Whaller

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

Contexte : *un grand nombre d'éditeurs logiciels (SaaS) s'affichent comme étant "SecNumCloud" alors qu'elles ne reposent que sur une infrastructure qualifiée SNC, sans être elles-mêmes qualifiées. L'objet de ce comparatif est d'exposer les différences que cela implique et de montrer l'insuffisance de telles offres. Ce comparatif expose aussi ce que l'offre* **Whaller DONJON, première plateforme collaborative à obtenir le Visa de sécurité ANSSI pour sa qualification SecNumCloud**,*met en pratique. Ce tableau reprend toutes les exigences du référentiel SecNumCloud v3.2.*

Exigences SecNumCloud		Whaller DONJON, solution collaborative qualifiée SecNumCloud	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 SecNumAcédémie.	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 puvant 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 respecxt 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…).		

Whaller

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

Contexte : *un grand nombre d'éditeurs logiciels (SaaS) s'affichent comme étant "SecNumCloud" alors qu'elles ne reposent que sur une infrastructure qualifiée SNC, sans être elles-mêmes qualifiées. L'objet de ce comparatif est d'exposer les différences que cela implique et de montrer l'insuffisance de telles offres. Ce comparatif expose aussi ce que l'offre* **Whaller DONJON, première plateforme collaborative à obtenir le Visa de sécurité ANSSI pour sa qualification SecNumCloud**,*met en pratique. Ce tableau reprend toutes les exigences du référentiel SecNumCloud v3.2.*

Exigences SecNumCloud		Whaller DONJON, solution collaborative qualifiée SecNumCloud	SaaS + IaaS qualifiés	IaaS qualifié seul (exemple RESANA)
Gestion des actifs	*Inventaire et propriété des actifs*	L'ensemble des actifs matériels et immatériels de Whaller sont répertoriés et un responsable désigné.	L'hébergeur doit inventorier ses actifs matériels et immatériels et désigner pour chacun d'eux un propriétaire. L'éditeur doit inventorier ses actifs matériels et immatériels et désigner pour chacun d'eux un propriétaire.	Seul l'hébergeur doit réaliser un inventaire de ses actifs matériels et immatériels et leur attribuer un propriétaire. L'éditeur n'a pas d'obligation d'inventaire, ce qui peux conduire à des défauts de suivi dans la vie des actifs (oublis dans le renouvellement de certificats, loggiciels obsolètes…).
	Restitution des actifs	Des procédures encadrent la restitution des actifs par les collaborateurs ou partenaires.	L'hebergeur et l'éditeur sont tenus de disposer de procédures encadrant la restitution d'actifs	Seul l'hébergeur est tenu de mettre en œuvre des procédures de restitutions des actifs. L'éditeur n'a aucune obligation ce qui peut augmenter les risques liés au projet (un collaborateur emporte avec lui des informations de clients alors qu'il quitte la structure).
	Identification des besoins de sécurité de l'information	La mise en application de la PSSI s'appuie sur un SMSI qui permet de s'assurer que les mesures/exigences de sécurité en vigueur sont toujours cohérentes avec les exigences règlementaires ou celles spécifiques de nos clients.	Les analyses de risque réalisés par l'hébergeur et l'éditeur chacun sur leur périmètre permettent de mettre en œuvre les mesures de sécurité adéquates pour protéger les actifs.	Seul l'hébergeur doit à partir des analyses de risque réalisées, mettre en œuvre les mesure de sécurité adéquate pour la protection de ses actifs. L'éditeur n'a aucune obligation, aucune garantie pour le client que les mesures de sécurité adpatées à la protection des actifs sont en place.
	Marquage et manipulation de l'information	Whaller dispose d'une politique de classification et de marquage de l'information qui permet de garantir un juste niveau de protection de l'information en fonction de sa sensibilité. La mise en application du principe du "droit d'en connaitre" permet de limiter les risques de fuite/divulgation accidentelle de l'information	L'hébergeur et l'éditeur sont tenus de mettre en place une politique de classification de l'information afin d'une part de définir la criticité d'une information et d'autre part définir les mesures de sécurité applicables à la protection de l'information.	Seul l'hébergeur est tenu de mettre en eouvre une politique de classification de l'information et les mesures de sécurité associées. L'éditeur n'a aucune obligation, la protection de l'information confiée par le client est incertaine
	Gestion des supports amovibles	L'utilisation de supports amovibles est proscrite.	L'hébergeur et l'éditeur doivent définir une politique d'usage des supports amovibles.	Seul l'hébergeur est tenu de définir une politique d'usage des supports amovibles et les mesures de protections associées pour son périmètre. L'éditeur n'a aucune obligation, les supports amovibles peuvent être à l'origine d'incident de sécurité (codes malveillants, fuite de données…).
Contrôle d'accès et gestion des identités	*Politique de contrôle d'accès*	Des revues de droits sont réalisées et documentées, une matrice des droits incompatibles est établie.	Les droits d'accès à l'infrastructure doit être encadré pour l'hébergeur et ses collaborateurs. Il en est de même pour l'éditeur qui doit définir les accès à l'applicatif mais également à ses serveurs hébergés en IaaS.	Les droits d'accès à l'infrastructure doit être encadré pour l'hébergeur et ses collaborateurs. L'éditeur n'a pas d'obligations, la gestion des droits d'accès à l'applicatif ou au serveur n'est pas garantie au client final.
	Enregistrement et desinscription des utilisateurs	Des procédures encadrent la gestion des droits utilisateurs dans l'aplication Whaller (pour nos clients) mais également dans le reste du SI de Whaller		
	Gestion des droits d'accès	Des revues de droits sont réalisées et documentées, une matrice des droits incompatibles est établie.	L'hébergeur doit assurer des revues de droits d'accès et des privilèges accordés à ses collaborateurs amis également à ses clients. L'éditeur doit assurer des revues de droits d'accès et des privilèges accordés à ses collaborateurs sur l'applicatif, les serveurs, le SI de sa structure,	L'hébergeur doit assurer des revues de droits d'accès et des privilèges accordés à ses collaborateurs amis également à ses clients. L'éditeur n'est tenu à aucune obligation, des collaborateurs peuvent cumuler des droits au fur et à mesure qu'ils changent de postes, des comptes de personnes ayant quitté la structure peuvent être toujours actifs…
	revue des droits utilisateurs			
	Gestion des authentifications des utilisateurs	L'authentifiction à facteur multiples est la règle dans l'application Whaller. Pour les collaborateurs Whaller l'utilisation d'authentification à facteurs multiples (OTP, carte à puce…) est en vigueur sur l'ensemble des outils utilisés pour assurer le service.	L'hébergeur doit mettre en place des mesures d'authentification correspondant à l'état de l'art pour ses clients. L'éditeur doit lui aussi mettre en place des mesures d'authentification à l'état de l'art pour ses clients.	L'hébergeur doit mettre en place des mesures d'authentification correspondant à l'état de l'art pour ses clients. L'éditeur n'est pas tenu de mettre en place des mesures d'auhtneitfiation à l'état de l'art entraiant des risques pour le client et la protection de ses accès.
	Accès aux interfaces d'administration	Les interfaces d'administration de la plateforme Whaller sont distinctes de l'accès utilisateur. Des politique de filtrage sont en place et encadrent les modalités d'accès. L'administration système est réalisée à partir de poste dédis à partir d'un environnement dédié et isolé du reste du SI.	L'hébergeur doit mettre en œuvre des interfaces d'administrations dédiées pour la gestion des ressources. Les actions d'administration doivent être réalisée à partir d'un réseau dédié. L'éditeur doit mettre en place des interfaces d'administration distinctes des accès utilisateurs sur sa plateforme. Il doit également disposer d'un réseau d'administration dédié pour l'administration des serveurs.	L'hébergeur doit mettre en œuvre des interfaces d'administrations dédiées pour la gestion des ressources. Les actions d'administration doivent être réalisée à partir d'un réseau dédié. L'éditeur n'a aucune obligation, il peut donc utiliser les mêmes accès que les utilisateurs pour l'administration de sa plateforme entrainant des risques en cas de compromission. Il n'est pas tenu non plus de disposer de ressources dédiées pour l'administration des serveurs ce qui peut conduire à des risque d'intrusion ou d'actions malveillantes sur les serveurs.
	Restriction d'accès à l'information	Principe du moindre privilège en vigueur et application du principe du *"droit d'en connaitre"*.		

Whaller

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

Contexte : *un grand nombre d'éditeurs logiciels (SaaS) s'affichent comme étant "SecNumCloud" alors qu'elles ne reposent que sur une infrastructure qualifiée SNC, sans être elles-mêmes qualifiées. L'objet de ce comparatif est d'exposer les différences que cela implique et de montrer l'insuffisance de telles offres. Ce comparatif expose aussi ce que l'offre* **Whaller DONJON, première plateforme collaborative à obtenir le Visa de sécurité ANSSI pour sa qualification SecNumCloud**,*met en pratique. Ce tableau reprend toutes les exigences du référentiel SecNumCloud v3.2.*

Exigences SecNumCloud		Whaller DONJON, solution collaborative qualifiée SecNumCloud	SaaS + IaaS qualifiés	IaaS qualifié seul (exemple RESANA)
Cryptologie	*Chiffrement des données stockées*	Une politique de chiffrement est en vigueur et impose le chiffrement des serveurs. Les données sont ainsi protégées des actions de maintenance de l'hébergeur (ex : changement de disque) et les clefs de chiffrement ne sont pas accessibles pour l'hébergeur. L'ensemble des postes de travail des collaborateurs sont chiffrés, des conteneurs chiffrés sont utilisés pour le transfert de l'information en fonction du niveau de classification appliqué.	L'hébergeur est tenu de mettre à disposition de son client des mesures de chiffrement, Il doit également mettre en œuvre du chiffrement en interne pour la protection des informations. L'éditeur est tenu de mettre en œuvre des mesures de chiffrement de l'information clients stockées sur ses serveurs. il doit également mettre en oeuvre du chiffrement pour la protection des informations sur les terminaux utilisés par es collaborateurs.	L'hébergeur est tenu de mettre à disposition de son client des mesures de chiffrement, Il doit également mettre en œuvre du chiffrement en interne pour la protection des informations. L'éditeur n'a pas d'obligation concernant la mise en œuvre du chiffrement des données des clients ou de mettre en œuvre les mesures proposées par l'hébergeur ou encore les postes des collaborateurs. La protection de l'information confiée par le client est incertaine.
	Chiffrement des flux	La politique de chiffrement impose une utilisation exclusive de flux de données chiffrés.	L'hébergeur et l'éditeur sont tenus d'utiliser des protocoles de transmission sécurisés et chiffrés	Seul l'hébergeur est tenu de chiffrer l'intégralité des flux. Léditeur peut utiliser des protocoles non chiffrés dans le fonctionnement de l'applicatif qu'il propose ou de manière générale dans ses usages. La confidentialité des échanges n'est pas garantie.
	Hachage des mots de passe	La politique de mot de passe impose la mise en œuvre de chiffrement non réversible avec du salt en respectant les critères définis par l'ANSSI.	Les hachages de mots de passe utilisés tant par l'hébergeur que l'éditeur doivent respecter les recommandations de l'ANSSI et ne doivent pas être réversibles	Seul l'hébergeur doit utiliser des algotrithmes de hachage validés par l'ANSSI. L'éditeur n'a pas d'obligation, les algorithmes utilisés pour le hachage peuvent présenter des faiblesse. La protection des secrrets n'est pas garantie.
	Non répuditation			
	Gestion des secrets	L'utilisation de coffre fort à mots de passe permet de garantir la protection des secrets. Des coffres distincts sont utilisés en fonction des usages.	L'hébergeur et l'éditeur doivent chacun pour leur périmètre respectifs mettre en œuvre des mesures de protection des secrets et disposer de politique en encadrant les modalités de transmission.	Seul l'hébergeur doit mettre en œuvre des mesures de protection des secrets et disposer de politique en encadrant les modalités de transmission. L'éditeur n'a aucune obligation, les secrets peuvent être insuffisament protégés.
	Racines de confiance	La politique de certification impose l'utilisation de certificats délivrés par des autorités de confiance au sens RGS et/ou EIDAS.	L'hébergeur et l'éditeur doivent recourrir à des autorités de confiance pour la délivrance de certificats sur les services proposés aux clients.	Seul l'hébergeur doit s'appuyer sur des autoriés de confiance pour la délivrance de certificats électroniques. L'éditeur n'a aucun obligation et peut donc faire usage de certificats auto-signés ou n'apportant pas de garanties sur l'autenticité du service.
Sécurité physique et envrionnementale	*Périmètre de sécurité physique*	Des zones de sécurité sont définies dans les locaux de Whaller afin de segmenter physiquement les activités en fonction de leur sensibilité.	L'hébergeur doit mettre en place des mesures de sécurité physique pour l'accès à ses locaux qu'il s'agisse des salles serveurs mais aussi des pièces utiliées par les collaborateurs. L'éditeur doit lui aussi mettre en place du contrôle physique de ses locaux utilisés par les collaborateurs.	Seul l'hébergeur est tenu de mettre en place du contrôle d'accès physique à ses locaux techniques ou administratifs. Aucune obligation pour l'éditeur ce qui peut augmenter le risque d'intrusio physique sur site et la mise en place de pièges numériques sur les installations sensibles.
	Contrôle d'accès physique	Un contrôle d'accès physique par badge est en vigeur pour controler les accès aux différentes zones en fonction des habilitations des collaborateurs.		
	Protection contre les menaces extérieures et environnementales	Une politique de sécurité physique et environementale encadre les mesures auxquelles doivent s'astreindre les collaborateurs de Whaller afin de se prémunir des risques sur la couche physique.	L'hébergeur et l'éditeur sont tenus de définir une politique de sécurité environmentale et physique et d'intégrer ces risques dans les analyses de risque réalisées.	Seul l'hébergeur doit prendre des mesures pour se protéger des menaces exterieures et environementales. L'éditeur n'a aucune obligation, réaction incertaine en cas d'incident sur la couche physique (incendie, inondation, cambriolage...).
	Travail dans les zones privées et sensibles	Une politique spécifique décrit précisement ce qu'il est possible de faire d'un point de vue numérique dans chacune des zones physiques ainsi que les conditions d'accès.	L'hébergeur et l'éditeur sont tenus de définir un zonage physique de leurs sites avec mises en place de mesures de sécurité associée à la sensibilité des zones mais également un processus d'habilitation des personnels pour entrer des les zones en question.	Seul l'hébergeur est tenu de mettre en place une segmentation physique de ses locaux et de définir des politiques d'accès. L'éditeur n'a aucune obligation, les équipements sensibles ne sont pas forcément protégés correctement.
	Sécurité du câblage	Le câblage de notre site de Suresnes à été intégralement refait en s'appuyant sur les recommandations du guide ANSSI.	L'hébergeur et l'éditeur sont tenus de s'assurer que le câblage informatique n'est pas exposé à des menaces externes telles que des écoutes ou du sabotage par exemple.	Seul l'hébergeur doit sécuriser son câblage. L'éditeur n'a aucune obligation, le câblage n'est paeut être pas maitrisé et des écoutes ou du piégeage sont possibles.
	Maintenance des matériels	Des procédures spécifiques décrivent les meusres de protection qui doivent être mise en œuvre pour protéger les actifs tout au long de leur vie.	L'hébergeur comme l'éditeur sont tenus de définir des procédures documentées pour la gestion des matériels que ce soit lors du stockage, du recyclage ou quand ces derniers quittent l'entreprise.	L'hébergeur est tenu de définir des procédures pour la gestion des matériels. L'éditeur n'a aucune obligation, des risques pour la sécurité des informations confiées existent pa rexemple lorsqu'un matériel est mis au rebus, il contient êut être encore des données confidentielles.
	Sortie des actifs			
	Recyclage sécurisé du matériel			
	Matériel en attente d'utilisation			

Whaller

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

Contexte : *un grand nombre d'éditeurs logiciels (SaaS) s'affichent comme étant "SecNumCloud" alors qu'elles ne reposent que sur une infrastructure qualifiée SNC, sans être elles-mêmes qualifiées. L'objet de ce comparatif est d'exposer les différences que cela implique et de montrer l'insuffisance de telles offres. Ce comparatif expose aussi ce que l'offre* **Whaller DONJON, première plateforme collaborative à obtenir le Visa de sécurité ANSSI pour sa qualification SecNumCloud**,*met en pratique. Ce tableau reprend toutes les exigences du référentiel SecNumCloud v3.2.*

Exigences SecNumCloud		Whaller DONJON, solution collaborative qualifiée SecNumCloud	SaaS + IaaS qualifiés	IaaS qualifié seul (exemple RESANA)
Sécurité liée à l'exploitation	*Procédures d'exploitation documentées*	Une centaine de procdéures d'exploitation sont rédigées et actualisées par la direction Technique de Whaller afin de couvrir l'ensemble des services nécessaires au bon fonctionnement de l'application Whaller et son système d'information.	L'hébergeur et l'éditeur sur leurs périmètres respectifs sont tenus de rédiger des procédures d'exploitation afin de documenter l'ensemble des opérations/configurations nécessaires au rendu du service.	Seul l'hébergeur est tenu de documenter le fonctionnement de son SI. L'éditeur n'a aucune obligation.
	Gestion des changements	Les changements sont encadrés par une procédure stricte qui implique par exemple de documenter les modifications apportées, de réaliser des tests, des analmyses d'impact ou de risques...	L'hébergeur et l'éditeur doivent avoir des procédures de gestion du changement afin d'éviter les régressions mais également de s'assurer que la sécurité n'est pas mise à mal par des évolutions.	Seul l'hébergeur doit avoir des procédures de gestion du changement. L'éditeur n'a pas d'obligation, les évolutions du produit peuvent entrainer des regressions ou ne pas garantir un niveau de sécurité équivalent.
	Séparation des environnements de dev/test/exploitation	Mise en œuvre des environnements de dev, de tests et de production différents.	L'hebergeur comme l'éditeur doivent disposer d'environnement de développement, de test et de productions distincts.	Seul l'hébergeur a une obligation de disposer d'une infrastructure dédiée au développement une autre pour les tests et enfin une pour la production. L'éditeur n'a aucune obligation, il n'y a donc pas de garantie pour le client que l'éditeur ne travaille pas directement sur la production.
	Mesures contre les codes malveillants	L'ensemble de nos serveurs sont équipés de solutions de détection de codes malveillants. L'ensemble des évenements étant reportés sous forme d'alertes dans notre SIEM.	L'herbergeur et l'éditeur ont l'obligation de mettre en place des mesures de protection contre les codes malveillant sur l'intégralité de leur SI, mais également de superviser l'activité détectée par les outils de lutte contre les codes malveillants.	Seul l'hebergeur a des obligations vis-à-vis de la protection contgre les codes malveillants. L'éditeur n'a aucune obligation ce qui peut se traduire par l'absence de solution antivirale sur les postes de travail des collaborateurs ou les serveurs utilisés pour le service commercialisé aux clients.
	Sauvegarde des informations	Une politique de sauvegarde a été définie impliquant une revue mensuelle des sauvegardes, de réaliser chaque mois des tests de restauration et de réaliser des sauvegrdes hors ligne.	L'hébergeur et l'éditeur ont pour obligation de mettre en œuvre uen politique de sauvegarde incluant la sauvegarde des données des clients, de mettre en œuvre les mesures nécessaires pour protéger ces dernières, mais aussi de réaliser des tests de restauration.	Seul l'hebergeur a l'obligation de mettre en œuvre une politique de sauvegarde. L'éditeur n'a aucune obligation, le client n'a aucune assurance que des sauvegardes à l'état de l'art sont réalisés ou que des tests de restaurations sont effectués.
	Journalisation des évenements	L'ensemble des serveurs et composants impliqués dans la fourniture du service sont journalisés. Les informations ainsi générées sont ensuite centralisées sur un puits de log opéra par Whaller.	L'hébergeur comme l'éditeur sont tenus de définir une politique de journalisation des évenements de sécurité sur l'ensemble du périmètre (journalisation des serveurs, des composants réseaux mais également de l'applicatif).	Seul l'hébergeur est tenu de mettre en œuvre une politique de journalisation. L'éditeur n'a aucune obligation, il n'est pas certain qu'en cas d'incident l'éditeur sera en mesure de produire les traces relatives à l'incident rendant par exemple le dépôt de plainte difficile.
	Protection de l'information journalisée	La politique de journalisation mise en place impose une protection des journaux contre les accès illégitime. Ainsi es journaux sont chiffrés avec une clef détenue par des personnels habilités.	L'hébergeur et l'éditeur sont tenus de protéger les journaux collectés contre les accès illégitimes.	Seul l'hébergeur est tenu de protéger les journaux collectés contre les actions illégitimes. L'éditeur n'a aucune obligation, l'intégrité et la confidantialité des journaux ne peut être garantie.
	Synchronisation des horloges	La politique de journalisation impose une synchronisation de l'ensemble des ressources sur la même source de temps.	L'hébergeur et l'éditeur sont tenus de synchroniser l'ensemble des horloges de ses serveurs et composants sur une même source de temps.	Seul l' hébergeur doit synchronirser les horloges de ses serveurs et composants sur une source unique de temps. L'éditeur n'a aucune obligation, ainsi ses serveurs peuvent ne pas présenter la même heure, les journaux d'activité des différentes ressources seront difficilement exploitables en cas d'incident.
	Analyse et corrélationdes évenments	L'ensemble des évenements de sécurité sont reportés dans notre SIEM. Ce dernier dispose de nombreuses alertes permettant la détection d'activité potentiellement malveillante. Les données provenant des activités suspectes sont capitalisées dans une instance MISP permettant la corrélation des évenements mais aussi le partage avec les services cybersécurité de nos clients des données afin de contribuer à leur protection.	L'hébergeur et l'éditeur sont tenus sur leur périmètre respectif d'analyser les évenements de sécurité qui s'y produise et d'être en capacité de les corréler avec d'autres sources d'informations.	Seul l'hebergeur est tenu d'analyser ce qu'il se passe sur les ressources numériques de son périmètre. L'éditeur n'a aucune obligation, la détection d'incident de sécurité est alors incertaine.
	Installation de logiciels sur des systèmes en exploitation	La liste des logiciels sur les serveurs ou les postes utilisateurs est inventoriée, des dispositifs permettent de maitriser ce qui peut être installé. Enfin des procédures d'exploitation encadrent l'installation de logiciels sur les serveurs en exploitation afin d'éviter des effets de bords ou régression.	L'hébergeur et l'éditeur sont tenus de connaitre et mainteniur la liste des logiciels et systèmes d'exploitation installés sur leur périmètre respectif. Ils doivent également s'assurer de ne pas faire usage de solutions qui ne soient plus maintenues ou obsolètes	Seul l'hébergeur sur le périmètre du service rendu doit s'assurer de lister les logiciels et systèmes d'exploitation utilisés et de ne pas recourrir à des solutions obsolètes. L'aditeur n'a aucune obligation, ainsi rien n'empêche l'éditeur d'utiliser des logiciels ou des systèmes d'exploitation obsolètes sur des serveurs pourtant hébergés enenvironnement qualifié SecNumCloud
	Gestion des vulnérabilités techniques	Une politique de gestion des correctifs de sécurité est en vigueur et encadre le déploiement des correctifs de sécurité en fonction de leur criticité. Nous nous appuyons sur des outils nous permettant de suivre en temps réel le niveau de vulnérabilité de nos ressources et d'en piloter le MCS (Maintien en Condition de Sécurité)	L'hébergeur et l'éditeur sont tenus d'assurer le MCS des différents composants qu'ils administrent. Ils doivent définir une politique d'application des correctifs de sécurité.	Seul l'hébergeur est tenu d'assurer le MCS des ressources qu'il exploite. L'éditeur n'a aucune obligation, ainsi des systèmes non mis à jour et présentant des vulnérabilités peuvent être présentes sur l'infrastructure qualifiée SecNumCloud.
	Administration	L'administration est réalisée à partir de postes dédiés déconnectés d'Internet. Une segmentation réseau est en place au iveau des serveurs mais aussi de nos locaux de Suresnes avec des règles de filtrage interdisant les communications ers le réseau d'admin et entre les différents réseaux. De la rupture protocolaire est en place ausune ressource n'étant administrée directement.	L'hébergeur et l'éditeur sont tenus de mettre en place des réseaux et des équipements dédiés aux tâches d'administration et isolé des autres réseaux dont Internet. Ils sont tenus de respecter le guide d'hygiène numérique de l'ANSSI.	Seul l'hébergeur doit sur son périmètre disposer de ressources dédiés à l'administration, ces ressources ne doivent pas accéder à Internet. L'éditeur n'a aucune obligation, l'administration des serveurs qualifiés peut être réalisée à partir d'un poste de travail standard accédant à Internet augmentant ainsi le risque d'intrusion sur le système hébergeant les données du client.
	Télédiagnostic et télémaintenance des composants de l'infrastructure	La supervision de notre installation est uniquement opérée à partir de nos propres serveurs avec un respect des flux de données. La maintenance est opérée exclusivement à partir de matériels dédiés.	L'hébergeur et l'éditeur doivent assurer la télémaintenance des installations en s'appuyant sur des outils d'accès distants sécurisés (VPN IPSEC). Les flux de supervision ne doivent pas contrevenir aux bonnes pratiques d'utilisation de pare-feu.	Seul l'hébergeur est tenu d'utiliser des protocoles sécurisés pour la supervision et l'administration des insatllations sous son contrôle. L'éditeur n'a aucune obligation, le client n'a aucune garantie sur les pratiques de l'éditeur concernant la supervision et la maintenance à distance. Les bonnes pratiques d'administrations ne sont pas garanties augemenant le risque d'intrusion sur les sytèmes opérés par l'éditeur.
	Surveillance des flux sortants de l'infrastructure	Des sondes de détection réseau sont déployées dans notre infrastructure afin de controler les flux de données et détecter des siutations anormales, le tout étant couplé à notre SIEM. Les flux sortants sont maitrisés par des règles de filtrage.	L'hébergeur comme l'éditeur ont l'obligation de mettre en œuvre des mesures organisationnelles et techniques afin de contrôler les flux sortants du SI.	Seul l'hébergeur doit sur son périmètre mettre en œuvre les mesures de supervision des flux sortants. L'éditeur n'a pas d'obligation, ce qui peut conduire d'une part à des flux sortants sans contrôle (pas de filtrage en sortie) mais également l'incapacité à détecter une fuite de données ou globalement du trafix sortant anormal.

Whaller

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

Contexte : *un grand nombre d'éditeurs logiciels (SaaS) s'affichent comme étant "SecNumCloud" alors qu'elles ne reposent que sur une infrastructure qualifiée SNC, sans être elles-mêmes qualifiées. L'objet de ce comparatif est d'exposer les différences que cela implique et de montrer l'insuffisance de telles offres. Ce comparatif expose aussi ce que l'offre* **Whaller DONJON, première plateforme collaborative à obtenir le Visa de sécurité ANSSI pour sa qualification SecNumCloud**,*met en pratique. Ce tableau reprend toutes les exigences du référentiel SecNumCloud v3.2.*

Exigences SecNumCloud		Whaller DONJON, solution collaborative qualifiée SecNumCloud	SaaS + IaaS qualifiés	IaaS qualifié seul (exemple RESANA)
Sécurité des communications	*Cartographie du système d'information*	Une cartographie de notre SI est maintenue à jour par la direction technique de Whaller.	L'hébergeur et l'éditeur doivent maintenir à jour une cartographie de leurs SI respectifs.	Seul l'hébergeur doit maintenir à jour une cartographie de son SI. L'éditeur n'a pas d'obligation, l'abasence de cartographie maintenue à jour peut conduire à des faiblesses avec un SI partiellement ou en tatoalité non maitrisé.
	Cloisonnement des réseaux	Chaque environnement Whaller Donjon est spécifique pour chaque client, et au sein de cet environnement du cloisonnement réseau est en place afin d'assurer la défense en profondeur. Il en est de même pour l'ensemble du SI de Whaller, offre standard, postes clients... Un découpage réseau est réalisé sur le site de Suresnes avec des règles de filtrage entre ces derniers.	L'hébergeur comme l'éditeur sont tenus de mettre en œuvre des mesures de défense en profoncdeur en définissant des règles entre les différentes zones du SI.	Seul l'hébergeur est tenu de mettre en œuvre des mesures de cloisonnement. L'éditeur n'a aucune obligation ainsi le SI de l'éditeur peut être poreux et faciliter les mouvements latéraux opérés par des attaquants. Les données et/ou infrmation du clients peuvent être insuffisamment protégées.
	Surveillance des réseaux	L'ensemble des équipements réseaux est supervisé pour détecter les dysfonctionnements et les évenements sont centralisés dans le puits de log et notre SIEM.	L'herbergeur et l'éditeur ont l'obligation de mettre en place des mesures visant à surveiller l'activité sur les réseaux dont ils ont la charge. Les informations doivent remonter dans un SIEM et être analysées.	Seul l'hébergeur doit mettre en palce des mesures pour surveiller l'activité sur les réseaux dont il a la charge. L'éditeur n'a aucune obligation, le client n'a aucune assurance que l'activité réseau est analysée quotidiennement et que l'éditeur sera en capacité de détecter des actions malveillantes sur les réseaux dont il a la charge.
Acquisition développement et mainteance du SI	*Politique de développement sécurisé*	Une politique de développement sécurisé est en place et connue des développeurs. Ces derniers sont tenus de s'y conformer et des contrôles de conformité sont effectués. Cette politique vise notamment au respect des bonnes pratiques définies par l'OWASP. Des contrôles de conformité du code sont conduites.	L'hébergeur comme l'éditeur doivent sur leur périmètre mettre en œuvre une politique de développement sécurisée visant à s'assurer que le code produit est fait dans les règles de l'art en s'appuyant par exemple sur les règles de l'OWASP et que ce dernier ne génère pas des vulnérabilités dans l'application	Seul l'hébergeur doit mettre en palce une politique de développement sécurisé sur son périmètre. L'éditeur n'a aucune obligation ainsi en dépit d'un hébergement qualifié SecNumCloud, le client n'a aucune garantie que le code développé par l'éditeur ne présente pas de vulnérabilités et que ce dernier a été développé dans les règles de l'art comme par exemple els bonnes pratiques de l'OWASP.
	Procédure de contrôle des changements de système	Les changements sont encadrés par une procédure stricte qui implique par exemple de documenter les modifications apportées, de réaliser des tests, des analmyses d'impact ou de risques...	L'hébergeur comme l'éditeur doivent mettre en place des procédures visant à d'une part contrôler que les changements effectués sur le code n'apportent pas de faiblesses et que d'autre part il n'y a pas de régression fonctionnelle.	Seul l'hébergeur doit mettre en place des procédures de contrôle sur les changement apportés. L'éditeur n'a aucune obligation ainsi au fur et à mesure des évolutions apportées à son code, des vulnérabilités peuvent être ajoutées ou des régressions de fonctionnalités sont possibles et ne seront pas détectées avant la mise en production
	Revue technique des applications après changement apporté à la plateforme d'exploitation			
	Environnement de développement sécurisé	Le guide d'hygiène numérique de l'ANSSI est appliqué sur l'ensemble des postes de travail comme ceux des développeurs. Aucun collaborateur de Whaller ne dispose des droits d'administration de son poste de travail, l'intégralité des postes sont chiffrés et équipés de protection contre les codes malveillants (les évenement de sécurité sont remontés au SIEM).	L'hébergeur et l'éditeur doivent mettre en œuvre des mesures techniques et organisationnelles afin de garantir que l'environnement de développement est l'état de l'art en terme de sécurité.	Seul l'hébergeur à l'obligation demettre en œuvre des mesures techiques et oragnisationnelles visant à sécuriser l'environnement de développement. L'éditeur n'a aucune obligation, le client n'a aucune garantie que des mesures de sécurité physique, de protection des postes des développeurs ou de mani-ère générale que les bonnes pratiques sont mises en oeuvre lors des étapes de développmment.
	Développement externalisé	Whaller ne fait pas appel à des sociétés tierces pour le développement de son code applicatif.	L'hébergeur et l'éditeur sont tenus, dans lequel où ils font appel à du développement externalisés, de s'assurer que le sous-traitant n'est pas soumis à des lois extra-européennes, qu'il met en œuvre des mesures techniques et organisationnelles visant à garantir que le code produit respectera les contraintes auxquelles eux-mêmes sont soumis	Seul l'hébergeur dans le cas où se dernier sous-traite ses développement, doit s'assurer que le sous-traitant respecte les mêmes contraintes que celles auquel lui-même est soumis. L'éditeur n'a aucune restriction dans le recours à des sous-traitants pour toute ou partie de son code. Le client n'a aucune garantie que le code produit est produit en respectant les bonnes pratiques de développement sécurisé ou que l'entreprise sous-traitante ne présente pas de risque pour l'activité du client (espionnage, mise en oeuvre de portes dérobées...)
	Tests de sécurité et conformité du système	Des tests de sécurité sont réalisés par la direction Cyber de Whalller, mais également des prestaires qualifiés PASSI. Le contrôle de la conformité est également réalisé et les non conformités documentés avec mise en place d'un plan d'amélioration continue de la sécurité.	L'hébergeur et l'éditeur sont tenus de mettre en place des procédures de tests et des contrôles de conformité du système. Ces tests et contrôles doivent être documentés.	Seul l'hébergeur doit mettre en eouvre des tests de sécurité et des contrôle de conformité sur son SI. L'éditeur n'a aucune obligation, ainsi le client n'a aucune garantie que le code produit n'entraine pas la création de failles de sécurité. Aucun contrôle n'est obligatoire sur la mise en oeuvre des mesures définies dans la PSSI, si elle existe.
	Protection des données de test	Les données de tests ne comportent aucune données personnelles , leur stockage est réalisé conformément aux obligations définies dans la PSSI.	L'hébergeur comme l'éditeur doivent protéger les données qui sont utilisées pour les tests afin que ces dernières ne soient pas altérées.	Seul l'hébergeur doit protéger ses données de tests mais en aucune manières celles de l'éditeur s'il en possède.
Relations avec les tiers	*Identification des tiers*	Whaller tient à jour une liste de l'ensemble de ses fournisseurs.	L'hébergeur comme l'éditeur doivent tenir à jour une liste de l'ensemble de leurs fournisseurs intervenant dans la fourniture du service.	Seul l'hébergeur doit tenir à jour la liste des sous-traitants intervenants dans la fourniture du service. L'éditeur dans le cadre du RGPD doit tenir la liste des sous-traitants intervenant dans le traitement des données personnelles seulement.
	La sécurité dans les accords conclus avec les tiers	Pour tout nouveau contrat avec un sous-traitant un PAS (Plan d'Assurance Sécurité) est mis en place.	L'hébergeur comme l'éditeur doivent contractualiser avec leurs sus-traitans le niveau de sécurité, des contrôles de conformité doivent être réalisés. Un engagement de confidentialité doit être établi avec les sous-traitants participant au fonctoinnement du service.	Seul l'éditeur doit contractulaiser sa relation avec les tiers et s'assure que'au fil du temps il n'y a pas de variation avec les niveaux de sécurité définis. L'éditeur n'a aucune obligation hormis le respect du RGPD, il peut faire appel à des sous-traitants n'apportant pas de garantie en terme de sécurité.
	Surveillance et revue des services des tiers			
	Engagement de confidentialité			

Whaller

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

Contexte : *un grand nombre d'éditeurs logiciels (SaaS) s'affichent comme étant "SecNumCloud" alors qu'elles ne reposent que sur une infrastructure qualifiée SNC, sans être elles-mêmes qualifiées. L'objet de ce comparatif est d'exposer les différences que cela implique et de montrer l'insuffisance de telles offres. Ce comparatif expose aussi ce que l'offre* **Whaller DONJON, première plateforme collaborative à obtenir le Visa de sécurité ANSSI pour sa qualification SecNumCloud**,*met en pratique. Ce tableau reprend toutes les exigences du référentiel SecNumCloud v3.2.*

Exigences SecNumCloud		Whaller DONJON, solution collaborative qualifiée SecNumCloud	SaaS + IaaS qualifiés	IaaS qualifié seul (exemple RESANA)
Gestion des incidents liés à la sécurité de l'information	*Responsabilités et procédures*	La direction Cybersécurité de Whaller est responsable de la gestion des incidents. Des procédures permettent de couvrir l'ensemble des étapes nécessaires au traitement d'un incident de sécurité.	L'hébergeur comme l'éditeur doivent assigner de façon formelle les responsabiltié en termes de sécurité des systèmes d'information. Des procédures doivent être rédigées afin de cadrer l'ensemble de étapes nécéssaires au traitement des incidents d'origine cyber.	Seul l'hébergeur sur son périmètre propre doit assigner de façon formelle la responsabilité en termes de sécurité du SI et rédiger des procédures pour la gestion des incidents. L'éditeur n'a aucune obligation en la matière ce qui peut conduire à une réaction incertaine en cas d'incident d'origine cyber (destruction/altération des preuves numériques, dépôt de bilan suite à un incident...).
	Signalement liés à la sécurité de l'information	Une procédure de signalement des incidents de sécurité est connue de tous les collaborateurs de Whaller. Un canal de communication interne spécifique est en place. Les contacts SSI avec nos clients sont identifiés.	L'hébergeur et l'éditeur doivent mettre en place sur leur périmètre une préocédure claire de signalement liés à la sécurité de l'information.	Seul l'hébergeur est tenu sur son périmètre de mettre en œuvre uen procédure claire pour le signalement liées à la sécurité de l'information. L'éditeur n'a aucune obligation, la réaction en cas d'incident risque d'être incertaine et tardive.
	Appréciation des évenements liés à la sécurité de l'information et prise de décision	Les évenements de sécurité observés sont tous analysés au moins quotidiennement par la direction Cyber. Un graphe de décision a été rédigé afin de déterminer quels incidents nécessitent la mise en place d'une cellule de crise Cyber.	L'hébergeur et l'éditeur doivent chacun mettre en œuvre des procédures visant à caractériser les évenements liés à la sécurité de l'information afin de favoriser la prise de décision sur les actions à réaliser pour faire face à la situation.	Seul l'hébergeur est tenu de mettre en place des processus d'aide à la décision en cas d'évenements affectant la sécurité de l'information sur son périmètre. L'éditeur n'ayant aucune obligation en la matière la réaction en cas d'incident risque d'être incertaine voire inadaptée.
	Réponse aux incidents liés à la sécurité de l'information	Une procédure de réponse à incident est en place, elle permet de couvrir les aspects d'analyse de l'incident, de collecte des éléments de preuve et la rédaction d'un rapport d'incident transmis au client et au CERT-FR de l'ANSSI. Suivant la nature de l'incident une plainte est également déposée auprès des autorités compétentes.	L'hébergeur et l'éditeur doivent définir des procédures de réponse en cas d'incident d'origine cyber. Ces procédures doivent permettre de collecter les éléments de preuve, de procéder à la remédiation mais aussi les aspects communication avec le client et les autorités.	Seul l'hébergeur doit formaliser des procédures de réponse à incident sur son périmètre. L'éditeur n'a aucune obligation, le fait de s'appuyer sur uné hebergeur qualifié SecNumCloud n'a aucune incidence sur la réponse à incident qui sera incertaine si elle n'est pas préparée.
	Tirer des enseignements des incidents liés à la sécurité de l'information	L'ensemble des incidents sont analysés et le fonctionnement de Whaller est ajusté en fonction des impacts potentiels ou réels identifiés. L'ensemble des données collectées sont capitalisées dans un outil dédiée à la gestion des incidents de cybersécurité. Suivant les cas ils sont partagés avec nos clients et partenaires au travers de notre plateforme d'échange d'IOC.	L'hébergeur et l'éditeur doivent capitaliser sur les incidents les ayant concerné. Ils doivent mettre des procédures afin d'améliorer les mesures de sécurité afin d'éviter que l'incident ne se reproduise.	Seul l'hébergeur est tenu de capitaliser sur les incidents subis et prendre les mesures pour éviter qu'ils ne se reproduisent L'éditeur n'a aucune obligation ainsi le client n'a aucune garantie qu'à l'issue d'un incident ayant affecté l'éditeur celui-ci prenne des mesures pour éviter que cela ne se reproduise
Continuité d'activité	*Organisation de la continuité de l'organisation*	Un PCA a été défini au sein de Whaller, il permet d'identifier les ressources nécessaire au maintien du service et d'identifier les actions de remédiations.	L'hébergeur et l'éditeur doivent chacun établir un Plan de Continuité de l'Activité (PCA) formalisé et mis en œuvre.	Seul l'hébergeur est tenu de définir et de formaliser un PCA sur son périmètre et le service rendu à ses clients. L'éditeur n'a aucune obligation, la continuité d'activité est incertaine en cas de défaillance dans son périmètre exploité par l'éditeur.
	Mise en œuvre de la continuité de l'information			
	Vérifier, revoir et évaluer la continuité d'activité	Des exercices de mise en application du PCA sont réalisés anuellement.	L'hébergeur et l'éditeur doivent chacun sur leur périmètre organiser des exercices, à minima annuellement, de test de leur PCA et le revoir et/ou en évaluer la pertience à l'issue.	Seul l'hébergeur est tenu de tester son PCA sur une base annuelle. L'éditeur n'a aucune obligation, le client n'a aucune garantie de la capacité de l'éditeur à faire face à un sinistre informatique et globalement d'évaluer les impacts en cas de sinistre.
	Disponibilité des moyens de traitement de l'information	Whaller s'engage dans sa convention de service à une disponibilité à 99% de son service.	L'hébergeur et l'éditeur doivent prendre des engagements contractuels dans la convention de service définie avec le client.	L'hébergeur doit prendre en engagement vis-à-vis de l'éditeur sur la disponibilité du service founi. L'éditeur n'est pas tenu de s'engager sur un niveau de disponibilité vis-à-vis de ses clients.
	Sauvegarde de la configuration de l'infrastructure technique	Des procédures d'exploitation complètent la politique de sauvegarde afin de s'assurer la pérénité des configurations de nos serveurs.	L'hébergeur et l'éditeur doivent chacun sur leur périmètre définir des procédures permettant de sauvegarder les configurations utiles au fonctionnement du service fourni.	Seul l'hébergeur est tenu de sauvegarder les configurations des éléments concourrant au service rendu à l'éditeur, il n'a pas vocation à assurer la sauvegarde des configurations mises en œuvre par l'éditeur.
	Mise à disposition d'un dispositif de sauvegarde des données du commanditaire	Les données des commanditaires sont sauvegardés et peuvent être restaurées à tout moment.	L'hébergeur et l'éditeur doivent mettre à disposition de leurs clients des moyens de sauvegarde des données du client.	Seul l'hébergeur est tenu de mettre à disposition de l'éditeur.
Conformité	*Identification de la legislationet des exigences contractuelles applicables*	Une procédure de veille technique et juridique pilotée par la direction Cyber permet à Whaller d'adapter les exigences de la PSSI aux exigences règlementaires applicables y compris celles spécifiques de certains de nos clients.	L'hébergeur et l'éditeur doivent identifier et se conformer aux legislations et exigences contractuelles auxquels ils sont soumis.	Seul l'hébergeur est tenu d'identifier et de se conformer aux legislation et exigences contractuelles auxquels il est soumis. L'éditeur n'a aucune obligation, ainsi le client n'a pas de certitude concernant la connaissance et donc le respect par l'éditeur des legislations et exigences contractuelles auxquels il est soumis.
	Revue indépendante de la sécurité de l'information	Des audits internes sont réalisés à l'initiative de Whaller sur une base annuelle complétés par ceux réalisés par nos clients. Des audits sont également réalisés par des prestataires qualifiés PASSI, un plan d'audit à 3 ans est défini.	L'hébergeur et l'éditeur sont tenus de faire auditer/évaluer les mesures de sécurité de l'information mise en œuvre par un prestataire externe qualifié PASSI. Un plan d'audit doit être défini à 3 ans et s'appuyer sur un auditeur qualifié PASSI.	Seul l'hébergeur est tenu de faiire auditer/eévaluer les mesures de sécurité mise en œuvre par un prestataire qualifié PASSI. L'éditeur n'a aucune obligation de faire auditer par exemple le code qu'il produit ou les mesures de sécurité technique et/ou organisationnelle mises en place. Le client n'a donc aucune garantie sur le niveau de sécurité de la solution proposée par l'éditeur.
	Conformité avec les politiques et les normes de sécurité	Des contrôles périodiques sont réalisés et documentés par la direction Cyber de Whaller. Ils peuvent être planifiés ou spontannés. Des audits sont également réalisés par des prestataires qualifiés PASSI, un plan d'audit à 3 ans est défini.	L'hébergeur et l'éditeur sont tenus de controler leur conformité aux politiques définies mais également les normes applicables. Un plan d'audit doit être défini à 3 ans et s'appuyer sur un auditeur qualifié PASSI.	Seul l'hébergeur est tenu de controler sa conformité aux politiques définies ou aux normes applicables. L'éditeur n'a aucune obligation ainsi le client n'a aucune assurance que les mesures de sécurité définies par l'éditeur sont réellement mises en place.
	Examen de la conformité technique	La conformité techique est également contrôlée en partie par la direction Cyber mais également par la direction techique qui dispose de ses propres procédures de contrôle interne. Des audits sont également réalisés par des prestataires qualifiés PASSI, un plan d'audit à 3 ans est défini.	L'hébergeur et l'éditeur doivent mettre en place chacun sur leur périmètre des procédures de contrôles internes et externes sur la conformité technique. Un plan d'audit doit être défini à 3 ans et s'appuyer sur un auditeur qualifié PASSI.	Seul l'hébergeur est tenu de controler et faire controler sa conformité technique. L'éditeur n'a aucune obligation, bien qu'hebergé sur de l'environnement SecNumCloud, le client n'a aucune garantie que les mesures techniques mises en œuvre par l'éditeur sont conformes à l'état de l'art.
	Convention de service	Une convention de service est systématiquement mise en œuvre avec le client	L'hébergeur doit établir une convention de service avec l'éditeur conformément aux 18 exigences du référentiel SecNumCloud. L'éditeur doit établir une convention de service avec ses clients conformément aux 18 exigences du référentiel SecNumCloud.	L'hébergeur doit établir une convention de service avec l'éditeur conformément aux 18 exigences du référentiel SecNumCloud. L'éditeur n'a aucune obligation de mettre en place une convention de service avec ses clients ni de faire contrôler la conformité de sa onvention de service.

Whaller

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

Contexte : *un grand nombre d'éditeurs logiciels (SaaS) s'affichent comme étant "SecNumCloud" alors qu'elles ne reposent que sur une infrastructure qualifiée SNC, sans être elles-mêmes qualifiées. L'objet de ce comparatif est d'exposer les différences que cela implique et de montrer l'insuffisance de telles offres. Ce comparatif expose aussi ce que l'offre* **Whaller DONJON, première plateforme collaborative à obtenir le Visa de sécurité ANSSI pour sa qualification SecNumCloud**,*met en pratique. Ce tableau reprend toutes les exigences du référentiel SecNumCloud v3.2.*

Exigences SecNumCloud		Whaller DONJON, solution collaborative qualifiée SecNumCloud	SaaS + IaaS qualifiés	IaaS qualifié seul (exemple RESANA)
Exigences supplémentaires	*Localisation des données*	Les données sont exclusivement localisées et traitées en France. L'administration et la supervision de la plateforme sont réalisés en France.	L'hébergeur et l'éditeur s'engagent à héberger et traiter les données sur le territoire européen ainsi qu'à réaliser les opérations d'administration à partir du territoire européen. Si des opréations doivent être réalisée en dehors du territoire européen la liste des opérations réalisées doit être documentée et la supervision assurée depuis le territoire européen.	Seul l'hébergeur est tenu de réaliser les traitement et l'hébergement dans l'union européenne de même pour le support. L'éditeur n'a aucune obligation hormis celles définies par le RGPD concernant le traitement des données personnelles, le support peut être réalisé à a partir d'un pays en dehors de l'UE.
	Régionalisation	Le service est avant tout fourni en langue française de même que le support de premier niveau.	L'hébergeur et l'édteur doivent proposer des interfaces en langue française et un support de premier niveau en français.	Seul l'hébergeur est tenu de fournir des interfaces et du support en langue française. L'édieur n'a aucune obligation et peut proposer des interfaces ou du sppourt dans une autre langue.
	Fin de contrat	La fin de contrat est cadrée dans la convention de service afin de définir les modalités de restitutions des données au client mais également de fixer les modalités d'effacement des supports utilisé pour la prestation y compris les données techniques.	L'hébergeur et l'éditeur à la fin du contrat (quel qu'en soit le motif) doivent mettre en place des mesures visant à garantir un effacement sécurisé des données du client ainsi que les données techniques associées.	Seul l'hébergeur est tenu à la fin du contrat de mettre en place des mesures d'effacement sécurisé des données du client et des données techniques associées. L'éditeur n'a aucune obligation, le client n'a aucune garantie sur la suppression sécurisée des données le concernant.
	Protection des données à caractère personnel	Whaller s'applique à être conforme aux exigences définies par le RGPD. Le service est conçu sur la base des concepts de securité par défaut et confidentialité par conception.	L'hébergeur et l'éditeur doivent justifier des principes de protection des données personnelles mis en œuvre.	L'hébergeur seul doit justifier des principes de protection des données personnelles mis en œuvre. L'éditeur doit simplement s'engager à les mettre en eouvre sans en apporter la preuve.
	Protection vis-à-vis du droit extra-européen	Whaller n'utilise aucune solution ou sous-traitant soumis à des lois extra-européenne pour le rendu du service Whaller DONJON. Conformément aux exigences du référentiel d'exigence SecNumCloud, Whaller n'est pas sous contrôle de fonds extra-européens Son siège est situé à Suresnes en France.	L'hébergeur et l'éditeur doivent satisfaire à 6 exigences définies dans le référentiel d'exigence SecNumCloud visant à garantir une immunité aus loix extra-européennes tant au niveau de la gouvernance de l'entreprise que dans ses choix technologiques.	L'hébergeur seul doit satisfaire à 6 exigences définies dans le référentiel d'exigence SecNumCloud visant à garantir une immunité aus loix extra-européennes tant au niveau de la gouvernance de l'entreprise que dans ses choix technologiques. L'éditeur n'a aucune obligation, le client n'a aucune garantie que l'éditeur n'est pas soumis à des lois extra-européennes bien que les données soient hébergées sur un environnement SecNumCloud.