PRÉSENTATION
CVOC

CONSTRUISONS
ENSEMBLE
VOTRE
CYBER-SÉRÉNITÉ

LORCYBER

SOMMAIRE

CVOC par LORCYBER

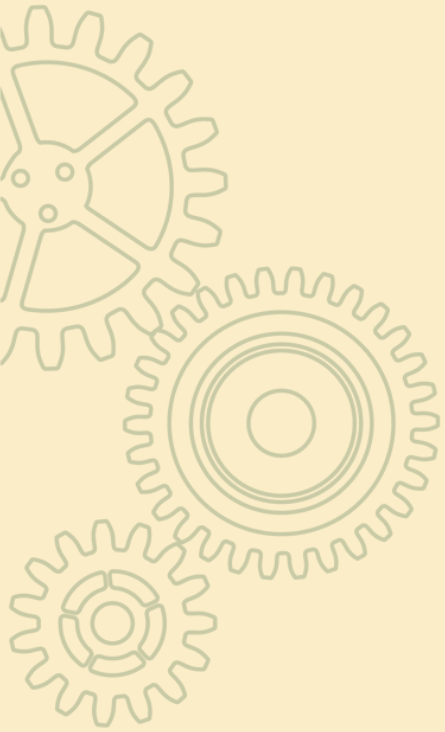
Afin d'industrialiser la cybersécurité, LORCYBER développe une plateforme SAAS à partir d'outils OpenSource pour gérer de manière centrale et simplifiée, la sécurité de ses clients.

La plateforme CVOC « Cyber Vulnerabilities Operation Center », 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**.**



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.

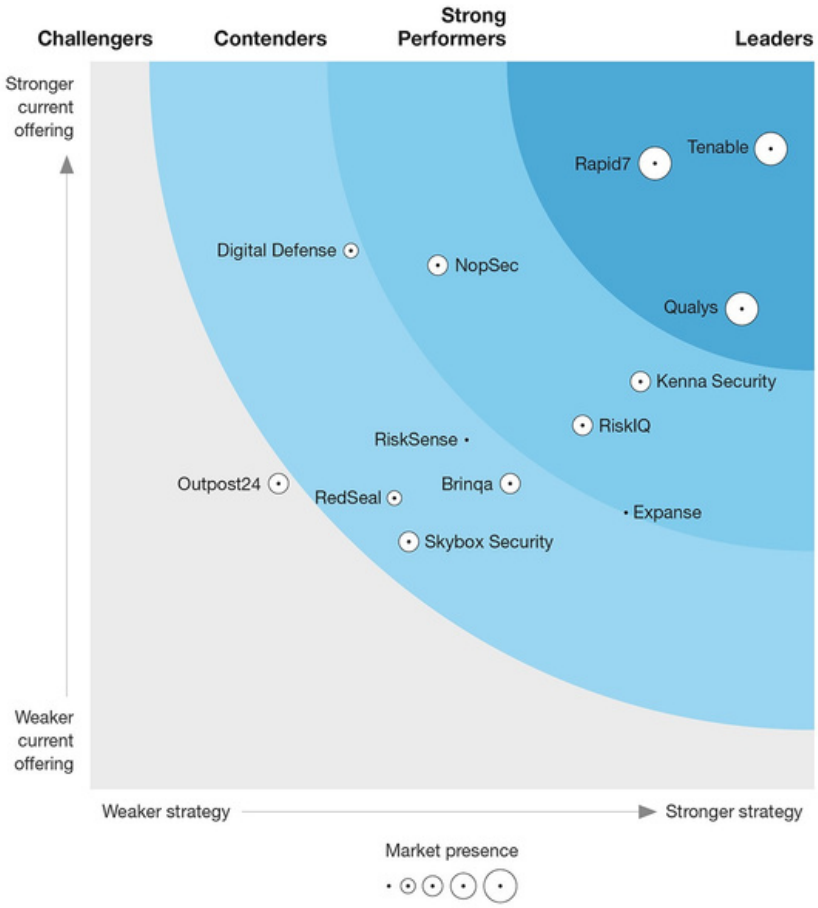
Ce plan d'actions doit également inclure, un volet «gestion de risques», certaines vulnérabilités pouvant être acceptées, si leur probabilité de survenance est faible, ou si l'impact est négligeable.

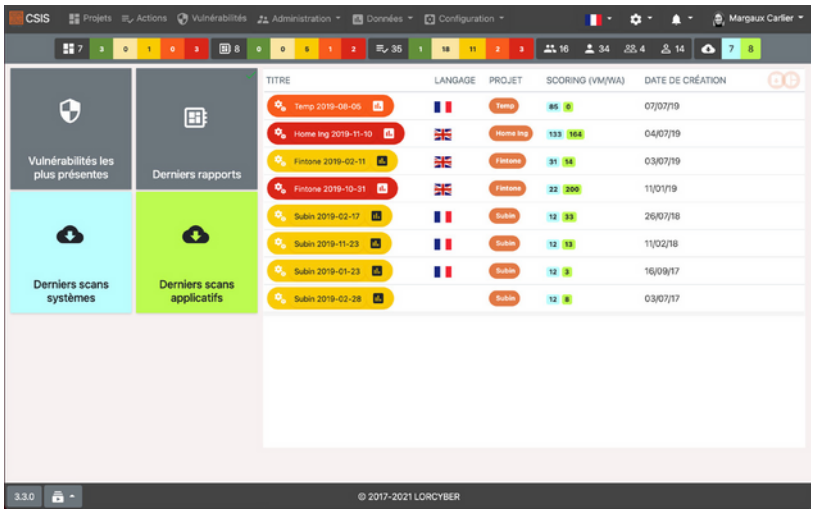
4 TABLEAU DE BORD ET SUIVI

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.

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 CVOC avec plusieurs leaders du marché du scan de vulnérabilités avec plusieurs leaders du marché du scan de vulnérabilités : Qualys, Rapid7, Cyberwatch, Zaproxy, Tenable (Nessus) et PortSwigger (Burp Suite)

4

Sur CVOC, 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 CVOC

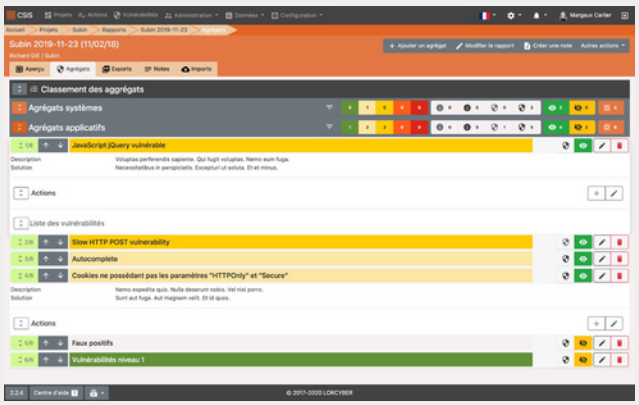
RAPIDITÉ / CLARTÉ / ACCESSIBILITÉ

OUTIL INTÉGRÉ

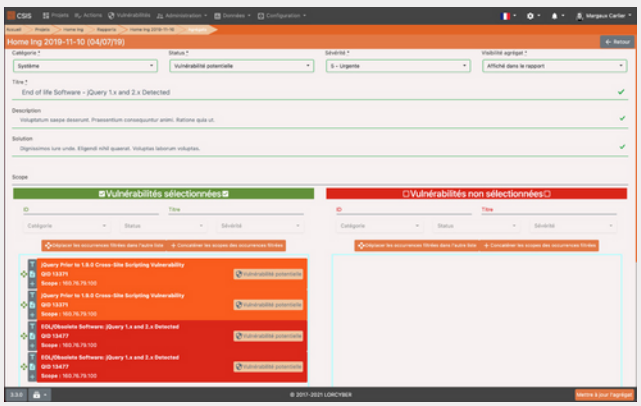
CVOC intègre le résultat des scans lancés sous votre scanner de vulnérabilités (Qualys, Rapid7, ...), et vous permet de créer vos rapports d'analyse de manière simple. Les ingénieurs sécurité ne se concentrent que sur l'analyse et la description des solutions à apporter.

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

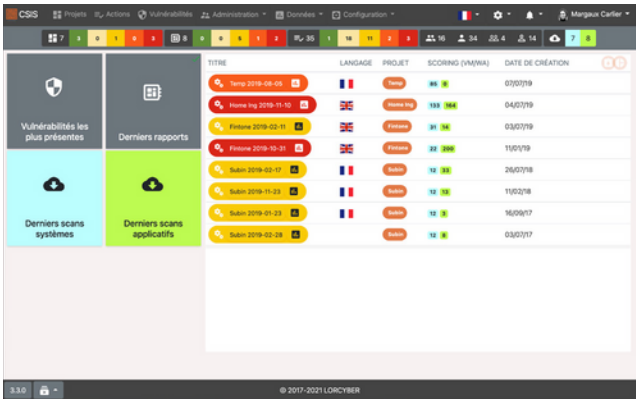
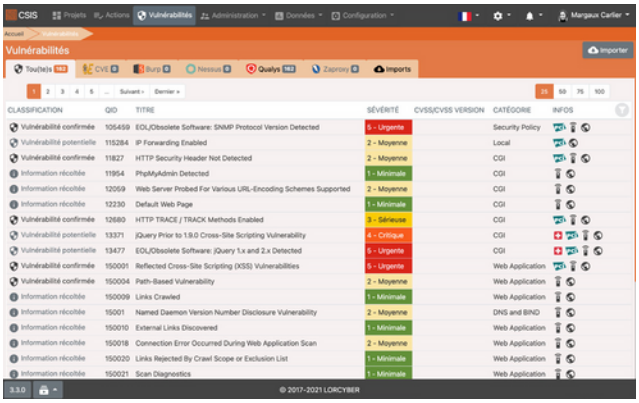
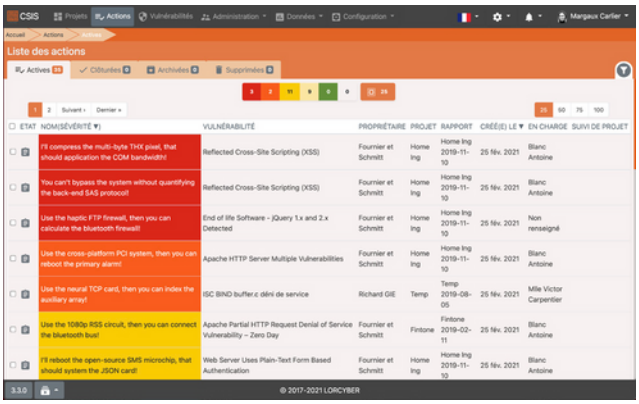


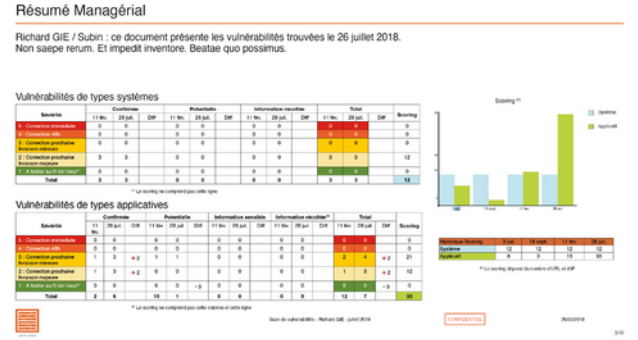
TABLEAU DE BORD PERSONNALISABLE



EXPLOREZ NOS BASES DE VULNÉRABILITÉS



LISTE DES ACTIONS



RÉSUMÉ MANAGÉRIAL

2 INTERFACES

Ingénieur Cybersécurité (pour l'analyse)
& Utilisateur (pour le suivi des corrections)

3 TYPES DE RAPPORTS

- Pentests
- Scans de vulnérabilités
- Imports de fichier Excel

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

SCANNERS DISPONIBLES

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

OUTILS DE TICKETING DISPONIBLES

Plateforme connectée à plusieurs outils de ticketing : Jira, ServiceNow, Matrix42

EXPORT DES RAPPORTS EN PDF

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

OUTIL EFFICACE

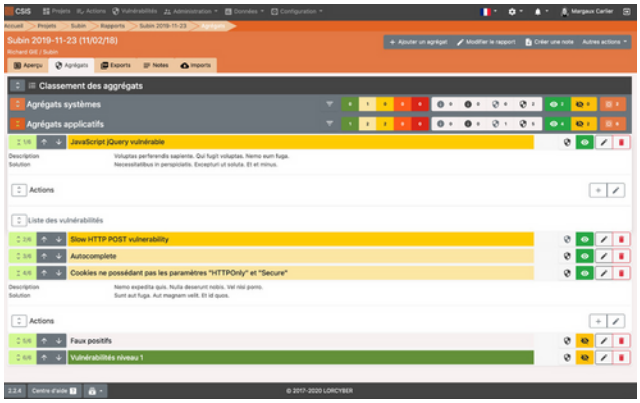
Le moteur de gestion des agrégats* de vulnérabilités permet de diviser jusqu'à 7 fois le temps passé sur chaque rapport.

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 his- toriques.

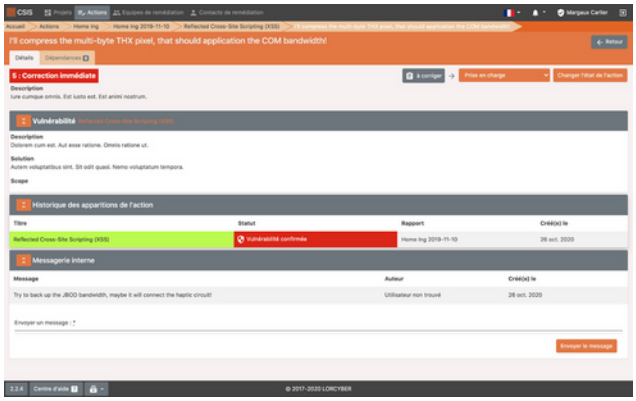
De plus, son interface multilingue, vous permet dans une organisation internationale de délivrer vos rapports dans la langue de vos interlocuteurs. L'analyse et la génération du rapport par nos équipes est effectuée en moins de deux heures en moyenne !

La description des actions de correc- tions peut ensuite être réalisée par nos équipes.

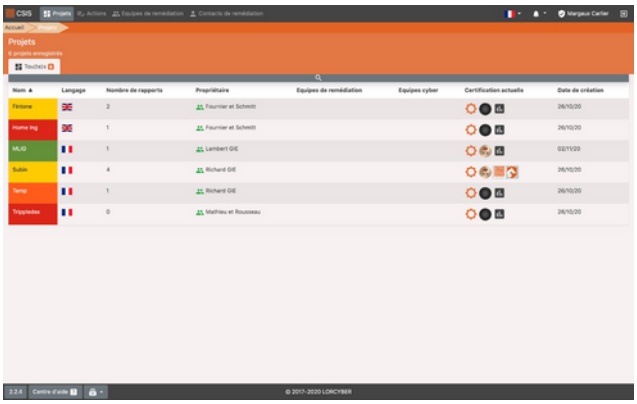
En une demi-journée, les équipes informatiques auront à disposition le rapport, ainsi que le tableau de suivi des actions de corrections dans leur interface utilisateur.



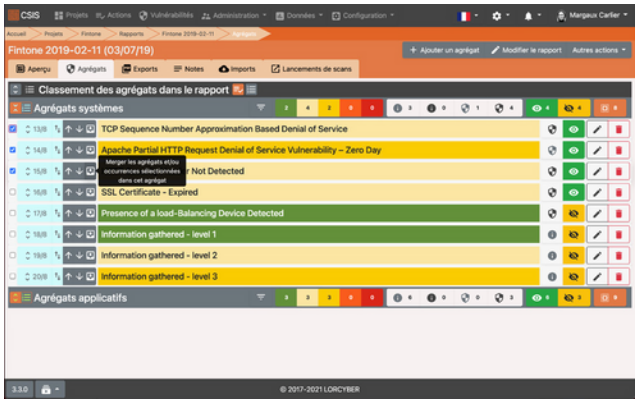
LISTE DES AGRÉGATS



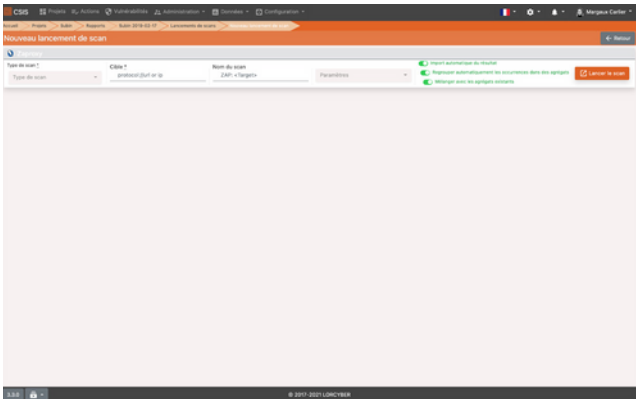
DÉTAIL D'UNE ACTION DE CORRECTION



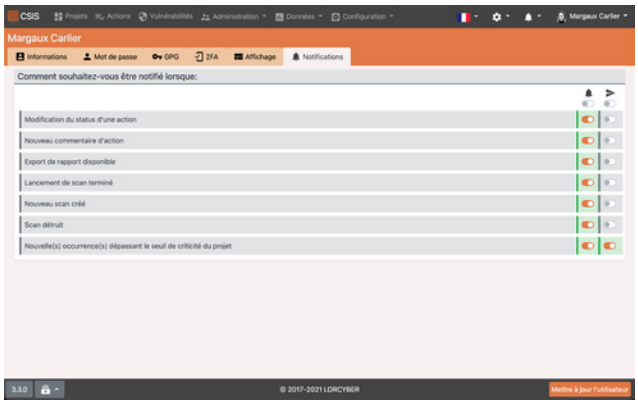
INTERFACE UTILISATEUR RAPPORTS



FUSION DES AGRÉGATS



LANCEMENT D'UN SCAN



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 !

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

AVEC SUIVI OPTIMISÉ DES CORRECTIONS

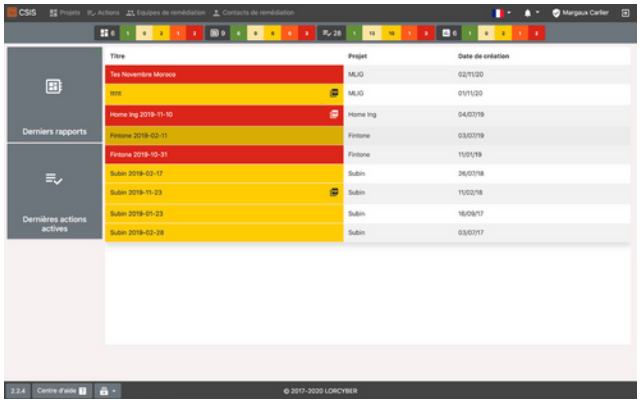
Les actions de corrections étant saisies également sous CVOC, l'ingénieur peut affecter, action par action, celles-ci à une équipe informatique.

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

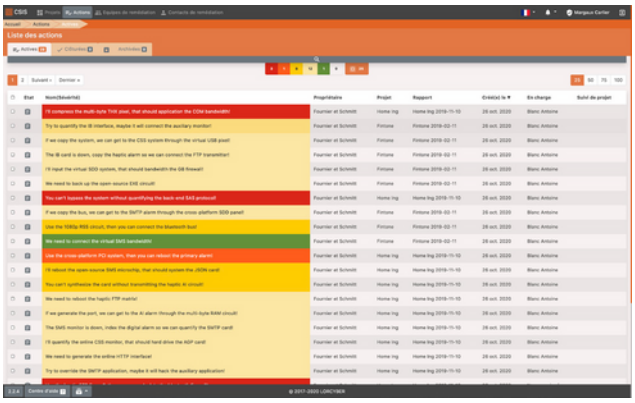
Une fois la correction effectuée, un workflow de validation est mis en oeuvre, sous le contrôle des ingénieurs sécurité en charge.

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

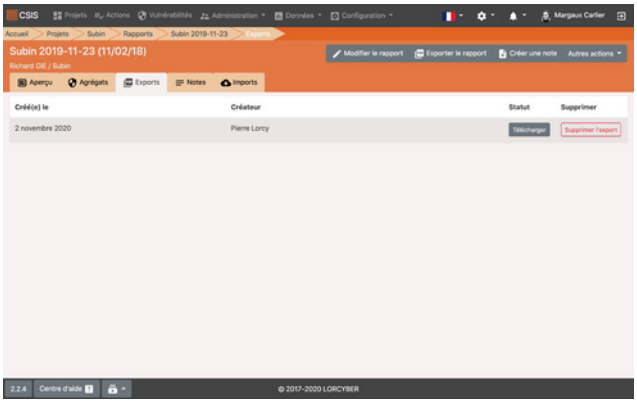
Un système de juridiction permet de ne montrer à chaque équipe que les actions qui les concernent.



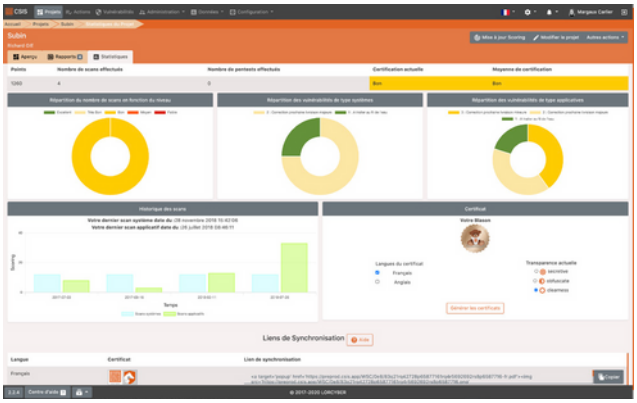
PAGE D'ACCUEIL ÉQUIPE IT



LISTE DES ACTIONS DE CORRECTIONS



INTERFACE DE GÉNÉRATION DES RAPPORTS

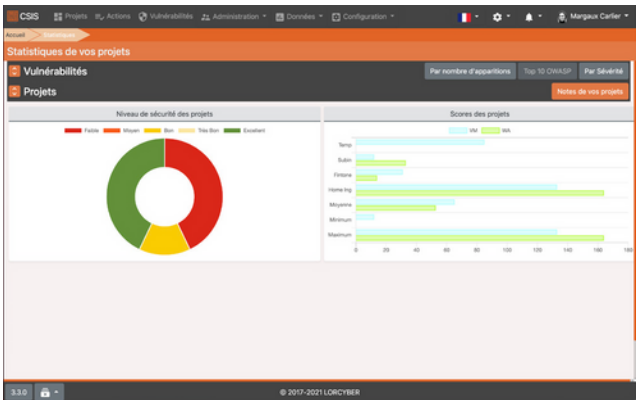


STATISTIQUE POUR UN PROJET

DES STATISTIQUES

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

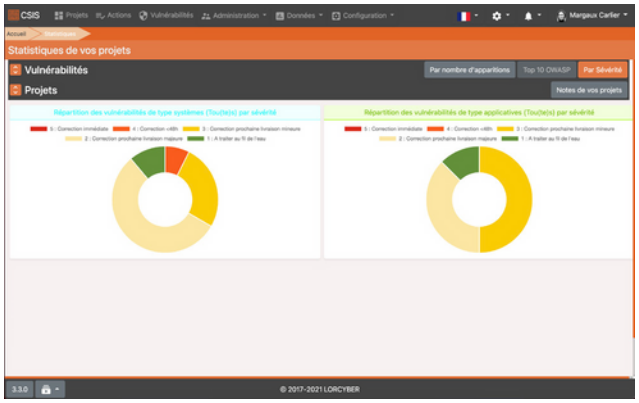
Un suivi statistique donne l'évolution des corrections pour chaque actif internet suivi.



STATISTIQUES DE VOS PROJETS*(PAR NOTES)*

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



STATISTIQUES DE VOS PROJETS*(PAR SÉVÉRITÉ)*

BADGE DE SUIVI DE SÉCURITÉ

DES CERTIFICATS

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

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»

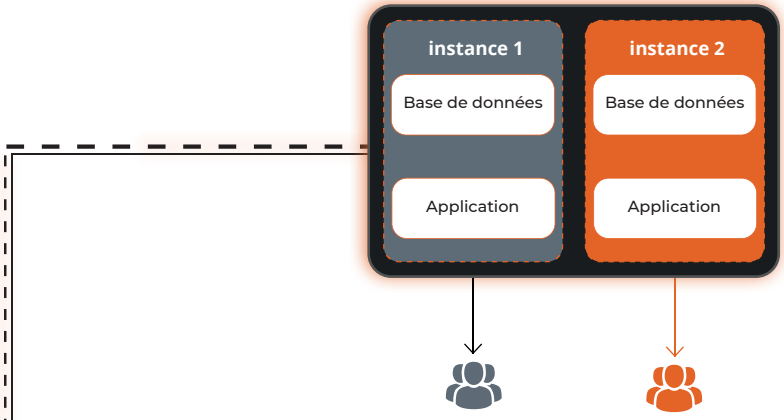
CERTIFICAT «CLEARNESS»

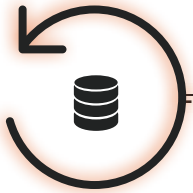
3 niveaux de suivi sont disponibles :

- 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.

ZOOM SUR NOTRE
PLATEFORME TECHNIQUE

MULTI-INSTANCE





SAUVEGARDE
EXTERNALISÉE

DOUBLE
AUTHENTIFICATION

Microsoft - Google
SAML

OASIS OPEN

PLATEFORME TECHNIQUE

Environnement
Kubernetes hébergé en
France (OVH)

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

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.

https://www.lorcyber.eu/

contact@lorcyber.eu

Avril 2024