OCI INFORMATIQUE & DIGITAL

CONDITIONS PARTICULIERES
« CYBER – TEST D'INTRUSION »

Version en vigueur au 2 mai 2026

Le présent document décrit les Conditions particulières applicables aux Prestations spécifiques à pour la réalisation de tests d'intrusions.

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. Champ d'application

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 sécuritaires du système d'information du Client et de formuler des recommandations à destination du Client à l'issue du test d'intrusion en vue d'améliorer les 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.

Article 2. Définitions spécifiques

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

« **Périmètre** » désigne le périmètre physique et/ou informatique du Client sur lequel le Prestataire réalise le Test d'intrusion et/ou des opérations d'ingénierie sociale, ce périmètre étant défini conjointement par les Parties lors de la réunion de lancement ;

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

« **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 et reprise à l'Offre commerciale ;

« **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 du Client, notamment afin de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des Données qu'il contient. Le Prestataire classifie les Vulnérabilités selon le niveau de risque lié, leur facilité d'exploitation et l'impact sur le système d'information audité (pour ce faire, il utilise l'échelle de classification des Vulnérabilités proposée par l'ANSSI). 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. Périmètre des Prestations

Le Client a souscrit à des Prestations par le biais d'une Offre commerciale qui s'inscrivent dans les présentes Conditions particulières.

Article 4. Description détaillée des Prestations

4.1. Prérequis

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 de son 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 d'intrusion), 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.*).

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

4.2. Planification des Prestations et définition du Périmètre

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 d'intervention du Prestataire (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.

Si le Client souhaite modifier le 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.

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.

4.3. Réalisation du Test d'intrusion

Au cours du Test d'intrusion, le Prestataire s'engage à :
- Réaliser des constats et observations factuels et étayés ;
- 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 ;
- 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, le Prestataire effacera toutes les 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 le Prestataire en informe le Client dans les meilleurs délais et peut lui conseiller des mesures correctives permettant de limiter le risque identifié.

4.4. 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 appliquera la procédure de Recette associée aux livrables documentaires (définie au sein CGS) pour valider le Rapport.

4.5. 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 5. Limites générales des Prestations

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 du Client (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 du Client, 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.

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 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.

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.

Article 6. Modalités spécifiques de Réversibilité

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