



SERENICITY

PROTÉGER ENSEMBLE à L'ÈRE NUMÉRIQUE

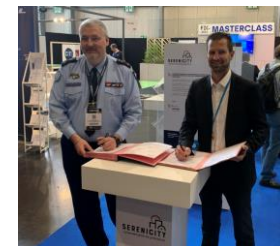
2023

serenicity.fr



SERENICITY en deux minutes

- **SERENICITY** des solutions matérielles et logicielles de cyberprotection de confiance
- Fondée en 2018, SERENICITY a déjà déposé **9** brevets et comporte **11** collaborateurs en 2022
- Les valeurs de SERENICITY sont l'indépendance, l'autonomie la souveraineté économique et la volonté de rendre accessible à tous, les dispositifs permettant de se protéger dans le cyberspace.
- Ce qui nous caractérise : "rendre visible l'invisible", "simple mais pas simpliste", "s'acheter du temps »
- Les trois produits phares de SERENICITY sont :
 - **DETOXIO™** : une sonde de détection et de neutralisation des flux toxiques circulant sur les réseaux informatiques
 - **CYMEALOG** : un super calculateur d'analyse de puits de logs en temps réel
 - **CONTROL** : un puissant outil de représentation visuel de la menace cyber détectée par DETOXIO™
- Afin d'assurer la pertinence de la protection effectuée par **DETOXIO™**, la technologie de détection et de catégorisation des menaces avancées brevetée par SERENICITY fait également l'objet de conventions signées avec les autorités telles que la DCPJ, le ComCyberGend.



L'**ambition de SERENICITY** est de renforcer la sécurité des systèmes d'information des petites, moyennes et grandes organisations en développant des solutions innovantes et **souveraines** permettant de détecter et de bloquer les flux réseaux présumés **toxiques** circulant sur le système d'information.

SERENICITY développe des briques technologiques permettant de faire bénéficier au plus grand nombre d'une **sécurité de précision** simple et efficace et nécessaire à la protection des moyens informatiques :

- Une plate-forme de constitution **d'une base d'IP réputation** basée sur une approche de « deceptive technology ».
- Une **solution d'analyse et de blocage** (type IDS) adaptable à toutes les configurations réseau existantes, de la plus simple à la plus complexe. Sur équipement physique ou en machine virtuelle.
- Une interface de **data visualisation** cartographiant les origines des attaques, les équipements contaminés, et présentant des indicateurs compréhensifs par les non spécialistes : la **CyberMétéo**.

2018 – 2021 : l'innovation prend forme

Trois ans de R&D et **9 brevets** déposés

L'innovation réside dans :

- L'industrialisation de la qualification de la menace cyber.
- L'automatisation du blocage en temps réel des attaques cyber.
- La simplification de la compréhension des événements.
- La mise en évidence des anomalies de paramétrage des équipements.
- Le calcul du taux de **cybertoxicité** (CyT™) des flux.
- L'outil de nettoyage des postes de travail contaminés.

Nos valeurs

Souveraineté : nous développons intégralement en France sans aucun recours à des technologies externalisées ou non maîtrisables.

Partage : nous faisons profiter notre base de connaissances aux utilisateurs de nos solutions.

2021 : les reconnaissances arrivent

- **Signature d'une convention avec la DCPJ (Direction Centrale de la Police Judiciaire).**
- Obtention du label UBCOM permettant d'exercer en Suisse
- Partenaire et membre AN2V (Vidéoprotection, CSU)
- **Un client sur + 1 000 sites (France et Europe) Laboratoire Santé / Healthcare**

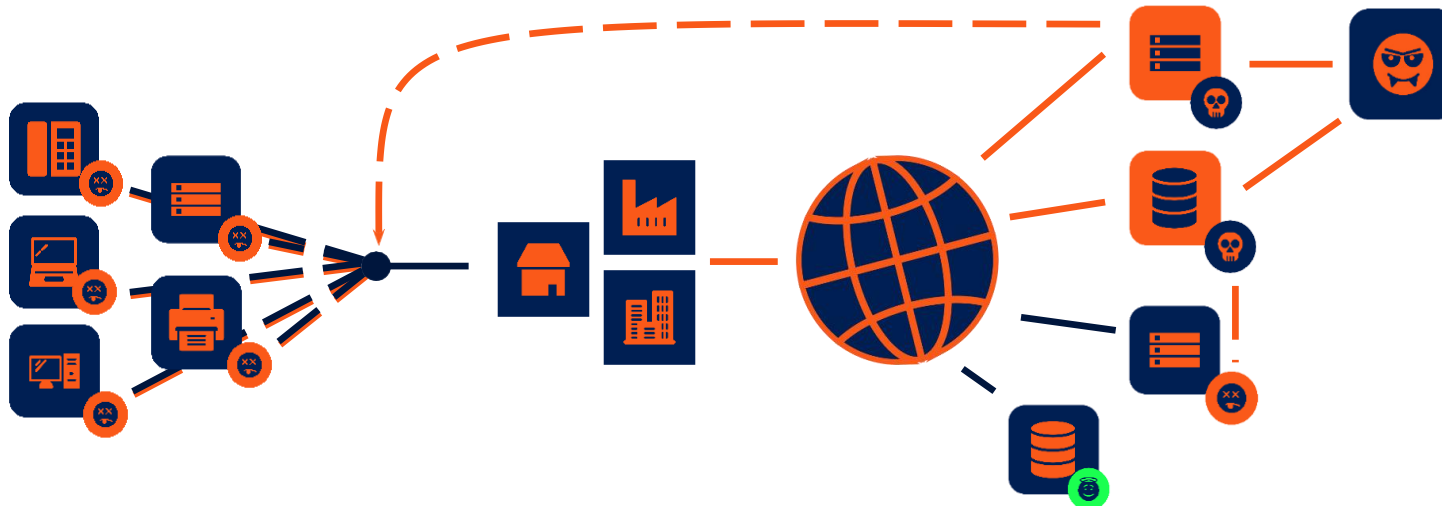
2022 : L'année de confirmation

- **Signature d'une convention avec le Général de Division Marc Boget ComCybergendarmerie**
- **Lauréat du trophée de la Sécurité avec la Télécybersécurité**
- **Mise en place d'un SOC dédié Serenicity**
- **Cybermétéo départementale** : Auto-protection de 30 communes de la LOIRE (324 à venir) Plan France Relance
- **Vainqueur Appel à Projet AURA Boitier DETOXIO-S, Hard, Soft, OS, 100% Souverain**
- Clients Institutionnel, Filière Pharma, Filière Aéronautique (Aéroport, Compagnie aérienne)

Contexte : une cybercriminalité en croissance

La **cybercriminalité** est une activité mondiale très **lucrative**, sans frontière, active 24h/24 7j/7.

Activités	CA 2018 (Md€)	CA 2020 (Md€)	CA2022 (Md€) prévisions
Cybercriminalité	660	1 000	6 000
Trafic de stupéfiants	330	330	



Lexique cyber-criminel

Rançongiciel / **Ransomware**
Spywares / **logiciel espion**
Déni de service / **DDOS**
Hameçonnage / **Phishing**
Cheval de Troie / **Trojan**
Menace persistante avancée
/ **Advanced Persistent Threat (APT)**
Ver / **Worms**

Pour **industrialiser** cette activité très rentable, les hackers malveillants utilisent des logiciels (**robots / bots**) permettant d'automatiser leurs délits et accroître leur outil de production.

Toute machine connectée est désormais une cible.

Le système de défense DETOXIO™



CERBERE

CERBERE™ une base de données qui s'enrichit tous les jours de 9000 à 12000 adresses IP toxiques.

La pertinence de cette base a permis à **SERENICITY** de signer des conventions avec la **Direction Centrale de la Police Judiciaire** et le **Commandement Cyber de la Gendarmerie**

La **DCPJ**, **l'ANSSI**, **le C3N** et **le ComCyberGend**, complètent ces marqueurs avec leurs bases d'IP (IP trouvées dans des enquêtes cyber)



DETOXIO

DETOXIO™ est un boîtier positionné dans l'entreprise entre le Firewall et le Switch.

La solution **DETOXIO™** se connecte, de manière sécurisée, toutes les 30 minutes avec **CERBERE™** pour mettre à jour sa base d'adresses IP toxiques.

Sa fonction est de **bloquer automatiquement** dès qu'il les détecte les flux en provenance ou à destination d'une adresse IP toxique.



**SERENICITY
CONTROL**

SERENICITY CONTROL™ est l'interface associée à chaque **outils SERENICITY™** qui vous permet :

D'être alerté (si vous le souhaitez) lorsqu'une faille apparaît

D'analyser la menace grâce à une cartographie et à la cybermétéo.

De qualifier la menace grâce à des outils simples et ergonomiques.

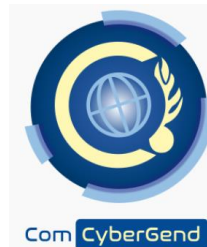
De remédier avec les Blacklist Whitelist dédiées ainsi que les domaines et URL.

CERBERE : CARACTERISATION DE LA MENACE

CERBERE est une technologie **brevetée** de **détection** et de **caractérisation** de la menace en temps réel.

CERBERE est alimentée par différents dispositifs d'écoute et de détection proactive des cybermenaces sur internet.

Les marqueurs de compromission remontés dans CERBERE sont répertoriés et cartographiés avec une technologie **souveraine** intégralement développée par **SERENICITY**.



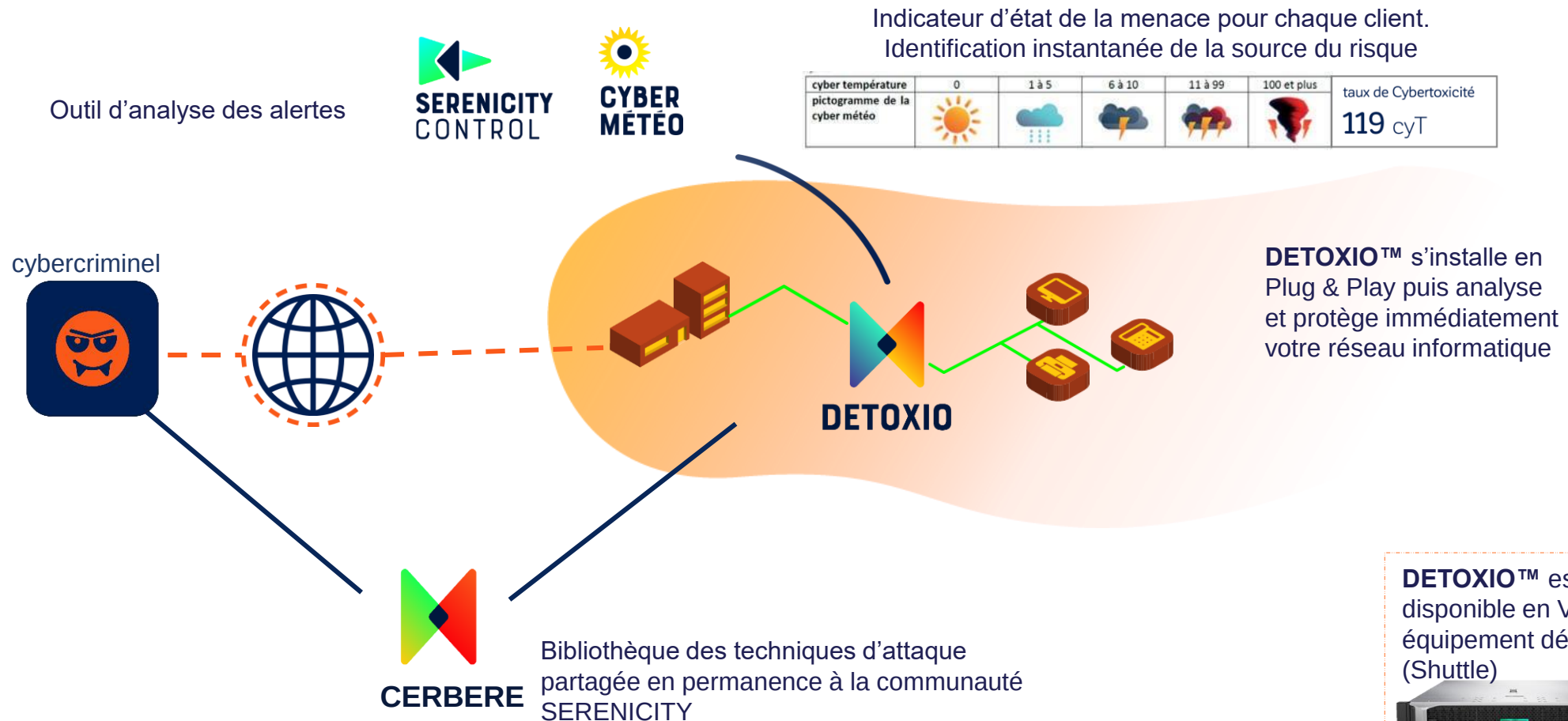
Les solutions **DETOXIO®** et **CYMEALOG®** mettent à jour leur base de menaces à partir des éléments contenus dans CERBERE
La datavisualisation est faite sous **CONTROL**

INTELLIGENCE-ONLINE, magazine spécialisé dans le périmètre des renseignements, a mis la technologie de **SERENICITY** en première page son édition du 15 septembre 2021



DETOXIO™ : analyse et remédiation

DETOXIO™ bloque les flux toxiques et vous permet de compléter les dispositifs de cybersécurité pour les TPE / PME



DETOXIO™ est disponible en VM ou en équipement dédié (Shuttle)

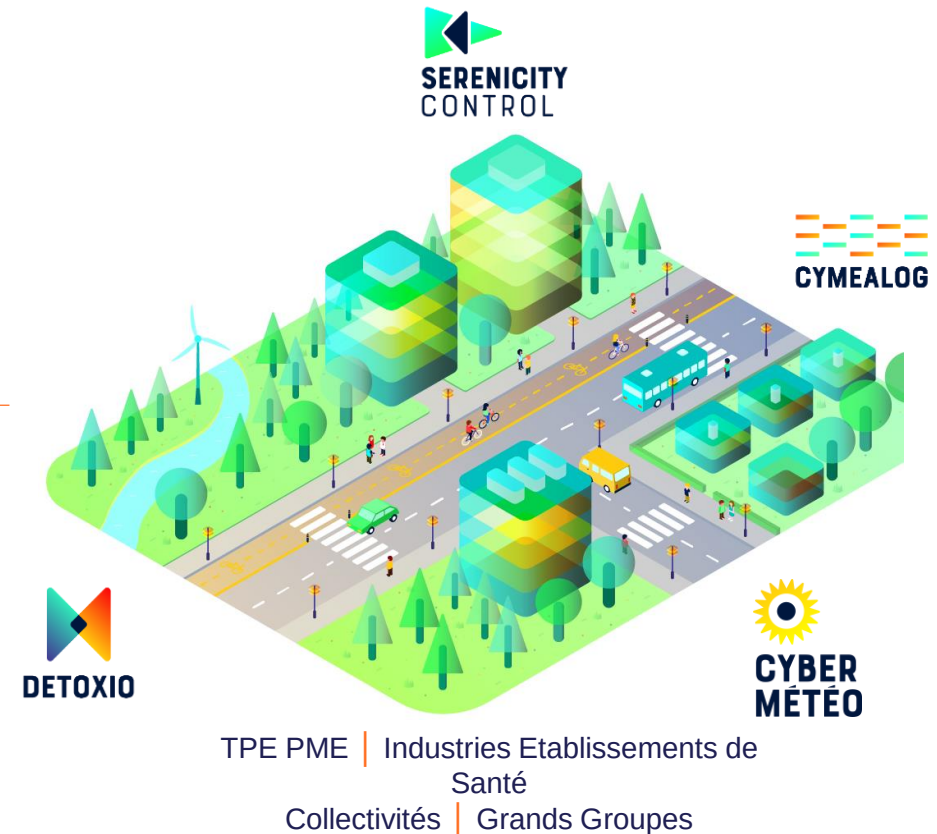


2 solutions de **cyberprotection** pour **protéger** les équipements et **alerter automatiquement** pour assurer la résilience du système d'information

- **DETOXIO®** analysent et bloquent les flux toxiques pouvant altérer, détruire ou voler le patrimoine informationnel des organisations
- **CYMEALOG®** est un puissant outil d'analyse qui s'appuie sur la base CERBERE de connaissances des menaces

1 outils de **supervision** et d'**alerte** pour connaître instantanément l'état de son SI

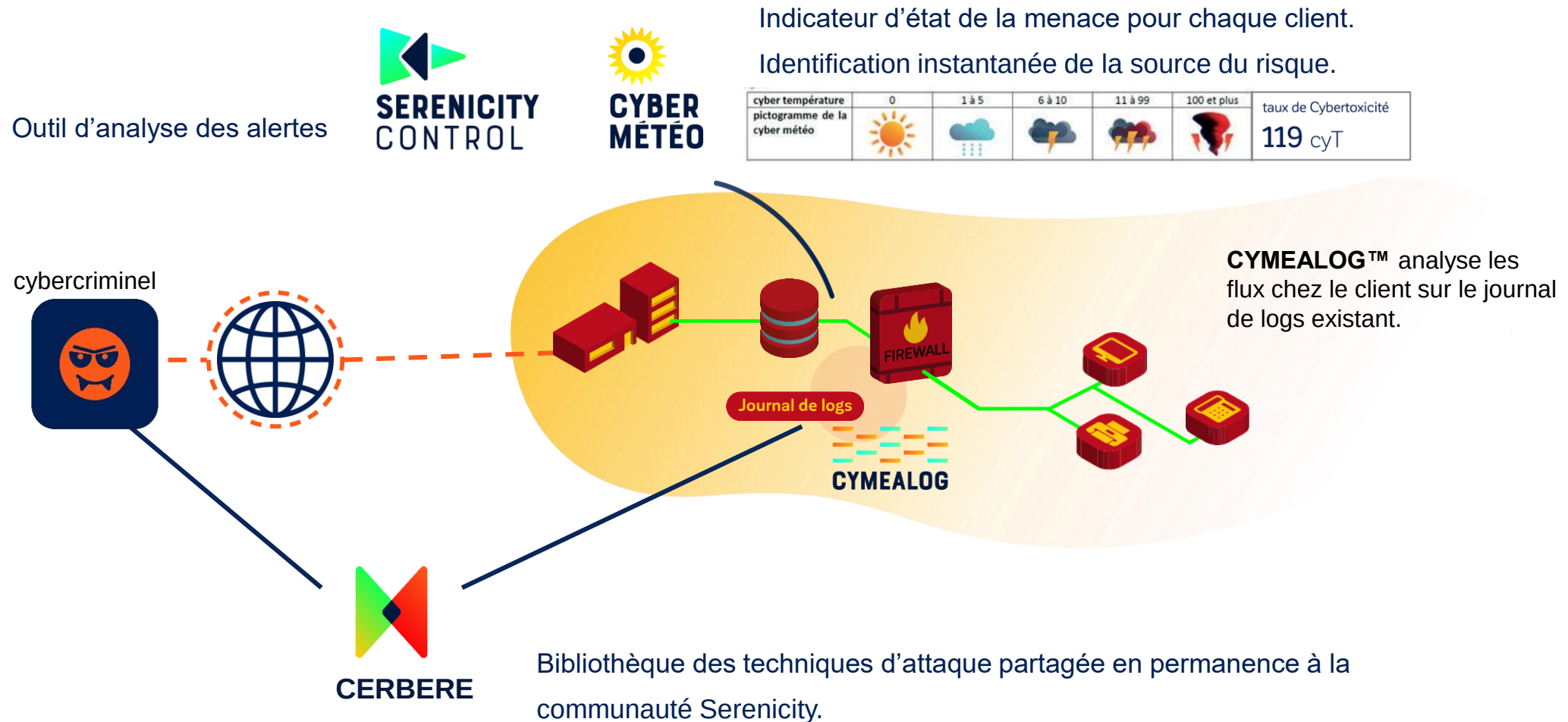
- La **CYBERMETEO®** est un indicateur qui présente une information simple accessible à tous sur l'état de la cybermenace.
- **CONTROL** est l'outil de supervision qui vous permet de piloter en toute sécurité l'ensemble de vos dispositifs depuis votre ordinateur ou votre smartphone.



Solutions brevetée de threat-intel via la constitution et de mise à jour en temps réel d'une base d'indices de compromission et d'IP réputation.

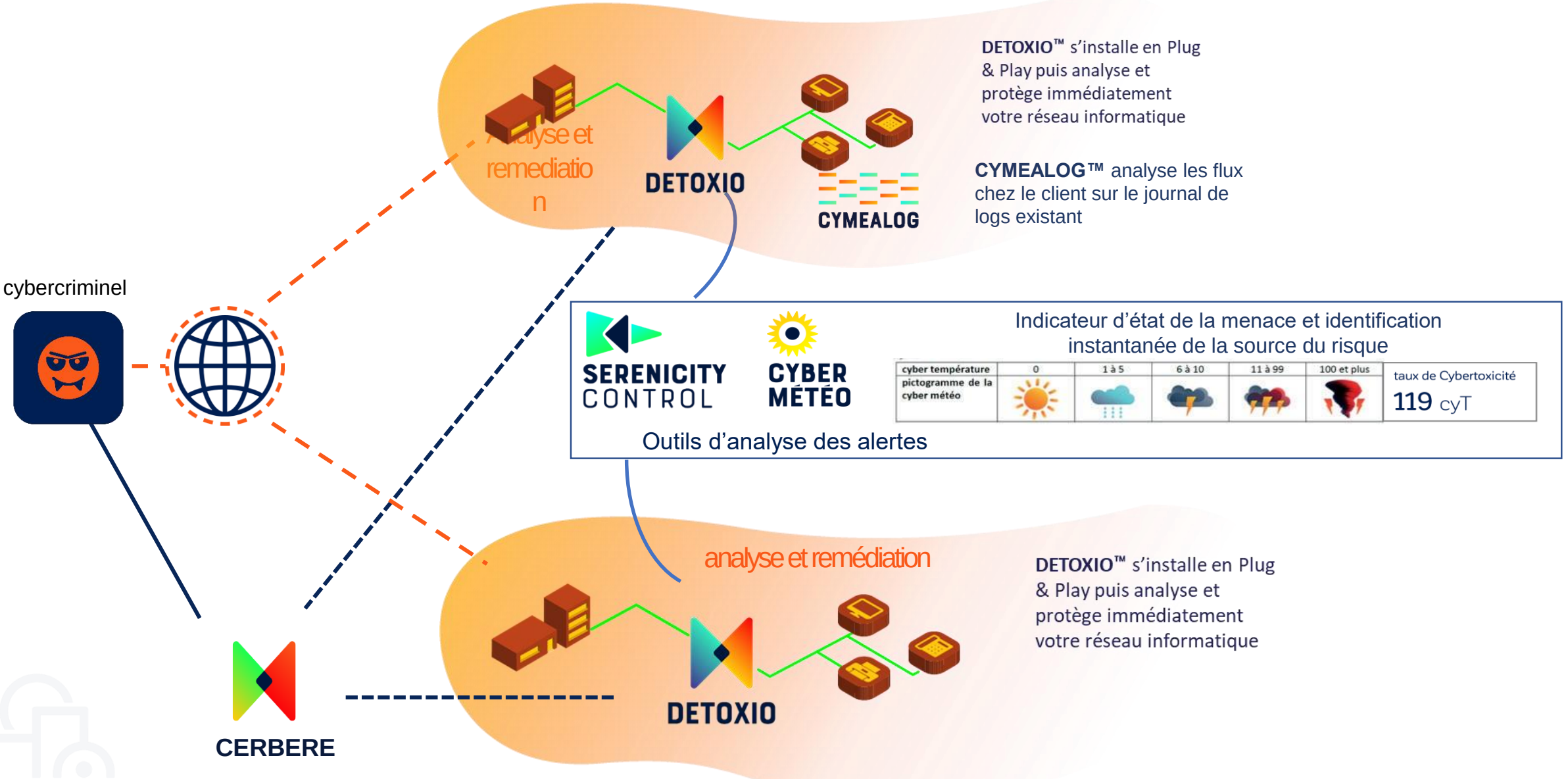
SERENICITY - des outils d'analyse simples, compréhensibles pour se protéger **ensemble**

CYMEALOG™ pour les organisations ayant des outils d'enregistrement des logs pour analyser rapidement l'ensemble des flux passés dans le réseau



Intégration globale

Les produits de SERENICITY s'intègrent pour offrir une solution globale à votre problématique de cybersécurité



Ils nous font confiance



Éditeur référencé
UGAP-SCC



ASSOCIATION
NATIONALE DE LA
VIDÉOPROTECTION



ONE LYON
ST-ETIENNE



Programme de certification

- **SERENICITY** propose un programme de **formation** progressif en 5 modules sur les différents produits :

- Control 
- DETOXIO niveau 1 
- DETOXIO niveau 2

Les premiers niveaux sont accessibles à tous. Il n'est pas nécessaire d'être un expert en cybersécurité pour y assister
Les modules de niveau 2 requièrent d'avoir acquis les mécanismes présentés lors des premiers niveaux.

- **SERENICITY** propose également un programme certification sur les différents produits :
 - Un diplôme est remis à l'issue des tests pour tout score atteignant au moins **80%** de réponses correctes.



La CyberProtection de Confiance



- Améliorer jusqu'à 30% les **performances** de son système d'information par un meilleur filtrage des flux toxiques
- Faire un bilan rapide de l'état de sa cybersécurité
- Bloquer automatiquement les flux indésirables en entrée et en sortie (**DETOXIO™**)
- Identifier d'où viennent les problèmes
- Compléter les solutions de firewalls existants
- Maintenir sa conformité **RGPD**
- Superviser la consommation internet de chaque équipement du SI et générer des alertes en cas d'anormalité

Quelle est votre cyber météo ?



Découvrez votre CyT (Cyber Toxicité) et rejoignez la communauté de défense à partir de **49 €HT/mois**

Serenicity : Le choix de nos clients ...

- Qualification de la base de données CERBERE (+ de 400 000 IP tox).
- Le produit est SOCable, je suis alerté dès qu'il y a un problème et je me concentre sur mon Core business.
- La conformité RGPD puisque les échanges filtrés en temps réel ne sont pas analysés dans leur contenu.
- Installation Detoxio Plug & Play en Shuttle ou VM, Cymealog lit et intègre des puits de log de Fortinet, Stormshield, Palo Alto ou autres ...
- Filtrage des flux entrants et sortants car bien souvent les flux sortants ne sont pas filtrés et demande une administration particulière et quasi manuelle dans les firewalls.
- Filtrage Detoxio de volume d'IP bien plus importante qu'un Firewall , 5 000 ip en moyenne pour un firewall contre 500 000 pour un Detoxio.
- Gestion des MAJ et MCO automatique toutes les 30 min vs CERBERE.
- Reprise du contrôle des SI et gestion à la demande ou gestion de crise par l'administrateur en instantané et en centralisation sur des sites distants via le superviseur Control.
- Superviseur Control = IHM simple avec rapports automatiques et visualisation en ligne des incidents et des attaques et de la remédiation.
- Superviser et Contrôler les échanges des équipements connectés avec internet et challenger les fournisseurs de services ou de produits sur le bienfondé de ces échanges ou le manque de mise à jour laissant passer des indices de compromissions connus, recherche de responsabilités
- S'acheter du « temps » pour analyse puisque les flux toxiques sont bloqués
- Malgré l'installation de différents produits, cette solution me permet de superviser la fiabilité de l'ensemble

DETOXIO™ en format matériel autonome.



⚠ **DETOXIO©** et **PROBIO©** n'inspectent pas le contenu des flux utilisateurs.
Seules les métadonnées sont traitées.



Adresses IP publiques
toxiques



Métadonnées

- Adresse MAC source
- Socket (@IP source , @IP destination, port)
- Protocole de transport
- Identifiant NETBIOS associé à l'adresse source
- Horodatage
- Journaux système (charge processeur, mémoire, etc...)

Flux d'administration

- Tunnel SSH pour l'administration des équipements DETOXIO©



Centre de traitement de SERENICITY

- **Tous** les serveurs sont localisés dans des hébergements privés et dédiés aux usages de SERENICITY.
- Les données transitent uniquement entre les équipements DETOXIO©, PROBIO© et le centre de traitement.
- Conformément à ses engagements vis-à-vis de la souveraineté, SERENICITY n'utilise pas de service en cloud



Roadmap produits et solutions

- Les outils **DETOXIO®**, **CYMEALOG®** et **CONTROL** sont développés sur les fonds propres de **SERENICITY**
- **CYBERCARBONE** dockerisation et intégration du calcul du Cyber Carbone (empreinte carbone des connexions externes du SI)
- **DETOXIO-S** : équipement souverain de cyber protection développé en interne et électronique élaborée en France (BIOS, Puce, ...)
- Cinq nouveaux projets sont prêts à être développés :
 - **FORENSIO** : deux équipements permettant la collecte de métadonnées (couche 7 du modèle OSI) et la production de rapport d'analyse de cyber sécurité
 - **APPLICATION FORENSIC** : application de production de cyber sécurité sur mesure
 - **INTELIO** : solution de collecte de métadonnées et de production de fiche de renseignement
 - **SUPPLIO** : solution de protection du donneur d'ordre et de sa chaîne d'approvisionnement et de sous-traitance (supply chain)



Merci de votre attention

