CONDITIONS PARTICULIERES
« CYBER – TEST D'INTRUSION »

Version en vigueur au 18 juillet 2025

Le présent document décrit les conditions particulières applicables aux Prestations spécifiques CYBER pour la réalisation de tests d'intrusion (ci-après « **CP CYBER Test d'intrusion** »). 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 réalisation d'un audit et/ou d'un test d'intrusion (« *pentest* » en anglais) en vue d'identifier les risques de sécurité du système d'information du Client.

Article 2. Définitions

Les termes portant une majuscule dans les CGS et réutilisés au sein des présentes CP CYBER Test d'intrusion 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 :

« **Périmètre** » : désigne tout ou partie du Système d'information, objet des Prestations ;

« **Test d'intrusion** » : désigne la Prestation qui consiste à tester plusieurs codes d'exploitation sur le Système d'Information du Client, dans la limite du Périmètre, afin de déterminer ceux qui donnent des résultats positifs, permettant de déterminer la sensibilité aux attaques ainsi que l'existence de Vulnérabilités et d'aboutir à l'évaluation des cyber risques potentiels – à titre de clarification, le Test d'intrusion n'inclut pas d'opérations d'ingénierie sociale (par exemple : déposer des clés USB compromises, entrer sur le Site sous de faux prétextes, *etc.*), sauf demande explicite du Client acceptée par le Prestataire ;

« **Rapport** » : désigne un livrable documentaire sous forme d'un document de synthèse, en français, élaboré par le Prestataire et remis au Client à l'issue des Prestations.

« **Sécurité d'un Système d'information** » : désigne l'ensemble des moyens techniques et non-techniques de protection, permettant à un Système d'information de résister à des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des Données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles ;

« **Système d'information** » : désigne l'infrastructure informatique du Client, comprenant l'ensemble des ressources, Matériels, Données, Produits logiciels ou logiciels-tiers, réseau, système d'exploitation, système de stockage des Données et processus interconnectés permettant la collecte, le stockage, le traitement et la diffusion d'informations au sein de l'organisation du Client ;

« **Vulnérabilités** » : désigne un défaut pouvant être créé par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser (par exemple : une mauvaise configuration ou une configuration non-mise à jour, faiblesse(s) dans l'exploitation). Elles peuvent être utilisées par un code d'exploitation et conduire à une intrusion dans le Système d'information, notamment afin de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des Données qu'il contient. A titre de clarification, ne sont pas considérées comme des Vulnérabilités au titre du présent Contrat les vulnérabilités de nature organisationnelle ou procédurale.

Article 3. Obligations des Parties

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

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 :

Les Prestations s'inscrivant dans les présentes CP CYBER Test d'intrusion sont décrites à l'**Annexe A** des présentes CP CYBER Test d'intrusion. Préalablement à la réalisation du Test d'intrusion, le Client doit valider le Périmètre en collaboration avec le Prestataire (voir **Annexe B**).

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

Si le Client souhaite modifier ledit Périmètre après sa validation (notamment en intégrant des éléments complémentaires non compris initialement dans le Test d'intrusion), il devra contacter le Prestataire par écrit. Aucune modification du Périmètre ne peut avoir lieu une fois le Test d'intrusion terminé.

Le Prestataire ne saurait être tenu pour responsable des dommages liés à une faute du Client dans le cadre de l'exécution du Contrat (par exemple : indisponibilité de ses référents internes, absence de respect de la réglementation applicable, absence de collaboration, *etc.*). Par ailleurs, et malgré le soin apporté à la réalisation des Prestations, le Prestataire ne saurait être responsable des dommages qui résulteraient d'un déni de service d'un élément quelconque du Système d'information du Client.

Article 5. Responsabilité

La section « Responsabilité » de l'article RESPONSABILITE des CGS est remplacée comme suit :

Responsabilité – La responsabilité du Prestataire, en cas de dommages directs prouvés survenus au Client, pour quelle que raison que ce soit et quel que soit le fondement

juridique invoqué ou retenu, tous préjudices confondus et cumulés au titre de tous les faits générateurs, sera expressément limitée et ne pourra en aucun cas excéder le cumul des sommes versées par le Client au titre des Prestations.

La responsabilité du Prestataire ne pourra toutefois être exclue ou plafonnée en cas de dommages corporels ou de dommages causés par le dol ou la faute lourde telle que définie par la jurisprudence.

L'article 12 RESPONSABILITE des CGS est complété comme suit :

Exclusions de responsabilité – Le Prestataire ne saurait être tenu pour responsable des dommages liés à une faute du Client dans le cadre de l'exécution du Contrat (par exemple : indisponibilité de ses référents internes, absence de respect de la réglementation applicable, absence de collaboration, *etc.*). Par ailleurs, et malgré le soin apporté à la réalisation des Prestations, le Prestataire ne saurait être responsable des dommages qui résulteraient d'un déni de service d'un élément quelconque du Système d'information du Client.

ANNEXE A – DESCRIPTION DES PRESTATIONS ET NIVEAUX DE SERVICE

Article 1. Description des Prestations

1.1. Prérequis aux Prestations

Préalablement à l'exécution des Prestations, le Client s'engage à fournir 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 (par exemple : politique de sécurité, analyse des risques, procédures d'exploitation de la sécurité, gestion de la production *etc.*) afin que le Prestataire soit en mesure de délimiter strictement les contours de son intervention et de mener les Prestations dans les meilleures conditions.

Plus spécifiquement, afin de permettre au Prestataire de réaliser les Prestations, le Client :

- Autorise le Prestataire à réaliser un Test d'intrusion sur le Périmètre défini entre les Parties (cibles auditées, Vulnérabilités connues par le Client à exploiter *etc.*) sur la période définie pour la réalisation du Test d'intrusion, et
- Réalise une sauvegarde préalable et sécurisée du Système d'information (notamment des Données et Contenus) dans le Périmètre du Test d'intrusion, et
- Fournit au Prestataire tous habilitations et droits nécessaires sur la période définie pour réaliser le Test d'intrusion (il est rappelé au Client qu'il lui reviendra de s'assurer que les habilitations et droits nécessaires ont été retirés à la fin de la période définie pour réaliser le Test), et
- Fournit au Prestataire une liste des Vulnérabilités déjà connues par lui et s'abstient de corriger ou dissimuler une Vulnérabilité dont il pourrait avoir connaissance avant la réalisation du Test d'intrusion, et
- Fournit au Prestataire une liste des actifs sur lesquels le Test d'intrusion ne peut être réalisé, et
- Vérifie l'auditabilité des tiers (sous-traitants, prestataires, clients, partenaires) qui pourraient entrer dans le Périmètre et le cas échéant à respecter la procédure convenue avec eux, notamment concernant leur information ou autorisation préalable et écrite à la réalisation du Test d'intrusion, et
- Fournit, sur demande du Prestataire, tout justificatif lié à cette auditabilité qui se réserve le droit de suspendre les Prestation jusqu'à l'obtention de ces justificatifs, et
- S'assure, si le Test d'intrusion doit être effectué dans un environnement de test, que celui-ci possède les mêmes caractéristiques que l'environnement de production pour que les résultats du Test d'intrusion puissent être parlants et s'engager à générer des informations d'identification factices permettant d'assurer le bon déroulement du Test d'intrusion, et
- S'abstient de prévoir la réalisation du Test d'intrusion en même temps qu'une opération importante sur son activité (par exemple : migration informatique, lancement d'une campagne commerciale, *etc.*), et

Par ailleurs, le Client peut informer, s'il le souhaite, les salariés concernés des conditions de réalisation du Test d'intrusion.

1.2. Planification des Prestations et définition du Périmètre

Les Parties déterminent ensemble, en considération des contraintes d'exploitation du Système d'Information du Client, le planning des Prestations. Sauf exception convenue entre les Parties (par exemple : dans l'Offre commerciale), les Prestations ont lieu durant les Heures Ouvrées.

Avant la réalisation du Test d'intrusion, les Parties s'engagent à réaliser une réunion de lancement pour définir les éléments suivants : (i) la méthodologie du Test d'intrusion, (ii) le type de profil en charge de la réalisation du Test d'intrusion, (iii) les éléments attendus de la part du Client par le Prestataire pour définir le Périmètre (notamment : Test d'intrusion externe et/ou interne, les cibles auditées, la période de réalisation, les habilitations et droits ouverts, la liste des Vulnérabilités connues et le cas échéant les exclusions), (iv) si cette personne n'a pas été désignée auparavant, le référent du Client. Après la réunion de lancement, le Client fournit au Prestataire les informations nécessaires sur le Périmètre. Après finalisation de ce Périmètre, le Prestataire fera parvenir au Client la fiche reprenant ce Périmètre et qui vaudra autorisation par le Client de réaliser le Test d'intrusion et qui constituera automatiquement l'**Annexe B** des présentes CP CYBER Test d'intrusion.

1.3. Réalisation du Test d'intrusion

Au cours du Test d'intrusion, le Prestataire s'engage à :

- Réaliser des constats et observations factuels et basés sur la preuve ;
- Tracer toute modification effectuée sur le Système d'Information du Client dans une main-courante ;
- Prendre toute précaution utile permettant de préserver la confidentialité et plus largement la sécurité des Données et Contenus relatifs au Client et/ou aux clients du Client ;
- Tracer les actions et résultats du Test d'intrusion ;
- A exploiter les Vulnérabilités découvertes par le Prestataire au cours des Prestations, sauf si une ou plusieurs d'entre elles sont connues pour rendre la cible de la Vulnérabilité instable voire provoquer un déni de service, sauf accord expresse du Client. Dans ce cas, le Client sera informé au préalable des conséquences potentielles de l'exploitation de ces Vulnérabilités par le Prestataire et fournira par écrit la liste des Vulnérabilités instables qu'il autorise le Prestataire à exploiter.
- A l'issue du Test d'intrusion, à effacer toutes ses traces, persistances et pivots qu'il a utilisés dans le cadre du Test d'intrusion et qu'il a répertoriés dans la

main-courante des actions qu'il a réalisées pour contourner les mécanismes de sécurité.

Pour les Tests d'intrusion réalisés en externe : Si au cours des Prestations, le Prestataire détecte une Vulnérabilité ou un ensemble de Vulnérabilités présentant un risque critique selon le référentiel figurant en **Annexe C**, le Prestataire en informe le Client dans les meilleurs délais et peut lui conseiller des mesures correctives permettant de limiter le risque identifié.

1.4. Livrables associés aux Prestations

Le Prestataire informe le Client de la fin du Test d'intrusion. Dans ce cadre, le Prestataire peut présenter les premiers constats et conclusions du Test d'intrusion (par exemple : présence de Vulnérabilités majeures ou critiques identifiée). Le Prestataire rédige ensuite le Rapport qu'il remet au Client dans les quinze (15) Jours Ouvrés suivant la fin du Test d'intrusion et qui comprend : (i) la liste des Vulnérabilités découvertes et exploitées par le Prestataire afin d'entrer dans le Système d'information du Client, (ii) l'ensemble des moyens mis en œuvre permettant de réaliser le Test d'intrusion, (iii) un tableau synthétique des résultats du Test d'intrusion (par exemple : synthèse des Vulnérabilités relevées classées selon une échelle de valeur ou synthèse des mesures correctives proposées classées par criticité, complexité de correction et/ou coût de mise en œuvre estimé) ainsi que (iv) la synthèse de l'analyse incluant les points forts et faibles relevés pendant l'audit. La partie du Rapport contenant le (iv) précisé ci-avant pourra être fourni par le Client à sa direction générale ainsi qu'aux services intéressés et autorisés à y accéder.

Le Client disposera d'un délai de huit (8) jours pour valider le Rapport. S'il souhaite formuler une ou plusieurs réserves, le Client reporte la nature et la raison des réserves sur le Rapport qu'il met à disposition du Prestataire ou par e-mail qu'il envoie au Prestataire. Les réserves devront être en lien direct avec les Prestations et imputables au Prestataire. Après confirmation par le Prestataire que les réserves sont justifiées, ce dernier procèdera à leur correction dans un délai de quinze (15) jours. Sans retour de la part du Client ou si le Client émet uniquement des réserves mineures dans le délai susmentionné, la recette est réputée prononcée par le Client et les Prestations sont considérées comme conformes.

1.5. Fin des Prestations

Lorsque le Client y a souscrit par le biais de l'Offre commerciale, les Parties peuvent convenir d'organiser une réunion de restitution des Prestations, celle-ci devant se tenir dans un délai de maximum deux (2) mois après la fin du Test d'intrusion. Cette réunion permettra notamment de présenter une synthèse des constats faits pendant le Test d'intrusion, des scénarios d'exploitation de certaines Vulnérabilités, des recommandations et d'organiser un jeu de questions/réponses.

Si le Client n'a pas souscrit à une telle réunion, le Prestataire lui fournit le Rapport par e-mail.

Article 2. Limites des Prestations

Dans le cadre des Prestations, le Prestataire a informé des risques inhérents à l'exécution des Prestations, notamment concernant la disponibilité (par exemple : en cas de survenance d'un déni de service lors du scan de Vulnérabilités d'une machine ou d'un serveur) et l'intégrité de la surface du Système d'information ciblé par le Test d'intrusion.

Le Prestataire a notamment informé le Client de la possibilité de réaliser les tests d'intrusion depuis l'intérieur ou depuis l'extérieur du système d'information (par exemple : depuis Internet ou le réseau interconnecté d'un tiers).

Par ailleurs, le Prestataire a informé le Client que la réalisation du Test d'intrusion ne saurait en aucun cas être exhaustive : le Test d'intrusion ne permet pas de révéler l'ensemble des Vulnérabilités potentielles du Système d'Information, y compris au sein du Périmètre. Il a uniquement pour but de démontrer l'existence de certaines Vulnérabilités au moment de la réalisation du Test d'intrusion et la possibilité d'en exploiter certaines.

Enfin, le Prestataire rappelle que les vulnérabilités de nature organisationnelle ou procédurale ne font pas partie des Vulnérabilités que le Prestataire cherche à découvrir et à exploiter et que les Prestations n'incluent pas d'opérations d'ingénierie sociale.

ANNEXE B – PERIMETRE ET MODALITES D'EXECUTION DU TEST D'INTRUSION

Ce document est fourni par le Prestataire et doit être complété entre les Parties préalablement à la réalisation du Test d'intrusion. Le document pourra évoluer sur accord des Parties.

ANNEXE C – ECHELLE DE CLASSIFICATION DES VULNERABILITES

Le Prestataire utilise l'échelle suivante de classification des Vulnérabilités proposée par l'ANSSI pour la réalisation du Test d'intrusion :

Article 1. Niveau de risque lié

- Mineur : faible risque sur le Système d'Information et pouvant nécessiter une correction ;
- Important : risque modéré sur le Système d'Information et nécessitant une correction à moyen terme ;
- Majeur : risque majeur sur le Système d'Information nécessitant une correction à court terme ;
- Critique : risque critique sur le Système d'Information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service.

Article 2. Facilité d'exploitation

Elle correspond au niveau d'expertise et aux moyens nécessaire à la réalisation de l'attaque.

- Mineur : exploitation triviale, sans outil particulier ;
- Important : exploitation nécessitant des techniques simples et des outils disponibles publiquement ;
- Elevée : exploitation de Vulnérabilités publiques nécessitant des compétences en Sécurité des systèmes d'information et le développement d'outils simples ;
- Difficile : exploitation de Vulnérabilités non publiées nécessitant une expertise en Sécurité des systèmes d'information et le développement d'outils spécifiques et ciblés.

Article 3. Impact

Il correspond aux conséquences que l'exploitation de la Vulnérabilité peut entraîner sur le Système d'Information du Client.

- Mineur : pas de conséquence directe sur la Sécurité du Système d'Information audité ;
- Important : conséquences isolées sur des points précis du Système d'Information audité ;

- Majeur : conséquences restreintes sur une partie du Système d'Information audité ;
- Critique : conséquences généralisées sur l'ensemble du Système d'Information audité.

Article 4. Niveau de risque

Exploitation / Impact	Difficile	Elevée	Modérée	Facile
Mineur	Mineur	Mineur	Important	Majeur
Important	Mineur	Important	Important	Majeur
Majeur	Important	Majeur	Majeur	Critique
Critique	Important	Majeur	Critique	Critique