SERENICITY

PROTÉGER ENSEMBLE À L'ÈRE NUMÉRIQUE

Octobre 2021

serenicity.fr

SERENICITY : Objections Detoxio

Le boitier va me générer des alertes, je n'ai pas le temps de m'en occuper.

Detoxio n'est pas qu'une sonde : les flux toxiques sont bloqués. Vous pouvez configurer des alertes de synthèse vous indiquant les équipements contaminés de votre réseau. Nous nous occupons de tout, nous vous transmettons des rapports et nous vous accompagnons lorsqu'il y a eu une alerte. Comprenez que c'est avant tout pour la sécurité de vos données.

Je vais avoir quelque chose de plus à gérer, je n'ai vraiment pas le temps pour ça.

Tout dépend de ce que vous souhaitez : Soit nous vous alertons régulièrement en fonction des attaques que vous subissez, soit la solution est totalement transparente pour vous. En tout état de cause nous restons vigilants et sommes à vos côtés pour la sécurité de votre SI.

C'est une charge en plus et pour couronner le tout cela ne me rapporte rien.

Et si vous perdez tout votre système d'information, que perdez-vous ? (Accès à vos mails, votre facturation, données clients, comptabilité, …)

Et si sans le savoir vous êtes responsable d'une attaque chez l'un de vos clients ?

Les donneurs d'ordres imposent de plus en plus de mettre en place une solution de cybersécurité à leur sous-traitant : ne pas en mettre en œuvre peut vous faire perdre des contrats, ou vous empêcher de répondre à certains.

SERENICITY : Objections Detoxio

Le RGPD : aucune importance pour moi.
Je vous invite toutefois à vous renseigner sur les risques auxquels vous vous exposez :
- Contrôle de la CNIL
- Amende de 4 % du chiffre d'affaires
De plus en plus de contrôles ont lieu, avec une annonce récente sur le recrutement de nouveaux contrôleurs CNIL.
En cas d'incident causé sans le savoir par votre informatique sur un tiers (rebond d'attaque), la CNIL pourra contrôler votre conformité au RGPD.

Comment j'intègre votre solution dans ma RGPD pour être conforme ?
Il n'y a pas de captation de données personnelles. Il n'y a pas de lecture des trames IP (du contenu des flux). Les seules données collectées soumises au RGPD sont les données à caractère commercial, et administratif. Elles répondent à la charte RGPD de Serenicity.
Les rapports issus de Control vous permettent de démontrer un engagement de moyen de cybersécurisation de vos données au titre de l'article 32 du RGPD.

Vous n'êtes pas certifié ANSSI ?
En effet, l'agrément a un coût financier (environ 40 000€) et prend 6 mois d'étude. Le principal obstacle est que dès que l'on apporte une modification sur le produit, il faut payer à nouveau. Or, nous l'améliorons toutes les semaines, donc ce n'est pas possible. Pour autant nous avons une collaboration étroite avec l'ANSSI et une convention avec la DCPJ et le C3N.

SERENICITY : Objections Detoxio

Mon informaticien/opérateur s'occupe déjà de tout. Il m'affirme que je suis protégé.

Oui vous avez des outils de protection informatique (firewall, antivirus, antispam, …)

Malheureusement, cela ne suffit plus : les failles de sécurité majeures sont quasi quotidiennes chez les éditeurs de solutions de protection informatique. DETOXIO est l'outil de contrôle automatisé des cybermenaces touchant le système d'information.

La personne qui vous dit que vous êtes protégés est la même qui vous vend la protection. C'est vous qui serez impacté en cas d'attaque réussie (comme les centaines d'exemples dans l'actualité) : comment vous assurez-vous que tout fonctionne ?

SERENICITY : Objections Detoxio

Comment expliquez vous que vous sachiez détecter les attaques mais pas les grands groupes ?
- *L'innovation* : nous sommes à ce jour la seule entreprise européenne qui collecte de manière automatisée des adresses IP toxiques. Cela fait l'objet de 3 brevets européens.
- *La méthode* : les grands groupes ne détectent pas les attaques de la même manière. Notre méthode consiste à détecter les menaces à partir de l'adresse IP. (Nous détectons Qui émet ou reçoit les flux ; les grands groupes observent les contenus des flux)
- Certains grands groupes ont choisi d'installer notre solution pour améliorer leur défense.

Qui me dit que vous n'allez pas espionner mes données ?
Nous ne regardons jamais le contenu des flux entrants et sortants, mais uniquement l'émetteur et le récepteur de ces flux (les logs). Je vous invite à prendre connaissance de notre RGPD
➔Convention DCPJ (Direction Centrale de la Police Judiciaire)

Vous collectez quoi comme données ? Et où sont-elles stockées ?
Les seules données que nous traitons sont les logs, constitués des IP source et de destination et ce de manière totalement anonyme.

SERENICITY : Objections Detoxio

Vous n'êtes là que pour faire de la vente additionnelle !
Les cybermenaces sont omniprésentes. Vous connaissez certainement dans votre entourage une personne ayant subi une attaque. Pourtant comme vous, elle pensait être en sécurité.
Nous sommes en train de vivre un changement d'ère, la sécurité informatique ne suffit plus. Ce que je vous propose est une solution de cybersécurité.

Quelle est la différence entre la cybersécurité et la sécurité informatique ?
Jusqu'à 'il y a 5 ans les risques qui pesaient sur votre SI étaient des risques majoritairement liés à l'usage aux matériels et aux défaillances informatiques. Ces menaces existent toujours et sont traitées par la sécurité informatique.
Malheureusement, la menace cyber (venant de l'extérieur) a pris une part prépondérante des risques pour votre système d'information. Aujourd'hui, ce sont des robots d'attaque (botnets) qui attaquent à haute fréquence les solutions traditionnellement utilisées qui sont maintenant dépassées face à cette typologie de risque. La cybersécurité est la réponse aux cybermenaces.

Je ne souhaite pas que mes flux/logs soient à l'extérieur de mon SI.
Les logs sont envoyés à notre serveur SSH (chiffrement, différentes couches de sécurité) puis remontés dans Control.
Si vous avez un tel niveau d'exigence, vous connaissez l'importance de la cybersécurité. Serenicity peut vous proposer une offre sur-mesure, allant de l'analyse de vos journaux de log sur place jusqu'à la mise en place d'une infrastructure dédiée.

SERENICITY : Objections Detoxio

Les FAS sont trop chers.

- Qu'est-ce que vous entendez par chers ?
- Chers par rapport à quoi ?
- A combien les évalueriez-vous ?

Vous êtes un firewall ? Vous êtes un IPS/IDS/EDR ?

Non, notre boitier DETOXIO permet d'avoir un double contrôle indépendant sur ce qui est réalisé par le Firewall ou les éléments de filtrage du type IPS. Le produit est complémentaire au Firewall, il le supervise et bloque les flux malveillants qui sont passé à travers celui-ci.

Mon Firewall fait IPS.

Le DETOXIO permet d'avoir un double contrôle indépendant sur ce qui est réalisé par le Firewall et l'IPS, il le supervise.

SERENICITY : Objections Detoxio

Comment qualifiez-vous les IP toxiques ? Comment et où collectez-vous les IP toxiques ?

Nous avons disposé des pièges à adresses IP toxiques, appelés Honey pot (Pot de miel) qui collectent jusqu'à 12 000 adresses IP par jour : à chaque fois qu'un hacker/bot tente de se connecter à un de nos serveurs son adresse IP est récupérée.

Ces adresses font l'objet d'un traitement qui supprime les faux positifs. À ce jour, les adresses IP toxiques collectées par SERENICITY sont fiables à 99%.

Par ailleurs, notre convention avec la DCPJ (Direction Centrale de la Police Judiciaire) et le C3N (gendarmes du numériques), ainsi que notre partenariat avec l'ANSII nous font bénéficier de leurs bases d'IOC (adresses IP malveillantes détectées dans les enquêtes judiciaires)

Quelles sont les métadonnées collectées ?

Nous collectons l'horodatage, l'adresse IP source et destination, le sens des flux, le protocole et le port, le noms Netbios, les métrique OUT en octet et les métrique IN en octet.

Combien de fois le Detoxio se synchronise-il dans la journée ?

Un Detoxio synchronise la base de données SERENICITY Cerbère 2 fois par heure, cela fait donc 48 mises-à-jours de sa base de données dans la journée.

SERENICITY : Objections Detoxio

L’interface est personnalisable ? Mais pas assez.

- Qu’attendez-vous en terme de personnalisation ?
- Y a-t-il une fonctionnalité dont vous auriez besoin ?

Votre solution couvre-t-elle l’ensemble des cybermenaces ? Est-ce que je suis protégé à 100% si j’achète votre solution ?

Celui qui vous dit que sa solution protège à 100% est un menteur. La cybermenace est une course permanente entre les hackers et les solutions de cybersécurité. Pour autant, l’ajout d’une solution de cybersécurité à vos solutions de sécurité informatique réduit considérablement le risque pesant sur votre système d’information.

J’ai une RC Pro qui me couvre pour ses problèmes.

Je vous invite fortement à relire votre contrat : les assureurs ne couvrent plus les risques cyber avec une RC Pro. Ils estiment que la cybermenace n’est plus un aléa. Or, les assureurs n’assurent que des aléas.

SERENICITY : Objections Detoxio

Pourquoi cette solution et pas une autre ?
- Nous sommes souverains (100% made in France).
- Nous automatisons la détection, l'analyse et le blocage des menaces.
- A même niveau de performance, nous sommes les moins chers du marché.
- Pour les TPE/PME il n'existe aucune offre comparable.

Vous gérez déjà mon informatique, pourquoi ne pas me l'avoir proposé plus tôt ?
Cette solution n'existait pas auparavant. C'est le seul produit de cybersécurité 100% français et adapté aux TPE/PME. Il existe bien d'autres produits mais ils n'offrent pas les mêmes services et sont entre 5 et 10 fois plus chers.

A part mon entreprise, qui a accès aux éléments transmis par Detoxio ?
Uniquement l'équipe d'administration du centre de traitement de Serenicity et nous-même.

C'est un sujet trop technique, aller voir mon informaticien, RSI ou DSI.
Cela peut paraître très technique, mais en réalité cela ne l'est pas du tout : DETOXIO qualifie les intrusions dans votre informatique avec une lecture très simple : c'est la cybermétéo.
En tant que chef d'entreprise vous êtes garant de la sécurité physique de vos collaborateurs et de vos locaux, avec Detoxio, nous vous rendons le pouvoir que vous auriez toujours dû avoir : le contrôle de la sécurité de vos données.

SERENICITY : Objections Detoxio

Pourquoi faire le choix d'une solution souveraine ? Française vs US ou GB ?

La souveraineté informatique est la condition indispensable pour la sécurité de vos données et de nos données. C'est l'affaire de tous et il en va de la sécurité de votre entreprise comme de notre pays.

A quoi sert votre solution ?

Notre solution permet de détecter les cybermenaces et de protéger votre système d'information.

C'est une petite sonde qui analyse tous les flux IP transitant dans votre réseau. Elle distingue les flux toxiques des flux non toxiques entrant et sortant du SI.

Si un flux toxique est détecté DETOXIO le bloque.

Qu'est-ce qu'une adresse IP ?

C'est l'identifiant d'une machine (serveur, PC, téléphone, imprimante …) qui lui permet d'être reconnue lorsqu'il communique avec une autre machine.

SERENICITY : Objections Detoxio

Mon activité n'est pas critique donc je n'ai pas besoin de protéger mes données.
Vos données n'ont aucune importance ? (Paie, contrat client, comptabilité, fichier client, …)
Savez-vous que sans le vouloir vous pouvez infecter un fournisseur, un client, ou même un hôpital.
81% des systèmes infectés servent d'outils aux pirates informatiques pour procéder à des attaques de grande ampleur. Vous souhaitez indirectement participer à une attaque contre un hôpital?
Le RGPD vous impose de maitriser la confidentialité des données hébergées dans votre SI : et si les scans des Cartes Nationales d'Identité de vos collaborateurs étaient usurpées ?

Si je subis une cyber-attaque je restaurerai tout grâce à mes sauvegardes.
Saviez-vous que les pirates travaillent sur un temps long : ils prennent le temps d'extraire puis de corrompre vos sauvegardes. Le jour ou vous voulez les charger, elles seront cryptées comme le reste de vos données.

Actuellement tout fonctionne correctement, donc pourquoi les hackers m'attaqueraient ?
Qu'entendez-vous par « tout fonctionne correctement » ?
81% des systèmes infectés servent d'outils aux pirates informatiques pour procéder à des attaques de grande ampleur. Vous souhaitez indirectement participer à une attaque contre un hôpital?
Je vous propose donc un audit gratuit pour vérifier si « ça fonctionne correctement ».

SERENICITY : Objections Detoxio

J’ai déjà des outils de contrôle de mes flux.

- Quels sont-ils ?
- Quelles technologies utilisent-ils ?

Detoxio est le seul a utiliser l’unique source automatisée de collecte d’adresse IP toxiques en Europe. (Technologie triplement brevetée)

La sonde que je vous propose est totalement complémentaire avec celles que vous détenez déjà.

DETOXIO est un produit 100% français.

Je ne souhaite pas mettre en place un équipement qui pourrait causer une coupure. Je ne veux pas que mes collaborateurs soient bloqués.

Y-a-t-il une autre raison pour laquelle vous ne souhaitez pas mettre un équipement en coupure ?

- Non il n’y a pas d’autre raison

SERENICITY propose une solution de DETOXIO en haute disponibilité (équipements redondés) et dans ce cas vous bénéficiez du filtrage automatisé des flux toxiques.

En tout état de cause si le boitier venait à être défaillant, il suffit juste de l’enlever.

SERENICITY : Objections Detoxio

Le boîtier peut-il communiquer avec les équipements de mon réseau ?
Non, DETOXIO est paramétré pour n'échanger aucune donnée avec votre système d'information. La seule communication que vous pouvez établir avec DETOXIO est de l'autoriser à utiliser les noms Net Bios et adresses MAC de votre réseau en lieu et place des adresses IP des équipements du réseau.

DETOXIO peut-il télécharger un virus ?
Non, il ne télécharge que des bases d'adresses IP. Un contrôle d'intégrité de la base est effectué à chaque téléchargement donc la base d'adresses IP ne peut pas « cacher » un virus.

Peut-il implanter un virus dans mon système d'information ?
Non, il n'émet aucune donnée vers le système d'information. Cela est vérifiable avec une sonde.

La solution peut-elle être infecté par une source extérieure (internet) ou par un équipement de mon réseau ?
Non, elle est paramétré pour ne communiquer que vers le centre de traitement de Serenicity. C'est DETOXIO qui crée la liaison vers Serenicity et le contraire est impossible. Il n'accepte aucune communication entrante si le tunnel d'administration n'est pas monté.

Pourquoi devrai-je faire confiance à votre boitier ? Qui me dit que ce n'est pas vous qui allez me contaminer ?
Le boitier ne fait qu'analyser les flux entrants et sortants de votre SI, il ne peut pas les inventer et il est tout à fait possible de vérifier leur existence avant de brancher le boitier. A aucun moment le boitier DETOXIO n'installe de logiciel sur votre SI. En revanche il saura couper les flux considérés comme toxiques.
➔ Convention DCPJ (Direction Centrale de la Police Judiciaire) et avec le C3N (gendarmes du numériques)

SERENICITY : Objections Detoxio

Peut-il créer une incompatibilité avec un périphérique de mon réseau ?
Non, DETOXIO est perçu comme un ordinateur banal sur le réseau. C'est pour cette raison que le boitier choisi par Serenicity est un mini PC.

Peut-il créer des perturbations dans l'usage de mon système d'information ?
Oui, si un flux est constaté comme toxique par DETOXIO, ce flux sera coupé. Il peut arriver que cet échange de données soit indispensable pour le fonctionnement de l'entreprise alors même qu'il est toxique. Dans ce cas de figure, il est possible de « whitelister » l'adresse ip incriminée dans Control pour ne pas perturber l'activité.

Va-t-il perturber le bon fonctionnement de ma connexion internet ?
Non, la latence (ralentissement) induite par le DETOXIO est < à 1 ms. Il n'y a pas de buffering (mise en mémoire tampon) donc pas d'impact sur la performance des flux même en cas de fort trafic.

Si le boîtier est éteint, altère-t-il ma connexion internet ?
Oui, l'impact est la coupure de votre accès internet. DETOXIO est positionné en « coupure » entre votre routeur (box) et votre réseau informatique. Le redémarrage met environ 60 secondes : il vous faudra donc attendre une minute avant de récupérer votre connexion.

SERENICITY : Objections Detoxio

S’il tombe en panne, cela aura-t-il une influence sur ma connexion internet ?
Oui, l’installation étant en « coupure », la liaison entre votre routeur (box) et votre réseau sera coupée si l’équipement n’est plus alimenté électriquement. Avec trois ans de recul, nous n’avons constaté aucune panne de ce type.
Toutefois il existe une solution DETOXIO en haute disponibilité (VM redondées).
En tout état de cause, il suffit alors d’enlever le boîtier de votre réseau.

DETOXIO améliorera-t-il la performance de mon accès internet ?
Lorsque le DETOXIO est en mode blocage, il améliore les performances de l’accès internet car en coupant les flux toxiques, vous récupérez la bande passante inutilement encombrée par les flux indésirables.

Quel traitement DETOXIO fait-il de mes données ?
Aucun traitement n’est effectué sur le contenu des flux. Il n’inspecte aucune donnée, n’émet ni ne reçoit de données depuis ou vers le système d’information.

Où se situe le traitement des données du DETOXIO ?
Le traitement des données du DETOXIO est effectué par le centre de traitement de Serenicity qui est situé en France dans des locaux sécurisés.

SERENICITY : Objections Detoxio

Serenicity peut-elle communiquer des éléments captés par DETOXIO à des tiers ?

Uniquement en cas de réquisition judiciaire effectuée par les autorités compétentes. Les données sont l'adresse IP locale, l'adresse MAC du périphérique associé, le nom NetBios du périphérique associé sur ce nom est disponible, l'adresse IP distante, le sens du premier flux pour l'adresse IP locale et l'adresse IP distante, le port utilisé, le volume total d'octets échangés et l'horodatage du flux. Il n'y a aucune autre donnée récupérée par le DETOXIO et le centre de traitement de Serenicity

DETOXIO enregistre les flux toxiques ? Sur quelle durée ? Comment ?

Les deux cartes réseaux de DETOXIO sont configurées en mode « bridge ».

En mode « Supervision seule », les flux non toxiques et toxiques sont enregistrés par analyse des paquets IP qui traversent le bridge. Ces flux sont envoyés au centre de données de Serenicity au début de l'heure suivante.

En mode « Supervision et filtrage », les flux non toxiques et toxiques sont enregistrés par analyse des paquets IP qui traversent le bridge. Les flux toxiques sont instantanément bloqués (un flux toxique est un flux dont l'adresse IP source ou destination est présente dans la base de données locales du DETOXIO d'adresses IP toxiques. Cette base de données est mise à jour toutes les heures. Elle peut être mis à jour en moins de dix minutes en cas de menace avérée). Ces flux sont envoyés au centre de données de Serenicity au début de l'heure suivante. La durée de conservation prévue est de 1 an pour les flux non toxiques et 3 ans pour les toxiques.