

DEEP INFOSEC / GUIDE PUBLIC

Audits, tests d’intrusion et assurance cybersécurité

Guide des tests autorisés, audits réalisés par des professionnels qualifiés ISO et suivi des corrections.

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 les périmètres d’évaluation, la maîtrise des essais et les documents remis aux équipes.

Audits et assurance sécurité

Un audit a de la valeur lorsque chaque conclusion relie une exigence, un contrôle, un fait observé et une action attribuée. Nos auditeurs qualifiés ISO organisent les échantillonnages, évaluent la conception et le fonctionnement des contrôles et produisent des constats que la direction peut traiter. Les périmètres PASC/OSPCRM applicables sont précisés pour chaque mission, avec une séparation nette entre conseil et assurance indépendante.

Tests d’intrusion

Un test d’intrusion utile montre comment un attaquant pourrait progresser et ce qui empêcherait cette progression. Nous partons d’une autorisation écrite et d’un périmètre défini, examinons applications, API, identités, infrastructure et certaines interfaces industrielles, puis remettons des constats reproductibles avec leurs corrections. Le contre-test permet de juger si le chemin d’attaque a réellement été interrompu.

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.

Travaux et livrables

Audits et assurance sécurité

Appui à l’audit interne, évaluation indépendante ou assurance continue ; les portées de qualification et d’accréditation sont communiquées dans le dossier de mission.

- Gouvernance et contrôles : tests fondés sur les risques selon ISO 27001/27002, ISO 22301, ISO 27701 et les référentiels applicables.
- Assurance technologique et fournisseurs : revue des identités, du cloud, des changements, journaux, sauvegardes et chaînes d’approvisionnement à partir d’échantillons probants.

Vous recevez : Lettre de mission, critères, indépendance et plan d’échantillonnage

Tests d’intrusion

Test ponctuel autorisé, campagne régulière ou contre-test. L’entité accréditée PASC et le périmètre concerné figurent dans le dossier fournisseur de la mission.

- Applications et API : tests autorisés web, API, mobile et logique métier, avec attention à l’authentification, l’autorisation et l’isolation entre locataires.
- Infrastructure et cloud : périmètres interne et externe, chemins d’attaque IAM, vérification des configurations et élévation de privilèges.

Vous recevez : Règles d’engagement signées, limites, contacts et conditions d’arrêt

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

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