



**DEEP INFOSEC / GUIDE PUBLIC**

# Deep InfoSec — Groupe et expertises

Présentation des prestations de cybersécurité, produits propriétaires, audits, programmes industriels et infrastructures souveraines.

Ingénierie, sécurité et capacité opérationnelle réunies autour du résultat recherché par votre organisation.

[deepinfosec.com](https://deepinfosec.com) • [sales.general@deepinfosec.com](mailto:sales.general@deepinfosec.com)

# Ce que cela apporte à votre organisation

Découvrez l'ensemble de nos métiers, notre méthode de réalisation et les formes de collaboration possibles.

## Conseil en cybersécurité

Une mission de conseil en cybersécurité doit produire un système qui fonctionne, pas seulement un score de maturité. Nos architectes étudient ensemble identités, réseaux, cloud, logiciels, fournisseurs et responsabilités d'exploitation. Ils aident les équipes à choisir les priorités, réaliser les changements, documenter le modèle de fonctionnement et arbitrer les risques résiduels.

## DeepShield

Une équipe de sécurité doit savoir ce que fait un équipement sur son réseau et pourquoi une intervention est proposée. DeepShield associe observation des flux, détection de comportements d'attaque, réponses encadrées par les politiques et chronologies d'événements. Nous commençons par les actifs à protéger, les chemins réseau, les limites d'intervention et les responsabilités d'escalade, afin d'articuler protection et continuité.

## Deep Advisor

Deep Advisor relie les constats provenant des scanners, des identités, du cloud et des terminaux pour révéler les chemins d'attaque exploitables. Plutôt que de traiter toutes les alertes comme urgentes, les équipes voient quels enchaînements menacent les services essentiels, quels contrôles rompent ces chemins et quelles corrections ont le plus d'effet. Les rapports associent constats, responsables, décisions et preuves.

## Énergie et minerais

Un programme énergétique n'a de valeur que si la mesure améliore le fonctionnement réel du réseau. Nous relions comptage, qualité de l'énergie, santé des équipements, maintenance et décisions d'investissement dans une architecture exploitable. Le diagnostic repère les angles morts, le pilote éprouve l'instrumentation et les tableaux de bord, puis l'extension suit les résultats observés et la capacité des équipes à maintenir l'ensemble.

## Centres de données managés

Un service de datacenter managé doit rester fiable lorsque les applications évoluent, que les liaisons tombent ou que les équipes changent. Nous concevons hébergement, segmentation, accès, sauvegardes, reprise et reporting selon la criticité des charges. Les services reposent sur des infrastructures certifiées ISO dans la portée de leurs opérateurs, avec résidence des données, maîtrise client et réversibilité intégrées.

# Travaux et livrables

## Conseil en cybersécurité

Conseil, experts intégrés, chantier de remédiation ou programme managé ; intégration de Deep Advisor ou DeepShield selon les besoins.

- Conseil RSSI et stratégie : modèle opérationnel, gouvernance, tableaux de bord, budget, politiques et programme de réduction du risque.
- Cloud, identités et DevSecOps : revues d'architecture, rapprochement IAM/SCIM, comptes privilégiés, Kubernetes, chaînes CI/CD, applications et API.

Vous recevez : Diagnostic de maturité et exposition par service métier

## DeepShield

Boîtier, capteur et intégration réseau ; observation, action contrôlée et orchestration selon le matériel et le périmètre autorisés.

- Observation réseau : collecte autorisée des flux, DNS et journaux sur les liens retenus, corrélation des activités suspectes et chronologie des événements.
- Détection : signatures, réputation, règles et analyse comportementale pour les tentatives d'hameçonnage, communications malveillantes, sorties anormales et objets connectés.

Vous recevez : Cartographie des actifs et des points d'intégration réseau

## Deep Advisor

Plateforme logicielle et expertise risque ; connecteurs, hébergement, résidence et droits d'automatisation sont définis pour la mission. L'IA assiste sans se substituer aux approbations humaines.

- Centralisation des preuves : connexion autorisée aux scanners, environnements cloud, Kubernetes, identités, CI/CD et incidents, sans remplacer les outils existants.
- Analyse des chemins d'attaque : liaison entre expositions, enchaînements exploitables, contrôles compensatoires et services métier critiques, avec séparation des faits et hypothèses.

Vous recevez : Matrice des sources, intégrations et couverture

# Une mission concrète, du cadrage à la remise

## 01 Cadrer la décision

Nous convenons du changement recherché, des systèmes concernés, de l'existant et des critères de réussite.

## 02 Évaluer sur le bon périmètre

Un diagnostic ou un pilote délimité fournit les informations nécessaires au choix d'une architecture réaliste et de ses critères de réception.

## 03 Réaliser et documenter

L'équipe remet les architectures, contrôles ou services convenus, les résultats des essais et les responsabilités d'exploitation.

## 04 Transmettre la capacité

Documentation, transfert de compétences, maintenance et suivi permettent au programme de durer.

## Échangez avec nos spécialistes

Découvrez les offres sur [deepinfosec.com](https://deepinfosec.com) et choisissez l'expertise correspondant à votre projet. Les brochures publiques sont accessibles librement ; les dossiers techniques et contractuels confidentiels disposent de leur propre circuit sécurisé.

[deepinfosec.com](https://deepinfosec.com) · [sales.general@deepinfosec.com](mailto:sales.general@deepinfosec.com)