CSIS

LORCYBER

GUIDE CSIS V3.3 - CSIS.APP GUIDE CSIS V3.3 - CSIS.APP GUIDE CSIS V3.3 - CSIS.APP GUIDE CSIS V3.3 - CSIS.APP GUIDE

SOMMAIRE

CSIS par LORCYBER

Afin d'industrialiser la cybersécurité, LORCYBER développe une plateforme SAAS pour gérer de manière centrale et simplifiée, la sécurité de ses clients.

La plateforme CSIS «Computer Security Information System», vous aide à obtenir une vision à 360° de vos failles de sécurité. Vous pouvez dorénavant unifier la gestion de vos scans de vulnérabilités et de vos tests d'intrusions.

Cette gestion unifiée de vos actifs informatiques va vous permettre de mieux anticiper et gérer les risques liés aux vulnérabilités présentes dans votre système d'information.

Le workflow d'échange avec les différents acteurs de l'informatique vous donne également à tout moment le suivi des corrections apportés par les équipes informatiques à vos actifs.

Vous supervisez ainsi d'une manière optimale la sécurité de votre système d'information avec un meilleur contrôle du risque Internet.

BÉNÉFICIEZ DE LA CYBER-SÉRENITÉ

CSIS

LORCYBER

QUELLES PROBLÉMATIQUES ?

1 DÉTECTION DES VULNÉRABILITÉS

Aujourd'hui, détecter les vulnérabilités des actifs présents sur Internet est devenu une obligation.

Tester les failles de ses sites internet, de ses sites intranet, de ses routeurs permet aux équipes informatiques de pouvoir corriger au plus vite celles-ci.

Désormais, les fuites de données, les intrusions dans votre système ne sont plus une fatalité.

2 QUELS OUTILS ET COMMENT LES UTILISER ?

De nombreux outils existent afin de détecter les vulnérabilités, des outils open source ou d'éditeurs de logiciels de sécurité.

Cependant, **leur utilisation est complexe**. L'exploitation de ces outils nécessitent une expertise pointue.

De plus, les **rapports générés ne sont pas adaptés** à être distribué tels quels à des équipes de production ou de développement informatique.

3 LA DÉTECTION N'EST PAS SUFFISANTE

Pour permettre à ses équipes informatiques de pouvoir corriger ses applications ou sa production, il faut avoir un plan d'actions clair, dans un langage précis.

Ce plan d'actions doit également inclure, un volet «gestion de risques», certaines vulnérabilités pouvant être acceptées, si leur probabilité de survenance est faible, ou si l'impact est négligeable.

4 TABLEAU DE BORD ET SUIVI

Le suivi de ce plan d'actions devient un impératif pour un responsable informatique.

Il est important de savoir à tout moment, l'état réel de son exposition au risque Internet.

NOUS AVONS L'EXPÉRIENCE, LA DÉMARCHE ET L'OUTIL POUR RÉPONDRE À VOS BESOINS

Gartner Magic Quadrant 2019 Vulnerabity Risk Management

Page d'accueil d'un ingénieur cyber: dans cette configuration, le tableau de bord présente synthétiquement une vue des derniers rapports.

2

Nous avons interconnecté CSIS avec plusieurs leaders du marché du scan de vulnérabilités : Qualys, Rapid7, Tenable (Nessus) et PortSwigger (Burp Suite)

Et également avec l'outil fourni par l'OWASP : Zaproxy

4

Sur CSIS, vous avez la possibilité de personnaliser votre tableau de bord afin d'afficher la vue la plus pertinente à vos yeux :

- vulnérabilités les plus présentes,
- derniers rapports,
- derniers scans systèmes,
- ou derniers scans applicatifs.

LA SOLUTION
CSIS

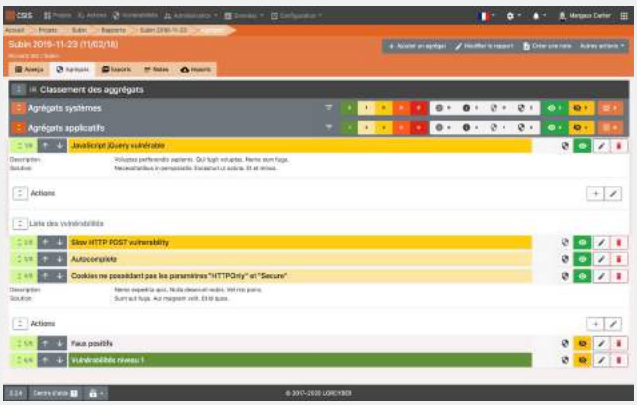
RAPIDITÉ / CLARTÉ / ACCESSIBILITÉ

OUTIL INTÉGRÉ

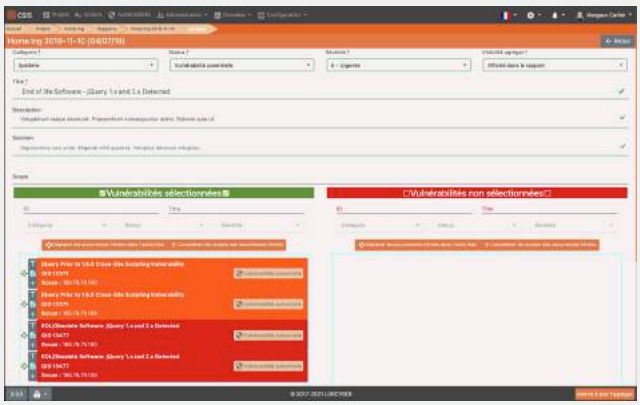
CSIS intègre le résultat des scans lancés sous votre scanner de vulnérabilités (Qualys, Rapid7, ...), et vous permet de créer vos rapports d'analyse de manière simple. Les ingénieurs sécurité ne se concentrent que sur l'analyse et la description des solutions à apporter.

Sur chacune des vulnérabilités que l'on souhaite intégrer dans le rapport, l'ingénieur sécurité peut créer une ou plusieurs actions à destination des équipes informatiques pour la correction.

La génération du rapport d'analyse se fait alors automatiquement, avec un résumé managérial, et un tableau de suivi sur l'évolution de l'actif analysé depuis le rapport précédent.



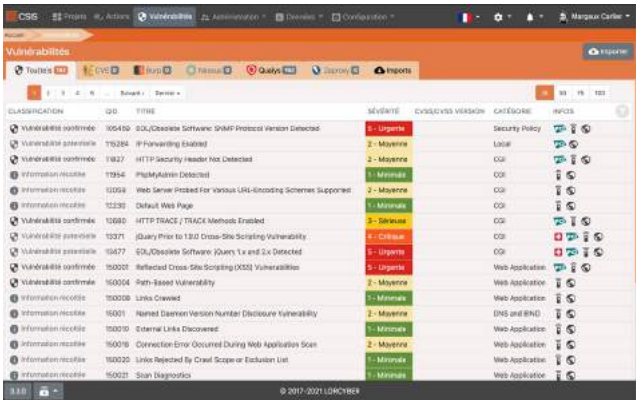
LISTE DES AGRÉGATS



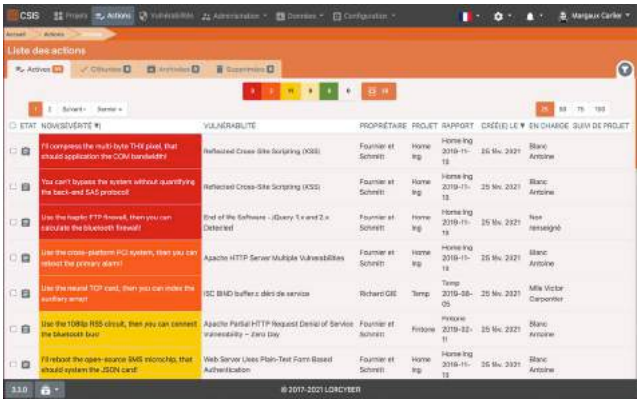
DÉTAIL D'UN AGRÉGAT

Agrégat* : ensemble cohérent de vulnérabilités sur lequel on apporte une solution

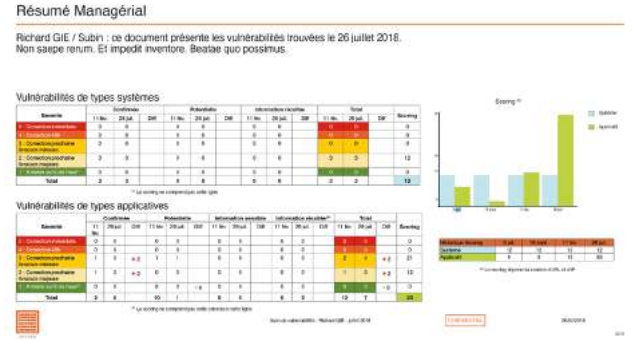
TABLEAU DE BORD PERSONNALISABLE



EXPLOREZ NOS BASES DE VULNÉRABILITÉS



LISTE DES ACTIONS



RÉSUMÉ MANAGÉRIAL

2 INTERFACES

Ingénieur Cybersécurité
(pour l'analyse)

& Utilisateur
(pour le suivi des corrections)

2 TYPES DE RAPPORTS PENTEST OU SCAN DE VULNÉRABILITÉS

Ainsi vous gérez de manière uniformisée les vulnérabilités de vos actifs informatiques

MULTICONNECTEURS DISPONIBLES

Plateforme connectée à plusieurs scanners : Qualys, Nessus, Nmap, Burp, Zaproxy, et Rapid7

BASE DE VULNÉRABILITÉS

CVE, Burp, Zaproxy, Qualys et Nessus

ASSISTANCE AUTOMATISÉE À LA CRÉATION DE RAPPORTS

Interface intuitive avec la possibilité d'agréger facilement les vulnérabilités. Pré-génération de rapports périodiques

ACTIONS DE CORRECTION

Possibilité de créer une ou plusieurs actions de correction à destination des équipes informatiques

EXPORT DES RAPPORTS EN PDF

Avec un résumé managérial et un tableau de suivi sur l'évolution de l'actif analysé

OUTIL EFFICACE

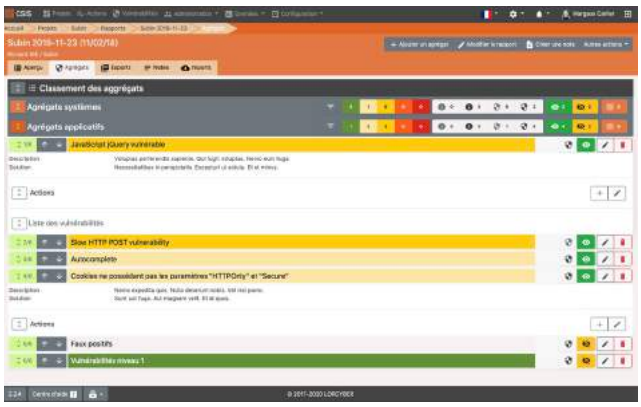
Le moteur de gestion des agrégats* de vulnérabilités permet de diviser jusqu'à 7 fois le temps passé sur chaque rapport.

L'accès utilisateur permet à vos équipes informatiques d'avoir, à tout moment, le dernier rapport d'analyse concernant l'ensemble des actifs analysés en un seul endroit, ainsi que les rapports historiques.

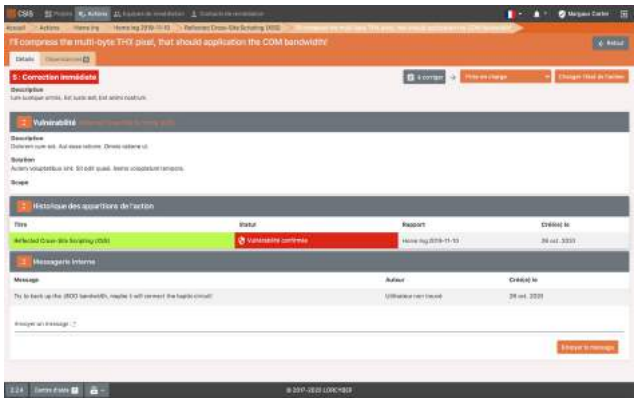
De plus, son interface multilingue, vous permet dans une organisation internationale de délivrer vos rapports dans la langue de vos interlocuteurs. L'analyse et la génération du rapport par nos équipes est effectuée en moins de deux heures en moyenne !

La description des actions de corrections peut ensuite être réalisée par nos équipes.

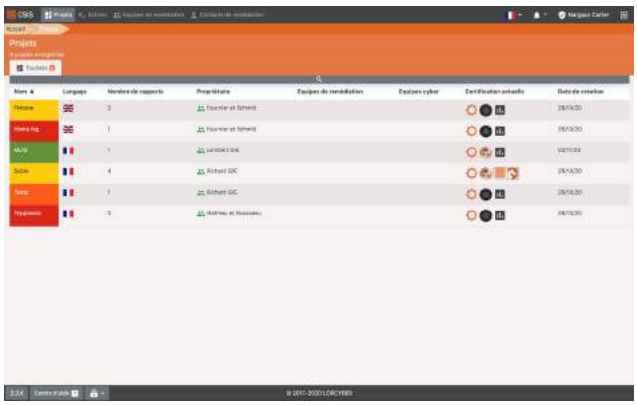
En une demi-journée, les équipes informatiques auront à disposition le rapport, ainsi que le tableau de suivi des actions de corrections dans leur interface utilisateur.



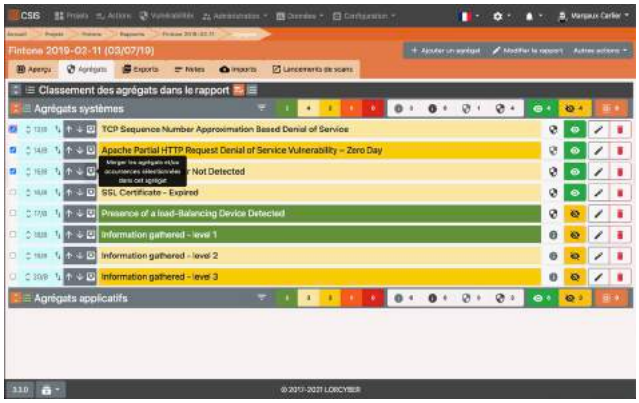
LISTE DES AGRÉGATS



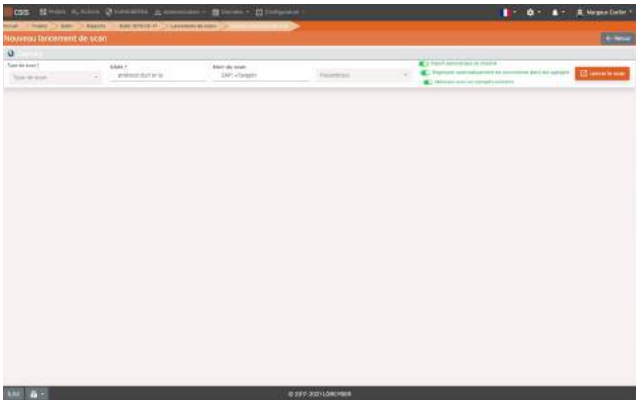
DÉTAIL D'UNE ACTION DE CORRECTION



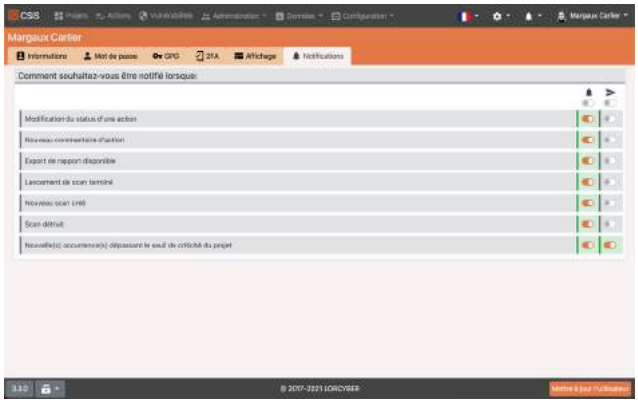
INTERFACE UTILISATEUR RAPPORTS



FUSION DES AGRÉGATS



LANCEMENT D'UN SCAN ZAPROXY



PARAMÉTRAGE DES NOTIFICATIONS

Désormais, la gestion optimisée des agrégats*, vous permet de reprendre des agrégats créés précédemment, afin de fusionner et de gagner encore plus de temps !

CSIS intègre également, en option, la plateforme Zaproxy et son scanner de vulnérabilités. Cette intégration permet de lancer directement depuis la plateforme CSIS des scans de vulnérabilités de façon ponctuelle ou périodique (quotidien, hebdomadaire, mensuel...)

L'outil Zaproxy ne remplace pas les scanners de vulnérabilités traditionnels mais son intégration vient compléter l'offre CSIS.

Dorénavant, recevez des notifications d'alertes via mail, dans l'application interne, ou bien sur vos outils collaboratifs préférés **(Teams, Slack, Zoho ou Google Chat)**.

Choisissez les sujets sur lesquels vous souhaitez être alertés au préalable :

- Modification du statut d'une action
- Nouveau commentaire d'action
- Export de rapport disponible
- Lancement de scan terminé
- Nouveau scan créé
- Scan détruit
- Nouvelle(s) occurrences dépassant le seuil de criticité du projet

Slack Google Chat Zoho Teams

AVEC SUIVI OPTIMISÉ DES CORRECTIONS

Les actions de corrections étant saisies également sous CSIS, l'ingénieur peut affecter, action par action, celles-ci à une équipe informatique.

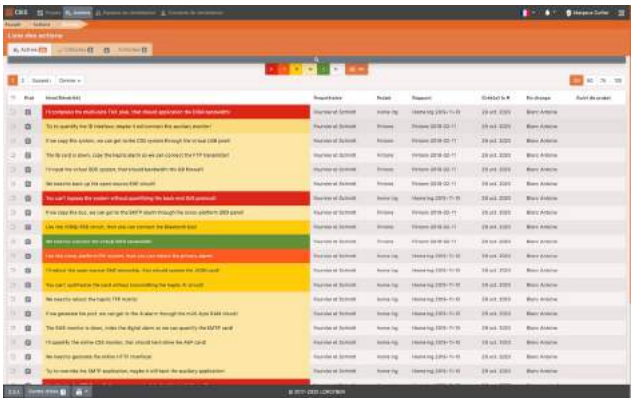
Les actions sont reçues par mail sécurisé, l'équipe destinataire via son interface utilisateur voit le détail précis des corrections à apporter.

Une fois la correction effectuée, un workflow de validation est mis en oeuvre, sous le contrôle des ingénieurs sécurité en charge.

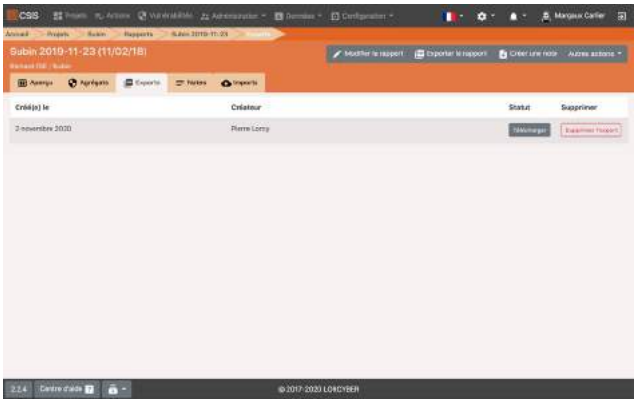
L'interface utilisateur dédiée aux équipes informatiques leur permet en un coup d'oeil de savoir l'état d'avancement de la correction.

Un système de juridiction permet de ne montrer à chaque équipe que les actions qui les concernent.

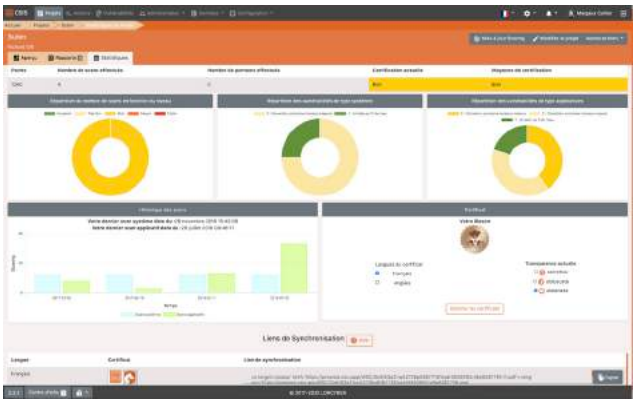
PAGE D'ACCUEIL ÉQUIPE IT



LISTE DES ACTIONS DE CORRECTIONS



INTERFACE DE GÉNÉRATION DES RAPPORTS

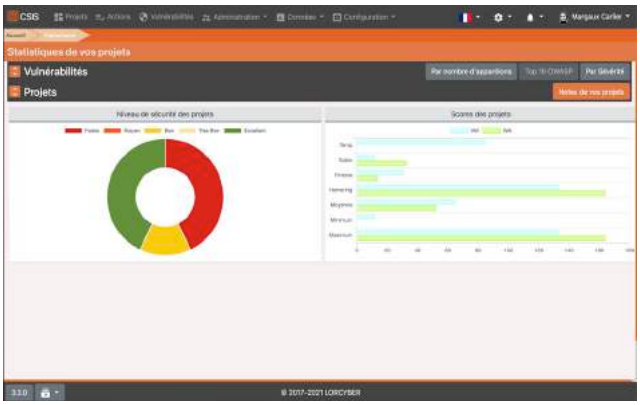


STATISTIQUE POUR UN PROJET

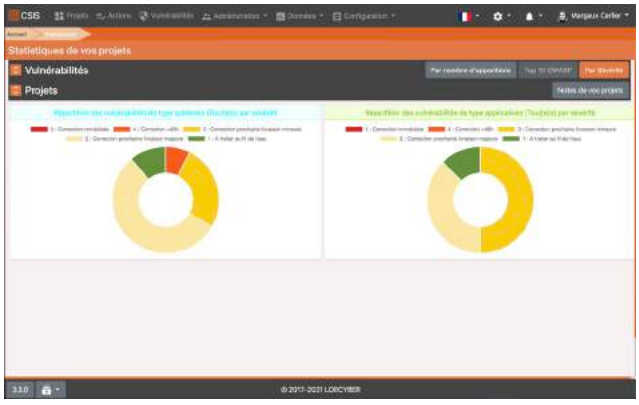
DES STATISTIQUES

Des tableaux de bords sont inclus dans CSIS pour permettre à chaque acteur de connaitre l'avancement de ses tâches.

Un suivi statistique donne l'évolution des corrections pour chaque actif internet suivi.



STATISTIQUES DE VOS PROJETS *(PAR NOTES)*



STATISTIQUES DE VOS PROJETS *(PAR SÉVÉRITÉ)*

Vous avez désormais la possibilité d'obtenir les statistiques de tous les projets avec différentes vues :

- par sévérité
- par nombre d'apparitions
- en fonction du TOP 10 OWASP

BADGE DE SUIVI DE SÉCURITÉ

DES CERTIFICATS

Vous pouvez également mettre en oeuvre une politique de certification interne des sites WEB suivis par CSIS.

Chaque site Internet ou Intranet suivi peut insérer sur ses pages, une icône indiquant le niveau de sécurité du site, un clic amenant sur un certificat en PDF, affichant le détail du suivi.

CERTIFICAT «CLEARNESS»

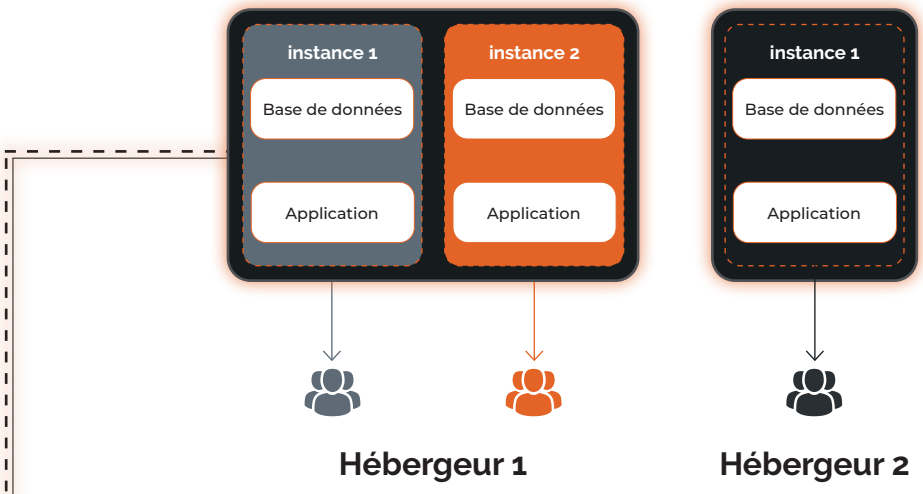
3 niveaux de suivi sont disponibles :

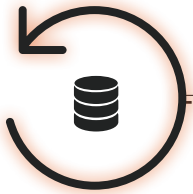
- clearness : la totalité des informations est affichée (avec historique) ;
- obfuscate : un résumé sans historique mais avec le niveau réel est affiché ;
- secretive : seule la date du scan est affichée sans mention de niveau de sécurité.

CERTIFICAT «CLEARNESS»

ZOOM SUR NOTRE
PLATEFORME TECHNIQUE

MULTI-INSTANCE
MULTI-HÉBERGEMENT





SAUVEGARDE
EXTERNALISÉE

DOUBLE
AUTHENTIFICATION

Microsoft - Google
SAML

PLATEFORME TECHNIQUE

Environnement Kubernetes
hébergé en France ou
à l'étranger (OVH, AWS)

Sécurisation renforcée
(chiffrement, authentification
renforcée, piste d'audit...)

UNE SOLUTION QUI S'ADAPTE À VOS BESOINS

Afin de profiter de notre solution de CSIS, nous avons conçu 3 offres annuelles afin de s'adapter au mieux à vos besoins. **La licence choisie correspond au nombre d'actifs que l'on souhaite intégrer,** serveur web **ou** adresse IP

Qualys. Cyberwatch ZAPROXY nessus professional BurpSuite RAPID7

DESCRIPTION DES OFFRES

Utilisateurs

Vous possédez un nombre illimité d'accès utilisateurs IT ou d'analystes cybersécurité.

Instance CSIS dédiée

Concerne l'offre Private, cela vous permet de bénéficier d'une étanchéité totale de votre environnement.

OWASP Zaproxy

En option pour les différentes offres. Cela vous permet de bénéficier à un accès à la plateforme Zaproxy.

vous pouvez retrouver le détail des offres sur: https://csis.app/fr/offers.html

CSIS ON PREMISE

Cette offre vous permet de bénéficier de la licence CSIS **hébergée sur vos serveurs.** Vos ingénieurs en cybersécurité sont autonomes, ils gèrent l'intégralité du processus.

Nous intégrons vos licences de scanners de vulnérabilités dans l'instance mutualisée et accessible uniquement par vos ingénieurs sécurité.

+ En option, vous pouvez bénéficier d'une instance dédiée et de Zaproxy

CSIS HOSTED

Cette offre est **hébergée sur nos serveurs** et permet de bénéficier d'une **instance CSIS mutualisée**. Vous bénéficiez ainsi d'une instance sécurisée. Vos ingénieurs en cybersécurité sont autonomes, ils gèrent l'intégralité du processus.

Nous intégrons vos licences de scanners de vulnérabilités dans l'instance mutualisée et accessible uniquement par vos ingénieurs sécurité.

+ En option, vous pouvez bénéficier d'une instance dédiée et de Zaproxy

CSIS PRIVATE

Cette offre **hébergée sur nos serveurs** et permet de bénéficier d'une **instance CSIS dédiée**. Vous bénéficiez ainsi d'une étanchéité totale de votre environnement. Vos ingénieurs en cybersécurité sont autonomes, ils gèrent l'intégralité du processus.

Nous intégrons vos licences de scanners de vulnérabilités dans votre instance.

+ En option, vous pouvez bénéficier de Zaproxy

LES CERTIFICATIONS CSIS PARTNER

PRÊT À ÊTRE RECONNU POUR VOTRE SAVOIR-FAIRE EN MATIÈRE DE SÉCURITÉ?

1

PROFITEZ D'UNE FORMATION COMPLÈTE CSIS

Vous bénéficierez d'une formation complète vous permettant de suivre les nouvelles fonctionnalités et les mises à jour

2

CONFIRMEZ ET OPTIMISEZ VOS CONNAISSANCES

La certification CSIS vous permet de démontrer votre niveau de connaissance et de monter en compétence quant à l'utilisation de CSIS tout en gagnant du temps!

3

ENRICHISSEZ VOTRE PROPOSITION DE VALEUR ET VOTRE EXPERTISE

En utilisant la plateforme CSIS, vous pourrez proposer à vos clients une expertise enrichie et simplifiée concernant la gestion des vulnérabilités

4

BÉNÉFICIEZ D'UN PARTENARIAT DURABLE

Vous serez bien évidemment formés aux évolutions de la plateforme et ses mises à jour afin de progresser dans vos certifications. Un outil évolutif pour répondre à vos besoins sur le long terme.

Les certifications CSIS visent à démontrer votre niveau de connaissance et d'utilisation de la plateforme SAAS CSIS

La formation pour votre certification vous prépare à installer, configurer et utiliser votre solution CSIS. Vous démontrerez donc votre capacité à utiliser CSIS comme logiciel clé de gestion des vulnérabilités.

4 CERTIFICATIONS DISPONIBLES

CSIS PARTNER comprend 4 types de certifications.
Chaque certification répond à une problématique et à un besoin spécifique.
Les certifications « certified vulnerability scans specialist », « certified pentests specialist » et « certified administrator » requièrent la certification de base « certified analyst ».

CERTIFIED ANALYST

Comment utiliser la plateforme CSIS ?

CERTIFIED VULNERABILITY SCANS SPECIALIST

Comment créer un rapport de scan complet ?

CERTIFIED PENTESTS SPECIALIST

Comment créer un rapport de pentest complet ?

CERTIFIED ADMINISTRATOR

Comment administrer la plateforme CSIS ?

COMMENT DEVENIR PARTENAIRE?

01

Vous devez justifier des connaissances en sécurité afin de pouvoir passer les différentes certifications.

02

Contactez nos équipes afin de nous proposer votre candidature et nous soumettre vos besoins.

https://csis.app/fr/contact.html

03

Nos équipes vous recontacterons afin d'échanger avec vous quant à la faisabilité du partenariat.

04

BÉNÉFICIEZ D'UN
SAVOIR FAIRE DÉMONTRÉ (ET CERTIFIÉ)

SUPPORTS
ET OUTILS

De nombreux supports sont à votre disposition afin de vous aider dans l'utilisation de la plateforme CSIS. Les différentes ressources permettront également à vos collaborateurs de retrouver toutes les informations en ligne grâce à nos différentes pages web.

Site web officiel LORCYBER
pour retrouver une présentation générale de CSIS, de nos différentes offres mais également découvrir notre programme partenaires.
Lien du site web : https://www.csis.app/fr/index.html

Site CSIS Support Center
pour vous aider à mieux comprendre les différentes fonctionnalités de CSIS (uniquement en anglais)
Lien du site web : https://support.csis.app/portal/en/home

Site CSIS Support Center
dispose d'une playlist de tutoriel vidéo dédiée à l'utilisation de CSIS afin de vous guider à travers les différentes fonctionnalités à votre disposition.
Lien du site web : https://support.csis.app/portal/en/home

Services de messagerie et de FAQ
disponibles sur tous nos sites web afin de répondre à toutes vos interrogations
Lien des sites web : https://support.csis.app/portal/en/home
https://www.csis.app/fr/index.html
https://www.lorcyber.eu/fr/index.html

CSIS

LORCYBER

À PROPOS DE LORCYBER

LORCYBER est un cabinet de conseil et éditeur de logiciel spécialisé dans la cybersécurité. Nous souhaitons rendre accessible la cybersécurité en amenant notre expérience des grands groupes.

Concrètement nous voulons baisser les coûts de la cybersécurité pour une même qualité de service en apportant un service industriel de qualité. Parce que vos besoins ne sont pas forcément les mêmes, nous avons créée des offres packagées afin de répondre au mieux à vos attentes.

Packages et Conseils : https://www.lorcyber.eu/fr/services.html

E-learning et Formation : https://www.lorcyber.eu/fr/formation.html

Nous avons également développé une plateforme SAAS pour gérer de manière centrale et simplifiée la sécurité de nos clients.
La plateforme CSIS « Computer Security Information System » vous aide à obtenir une vision à 360° de vos failles de sécurité.

Construisons ensemble votre cyber-sérénité

DÉCOUVREZ LE LOGICIEL CSIS

DEMANDEZ UNE DÉMO SUR CSIS.APP