Whaller

Whaller annonce le lancement de son CSIRT

Suresnes, 25 mars 2024 – *Whaller, pionnier des solutions de collaboration numérique sécurisées, renforce son engagement en faveur de la cybersécurité en annonçant la création de son propre Computer Security Incident Response Team (CSIRT). Cette équipe dédiée à la sécurité informatique a pour mission de détecter, analyser et répondre aux incidents de sécurité, afin de garantir la protection optimale des données de ses utilisateurs et d'améliorer la résilience face aux cybermenaces.*

Un CSIRT, qu'est-ce que c'est et quels sont les bénéfices pour les clients de Whaller ?

Un **CSIRT** est une équipe d'experts en cybersécurité chargée de surveiller en permanence la plateforme, de détecter les éventuelles vulnérabilités et menaces, et d'intervenir rapidement en cas d'incident de sécurité. Le **CSIRT** collabore étroitement avec les équipes de développement et d'exploitation de Whaller pour intégrer les meilleures pratiques en matière de sécurité dans le cycle de vie du produit.

Pour les clients de Whaller, la création d'un CSIRT présente plusieurs avantages :

1. **Une réactivité accrue face aux cybermenaces :** Grâce à une surveillance constante et à une expertise pointue, le **CSIRT Whaller** est en mesure de détecter et de réagir rapidement aux incidents de sécurité, réduisant ainsi les risques de compromission des données.
2. **Un environnement de communication et de collaboration plus sécurisé :** Le **CSIRT** contribue à renforcer la sécurité globale de la plateforme Whaller, offrant aux utilisateurs un espace de travail numérique toujours plus fiable et sécurisé.
3. **Une conformité réglementaire :** Le **CSIRT Whaller** garantit la conformité de la plateforme avec les exigences réglementaires et les recommandations de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), assurant ainsi aux clients un niveau de sécurité optimal.

Thomas Fauré, Président Fondateur de Whaller, déclare : *« La sécurité de nos utilisateurs est au cœur de nos préoccupations depuis la naissance de Whaller. Avec la création de notre **CSIRT**, nous franchissons une nouvelle étape dans notre engagement à leur offrir un environnement de communication et de collaboration toujours plus sécurisé et fiable. »*

Cyril Bras, Directeur Cybersécurité de Whaller et VP d'Hexatrust, ajoute : *« Notre **CSIRT** nous permet de réagir encore plus efficacement face aux cybermenaces et de renforcer la confiance de nos utilisateurs. Nous sommes déterminés à leur offrir un niveau de sécurité optimal et à les accompagner dans la protection de leurs données. »*

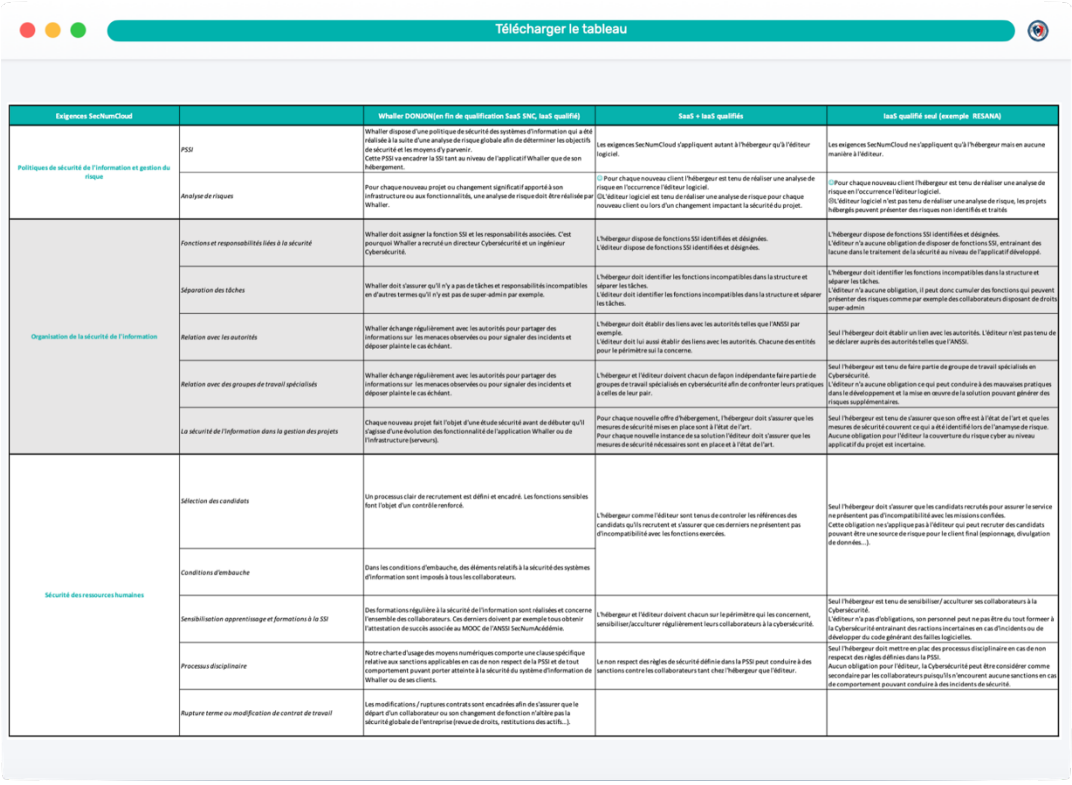
Une démarche globale de sécurisation des données

Le CSIRT Whaller est localisé en France et a pour missions :

- la réponse à incident,
- le suivi des vulnérabilités,
- l'analyse des codes malveillants,
- la collecte d'artefacts techniques (IOC),
- être le point de contact unique pour les incidents d'origine cyber internes ou externes,
- assurer une veille sur la menace en interne et en externe.

Le lancement du **CSIRT Whaller** s'inscrit dans une démarche globale de sécurisation des données et de renforcement de la résilience face aux cybermenaces. En effet, **Whaller DONJON, la solution SaaS la plus sécurisée de Whaller, est actuellement en cours de qualification SecNumCloud**, la qualification délivrée par l'ANSSI aux prestataires de services cloud répondant aux exigences les plus élevées en matière de sécurité.

En outre, Whaller a récemment publié un **comparatif des solutions SaaS Qualifiées SecNumCloud et des solutions reposant uniquement sur un hébergement qualifié (IaaS).** Ce comparatif met en évidence les différences entre ces deux types d'offres et démontre l'insuffisance des solutions qui ne sont pas elles-mêmes qualifiées SecNumCloud.



Exigences SecNumCloud		Whaller DONJON(en fin de qualification SaaS SNC, IaaS qualifié)	SaaS + IaaS qualifiés	IaaS qualifié seul (exemple RESANA)
Politiques de sécurité de l'information et gestion du risque	PSSI	Whaller dispose d'une politique de sécurité des systèmes d'information qui a été réalisée à la suite d'une analyse de risque globale afin de déterminer les objectifs de sécurité et les moyens d'y parvenir. Cette PSSI va encadrer la SSI tant au niveau de l'applicatif Whaller que de son hébergement.	Les exigences SecNumCloud s'appliquent autant à l'hébergeur qu'à l'éditeur logiciel.	Les exigences SecNumCloud ne s'appliquent qu'à l'hébergeur mais en aucune manière à l'éditeur.
	Analyse de risques	Pour chaque nouveau projet ou changement significatif apporté à son infrastructure ou aux fonctionnalités, une analyse de risque doit être réalisée par Whaller.	☐ Pour chaque nouveau client l'hébergeur est tenu de réaliser une analyse de risque en l'occurrence l'éditeur logiciel. ☐L'éditeur logiciel est tenu de réaliser une analyse de risque pour chaque nouveau client ou lors d'un changement impactant la sécurité du projet.	☐Pour chaque nouveau client l'hébergeur est tenu de réaliser une analyse de risque en l'occurrence l'éditeur logiciel. ☒L'éditeur logiciel n'est pas tenu de réaliser une analyse de risque, les projets hébergés peuvent présenter des risques non identifiés et traités
Organisation de la sécurité de l'information	Fonctions et responsabilités liées à la sécurité	Whaller doit assigner la fonction SSI et les responsabilités associées. C'est pourquoi Whaller a recruté un directeur Cybersécurité et un ingénieur Cybersécurité.	L'hébergeur dispose de fonctions SSI identifiées et désignées. L'éditeur dispose de fonctions SSI identifiées et désignées.	L'hébergeur dispose de fonctions SSI identifiées et désignées. L'éditeur n'a aucune obligation de disposer de fonctions SSI, entrainant des lacune dans le traitement de la sécurité au niveau de l'applicatif développé.
	Séparation des tâches	Whaller doit s'assurer qu'il n'y a pas de tâches et responsabilités incompatibles en d'autres termes qu'il n'y est pas de super-admin par exemple.	L'hébergeur doit identifier les fonctions incompatibles dans la structure et séparer les tâches. L'éditeur doit identifier les fonctions incompatibles dans la structure et séparer les tâches.	L'hébergeur doit identifier les fonctions incompatibles dans la structure et séparer les tâches. L'éditeur n'a aucune obligation, il peut donc cumuler des fonctions qui peuvent présenter des risques comme par exemple des collaborateurs disposant de droits super-admin
	Relation avec les autorités	Whaller échange régulièrement avec les autorités pour partager des informations sur les menaces observées ou pour signaler des incidents et déposer plainte le cas échéant.	L'hébergeur doit établir des liens avec les autorités telles que l'ANSSI par exemple. L'éditeur doit lui aussi établir des liens avec les autorités. Chacune des entités pour le périmètre sui la concerne.	Seul l'hébergeur doit établir un lien avec les autorités. L'éditeur n'est pas tenu de se déclarer auprès des autorités telles que l'ANSSI.
	Relation avec des groupes de travail spécialisés	Whaller échange régulièrement avec les autorités pour partager des informations sur les menaces observées ou pour signaler des incidents et déposer plainte le cas échéant.	L'hébergeur et l'éditeur doivent chacun de façon indépendante faire partie de groupes de travail spécialisés en cybersécurité afin de confronter leurs pratiques à celles de leur pair.	Seul l'hébergeur est tenu de faire partie de groupe de travail spécialisés en Cybersécurité. L'éditeur n'a aucune obligation ce qui peut conduire à des mauvaises pratiques dans le développement et la mise en œuvre de la solution pouvant générer des risques supplémentaires.
	La sécurité de l'information dans la gestion des projets	Chaque nouveau projet fait l'objet d'une étude sécurité avant de débuter qu'il s'agisse d'une évolution des fonctionnalité de l'application Whaller ou de l'infrastructure (serveurs).	Pour chaque nouvelle offre d'hébergement, l'hébergeur doit s'assurer que les mesures de sécurité mises en place sont à l'état de l'art. Pour chaque nouvelle instance de sa solution l'éditeur doit s'assurer que les mesures de sécurité nécessaires sont en place et à l'état de l'art.	Seul l'hébergeur est tenu de s'assurer que son offre est à l'état de l'art et que les mesures de sécurité couvrent ce qui a été identifié lors de l'anamyse de risque. Aucune obligation pour l'éditeur la couverture du risque cyber au niveau applicatif du projet est incertaine.
Sécurité des ressources humaines	Sélection des candidats	Un processus clair de recrutement est défini et encadré. Les fonctions sensibles font l'objet d'un contrôle renforcé.	L'hébergeur comme l'éditeur sont tenus de controler les références des candidats qu'ils recrutent et s'assurer que ces derniers ne présentent pas d'incompatibilité avec les fonctions exercées.	Seul l'hébergeur doit s'assurer que les candidats recrutés pour assurer le service ne présentent pas d'incompatibilité avec les missions confiées. Cette obligation ne s'applique pas à l'éditeur qui peut recruter des candidats pouvant être une source de risque pour le client final (espionnage, divulgation de données...).
	Conditions d'embauche	Dans les conditions d'embauche, des éléments relatifs à la sécurité des systèmes d'information sont imposés à tous les collaborateurs.		
	Sensibilisation apprentissage et formations à la SSI	Des formations régulière à la sécurité de l'information sont réalisées et concerne l'ensemble des collaborateurs. Ces derniers doivent par exemple tous obtenir l'attestation de succès associée au MOOC de l'ANSSI SecNumAcadémie.	L'hébergeur et l'éditeur doivent chacun sur le périmètre qui les concernent, sensibiliser/acculturer régulièrement leurs collaborateurs à la cybersécurité.	Seul l'hébergeur est tenu de sensibiliser/acculturer ses collaborateurs à la Cybersécurité. L'éditeur n'a pas d'obligations, son personnel peut ne pas être du tout formeer à la Cybersécurité entrainant des ractions incertaines en cas d'incidents ou de développer du code générant des failles logicielles.
	Processus disciplinaire	Notre charte d'usage des moyens numériques comporte une clause spécifique relative aux sanctions applicables en cas de non respect de la PSSI et de tout comportement pouvant porter atteinte à la sécurité du système d'information de Whaller ou de ses clients.	Le non respect des règles de sécurité définie dans la PSSI peut conduire à des sanctions contre les collaborateurs tant chez l'hébergeur que l'éditeur.	Seul l'hébergeur doit mettre en plac des processus disciplinaire en cas de non respect des règles définies dans la PSSI. Aucun obligation pour l'éditeur, la Cybersécurité peut être considérer comme secondaire par les collaborateurs puisqu'ils n'encourent aucune sanctions en cas de comportement pouvant conduire à des incidents de sécurité.
	Rupture terme ou modification de contrat de travail	Les modifications / ruptures contrats sont encadrées afin de s'assurer que le départ d'un collaborateur ou son changement de fonction n'altère pas la sécurité globale de l'entreprise (revue de droits, restitutions des actifs...).		

Figure 1 - Comparatif des solutions SaaS Qualifiées SecNumCloud et des solutions reposant seulement sur un hébergement qualifié (IaaS)

Whaller

À propos de Whaller :

Whaller est une plateforme sociale et collaborative sécurisée pouvant accueillir plusieurs milliers de personnes. Whaller est le seul outil simple et complet pouvant répondre à un spectre aussi large d'usages. Whaller permet de construire des réseaux collaboratifs de toutes tailles et de toutes natures et ce, pour tous types de structures : entreprises, administrations, associations, écoles et universités, institutions, ministères, familles… L'incessibilité et la non-exploitation des données personnelles constituent deux principes fondamentaux de la plateforme. En se basant sur des communautés appelées des « sphères », indépendantes les unes des autres, Whaller permet à ses utilisateurs de maîtriser leurs communautés, leurs communications et leurs audiences. Whaller a été créé en 2013 par Thomas Fauré, la plateforme regroupe aujourd'hui plus de 1 000 000 utilisateurs pour 50 000 réseaux créés. https://whaller.com

Contacts Presse :

Whaller
Grégory Saccomani, Directeur Marketing et Communication
gregory.saccomani@whaller.fr