



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**SECRETARIAT GENERAL DU GOUVERNEMENT
DIRECTION DES SERVICES ADMINISTRATIFS ET FINANCIERS**

Prestations de service de sécurité informatique (sécurité périmétrique et cyber-sécurité) ainsi que des prestations et fournitures associées au profit du Défenseur des droits

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

N° de consultation : 26_BAM_057_AC00

Procédure de passation : Accord-cadre est passé selon la procédure d'appel d'offres ouvert en application des articles L 2124-2, R 2124-1, R 2124-2, R 2161-2 à R 2161-5 du code de la commande publique.

TABLE DES MATIÈRES

Article 1 - Identification des parties	4
1.1 Désignation du représentant du pouvoir adjudicateur	4
1.2 Titulaire	4
1.3 Bénéficiaire	4
Article 2 - Terminologie	4
Article 3 - Généralités	5
3.1 Contexte	5
3.2 Objet du marché	5
3.3 Décomposition du marché	6
3.4 Lieu d'exécution	6
Article 4 - Prérequis techniques	6
Article 5 - POSTE 1 : Initialisation technique du marché	7
5.1 Nature du poste	7
5.2 Objet de la prestation	7
5.3 Opérations nécessaires à l'initialisation du marché	7
5.4 Cartographie du système réseau d'information du DDD	7
5.5 Modalités d'interconnexion entre les SI du bénéficiaire et du titulaire	8
5.6 Assistance du bénéficiaire	8
5.7 Délais de réalisation	8
5.8 Assistance réversibilité	9
Article 6 - POSTE 2 : Gestion et maintenance de la sécurité périmétrique	9
6.1 Nature du poste	9
6.2 Mise à jour Cartographie du système réseau du DDD	9
6.3 Périmètre des prestations de maintenance des équipements et solutions	9
6.4 Processus de mise à jour	9
6.5 Gestion des incidents	11
Article 7 - POSTE 3 : Gestion de cyber-sécurité	14
7.1 Nature du poste et UO	14
7.2 Objet des prestations	14
7.3 Mise en place du SOC ou COS (centre opérationnel de sécurité)	14
7.4 Remédiation	15
7.5 Maintenance éditeur MCO et MCS sur solution de détection et de protection contre les menaces informatiques avancées	16
7.6 Maintenance éditeur, MCO et MCS sur solution de décryptage de flux SSL	17
7.7 Modalités et délais des prestations	18
Article 8 - POSTE 4 : Gestion des logs réseaux et archivage	20
8.1 Nature du poste	20
8.2 Objet des prestations	20

8.3 Définition du service de reporting, corrélation et archivage de logs.....	20
8.4 Tableaux de bord attendus	21
8.5 Condition de sauvegarde et d'archivage des logs.....	22
Article 9 - POSTE 5 : Assistance au paramétrage des actifs réseaux	22
9.1 Nature du poste et Unité d'Œuvre	22
9.2 Objet et périmètre limitatif des prestations.....	22
9.3 Définitions.....	22
9.4 Modalités d'exécution et de consommation des CT.....	23
Article 10 - POSTE 6 : Assistance à l'exploitation du système réseau – Nouveau projet	23
10.1 Nature du poste et Unité d'Œuvre.....	23
10.2 Objet des prestations	23
10.3 Modalités d'exécution et d'estimation	23
Article 12 - POSTE 7 : Renouvellement des maintenances logicielles	26
12.1 Nature du poste et liste des UO	26
12.2 Objet des prestations	27
12.3 Fourniture et installation de matériel.....	27
12.4 Autre obligation.....	27
Article 14 - POSTE 8 : Réversibilité.....	27
14.1 Nature du poste et liste des UO	27
14.2 Processus de réversibilité	27
14.3 Transfert de compétences et connaissances	28
14.4 Eléments en entrée	28
14.5 Actions	28
14.6 Obligation du titulaire	28
Article 15 - Liste des annexes	29
Article 16 - Dérogations au CCAG-TIC	29

Article 1 - Identification des parties

1.1 Désignation du représentant du pouvoir adjudicateur

L'État représenté par :

La Direction des Services Administratifs et Financiers (DSAF) du Premier ministre
Secrétariat Général du Gouvernement
20 Avenue de Ségur — TSA 70723 - 75 334 PARIS CEDEX 07

Nom, prénom, qualité du signataire du marché public et personne habilitée à donner les renseignements prévus aux articles R2191-60 et R2191-61 du code de la commande publique (nantissement ou cessions de créances) :

Monsieur Serge Duval, Directeur des services administratifs et financiers du Premier ministre, nommé par décret du 7 mai 2015 publié au JO n° 0107 du 8 mai 2015.

La mention « acheteur » renvoie au pouvoir adjudicateur.

1.2 Titulaire

Le titulaire désigne l'opérateur économique déclaré attributaire de la consultation n°26_BAM_057_AC00.

1.3 Bénéficiaire

Le bénéficiaire du marché est le Défenseur des droits (DDD). Le Défenseur des Droits est également désigné par l'expression « le bénéficiaire ».

Article 2 - Terminologie

Le lexique du présent accord-cadre est le suivant :

- « DSAF » : renvoie à la Direction des Services Administratifs et Financiers du Premier ministre ;
- « DDD » : renvoie au « Défenseur Des Droits » ;
- « CCAP » : renvoie au « Cahier des Clauses Administratives Particulières » ;
- « CCTP » : renvoie au « Cahier des Clauses Techniques Particulières » ;
- « CCAG-TIC » : renvoi au « Cahier des Clauses Administratives Générales des marchés publics de Techniques de l'Information et de la Communication » issu de l'arrêté du 30 mars 2021 ;
- « Jour ouvré » : peut désigner le lundi, le mardi, le mercredi, le jeudi, le vendredi ;
- « Jours ouvrés » : du lundi au vendredi ;
- « Jour non ouvré » : le samedi ;
- « Jours fériés » : jours fériés légaux (au sens des articles L 3133-1 et L 3133-4 du Code du travail) en France et le dimanche ;
- « Heure ouvrée » : de 8h à 18h ;
- « Heure non ouvrée » : heure non compris dans la mention « heure ouvrée » ;
- « GTI » : Gestion des Temps d'Intervention ;
- « GTR » : Gestion des Temps de Résolution ;
- « SLA » : renvoi à « Service Level Agreement » traduit comme « niveau d'engagement de service » ;
- « MCO » : renvoie au « Maintien en Condition Opérationnelle » ;
- « MCS » : renvoie au « Maintien en Condition de Sécurité » ;
- « MAJ » : renvoie à « Mise à Jour », soit une modification technique ou fonctionnelle d'un périmètre applicatif donné ;
- « SOC » : renvoi à « Security Operation Center » traduit comme « centre opérationnel de sécurité » ;
- « C&C » : renvoi à « Command and Control » traduit comme « système de commande et de contrôle ».

3.1 Contexte

Le Défenseur des droits est une autorité administrative indépendante chargée d'un ensemble de missions visant à la protection des droits et libertés des citoyens et des personnes.

Le paysage des menaces se caractérise par des malwares sophistiqués permettant de traverser les défenses réseaux classiques comme les FireWalls, IDS/IPS, antivirus et filtrage Web et mail. Les attaquants sont capables de contourner facilement ces défenses traditionnelles basées sur des signatures.

Les techniques couramment utilisées par les attaquants incluent l'exploitation de vulnérabilités « zero-day » du java script cache et des charges polymorphiques. Chacune de ces techniques permet à un malware bien écrit de passer inaperçu à travers les solutions de défense classiques.

Les malwares prolifèrent, avec des milliers de versions entièrement nouvelles, ainsi que des variations personnalisées de vieilles attaques, des attaques combinées, des attaques encryptées, les attaques polymorphes et les attaques ciblées. Ces types d'attaques, désormais courantes, rendent les défenses fondées sur les signatures traditionnelles inutiles, indépendamment du fait que les défenses reposent sur des signatures et des vulnérabilités connues.

Fondées sur les caractéristiques actuelles des botnets, des malwares avancés et des menaces persistantes avancées (APT), la détection et l'éradication sont de plus en plus difficiles.

Ainsi, le Défenseur des Droits a besoin de réduire et de prévenir ces risques en matière de sécurité informatique, tout en s'assurant que l'occurrence est traitable afin de limiter les impacts sur son système informatique.

3.2 Objet du marché

Le présent marché a pour objet de faire assurer par le titulaire un ensemble de prestations informatiques relatives à la protection des systèmes d'information du DDD, de prévenir des menaces informatiques, d'assurer la **sécurité périmétrique** et la **cyber-sécurité** de l'intégralité de l'environnement informatique du DDD.

Le bénéficiaire dispose d'une architecture réseau spécifique contre les menaces informatiques avancées et d'un système de réponse sur incident.

Les prestations attendues au titre du présent marché couvrent plusieurs types de prestations :

- La détection du trafic réseau malicieux (requête DNS vers les serveurs de « Command and Control » (C&C);
- L'identification des systèmes compromis;
- Les actions d'analyse du système d'information en temps réel;
- La localisation des éléments réseau « malware » et de la/les source(s) de l'infection réseau;
- Le MCO et le MCS des éléments actifs réseaux;
- L'assistance téléphonique;
- Le paramétrage spécifique;
- L'évolution spécifique d'applicatif sécurité réseau;
- La mise en place et la gestion d'un SOC/COS;
- Le cas échéant, la fourniture de matériels « hardware » spécifiques et identiques à ceux du bénéficiaire pour la mise en clusters.

3.3 Décomposition du marché

Les prestations se décomposent de la manière suivante:

POSTE	OBJET	Référence CCTP	TRAITEMENT
Poste 1 - Initialisation technique du marché		Article 5	
2	Gestion et maintenance de la sécurité périmétrique	Article 6	Bons de commande
3	Gestion de cyber-sécurité	Article 7	Bons de commande
4	Gestion des logs réseaux et archivage	Article 8	Bons de commande
5	Assistance au paramétrage des actifs réseaux	Article 9	Forfait annuel
6	Assistance à l'exploitation du système réseau – Nouveau projet	Article 10	Bons de commande
7	Renouvellement des maintenances logicielles	Article 12	Bons de commande
8	Réversibilité	Article 14	Bons de commande

Le titulaire procède à l'initialisation technique du marché dans les conditions définies à l'article 5 du présent CCTP.

3.4 Lieu d'exécution

Les prestations s'exécutent principalement dans les locaux du titulaire et, le cas échéant, dans les locaux du bénéficiaire. Les locaux du bénéficiaire sont situés 3 place de Fontenoy, Paris 7^e.

Le cas échéant, le titulaire prend toute disposition utile (télétravail, etc.) pour assurer, sans interruption, la continuité des prestations.

Article 4 - Prérequis techniques

Pour des raisons de sécurité et conformément aux dispositions légales, réglementaires et notamment l'INT-AQ-PSL (objectif 7) de la PSSIE en vigueur, le titulaire du marché et/ou son sous-traitant/co-traitant doit être certifié des certifications et/ou qualifications ANSSI ou équivalentes et sur les outils composant le socle cyber-sécurité de l'institution :

1. PASSI (Prestataires d'audit de la sécurité des systèmes d'information)*;
2. Certification sur les outils composant le socle de Cyber-sécurité de l'institution : Menaces avancées — Déchiffrement SSL — EDR.

Seront appréciés les certifications suivantes : PDIS (Prestataires de détections d'incidents de sécurité) et/ou PRIS (Prestataires de réponses sur incidents de sécurité), en cours de certification ou déjà acquises.

*N.B. : est admis le titulaire qui serait en cours de certification/qualification ANSSI (PASSI). Les certifications sur les outils composant le socle cyber-sécurité devront être acquises au plus tard trois (3) mois après la notification du présent accord-cadre. Pour la formation à la certification PASSI qui démarrerait à la notification du présent marché, un délai supplémentaire de 18 mois pour la validation est autorisé, le titulaire devra apporter la preuve de son inscription à cette certification.

Article 5 - POSTE 1 : Initialisation technique du marché

5.1 Nature du poste

Le poste 1 constitue une phase préalable indispensable à l'exécution des prestations des postes 2 à 4. Il ne donne pas lieu à facturation et correspond à la mise en ordre de marche technique du marché.

Le titulaire propose le mode de communication entre les équipes techniques du Défenseur des droits, le SOC et le support téléphonique qui sera mis en œuvre.

Ce poste permet de définir également les moyens de connexion sécurisée (VPN, BASTION, etc.) qui permettront au titulaire de superviser à distance les équipements de sécurité informatique (pare-feu, switch, etc.).

5.2 Objet de la prestation

Le titulaire, à l'issue de la notification de l'accord-cadre, initie toutes les opérations nécessaires à la mise en fonction des prestations associées aux postes 2 à 4.

En outre, il effectue les opérations connexes aux prestations associées aux postes 2 à 4 de mise à jour de la cartographie de l'ensemble des systèmes informatiques du bénéficiaire en lien avec les prestations.

5.3 Opérations nécessaires à l'initialisation du marché

Le titulaire définit dans son offre l'ensemble des opérations nécessaires à la mise en fonction des prestations associées aux postes 2 à 4.

Les opérations doivent être conformes aux clauses du CCTP, CCAP du marché et à l'état de l'art.

Le titulaire s'engage dans une démarche de certification de formation des outils du socle de cyber sécurité de l'acheteur s'il ne dispose pas déjà de ces certifications. À compter de la date de notification, le titulaire dispose un délai de 3 mois au plus tard à compter de la notification du marché pour transmettre les documents attestant de la certification sur les outils composant le socle de Cyber-sécurité de l'institution : Gestion des menaces avancées — Déchiffrement SSL — EDR.

Le titulaire doit démontrer qu'il a validé, ou qu'il est en cours validation de la certification PASSI (Prestataires d'audit de la sécurité des systèmes d'information).

La validation de ces formations certifiées est intégrée dans le procès-verbal de la bonne exécution de l'initialisation technique du présent marché.

5.4 Cartographie du système réseau d'information du DDD

Le titulaire rédige et fournit à l'issue de la notification du présent marché et indépendamment de toute commande d'unités d'œuvre, un document de la cartographie des matériels et logiciels qui constitue le périmètre de son intervention.

Cette cartographie du réseau du SI du DDD est rédigée conformément aux stipulations du CCAP.

En outre, cette cartographie doit comprendre :

- les éléments matériels et logiciels du réseau du SI;
- les interactions fonctionnelles et logiques des environnements réseaux.

Le délai de transmission du livrable est de **30 jours calendaires à compter de la notification du présent marché.**

Cette cartographie permet de démontrer au DDD que le titulaire a pris en compte l'ensemble des matériels et logiciels qui font partie de son périmètre d'intervention dans le présent marché.

La cartographie réalisée est amendée avant et après chaque intervention du poste 2.

La cartographie est amendée après chaque modification majeure des matériels et logiciels compris dans le périmètre d'intervention du titulaire.

5.5 Modalités d'interconnexion entre les SI du bénéficiaire et du titulaire

5.5.1 Respect des exigences de sécurité du bénéficiaire

Au même titre que les agents de l'acheteur, le titulaire prend connaissance et applique les règlements internes de l'acheteur (PSSIE, directive d'utilisation des systèmes d'information, directive d'utilisation de la messagerie, etc.).

5.5.2 Respect des standards et méthodologies de l'acheteur :

Le titulaire respecte les standards et les méthodologies préconisés par le bénéficiaire et figurant en annexe au CCTP du présent marché.

5.5.3 Respect du périmètre de la prestation :

Le titulaire ne doit pas tenter d'accéder à des informations ou à des ressources informatiques ne faisant pas partie du périmètre de la prestation.

5.5.4 Interconnexion des SI de l'acheteur et du titulaire :

En cas d'interconnexion des SI de l'acheteur et du titulaire, le titulaire doit prendre les mesures de sécurité nécessaires afin de maintenir le niveau de sécurité global des SI. L'interconnexion devra être réalisée via des infrastructures d'accès validées par l'acheteur au travers d'une étude ciblée, dans le respect du cadre technique et des règles de sécurité de l'acheteur.

Pour chaque interconnexion, les éléments suivants doivent être définis :

- Flux et protocoles autorisés, ainsi que les ressources auxquelles le titulaire est autorisé à accéder au travers de la zone « partenaire ». Ces éléments doivent être restreints au strict nécessaire ;
- Les modalités d'authentification requises : authentification par mot de passe, par mot de passe unique et/ou par certificat ;
- Les modalités de chiffrement des échanges : chiffrement des flux transitant sur internet est requis ;
- Les exigences spécifiques de traçabilité des accès
- Les moyens de sécurité supplémentaire à mettre en œuvre : contrôle de conformité, outils de détection ou de prévention d'instruction, contrôle de contenu, filtrage applicatif, etc....

5.6 Assistance du bénéficiaire

Le bénéficiaire assiste le titulaire sur l'ensemble des opérations du titulaire.

Le bénéficiaire assiste le titulaire afin que ce dernier puisse effectuer les opérations nécessaires à la réalisation de ce poste et in fine, nécessaire à la mise en place des prestations.

5.7 Délais de réalisation

Le titulaire se conforme aux délais indiqués dans son offre quant à la réalisation de l'ensemble des opérations nécessaires à la mise en marche des prestations des postes 2 à 4.

Seule la cartographie du système comporte un **délai maximal de 30 jours** à compter de la notification du marché.

5.8 Assistance réversibilité

Le titulaire peut être assisté sur cette prestation d'initialisation par l'acheteur.

Article 6 - POSTE 2 : Gestion et maintenance de la sécurité périmétrique

6.1 Nature du poste

Le poste 2 est réalisé tous les trois mois et donne lieu à l'établissement d'un bon de commande au préalable

Le bénéficiaire peut réaliser des actions autonomes sur tout ou partie de son système d'information. Le titulaire est informé des modifications réalisées par le bénéficiaire.

6.2 Mise à jour Cartographie du système réseau du DDD

Le titulaire met en place, en fonction de la réalisation des prestations attendues au titre du marché, une mise à jour trimestrielle du document « cartographie du système réseau d'information du DDD » selon les mêmes modalités que celles présentées à l'article 5.4 du présent CCTP.

La fréquence de mise à jour est trimestrielle.

La mise à jour du document intervient à l'issue d'une mise à jour de tout ou partie du périmètre réseau du DDD.

6.3 Périmètre des prestations de maintenance des équipements et solutions

Le périmètre d'intervention concerne les environnements logiciels :

- Solution Microsoft de cryptage de disques durs ;
- Solution Microsoft réseau de type 802.X

Le périmètre d'intervention concerne les environnements matériels suivants :

- Pare-feux et solution MFA2 associée ;
- serveur VPN ;
- serveur anti-spam ;
- appliance et bornes wifi ;
- switchs (cœur de réseau et switch d'étage et switchs serveurs).

L'ensemble du périmètre logiciel et matériel concerné par les prestations du poste 2 est décrit dans les annexes 1 et 2 du présent document.

En outre, le périmètre des prestations comprend aussi l'ensemble des éléments cartographiés au titre de la cartographie du système réseau d'information du DDD.

6.4 Processus de mise à jour

6.4.1 Origine des documents numériques des mises à jour

Les documents numériques (fichier, code, documentation, etc....) pour effectuer les mises à jour sont les documents officiels proposés par les différents éditeurs des solutions en place et mis à disposition par le Défenseur des droits au travers de son contrat avec les différents éditeurs.

Le titulaire applique, à l'issue de la mise à disposition des dits documents par le DDD, les mises à jour des logiciels du périmètre.

6.4.2 Périmètre de mise à jour

Le périmètre des prestations de mise à jour est décrit à l'article 6.3 du présent CCTP.

6.4.3 Fréquence de mise à jour

À l'exception des mises à jour relatives à la correction de failles de sécurité qui sont réalisées sous une (1) semaine dès détection de la faille, les opérations de mise à jour réseau sont effectuées tous les trimestres dans les conditions décrites ci-après.

6.4.4 Étendue de la prestation

6.4.4.1 Opération préalable à la mise à jour

Le titulaire procède à la réalisation d'une étude d'impact permettant de s'assurer que les mises à jour ne dégraderont pas l'environnement.

À cet effet, le titulaire décrit dans un document intitulé «Étude d'impact», et préalablement à la réalisation de chaque mise à jour, les éléments suivants :

- les éléments mis à jour (matériels et logiciels);
- les incompatibilités;
- les risques sur le SI (interruption, risques SSI, etc....);
- les mesures de prévention à prendre (dont répartition des charges entre le titulaire et le bénéficiaire le cas échéant);
- les conséquences estimées sur la performance globale du SI du DDD;
- les pré-requis techniques de la mise à jour;
- la durée de la mise à jour;
- des recommandations (notamment sur les incompatibilités qui seraient hors périmètre du titulaire dans le cadre de la présente prestation).

Le bénéficiaire doit approuver en tout ou partie le dispositif proposé issu de «l'étude d'impact» avant toute opération de mise à jour, avant le début des opérations.

Le titulaire dispose d'un délai d'une (1) semaine à compter du démarrage de la maintenance pour rendre ce livrable. Ce délai court chaque trimestre, à compter du démarrage de la prestation de maintenance, indépendamment des opérations de contrôle encore en cours sur les mêmes prestations au titre d'un ou plusieurs trimestres précédents.

Le bénéficiaire se prononce sur l'étude d'impact (alternativement) :

- admission de la mise à jour sans prise en compte des recommandations;
- admission de la mise à jour avec prise en compte totale des recommandations;
- admission de la mise à jour avec prise en compte partielle des recommandations.

6.4.4.2 Opération de mise à jour

1. Délais

Le titulaire dispose d'un délai d'une (1) semaine pour effectuer la Mise en Ordre de Marche (MOM) d'une mise à jour. Ce délai court à compter de la validation de l'étude d'impact.

2. Garantie de compatibilité

Le titulaire garantit au bénéficiaire, au titre des opérations de mise à jour trimestrielle, les compatibilités ascendantes des versions logicielles et/ou capacité et/ou versions matérielles hardware du périmètre de l'architecture réseau du DDD telles que décrites dans les annexes du présent CCTP.

3. Mise en ordre de marche

Le titulaire assure la Mise en Ordre de Marche (MOM) des mises à jour issues des différents éditeurs et celles d'élément(s) du périmètre du DDD requises au titre de la garantie de compatibilité.

4. Rapport d'opération de mise à jour

Dans un délai maximum d'une (1) semaine à l'issue de la Mise en Ordre de Marche (MOM), le titulaire fournit au bénéficiaire un rapport d'opération de mise à jour. Celui-ci concatène l'ensemble des données des éléments informatiques du périmètre du DDD mis à jour ainsi que les erreurs induites, le cas échéant.

5. Mise à jour de la cartographie du réseau du SI

Le titulaire met à jour la cartographie dans les conditions décrites au présent CCTP.

6.4.4.3 Opérations de contrôle

1. Vérification d'Aptitude (VA)

La décision de VA est produite dans un délai d'une (1) semaine à compter de la Mise en Ordre de Marche (MOM) des éléments par le titulaire.

2. Vérification de Service Régulier (VSR)

Par dérogation à l'article 32.4 du CCAG-TIC, la VSR se fait sur un délai de deux (2) semaines. Ce délai de 2 semaines court à compter de la décision d'admission de la VA. Elle a pour objet de contrôler l'application effective et pérenne des mises à jour.

3. Décision après vérifications

Les décisions après vérifications se font dans les conditions prévues à l'article 33 du CCAG-TIC.

6.4.5 Livrables associés à la prestation

Le bénéficiaire fournit au bénéficiaire, dans les conditions et délais prévus au présent CCTP, les livrables suivants :

- cartographie du réseau du SI ;
- étude d'impact des mises à jour ;
- rapport d'opération de mise à jour.

6.5 Gestion des incidents

6.5.1 Objet de la prestation

Au titre du poste 2, est attendue une prestation de gestion des incidents logiciels et matériels sur le périmètre informatique défini à l'article 6.3 du présent CCTP.

Le présent article a pour objet de définir les attentes minimales du bénéficiaire au titre de la gestion des incidents sur son infrastructure virtuelle.

6.5.2 Définition et cadrage des attendus

Un(e) incident/anomalie renvoie à une erreur matérielle ou logicielle conduisant à une défaillance du système informatique entre un état de temps n et n-1. Par nature, l'incident affecte la performance du système informatique.

6.5.3 Suivi des incidents

Le titulaire propose dans son offre un outil (logiciel) et/ou une chaîne de traitement d'incident.

Le titulaire peut proposer un outil d'initialisation des incidents (outil de « ticketing ») et de suivi de l'état des incidents. Le bénéficiaire doit avoir accès au dit outil.

6.5.4 Support téléphonique

Le titulaire propose dans son offre un support téléphonique.

Ce support téléphonique est à minima un support de niveau 0. Il est accessible aux jours et heures ouvrés (du lundi au vendredi de 9h à 18h).

Ce support permet (ou permet de mettre en lien le bénéficiaire avec un tiers service du titulaire) :

- d'apporter des renseignements, une aide à l'analyse et/ou la résolution d'incidents;
- d'initier pour le compte du bénéficiaire un ticket d'incident dans l'outil logiciel associé présenté dans son offre.

6.5.5 Classification des incidents

La classification associée aux anomalies est la suivante :

- anomalie bloquante : le dysfonctionnement bloque l'utilisation de l'élément logiciel ou matériel;
- anomalie majeure : le dysfonctionnement ne bloque pas l'utilisation du logiciel ou matériel, mais reste préjudiciable aux missions du bénéficiaire;
- anomalie mineure : le dysfonctionnement ne bloque en rien l'activité des logiciels et/ou matériels, mais affecte sa performance.

La classification associée aux incidents de sécurité est la suivante :

- incidents de sécurité critique : le dysfonctionnement concerne une faille de sécurité directe ou indirecte sur des éléments logiciels ou matériels conduisant à un arrêt total du système d'information entrant dans le périmètre défini à l'article 6.3 du présent CCTP;
- incidents de sécurité majeure : le dysfonctionnement concerne une faille de sécurité directe ou indirecte sur des éléments logiciels ou matériels conduisant à une mise en quarantaine d'une partie du système d'information entrant dans le périmètre défini à l'article 6.3 du présent CCTP;
- incidents de sécurité mineure : le dysfonctionnement concerne une faille de sécurité directe ou indirecte sur des éléments logiciels ou matériels conduisant une défaillance n'entrant pas dans les autres qualifications.

6.5.6 Conditions de traitement des incidents et anomalies

1. Remontée d'alerte

Le service de supervision du titulaire met en place un système de remontée d'alerte au bénéficiaire, afin de détecter tout comportement anormal sur le périmètre SI lié aux prestations (ex. : montée en charge du réseau), vols ou pertes d'informations sensibles appartenant à l'acheteur (documentation technique en particulier).

Le titulaire s'assure de l'état de fonctionnement permanent des équipements et logiciel sur son domaine SI.

Toute anomalie détectée par le titulaire doit être signalée aux équipes techniques du bénéficiaire, le titulaire met tout en œuvre pour rétablir le fonctionnement normal de l'équipement.

2. Enregistrement, traçabilité et gestion des incidents de sécurité

Le titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

3. Traitement des incidents de sécurité :

Le titulaire contacte les interlocuteurs de sécurité du bénéficiaire désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI du bénéficiaire. De plus :

- si cet incident a lieu sur le SI de du bénéficiaire, le titulaire participera, à la demande du bénéficiaire, au traitement de l'incident ;
- si cet incident a lieu sur le SI du titulaire, le titulaire autorisera le bénéficiaire ou un tiers désigné à participer au traitement de l'incident (si le bénéficiaire le souhaite).

6.5.7 Convention de service

Le titulaire, par l'outil logiciel de gestion des incidents qu'il met à disposition du bénéficiaire, traite les incidents qui lui sont remontés sur ledit outil.

Est considéré comme traité un incident qui est résolu (hors solution de contournement) et dont le système informatique retourne à son état d'avant défaillance.

Les délais d'engagement de service sont les suivants :

SLA	GTI	GTR	
Type d'anomalie	Délai d'intervention et/ou de prise en compte	Délai de fourniture d'une solution de contournement	Délai de fourniture d'une solution de résolution
Anomalie bloquante	1 heure ouvrée	3 heures	12 heures ouvrés
Anomalie majeure	1 heure ouvrée	1 jour ouvré	2 jours ouvrés
Anomalie mineure	4 heures ouvrées	3 jours ouvrés	6 jours ouvrés
Incident de sécurité critique	1 heure ouvrée	3 heures	6 heures
Incident de sécurité majeur	1 heure ouvrée	6 heures	12 heures
Incident de sécurité mineur	2 heures ouvrées	12 heures ouvrées	3 jours ouvrés

Les délais sont suspendus à la mise en ordre de marche de l'action de modification matérielle et/ou logicielle visant à traiter un incident par le titulaire.

Un ticket est fermé lorsque le bénéficiaire valide le traitement conforme d'un incident donné.

En cas de refus de validation du correctif apporté par le titulaire, le délai suspendu est reconduit (le titulaire ne dispose pas d'un nouveau délai plein).

Tout incident de sécurité déclaré pendant les périodes ouvrées doit être traité même si ce délai dépasse la période ouvrée

Ex : un ticket ouvert en heure ouvrée (16h00) qui nécessitera 4h d'intervention verra la fin d'intervention à 20h00

Toute prestation débutée pendant les heures ouvrées doit être réalisée conformément au délai indiqué dans le ticket d'ouverture de l'incident.

Le titulaire ne peut être tenu responsable d'un incident qui surviendrait pendant les heures non ouvrées.

Le titulaire peut s'il le souhaite et à ses frais prévenir le bénéficiaire d'un incident critique via un mécanisme de notification automatique. Le bénéficiaire décide des mesures qu'il conviendra de prendre, la prestation réalisée en dehors des heures ouvrées relèveront des prestations du poste 6.

6.5.8 Modalités d'exécution de la prestation

La prestation de gestion des incidents se fait via l'outil informatique proposé par le titulaire au profit du bénéficiaire.

Le titulaire est tenu à une obligation de vigilance, et peut initier l'ouverture d'un ticket incident en vue de sa résolution.

Article 7 - POSTE 3 : Gestion de cyber-sécurité

7.1 Nature du poste et UO

Le poste 3 est un service continu de gestion de la cyber-sécurité, exécuté par bons de commande, la durée totale du marché, reconduction(s) comprise(s).

UO	Prestations	Référence CCTP
UO-SOC-CYBER	Gestion cyber-sécurité	7.2 à 7.8 sauf 7.5

7.2 Objet des prestations

L'objet du poste 3 « gestion de cyber-sécurité » est de fournir au bénéficiaire un ensemble de solutions humaines, logicielles, organisationnelles de prévention et de traitement des menaces informatiques avancées dans le cadre de prestations dites de cyber-sécurité.

Au titre de ce poste sont attendus le MCO et le MCS correspondant à l'environnement de cybersécurité du bénéficiaire tel que présenté à l'annexe 2 du présent CCTP.

Le titulaire prend connaissance de l'environnement de cyber-sécurité du bénéficiaire, tel que présenté aux annexes 1 et 2 du présent CCTP, et propose des solutions adaptées à cet environnement.

Ainsi, le titulaire décrit dans un document les éléments suivants :

- mise en place du SOC et son interconnexion avec les SI du bénéficiaire ;
- mise en place des process de traitement des menaces avancées ;
- mise en place et gestion des systèmes de remédiation ;
- analyse et traitement des menaces avancées de type cyber ;
- MCO et MCS matériel et logiciel du périmètre SI attendu au titre de ce poste.

7.3 Mise en place du SOC ou COS (centre opérationnel de sécurité)

L'offre du titulaire décrit les éléments de son « COS » sur les aspects suivants :

- localisation ;
- numéro de support ;
- modèle de gestion ;
- personnels associés intervenants et surveillant les SI du bénéficiaire.

Le COS peut être mutualisé avec des tiers, être exclusivement dédié au bénéficiaire ou être sous modèle dit « hybride ».

En toute hypothèse, les données du bénéficiaire transitant par le COS doivent être strictement séparées et indépendantes de celles de tout autre tiers client du titulaire.

Depuis son centre de supervision, le titulaire surveille le bon fonctionnement et l'efficacité des équipements de sécurité du bénéficiaire. À l'aide d'outils propres au titulaire, les experts du titulaire sont alertés des incidents (pannes, défaillances, attaques...) et réagissent suivant le niveau retenu en fonction de la sévérité.

Les administrateurs du titulaire prennent en charge la gestion au quotidien des règles de sécurité des équipements de l'environnement technique du bénéficiaire. Sur appel téléphonique ou tout autre moyen validé par les deux parties, et après vérification de l'identité du demandeur, les administrateurs du titulaire interviennent à distance via un portail VPN permanent fourni par le Défenseur des droits pour effectuer les modifications demandées. Toutes les modifications sont enregistrées et résumées puis mises à disposition des administrateurs du bénéficiaire. Un dispositif de type BASTION sécurisé est aussi envisageable. Les connexions à distance doivent être sécurisées par des protocoles robustes et authentifiés par des mécanismes forts.

Toutes les connexions au travers de ces dispositifs doivent être tracées et identifiables.

7.4 Remédiation

Le service de remédiation actuellement en place est organisé sous forme de service permettant de répondre, dans un délai garanti, aux menaces détectées par les solutions déployées. Il doit être maintenu à l'identique.

Le titulaire devra disposer d'une certification sur le produit déjà en place au plus tard trois (3) mois suivant la date de notification du présent marché.

Le service de remédiation doit être assuré par le titulaire qui s'engagera dans le processus de remédiation.

Le titulaire a connaissance des capacités de la solution logicielle (**cf. annexes 1 et 2**) et son offre est basée sur celle-ci.

Il est précisé que les terminaux présents dans l'institution fonctionnent sous de multiples environnements (Windows 10, W Serveur 2016, 2019, Linux, etc.). De ce fait, la solution déployée est agnostique et fonctionne, quel que soit le système d'exploitation présent sur le terminal.

La prestation de remédiation est un service qui comprend :

- la fourniture des licences ;
- la supervision ;
- l'analyse.

Le service de remédiation permet de transmettre l'alerte en temps réel au bénéficiaire et au titulaire.

Le service fonctionne **de 9h à 18h du lundi au vendredi**.

Le délai de prise en compte (accusé de réception de l'alarme) se fait dans un délai maximum d'une (1)

heure, les premières mesures visant à assurer la sécurité sont réalisées dans un délai de quatre (4) heures.

Dans cette tranche horaire, les interventions se font à distance et peuvent être réalisées sur site pendant les heures ouvrées. Le déplacement est à la charge du titulaire (exemple : une mise à jour d'un équipement qui nécessite une présence physique).

Cependant, en cas de besoin, si une intervention en dehors des heures ouvrées, sur site s'avère nécessaire, cela donne à l'émission d'un bon de commande basé sur les prestations du poste 6.

Les interventions de maintenance se font selon le même mode opératoire.

Les matériels et logiciel du socle cyber sécurité du bénéficiaire doivent être mis à jour à chaque fois que l'éditeur propose une mise à jour critique (exemple s'il y a 2 mises à jour critique sur une semaine elles doivent obligatoirement être appliquées). Les mises à jour sont testées avant d'être déployées en production.

Tout incident relevé pendant la période couverte donne lieu à un traitement hors plage horaire.

Tout incident de cyber sécurité détecté pendant les heures ouvrées doit être traité même si ce délai dépasse la période ouvrée.

Ex : un incident ouvert en heure ouvrée (16h00) qui nécessitera 4h d'intervention verra la fin d'intervention à 20h00.

Un incident ouvert en période ouvrée ne peut être fermé pour cause de fin de période ouvrée.

Le titulaire ne peut être tenu responsable d'un incident qui surviendrait en période non ouvrée.

Le titulaire peut s'il le souhaite et à ses frais prévenir le bénéficiaire d'un incident critique via un mécanisme de notification automatique. En cas de besoin, si une intervention en dehors des heures ouvrées, sur site s'avère nécessaire, cela donne lieu à l'émission d'un bon de commande basé sur les prestations du poste 6.

Le titulaire propose dans son offre les différents modes de réaction et précise les modalités de prise en charge, de l'analyse à la suppression des codes malveillants détectés sur le système informatique.

La solution de remédiation actuellement déployée s'interface avec la solution de détection des menaces avancées en place (cf. annexes 1 et 2).

7.5 Maintenance éditeur MCO et MCS sur solution de détection et de protection contre les menaces informatiques avancées

Le bénéficiaire dispose déjà d'une solution fondée sur un boîtier dédié et composée des fonctionnalités de bases ci-après.

Le titulaire doit disposer d'une certification sur le produit déjà en place au plus tard trois (3) mois à compter de la date de notification du présent marché.

Description générique de la solution détection et protection contre les menaces avancées
La solution détecte des attaques technologiquement évoluées, notamment des attaques Zero-Day et APT.
La solution est capable de bloquer les tentatives d'exfiltrations de données en temps réel.
La solution détecte les trois étapes du cycle de vie d'une attaque via un malware avancé et met en évidence chaque étape de l'attaque : Exploit ; Dropper ; Data exfiltration.

La solution est invisible tant du côté de l'attaquant que de l'utilisateur interne.
La solution de détection n'ajoute pas de latence notable sur le réseau.
La solution détecte une attaque locale sans export de fichiers vers un service Cloud. Les systèmes préservant la confidentialité des données du DDD telle que l'échange de signatures sont acceptés et ne sont pas écartés.
La solution est capable de bloquer des communications sortantes vers des « command & control » depuis un poste compromis. Ainsi elle est installée en coupure et offre la possibilité de bloquer des communications sortantes malveillantes.
La solution est en mesure d'identifier avec précision les malwares et de maintenir un taux de faux positifs très faible. La détection inclut la protection contre les logiciels malveillants manquée par les produits de sécurité existants.
La solution utilise un « Global Intelligence Network » (une base de connaissance partagée) pour bénéficier des informations recueillies par les efforts de recherche de l'éditeur, dans lequel les abonnés reçoivent et éventuellement partagent, les renseignements concernant les logiciels malveillants.
La solution empêche la communication réseau à partir de l'analyse VM/Sand-box vers internet. Le malware analysé à l'intérieur de la VM (sand-box) n'est pas autorisé à communiquer avec un C & C ou URL sur Internet (analyse en interne)
La solution permet d'identifier les postes générant des alertes lorsqu'elle est déployée derrière un serveur proxy.

La liste reprend de manière non exhaustive les fonctionnalités génériques de la solution actuellement en place, le titulaire prendra connaissance de la version logicielle et matérielle qui a été installée sur le site (**voir annexes 1 et 2**) et se renseignera sur les aspects techniques de la solution auprès du fabricant/éditeur.

7.6 Maintenance éditeur, MCO et MCS sur solution de décryptage de flux SSL

Le bénéficiaire dispose déjà d'une solution fondée sur un boîtier dédié. Elle est composée des fonctionnalités de base décrites ci-après.

Le titulaire doit disposer d'une certification sur le produit déjà en place au plus tard trois (3) mois à compter de la date de notification du présent marché.

L'utilisation des protocoles de chiffrement, TLS ou SSL, pour protéger le contenu Web et celui du courrier électronique entre actuellement dans sa deuxième décennie, le nombre d'internautes qui chiffrent leurs communications en ligne a considérablement augmenté. Le Défenseur des droits dispose de moyens qui lui permettent de déchiffrer ce trafic de façon sélective. Cette stratégie de gestion du trafic chiffré prend en compte les exigences de conformité et respecte les réglementations locales en matière de confidentialité. La solution actuellement installée permet d'observer systématiquement le trafic chiffré utilisé pour les logiciels malveillants, le contrôle de ces derniers, ainsi que pour d'autres types d'activités malveillantes.

Ainsi, le Défenseur des Droits peut déchiffrer le flux de données web pour analyser automatiquement son contenu avec des outils de sécurité ad-hoc, avant de re-chiffrer le flux et de le renvoyer vers sa destination. Le recours au déchiffrement est encadré conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés.

- Compte tenu de la puissance de calcul nécessaire au traitement de ces flux, la solution matérielle (type Appliance), actuellement en place, peut absorber la charge actuelle et future.

- Le boîtier dispose de performances réseau significatives, permet le déchiffrement de tout protocole SSL/TLS sans pré-configuration imposée et est compatible avec les méthodes connects et starttls, elle permet également le traitement des flux.
- Le boîtier peut définir des vitesses de connexion/nombre de flux et le déploiement de l'Appliance SSL est transparent sur les systèmes finaux et les éléments de réseau intermédiaires. Il ne nécessite aucune modification au niveau de la configuration réseau, des adresses ou de la topologie d'IP, des IP clientes ou des configurations de navigateur Web.
- L'application préserve les applications (le texte brut décrypté est distribué sur l'Appliance de sécurité en tant que flux TCP généré avec les en-têtes de paquet comme s'ils étaient reçus).
- La solution permet une mise en miroir en sortie, dispose d'une interface de gestion en mode Web.
- Le boîtier permet différents modes de certifications et il est capable d'adresser des alertes par email.
- La solution de déchiffrement est compatible avec les débits des flux constatés au Défenseur des Droits et dispose d'une configuration en coupure (avec ou sans haute dispo) du système de détection.
- La solution intègre parfaitement les caractéristiques techniques suivantes : (Total Packet Processing, SSL Visibility Throughput, ConcurrentSSL Flow States [CPS], Full Handshake SSL sessions [CPS] selon le type de clés 1024-bit keys•2048-bit keys•ECDHE256, Input / Output, ports fibre et cuivre mode coupure).

La liste reprend de manière non exhaustive les fonctionnalités génériques de la solution actuellement en place, le titulaire prendra connaissance de la version logicielle et matérielle qui a été installée sur le site (cf. annexe 1 et 2) et se renseignera sur les aspects techniques de la solution auprès du fabricant/éditeur.

7.7 Modalités et délais des prestations

Les modalités suivantes s'appliquent à tous les services de type MCO et MCS.

7.7.1 Suivi des états et des incidents

Quel que soit le moyen de communication utilisé (courriel ou téléphone), la langue de correspondance entre le titulaire et l'administration est le français.

Le titulaire fait parvenir trimestriellement au Défenseur des Droits, un état récapitulatif des demandes reçues et des incidents apparus sur la période précédente. Cet état indique notamment :

- le numéro de la demande ;
- la date et l'heure de la demande ;
- son statut : ouverte, close ;
- un compte rendu détaillé des échanges entre le titulaire et le Défenseur des Droits et des actions réalisées par le titulaire pour traiter la demande.

Le titulaire met en place un COPIL trimestriel (en présentiel ou à distance) où sera présentée sous forme de tableaux de bord schématiques l'activité de cyber-défense de la solution actuellement en place. Toutes les alertes et solutions qui ont été mises en œuvre seront reprises dans les tableaux de bord. Le formalisme des tableaux de bords actuel sera repris, à minima, à l'identique.

7.7.2 Taux de décrochage :

Le contact téléphonique donnant lieu à la création d'un ticket généré par le support SOC doit fonctionner de la manière suivante :

- Une alerte est déclenchée par les équipes du Défenseur des droits auprès du support SOC fourni par le titulaire.
- Une alerte est déclenchée par le support SOC du titulaire auprès des équipes du Défenseur des Droits.

Cet échange permet de définir le contexte et la criticité de l'incident (bloquant ou non bloquant). La personne en charge de la résolution du problème devra recontacter, par téléphone ou courriel, les équipes techniques du Défenseur des droits au plus tard dans les trente (30) minutes qui suivent et l'informer de la ressource technique qui sera désignée et de la programmation de l'intervention pour le traitement de l'incident.

Les modalités d'intervention sont les suivantes :

- **Anomalie bloquante** : Le titulaire s'engage à intervenir à distance ou sur site, dans un délai de 4 h 00 à compter du moment où il est informé d'une anomalie bloquante. Un incident critique signifie que la production est hors service.
- **Anomalie non Bloquante** : Le titulaire s'engage à intervenir à distance ou sur site, dans un délai de 8 h 00 à compter du moment où il est informé d'une anomalie non bloquante. Dans le cas d'une anomalie non bloquante, une programmation dans un délai plus long pourra être envisagée entre le Défenseur des Droits et le titulaire.

7.7.3 Modalités de prise en charge

Le titulaire propose les différents modes de réaction et précise les modalités de prise en charge avec une granularité allant de la simple analyse/remédiation jusqu'à la prestation de forensique (Poste 7).

Il précise de manière détaillée et dans un format clair et compréhensible (tableau, matrice,...) les services, processus, livrables et SLA correspondant aux prestations. Par ailleurs le Défenseur des Droits accèdera à une interface (portail) sécurisée permettant d'avoir un accès aux tableaux de bord. Le titulaire assurera le maintien en condition opérationnelle des outils de cyber-sécurité pendant toute la durée du marché. De la même façon, le titulaire assurera la collecte et la conservation des logs provenant des solutions existantes.

7.7.4 Renouvellement des maintenances éditeurs des solutions

Le titulaire propose le renouvellement des maintenances éditeurs aux dates anniversaires des différents produits installés. Ces maintenances sont décrites dans le poste 7 à l'article 11 du présent document.

7.7.5 Coordination des prestations

Le titulaire désigne un responsable technique pour l'ensemble des prestations. Il est l'interlocuteur principal du service informatique du Défenseur des Droits. Il assure la coordination des prestations relatives aux interventions sur site et à la mise à jour des documents techniques.

7.7.6 Pilotage et procédure de réaction sur détection

Le titulaire constitue un dossier comprenant les scénarios d'intrusion et les modes de réaction associés. Par ailleurs ce dossier devra être enrichi durant tout le marché et notamment par l'ajout de scénarios complémentaires ou non envisagés au départ de la prestation. Le livrable se fait sur un support numérique sur la base d'un document (word, pdf, powerpoint).

Le titulaire reprend les tableaux de bord de restitution existant chez le bénéficiaire. Ceux-ci sont transmis à l'issue de la notification de l'accord-cadre.

Une réunion d'avancement se déroule chaque trimestre, par téléphone ou en présentiel, afin de s'assurer de l'adéquation entre le besoin exprimé et la prestation réalisée. À l'issue de chaque réunion, une fiche liaison technique est complétée. Les comptes rendus sont rédigés par le titulaire. La gestion des actions soulevées lors de ces réunions d'avancement est faite par le représentant du titulaire. Ces réunions ne donnent pas lieu à facturation.

7.7.7 Dossier de procédure et de rédaction sur détection – Plan assurance qualité

Le titulaire constitue un dossier comprenant les scénarios d'intrusion et les modes de réactions associés. Par ailleurs ce dossier doit être enrichi durant toute l'exécution du marché et notamment par les rapports d'incident.

À cet égard, le titulaire élabore un plan assurance qualité d'exploitation et en démontre le caractère opérationnel en détaillant les procédures suivantes : gestion documentaire, gestion des incidents...

Article 8 - POSTE 4 : Gestion des logs réseaux et archivage

8.1 Nature du poste

Le poste 4 est à bon de commande. Les prestations associées à ce poste sont relatives à un service continu, reconduites, le cas échéant, chaque année.

8.2 Objet des prestations

L'objet de ce poste est de permettre au bénéficiaire de stocker l'ensemble des opérations informatiques ayant lieu pendant toute la durée du marché sur ses serveurs internes.

8.3 Définition du service de reporting, corrélation et archivage de logs

Ce service propose la collecte de l'ensemble des logs des équipements de sécurité, leur indexation, leur archivage et leur restitution aux administrateurs du Défenseur des Droits sur un support défini et accessible par les logiciels du moment (portail d'accès, disque dur externe, clé USB de grande capacité, CD/DVD). Cette prestation peut être accompagnée d'une option de corrélation des événements afin d'opter pour une détection plus « pointue » des comportements anormaux.

Un reporting récurrent et programmé avec les administrateurs du Défenseur Des droits est adressé de façon récurrente et régulière. Le Défenseur des droits dispose d'une solution d'archivage des logs en open source (GREYLOG).

Exemples d'items supervisés :

- **Switch d'étage et Cœur de réseau :** Supervision des équipements (disponibilité, vitesse des ports, charge CPU, charge Ram), sauvegarde régulière des configurations (périodique, à chaque modification, archivage), sauvegarde des firmwares, monitoring du trafic réseau, définition des seuils d'alerte, remontée des anomalies.
Le titulaire peut effectuer des opérations directes sur les équipements supervisés (sauvegarde des configurations, modifications des règles, extraction de rapports, gestion des licences, up-times...).
- **Firewalls :** Gestion des abonnements et des maintenances des différents éditeurs et constructeurs (l'achat des licences restant à la charge du bénéficiaire), surveillance du bon fonctionnement des équipements, sauvegarde des configurations pré et post modification, gestion des règles de sécurité, modifications des règles (illimitées), mise à jour des firmwares (si nécessaire), applications des correctifs (si nécessaire), modification de paramétrages, reporting mensuel, envoi de rapports détaillés sur l'utilisation des équipements.
- **Serveur VPN SSL :** Surveillance du bon fonctionnement des équipements, sauvegarde des configurations pré et post modification, gestion des règles de sécurité, création de nouveaux utilisateurs, création des bookmarks et des règles d'accès, modifications des règles (illimitées), mise à

jour des firmwares (si nécessaire), applications des correctifs (si nécessaire), modifications de paramètres, reporting mensuel, alertes sur Login failed, alertes sur dépassement de seuil.

- **Serveur Antispam – bornes Wifi** : Surveillance du bon fonctionnement des équipements, sauvegarde des configurations pré et post modification, gestion des règles de sécurité, modifications des règles (illimitées), mise à jour des firmwares (si nécessaire), applications des correctifs (si nécessaire), modifications de paramètres, reporting mensuel.
- **Environnement physique d'équilibrage des flux des messageries** : Surveillance du bon fonctionnement des équipements, sauvegarde des configurations pré et post modification, gestion des règles de sécurité, modifications des règles (illimitées), mise à jour des firmwares (si nécessaire), applications des correctifs (si nécessaire), modifications de paramètres, reporting mensuel.

Les prestations comprendraient les items suivants :

- intégration des équipements dans l'environnement de gestion de logs;
- création et paramétrage des parseurs spécifiques;
- définition des alertes;
- définition du reporting mensuel;
- choix du support pour la restitution des logs annuels.
- conservation des anciennes logs

Le titulaire prend en charge la collecte des logs et intègre les équipements non référencés pour la collecte

8.4 Tableaux de bord attendus

Le titulaire propose des copies d'écran de monitoring des éléments actifs. Les tableaux contiennent :

8.4.1 Tableau de bord Proxy

Les domaines les plus visités, les premiers « n » (*) utilisateurs/adresses IP par Hits, les premiers « n » utilisateurs/adresses IP par durée de session, les statistiques sur le statut de proxy, les types de fichiers, les moteurs de recherches, les mots clefs..., le pays, l'OS, le navigateur le plus visité...

(*) « n » = le nombre est défini par le bénéficiaire en lien avec le titulaire.

8.4.2 Tableau de bord de détection d'intrusion

Les premiers « n » messages triés par Hits, la destination d'alerte par niveau, la source d'attaque par niveau, les messages d'alertes par source, les messages d'alertes par destination, les premières attaques...

8.4.3 Tableau de bord des statistiques de site web/Url

Les informations générales sur le statut des pages web, les sources les plus actives triées par visite, les Hits par mois, par jour du mois, par heure..., les visites par mois, par jour du mois, par heure..., les informations sur les moteurs de recherche, les informations sur les référés, les informations sur les navigateurs, les informations sur les pays.

8.4.4 Tableau de bord du filtrage du contenu

Les informations générales sur les virus, les virus reçus et envoyés par jour, les informations générales sur les emails, les informations générales sur les spams, les virus entrants pour les adresses internes, les virus sortants pour les expéditeurs internes, le volume d'emails sortants par serveur SMTP...

8.4.5 Tableau de bord des statistiques VPN SSL

Les statistiques générales, le trafic par heure/par jour, les tentatives d'accès refusés, la durée des sessions,

etc...

8.4.6 Tableau de bord des statistiques sur les accès wifi

Les statistiques générales, le trafic par heure/par jour, les tentatives d'accès refusées, la durée des sessions, etc...

Des rapports mensuels au format PDF sont mis à disposition du bénéficiaire et reprennent les tableaux de bord susmentionnés.

8.5 Condition de sauvegarde et d'archivage des logs

Les données récoltées sont sauvegardées et archivées sur un support offrant une garantie de relecture supérieure. Les données stockées sont horodatées, signées, compressées, puis chiffrées via un algorithme de 128 bits.

Les données sont récoltées via la solution logicielle du bénéficiaire installée sur son Système d'Information (SI).

Le titulaire peut proposer un autre outil de collecte des logs. Cet outil sera installé par le titulaire (à ses frais) sur le site du bénéficiaire et il ne sera pas soumis à une licence d'exploitation. Le titulaire devra réaliser un transfert (à ses frais) de compétence au bénéficiaire

Les données sont collectées sur les serveurs du bénéficiaire sans transit intermédiaire par le titulaire.

Article 9 - POSTE 5 : Assistance au paramétrage des actifs réseaux

9.1 Nature du poste et Unité d'Œuvre

Le poste 5 est traité à prix forfaitaire annuel. Les UO sont déclinées de la manière suivante :

UO	Volume de crédit temps annuel
EXT CT HO	250 heures ouvrées

9.2 Objet et périmètre limitatif des prestations

L'objet de ce poste est de permettre au bénéficiaire de paramétrer ses éléments logiciels ou matériels non couverts par les prestations des postes 1 à 4.

9.3 Définitions

Est défini au sens du présent article :

- Le compte crédit temps est le compte du bénéficiaire cumulant l'ensemble des crédits temps à disposition du DDD pour des prestations de paramétrage sur le périmètre défini dans la cartographie du SI par le titulaire.
- Le paramétrage vise l'ensemble des prestations conduisant au paramétrage demandé par le bénéficiaire.
- 1 crédit temps (CT) correspond à une (1) heure de production intellectuelle pour la réalisation de paramétrages logiciels et/ou matériels.
- Le décompte de consommation est l'opération par laquelle le titulaire propose au bénéficiaire une consommation de CT en fonction des efforts nécessaires.
- Le solde du compte crédit temps correspond au nombre de crédit temps disponible.

9.4 Modalités d'exécution et de consommation des CT

Les prestations associées à ce poste permettent la réalisation de paramétrages logiciels ou matériels entrants dans le périmètre du marché et qui ne seraient pas couverts par les prestations associées.

Le compte crédit temps ne peut être négatif. Le titulaire peut refuser une demande de paramétrage si celle-ci conduit à un solde négatif.

À l'issue de la réalisation d'un paramétrage, le titulaire propose un « décompte de consommation » du « compte crédit temps ». À l'issue de la validation par le bénéficiaire du décompte de consommation, le titulaire fournit le solde du « compte crédit temps » sous 30 jours ouvrés.

Le titulaire fournit le solde du compte crédit temps à tout moment sur simple demande du bénéficiaire.

Tout crédit temps non consommé au titre de l'année « n » est reporté l'année « n+1 ».

Si le solde en fin de marché est positif (c'est-à-dire le nombre d'heures non consommées), alors ce solde du compte crédit temps est restitué financièrement par le titulaire au bénéficiaire au prorata Numéris de l'UO EXT CT HO du poste 5.

Article 10 - POSTE 6 : Assistance à l'exploitation du système réseau – Nouveau projet

10.1 Nature du poste et Unité d'Œuvre

Le poste 6 est traité à bons de commande. Les UO sont déclinées de la manière suivante :

Dénomination UO	Complexité	Effort associé
DEVNP-S-S	Simple	Simple
DEVNP-M-I	Intermédiaire	Intermédiaire
DEVNP-C-E	Complexe	Elevé

10.2 Objet des prestations

L'objet de ce poste est de permettre au bénéficiaire de faire évoluer son environnement tout en conservant les matériels en place.

10.3 Modalités d'exécution et d'estimation

10.3.1 Expression de besoin

Toute commande est précédée par l'établissement du devis associé au projet informatique, objet de la commande. Le devis permet de dimensionner le BDC sur la base des UO et au regard de la complexité de la prestation à exécuter. Le titulaire veille à la production systématique de ce devis préalable lorsque le bénéficiaire émet un besoin en lien avec ce poste.

Toute demande d'évolution spécifique ou « non programmée » fait l'objet d'une expression de besoin par le bénéficiaire.

10.3.2 Coordination des développements

Le titulaire désigne un responsable technique pour l'ensemble des prestations, il est l'interlocuteur principal du service informatique du bénéficiaire. Il assure la coordination des prestations relatives aux interventions sur site et à la mise à jour des documents techniques pendant toute la durée du présent

accord-cadre.

10.3.3 Étendue des prestations

Ces prestations de développement non programmées peuvent couvrir les évolutions suivantes :

- les évolutions fonctionnelles demandées par la maîtrise d'ouvrage qui nécessitent des développements sur l'application Agora portant sur les traitements et les données;
- les évolutions techniques comme le changement de version d'un composant logiciel système (Linux, Apache, Php, PostgreSQL,...) ou la migration vers un autre environnement technique.

Cette liste de prestations n'est pas exhaustive et peut être complétée par d'autres besoins de développement pouvant apparaître durant l'exécution de l'accord-cadre.

Chaque évolution/développement non programmé comprend :

- l'analyse et la rédaction éventuelle de spécifications techniques de l'opération de développement;
- la réalisation/le développement et les tests unitaires préalablement à l'envoi des documents numériques au bénéficiaire dans les locaux du titulaire;
- l'assistance à l'installation sur la plateforme de développement du maître d'ouvrage puis sur celle de production (avec les éventuels ajustements);
- l'assistance au démarrage et/ou le support téléphonique pour la mise en œuvre ou l'utilisation de la nouvelle fonctionnalité/évolution.

10.3.4. Livrables

Constituent des livrables dans le cadre du présent accord-cadre :

- les programmes créés ou modifiés ou le langage de commande modifié;
- les éléments relatifs au paramétrage et à la configuration de la nouvelle couverture fonctionnelle ou technique;
- la documentation technique d'exploitation ou d'assistance.

Le livrable est remis au plus tard dans un délai de cinq (5) jours ouvrés à partir de la fin du délai d'exécution du projet précisé sur le bon de commande (à défaut d'une telle précision, le délai d'exécution du projet est de deux [2] mois calendaires maximum) à compter de la notification du bon de commande. Les livrables d'une prestation intellectuelle doivent être fournis sous forme dématérialisée. Le titulaire doit privilégier les formats de fichiers relevant de normes internationales et sous chiffrage **Zed**.

10.3.5. Identification des éléments nécessaires à la réalisation de la/les prestations(s)

Avant le début d'une prestation et l'émission d'un bon de commande, le maître d'ouvrage prend contact avec le responsable technique du titulaire afin qu'ils définissent, d'un commun accord, la typologie des prestations en se référant aux niveaux de complexité et d'efforts définis dans le tableau ci-dessous.

Une prise de contact téléphonique ou une réunion sur site est planifiée à l'issue de l'intervention pour faire le point de la situation.

Trois (3) niveaux de complexité sont identifiés : **simple, intermédiaire, complexe**.

Simple	Une prestation simple correspond au besoin d'une compétence pour une intervention logicielle. Une intervention simple ne nécessite pas un pilotage au sens gestion de projet. (Exemple : mise à jour d'un service pack au niveau d'un équipement réseau). Un développement simple doit faire l'objet d'une proposition préalable qui précise le nom de l'intervenant, la date de réalisation et la durée de la prestation. Livrable :
---------------	--

	Après chaque intervention simple, un document d'intervention et d'exploitation lié à la prestation est délivré par l'intervenant
Intermédiaire	<p>Une prestation intermédiaire correspond au besoin de plusieurs compétences pour des interventions matérielles ou logicielles indépendantes les uns des autres. Une intervention intermédiaire ne nécessite pas un pilotage au sens gestion de projet. (Exemple : mise à jour d'un service pack au niveau d'un équipement réseau, modification du paramétrage de l'équipement pare-feu).</p> <p>Un développement doit faire l'objet d'une proposition préalable qui précise les noms des intervenants, la date de réalisation et la durée des prestations.</p> <p>Livrable : Après chaque intervention intermédiaire, un document d'intervention et d'exploitation lié aux différentes prestations est délivré par l'intervenant.</p>
Complexe	<p>Une prestation élevée correspond au besoin de plusieurs compétences pour des développements logiciels dépendant les uns des autres. Une intervention élevée nécessite un pilotage au sens gestion de projet. Une prestation élevée doit suivre un ordre chronologique précis. (Exemple : déploiement d'une solution wifi, déploiement d'un nouveau matériel de pare-feu qui nécessitent plusieurs compétences matérielles et logicielles)</p> <p>Un développement complexe doit faire l'objet d'une proposition préalable détaillée qui précise les noms des intervenants et du chef de projet, la date de réalisation et la durée du projet.</p> <p>Livrable : Après chaque intervention élevée, un document d'intervention et d'exploitation lié au projet est délivré par le chef de projet.</p>

Quatre (4) niveaux d'efforts indicatifs sont identifiés : **très simple, simple, intermédiaire, élevé** sous réserve des propositions complémentaires que le titulaire propose et quantifie dans son mémoire technique. Étant entendu que la combinaison des 3 niveaux de complexité et des 4 niveaux d'effort couvre l'ensemble des besoins de développement susceptible d'être commandé au titre du présent accord-cadre.

Très simple	L'effort indicatif associé à la tâche ne dépasse pas la journée pour l'ensemble de la réalisation, de la prise en charge de la demande et de sa mise en œuvre, jusqu'à la clôture de la demande client.
Simple	L'effort indicatif associé à la tâche ne dépasse pas cinq (5) jours à compter de la prise en charge de la demande et de sa mise en œuvre, jusqu'à la clôture de la demande client.
Intermédiaire	L'effort indicatif associé à la tâche ne dépasse pas dix (10) jours à compter de la prise en charge de la demande et de sa mise en œuvre, jusqu'à la clôture de la demande client.
Elevé	L'effort indicatif associé à la tâche ne dépasse pas vingt (20) jours à compter de la prise en charge de la demande et de sa mise en œuvre, jusqu'à la clôture de la demande client.

la combinaison des niveaux d'effort et de complexité permet de déterminer le type d'intervention et la charge de travail prévisible pour chaque prestation

Pour chaque commande le titulaire précise le niveau d'effort associé à la prestation retenue.

10.3.6. Délais de réalisation de l'opération

Les délais sont indiqués dans le devis du titulaire sous réserve de sa validation via l'émission d'un bon de commande émis par le bénéficiaire. Toutefois, le délai de démarrage des prestations ne doit pas dépasser 3 mois.

Le délai de fin de réalisation correspond à la date de réception des livrables.

Article 11 - POSTE 7 : Renouvellement des maintenances logicielles

11.1 Nature du poste et liste des UO

Le poste 7 concerne le renouvellement des maintenances logicielles des solutions de sécurités lises en place au sein des SI du Défenseur des droits, ainsi que la fourniture et l'installation de matériel de remplacement en cas de fin de vie des équipements existants.

Le titulaire fournit régulièrement au bénéficiaire les maintenances éditeurs des solutions mises en place au sein des SI du bénéficiaire (se reporter aux annexes du présent CCTP) :

- système de décryptage des flux SSL ;
- système de détection des menaces avancées ;
- système EDR.

Le titulaire s'assure que les comptes clients du bénéficiaire chez ces éditeurs sont à jour et accessibles par le bénéficiaire. Le bénéficiaire, à la notification du marché, fournira l'ensemble des échéances de ses supports en cours sur lesdites solutions.

Concernant la solution EDR actuellement en place et basée sur des machines virtuelles sous vmware, le titulaire peut proposer, pendant toute la durée de l'accord-cadre, une autre solution EDR complètement virtualisée en mode « on premise », c'est-à-dire en dehors de tout environnement cloud. Le nouvel EDR doit disposer des mêmes fonctionnalités que celui actuellement en place et apporter de nouvelles capacités qui améliorent le niveau de protection et de détection. Le coût financier ne doit pas excéder le coût actuellement en place au niveau du renouvellement des maintenances et de la partie MCO et MCS. Toute proposition de solution EDR alternative doit être accompagnée d'une étude comparative détaillée présentant les avantages de la nouvelle solution par rapport à la solution existante ainsi qu'une analyse du retour sur investissement.

Le poste 7 est traité à bons de commande. Les UO sont déclinées de la manière suivante :

Nommage UO	Contraintes techniques	Prestation/fourniture associée
MNT-EDT-SSL	Support éditeur un (1) an sur solution de décryptage des flux SSL	Installation des licences associées à la nouvelle maintenance logicielle
MNT-EDT-MAV	Support éditeur un (1) an sur solution système de détection des menaces avancées	Installation des licences associées à la nouvelle maintenance logicielle
MNT-EDT-EDR	support éditeur un (1) an sur solution système EDR	Installation des licences associées à la nouvelle maintenance logicielle
MNT-PAR-FEU (prog 129)	Support éditeur solution associée à la solution de pare feu	Installation des licences associées à la nouvelle maintenance logicielle
MNT-PORTAIL-VPN (prog 129)	Support éditeur solution associée à la solution de portail VPN	Installation des licences associées à la nouvelle maintenance logicielle
UO BTR-DTT	fourniture et installation d'un boîtier de remplacement pour la détection et blocage des	Installation matérielle et logicielle associée

	menaces avancées.	
UO BTR-DCY	fourniture et installation d'un boîtier de remplacement pour le décryptage des flux SSL	Installation matérielle et logicielle associée

11.2 Objet des prestations

L'objet de ce poste et des UO associées est de permettre au bénéficiaire d'étendre ou de remplacer les outils de détection et de protection contre les menaces informatiques avancées, ainsi que les outils de décryptage de flux SSL ; à l'issue de la fin de vie des matériels signalées par l'éditeur.

Cela permet de maintenir à jour les solutions de sécurité du bénéficiaire, tant sur le plan logiciel que matériel afin de garantir un niveau de protection optimal contre les menaces informatiques.

11.3 Fourniture et installation de matériel

Le titulaire fournit au bénéficiaire le même matériel (à l'identique) que celui indiqué dans l'annexe 2 au présent CCTP et l'installe dans les locaux du bénéficiaire.

Les UO correspondantes sont les suivantes :

- UO BTR-DTT : fourniture et installation d'un boîtier pour la détection et blocage des menaces avancées.
- UO BTR-DCY : fourniture et installation d'un boîtier pour le décryptage des flux SSL.

Le titulaire dispose d'un délai de deux (2) mois à compter de l'émission du bon de commande pour réaliser l'ensemble des opérations de livraison et d'installation du/des matériels commandés.

En cas de non-respect du délai de livraison et d'installation, le titulaire informe le bénéficiaire dans les plus brefs délais et propose un nouveau délai. Le titulaire se réserve le droit d'appliquer des pénalités de retard en cas de dépassement du délai initialement prévu.

11.4 Autre obligation

Le titulaire met à jour la cartographie du système d'information du bénéficiaire en fonction des commandes qui lui sont faites au titre de ce poste au plus tard lors de la prochaine mise à jour trimestrielle prévue au titre présent accord-cadre.

Article 12 - POSTE 8 : Réversibilité

12.1 Nature du poste et liste des UO

Ce poste, traité à bon de commande, correspond à une prestation de transfert de compétences et de données.

L'UO est désigné de la manière suivante :

- UO REV

12.2 Processus de réversibilité

Le titulaire précise dans le détail les moyens et le périmètre concerné pour la mise en place d'une réversibilité.

Il s'engage à fournir la description des applications qu'il a mis en place et le paramétrage associé.

Il s'engage à fournir la description et l'inventaire des matériels installés (version, IP, règle de routage,) et fournit les dernières sauvegardes de configurations des matériels et logiciels.

Il décrit les ressources en personnes (avec leurs qualifications) nécessaires à la transmission de cette réversibilité ainsi que la nombre de jours/heures de travail prévus pour chaque tâche.

12.3 Transfert de compétences et connaissances

Cette prestation a pour but d'organiser un transfert de connaissances du titulaire aux personnels du Défenseur des Droits. Cette prestation peut être demandée une seule, au terme du marché ou en cas de fin anticipée de celui-ci

12.4 Eléments en entrée

Le titulaire assure sur un temps imparti, qui ne pourra excéder trois (3) mois calendaires, une totale réversibilité concernant le transfert de gestion (routage sur l'Internet compris). Le titulaire s'engage à apporter toute l'assistance nécessaire à la bonne fin de cette opération. La prestation est assurée par les intervenants les plus qualifiés dans le domaine considéré.

La prestation de réversibilité comprend les activités suivantes :

- L'organisation de sessions de travail sur les domaines suivants :
 - l'architecture technique;
 - les environnements mis en œuvre;
 - la présentation détaillée de toute la documentation maintenue et la description de l'organisation de la documentation de référence;
 - l'état des lieux des difficultés particulières et des dossiers en cours;
 - le journal du traitement des incidents.
- L'assistance technique pendant une période permettant la prise en charge de la gestion des adresses IP par le Défenseur des Droits.
- Fourniture d'une documentation complète et à jour, incluant les manuels d'utilisation, les schémas techniques, et les procédures de maintenance

12.5 Actions

Réunion de lancement : à la commande de la prestation, une réunion de lancement permet de définir le calendrier détaillé de la prestation, les points de contact et les modalités de communication. Un compte rendu de cette réunion est établie et validé par les deux parties.

Plan de transfert : le titulaire soumet dans les délais convenus suivant la réunion de lancement, un plan de transfert détaillé, incluant :

- La méthodologie de transfert des connaissances, avec les étapes clés, les jalons et les critères d'évaluation
- L'identification des ressources (humaines et matérielles) affectées à la prestation
- Les modalités de transferts des données, incluant les formats, les procédures et les délais
- Les modalités de formation des équipes du Défenseur des droits, incluant le contenu, les supports et les modalités d'évaluation
-

Validation du plan de transfert : le titulaire met en œuvre le plan de transfert selon le calendrier et les modalités définies. Des réunions de suivi régulières sont organisées pour assurer le déroulement de la prestation

- Réception de la prestation : à l'issue de la prestation, le Défenseur des droits vérifie la conformité des livrables et la qualité du transfert de connaissances. Un procès-verbal de réception est établi et signé par les deux parties.

12.6 Obligation du titulaire

Le titulaire fournit au Défenseur des Droits les livrables suivants :

- le plan de transfert, présentant la méthodologie de transfert de connaissances ;
- les comptes rendus des réunions de transfert de connaissances faisant apparaître le contenu, les intervenants et les participants, la documentation support, les résultats d'évaluation ;
- l'intégralité de la documentation technique ;
- l'intégralité de la base de connaissance, à jour.

Le titulaire s'engage, après la réalisation de cette prestation, à ne plus conserver de données relatives à l'objet du marché. L'intégralité de ces données doit être supprimée des infrastructures du titulaire, y compris les sauvegardes.

Le titulaire remet au Défenseur des Droits l'ensemble des données de l'application. Ces données sont remises en version électronique dans un format compatible avec les outils utilisés par le Défenseur des Droits. Le titulaire est informé de l'outil utilisé par le DDD au moins quinze (15) jours avant la remise de ces données par le titulaire.

Article 13 - Liste des annexes

Annexe 1 : Architecture réseau du DDD ;

Annexe 2 : Liste des matériels et logiciels du SI DDD.

Article 14 - Dérogations au CCAG-TIC

Les dérogations au CCAG-TIC du présent document sont présentées dans le tableau récapitulatif ci-après :

Article du présent CCTP	Article du CCAG-TIC auquel il est fait dérogation
6.4.4.3	32.4