

DEEP INFOSEC / GUIDE PUBLIC

Infrastructures souveraines et connectées

Datacenters sécurisés, sites connectés, continuité des services essentiels et maîtrise opérationnelle locale.

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

deepinfosec.com • sales.general@deepinfosec.com

Ce que cela apporte à votre organisation

Comprenez comment réunir architecture, connectivité, sauvegardes, contrôle des accès et maintenance.

Solutions numériques souveraines

La souveraineté numérique prend son sens lorsque l'organisation maîtrise ses données, ses dépendances et ses choix. Nous concevons les architectures autour de la résidence des informations, des clés contrôlées par le client, de l'interopérabilité, des accès privilégiés et de la reprise. L'objectif est une indépendance pratique : pouvoir exploiter, enquêter, migrer et améliorer les systèmes critiques en connaissance de cause.

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.

IoT et systèmes connectés

Un objet connecté appartient à une chaîne opérationnelle, ce n'est pas un capteur isolé. Nous concevons identité de l'équipement, communication sécurisée, traitement edge, cycle de vie du firmware, intégration et maintenance autour de l'usage réel. Pour un campus, une flotte ou un réseau public, le client doit disposer de données utiles et d'un parc maintenable plusieurs années après l'installation.

Sécurité industrielle OT

La cybersécurité industrielle ne doit pas interrompre le procédé qu'elle protège. Nous cartographions les actifs sensibles, les fenêtres de maintenance, les dépendances des réseaux de commande et les conditions de reprise avant toute recommandation de segmentation ou de supervision. Le dossier d'ingénierie fournit aux équipes d'exploitation et de sécurité un plan commun, adapté au site et vérifiable.

Travaux et livrables

Solutions numériques souveraines

Conception, numérisation contrôlée, ingénierie et exploitation managée ; éléments propriétaires et interfaces exportables sont identifiés.

- Architecture souveraine : maîtrise des données, identités, chiffrement, conservation des clés, juridictions et déploiement pour institutions et opérateurs régulés.
- Numérisation sécurisée : capture, métadonnées, indexation, préservation et accès contrôlé pour archives historiques, dossiers et recherche.

Vous recevez : Matrice de souveraineté et de circulation des données

Centres de données managés

Hébergement managé, cloud hybride ou assistance conception/réalisation ; sites, portées de certification et engagements de disponibilité sont définis contractuellement.

- Architecture d’hébergement souverain : sites, calcul, réseaux, stockage, identités et chiffrement selon les juridictions et exigences de résidence.
- Infrastructure managée : déploiement et exploitation des environnements virtualisés, hybrides ou privés sur des infrastructures certifiées ISO dans le périmètre contractuel.

Vous recevez : Architecture d’hébergement, résidence et partage de responsabilités

IoT et systèmes connectés

Revue de conception, ingénierie d’intégration ou opérations de flotte ; les protocoles et matériels partenaires sont examinés selon le projet.

- Sécurité des objets : modèles de menace, démarrage sûr, stratégie de mise à jour des firmwares, identité des équipements, clés et protection du cycle de vie.
- Edge et communications : passerelles, segmentation, protocoles sûrs, secours local et résilience lors des pertes de liaison cloud.

Vous recevez : Modèle de menace et matrice de sécurité par équipement

Sécurité industrielle OT

Diagnostic, conception puis mise en œuvre sous autorité de l’exploitant ; principes IEC 62443 lorsque pertinents au site.

- Découverte industrielle : inventaire automate, IHM, historien, SCADA, stations d’ingénierie et accès distants par des méthodes passives ou autorisées.
- Architecture en zones : segmentation inspirée de Purdue, conduits, passerelles, accès maintenance et supervision, sans plaquer les règles bureautiques sur l’usine.

Vous recevez : Inventaire des équipements ICS/OT et des échanges par zone

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 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 · sales.general@deepinfosec.com