

CSL Sécurisation

CyberSmartLearn, est un logiciel de cybersécurité innovant conçu par Aphelio. CSL Sécurisation est une solution complète réalisant le maintien en condition de sécurité (MCS) des équipements, elle scanne les potentielles vulnérabilités, calcule leur niveau de criticité et vous propose des solutions de remédiation. CSL s'adapte aux environnements de toutes tailles et existe en format matériel ou logiciel.

Ce module propose un MCS sur des équipements dédiés aux métiers :

- Transport (borne d'appels d'urgence, PMV, IoT, péage, billettique, supervision, automates...)
- Sûreté (caméras, VMS, stockeur, gestionnaire de contrôle d'accès, UTL...)
- Industrie 4.0 (Scada, automates, capteurs, PC industriel...)
- Smart City (IoT, GTC, GTB, feux de signalisation, vidéoprotection, bornes escamotables, parking...)

CSL permet ainsi d'augmenter la disponibilité de l'installation surveillée, d'éviter certains risques majeurs (fuite de données, intégrité des données...) et de mesurer la bonne tenue du contrat de maintenance par l'opérateur. Il permet également d'avoir une visibilité claire de l'inventaire logiciel et matériel mais également de se conformer aux recommandations de l'ANSSI sur la sécurité des systèmes métiers.

Avantages de CSL

Indépendance

Possibilité de s'affranchir d'experts cyber

Facilité

Déploiement et maintenance facilités

Souveraineté

Solution 100% française

Assurance

Technologie brevetée

Adaptabilité

Adaptation de la plateforme à votre installation existante

Ergonomie

Solution ergonomique et agréable d'utilisation

Robustesse

Plateforme robuste et évolutive

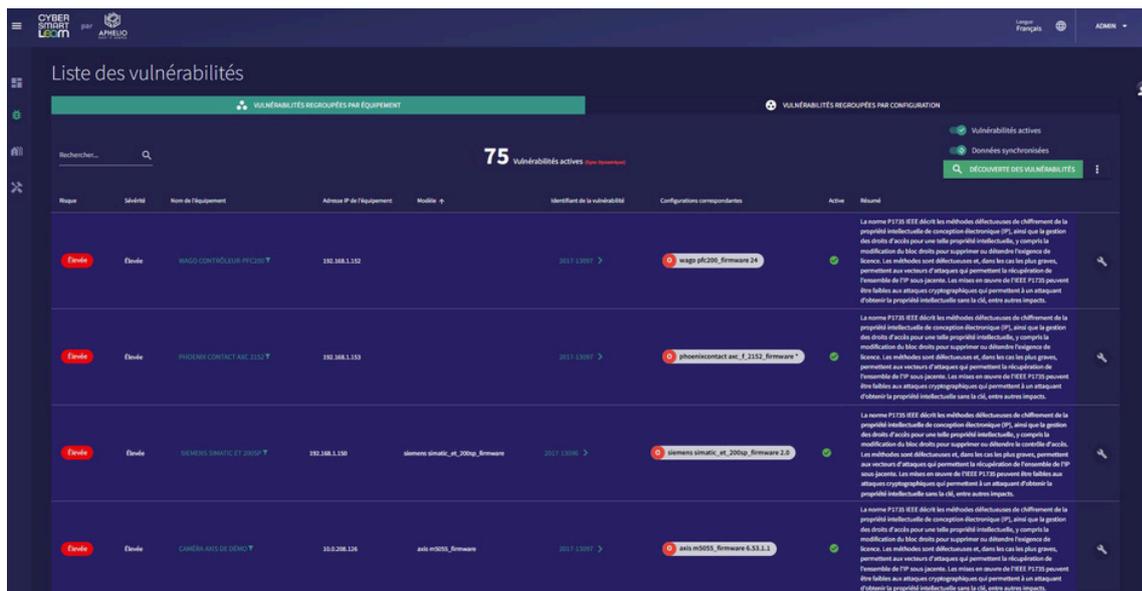
Instantanéité

Calcul du risque en temps réel



Gestion des vulnérabilités

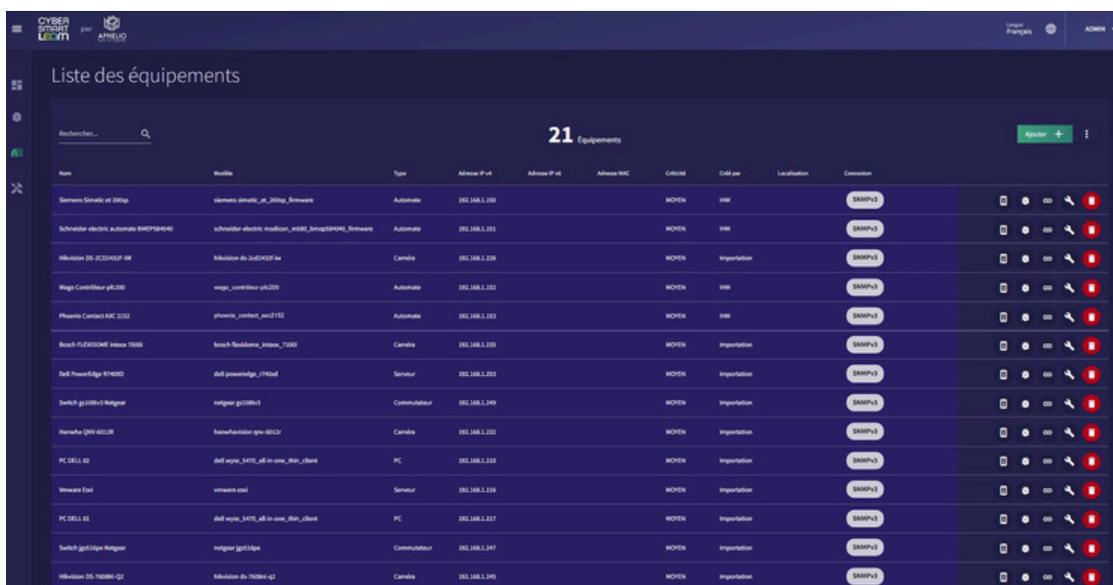
CSL Sécurisation effectue une veille technologique et possède une base de données comprenant les constructeurs, les éditeurs et les agences tels que CERT-FR et NIST. Il vise à identifier les vulnérabilités dans les domaines de l'IT, OT, IoT et de la sûreté tout en évaluant la sévérité de ces vulnérabilités selon l'équipement concerné et suggère des solutions de remédiation.



Risque	Sévérité	Nom de l'équipement	Adresse IP de l'équipement	Modèle	Identifiant de la vulnérabilité	Configurations correspondantes	Acte	Résumé
Élevée	Élevée	WAGO CONTRÔLEUR PID20T	192.168.1.132		2017-13007	Wago pID20_ firmware 24	✓	La norme P1372 IEEE décrit les méthodes d'effacement de chiffrement de la propriété intellectuelle de conception électronique (IP), ainsi que la gestion des droits d'accès pour une telle propriété intellectuelle, y compris la modification du bloc droits pour supprimer ou déstabiliser l'urgence de BootX. Les méthodes sont différentes et, dans les cas les plus graves, permettent au vecteur d'attaque qui permet la récupération de l'ensemble de TP sous jacent. Les mises en œuvre de TEE P1372 peuvent être faibles aux étapes d'implémentation qui permettent à un attaquant d'évaluer la propriété intellectuelle sans la CSL, contre autres impacts.
Élevée	Élevée	PHOENIX CONTACT AXC1312T	192.168.1.133		2017-13007	Phoenixcontact axc_1_1312_ firmware 7	✓	La norme P1372 IEEE décrit les méthodes d'effacement de chiffrement de la propriété intellectuelle de conception électronique (IP), ainsi que la gestion des droits d'accès pour une telle propriété intellectuelle, y compris la modification du bloc droits pour supprimer ou déstabiliser l'urgence de BootX. Les méthodes sont différentes et, dans les cas les plus graves, permettent au vecteur d'attaque qui permet la récupération de l'ensemble de TP sous jacent. Les mises en œuvre de TEE P1372 peuvent être faibles aux étapes d'implémentation qui permettent à un attaquant d'évaluer la propriété intellectuelle sans la CSL, contre autres impacts.
Élevée	Élevée	SIEMENS SIMATIC 300SP T	192.168.1.130	siemens simatic_et_200sp_ firmware	2017-13006	siemens simatic_et_200sp_ firmware 2.0	✓	La norme P1372 IEEE décrit les méthodes d'effacement de chiffrement de la propriété intellectuelle de conception électronique (IP), ainsi que la gestion des droits d'accès pour une telle propriété intellectuelle, y compris la modification du bloc droits pour supprimer ou déstabiliser l'urgence de BootX. Les méthodes sont différentes et, dans les cas les plus graves, permettent au vecteur d'attaque qui permet la récupération de l'ensemble de TP sous jacent. Les mises en œuvre de TEE P1372 peuvent être faibles aux étapes d'implémentation qui permettent à un attaquant d'évaluer la propriété intellectuelle sans la CSL, contre autres impacts.
Élevée	Élevée	CAMERA AXIS DE GENIY T	192.168.1.126	axis m3055_ firmware	2017-13007	axis m3055_ firmware 6.53.1.1	✓	La norme P1372 IEEE décrit les méthodes d'effacement de chiffrement de la propriété intellectuelle de conception électronique (IP), ainsi que la gestion des droits d'accès pour une telle propriété intellectuelle, y compris la modification du bloc droits pour supprimer ou déstabiliser l'urgence de BootX. Les méthodes sont différentes et, dans les cas les plus graves, permettent au vecteur d'attaque qui permet la récupération de l'ensemble de TP sous jacent. Les mises en œuvre de TEE P1372 peuvent être faibles aux étapes d'implémentation qui permettent à un attaquant d'évaluer la propriété intellectuelle sans la CSL, contre autres impacts.

Liste des équipements

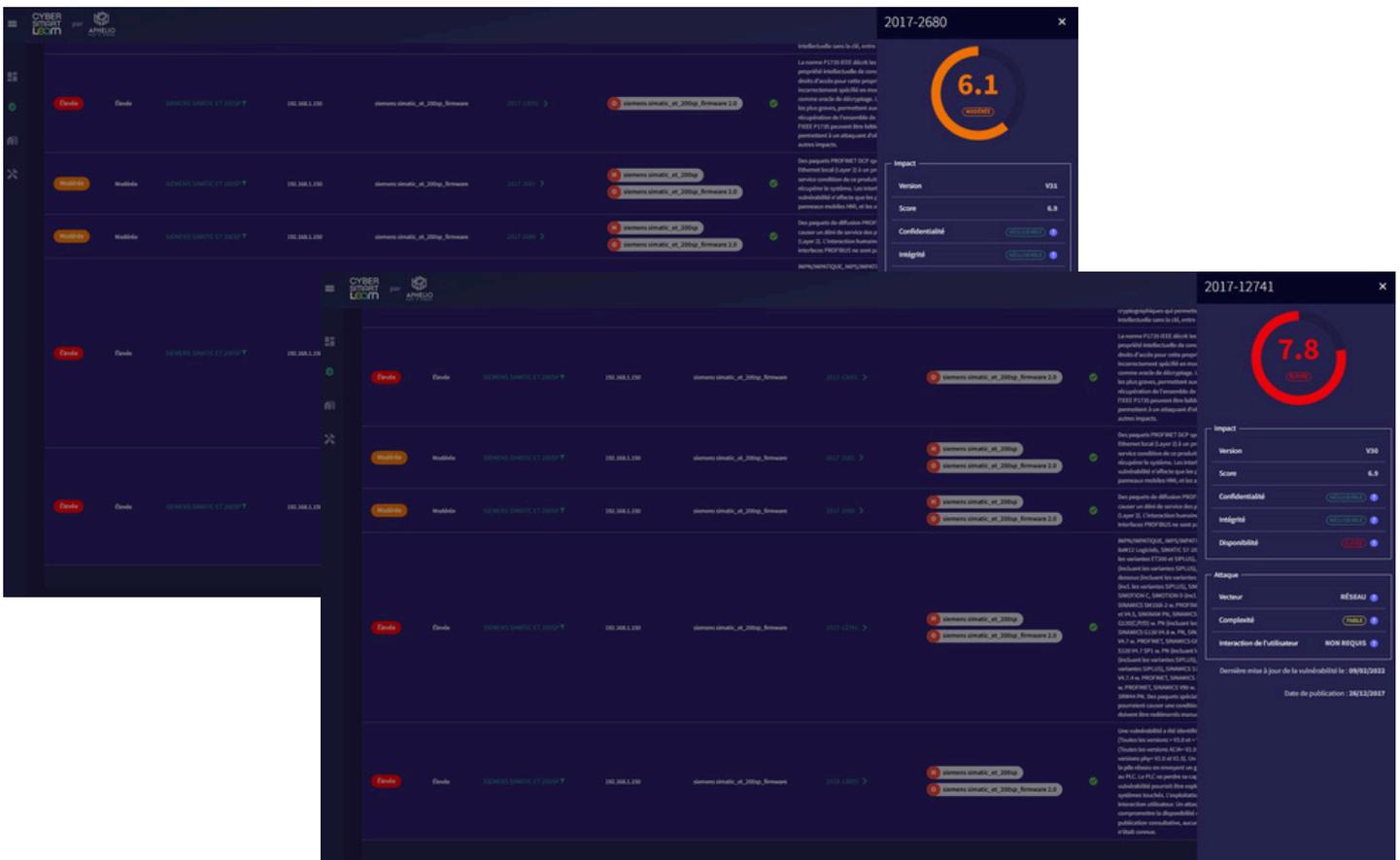
CSL gère les équipements ainsi que les applications, OS, matériels et firmwares associés. Il détecte les versions des actifs et les met à jour de manière automatique, ce qui permet un gain de temps considérable. Il n'est plus nécessaire de reconstruire sa cartographie, c'est CSL qui s'en charge.



Nom	Modèle	Type	Adresse IP v4	Adresse IP v6	Adresse MAC	Critical	Créé par	Localisation	Connexion
Siemens Simatic et 200sp	siemens simatic_et_200sp_ firmware	Automate	192.168.1.130			NOYEX	me		SEMAPHORE
Schneider electric automates BMEP40404	schneider electric modicon_m381_firmwareBMEP40404_ firmware	Automate	192.168.1.131			NOYEX	me		SEMAPHORE
Mikulson DS 30204207 3W	Mikulson ds_30204207_3w	Caméra	192.168.1.126			NOYEX	Importation		SEMAPHORE
Wago Contrôleur pID20	wago_contrôleur pID20	Automate	192.168.1.132			NOYEX	me		SEMAPHORE
Phoenix Contact AXC 1312	phoenix_contact_axc1312	Automate	192.168.1.133			NOYEX	me		SEMAPHORE
Beckhoff Automation Busch 7300	busch_beckhoff_busch_7300	Caméra	192.168.1.126			NOYEX	Importation		SEMAPHORE
Dell PowerEdge R740XD	dell_poweredge_r740xd	Serveur	192.168.1.203			NOYEX	Importation		SEMAPHORE
Switch g3188v1 Mikulson	mikulson g3188v1	Commutateur	192.168.1.249			NOYEX	Importation		SEMAPHORE
HomeKit QN1 40128	homekitation qn1_40128	Caméra	192.168.1.232			NOYEX	Importation		SEMAPHORE
PC DELL 02	dell_xps_3470_x86_in-one_02n_02n	PC	192.168.1.239			NOYEX	Importation		SEMAPHORE
Siemens Fan	siemens fan	Serveur	192.168.1.236			NOYEX	Importation		SEMAPHORE
PC DELL 01	dell_xps_3470_x86_in-one_01n_01n	PC	192.168.1.237			NOYEX	Importation		SEMAPHORE
Switch g3188v1 Mikulson	mikulson g3188v1	Commutateur	192.168.1.247			NOYEX	Importation		SEMAPHORE
Mikulson DS 7008W Q1	Mikulson ds_7008w_q1	Caméra	192.168.1.245			NOYEX	Importation		SEMAPHORE

Calcul de la criticité

CSL Sécurisation calcule le niveau de criticité d'une vulnérabilité en fonction de l'équipement et de la vulnérabilité détectée. Dès qu'une vulnérabilité est publiée, son périmètre d'application est comparé instantanément à la liste des actifs dans CSL. Si un actif est concerné, la vulnérabilité est affichée en alerte avec son niveau de sévérité. En fonction de la criticité de l'équipement, un calcul de risque est effectué pour alerter les utilisateurs de la dangerosité de cette nouvelle vulnérabilité.



Suivi des opérations de maintenance

Avec CSL sécurisation, la qualité des opérations de maintenance est mesurable. Après une opération de maintenance, qu'elle soit de MCO ou MCS, CSL permet d'identifier très rapidement les actions qui ont été effectuées par le mainteneur sur l'infrastructure (mise à jour des équipements, changement de version des logiciels, traitements des vulnérabilités...).

De ce fait, il devient plus aisé de maîtriser l'évolution de l'infrastructure car l'inventaire est toujours à jour.