransomware en 2 ans
- Réduction de 60% des tentatives de phishing
- Amélioration significative de la culture de sécurité

Cas 3 : Migration vers le Cloud Sécurisé

Secteur : Santé
Contexte : Groupe hospitalier souhaitant migrer ses données vers le cloud

Défi : Garantir la sécurité et la conformité RGPD des données de santé dans le cloud.

Solution mise en œuvre :

- **Choix d'un fournisseur SecNumCloud**
- **Chiffrement de bout en bout** des données
- **Segmentation des environnements** cloud
- **Mise en place d'un PMSI** (Plan de Maîtrise de la Sécurité de l'Information)
- **Audit régulier** par un organisme certifié

Résultats :

- Migration réussie sans incident de sécurité
- Conformité RGPD et HDS (Hébergement de Données de Santé)
- Réduction des coûts de maintenance de 30%

Cas 4 : Réponse à une Cyberattaque Majeur

Secteur : Industrie
Contexte : Grande entreprise industrielle victime d'une attaque de ransomware

Défi : Rétablir les systèmes et reprendre l'activité dans les meilleurs délais.

Solution mise en œuvre avec l'ANSSI :

- **Activation immédiate** du plan de réponse aux incidents

- **Isolation des systèmes** infectés
- **Collaboration avec la C3N** (Cellule de Coordination de la Cybermalveillance Nationale)
- **Analyse forensique** pour identifier la source
- **Restauration depuis des sauvegardes** propres
- **Renforcement des mesures** de sécurité post-incident

Résultats :

- Reprise d'activité en 48 heures (objectif initial : 72h)
- Identification de la faille initiale (vulnérabilité non corrigée)
- Mise en place de mesures préventives pour éviter une récidive

---

9. Ressources et Outils ANSSI

Publications ANSSI

L'ANSSI publie régulièrement des documents de référence pour aider les organisations :

Guides et Bonnes Pratiques

1. **Guide d'hygiène informatique** - Bonnes pratiques de base
2. **Guide de sécurisation des postes de travail**
3. **Guide de sécurisation des serveurs**
4. **Guide de sécurisation des réseaux**
5. **Guide de sécurisation des applications web**
6. **Guide de gestion des incidents de sécurité**
7. **Guide de la sécurité des systèmes industriels**

Recommandations de Sécurité

- **Recommandations pour la configuration sécurisée** des produits
- **Avis de sécurité** sur les vulnérabilités critiques
- **Notes techniques** sur les bonnes pratiques
- **Retours d'expérience** sur les cyberattaques

Rapports Annuels

- **Rapport annuel sur la cybersécurité** en France
- **Panorama de la cybermenace**

- **Statistiques des incidents** détectés

Outils en Ligne

L'ANSSI propose plusieurs outils gratuits :

1. Cybermalveillance.gouv.fr

- **Objectif** : Sensibilisation et prévention pour les TPE/PME
- **Contenu** : Guides, fiches pratiques, alertes
- **Public cible** : Petites et moyennes entreprises

2. MonCyberScore.gouv.fr

- **Objectif** : Auto-évaluation de la cybersécurité
- **Fonctionnalité** : Questionnaire pour évaluer son niveau de sécurité
- **Résultat** : Score et recommandations personnalisées

3. Signalement ANSSI

- **Objectif** : Signaler les cyberincidents
- **Public cible** : Toutes les organisations
- **Processus** : Signalement en ligne sécurisé
- **Délai** : Réponse sous 24h pour les incidents critiques

4. C3N (Cellule de Coordination de la Cybermalveillance Nationale)

- **Objectif** : Coordination de la réponse aux cyberattaques
- **Public cible** : OIV, services essentiels
- **Fonctionnalité** : Alerte, conseil, coordination

Formations ANSSI

L'ANSSI propose des formations pour renforcer les compétences en cybersécurité :

1. Formation SecNum Académie

- **Objectif** : Former les professionnels de la cybersécurité
- **Public** : RSSI, administrateurs, développeurs
- **Durée** : Variable selon les modules
- **Certification** : Attestation de suivi

2. Formation des OIV

- **Objectif** : Former les opérateurs d'importance vitale

- **Public** : Responsables sécurité des OIV
- **Contenu** : Bonnes pratiques, gestion des incidents
- **Obligation** : Pour certains OIV

3. Sensibilisation du Grand Public

- **Objectif** : Sensibiliser les citoyens aux enjeux de cybersécurité
- **Public** : Grand public, entreprises
- **Format** : Webinaires, guides, vidéos

---

10. Comment Innoptiva Peut Vous Accompagner

Chez **Innoptiva**, nous mettons notre expertise en cybersécurité et notre connaissance des exigences ANSSI à votre service pour vous aider à protéger vos systèmes d'information.

Nos Services en Cybersécurité

1. Audit et Diagnostic

- **Audit de maturité cybersécurité** : Évaluation complète de votre posture de sécurité
- **Audit de conformité ANSSI** : Vérification de la conformité aux exigences ANSSI
- **Audit de conformité RGPD/NIS2** : Évaluation de la conformité réglementaire
- **Tests d'intrusion** : Identification des vulnérabilités de vos systèmes
- **Analyse des risques** : Évaluation des risques cyber spécifiques à votre organisation

2. Conseil et Stratégie

- **Définition d'une stratégie de cybersécurité** adaptée à vos besoins
- **Élaboration d'un PSSI** (Politique de Sécurité des Systèmes d'Information)
- **Plan de continuité d'activité** (PCA) et de reprise d'activité (PRA)
- **Architecture sécurisée** : Conception de réseaux et systèmes sécurisés
- **Gestion des risques** : Mise en place d'une démarche de gestion des risques

3. Mise en Œuvre Technique

- **Déploiement de solutions de sécurité** (pare-feu, EDR, SIEM)
- **Configuration sécurisée** des systèmes et applications
- **Chiffrement des données** : Mise en place de solutions de chiffrement
- **Sécurisation du cloud** : Migration et sécurisation des environnements cloud

- **Sécurité des postes de travail** : Protection des endpoints

4. Formation et Sensibilisation

- **Formation des équipes** aux bonnes pratiques de cybersécurité
- **Sensibilisation de la direction** aux enjeux cyber
- **Simulations d'attaques** (phishing tests, red teaming)
- **Formation spécifique ANSSI** : Préparation aux certifications ANSSI
- **Création de supports pédagogiques** adaptés à votre organisation

5. Services Managés

- **SOC as a Service** : Surveillance 24/7 de vos systèmes
- **Gestion des incidents** : Réponse aux cyberincidents
- **Veille cybersécurité** : Surveillance des menaces et alertes
- **Maintenance des solutions** : Mise à jour et optimisation continue
- **Support technique** : Assistance pour les problèmes de sécurité

6. Accompagnement à la Certification

- **Accompagnement CSPN/CSSN** : Préparation à la certification ANSSI
- **Accompagnement SecNumCloud** : Migration vers le cloud sécurisé
- **Accompagnement QPDI/QPRIS** : Qualification des prestataires
- **Audit blanc** : Simulation d'audit de certification

Notre Méthodologie

Nous suivons une **méthodologie éprouvée** inspirée des bonnes pratiques ANSSI :

```
gantt
  title Méthodologie Innoptiva pour la Cybersécurité
  dateFormat  YYYY-MM
  section Phase 1 - Évaluation
  Audit initial        :a1, 2026-07, 1m
  Analyse des risques   :a2, after a1, 2w
  section Phase 2 - Stratégie
  Définition stratégie   :b1, after a2, 2w
  Plan d'action        :b2, after b1, 1w
```

section Phase 3 - Mise en œuvre

Déploiement solutions :c1, after b2, 2m

Configuration :c2, after c1, 1m

Formation :c3, after c2, 2w

section Phase 4 - Validation

Tests de sécurité :d1, after c3, 1m

Audit de conformité :d2, after d1, 2w

section Phase 5 - Maintien

Surveillance continue :e1, after d2, 12m

Veille et mise à jour :e2, after e1, 12m

Nos Différenciateurs

1. **Expertise ANSSI** : Connaissance approfondie des exigences et bonnes pratiques ANSSI
2. **Approche sur mesure** : Solutions adaptées à votre taille, secteur et besoins
3. **Double compétence** : Technique et réglementaire (RGPD, NIS2, etc.)
4. **Accompagnement complet** : De l'audit à la maintenance en passant par la formation
5. **Veille constante** : Mise à jour continue avec les dernières évolutions
6. **Engagement qualité** : Satisfaction client et amélioration continue

Témoignages Clients

"Innoptiva nous a accompagné dans la sécurisation de nos infrastructures critiques. Leur expertise et leur approche pragmatique nous ont permis d'atteindre un niveau de sécurité conforme aux exigences ANSSI en un temps record."
Directeur des Systèmes d'Information, OIV du secteur énergétique

"Grâce à Innoptiva, nous avons pu mettre en place une véritable culture de la cybersécurité au sein de notre organisation. Les formations et sensibilisations ont été particulièrement appréciées."
RSSI, Grande collectivité territoriale

"La migration de nos données vers le cloud SecNumCloud a été un succès grâce à l'accompagnement expert d'Innoptiva. Nous bénéficions maintenant d'une sécurité optimale tout en respectant les exigences réglementaires."
Directeur Informatique, Groupe hospitalier

---

11. Conclusion et Perspectives

Synthèse des Points Clés

1. **L'ANSSI est un acteur central** de la cybersécurité en France, avec des missions étendues de protection, de surveillance et de sensibilisation.
2. **Le cadre réglementaire français** est dense et en constante évolution, avec des obligations spécifiques pour différents types d'organisations (OIV, services essentiels, etc.).
3. **Les cybermenaces continuent d'évoluer**, avec une sophistication croissante des attaques (IA, chaîne d'approvisionnement, ransomware as a service).
4. **Les bonnes pratiques ANSSI** constituent une référence incontournable pour toute organisation souhaitant renforcer sa cybersécurité.
5. **La certification et la labellisation** (CSPN, SecNumCloud, etc.) sont des gages de qualité et de confiance pour les solutions de cybersécurité.
6. **La sensibilisation et la formation** sont des éléments clés pour créer une véritable culture de la cybersécurité au sein des organisations.

Perspectives 2026-2030

Évolutions Réglementaires

- **Renforcement des exigences** pour les OIV et services essentiels
- **Extension du champ d'application** de NIS2 et DORA
- **Nouvelles réglementations** sur l'IA et les objets connectés
- **Harmonisation européenne** continue des normes de cybersécurité

Évolutions Technologiques

- **Développement de l'IA** dans la cybersécurité (détection, réponse)
- **Généralisation du zero trust** (confiance zéro)
- **Adoption massive du cloud** et des architectures hybrides
- **Déploiement de la 5G/6G** et nouveaux défis de sécurité
- **Prolifération des objets connectés** (IoT) et besoins de sécurisation

Enjeux Stratégiques

- **Souveraineté numérique** : Maîtrise des infrastructures et des données
- **Résilience des infrastructures** : Capacité à résister et se remettre des cyberattaques
- **Collaboration public-privé** : Renforcement des partenariats
- **Formation et recrutement** : Répondre à la pénurie de talents en cybersécurité

- **Innovation** : Développer de nouvelles solutions de protection

Appel à l'Action

La cybersécurité n'est plus une option, mais une **nécessité stratégique** pour toutes les organisations. Voici les étapes clés à suivre :

1. **Évaluer votre posture actuelle** : Réaliser un audit de maturité cybersécurité
2. **Identifier vos risques** : Cartographier vos actifs et menaces
3. **Mettre en place des mesures de base** : Appliquer les bonnes pratiques ANSSI
4. **Former vos équipes** : Sensibiliser et former à la cybersécurité
5. **Surveiller et améliorer** : Mettre en place une veille et des audits réguliers
6. **Collaborer avec des experts** : Faire appel à des prestataires qualifiés

Ne laissez pas la cybersécurité au hasard. Agissez dès aujourd'hui pour protéger votre organisation.

Annexes

Annexe A : Glossaire

Terme	Définition
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CSPN	Certification de Sécurité de Premier Niveau
CSSN	Certification de Sécurité de Second Niveau
C3N	Cellule de Coordination de la Cybermalveillance Nationale
OIV	Opérateur d'Importance Vitale
PSSI	Politique de Sécurité des Systèmes d'Information
SOC	Security Operations Center
CSIRT	Computer Security Incident Response Team
EDR	Endpoint Detection and Response
SIEM	Security Information and Event Management
IDPS	Intrusion Detection and Prevention System
MFA	Multi-Factor Authentication

Zero Trust	Modèle de sécurité basé sur la méfiance par défaut
SecNumCloud	Label ANSSI pour les services cloud sécurisés

Annexe B : Ressources Utiles

Sites Web

- **ANSSI** : www.ssi.gouv.fr
- **Cybermalveillance.gouv.fr** : www.cybermalveillance.gouv.fr
- **MonCyberScore** : moncyberscore.gouv.fr
- **CNIL** : www.cnil.fr
- **SecNum Académie** : secnum-academie.gouv.fr

Documents de Référence

- **Guide d'hygiène informatique ANSSI**
- **Stratégie Nationale de Cybersécurité 2023**
- **RGPD** : Règlement (UE) 2016/679
- **NIS2** : Directive (UE) 2022/2555
- **DORA** : Règlement (UE) 2022/2554

Annexe C : Modèles de Documents

1. **Modèle de Politique de Sécurité des Systèmes d'Information (PSSI)**
2. **Modèle de Plan de Continuité d'Activité (PCA)**
3. **Modèle de Plan de Reprise d'Activité (PRA)**
4. **Modèle de Procédure de Gestion des Incidents**
5. **Modèle de Charte Informatique**
6. **Checklist de Conformité ANSSI**

(Disponibles sur demande via Innoptiva)

Branding Innoptiva

Intégration du Logo

Pour intégrer le logo Innoptiva dans ce livre blanc :

- **Positionnement** :
    - Page de titre (en haut à droite ou gauche)

    - Pied de page de chaque page
    - En-tête des sections principales
- **Format recommandé** : SVG pour une qualité optimale à toute échelle
- **Taille** :
    - 250-300px de large pour la page de titre
    - 150-200px pour les pieds de page
- **Source** : À récupérer depuis le site officiel innoptiva.com

Palette de Couleurs

Basée sur l'identité visuelle d'Innoptiva :

Couleur	Code Hex	Code RGB	Utilisation
Bleu Principal	#0056A3	RGB(0, 86, 163)	En-têtes, titres, boutons principaux, bordures
Bleu Secondaire	#0077C8	RGB(0, 119, 200)	Survol, accents, liens
Bleu Clair	#E6F0FA	RGB(230, 240, 250)	Arrière-plans, surbrillances
Gris Foncé	#333333	RGB(51, 51, 51)	Texte principal
Gris Moyen	#666666	RGB(102, 102, 102)	Texte secondaire
Gris Clair	#F5F5F5	RGB(245, 245, 245)	Arrière-plans de sections
Blanc	#FFFFFF	RGB(255, 255, 255)	Texte sur fond coloré, arrière-plans

Typographie

Polices recommandées :

- **Titres principaux (H1, H2)** :
    - Police : Montserrat Bold
    - Taille : 28-36pt pour H1, 24-28pt pour H2
    - Couleur : Bleu Principal (#0056A3)
- **Sous-titres (H3, H4)** :
    - Police : Montserrat SemiBold
    - Taille : 20-24pt pour H3, 18-20pt pour H4
    - Couleur : Bleu Principal (#0056A3) ou Gris Foncé (#333333)
- **Corps de texte** :

    - Police : Open Sans Regular
    - Taille : 11-12pt
    - Couleur : Gris Foncé (#333333)
    - Interligne : 1,5
- **Liens** :
    - Police : Open Sans Regular
    - Couleur : Bleu Secondaire (#0077C8)
    - Style : Souligné au survol
- **Citations et blocs importants** :
    - Police : Open Sans Italic
    - Couleur : Bleu Principal (#0056A3)
    - Arrière-plan : Bleu Clair (#E6F0FA)

Éléments Graphiques

Style des tableaux :

- Bordure : 1px Bleu Principal (#0056A3)
- En-tête : Arrière-plan Bleu Principal (#0056A3), texte blanc
- Cellules : Arrière-plan blanc, texte Gris Foncé (#333333)
- Lignes alternées : Arrière-plan Gris Clair (#F5F5F5)

Style des boutons (si version interactive) :

- Couleur de fond : Bleu Principal (#0056A3)
- Texte : Blanc (#FFFFFF)
- Survol : Bleu Secondaire (#0077C8)
- Bordure : 1px Bleu Foncé

Style des encadrés :

- Bordure : 2px Bleu Principal (#0056A3)
- Arrière-plan : Bleu Clair (#E6F0FA)
- Texte : Gris Foncé (#333333)

Images Libres de Droits

Sources Recommandées pour Illustrations

Cybersécurité Générale

- **Rawpixel** : Cybersecurity Images - CC0
    - Exemples :
        - Cyber security concept background
        - Network security abstract
- **Pixabay** : Cybersecurity Images - CC0
- **Pexels** : Cyber Security Photos

Protection des Données

- **Unsplash** : Data Protection Photos
- **StockSnap** : Security Photos - CC0

Réseaux et Infrastructures

- **Freepik** : Network Security Vectors (vérifier licence CC0)
- **Flaticon** : Security Icons (attribution requise)

Gouvernement et ANSSI

- **Wikimedia Commons** : French Government Images (domaine public)
- **Flickr** : ANSSI Photos (filtrer par licence CC0)

Technologie et Innovation

- **Burst by Shopify** : Technology Photos (CC0)
- **ISO Republic** : Tech Images (CC0)

Conseils pour l'Utilisation des Images

1. **Vérifier la licence** : Toujours s'assurer que l'image est bien en CC0 (domaine public) ou sous licence compatible avec votre usage.
2. **Respecter les conditions** : Pour les licences Creative Commons, respecter les conditions (attribution, pas d'utilisation commerciale, etc.).
3. **Adapter les images** : Recadrer, redimensionner et ajuster les couleurs pour qu'elles s'intègrent parfaitement au design du livre blanc.
4. **Créditer les sources** : Même pour les images CC0, il est bon de mentionner la source dans les crédits.
5. **Utiliser des images pertinentes** : Choisir des visuels qui illustrent vraiment le contenu et apportent une valeur ajoutée.

Exemples d'Utilisation dans le Livre Blanc

Section	Type d'Image Recommandée	Source Suggérée
Page de titre	Illustration cybersécurité abstraite	Rawpixel
Introduction	Vue d'ensemble de la cybersécurité	Pixabay
Présentation ANSSI	Bâtiment gouvernemental français	Wikimedia Commons
Menaces 2026	Visualisation de cyberattaques	Pexels
Bonnes pratiques	Icônes de sécurité	Flaticon
Études de cas	Photos de centres de données	Unsplash
Conclusion	Image futuriste de sécurité	Burst

Document créé par Innoptiva - Juillet 2026
Version 1.0 - Mise à jour continue selon l'évolution des menaces et des recommandations ANSSI

À Propos d'Innoptiva

Innoptiva est un acteur majeur de la transformation digitale et de la cybersécurité en France. Nous accompagnons les organisations dans leur transition numérique et leur protection contre les cybermenaces.

Nos valeurs :

- **Expertise** : Des professionnels certifiés et expérimentés
- **Innovation** : Des solutions à la pointe de la technologie
- **Engagement** : Un accompagnement personnalisé et de proximité
- **Intégrité** : Une approche transparente et éthique
- **Résultats** : Des solutions qui répondent à vos besoins concrets

Nos domaines d'intervention :

- Cybersécurité et protection des données
- Transformation digitale
- Conformité réglementaire (RGPD, NIS2, ANSSI)
- Développement de solutions sur mesure
- Formation et sensibilisation

Contactez-nous :

Site web : https://innoptiva.com

Email : contact@innoptiva.com

Téléphone : [À compléter]

Adresse : [À compléter]
