AGENCE
DU NUMÉRIQUE
EN SANTÉ

Présentation du test d'intrusion & exigences SSI

Ségur numérique Vague 2

26 Avril 2024

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Test d’intrusion

Ségur numérique vague 2

/ 01 Contexte de réalisation

Contexte de la réalisation du test d'intrusion

L'un des principaux piliers du programme Ségur Numérique **est la sécurité**. Par conséquent, chaque solution **candidate fait l'objet d'une évaluation cyber** afin de s'assurer qu'elle ne présente pas de vulnérabilités potentiellement exploitables.

CADRE

- A ce titre, les éditeurs sont tenus de **réaliser un test d'intrusion** en vue de se conformer à **l'exigence SC.SSI/GEN.18**.
- Ce test d'intrusion donne lieu à la **complétion d'un formulaire** par l'auditeur, qui sera ensuite soumis par l'éditeur dans le cadre de la demande de référencement.

INTERVENANTS

- Le test d'intrusion doit être réalisé **par un prestataire qualifié PASSI.**
- Cependant, **il ne s'agit pas d'un audit PASSI** (la certification PASSI n'est pas requise pour l'auditeur et les conditions de réalisation du test d'intrusion ne sont pas celles d'un audit PASSI).

DOCUMENTS POUR LA RÉALISATION DU TEST D'INTRUSION

Guide d'utilisation : **Lecture préalable nécessaire** avant de commencer le test d'intrusion, détaillant ses spécificités

Formulaire Excel : Grille d'audit à télécharger depuis la plateforme Convergence, à **transmettre à l'auditeur** afin qu'il puisse la compléter

/ 02

Contenu et critères de validation du test d’intrusion

Base de conception du test d'intrusion

L'OWASP (Open Web Application Security Project) est une organisation à but non lucratif mondialement reconnue en matière de cybersécurité. Elle offre des ressources et des outils pour aider à construire et à maintenir la sécurité informatique des applications. Ainsi, l'OWASP publie et met à jour la liste du **top 10 de l'OWASP**, qui répertorie les **dix principales menaces et vulnérabilités cyber**

Couverture SSI

Les points de contrôle du test d'intrusion sont basés sur le référentiel du **Top 10 de l'Open Web Application Security Project – OWASP**, ce qui permet de cibler les vulnérabilités courantes et spécifiques aux différents types d'application (Web, clients lourds, mobile)

Clarté & précision

Une description et les liens entre les principales vulnérabilités de l'OWASP et le formulaire du test d'intrusion sont proposés dans le guide d'utilisation du formulaire

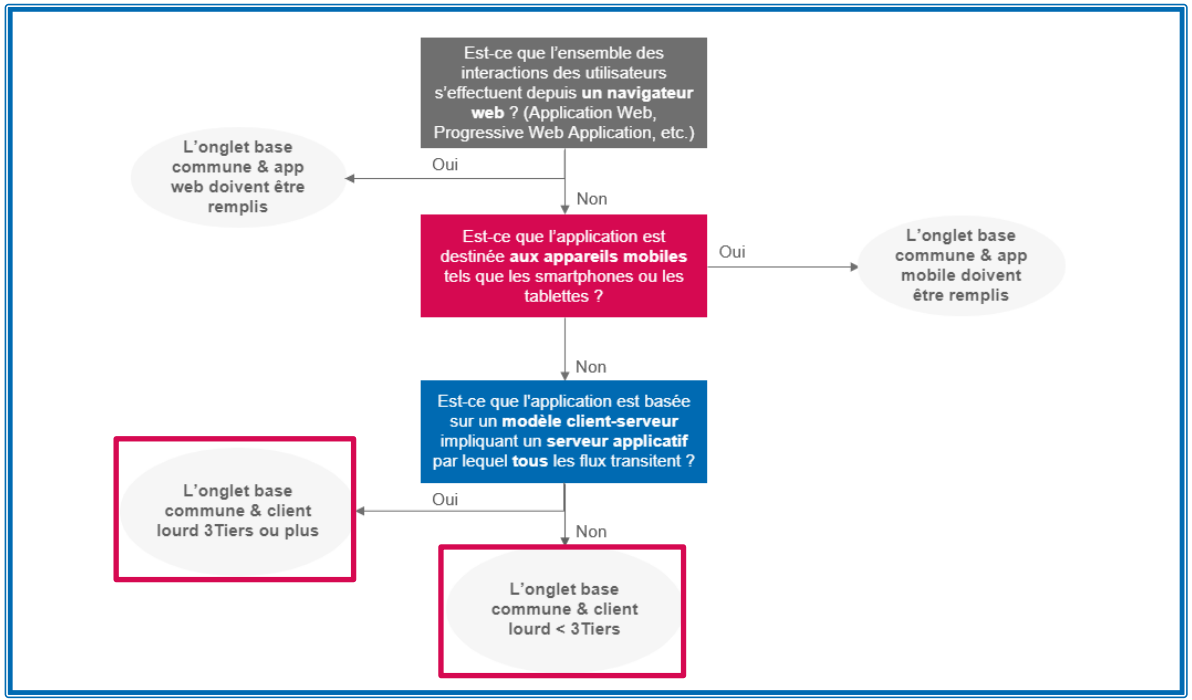
Equité

La description dans le formulaire des points de contrôle précis à auditer lors du test d'intrusion permet de garantir que le **périmètre de couverture sera identique** quel que soit l'auditeur intervenant (prestataire PASSI disposant de compétences suffisantes pour réaliser l'audit)

A01:2021	Broken Access Control
A02:2021	Cryptographic Failures
A03:2021	Injection
A04:2021	Insecure Design
A05:2021	Security Misconfiguration
A06:2021	Vulnerable and Outdated Components
A07:2021	Identification and Authentication Failures
A08:2021	Software and Data Integrity Failures
A09:2021	Security Logging and Monitoring Failures
A010:2021	Server-Side Request Forgery

Catégorisation des applications

- ✓ Le formulaire du test d'intrusion comprend à la fois des points de contrôle valables pour toutes les applications et des points de contrôle spécifiques à chaque type d'application ***(web, mobile, client lourd moins de 3 tiers, client lourd 3 tiers ou plus).***
- ✓ Pour faciliter l'identification des applications, un aperçu de leur classification est fourni via le logigramme ci-dessous :



Nouveaux ajouts

Logigramme de catégorisation des applications

Seuils de validation du test d'intrusion

- Les points de contrôle se divisent en **18 points communs, applicables à toutes les applications**, ainsi que **21 à 24 points spécifiques à chaque type d'application**.
- Chaque point de contrôle est classé selon deux niveaux de gravité : " ***Moyenne*** " ou " ***Haute***

SEUIL DE CONFORMITÉ AU FORMULAIRE DU TEST D'INTRUSION

GRAVITÉ HAUTE

La non-conformité au point de contrôle est éliminatoire : L'éditeur ne sera pas éligible au référencement dans ce cas

GRAVITÉ MOYENNE

Jusqu'à **10 réponses négatives à l'ensemble des points de contrôles de gravité moyenne** sont tolérées

Uniquement dans le cas des architectures inférieures à 3-Tiers (standalone & architectures 2-Tiers), certains points de contrôle ne rentrent pas dans l'évaluation du score. Dans ce cas, la gravité est indiquée dans le formulaire avec la mention « NA ». Ces points de contrôles doivent néanmoins impérativement **être audités pour valider le processus de référencement**.

/ 03 Planning et phases de l’audit

Description des phases du processus de test d'intrusion

Le test d'intrusion se déroule généralement sur **une période d'une semaine (5 jours/homme)** et s'organise en **quatre phases** définies ci-dessous :

Phase de cadrage

Contractualisation avec un PASSI

Signature du contrat (audit PASSI non requis), incluant une « clause de revoyure » pour les points de contrôles non-validés

Communication des entrants à l'auditeur

Dates de réalisation de l'audit, solution logicielle, prérequis, contacts ainsi que le formulaire du test d'intrusion et son guide d'utilisation

Phase de test

Réalisation des tests sur la brique logicielle

Réalisation des tests sur la brique logicielle, sur une période de 3 à 4 jours

Recensement des non-conformités

Identification des failles et des vulnérabilités de l'application pour une évaluation complète de sa sécurité

Remplissage du Formulaire du test d'intrusion

Complétion de l'onglet « Base commune » ainsi que de l'onglet correspondant au type de l'application

Génération du PDF

Génération automatique du PDF à partir de la macro du fichier Excel ou de façon manuelle

Signature électronique du PDF

Signature électronique du PDF avec un certificat de signature délivré par TSP

Transmission du formulaire à l'éditeur

Transmission par l'auditeur à l'éditeur du formulaire du test d'intrusion

Phase de rapport

[optionnel] Réévaluation

Réalisation des tests uniquement sur les points de contrôle non validés pour valider la correction des non-conformités

Soumission du formulaire

Envoi du formulaire sur la plate-forme convergence pour la demande de référencement

Phase de communication des résultats

Référencement

Validation du test d'intrusion dans l'absence de toute gravité haute et si moins de 10 gravité moyennes ont été identifiées.

Rôle de l'éditeur lors de la phase de cadrage (1/2)

Pour garantir le succès du test d'intrusion, l'éditeur doit préalablement préparer son produit en vue de cette évaluation :

01

ISO-prod

Le test d'intrusion doit être réalisé de préférence **sur un environnement « iso-prod »** (ex: environnement de développement, de test, etc.), dans des conditions proches de celles d'un environnement de production

02

Version identique

S'assurer que l'application fournie correspond à la même **version majeure** que celle actuellement en production, en incluant des critères tels que la similarité des données, un niveau de sécurité adéquat et une configuration identique

03

Audit du produit

Vérifier que tous les **dispositifs de sécurité**, tels que le pare-feu d'application web (WAF), les sondes, les passerelles, etc., soient désactivés s'ils ne font pas partie de la solution commercialisée

04

Type d'application

Pré-identifier **le type d'application** à l'aide du logigramme fourni dans le guide d'utilisation

Rôle de l'éditeur lors de la phase de cadrage (2/2)

Pour garantir le bon déroulement de la prestation, l'éditeur doit fournir à l'auditeur les informations suivantes, en fonction de la catégorie de l'application testée.

Pour une application Web

› **L'application**, une URL ou une adresse IP

Pour une application Mobile

› Une **APK sans pinning de certificat et sans vérification du débridage** du téléphone. Si possible, des terminaux débridés (accès complet pour déverrouiller les fonctionnalités)

Pour un client lourd

› **Le client et des accès pour examiner les configurations** possibles de l'application

Pour tous les types de solutions :

› **Plusieurs comptes** avec différents niveaux de privilèges (compte utilisateur, compte à privilège) ;

› La **liste des comptes génériques** pour vérifier l'exposition de ces derniers ;

› **Une matrice des flux** spécifiant les flux essentiels au fonctionnement du système ;

› Une **extraction des logs techniques** sur les tests réalisés lors du **premier jour opérationnel** afin de suivre les tentatives d'authentification, la présence de données sensibles (toute donnée à caractère personnel, qu'elle soit ou non de santé, ou participant à la sécurité du système d'information constitué par le système seul ou le système d'information auquel il participe) et le format des événements. Ces logs doivent être transmis le plus rapidement à l'auditeur.

› **L'éditeur doit informer l'auditeur** de **toutes les vulnérabilités connues**, ainsi que des **mesures de sécurité mises en œuvre** pour les traiter.

AGENCE DU NUMÉRIQUE EN SANTÉ

Présentation du formulaire du test d'intrusion

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Avez-vous des questions ?

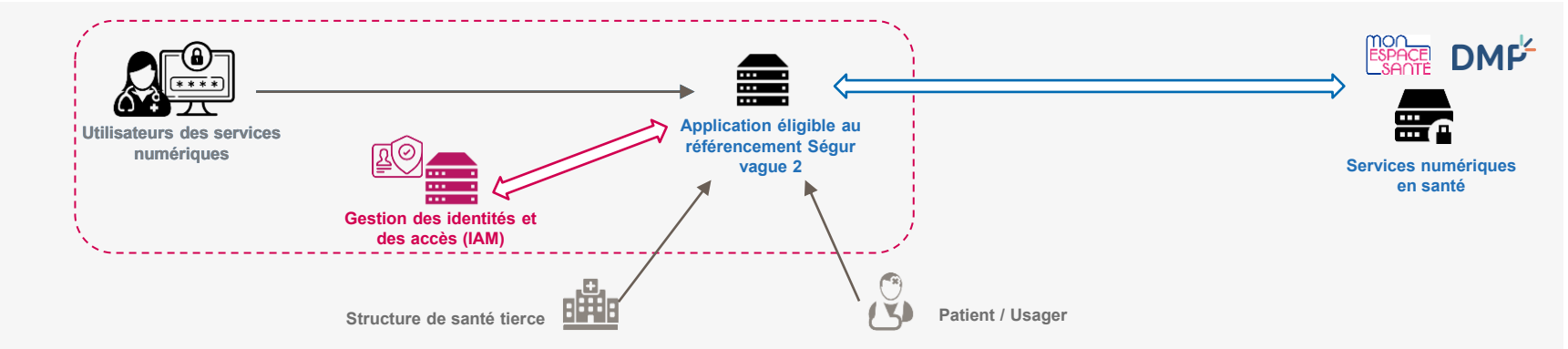
AGENCE
DU NUMÉRIQUE
EN SANTÉ

Exigences SSI

Ségur numérique vague 2

/ 01 Périmètre d’applicabilité des exigences SSI

Vague 2 – Synthèse des exigences SSI



Socle commun d'exigences SSI

- **7 exigences critiques** permettant de garantir un **niveau de sécurité suffisant** de la solution (synthèse des exigences SSI s'appliquant aux éditeurs)
- Intégration de ce socle commun **pour l'ensemble des Tasks Forces** ;
- Les exigences sont validées en se basant sur la **revue documentaire** ainsi que sur la **validation du test d'intrusion**.

Exigences sur l'Identification Electronique

- **Pour les DPI : Une demi-douzaine d'exigences** en lien avec le référentiel IE, dans la situation où le produit à référencer permet la **connexion de professionnels de santé.**
- **Pour les PFI : 2 exigences** permettant de gérer la **gestion des comptes**, des **permissions** et des sessions des **administrateurs** et des **utilisateurs**

Exigences sur la gestion des identités

- **Pour les DPI : 5 exigences** répondant aux objectifs de déploiement d'une **solution de SSO puis d'IAM** pour les ES et à une forte demande des DSI d'ES de pouvoir intégrer plus facilement les logiciels dans une approche urbanisée.
- **Pour les PFI : 2 exigences** permettant d'améliorer le **monitoring** ainsi que **gouvernance** / **cycle de vie** des comptes

/ 02 Synthèse des exigences SSI

Synthèse des exigences du socle commun SSI

ID de l'exigence	Fonction	Descriptif simplifié de l'exigence	Couloir
SC.SSI/GEN.1	Désignation des responsables du suivi et maintien des mesures de sécurité	Dans les équipes en charge de la solution, les responsables de la sécurité doivent être identifiés ainsi que leurs responsabilités (activités de conception, de développement, d'installation, d'exploitation, d'administration, de maintenance et de support)	DPI & PFI
SC.SSI/GEN.2	Sensibilisation des équipes en charge	Une sensibilisation à la SSI doit être menée pour l'ensemble des équipes du système en charge des activités de conception, de développement, d'installation, d'exploitation, d'administration, de maintenance et de support. Dans le cas où le système est destiné à traiter des données à caractère personnel, ALORS la sensibilisation DOIT intégrer les obligations légales.	DPI & PFI
SC.SSI/GEN.3	Plan d'Assurance Sécurité du produit	Si l'industriel ou un tiers sous sa responsabilité assure l'hébergement de tout ou partie des composants du système, ou fournit tout ou partie du système sous forme de service (SaaS) ALORS, il DOIT intégrer dans le PAS du système les mesures de sécurité et les engagements entre l'hébergeur et la structure utilisatrice, pour l'environnement de mise en œuvre.	DPI & PFI
SC.SSI/GEN.11	Développement sécurisé	Les bonnes pratiques pour le développement et la configuration sécurisés doit être défini et suivi tant dans la création du système que dans l'implémentation de nouvelles fonctionnalités (vérification de qualité du code, gestion de l'obsolescence des bibliothèques, sécurisation de la plateforme système, etc.)	DPI & PFI
SC.SSI/GEN.18	Recherche de vulnérabilités	Le système doit faire l'objet d'un test d'intrusion réalisé par un prestataire d'audit qualifié (PASSI). Ce test d'intrusion est à la charge de l'éditeur et doit être réalisé conformément au guide d'utilisation mis à sa disposition. Il donne lieu au remplissage par le prestataire d'un formulaire qui permet de valider la conformité du système à des points de contrôles. Ce formulaire constitue une preuve et DOIT afficher le caractère éligible au référencement du système, être daté de moins d'un an et être signé électroniquement par le prestataire ayant réalisé l'audit.	DPI & PFI
SC.SSI/GEN.20	Veille et patch management	Un processus de veille sur les vulnérabilités des composants de la solution doit être défini et appliqué. Un processus de patch management ou de distribution des patchs (dans le cas d'une solution hébergée par une structure utilisatrice) doit être déterminé et mis en œuvre (application / distribution des patchs, des mises à jour des composants, etc.)	DPI & PFI
SC.SSI/GEN.21	Réalisation des sauvegardes	Pour toutes les solutions, l'industriel DOIT proposer une procédure de sauvegarde et de restauration ainsi que la documentation associée.	DPI & PFI

Synthèse des exigences IAM

ID de l'exigence	Fonction	Descriptif simplifié de l'exigence	Couloir
SC.SSI/IAM.80	Intégration d'une solution de webSSO	Le système doit être compatible avec le standard OpenID Connect et le flux Authentication Code Flow en tant que « relying party » . Le système doit permettre de configurer au moins 2 fournisseurs d'identités en même temps et laisser les utilisateurs sélectionner celui à utiliser. L'un de ces fournisseurs d'identités doit être Pro Santé Connect	DPI
SC.SSI/IAM.83	Gestion des éléments d'identités	Le système doit permettre la synchronisation des données de la base de comptes de manière régulière auprès d'un fournisseur d'identités ou auprès d'un référentiel local : synchronisation des données d'identité et des permissions macro	DPI
SC.SSI/IAM.91	Conservation des traces de type IAM	Le système doit conserver des traces de toutes les opérations réalisées en lien avec le cycle de vie des comptes (modification d'attributs d'identité, permissions, tentative de connexion et de modification de mot de passe)	DPI & PFI
SC.SSI/IAM.92	Politique de mot de passe pour les comptes d'administration	Le système doit permettre à la structure de santé de mettre en place une politique de mots de passe robuste sur les comptes d'administration sur la base de certains critères (caractères minimum, jeu de caractères, délais d'expiration, blocage du compte)	DPI & PFI
SC.SSI/IAM.94	Extraction des éléments d'identités et des permissions	Le système doit permettre d'extraire les données de comptes (données d'identité et de permissions), afin de permettre la revue et mise à jour de ces éléments par l'administrateur.	DPI

Synthèse des exigences sur l'identification électronique (IE)

ID de l'exigence	Fonction	Descriptif simplifié de l'exigence	Couloir
SC.SSI/IE.31	Gestion des comptes des utilisateurs	SI le système réalise une association entre l'identité du professionnel et ses coordonnées et si ces informations sont utilisées dans les mécanismes d'authentification ou de récupération de compte, ALORS le système DOIT vérifier, à la création d'un compte et à chaque modification, l'adresse de messagerie ou le numéro de téléphone portable du professionnel. Cette vérification peut se faire par l'envoi d'un code ou d'un lien d'activation.	DPI
SC.SSI/IE.32	Gestion des comptes des utilisateurs	SI le professionnel peut modifier ses attributs d'identité, son adresse de messagerie ou son numéro de téléphone, ALORS le système DOIT : - Vérifier les informations soumises par une méthode aussi fiable que lors de l'enregistrement initial ; - Envoyer, après modification, une notification au professionnel en utilisant l'ancienne coordonnée et une éventuelle autre coordonnée qui aurait été renseignée.	DPI
SC.SSI/IE.33	Gestion des comptes des utilisateurs	Le système DOIT gérer a minima les identifiants et attributs suivants d'un PS : - Numéro RPPS (si existant) - Identifiant privé (si existant), dont l'unicité doit être assurée - Nom d'exercice ; - Prénom ; - Profession ou une mention appropriée à la situation de la personne.	DPI
SC.SSI/IE.36	Connexion au système	SI le système propose un mot de passe comme facteur unique d'authentification, ALORS il DOIT : - Permettre d'implémenter les mesures de restriction d'accès et de vérification de complexité des mots de passe prévues par le Référentiel d'identification électronique ; - Être conforme à ces exigences dans sa configuration par défaut.	DPI & PFI
SC.SSI/IE.38	Déconnexion du système	Le système DOIT permettre au professionnel de fermer sa session.	DPI
SC.SSI/IE.39	Déconnexion du système	Le système DOIT forcer la déconnexion automatique d'un professionnel après une durée paramétrable d'inactivité.	DPI & PFI

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Avez-vous des questions ?

AGENCE
DU NUMÉRIQUE
EN SANTÉ

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante