



PRÉSENTATION CVOC

CONSTRUISONS
ENSEMBLE
VOTRE
CYBER-SÉRÉNITÉ



LORCYBER

SOMMAIRE

3

CVOC PAR LORCYBER

4

QUELLES PROBLÉMATIQUES ?

6

LA SOLUTION CVOC

13

NOTRE PLATEFORME TECHNIQUE

CVOC par LORCYBER

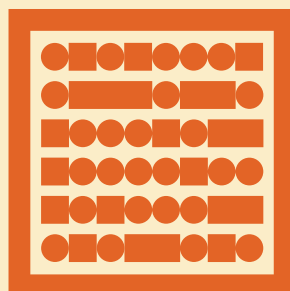
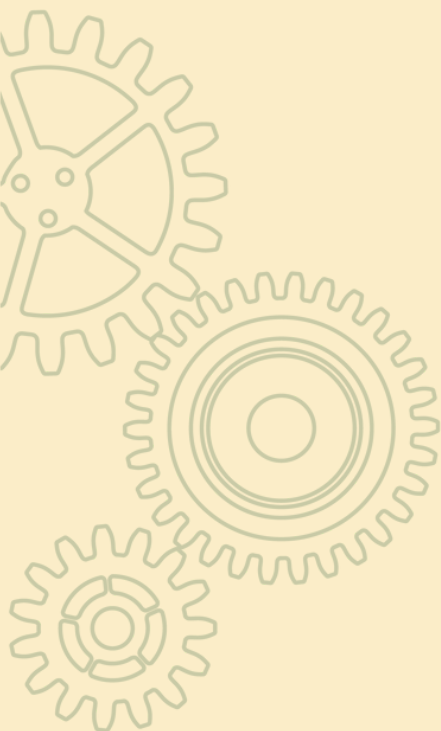
Afin d'industrialiser la cybersécurité, LORCYBER développe une plateforme SAAS à partir d'outils OpenSource pour gérer de manière centrale et simplifiée, la sécurité de ses clients.

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 distribués 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.

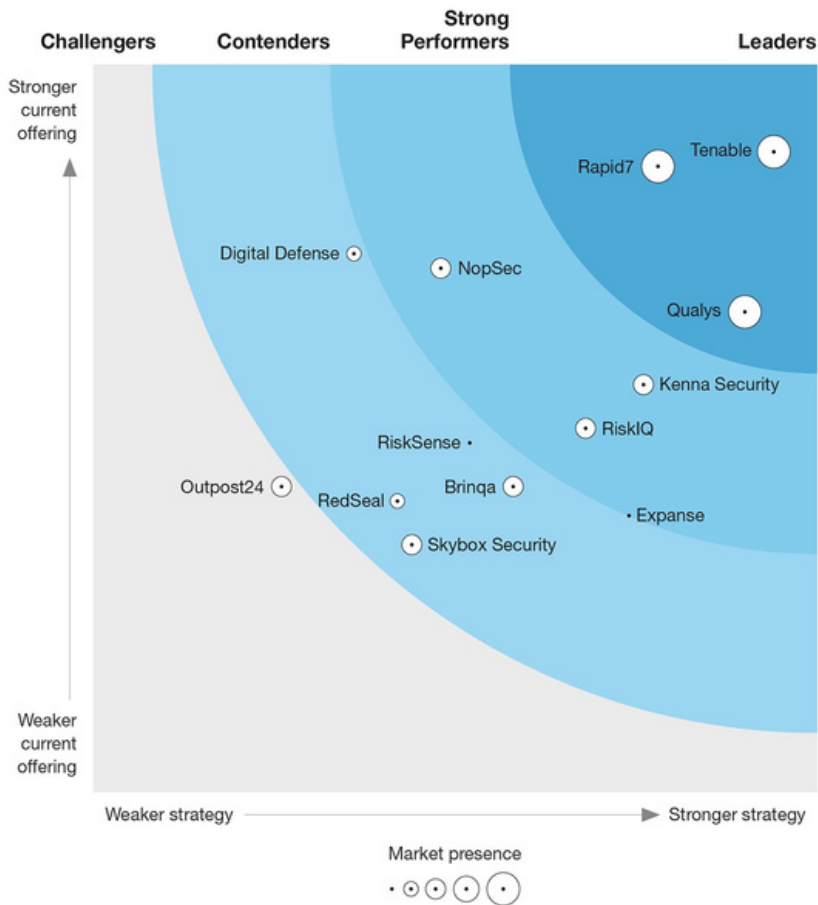
Ce plan d'actions doit également inclure, un volet «gestion de risques», certaines vulnérabilités pouvant être acceptées, si leur probabilité de survenance est faible, ou si l'impact est négligeable.

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 Vulnerability Risk Management



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.

TITRE	LANGUE	PROJET	SCORING (VM/WA)	DATE DE CRÉATION
Temp 2019-09-06	FR	Temp	85 8	07/07/19
Home Ing 2019-11-10	FR	Home Ing	133 164	04/07/19
Finlane 2019-02-11	FR	Finlane	31 14	03/07/19
Finlane 2019-10-31	FR	Finlane	22 200	11/01/19
Subin 2019-02-12	FR	Subin	12 33	26/07/18
Subin 2019-11-23	FR	Subin	12 33	11/02/18
Subin 2019-01-23	FR	Subin	12 3	16/09/17
Subin 2019-02-28	FR	Subin	12 8	03/07/17

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

LA SOLUTION CVOC

RAPIDITÉ / CLARTÉ / ACCESSIBILITÉ

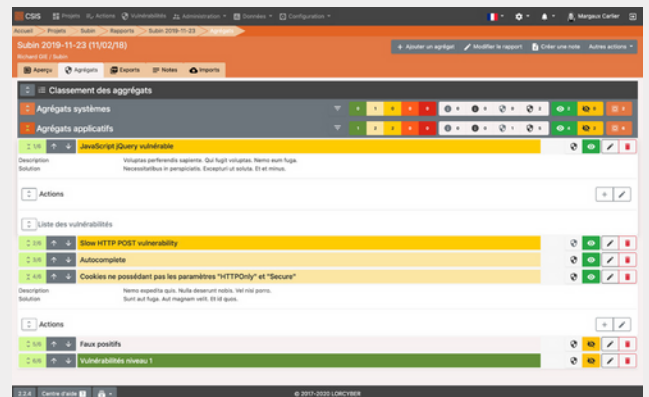


OUTIL INTÉGRÉ

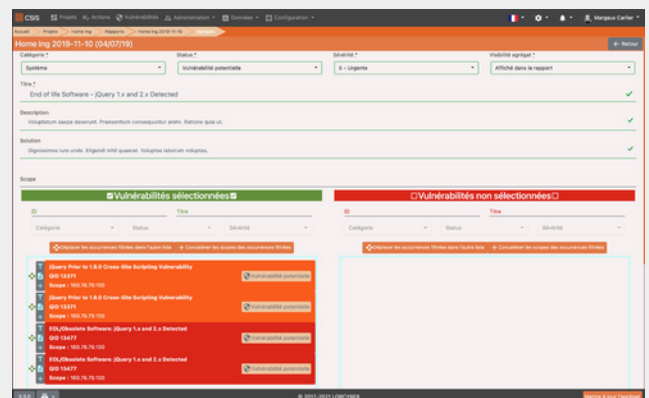
CVOC intègre le résultat des scans lancés sous votre scanner de vulnérabilités (Qualys, Rapid7, ...), et vous permet de créer vos rapports d'analyse de manière simple. Les ingénieurs sécurité ne se concentrent que sur l'analyse et la description des solutions à apporter.

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

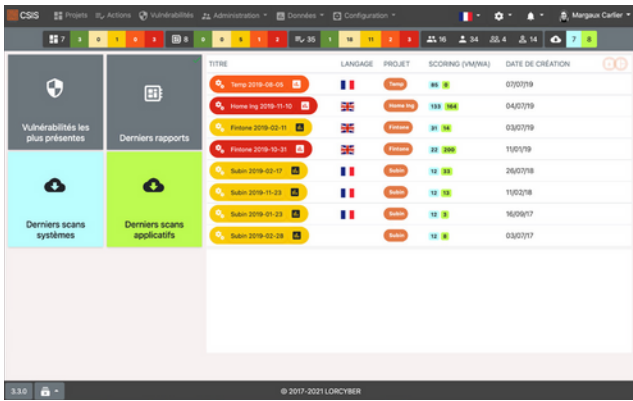
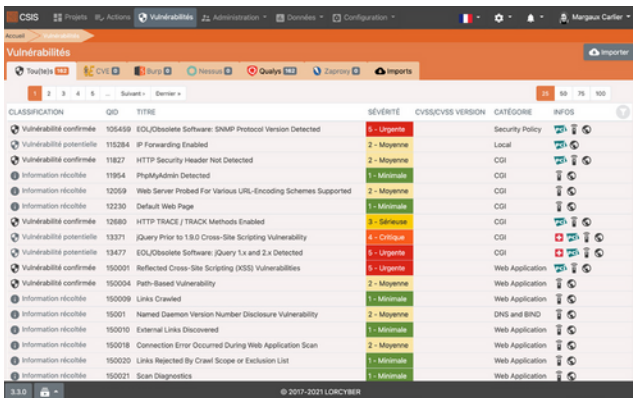
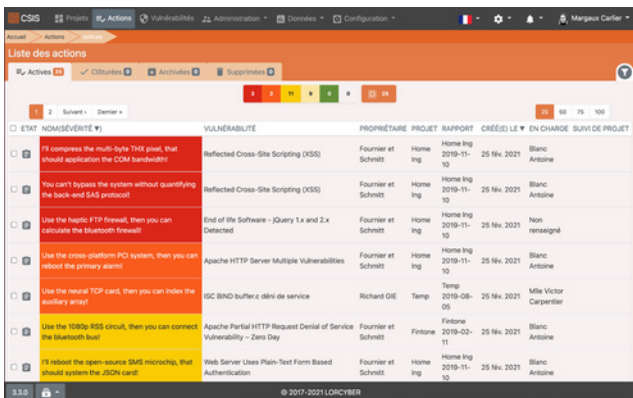


TABLEAU DE BORD PERSONNALISABLE



EXPLOREZ NOS BASES DE VULNÉRABILITÉS



LISTE DES ACTIONS

Résumé Managérial

Richard GiE / Subin ; ce document présente les vulnérabilités trouvées le 26 juillet 2018. Non saepe rerum. Et impedit inventore. Beatae quo possimus.



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

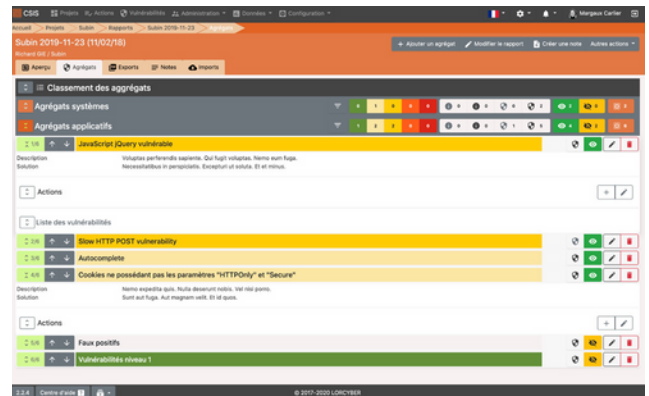
Le moteur de gestion des **agrégats*** de vulnérabilités permet de **diviser jusqu'à 7 fois le temps passé sur chaque rapport**.

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 historiques.

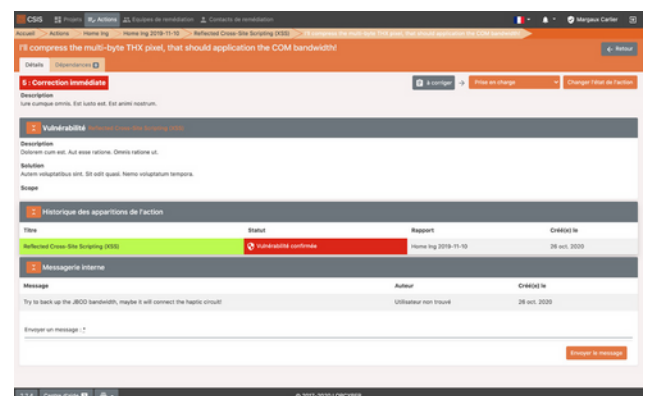
De plus, son interface multilingue, vous permet dans une organisation internationale de **délivrer vos rapports dans la langue de vos interlocuteurs**. L'analyse et la génération du rapport par nos équipes est effectuée en moins de deux heures en moyenne !

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

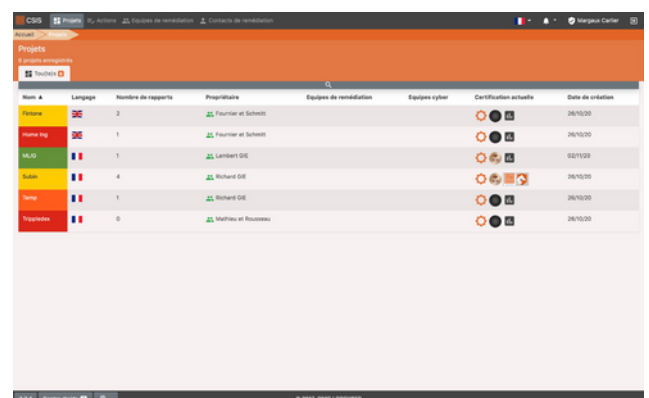
En une demi-journée, les équipes informatiques auront à disposition le rapport, ainsi que le tableau de suivi des actions de corrections dans leur interface utilisateur.



LISTE DES AGRÉGATS



DÉTAIL D'UNE ACTION DE CORRECTION



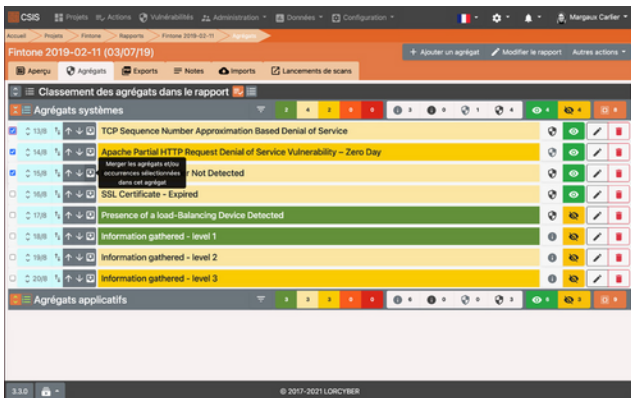
INTERFACE UTILISATEUR RAPPORTS

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

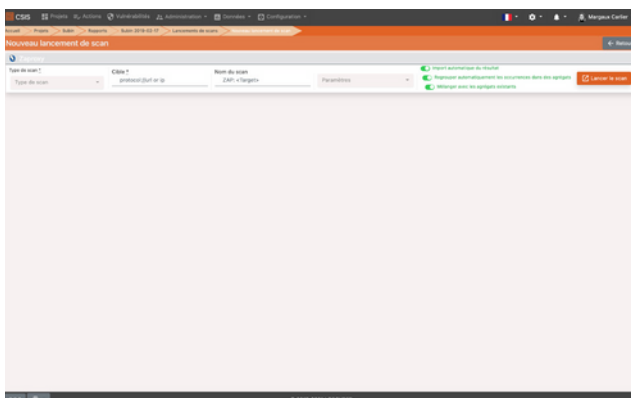
Dorénavant, recevez des notifications d'alertes via mail, dans l'application interne, ou bien sur vos outils collaboratifs préférés (Teams, Slack, Zoho ou Google Chat).

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

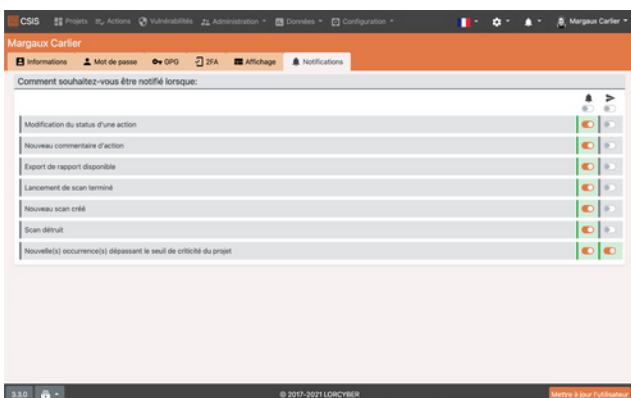
- Modification du statut d'une action
- Nouveau commentaire d'action
- Export de rapport disponible
- Lancement de scan terminé
- Nouveau scan créé
- Scan détruit
- Nouvelle(s) occurrence(s) dépassant le seuil de criticité du projet



FUSION DES AGRÉGATS



LANCEMENT D'UN SCAN



PARAMÉTRAGE DES NOTIFICATIONS



Slack



Google Chat



Zoho



Teams



AVEC SUIVI OPTIMISÉ DES CORRECTIONS

Les actions de corrections étant saisies également sous CVOOC, 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.

Titre	Projet	Date de création
Les Nouveaux Menus	MLIO	02/11/20
Home Ing 2019-11-10	Home Ing	04/07/19
Finions 2019-02-11	Finions	03/07/19
Finions 2019-05-31	Finions	15/01/19
Subin 2019-02-17	Subin	26/07/18
Subin 2019-11-23	Subin	11/02/18
Subin 2019-01-23	Subin	16/09/17
Subin 2019-02-28	Subin	03/07/17

PAGE D'ACCUEIL ÉQUIPE IT

Stat	Responsabilité	Projet	Rapport	Créé le	En charge	Statut de projet
🔍	To complete the multi-Lyre 700 panel, that should activate the CDR bandwidth	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	To fix the issue of the interface, make it all control the auxiliary device	Fourier at Schindler	Finions	Finions 2019-02-11	26 oct. 2020	Blanc Antenne
🔍	Plan with the system, we can get to the CDR system through the virtual SDP panel	Fourier at Schindler	Finions	Finions 2019-02-11	26 oct. 2020	Blanc Antenne
🔍	The @ card is blank, only the North alarm is not connected to the PIP controller	Fourier at Schindler	Finions	Finions 2019-02-11	26 oct. 2020	Blanc Antenne
🔍	To read the virtual SDP system, that should bandwidth the SDP board	Fourier at Schindler	Finions	Finions 2019-02-11	26 oct. 2020	Blanc Antenne
🔍	We need to back up the open source CDR circuit	Fourier at Schindler	Finions	Finions 2019-02-11	26 oct. 2020	Blanc Antenne
🔍	We can't bypass the system without specifying the base and SDP protocol	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	If we copy the bus, we can get to the SDP alarm through the cross platform SDP panel	Fourier at Schindler	Finions	Finions 2019-02-11	26 oct. 2020	Blanc Antenne
🔍	Use the 70000-800 circuit, that can connect the bandwidth board	Fourier at Schindler	Finions	Finions 2019-02-11	26 oct. 2020	Blanc Antenne
🔍	We need to connect the virtual SDP bandwidth	Fourier at Schindler	Finions	Finions 2019-02-11	26 oct. 2020	Blanc Antenne
🔍	Use the cross platform CDR system, that you can release the primary alarm	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	To bypass the open source CDR controlling, that should control the 2000 card	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	The card bandwidth will not allow controlling the width of circuit	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	We need to release the North PIP control	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	If we generate the part, we can get to the @ alarm through the multi-Lyre 800 circuit	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	The SDP monitor is blank, when the digital alarm is not connected to the SDP card	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	To quantify the entire CDR monitor, that should read down the SDP card	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	We need to generate the entire 7174 interface	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne
🔍	To connect the SDP application, make it all have the auxiliary application	Fourier at Schindler	Home Ing	Home Ing 2019-11-10	26 oct. 2020	Blanc Antenne

LISTE DES ACTIONS DE CORRECTIONS

Subin 2019-11-23 (11/02/18)

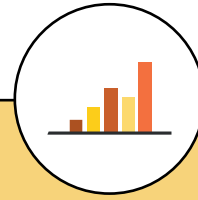
Créé le: 2 novembre 2020

Créateur: Pierre Lorcy

Statut: [Modifier le rapport] [Exporter le rapport] [Créer une note] [Autres actions]

Supprimer le rapport

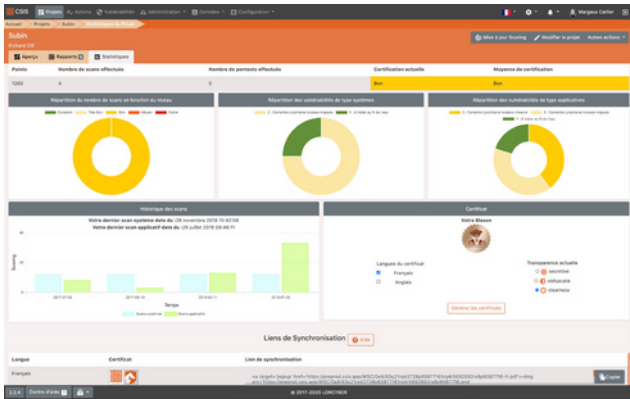
INTERFACE DE GÉNÉRATION DES RAPPORTS



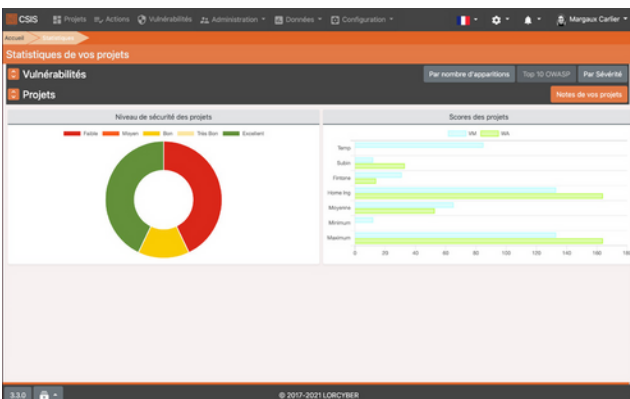
DES STATISTIQUES

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

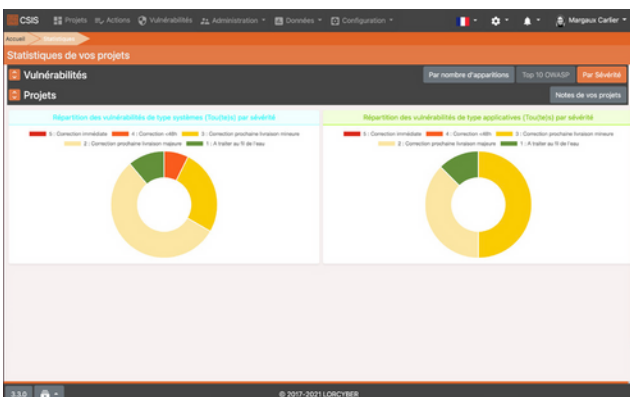
Un suivi statistique donne l'évolution des corrections pour chaque actif internet suivi.



STATISTIQUE POUR UN PROJET



STATISTIQUES DE VOS PROJETS(PAR NOTES)

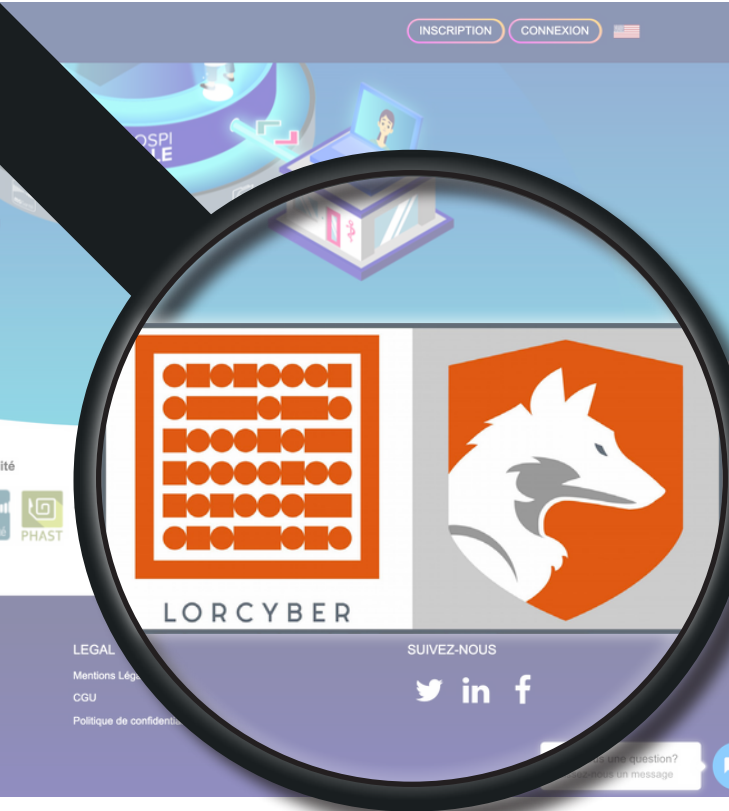


STATISTIQUES DE VOS PROJETS(PAR SÉVÉRITÉ)

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



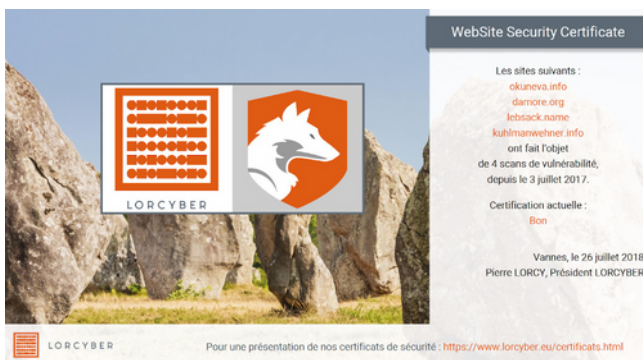
BADGE DE SUIVI DE SÉCURITÉ



DES CERTIFICATS

Vous pouvez également mettre en oeuvre une **politique de certification interne des sites WEB suivis 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»

3 niveaux de suivi sont disponibles :

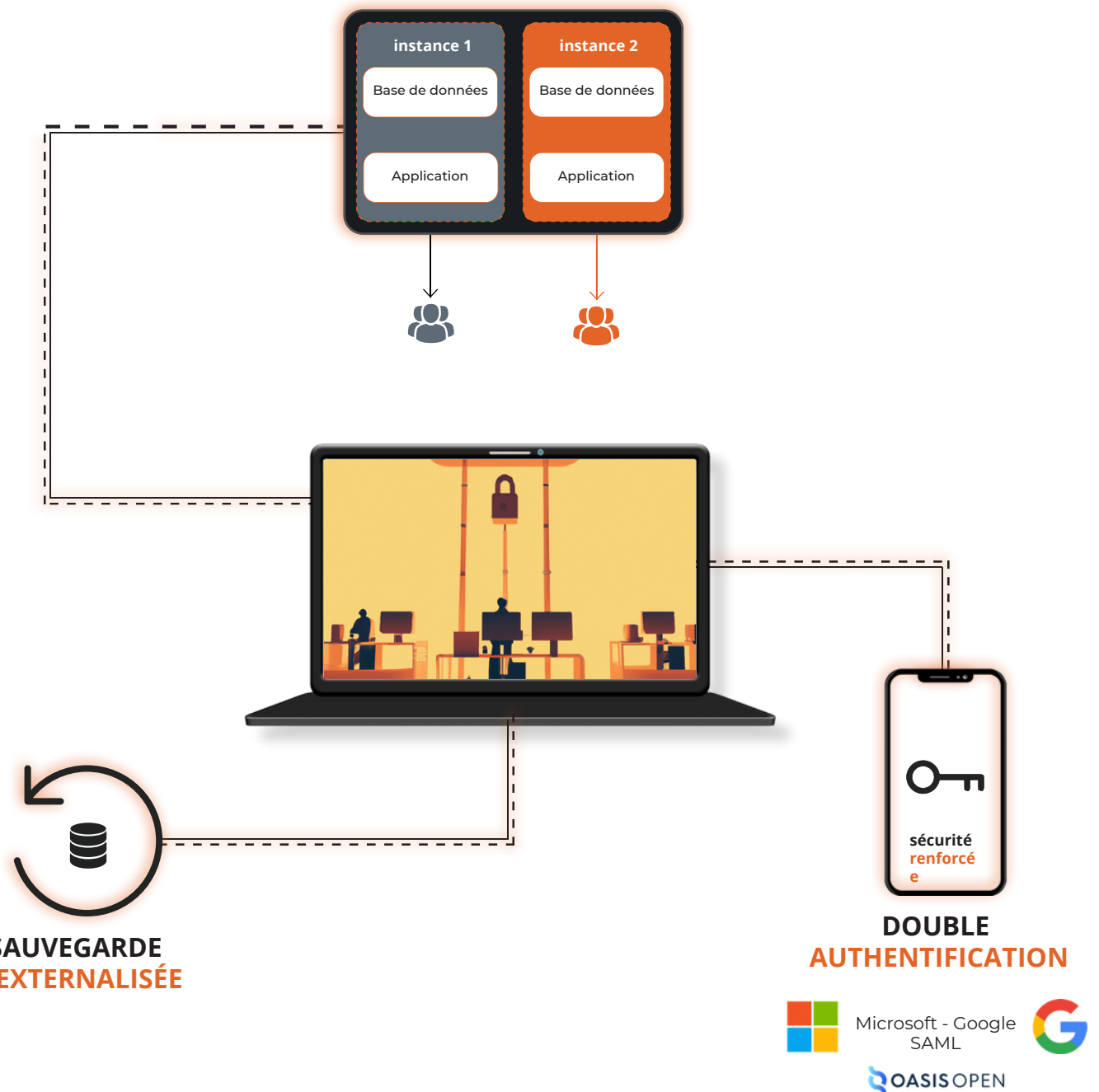
- **clearness** : la totalité des informations est affichée (avec historique) ;
- **obfuscate** : un résumé sans historique mais avec le niveau réel est affiché ;
- **secretive** : seule la date du scan est affichée sans mention de niveau de sécurité.



CERTIFICAT «CLEARNESS»

ZOOM SUR NOTRE PLATEFORME TECHNIQUE

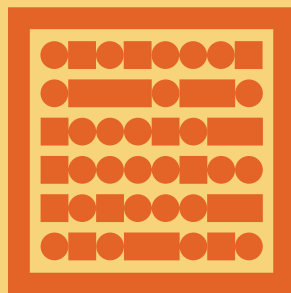
MULTI-INSTANCE



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 créé des offres packagées afin de répondre au mieux à vos attentes.

<https://www.lorcyber.eu/>

contact@lorcyber.eu