CONDITIONS PARTICULIERES

« CYBER – SURVEILLANCE DES EVENEMENTS DE SECURITE »

Version en vigueur au 2 mai 2026

Le présent document décrit les Conditions particulières applicables aux Prestations spécifiques relatives à la réalisation du service 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/ (ci-après les « **CGS** »).

Article 1. Champs d'application

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) afin que celui-ci mette en place un système permettant de répondre aux besoins du Client en matière de détection et d'analyse des incidents de sécurité afin de maîtriser ses risques et d'augmenter le niveau de sécurité de son système d'information.

Article 2. Définitions spécifiques

En sus des définitions prévues aux CGS, certaines définitions sont spécifiquement applicables aux prestations couvertes par les présentes Conditions particulières :

« **Alerte** » : désigne une alerte de sécurité remontée par la Solution SOC et faisant l'objet d'un Diagnostic ;

« **Contrat CSIRT** » : désigne un abonnement récurrent ouvrant droit au Client d'accéder à un centre de réponse à incident (cyber) opéré par le Prestataire et de bénéficier de tarifs préférentiels sur des prestations de réponse à incident. Les modalités et prestations incluses au Contrat CSIRT ainsi que les tarifs associés sont alors prévus à l'Offre commerciale concernée.

« **Diagnostic** » : désigne l'analyse par le Prestataire d'une Alerte permettant de conclure si l'Alerte constitue un Incident de sécurité ;

« **Incident de sécurité** » : désigne un ou plusieurs événements de sécurité de l'information indésirables ou inattendus présentant une probabilité de compromettre les opérations liées à l'activité du Client et/ou de menacer la sécurité de l'information ;

« **Limitation** » : désigne la ou les actions prises par le Service SOC après Diagnostic, par le biais des moyens à disposition dans la Solution SOC et visant à bloquer ou à limiter la propagation de l'Incident de sécurité ;

« **Périmètre surveillé** » : désigne les éléments du système d'information du Client objet des Prestations ;

« **Règle(s) de détection** » : désigne une liste d'éléments techniques permettant d'identifier un Incident de sécurité à partir d'un ou de plusieurs événements : une règle de détection peut être un marqueur, une signature ou une règle comportementale basée sur un comportement défini comme anormal. La règle de détection peut provenir de l'éditeur de la Solution SOC, 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 ;

« **Remédiation** » : désigne une Prestation de réponse simple à un Incident de sécurité localisé sur l'environnement numérique d'un Utilisateur, traitable à distance et en moins de trois (3) heures, réalisée après le Diagnostic et la Limitation et visant à limiter les conséquences de l'Incident de sécurité et/ou, si cela est techniquement faisable, d'y remédier ;

« **Réponse à incident** » : désigne une Prestation de réponse complexe à un Incident de sécurité réalisée après le Diagnostic et la Limitation et pouvant inclure, selon les demandes du Client et la faisabilité technique : la limitation des conséquences de l'Incident de sécurité et/ou sa clôture, l'investigation, la collecte d'éléments de preuve et la gestion de crise ;

« **Service SOC** » : désigne le service de surveillance par lequel le Prestataire procède au Diagnostic des Alertes et le cas échéant à la Limitation des Incidents de sécurité ;

« **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, sauf cas spécifique où le Client dispose déjà d'une Solution SOC qui est mise à disposition du Prestataire ;

Article 3. Obligations spécifiques des Parties

3.1. Obligations spécifiques du Prestataire

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 ledit tiers sera facturée au temps passé selon la grille tarifaire de réponse à incident en vigueur à la date de Sollicitation.

3.2. Obligations spécifiques du Client

Autorisation générale – Le Client autorise le Prestataire et ses équipes, 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 et le cas échéant à traiter les données qui y

sont hébergées en vue de leur reproduction, collecte et analyse. En sus, le Client autorise le Prestataire à conserver les données relatives aux Règles de détection, indicateurs de compromission, évènements collectés et Incidents de sécurité détectés.

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.

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, bénéficie d'un processus de gestion de crise à mettre en œuvre en cas de détection d'un Incident de sécurité majeur.

Article 4. Description détaillée des Prestations

4.1. Description du Service SOC

En parallèle de la souscription à la Solution SOC retenue par le Client pour les assets concernés, il est précisé que l'abonnement au Service SOC inclut les Prestations suivantes :
- La surveillance, l'optimisation et l'analyse des données de la Solution SOC ;
- La réalisation d'un Diagnostic pour chaque Alerte conformément aux Niveaux de service repris ci-dessous ;
- En cas d'Incident de sécurité avéré, la Limitation.

4.2. Mise en place des Prestations

Le Prestataire réalise les Prestations en plusieurs phases :
- Durant la **phase d'intégration** (« *build* »), le Prestataire acquiert les informations nécessaires et procède aux opérations préalables nécessaires à la mise en place du Service SOC, notamment en définissant avec le Client les modalités de réalisation de la phase d'exploitation (par exemple : formalisation du plan de communication). Dans ce cadre, le Client fournit un descriptif des actions menées dans le cadre de la constitution et de la gestion de son système d'information (par exemple : politique de sécurité, analyse des risques, procédures d'exploitation de la sécurité, etc.). 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.
- Durant la **phase d'exploitation** (« *run* »), le Prestataire réalise le Service SOC selon les modalités définies à l'Offre commerciale. Cette phase 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. Les Niveaux de service s'appliquent à compter de la date à laquelle les Parties ont validé la date de mise en production à l'issue de la phase d'intégration.

4.3. Fonctionnement de la phase d'exploitation

4.3.1. Diagnostic

Le Diagnostic est réalisé conformément aux Niveaux de service repris ci-après :

Niveaux de criticité de l'Alerte	Délai de prise en compte de l'Alerte sur les Heures Ouvrées	Niveau de service (pourcentage des Alertes 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	

En Heures non-Ouvrées, le Client doit préciser au Prestataire toute information et spécificité qui pourraient nécessiter un ajustement des procédures applicables, définies avec le Client en phase d'intégration. En tout état de cause, le Prestataire applique les Niveaux de service associés aux Alertes de Niveau 4 :

Niveaux de criticité de l'Alerte	Délai de prise en compte de l'Alerte sur les Heures Ouvrées	Niveau de service (pourcentage des Alertes prises en compte dans les délais sur une période de trois (3) mois)
Niveau 4 (critique)	2 heures	95 %

4.3.2. Traitement de l'Incident de sécurité

Après la Limitation, le Prestataire procède à la Remédiation ou à la Réponse à Incident.

4.3.2.1. *Remédiation*

La Remédiation est réalisée dans le cadre d'un Ticket ouvert par le Prestataire automatiquement après un Diagnostic ayant conclu à un Incident de sécurité et sera facturée au temps passé selon le tarif applicable en vigueur chez le Prestataire au moment de la Remédiation (sauf accord autre entre les Parties, par exemple : Contrat CSIRT).

4.3.2.2. *Réponse à Incident*

La Réponse à Incident fait l'objet d'une facturation au temps passé les trois premières heures selon le tarif applicable en vigueur chez le Prestataire au moment de la Réponse à Incident (sauf accord autre entre les Parties, par exemple : Contrat CSIRT) et/ou d'une Offre commerciale distincte précisant les conditions tarifaires de la Réponse à incident. Lorsqu'une intervention d'ordre cyber est nécessaire (par exemple : gestion de crise, réponse à incident d'ordre cyber, recherches de preuves), le centre de réponse à incident du Prestataire peut être amené à intervenir et les Parties conviendront des modalités financières et opérationnelles de cette intervention. En cas d'urgence ou de circonstances exceptionnelles, les Parties peuvent convenir d'un accord par simple échange d'e-mail que le Client s'engage à régulariser si nécessaire dès que cela est possible.

4.4. 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 de la typologie des Incidents de sécurité de la dernière période, les décisions prises en comité et le plan d'actions associé.

4.5. Evolution du périmètre

A échéances régulières (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 état des lieux 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 ou l'émission d'une nouvelle Offre commerciale.

Article 5. Limites générales des Prestations

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

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.

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.

Pour rappel, le Client est tenu de désigner un interlocuteur privilégié pour le suivi de la réalisation des Prestations. Celui-ci doit bénéficier de compétences, expériences et fonctions suffisantes pour mener à bien son rôle et notamment, le cas échéant, mettre en relation l'interlocuteur du Prestataire avec les différents correspondants impliqués.

Enfin, 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.

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).

Article 6. Modalités spécifiques de Réversibilité

La Réversibilité ne s'applique pas dans le cadre des Prestations couvertes par les présentes Conditions particulières.