Expertise Sécurité SI

La solution Expertise sécurité SI permet de s'assurer qu'un SI réponde aux exigences du référentiel de votre entreprise et en cohérence avec le référentiel sécurité du Groupe EDF.

Description du service

Group Support Services vous propose la solution Expertise sécurité SI pour répondre à vos préoccupations dans le domaine de la sécurité SI, selon différentes modalités :

a) Audit de Sécurité

Cette modalité permet de répertorier les points forts de sécurité de votre application, mais aussi ses vulnérabilités. Celles-ci sont alors associées à un ou plusieurs plans de remédiation qui vous permettront, par exemple, de réagir face une attaque, de vérifier la bonne application de la Politique de Sécurité du SI (PSSI) du Groupe EDF, de tester un nouvel équipement et d'évaluer l'évolution du niveau de sécurité de vos applications et infrastructures.

Nous proposons trois niveaux de prestation afin de répondre à vos besoins :

- **Le diagnostic « sécurité »** permet d'évaluer rapidement le niveau de sécurité technique d'un périmètre restreint en se focalisant uniquement sur des tests d'intrusion.
- **L'audit « standard »,** plus complet qu'un diagnostic de sécurité propose une analyse organisationnelle (revue d'habilitation, adéquation entre vos besoins sécurité métiers et l'architecture mise en place) à travers les prestations suivantes :
  - Des tests d'intrusion avec un périmètre plus important,
  - Une analyse documentaire,
  - L'organisation d'ateliers avec les acteurs clés.
- **L'audit « étendu »** pour des besoins complexes sur un périmètre à fort enjeux métier.

b) Analyse de Risque

Cette modalité permet d'identifier les besoins de sécurité d'une application ou d'une architecture en fonction des données et processus manipulés tout au long de la vie du projet. Vous aurez le choix de réaliser des mesures correctives ou non. Nous vous proposons encore plusieurs niveaux d'analyses :

- L'Analyse de Risque Simple (ARIS) :
  - Une analyse basée sur un questionnaire qui permet d'avoir une photo instantanée de la sécurité de votre projet en collaboration avec les métiers,
  - La mise à disposition et la présentation d'un fichier d'analyse :
    - Besoins de sécurité selon les critères : Disponibilité, Intégrité, Confidentialité et Traçabilité (DICT),
    - Listes des risques et mesures associées, synthèse des mesures pour simplifier la mise en œuvre,
    - Vérification de la conformité des traitements sur les données à caractère personnel en regard du Règlement Général sur la Protection des Données (RGPD).
- L'Analyse de Risque SaaS :
  - Une analyse de risques simple et plus détaillée qui permet d'identifier les risques et les mesures spécifiques d'une application hébergée en SaaS,
  - Un accompagnement pour préparer un passage en BIPSE (Bureau d'Instruction des Projets de Services Externes).
- L'Analyse de Risque Standard* :
  - Une analyse de risque détaillée du SI comportant des ateliers de cadrage afin d'identifier les besoins,
  - Une analyse de risque adaptée à vos besoins spécifiques (périmètre, planning, etc.),
  - Une Etude d'Impact sur la Vie Privée (EIVP) comprise,
  - La mise à disposition et présentation d'une synthèse détaillée et d'un rapport d'analyse de risque.
- L'Analyse de Risque Complexe* :
  - Une analyse encore plus approfondie du SI – évaluation précise des niveaux de risques et de leurs évolutions possibles,
  - Des livrables identiques à la prestation d'Analyse Standard avec en complément la présentation des recommandations et des mesures de correction.

* *L'application de la méthode EBIOS RM (Risk Management) qui présente les scénarios de risque métier ou la méthode EBIOS 2010 pour une approche plus exhaustive.*

c) Prestations en amont pour le de cadrage et l'accompagnement à la mise en œuvre de la politique Sécurité SI dans vos projets :

- L'accompagnement à la classification de vos informations :
  - Identification des niveaux de sensibilité des informations de manière à définir les mesures de sécurité à mettre en œuvre pour les protéger efficacement,
  - Association (lorsque cela est possible) des prestations d'urbanisme (cartographie des applications et des flux d'informations),
  - Aide à la réalisation de la classification, c'est-à-dire, à l'affectation à chaque famille d'information un niveau de sensibilité (de 1 à 3) sur chacun des 4 critères (disponibilité, intégrité, confidentialité et traçabilité),
  - Aide à la définition du niveau de protection à mettre en œuvre dans les différentes étapes du cycle de vie de ces informations.
- L'appui à l'expression de vos besoins en sécurité SI,
- L'aide à la rédaction de vos cahiers des charges ou de vos Cahiers des Clauses Techniques Particulières (CCTP) pour intégrer et clarifier les enjeux de sécurité.

Tout au long du cycle projet, des prestations d'expertise sécurité SI, dans plusieurs domaines :

- L'appui et l'accompagnement sur les sujets portés par le client avec la mise en place de solutions ou de plans d'actions résultant des revues de sécurité et de la classification des informations,
- L'accompagnement du projet, de la conception à la mise en exploitation, pour l'intégration des solutions de sécurisation,
- La recherche de solutions pour les domaines non couverts.

d) Prestations en aval du projet et tout au long de la vie de vos SI, pour vous permettre d'évaluer leur niveau de sécurité :

- La réalisation de revues de sécurité, qui permettent de mesurer le niveau de sécurité de votre SI et de vérifier qu'il est en adéquation avec le niveau requis par la Politique de Sécurité des SI (PSSI) du Groupe EDF et de vos exigences Métiers.

Elles peuvent prendre trois formes différentes :

- Revues organisationnelles (structure, processus, procédures),
- Revues fonctionnelles (ou de projets) – intégration des solutions de sécurité SI aux différents stades de développement de vos SI,
- Tests d'intrusion et revues de vulnérabilités techniques.

Pour chaque modalité de la solution Expertise Sécurité SI, nous rédigeons une note de cadrage pour contractualiser la prestation si le volume de l'affaire le justifie. Nous fournissons également les résultats sous forme de rapports d'études, de synthèses ou de recommandations.

Prérequis

Vous devez nous :

- Fournir l'ensemble des informations et interlocuteurs nécessaires à l'analyse,
- Mettre à disposition une plateforme pour les besoins de tests techniques pendant une durée de 5 jours ouvrés pour un diagnostic et 10 jours ouvrés pour un audit standard,
- Désigner un ou plusieurs expert(s) fonctionnel(s) qui seront joignables tout au long du projet.

Options disponibles

- L'accompagnement à la réalisation technique du plan d'actions,
- Le test de présence des vulnérabilités des applications en production,
- La présentation des vulnérabilités et des risques identifiés (hébergeur, éditeur…).

/!\ Les domaines techniques et les solutions de sécurité couvrent plusieurs périmètres :

- Les postes de travail et les serveurs,
- Les infrastructures réseaux et télécoms,
- Les applications : logiciels et progiciels, gestion des droits des utilisateurs.

Nos engagements

Modalité Audit de sécurité SI

Accusé réception de la demande	Sous 5 jours ouvrés
Proposition de planning	Définition du périmètre et proposition d'un planning détaillé, lors de la réunion de lancement

Modalité Analyse de risque

Analyse de risque simplifiée	• Fourniture d'un planning : 2 semaines à réception des informations nécessaires à l'analyse. • Démarrage de la prestation : au plus tard 1 mois après la validation du devis.
Analyse de risque complexe	• Fourniture d'un planning : 1 mois à réception des informations nécessaires à l'analyse. • Démarrage de la prestation : au plus tard 2 mois après la validation du devis.

Autres prestations

Mise à disposition	• Accusé de réception de votre demande et affectation d'une ressource sous 5 jours ouvrés. Mise à disposition des livrables : conforme au planning défini avec vous.

Domaine d'application

Solution ouverte aux filiales du Groupe EDF (hors ENEDIS).

Durée de l'engagement

La durée d'engagement est conditionnée par le contrat entre le Client et G2S.

Modalités de souscription

Pour plus d'information, contactez votre responsable commercial.

Références clients