CONDITIONS PARTICULIERES SPECIFIQUES AUX CONDITIONS GENERALES DE SERVICE « CYBERSECURITE »

-

Endpoint Detective Response

Version en vigueur à compter du 1er janvier 2023 – v1.0

Ces Conditions particulières viennent compléter les Conditions générales de service de cybersécurité que les Parties ont conclu. Elles viennent préciser le périmètre et les modalités de Prestation Endpoint Detective Response (EDR) – dans le cas où elle est souscrite, que cette Prestation fasse l'objet d'une supervision par le Prestataire ou non.

1. Objet des Prestations

Le Client peut souscrire, à tout moment, auprès du Prestataire à des licences d'utilisation de Progiciels d'EDR édités par des tiers (les modalités de souscription sont définies dans les CGMD disponibles sur le site internet du Prestataire à l'adresse suivante : www.oci.fr/conditions-generales/). En complément, le Client a la possibilité de souscrire à une Prestation de supervision pour ces Progiciels qui s'applique alors au Système d'information faisant l'objet de la Prestation.

La Prestation est souscrite par le biais de l'Offre commerciale et / ou du Bon de commande concerné qui précise notamment les conditions financières.

Le Progiciel et la Prestation de supervision constituent le pack EDR.

L'EDR est un logiciel qui monitore en continu les cybermenaces sur le Système d'information et permet au Client de mettre en place une procédure de détection, prise en compte et de traitement d'alertes sur les plages-horaires qu'il a définies en concertation avec le Prestataire.

Le Progiciel retenu par le Client génère des alertes par le biais d'une intelligence artificielle qui surveille les postes et serveurs du Système d'information (surveillance comportementale). Ces alertes sont associées à un niveau de sévérité allant de 1 à 5 :

- 1 (*severe*)
- 2 (*high*)
- 3 (*medium*)
- 4 (*low*)
- 5 (*informational*)

2. Progiciels

a. Installation

La Mise en Service se fait conformément aux modalités définies entre les Parties au sein des CGC et du présent document.

b. Paramétrage

L'EDR fait remonter des « alertes » dans la console de supervision du Progiciel.

Le paramétrage des informations disponibles est défini par l'éditeur et le Prestataire ne peut le modifier, ce que le Client reconnaît.

Sans service de supervision associé, c'est le Client qui accède et assure le suivi de la console. Il peut demander au Prestataire une prestation complémentaire pour que ce dernier configure la console pour les interlocuteurs habilités du Client. De même, il peut demander le traitement ponctuel d'une information par le biais d'une prestation complémentaire.

3. Supervision

Lorsque le Client souscrit au Service de supervision, le Prestataire surveille la console qu'il a paramétrée selon les besoins soumis par le Client et, le cas échéant, intervient – en collaboration avec le Client –, pour traiter les informations qui remontent telles que paramétrées par l'éditeur du logiciel concerné dans les conditions définies ci-après :

- Les alertes de niveaux 1 à 3 sont traitées par l'équipe Cybersécurité du Prestataire sur les Heures d'ouverture du support. Il est précisé que lorsque le Client souscrit à de l'astreinte, l'équipe d'astreinte prend les premières mesures (notamment : d'isolation et de création du ticket) pour toutes les alertes générées sur la période d'astreinte correspondent aux niveaux 1 et 2, puis les tickets associés sont traités par l'équipe Cybersécurité sur les Heures d'ouverture du support.
- Dans un premier temps, le Prestataire analyse la véracité de l'alerte remontée et distingue les faux positifs des alertes suspicieuses ou avérées (ci-après les « **Menaces** »). De manière générale, le Prestataire préviendra le Client des Menaces qu'il considère comme devant faire l'objet d'une information au Client en lui envoyant un e-mail ou en le contactant par téléphone sur les Heures d'ouverture du support.
- En cas de Menace, l'équipe Cybersécurité prend les mesures qui lui paraissent adéquates, permettant de limiter / d'isoler la Menace observée et prévient le Client qui décide de la suite à donner pour le traitement de la Menace. L'intervention du Prestataire a pour objectif de limiter l'impact que peut avoir la Menace pour le Client et prend des mesures défensives. Sur la période d'astreinte, l'équipe d'astreinte isole la Menace et crée un ticket à traiter par l'équipe Cybersécurité sur les Heures d'ouverture du support.

L'intervention du Prestataire est comprise dans la Redevance payée par le Client au titre de cette Prestation dans la limite de cinq (5) minutes. Tout dépassement fera l'objet d'une facturation en sus.

Détails de la prestation	**Pack EDR**	**Inclus dans le prix**
Alertes générées	Automatique	Oui
Typologie des anomalies prises en compte	Anomalies de sévérité 1 à 3 remontées automatiquement	Oui
Garantie de temps d'interventio	En fonction de la sévérité de l'alerte, ce délai	Oui

n sur les Heures d'ouverture du support	étant décompté sur les Heures d'ouverture du support, après réception de l'e-mail par le Prestataire reprenant l'alerte générée par l'EDR : - Sévérité 1 : 1 heure - Sévérité 2 : 2 heures - Sévérité 3 : 4 heures	
Supervision et détection des anomalies sur les Heures d'ouverture du support	Oui	Oui
Notification au Client (appel téléphonique et/ou e-mail)	Oui	Oui
Astreinte en Heures non-ouvrées	Oui, en option Pendant l'astreinte, le Prestataire ne tient compte que des alertes de niveau 1 ou 2. Lors de la détection de telles alertes, l'équipe d'astreinte isole la Menace et crée un ticket qui sera traité sur les Heures d'ouverture du support par l'équipe Cybersécurité.	Non
Réponse apportée à la Menace	Intervention	Oui pour les cinq (5) premières minutes Tout dépassement est facturé : - Soit le temps est décompté d'un CTR associé au Service concerné et souscrit par le Client - Soit par le biais d'une facture sur la base des tarifs en vigueur chez le Prestataire
Formations aux Progiciels	Possible en option	Non
Analyse et rapports lors d'un Comité de pilotage de Cybersécurité période (réunion à distance)	Possible en option	Non

4. Informations complémentaires

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

Lorsque le Client souscrit à l'astreinte, 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 sur les heures d'astreinte (voir la ligne « Astreinte » dans le tableau ci-dessus).

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