CONDITIONS PARTICULIERES

« CYBER – GESTION DES EVENEMENTS DE SECURITE »

Version en vigueur à compter du 1er juillet 2025

Le présent document décrit les conditions particulières applicables aux Prestations spécifiques SOC (ci-après « **CP CYBER SOC** »). Elles viennent préciser les conditions générales de service du Prestataire dans leur dernière version en vigueur disponible sur son site Internet à l'adresse suivante : https://www.oci.fr/conditions-generales/ (les « **CGS** »).

Article 1. Champ d'application

Le paragraphe « Champ d'application des CGS et opposabilité » de l'article 1 RELATION CONTRACTUELLE ENTRE LES PARTIES des CGS est complété comme suit :

Les Prestations se rapportent à la mise à disposition au Client par le Prestataire de son centre opérationnel de sécurité (« *Security Operation Center* » ou « SOC » en anglais). Le Client a souhaité bénéficie des services du Prestataire afin que celui-ci mette en place un système permettant de répondre à ces besoins, notamment en matière de détection et de réponse à des incidents de sécurité afin de maîtriser ses risques et augmenter le niveau de sécurité de son Système d'information.

Article 2. Définitions

Les termes portant une majuscule dans les CGS et réutilisés au sein des présentes CP CYBER SOC ont la même signification que celle qui leur est donnée dans les CGS.

Les définitions suivantes sont ajoutées à l'article 2 DEFINITIONS des CGS :

« **Incident de sécurité** » : désigne un ou plusieurs événements(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité de compromettre les opérations liées à l'activité du Client et/ou de menacer la sécurité de l'information.

« **Indicateur de compromission** » : désigne la combinaison d'informations techniques représentative d'une manifestation de compromission, dont la présence peut être identifiée à partir de l'analyse d'un système, d'un code malveillant ou de traces réseau.

« **Périmètre surveillé** » : désigne tout ou partie du système d'Information du Client, objet des Prestations.

« **Règle de détection** » : désigne une liste d'éléments techniques permettant d'identifier un Incident à partir d'un ou de plusieurs événements. Une règle de détection peut être un ou des marqueurs, une ou des signatures ou une règle comportementale basée sur un comportement défini comme anormal. Une règle de détection peut provenir de l'éditeur des outils techniques d'analyse utilisés pour les Prestations, du Prestataire (veille sur de nouveaux incidents, règle utilisée pour un autre client, etc.), d'un partenaire, d'un Fournisseur spécialisé ou encore avoir été créée spécifiquement pour répondre à un besoin du Client.

« **Solution SOC** » : désigne l'outil ou les outils de surveillance édités par un tiers et utilisés par le Prestataire pour réaliser les Prestations. La Solution SOC retenue est précisée à l'Offre commerciale.

Article 3. Obligations des Parties

L'article 5.1 OBLIGATIONS DU PRESTATAIRE des CGS est complété comme suit :

Le paragraphe « Obligation de conseil » de l'article 5.1 OBLIGATIONS DU PRESTATAIRE des CGS est remplacé comme suit :

Obligation de conseil – Le Prestataire s'engage à respecter l'obligation de conseil et de mise en garde qui lui incombe. Il fournit ainsi au Client l'ensemble des conseils, mises en garde et recommandations nécessaires à la bonne exécution du Contrat. Il s'engage en particulier à :

- Fournir toute information et conseil nécessaires permettant au Client d'accepter l'Offre commerciale en connaissance de cause, dans la limite des éléments mis à la disposition du Prestataire ; et
- Fournir les conseils et mises en garde relatifs notamment à l'utilisation, au maintien et à l'évolution des services compris dans les Prestations ainsi qu'à leurs limites potentielles.
- Informer le Client pendant la durée de réalisation des Prestations d'éventuelles évolutions (méthodes, techniques, procédures) qui surviendraient dans le champ de son intervention.

L'article 5.1 OBLIGATIONS DU PRESTATAIRE des CGS est complété comme suit :

Qualité des Prestations – Le Prestataire met en place une procédure d'amélioration permanente de l'efficacité des Prestations qu'il réalise.

Collaboration avec les tiers mandatés – Le Prestataire collabore avec des tiers mandatés et / ou autorisés par le Client, tout particulièrement dans les cas où le Prestataire n'interviendrait pas en réponse aux Incidents de sécurité. La collaboration avec un tiers sur une réponse à incident sera facturée au temps passé selon la grille tarifaire de réponse à incident en vigueur à la date de sollicitation.

L'article 5.2 OBLIGATIONS DU CLIENT des CGS est complété comme suit :

Référent interne, organisation et suivi des Prestations – Le Client s'engage à désigner un référent interne principal ainsi qu'un référent suppléant. Le référent principal a pour rôle de suivre le bon déroulement opérationnel des Prestations et notamment de mettre en relation l'interlocuteur du Prestations avec les différents correspondants impliqués. Compte-tenu du rôle du référent, le Client s'engage à désigner une personne dont les compétences, l'expérience et les fonctions lui permettront de mener à bien ce rôle. Le Client informe sans délai le Prestataire de tout changement de référent interne.

Collecte et analyse d'informations – Le Client s'engage à remplir toutes les obligations légales nécessaires à la réalisation des Prestations et notamment celles relatives à la collecte et à l'analyse d'informations.

Documentation – Le Client s'engage à fournir, préalablement à l'exécution des Prestations un descriptif des actions menées dans le cadre de la constitution et de la gestion de son système d'Information et qui pourraient impacter les Prestations. Il s'engage également à fournir toute information utile et/ou demandée par le Prestataire avant la réalisation des Prestations (ex : politique de sécurité, analyse des risques, procédures d'exploitation de la sécurité, etc.) afin que le Prestataire soit en mesure de délimiter strictement les contours de son intervention et de réaliser les Prestations dans les meilleures conditions.

Evolution de l'infrastructure – Le Client s'engage à mettre en place un processus de gestion des changements lui permettant d'informer le Prestataire de toutes modifications sur le Périmètre surveillé (configuration, paramètres, versions logicielles, nouvelles prestations etc.).

Gestion de crise – Le Prestataire informe le Client que la bonne pratique en la matière veut que le Client, à l'issue de la phase d'intégration, d'un processus de gestion de crise à mettre en œuvre en cas de détection d'un Incident de sécurité majeur au sein de son Système d'Information.

Sauvegardes – Le Client prend les mesures de sauvegarde nécessaires à la protection de son Système d'Information et des données associées préalablement et au cours de l'exécution des Prestations. Il réalise cette démarche en collaboration avec le Prestataire afin de ne pas gêner ses activités (notamment d'analyse, y compris concernant l'intégrité des traces d'activités malveillantes).

Autorisation générale – Le Client autorise le Prestataire et ses équipes, à titre provisoire, pendant toute la durée et aux seules fins de réaliser les Prestations, à accéder (y compris à distance) à tout ou partie du Périmètre surveillé tel que convenu entre les Parties et le cas échéant à traiter les données qui y sont hébergées (reproduction, collecte et analyse) et ce, quelle que soit la nature de ces données. Par ailleurs, le Client autorise le Prestataire à conserver toutes données concernant les évènements collectés et les Incidents de sécurité détectés.

Article 4. Description du périmètre des Prestations

Le paragraphe « Périmètre des Prestations » de l'article 6 ETENDUE DES PRESTATIONS des CGS est complété comme suit :

Les Niveaux de service (auxquels il est fait référence dans les CGS) applicables aux Prestations sont définis en **Annexe A** des présentes CP CYBER SOC.

Le paragraphe « Evolution des Prestations » de l'article 6 ETENDUE DES PRESTATIONS des CGS est complété comme suit :

A échéance régulière (par exemple lors d'un comité lorsque la prestation est souscrite par le Client ou par le biais des informations définies dans la console ou au moment du renouvellement), un point sera réalisé sur le nombre d'assets surveillé comparé au nombre d'asset souscrits afin de régulariser la facturation.

En cas d'augmentation égale ou supérieure à cinq pourcents (5 %) du total souscrit entre deux vérifications, une régularisation sera obligatoire. La tarification retenue sera celle en vigueur chez le Prestataire au moment du changement et proratisée au temps restant sur l'année d'abonnement en cours.

L'évolution du Périmètre surveillé est alors une Prestation additionnelle qui s'appliquera jusqu'à la prochaine vérification, la résiliation des Prestations ou l'émission d'une nouvelle Offre commerciale.

Un paragraphe « Prestations de réponse à incident » est ajouté à l'article 6 ETENDUE DES PRESTATIONS des CGS :

Prestations de réponse à incident – Le Client peut, ponctuellement et à tout moment, souhaiter souscrire à des prestations de réponse à incident, sous réserve de l'acceptation du Prestataire et au tarif en vigueur chez le Prestataire au moment de la Sollicitation.

Le Client a également la possibilité de souscrire à un abonnement récurrent lui ouvrant un droit d'accès à un centre de réponse à incident opéré par le Prestataire. Cet abonnement lui permet de bénéficier de tarifs préférentiels négociés sur des prestations de réponse à incident (ci-après le « **Contrat CSIRT** »). Les modalités et prestations incluses au Contrat CSIRT ainsi que les tarifs associés sont alors prévus à l'Offre commerciale concernée. Sauf disposition contraire dans l'Offre commerciale, le Contrat CSIRT se renouvelle par tacite reconduction à l'issue de la période initiale d'engagement et ce, pour la même durée que la période initiale, sauf si le Client a résilié le Contrat CSIRT par l'envoi d'une lettre recommandée avec accusé de réception au minimum trois (3) mois avant l'échéance du terme de la période en cours.

Lorsque la prestation de réponse à incident inclut le prépaiement de crédits consommables dans le cadre de réponses à incident, ces crédits sont valables jusqu'à leur consommation totale et dans un délai maximum de trois (3) ans après souscription.

Article 5. Modalités de réalisation des Prestations

Les sections et paragraphes suivants sont ajoutés à l'article 7 MODALITES DE REALISATION DES PRESTATIONS des CGS :

Phases des Prestations

Le Prestataire réalise les Prestations en plusieurs phases :

- La phase d'intégration (« *build* ») : elle permet au Prestataire d'acquérir les informations et de procéder aux opérations préalables nécessaires à la mise en place du service SOC et notamment de définir avec le Client des modalités de réalisation de la phase d'exploitation. La phase d'intégration permet de définir le Périmètre surveillé initial, ce Périmètre pouvant évoluer au fur et à mesure de l'exécution du Contrat.
- La phase d'exploitation (« *run* ») : elle consiste en la réalisation des Prestations d'exploitation du SOC telle que définie à l'Offre commerciale. Elle débute lors de la réception par le Prestataire de l'instance ou du provisionnement de la licence ;

Les phases d'intégration et d'exploitation sont concomitantes.

Pilotage des Prestations

Lorsque le Client a souscrit à cette Prestation, le Prestataire met en place et anime en présence du Client un comité opérationnel selon la récurrence précisée à l'Offre commerciale.

Le comité opérationnel a pour objectifs (i) de réaliser un bilan du service de détection des Incidents de sécurité, ce bilan pouvant inclure, à la demande du Client, la revue de l'atteinte des Niveaux de service sur une période de trois mois précédant la tenue du comité de pilotage, (ii) d'ajuster si nécessaire le Périmètre des Prestations et (iii) d'exposer les évolutions liées au service et aux solutions et les impacts éventuels et ajustements nécessaires des Prestations.

Le Prestataire rédige un compte-rendu à la suite de chaque comité opérationnel et le transmet au Client pour validation dans les dix (10) jours ouvrés suivant la tenue du comité.

Ce compte-rendu contient au minimum la liste des participants, les indicateurs définis lors de la phase d'intégration, la liste des différents incidents ou « vrais positifs » de la dernière période, les décisions prises en comité et le plan d'action associé.

Limites générales des Prestations

Les informations disponibles dans la Solution SOC sont paramétrées par l'éditeur et le Client reconnaît que le Prestataire ne peut pas modifier lesdits paramétrages.

Le Client reconnaît qu'il existe des comportements de nature à contourner les mesures de protection mises en place par le biais de la Solution SOC. Par exemple, il existe des comportements dits « anti-SOC » qui sont susceptibles de ne pas être détectés par la Solution SOC et donc ne pas être traités par le Prestataire ou le Client. Le Prestataire ne pourra être tenu responsable de la non-remontée par le SOC d'une alerte et de sa non-intervention sur la Menace, aléa que le Client accepte.

Lorsque le Client souscrit à des interventions en Heures non-Ouvrées, le Client doit préciser au Prestataire toute information et spécificité qui pourrait nécessiter un ajustement de la procédure mise en place en standard chez le Prestataire.

Le Client reconnaît avoir été dûment informé des limites inhérentes à la réalisation des Prestations, notamment concernant la disponibilité et l'intégrité de la surface du Système d'Information ciblé dans le Périmètre surveillé. Le Prestataire a ainsi informé le Client que les Prestations ne permettent pas par essence de détecter (et par voie de conséquence de résoudre) l'ensemble des Incidents de sécurité pouvant impacter le Périmètre surveillé.

Le Client reconnaît en outre que par leur nature réactive, les prestations ne sont pas une garantie d'absence de conséquences nuisibles pour le Client, que ces conséquences soient dues à l'Incident de sécurité lui-même ou aux mesures prises par le Prestataire ou aux mesures prises ou non-prises par le Client.

Article 6. Force majeure

Le premier paragraphe de l'article 13 – FORCE MAJEURE des CGS est modifié comme suit :

Les Parties conviennent que les cas suivants sont des cas de force majeure :
- L'indisponibilité de la Solution SOC si cette indisponibilité est liée à l'éditeur ou à un cas de force majeure affectant l'éditeur.

Les Parties conviennent que les actes de piratage informatique ne constituent pas un cas de force majeure si un tel acte (1) affecte le Périmètre surveillé et (2) que le Prestataire a apporté une réponse inadaptée au regard de ses engagements contractuels.

Annexe A - Niveaux de service

Le service SOC concerne le service de surveillance par le biais d'une Solution SOC souscrite par le Client, sur la plage horaire souscrite par le Client. Ces éléments sont repris à l'Offre commerciale concernée.

A l'issue de la phase d'intégration, les Parties valident entre elles une date de mise en production qui constitue la date à compter de laquelle le Prestataire applique les niveaux de service précisés ci-après (phase d'exploitation).

Le service SOC inclut :
- La surveillance, l'optimisation et l'analyse des données de la Solution SOC ;
- L'analyse des alertes de sécurité détectées par le biais de la Solution SOC et confirmées par le service SOC comme pouvant être ou étant un Incident ;
- L'analyse et la remontée des Incidents ;
- Le suivi, le blocage ou la limitation immédiate de la propagation de l'Incident ;
- La recherche d'indicateurs de compromission et indicateurs d'attaque.

Les niveaux de service dépendent de la criticité de l'alerte :

Niveaux de criticité	Délai de prise en compte de l'alerte sur les Heures Ouvrées	Niveau de service (pourcentage des alertes de sécurité prises en compte dans les délais sur une période de trois (3) mois)
Niveau 4 (critique)	2 heures	95 %
Niveau 3 (haute)	4 heures	
Niveau 2 (moyenne)	8 heures	
Niveau 1 (basse)	12 heures	

Lorsque le Client souscrit au service SOC 24/7, le Prestataire traite les alertes de Niveau 4 (criticité), sur les Heures non-Ouvrées, selon le délai de prise en compte précisé ci-dessus.

Ces Niveaux de service pourront être étudiés lors d'un comité de pilotage, conformément au paragraphe « Pilotage des Prestations » de l'article 5 des présentes CP CYBER SOC.

Le service SOC n'inclut pas :
- La réponse à Incident ;
- La gestion de crise ;
- L'investigation après le blocage, l'isolation ou l'éradication de la menace immédiate ;
- Le suivi et le pilotage des Prestations (sauf comités souscrits).

Il s'agit alors de Prestations complémentaires auxquelles le Client peut souscrire conformément aux dispositions contractuelles.

Le Prestataire utilise une Solution SOC éditée par un tiers, qui est disponible en principe selon le taux de disponibilité sur lequel l'éditeur-tiers s'engage.