AGENCE DU NUMÉRIQUE EN SANTÉ

Webinaire à destination des prestataires d’audit PASSI

Ségur numérique Vague 2

17/10/2024

Objectifs du webinaire

Ce webinaire a pour objectif de :

- présenter aux auditeurs PASSI le **processus de référencement** ;
- partager les **attendus du test d'intrusion** pour lequel les éditeurs en santé seront amenés à faire appel à leur expertise.

/ 01 Test d’intrusion : Introduction & Contexte

Un programme autour des éditeurs en santé et de la SSI

Le dispositif SONS est un financement incitatif proposé par l'Etat pour soutenir la modernisation et la sécurisation des logiciels métiers en santé. Dans ce cadre, la conformité des solutions candidates au référencement est évaluée afin de s'assurer de l'atteinte d'un niveau de maturité et de la conformité avec les **réglementations et initiatives** en cours dans l'écosystème santé

Contexte

- L'actualité fait régulièrement état de cyberattaques **touchant des structures de santé**
- Le fonctionnement de ces structures peut être impacté de **façon grave voire même irréversible** dans certains cas
- Les structures de santé manipulent au sein de leurs systèmes d'information des données de santé à **caractère personnel**, données particulièrement **sensibles** et qui doivent être protégées en conséquence.

Enjeux de sécurité

- Les applications utilisées sont progressivement amenées à s'interconnecter avec **Mon Espace Santé et notamment le DMP**
- L'application des bonnes pratiques de sécurité est plus que jamais **indispensable** sur les SI des structures de santé et doit être prise en compte dans **les solutions numériques qu'elles utilisent au quotidien**
- Les solutions logicielles font partie des **vecteurs d'attaque** qui peuvent être utilisés pour **accéder au SI d'un établissement de santé**

L'ambition du Ségur numérique est le partage fluide et **sécurisé** des données de santé. Il est donc essentiel que la dimension cybersécurité soit abordée dans le cadre du Ségur numérique et que cela vise les logiciels métiers utilisés au sein des structures de santé

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 au **remplissage 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 par l'éditeur depuis la plateforme **Convergence, puis à transmettre à l'auditeur pour complétion.**

/ 02

Contenu 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.** Ce classement est une référence mondiale qui permet de **cibler en priorité les vulnérabilités présentant les risques les plus critiques**.

Couverture SSI

Les points de contrôle du formulaire de test d'intrusion sont basés sur le **Top 10 de l'OWASP**, afin de se concentrer sur les vulnérabilités qui présentent le plus de risques

Clarté & légitimité

Les liens entre les points de contrôle du test d'intrusion et les principales vulnérabilités de l'OWASP ont été établis et précisés dans le guide du test d'intrusion fourni à l'éditeur et à l'auditeur. Cela apporte clarté et crédibilité à la démarche (appui sur une référence internationalement reconnue).

Equité

La description des points de contrôle précis qui devront être audités 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

Contenu du test d'intrusion à compléter par l'auditeur

Deux types de points de contrôle

- **18 points de contrôle communs à toutes les solutions** (**obligatoirement analysés** par l'auditeur quelle que soit la solution concernée)
- **21 à 24 points de contrôle spécifiques au type de périmètre testé** (certaines mesures de sécurité devront être évaluées **selon l'architecture de la solution**)

Deux niveaux de « gravité » définis

GRAVITÉ HAUTE

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

GRAVITÉ MOYENNE

Jusqu'à **10 réponses négatives à des points de contrôles de gravité moyenne** peuvent être acceptées au maximum.

NA

Pour les architectures inférieures à 3-Tiers uniquement : Les points de contrôle notés « NA » **doivent être audités** pour valider le processus de référencement, mais **ne rentrent pas dans l'évaluation du score**.

Le formulaire du test d'intrusion intègre une **macro qui génère automatiquement le rapport d'audit** et confirme la validation du pentest **sur la base des champs complétés par l'auditeur**.

/ 03 Planning et phases de la prestation

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.

Éléments attendus lors de la phase de cadrage

Pour assurer le bon déroulement du test d'intrusion, l'auditeur doit d'abord vérifier quelques prérequis et s'assurer que certains éléments ont été transmis par l'éditeur

01 Prérequis

- Veiller à ce que l'environnement proposé par l'éditeur soit un **environnement iso-prod**
- S'assurer que l'application fournie soit **dans la version majeure** pour laquelle l'éditeur candidate
- Vérifier que tous les **dispositifs de sécurité** (WAF, sondes, passerelles, etc.) sont désactivés
- Vérifier que l'éditeur a bien **renseigné le type d'application** dans le formulaire

02 Entrants

Pour toutes les applications

- Plusieurs **comptes avec différents niveaux de privilèges**
- Liste des **comptes génériques**
- **Matrice des flux**
- Extraction des **logs techniques** sur les tests réalisés lors du premier jour opérationnel
- Information sur **les vulnérabilités connues** et les **mesures de sécurité mises en œuvre** pour les contourner

Selon le type d'application

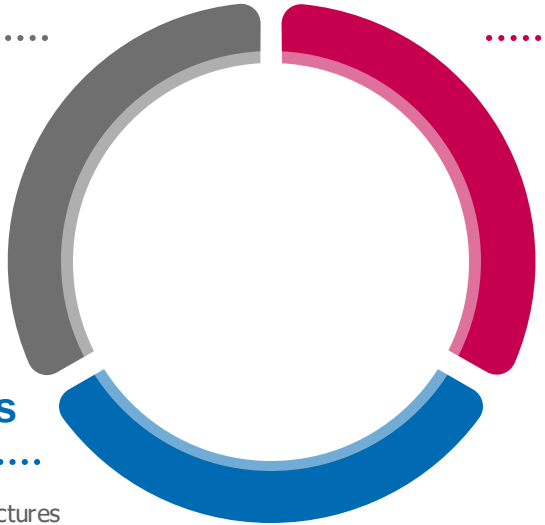
- **App Web** : URL ou adresse IP
- **App mobile** : APK sans pinning de certificat et sans vérification du débridage du téléphone et, si possible, terminaux débridés
- **Client lourd** : client et accès aux configurations

Règles de remplissage du formulaire

L'auditeur doit tester tous les points de contrôle énumérés dans le formulaire de test d'intrusion et évaluer la conformité de l'application à ces points. Ensuite, il peut remplir le formulaire de test en respectant les instructions suivantes :

Remplissage de 2 onglets

Seuls deux onglets doivent être remplis par l'auditeur : l'onglet « Base Commune » ainsi que l'onglet correspondant au type d'application audité.



Notation des règles

Seule la notation "Oui, Non ou N/A" est autorisée. Pour chacune des règles de sécurité, une notation doit être attribuée.

N.B.

La notation "N/A" ou "NON" **doit être limitée** et nécessite une **justification en commentaire**.

La notation N/A est utilisée lorsque la règle de sécurité ne dépend pas de l'éditeur mais de la structure utilisatrice ou n'est pas applicable au système.

Cas des architectures multiples

Si l'application possède plusieurs types d'architectures (ex : app Web et app mobile) ou d'infrastructures (SaaS, on-premise, etc.), **un formulaire doit être réalisé pour chaque partie**.

Génération et signature du rapport

- Une fois le formulaire rempli, un fichier PDF reprenant les éléments qu'il contient doit être généré à partir de la macro du formulaire du test d'intrusion puis signé électroniquement, avec l'approbation d'un TSP (Trust Service Provider).
- Le formulaire doit ensuite être transmis à l'éditeur, qui doit le soumettre dans le cadre de sa demande de référencement Ségur sur la plateforme Convergence.

Deux options sont possibles pour la signature électronique du test d'intrusion

1

Au moyen d'une application bureautique telle qu'Adobe Acrobat, en utilisant un certificat de signature délivré par un TSP

2

Par le biais d'une plateforme de signature électronique reconnue telle que DocuSign, YouSign, etc.

Dans le cas où l'éditeur devrait apporter **des corrections aux vulnérabilités pour se conformer au seuil de validation**, il doit **informer l'auditeur** des vulnérabilités corrigées. Ensuite, **l'auditeur teste ces points** pour vérifier les corrections et **met à jour le formulaire**.

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Démo de remplissage du formulaire de test d'intrusion

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Avez-vous des questions ?

Questions fréquentes – Processus

- **Le test d'intrusion peut-il être rempli sur la base d'un pentest réalisé précédemment ?**

  Le formulaire du test d'intrusion Ségur peut être complété à posteriori par un auditeur PASSI sur la base d'un test d'intrusion qu'il aurait réalisé précédemment pour la même solution, à condition que la preuve soit datée de moins d'un an à date de dépôt par l'éditeur sur la plateforme Convergence.

- **Quelle est la finalité de la phase de rapport ?**

  La phase de rapport a pour finalité d'échanger sur le rapport du test d'intrusion, notamment si des manquements aux règles de sécurité sont détectés. L'auditeur devra communiquer les résultats du test d'intrusion à l'éditeur en clarifiant les points suivants :
  - Les détails techniques des vulnérabilités identifiées ;
  - L'impact potentiel des non-conformités aux règles de sécurité et le niveau de risque associé ;
  - Les solutions concrètes permettant de corriger les potentielles failles ;
  - La définition des prochaines étapes (définition d'une date permettant d'évaluer de nouveau les vulnérabilités recensées).

Questions fréquentes – Conformité

- **Existe-t-il des exceptions permettant de valider des points de contrôle même s'ils ne sont pas conformes ?**

  Lorsque l'auditeur juge que l'exploitation d'une vulnérabilité est complexe en raison du contexte applicatif de la solution, le score CVSS peut être revu à la baisse par l'auditeur sur la base de cette observation.