



RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité



SERVICE SILENE

1. DESCRIPTION DU SERVICE

L'ANSSI met à disposition des opérateurs réglementés et de la sphère publique une capacité de cartographie de la surface d'exposition sur Internet au travers du service SILENE.

Cette capacité vise à donner de la visibilité à ces opérateurs sur leur niveau d'exposition et à les accompagner par l'application progressive de mesures adéquates pour le réduire. Cette prestation s'appuie sur l'expérience et l'expertise acquises par l'Agence lors des audits et s'enrichit également, au fil du temps, de l'observation des modes opératoires utilisés par les attaquants.

Les scans réseaux effectués par l'Agence dans le cadre de ce service visent spécifiquement les ports les plus classiquement ciblés lors des campagnes de cyberattaques.

De plus, les données échangées au niveau applicatif respectent les standards établis sans jamais essayer de contourner les protocoles définis. Les requêtes effectuées dans le cadre de ce service sont similaires à celles auxquelles vos équipements sont régulièrement exposés sur Internet.

Le service SILENE est pensé à la fois pour les chaînes SSI et les équipes d'exploitation. Pour les premières, l'application fournit une vision globale et synthétique à travers des tableaux de bord et indicateurs associés ; pour les secondes, elle détaille les recommandations à appliquer et accompagne les opérateurs dans le pilotage de leurs équipes techniques ou de leurs prestataires.

2. MODALITÉS D'ACCÈS AU SERVICE

Pour bénéficier du service, la procédure à suivre est la suivante :

1	Faire la demande de création d'un compte nominatif en lançant la procédure d'inscription sur https://club.ssi.gouv.fr
2	Connectez-vous sur le portail Club SSI.
3	Déclarez adresses IP publiques et noms de domaine sous votre responsabilité dans l'onglet « Services d'audits automatisés > SILENE » en cliquant sur le bouton « Nouveau périmètre »
4	Vous recevrez mensuellement un rapport pour chaque périmètre déclaré à partir du début du mois suivant votre demande.

Dès réception des adresses IP et des noms de domaine, l'ANSSI partagera périodiquement les résultats de la cartographie avec les bénéficiaires du service, sous forme d'un rapport détaillé présentant les différents points de contrôle qui ont révélé des défauts de configuration pouvant entraîner des risques de sécurité.

3. UNE APPROCHE LUDIQUE ET PERSONNALISÉE

Le rapport SILENE développe un certain nombre de points de contrôle et met en évidence des déviances ou des mauvaises pratiques qui pourraient permettre à un attaquant de prendre pied sur le système d'information.

Les résultats sont mis à disposition au travers d'une interface web qui détaille et classe les vulnérabilités et recommandations afférentes. Lors de chaque audit, le niveau de sécurité des services exposés sur Internet est traduit par un niveau qui se situe sur une échelle de 1 à 5. Le niveau obtenu dépend de la gravité des vulnérabilités trouvées, le niveau 1 étant synonyme de défauts critiques, le niveau 3 d'une sécurité non dégradée

(installation de services légitimes, sans durcissement particulier) et le niveau 5 d'un niveau de sécurité à l'état de l'art.

Un niveau donne ainsi accès à une liste de recommandations adaptées. L'administrateur réseau peut alors démontrer de manière objective et factuelle que les actions menées améliorent significativement le niveau de sécurité des services exposés sur Internet, et par conséquent la difficulté pour des acteurs malveillants de pouvoir accéder au SI de l'organisation. L'application de l'ensemble des recommandations portant sur les points importants d'un niveau permet de passer au niveau supérieur et d'accéder à une liste complémentaire de recommandations.



DES QUESTIONS SUR LE SERVICE ?

Consultez la FAQ accessible sur <https://club.ssi.gouv.fr/#/faq>
ou contactez-nous par email à club@ssi.gouv.fr

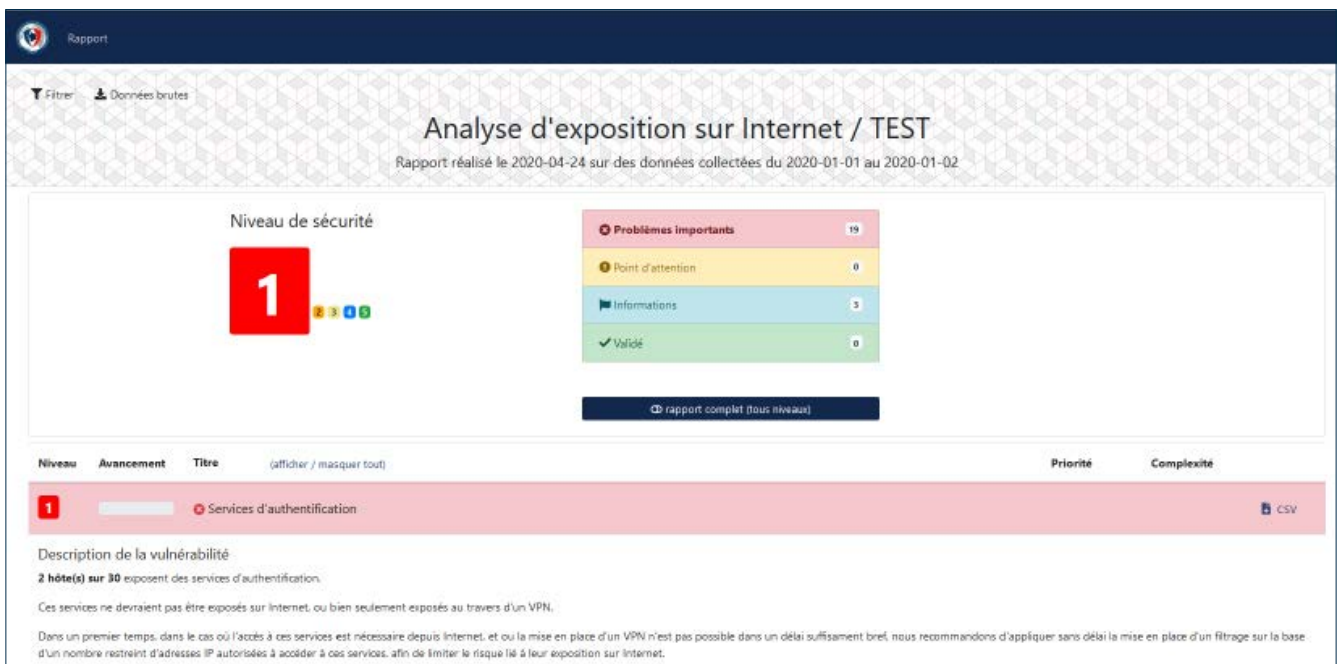
4. EN SAVOIR PLUS

CONNAÎTRE L'EXPOSITION DE SES SERVICES SUR INTERNET

Il est indispensable de bien maîtriser son exposition sur Internet, et de conserver une visibilité sur cet aspect fondamental de la sécurité d'un système d'information dans la durée. En effet, les services exposés sur Internet peuvent être exploités par des acteurs malveillants ou par des robots. Ils permettent alors parfois simplement de recueillir des

données techniques sur l'infrastructure d'une organisation mais peuvent également constituer un point d'entrée dans le cadre d'une compromission d'un système d'information.

De mauvaises pratiques, des erreurs de configuration des équipements filtrants ou encore des oublis d'anciens services obsolètes ont souvent comme résultat l'exposition d'interfaces d'administration ou de services internes qui sont autant de points d'entrée dans le système d'information.



Pour un niveau donné, le rapport détaille trois catégories d'indications :

- **Des problèmes importants** : vulnérabilités critiques qui devront être corrigées pour passer au niveau supérieur ;
- **Des points d'attention** : vulnérabilités logicielles potentielles faisant l'objet d'une attention prioritaire par l'Agence, services exposés sur les ports hauts ;
- **Des points d'information** : informations sur certains points-clé. Par exemple, sont ou seront indiqués :
 - L'ensemble des services exposés ;
 - L'ensemble des services exceptés les services classiques (par exemple : web, mail, etc) ;
 - L'ensemble des services web, mail et de téléphonie ;
 - L'ensemble des services d'administration ;
 - L'ensemble des fichiers partagés sans authentification.

Détails des niveaux	
1	Compromission instantanée possible ;
2	Exposition de services internes qui peuvent affaiblir le niveau de sécurité du SI, ou mettre en danger l'intégrité des données ;
3	Services inconnus, ou configuration non optimale de services exposés ;
4	Services sur des ports non standards ;
5	Aucun problème relevé.

L'ambition de l'ANSSI est d'accompagner progressivement les opérateurs vers une exposition réseau aussi limitée que possible grâce à l'application de recommandations adéquates et dans une approche ludique.

Ainsi, les opérateurs sont en capacité de définir un plan d'action en fonction de la sévérité des vulnérabilités identifiées tout en prenant en compte les exigences de leurs activités.