OCI INFORMATIQUE & DIGITAL

CONDITIONS PARTICULIERES
« CYBER – SURVEILLANCE DES EVENEMENTS DE SECURITE »

Version en vigueur au 18 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 :

« **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 lui permettant de bénéficier de tarifs préférentiels négociés 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 ;

« **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 ;

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

« **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 ;

« **Remédiation** » : désigne une Prestation de réponse simple (c'est-à-dire que l'Incident de sécurité qui fait l'objet de la Remédiation est localisé sur l'environnement numérique d'un Utilisateur, traitable à distance et en moins de trois (3) heures) à un Incident de sécurité réalisée après le Diagnostic et la Limitation et visant à limiter les conséquences de l'Incident de sécurité 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, la limitation des conséquences de l'Incident de sécurité, la clôture de l'Incident de sécurité sous réserve de faisabilité technique, l'investigation voire la collecte d'éléments de preuve relatifs à l'Incident de sécurité 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 ;

Article 3. Obligations des Parties

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

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.

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

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 Règles de détection, les Indicateurs de compromission, évènements collectés et les Incidents de sécurité détectés.

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.

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).

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.

Interlocuteur privilégié – Le Client est informé, s'agissant de l'interlocuteur qu'il désigne conformément à la section « Interlocuteur privilégié » de l'article 5.2 OBLIGATIONS DU CLIENT des CGS que 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.

Article 4. Description du Périmètre et des Prestations

La section « Périmètre des Prestations » de l'article 6 ETENDUE DES PRESTATIONS des CGS est complétée comme suit :

Le Service SOC ainsi que 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.

La section « Evolution des Prestations » de l'article 6 ETENDUE DES PRESTATIONS des CGS est complétée 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.

ANNEXE A – DESCRIPTION DES PRESTATIONS ET NIVEAUX DE SERVICE

Article 1. Description des Prestations

1.1. Mise en place des Prestations

Le Prestataire réalise les Prestations en plusieurs phases :

- La **phase d'intégration** (« *build* ») 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* ») consiste en la réalisation des Prestations d'exploitation du Service 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. 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.

1.2. Description du Service SOC

L'abonnement au Service SOC inclut les Prestations suivantes :

- La souscription à la Solution SOC retenue pour les équipements concernés,
- 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 à l'article 2 de la présente annexe.
- En cas d'Incident de sécurité, la Limitation.

1.3. Description du traitement de l'Incident de sécurité

Après la Limitation, le Prestataire procède à la Remédiation ou à la Réponse à Incident selon les modalités suivantes.

1.3.1. 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.

Le tarif applicable dépend des Prestations souscrites par le Client : s'il a un contrat DAC incluant ou non un CTR DAC ou un CTR CYBER, le Prestataire défalque le CTR associé (le tarif à l'heure diffère en fonction de la plage-horaire durant laquelle la Remédiation a lieu) ou applique les tarifs préférentiels applicables au Client. Dans le cas contraire, le Prestataire applique son tarif en vigueur au moment de la Remédiation.

1.3.2. Réponse à Incident

La Réponse à Incident fait l'objet d'une facturation au temps passé les trois premières heures 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.

Le tarif applicable dépend des Prestations souscrites par le Client : s'il a souscrit à un contrat CSIRT, le Client bénéficie de tarifs préférentiels qui seront appliqués à la prestation de réponse à incident d'ordre cyber. 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.

Lorsque la Remédiation a lieu sans souscription préalable par le Client au Service DAC ou à un contrat CSIRT, le Prestataire pourra utiliser un CTR Cyber qui sera défalqué différemment en fonction de la plage-horaire de la Remédiation ou en l'absence d'un tel CTR, au temps passé selon tarif en vigueur chez le Prestataire au moment de la Sollicitation applicable.

1.4. 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.

Article 2. Niveaux de Service

2.1. Délai de réalisation du Diagnostic

Le Diagnostic est réalisé conformément aux Niveaux de service repris ci-après, sauf mention autre dans l'Offre commerciale :

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	

En Heures non-Ouvrées, le Prestataire applique les Niveaux de service associés aux Alertes de Niveau 4.

Ces Niveaux de service pourront être étudiés lors d'un comité de pilotage, conformément à l'article 1.3 de la présente annexe.

2.2. Taux de disponibilité de la Solution SOC

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.

Article 3. 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.