Cahier des clauses techniques particulières (CCTP)

Prestation d'infogérance Réseau, Sécurité & Surveillance Cyber Sécurité (SOC)

Table des matières

1 Objet du marché 6
1.1 Présentation du Pouvoir Adjudicateur 6
1.2 Gestion du Système d'Information 6
1.3 Objet 6
2 Présentation du Système d'Information 7
2.1 Datacenters 7
2.2 Architecture Réseau 7
2.2.1 Description 7
2.2.2 Schéma Réseau 8
2.3 Architecture Infrastructure 8
2.3.1 Description 8
2.3.2 Schéma d'Infrastructure 9
2.4 Inventaire et cartographie 9
2.4.1 Utilisateurs, identités et postes de travail 9
2.4.2 Matériel Réseau 9
2.4.3 Matériel d'Infrastructure 9
2.4.4 Cartographie applicative actuelle 9
2.4.5 Volumétrie tickets 11
3 Interlocuteurs du Pouvoir adjudicateur / l'acheteur 12
3.1 Référents contractuels et organisationnels 12
3.2 Référents techniques et opérationnels 12
3.3 Délégué à la protection des données 13
3.4 Direction des marchés 13
3.5 Mise à jour des interlocuteurs 13
4 Périmètre de la prestation 14
4.1 Périmètre inclus 14
4.2 Hors périmètre 14
4.3 Volumétrie contractuelle des tickets et priorisation 15
4.3.1 Tickets à traitement prioritaire 16

4.3.2 Suivi des volumes consommés et modalités de dépassement 16
4.4 Périmètre cible et évolutions prévues 17
4.5 Modalités d'évolution du périmètre 17
5 Prestations attendues 18
5.1 Phase d'initialisation de l'infogérance 18
5.1.1 Réseau et sécurité 18
5.1.2 SOC 18
5.2 Outillages 19
5.2.1 Outil(s) de ticketing 19
5.2.2 Outil(s) de supervision 19
5.2.3 Outil(s) SOC 20
5.3 Infogérance 23
5.3.1 Dispositions communes à l'ensemble du périmètre 23
5.3.2 Infogérance Réseau 26
5.3.3 Infogérance Sécurité 27
5.3.4 Infogérance SOC 30
5.3.5 Continuité d'activité (PCA/PRA) 40
5.3.6 Prestations complémentaires 41
6 Gouvernance et organisation 44
6.1 Organisation 44
6.1.1 Modalités d'intervention 44
6.1.2 Gestion et stockage de la documentation 45
6.1.3 Plages de services 45
6.1.4 Organisation opérationnelle de l'infogérance 46
6.1.5 Support et niveaux de prise en charge 47
6.1.6 Organisation des escalades 48
6.1.7 Référents opérationnels 49
6.1.8 Référent commercial 50
6.2 Processus et principes de gestion 51
6.2.1 Gestion de la supervision 51
6.2.2 Gestion des incidents 55
6.2.3 Gestion des demandes 61

6.2.4 Patch Management – Gestion des correctifs 66
6.2.5 Gestion de la documentation et de la connaissance 71
6.2.6 Amélioration continue 74
6.3 Gouvernance et pilotage 75
6.4 Instances de pilotage 75
6.4.1 Comité technique (COTECH) 75
6.4.2 Comité de pilotage (COPIL) 76
6.4.3 Comité stratégique (COSTRAT) 77
6.5 Modalités communes aux instances 78
6.6 Reporting et indicateurs 78
6.6.1 Météo quotidienne des services 78
6.6.2 Tableaux de bord et indicateurs de performance (KPI) 79
6.7 Phase d'initialisation 80
6.7.1 Organisation et ressources mobilisées 81
6.7.2 Reprise du périmètre Infogérance Réseau et Sécurité 82
6.7.3 Construction et mise en service du SOC 82
6.7.4 Gouvernance spécifique 84
6.7.5 Validation de la phase d'initialisation 85
6.8 Réversibilité 85
7 Engagements de service (SLA) 86
7.1 Définitions des différents délais 86
7.1.1 Délai de prise en charge 86
7.1.2 Délai de qualification 86
7.1.3 Délai de rétablissement 86
7.1.4 Délai de résolution 86
7.2 Niveaux et engagements de service (SLA) 87
7.2.1 Principes généraux 87
7.2.2 Mesure du rétablissement 87
7.2.3 SLA – Supervision 24/7 87
7.2.4 SLA – Gestion des incidents 88
7.2.5 SLA – Gestion des événements de sécurité par le SOC 88
7.2.6 SLA – Activités récurrentes du SOC 89

7.2.7 SLA – REX Incident 90
7.2.8 SLA – Gestion des demandes 90
7.2.9 SLA – Traitement des correctifs sécurité 92
7.2.10 SLA – Conformité des versions et maintenance préventive 93
7.2.11 SLA – Gouvernance et pilotage 93
7.2.12 SLA – Phase d'initialisation 95
7.2.13 Mesure de la performance globale 95
8 Exigences techniques et de sécurité 97
8.1 Exigences techniques générales 97
8.2 Exigences liées à l'utilisation l'IA 97
8.3 Exigences relatives aux services Cloud et aux données 99
8.4 Exigences de sécurité 99
8.4.1 Authentification et gestion des accès 100
8.4.2 Gestion des secrets et mots de passe 100
8.4.3 Environnement technique du Titulaire 101
8.4.4 Sécurité des sauvegardes 101
8.5 Exigences relatives aux sous-traitants 102
8.6 Conformité et réglementation 102
8.7 Confidentialité 103
9 Livrables attendus 104
9.1 Livrables contractuels pendant l'exécution du marché 104
9.1.1 Livrables de la phase d'initialisation 104
9.1.2 Livrables récurrents en phase d'exploitation 106
9.1.3 Livrables de réversibilité 108
10 Annexe : Sites 110
10.1 Hors périmètre 110

1 Objet du marché

1.1 Présentation du Pouvoir Adjudicateur

L'OPCO-SANTE est un opérateur de compétences du secteur privé de la santé qui a pour missions

- De contribuer au développement de l'emploi, des compétences, des qualifications et des parcours professionnels.
- D'accompagner les transformations sectorielles, les enjeux emploi-formation des métiers du soin et de l'accompagnement.
- De répondre aux besoins de ses adhérents qui, malgré des activités et des publics différents, partagent des enjeux communs.

Les locaux d'OPCO-SANTE sont répartis sur **21 sites** (Siège à Levallois et 20 sites en régions) regroupant **450 collaborateurs.**

1.2 Gestion du Système d'Information

La DOSI (Direction de l'Organisation et du Système d'Information) de l'OPCO-SANTE et plus particulièrement en son sein le Service Système d'Information, basé au siège de Levallois, est responsable de la gestion du Système d'Information.

Les équipes internes du service des systèmes d'information sont notamment assistées dans leurs missions par :

- Un prestataire chargé de l'infogérance des infrastructures et des systèmes ;
- Un prestataire chargé de l'infogérance du réseau et de la sécurité, objet du présent marché.

Le titulaire devra collaborer avec les équipes de l'OPCO-SANTE et les autres prestataires intervenant sur le système d'information, dans les limites des responsabilités définies par le marché.

1.3 Objet

Le marché a pour objet la fourniture de prestations d'infogérance, de maintien en condition opérationnelle et de sécurité des infrastructures réseau et des composants de sécurité.

Il comprend également la mise en place et l'exploitation d'un service de surveillance et de réponse aux incidents de cybersécurité de type SOC managé.

Les prestations couvrent notamment la supervision, l'administration, le support, le traitement des incidents et des demandes, la gestion des changements, le conseil, l'accompagnement des évolutions, ainsi que les prestations de transition et de réversibilité.

2 Présentation du Système d'Information

Les éléments présentés dans le présent chapitre ne relèvent pas nécessairement de l'administration du Titulaire. Ils sont décrits afin de lui permettre de comprendre l'environnement technique et les interdépendances avec son périmètre.

2.1 Datacenters

L'hébergement du Système d'Information est confié à un prestataire privé, responsable de la fourniture des services suivants :

- Hébergement de 2 baies informatiques dédiées reparties sur 2 datacenters (principal et secours)
- Interconnexion entre les 2 datacenters
- Accès internet haut débit

Les sites d'OPCO-SANTE sont constitués de 3 sites principaux (Levallois, Malakoff et Marseille) et 18 sites régionaux.

2.2 Architecture Réseau

2.2.1 Description

2.2.1.1 Datacenters

L'infrastructure réseau des datacenters repose sur 2 environnements, Production et secours (PRA), d'architecture identique. Chaque environnement est composé des éléments suivants :

- **3 clusters de switches**, chacun dédié à une fonction :
  - le **cluster LAN**, qui dessert le réseau interne et les VMs du périmètre LAN ;
  - le **cluster DMZ**, qui dessert les VMs exposées en zone démilitarisée ;
  - le **cluster d'interconnexion (interco)**, qui dessert l'accès au stockage partagé pour les clusters ESXi (via la technologie iSCSI) et assure l'interconnexion entre les deux datacenters ;
- **1 cluster de 2 firewalls**, réparti sur les deux sites (un nœud sur le site principal, le second sur le site de secours) ;
- **1 switch standalone**, qui dessert les réseaux de management.

La fonction de routage inter-VLAN est assurée par le firewall, à l'exception des flux vers les baies de stockage de Production et de Backup, qui transitent directement par le cluster d'interconnexion.

Les deux datacenters sont reliés entre eux par des liens d'interconnexion dédiés, supportant notamment les flux de réplication entre le site de Production et le site de PRA.

L'OPCO-SANTE dispose également d'un **datacenter dans le cloud Microsoft Azure**, hébergeant une cinquantaine (50) VMs VDI ainsi que des services Azure Kubernetes Service

(AKS). Ce dernier est interconnecté aux datacenters via un VPN IPSec reposant sur un firewall virtuel Palo Alto.

2.2.1.2 Sites OPCO

Chaque site est disposé baie informatique qui héberge un cluster de switches réseau, un firewall et d'un onduleur. Les 3 sites principaux (critiques) sont équipés d'un accès internet (FTTO) redondé et les 18 sites régionaux sont équipés d'un accès internet (FTTO) non redondé, d'une baie informatique qui héberge 2 switches réseau, d'un firewall et d'un onduleur.

Chacun de ces sites est interconnecté aux datacenters à travers un VPN IPSec.

Le site de **Levallois constitue le siège** de l'OPCO-SANTE. Il est réparti sur **2 bâtiments** :

- le **bâtiment 1**, comprenant 9 étages ;
- le **bâtiment 2**, comprenant un rez-de-chaussée et un étage.

Chaque bâtiment est équipé de son propre **cœur de réseau**, auquel sont raccordés les **switches de distribution** répartis dans les étages.

2.2.2 Schéma Réseau

« Se référer aux documents annexés au présent CCTP. »

2.3 Architecture Infrastructure

2.3.1 Description

L'infrastructure système repose sur 2 environnements, Production et PRA, d'architecture identique. Chaque environnement est composé des éléments suivants :

- **2 clusters de calcul ESXi** :
  - un cluster **LAN** de 5 hôtes ESXi, hébergeant les VMs du LAN ;
  - un cluster **DMZ** de 3 hôtes ESXi, hébergeant les VMs de la DMZ ;
- **1 baie de stockage de Production**, partagée par les deux clusters ESXi ;
- **1 serveur et 1 baie de stockage de Backup**, dédiés à la sauvegarde.

L'accès des clusters ESXi au stockage partagé (Production et Backup) est assuré via la technologie iSCSI, portée par le cluster d'interconnexion réseau décrit au paragraphe « Architecture Réseau ».

La sauvegarde et la réplication sont assurées par la technologie Veeam, hébergée sur un serveur dédié, lui-même interconnecté aux clusters ESXi de Production et de DMZ via les switches d'interconnexion. Ce dispositif assure 2 fonctions :

- la sauvegarde, stockée sur la baie de Backup dédiée au serveur Veeam ;
- la réplication asynchrone de l'infrastructure VMware et du plan de sauvegarde vers le site de PRA.

2.3.2 Schéma d'Infrastructure

« Se référer aux documents annexés au présent CCTP. »

2.4 Inventaire et cartographie

Les quantités présentées ci-dessous constituent la configuration de référence retenue pour le dimensionnement et le chiffrage des prestations à la date de lancement de la consultation. Elles sont susceptibles d'évoluer pendant l'exécution du marché selon les modalités prévues au chapitre relatif à l'évolution du périmètre.

2.4.1 Utilisateurs, identités et postes de travail

Quantité	Élément
550	Comptes utilisateurs, BAL Microsoft 365
450	Postes de travail
160	Terminaux mobiles
2	1 Entra Internal ID /1 Identités externes (Azure B2C)
25	Salles Visio-conférence

2.4.2 Matériel Réseau

Quantité	Matériel Réseau
27	Firewall (2 DC, 1 Azure, 2 Levallois, 2 Malakoff, 20 Régions (dont 2 à Marseille)
14	Switch de Datacenter (7 par DC)
8	Switch cœur de réseau
53	Switch d'accès (tous sites confondus)
2	Lien d'interconnexion entre Datacenters
4	Accès internet datacenter (2 par DC)
25	Accès internet FTTO : 3 Levallois, 2 Malakoff, 20 Régions (dont 2 à Marseille)
25	Tunnel VPN IPESEC
1	Tenant Contrôleur Wi-Fi en SaaS
120	Bornes Wi-Fi (40 Siège / 78 Régions)
1	Instance/tenant EDR en SaaS
1	Instance/tenant Anti-spam en SaaS
1	Cluster Reserve-Poxy/WAF
1	4 VM : 1 Cluster Bastion et 1 Cluster access manager
1	PKI Serveur
1	Instance/Tenant Azure interconnecter via VPN IPsec aux datacenters

2.4.3 Matériel d'Infrastructure

Quantité	Élément
16	ESXi (8 par DC)
2	Baies de stockage PROD (1 par DC)
2	Serveurs de sauvegardes (BACKUP) (1 par DC)
2	Baies de stockage sauvegardes (BACKUP) (1 par DC)
250	VMs (70 % Windows/ 30% Linux)

2.4.4 Cartographie applicative actuelle

Les services applicatifs sont listés dans le tableau suivant :

Application	Description / Technologie	Hébergement/Exposition	Responsable/ Gestionnaire
SI Finance	SAGE / ILuccca	SaaS / externe	Intégrateur
SI RH	Quarksup / Kelio	SaaS / externe	Intégrateur
ERP	SIRUS (développé en interne OPCO)	On-premise / Interne	OPCO
CRM	EDEAL	On-premise / Interne	Intégrateur
SGBD	Microsoft SQL Server / Postgres	On-premise / Interne	OPCO
Sauvegarde O365	Carbonite	SaaS / externe	OPCO
Sauvegarde VM	Veeam	On-premises / Interne	Infogérant
Annuaire et gestion identités internes	MS Active directory/Microsoft Entra ID	On-premises / Interne SaaS / externe	Infogérant
Annuaire et gestion identités externes	Azure B2C	SaaS / externe	OPCO
Infrastructure de gestion des certificats / PKI	PKI Microsoft / Services de certificats Active Directory (AD CS)	On-premise / Interne	Infogérant
Authentification réseau / Service RADIUS	Microsoft Windows Server – Service RADIUS	On-premise / Interne	Infogérant
Gestion des Devices (PC , mobile)	Microsoft Intune Autopilote	SaaS / externe	
Bastion d'administration / PAM	WALLIX Bastion	On-premise / Interne	OPCO
Partage de Fichier	Système de partage Windows / SharePoint Online	On-premise / Interne SaaS / externe	Infogérant
Protection postes et serveurs (EDR)	Sentinel One	SaaS / externe	Infogérant
Outils collaboratifs (Word, Excel, etc …)	Microsoft 365 (E5)	SaaS / externe	Infogérant
Messagerie	Microsoft 365 Exchange online	SaaS / externe	Infogérant
Téléphonie	Softphone sur Teams / Direct connect Bouygtelecom	SaaS / externe	Infogérant
Infrastructure Wi-Fi – Siège	Cisco Meraki / Portail captif Weblib	SaaS / externe	OPCO
Infrastructure Wi-Fi – Régions	Extrême Cloud IQ	SaaS / externe	Infogérant
Pare-feu / VPN	Palo Alto Networks / GlobalProtect	On-premise / Interne	Infogérant
Reverse Proxy / Publication applicative	KEMP LoadMaster	On-premise / Interne	Infogérant
Sécurité de la messagerie / Anti-spam	Mimecast	On-premise / Interne	Infogérant
Filtrage/sécurisation navigation Web	Cisco Umbrella	SaaS / externe	Infogérant
Middleware : API Management / Intégration applicative	Axway API Management / Axway Fusion	On-premise / Interne	OPCO
Authentification multifacteur (MFA)	TrustBuilder	SaaS / Externe	Infogérant
Prise en main à distance	BeyondTrust Remote Support	SaaS / Externe	Infogérant
ITSM / Gestion des services IT	ServiceNow / Jira	SaaS / Externe	OPCO

Application	Description / Technologie	Hébergement/Exposition	Responsable/ Gestionnaire
BI / Analyse de données	Microsoft SQL Server Integration Services (SSIS) / SQL Server Analysis Services (SSAS)	On-premise / Interne	Infogérant
MDM / Data Management	TIBCO EBX	On-premise / Interne	Infogérant
Système de Visio	Cisco Webex control Hub	On-premise / Interne	OPCO
Services Azure	DEVOPS / AKS	SaaS / Externe	OPCO

2.4.5 Volumétrie tickets

Ces données sont communiquées à titre indicatif sur la base de l'activité constatée en 2025. Elles ne constituent pas un engagement de volumétrie pour la durée du marché.

Répartition des tickets par catégorie

Trimestre	Incidents	Demandes	Total
T1	17	20	**37**
T2	18	20	**38**
T3	33	30	**63**
T4	30	13	**43**
TOTAL	**98**	**83**	**181**
Total %	**54 %**	**46 %**	

Répartition des tickets par niveaux de priorité

Priorité	Répartition annuelle
P1	**2 %**
P2	**8 %**
P3	**90 %**

Disponibilité de l'infrastructure constatée (sur les 12 derniers mois)

Périmètre d'infrastructure	Taux de disponibilité annuel
Equipements Siège	**99,78 %**
Equipement Sites régionaux	**99,17 %**
Equipements Datacenter	**99,97 %**
Périmètre d'infrastructure	**Taux de disponibilité annuel**
Équipements sous astreinte	**99,92 %**
Pare-feux	**98,76 %**

3 Interlocuteurs du Pouvoir adjudicateur / l'acheteur

3.1 Référents contractuels et organisationnels

Le Responsable du Système d'Information et le Responsable du Pôle Infrastructure sont les principaux interlocuteurs du Titulaire pour le pilotage de la prestation.

Ils assurent notamment :

- le suivi de la bonne exécution des prestations ;
- le pilotage de la relation avec le Titulaire ;
- la validation des orientations opérationnelles ;
- l'arbitrage des priorités ;
- le suivi des engagements contractuels et des niveaux de service ;
- la validation des livrables, plans d'action et comptes rendus ;
- le traitement des difficultés nécessitant une décision de l'acheteur.

Les personnes nominativement désignées ainsi que leurs coordonnées sont communiquées au Titulaire au démarrage des prestations et tenues à jour pendant toute la durée du marché.

3.2 Référents techniques et opérationnels

Sous l'autorité du Responsable du Pôle Infrastructure, le Responsable de Production, le Responsable d'Exploitation ainsi que leurs équipes constituent les principaux interlocuteurs techniques et opérationnels du Titulaire.

Ils participent notamment :

- au suivi quotidien des prestations ;
- à la qualification et à la priorisation des incidents, demandes et changements ;
- à la transmission des informations techniques nécessaires ;
- à l'analyse des incidents et problèmes ;
- au suivi des actions correctives ;
- à la vérification technique des prestations et livrables ;
- à la coordination avec les autres équipes et prestataires intervenant sur le système d'information.

Les échanges avec les référents techniques et opérationnels ne peuvent avoir pour effet de modifier le périmètre, les prix, les délais contractuels ou les autres obligations du marché sans validation préalable selon les modalités prévues par les pièces contractuelles.

3.3 Délégué à la protection des données

L'OPCO-SANTE dispose d'un Délégué à la protection des données, susceptible d'être associé aux sujets concernant la protection des données à caractère personnel.

Le Titulaire coopère avec les interlocuteurs désignés par l'OPCO-SANTE et leur communique les informations nécessaires à la vérification du respect des obligations relatives à la protection des données.

Les obligations applicables au Titulaire en matière de protection des données sont définies dans les pièces administratives du marché et, le cas échéant, dans l'annexe relative à la protection des données à caractère personnel.

Toute évolution susceptible de modifier les obligations contractuelles du Titulaire ou les conditions de traitement des données est mise en œuvre conformément aux modalités prévues par le marché.

3.4 Direction des marchés

La Direction des marchés intervient dans le suivi administratif et contractuel du marché.

Elle est notamment associée :

- aux difficultés susceptibles d'engager la responsabilité contractuelle du Titulaire ;
- au suivi des manquements et à la mise en œuvre des leviers contractuels ;
- aux évolutions du périmètre ayant une incidence juridique ou financière ;
- à l'interprétation et à la modification des pièces contractuelles ;
- à la mise en œuvre des procédures administratives prévues par le marché.

Toute demande susceptible de modifier le périmètre des prestations, les prix, les délais ou les autres obligations contractuelles doit être formalisée et validée conformément aux dispositions du marché.

3.5 Mise à jour des interlocuteurs

Chaque partie informe l'autre, dans les meilleurs délais, de tout changement concernant ses interlocuteurs contractuels, organisationnels, techniques ou opérationnels.

La modification des personnes nominativement désignées ne constitue pas une modification du marché dès lors qu'elle n'affecte pas la répartition contractuelle des responsabilités.

4 Périmètre de la prestation

4.1 Périmètre inclus

Le périmètre technique de la prestation couvre les composants du système d'information décrits au chapitre : ***2.4 Inventaire et cartographie***. Le niveau d'expertise attendu du Titulaire est précisé ci-dessous. Les modalités d'exploitation associées (MCO, MCS, supervision, traitement des demandes) sont détaillées au chapitre : ***5.3 Infogérance***.

N1, N2 et expertise N3 obligatoire

- LAN Bureaux
- Wi-Fi Bureaux
- LAN datacenters et accès distants (VPN IPsec)
- Sécurité périmétrique et VPN client (pare-feu, VPN)
- Exposition sécurisée des services (FW, reverse proxy, WAF)
- Service d'authentification réseau RADIUS
- Landing Zone Azure
- Gestion opérationnelle des certificats publics et PKI interne
- Protection de la messagerie (Antispam)
- Administration de la solution EDR / XDR
- SIEM (collecte, corrélation, rétention des journaux)
- Détection et réponse SOC (surveillance de sécurité, CSIRT)

N1, N2 obligatoires et expertise N3 souhaitée

- Accès Internet des sites
- Accès Internet des datacenters
- Filtrage de la navigation Web
- Authentification multi facteurs (MFA)
- Administration de la solution de gestion des accès à privilèges (PAM / bastion)
- Détection et suivi des vulnérabilités
- Surveillance de la surface d'attaque interne et externe
- Surveillance du dark web

4.2 Hors périmètre

Les éléments listés ci-dessous ne sont pas compris dans le périmètre :

- La gestion de l'infrastructure système
- La gestion des postes de travail
- La fourniture des accès internet

4.3 Volumétrie contractuelle des tickets et priorisation

La volumétrie historique présentée au chapitre : ***2.4.5 Volumétrie tickets*** relatif à l'existant constitue une donnée de référence permettant aux candidats d'apprécier le niveau d'activité actuellement constaté sur le périmètre Réseau et Sécurité.

Pour les besoins du dimensionnement et du chiffrage de la prestation, le Pouvoir adjudicateur retient la volumétrie contractuelle de référence suivante.

Ces volumes correspondent à la capacité de traitement incluse dans le forfait et ne constituent pas un objectif de consommation.

Infogérance Réseau et Sécurité

Nature du ticket	**Volumétrie mensuelle de référence**	**Volumétrie trimestrielle incluse**
Incidents	20	60
Demandes / changement	10	30
Total	**30**	**90**

SOC

Nature du ticket	**Volumétrie mensuelle de référence**	**Volumétrie trimestrielle incluse**
Incidents	20	60
Demandes (investigations) / changement	10	30
Total	**30**	**90**

Le Pouvoir adjudicateur ne disposant pas actuellement d'un SOC opérationnel, aucune volumétrie historique représentative ne peut être communiquée pour cette activité.

Afin de disposer d'une base commune pour le dimensionnement et la comparaison des offres, le Pouvoir adjudicateur retient une hypothèse de **Trente (30) tickets SOC par mois**.

Cette volumétrie ne correspond pas au nombre d'alertes ou d'événements de sécurité générés par les outils de détection et de supervision, dont l'analyse et le traitement courant sont intégrés au fonctionnement normal du SOC. Elle correspond aux tickets déclaratifs nécessitant une prise en charge individualisée dans le cadre des processus de gestion des incidents ou des demandes.

Si le candidat estime, au regard du périmètre à superviser, des sources de données, des cas d'usage proposés, du modèle opérationnel retenu ou de son retour d'expérience, que cette hypothèse de volumétrie n'est pas adaptée au besoin, il pourra proposer dans son mémoire technique une volumétrie différente.

Toute proposition d'ajustement devra être clairement identifiée et justifiée. Le candidat précisera notamment :

- la volumétrie qu'il estime nécessaire ;
- les hypothèses techniques et opérationnelles retenues ;
- les éléments conduisant à l'ajustement proposé ;
- l'incidence éventuelle sur le dimensionnement des ressources ;
- l'incidence éventuelle sur le forfait proposé et sur les prix unitaires du BPU.

La volumétrie du SOC sera réexaminée et, le cas échéant, ajustée au cours de la phase d'initialisation, notamment au regard du périmètre effectivement supervisé, des sources intégrées, des cas d'usage mis en œuvre et des premières données d'activité disponibles.

4.3.1 Tickets à traitement prioritaire

En complément des règles habituelles de qualification et de priorisation, le Pouvoir adjudicateur pourra désigner jusqu'à **quinze (15) tickets par année contractuelle**, qu'il s'agisse d'incidents ou de demandes, comme devant faire l'objet d'un traitement prioritaire.

Cette faculté permet au Pouvoir adjudicateur de demander l'accélération ponctuelle du traitement d'un ticket présentant un enjeu opérationnel particulier, indépendamment de son niveau de priorité initial.

Les modalités de notification, de prise en compte, de suivi et de comptabilisation de ces tickets prioritaires seront définies et convenues entre le Titulaire et le Pouvoir adjudicateur au cours de la phase d'initialisation.

4.3.2 Suivi des volumes consommés et modalités de dépassement

Les volumes mensuels définis au présent CCTP constituent des références de dimensionnement. Leur consommation et les éventuels dépassements sont appréciés sur une base trimestrielle. En conséquence, un dépassement ponctuel constaté sur un mois donné n'entraîne pas, à lui seul, de facturation complémentaire dès lors que la volumétrie trimestrielle contractuelle correspondante n'est pas dépassée.

À la fin de chaque trimestre, le Titulaire présentera au COPIL un état consolidé des volumes réellement consommés pour chacune des catégories de tickets.

Après validation du dépassement par le Pouvoir adjudicateur, les volumes excédentaires feront l'objet d'une facturation complémentaire sur la base des prix unitaires correspondants prévus au Bordereau des Prix Unitaires (BPU).

Aucune facturation complémentaire liée à un dépassement de volumétrie ne pourra être appliquée sans présentation des éléments justificatifs et validation préalable du dépassement par le Pouvoir adjudicateur.

4.4 Périmètre cible et évolutions prévues

Dans la continuité d'un projet de modernisation du réseau et du Wi-Fi entamé en 2026, le déploiement et l'intégration des switches et des bornes Wi-Fi de nos sites régionaux sont à planifier en 2027.

Compte tenu des échéances relatives aux fins de support à venir sur une partie des pare-feux Palo Alto, le remplacement des pare-feux de 2 sites majeurs est à planifier en 2029.

D'autres projets potentiels sont encore à l'étude et pourraient faire évoluer le périmètre. Les sujets identifiés (liste non exhaustive) sont les suivants :

- Remplacement de l'EDR par un XDR
- Remplacement du Reverse Proxy par une solution leader du marché
- Évolution de la solution MFA vers une plateforme de fédération des identités / Identity Broker, permettant de centraliser les mécanismes de MFA et de SSO et d'assurer l'interopérabilité avec plusieurs fournisseurs d'identité (IdP), notamment Microsoft Entra ID / Entra External ID (Azure B2C) et des IdP tiers

Les projets et évolutions mentionnés ci-dessus sont présentés à titre indicatif et ne constituent pas un engagement quant à leur réalisation, leur calendrier ou leur périmètre. Leur mise en œuvre éventuelle sera conditionnée aux arbitrages techniques, budgétaires et organisationnels à venir et pourra, le cas échéant, conduire à une évolution du périmètre de la prestation dans les conditions prévues au marché.

4.5 Modalités d'évolution du périmètre

Tout changement (augmentation ou réduction) des besoins de l'OPCO-SANTE fera l'objet d'une étude d'impact par le prestataire.

Si cette étude induit des coûts supplémentaires (nécessité pour le prestataire d'allouer des ressources supplémentaires), le prestataire adressera un devis argumenté à l'OPCO-SANTE et les conséquences éventuelles seront traitées, soit par avenant, soit au travers des prix présents dans l'annexe financière du marché.

Si au contraire cette étude induit une réduction des coûts, la mise à jour se traitera, soit par avenant, soit au travers des prix présents dans l'annexe financière du marché.

L'instance chargée de la gestion et de la validation des changements ayant un impact sur le contrat est le comité de pilotage tel que décrit dans le chapitre : ***6.3.1 Instances de pilotage***

Une instance spécifique pourra être mise en place si les délais le justifient.

Chaque changement de périmètre donnera lieux lorsque pertinent, à une analyse et une révision du catalogue de services et la volumétrie mensuelle des tickets (incidents et demandes). **Le catalogue de services pourra être amené à évoluer durant le marché avec l'accord des deux parties.**

5 Prestations attendues

5.1 Phase d'initialisation de l'infogérance

Une phase d'initialisation est prévue préalablement au passage en exploitation des prestations.

Le Titulaire met en œuvre les ressources et le pilotage nécessaires à la bonne exécution de cette phase, conformément aux dispositions définies au chapitre : **Gouvernance et organisation / Phase d'initialisation**.

5.1.1 Réseau et sécurité

Les prestations d'infogérance Réseau et Sécurité étant déjà assurées avant le démarrage du présent marché, cette phase consiste principalement en une **reprise de l'existant, avec actualisation du périmètre et un transfert de responsabilité vers le Titulaire**.

Le Pouvoir adjudicateur met à disposition la documentation existante nécessaire à cette reprise, notamment les DAT, DEX, inventaires, procédures et éléments disponibles relatifs aux différents domaines.

La phase d'initialisation comprend notamment :

- la prise de connaissance et la validation du périmètre technique et documentaire ;
- la mise en place des moyens d'accès et d'interconnexion nécessaires à l'exploitation ;
- la mise en œuvre et le paramétrage des outils nécessaires à la prestation, notamment le ticketing et la supervision ;
- la reprise ou la constitution de l'inventaire du périmètre infogéré ;
- la reprise, l'adaptation ou la création des procédures et documentations nécessaires à l'exploitation ;
- la mise en place des indicateurs, rapports et tableaux de bord attendus ;
- la préparation et la validation des modalités opérationnelles nécessaires au passage en exploitation.

Les modalités détaillées d'organisation, de gouvernance, de gestion des incidents, demandes, changements et escalades sont définies dans les chapitres correspondants du présent CCTP et sont déclinées opérationnellement au cours de cette phase.

5.1.2 SOC

Le Pouvoir adjudicateur ne disposant pas actuellement d'un SOC, la phase d'initialisation comprend la conception, la construction, l'intégration et la mise en service du dispositif SOC.

Elle comprend notamment la définition et la validation de l'architecture technique cible, la confirmation du dimensionnement des outils et services associés, ainsi que leur déploiement, leur paramétrage et leur intégration au Système d'Information.

Le dispositif SOC s'appuie notamment sur une solution SIEM proposée par le titulaire dans son offre et destinée à être souscrite, acquise et détenue par le Pouvoir adjudicateur.

Les exigences et travaux attendus pour la construction et la mise en service du SOC sont détaillés au chapitre « Gouvernance et organisation / Phase d'initialisation ».

5.2 Outillages

Outre les prestations d'infogérance, le présent marché comprend la fourniture par le Titulaire des outillages nécessaires à la réalisation et à l'exploitation des services attendus, notamment :

5.2.1 Outil(s) de ticketing

Le titulaire devra mettre à disposition de l'OPCO-SANTE l'outil de ticketing qui sera utilisé pour supporter la prestation. Cet outil intègrera la base de connaissances ou sera connecté avec celle-ci.

Toutes les informations dans cet outil (traçabilité des incidents et demandes incluant les résolutions, base de connaissances) doivent être sécurisées, accessibles, exploitables et exportables en cas de besoin.

Le contenu de la base de connaissances appartient à l'OPCO-SANTE et devra être accessible aux équipes du Titulaire et de l'OPCO-SANTE durant le marché.

5.2.2 Outil(s) de supervision

Le Titulaire devra mettre en place et paramétrer un ou des outil(s) de supervision pertinent(s) fourni(s) par ses soins afin de surveiller les composants du périmètre technique.

Le Titulaire aura la charge de paramétrer les seuils convenus avec l'OPCO-SANTE issus de l'infogérance précédente le cas échant, durant la phase d'initialisation.

Le Titulaire devra fournir un compte d'accès à cet(s) outil(s) pour l'OPCO-SANTE.

Le Titulaire assure la surveillance permanente des outils de supervision et garantit la continuité du dispositif de supervision pendant toute la durée du marché.

Le dispositif de supervision étant nécessaire à la fourniture du service 24/7, le Titulaire assure la surveillance de son propre fonctionnement.

Indisponibilité du dispositif de supervision

Toute indisponibilité totale ou partielle du dispositif de supervision susceptible d'entraîner une perte de visibilité sur un service fait l'objet d'une prise en charge immédiate.

Le Titulaire met en œuvre les mesures nécessaires afin de détecter toute perte de supervision, notamment :

- perte de communication avec un équipement ;
- absence anormale de remontée de métriques ;
- défaillance d'un collecteur ;
- dysfonctionnement d'une sonde ;

- interruption d'un flux de supervision ;
- indisponibilité de la plateforme de supervision.

Le Titulaire définit les procédures permettant de maintenir un niveau de surveillance adapté pendant l'indisponibilité et la communication vers le Pouvoir Adjudicateur.

Maintenance et évolution de la supervision

Le Titulaire assure le maintien en condition opérationnelle du dispositif de supervision relevant de son périmètre. Il assure notamment :

- la maintenance des outils ;
- le maintien des agents et sondes ;
- la gestion des configurations ;
- la mise à jour des règles de supervision ;
- l'adaptation des seuils ;
- l'intégration des nouveaux composants ;
- la suppression des composants décommissionnés ;
- le maintien des tableaux de bord ;
- la vérification périodique du bon fonctionnement des contrôles.

Le Titulaire est force de proposition concernant toute évolution permettant d'améliorer la couverture, la pertinence ou l'efficacité de la supervision.

5.2.3 Outil(s) SOC

En complément des outils nécessaires aux prestations d'infogérance indiqués ci-dessus, Le Titulaire assure la fourniture, le déploiement, le paramétrage, et le cas échéant, le maintien en conditions opérationnelles de l'ensemble des outils nécessaires à la réalisation de sa prestation SOC, sauf lorsque certains outils sont explicitement fournis ou mis à disposition par le Pouvoir adjudicateur.

Le Titulaire doit proposer une chaîne d'outillage cohérente avec les prestations attendues, le périmètre supervisé, les engagements de service et l'organisation opérationnelle de son SOC.

À ce titre, il précise dans sa réponse l'ensemble des outils nécessaires au fonctionnement du service et identifie clairement, pour chacun d'eux :

- sa fonction dans le dispositif SOC ;
- son mode de fourniture ;
- son mode d'hébergement ;
- son propriétaire ;
- les responsabilités respectives du Titulaire et du Pouvoir adjudicateur en matière d'administration, d'exploitation, de maintenance et de support ;
- les éventuelles dépendances techniques avec d'autres composants du Système d'Information ;
- les coûts inclus dans la prestation et, le cas échéant, ceux nécessitant une acquisition ou une souscription complémentaire.

5.2.3.1 Cas particulier du SIEM et exigences relatives

Le SIEM constitue un composant structurant du dispositif SOC. Le titulaire aura proposé dans sa réponse une solution SIEM répondant aux besoins et exigences du présent CCTP. Cette solution est destinée à être souscrite ou acquise pour le compte du Pouvoir Adjudicateur et ne doit pas dépendre du maintien du contrat SOC avec le Titulaire pour permettre la conservation des données et la continuité de son exploitation.

Le Titulaire précise notamment :

- la solution et l'éditeur proposés ;
- l'architecture et le mode d'hébergement ;
- le modèle de licence ou de souscription ;
- les modalités d'acquisition ou de souscription ;
- les capacités d'intégration avec le Système d'Information ;
- les hypothèses de dimensionnement ;
- les modalités de conservation et d'archivage ;
- les conditions de sécurité, de localisation des données et de réversibilité ;
- le coût de la solution selon les modalités prévues dans les pièces financières.

Le Titulaire engage son offre sur une solution SIEM déterminée. La phase d'initialisation permet d'en confirmer le dimensionnement et les modalités détaillées de mise en œuvre.

La solution doit permettre d'assurer les fonctions nécessaires au SOC, notamment la collecte, la centralisation, la normalisation, l'enrichissement, la corrélation, la recherche, la détection, l'investigation et la conservation des événements de sécurité.

Elle doit permettre l'intégration de sources hétérogènes issues notamment des environnements on-premise, Cloud et SaaS du Pouvoir adjudicateur.

Intégration des sources

La solution SIEM doit permettre l'intégration de sources de données hétérogènes, y compris de sources spécifiques ne disposant pas d'un connecteur natif.

Elle doit permettre la mise en œuvre de mécanismes d'intégration adaptés, notamment au moyen de connecteurs, API, agents, collecteurs, parseurs ou mécanismes équivalents.

Le candidat précise dans son offre, au regard des sources identifiées dans le présent CCTP :

- le taux de couverture assuré par des connecteurs ou intégrations disponibles nativement ;
- les sources nécessitant une intégration ou un développement spécifique ;
- les éventuelles limitations techniques identifiées.

Les intégrations spécifiques nécessaires au fonctionnement du SOC devront pouvoir être documentées, maintenues et adaptées pendant la durée du marché.

Maîtrise, localisation et protection des données

Les données collectées et conservées dans le SIEM demeurent sous la maîtrise du Pouvoir adjudicateur.

Les données doivent être hébergées au sein de l'Union européenne, sauf dérogation expressément acceptée par le Pouvoir adjudicateur et être **chiffrées au repos ainsi que lors de leur transmission**.

Le candidat précise dans son offre :

- la localisation des données ;
- les conditions d'accès par l'éditeur, le Titulaire ou leurs éventuels sous-traitants ;
- les mécanismes de chiffrement pour les données au repos et en transit ;
- les mécanismes de contrôle et de traçabilité des accès.

Le candidat indique si la solution ou son environnement d'hébergement bénéficie d'une qualification SecNumCloud ou présente des garanties de sécurité équivalentes.

Accès et administration

La solution doit permettre une gestion sécurisée et traçable des accès, fondée notamment sur l'authentification forte, la gestion des rôles et le principe de moindre privilège.

Le Pouvoir Adjudicateur doit disposer des droits nécessaires au contrôle et au suivi de la solution.

Conservation des données

Les événements et journaux de sécurité doivent être conservés pendant une durée minimale de **douze (12) mois.** Cette conservation peut combiner une période de consultation immédiate et une période d'archivage.

Le candidat précise dans son offre les modalités retenues, les délais de restitution des données archivées.

Réversibilité et portabilité

Les données, configurations, règles de détection, cas d'usage et autres éléments produits ou adaptés doivent pouvoir être restitués dans des formats standards et exploitables.

L'architecture proposée ne doit pas créer une dépendance technique susceptible de compromettre la continuité du service en cas de changement de prestataire ou de produits.

5.3 Infogérance

5.3.1 Dispositions communes à l'ensemble du périmètre

5.3.1.1 Exploitation, MCO et MCS

Le Titulaire assure l'exploitation, le **Maintien en Conditions Opérationnelles (MCO)** et le **Maintien en Conditions de Sécurité (MCS)** de l'ensemble des composants relevant du périmètre de l'infogérance, indépendamment de leur nature, de leur localisation, de leur mode d'hébergement ou de leur modèle de mise à disposition.

À ce titre, le Titulaire assure notamment :

- la supervision de la disponibilité, du bon fonctionnement, des performances et des capacités des équipements, solutions, services et composants du périmètre ;
- la détection, la qualification et le traitement des alertes et anomalies susceptibles d'affecter la disponibilité, les performances, la sécurité ou le bon fonctionnement des services ;
- le diagnostic des incidents et la mise en œuvre des actions correctives ou de rétablissement relevant de son périmètre ;
- la surveillance des ressources et des capacités, ainsi que le capacity planning nécessaire pour anticiper les besoins d'évolution ;
- le suivi des versions des équipements, logiciels, firmwares et autres composants techniques du périmètre ;
- la mise en œuvre des correctifs, mises à jour et montées de version conformément aux exigences du présent CCTP, aux bonnes pratiques et aux recommandations des éditeurs ;
- le maintien des configurations dans un état conforme aux exigences de sécurité et aux standards définis ;
- le traitement des incidents, demandes, changements de configuration, corrections et évolutions relevant de la prestation ;
- la mobilisation des niveaux d'expertise nécessaires au traitement des incidents, demandes et évolutions ;
- la relation technique avec les éditeurs et constructeurs lorsque leur intervention est nécessaire, le Pouvoir adjudicateur assurant, le cas échéant, la souscription aux contrats de support requis ;
- assurer le capacity planning des composants techniques du périmètre
- assurer et maintenir le niveau d'expertise nécessaire sur l'ensemble des technologies mises en œuvre dans le périmètre
- le maintien à jour de la documentation technique, des configurations, procédures et informations nécessaires à l'exploitation du périmètre.

5.3.1.2 Niveaux de support (N1, N2, N3)

Dans le cadre de la prestation, le Titulaire met en œuvre une organisation de support structurée, de type centre de services, permettant la mobilisation des différents niveaux de prise en charge et d'expertise nécessaires au traitement des incidents, demandes et évolutions.

Les modalités d'organisation, les responsabilités associées et les niveaux de support N1, N2 et N3 sont détaillés au chapitre : ***6.1.5 Support et niveaux de prise en charge***

Le dispositif proposé doit permettre la mobilisation des compétences adaptées à la nature, à la complexité et à la criticité des situations rencontrées, sans rupture de prise en charge pour le Pouvoir adjudicateur.

Le Titulaire peut proposer une organisation mutualisant certains niveaux de support, notamment les niveaux N1 et N2, sous réserve de garantir les niveaux de service et d'expertise attendus

5.3.1.3 Documentation et base de connaissances

Le Titulaire assure, pendant toute la durée de la prestation, le maintien à jour, l'enrichissement et, lorsque nécessaire, la création des documentations relatives aux composants et services relevant de son périmètre.

Le corpus documentaire existant, notamment les documents d'architecture technique (DAT), dossiers d'exploitation (DEX), procédures et documents de référence, est mis à disposition du Titulaire lors de la phase d'initialisation. Les modalités de gestion documentaire, de validation, de stockage, de nommage et de mise à jour sont définies dans le cadre de cette phase.

Le Titulaire veille à ce que toute évolution significative du périmètre, de son architecture, de ses configurations ou de ses modalités d'exploitation donne lieu à la mise à jour des documents concernés.

Les documents créés ou modifiés par le Titulaire, le Pouvoir adjudicateur ou un tiers sont intégrés au corpus documentaire après validation selon les modalités définies entre les parties.

La documentation nécessaire au nouveau périmètre SOC est constituée et maintenue selon les mêmes principes.

En complément de ce corpus, le Titulaire maintient et enrichit une base de connaissances opérationnelle destinée à faciliter l'exploitation des services ainsi que le traitement des demandes, incidents et problèmes.

Cette base de connaissances capitalise notamment les procédures de diagnostic, solutions de contournement, erreurs connues, procédures de résolution, bonnes pratiques, enseignements issus des incidents et retours d'expérience, ainsi que les actions correctives ou préventives présentant un intérêt pour l'exploitation.

Le Titulaire exploite cette capitalisation afin d'améliorer progressivement l'efficacité du support et de réduire la récurrence des incidents.

L'ensemble de la documentation produite spécifiquement dans le cadre du marché est restituable au Pouvoir adjudicateur et reste soumis aux dispositions contractuelles applicables en matière de propriété intellectuelle et de réversibilité.

5.3.1.4 Gestion des versions, correctifs et vulnérabilités

Le Titulaire assure, sur les composants placés sous son administration, une veille technique et éditeur continue ainsi que le maintien des versions et correctifs nécessaires au maintien en conditions opérationnelles et de sécurité.

À ce titre, il assure notamment :

- le maintien des équipements, logiciels et composants dans des versions supportées, stables et compatibles avec l'environnement du Pouvoir adjudicateur ;
- le suivi des fins de support, fins de maintenance et situations d'obsolescence ;
- la mise en œuvre des correctifs et actions de remédiation relevant de son périmètre ;
- la proposition des actions de mise à niveau, migration, renouvellement ou remplacement nécessaires ;
- l'élaboration et la mise à jour d'un plan annuel de maintenance prévisionnel.

Lors de la phase d'initialisation, le Titulaire établit un état initial des versions, niveaux de support et principales échéances de fin de vie des composants relevant de son périmètre.

Le plan annuel de maintenance est actualisé en fonction des évolutions du périmètre, des recommandations des constructeurs et éditeurs, des risques identifiés et des contraintes d'exploitation.

La maintenance planifiée ne dispense pas le Titulaire de mettre en œuvre les opérations correctives ou urgentes rendues nécessaires par une vulnérabilité, un incident ou un risque spécifique.

Les modalités détaillées de veille, de qualification, de priorisation et de déploiement des correctifs sont définies au chapitre : ***6.2.4 Patch Management – Gestion des correctifs***.

Le patch management des postes de travail et serveurs relevant du périmètre Système reste hors du périmètre du présent marché.

5.3.1.5 Gestion des configurations

Le Titulaire assure la gestion et le maintien des configurations des composants relevant de son périmètre.

Il veille notamment à maintenir des configurations maîtrisées, documentées et cohérentes avec l'architecture de référence, et assure leur sauvegarde et leur restauration lorsque les technologies concernées le permettent.

Toute modification de configuration, ajout ou retrait de composant, évolution de supervision ou modification d'architecture fait l'objet d'une préparation, d'une analyse d'impact et, lorsque nécessaire, d'une validation préalable du Pouvoir adjudicateur.

Le Titulaire définit les prérequis, les modalités d'intervention et, lorsque cela est pertinent, les modalités de retour arrière. Il assure la traçabilité des opérations réalisées.

Toute modification durable du périmètre donne lieu, lorsque nécessaire, à la mise à jour des configurations de référence, des outils associés et de la documentation technique.

5.3.2 Infogérance Réseau

5.3.2.1 Administration et exploitation LAN

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles des équipement (switch) constituant le réseau local (LAN) des différents sites de l'OPCO-SANTE.

5.3.2.2 Administration et exploitation Wi-Fi

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles de l'infrastructure de réseau sans fil, incluant les contrôleurs de gestion et les points d'accès déployés sur l'ensemble des sites

5.3.2.3 LAN datacenters et accès distants (VPN IPsec)

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles :

- Des infrastructures de commutation (switches) des datacenters, garantissant la connectivité des équipements techniques associés (virtualisation, sécurité, sauvegarde, etc.) hébergeant le Système d'Information de l'OPCO-SANTE
- Des interconnexions entre les datacenters ainsi que des liaisons sécurisées de type VPN IPsec permettant l'interconnexion des sites de l'OPCO-SANTE et les accès des partenaires ou intervenants externes autorisés.

5.3.2.4 Accès Internet des sites et des datacenters

Les accès Internet des différents sites et des datacenters de l'OPCO-SANTE sont fournis par des Fournisseurs (FAI) tiers.

Le Titulaire assure l'exploitation et la supervision de ces accès ainsi que le suivi de leur disponibilité et de leurs performances. À ce titre, il assure la relation technique et opérationnelle avec les FAI, notamment pour le diagnostic et le suivi des incidents, les demandes d'évolution et l'adaptation des caractéristiques et configurations des accès aux besoins du Système d'Information de l'OPCO-SANTE.

5.3.3 Infogérance Sécurité

5.3.3.1 Sécurité périmétrique et VPN client

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles et de sécurité des équipements et solutions de sécurité périmétrique déployés sur les différents sites et datacenters de l'OPCO-SANTE.
La prestation couvre notamment les FW, leurs plateformes centralisées d'administration et de management, ainsi que les solutions de VPN client permettant l'accès distant sécurisé des utilisateurs au Système d'Information.

5.3.3.2 Exposition sécurisée des services (reverse proxy, WAF)

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles et de sécurité des solutions permettant l'exposition sécurisée des applications et services du Système d'Information vers l'extérieur.

Ce périmètre comprend notamment les fonctions de reverse proxy et de WAF pare-feu applicatif (WAF), ainsi que la gestion des configurations et politiques associées nécessaires à la publication, au filtrage et à la protection des services exposés. Le Titulaire assure également les évolutions nécessaires à l'exposition de nouveaux services ou à la modification des services existants, en coordination avec les équipes de l'OPCO-SANTE et, le cas échéant, les autres intervenants concernés.

5.3.3.3 Service d'authentification réseau (RADIUS)

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles et de sécurité du service RADIUS utilisé pour l'authentification et le contrôle des accès aux infrastructures réseau de l'OPCO-SANTE, notamment dans le cadre des mécanismes d'authentification 802.1X.

La prestation comprend notamment :

- L'administration et le maintien en condition du service RADIUS et de ses composants techniques ;
- La gestion des configurations, politiques d'authentification et autorisations d'accès ;
- La gestion des équipements et services réseau clients du RADIUS ;
- La supervision de la disponibilité, du bon fonctionnement et des performances du service ;
- Le diagnostic et le traitement des incidents d'authentification et d'accès réseau ;
- Le maintien des versions et l'application des correctifs de sécurité conformément aux exigences du présent CCTP ;
- Le suivi des journaux techniques et la coordination avec le SOC en cas d'événement de sécurité.

Le Titulaire assure également la coordination avec les intervenants responsables des services d'annuaire, des certificats et des infrastructures système dont dépend le fonctionnement du service RADIUS.

Les demandes d'exploitation et d'évolution sont traitées conformément au catalogue de services annexé au présent CCTP.

5.3.3.4 Filtrage Web

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles et de sécurité de la solution de filtrage Web de l'OPCO-SANTE.

La solution repose sur un service centralisé en mode SaaS permettant de contrôler et de sécuriser les accès Web des utilisateurs. Elle s'appuie notamment sur des mécanismes de traitement du trafic depuis le réseau de l'OPCO-SANTE ainsi que sur des agents installés sur les postes de travail, permettant d'assurer la protection des utilisateurs sur site comme en situation de mobilité.

Le Titulaire assure notamment la gestion des configurations et des politiques de filtrage, des catégories et des règles d'accès, ainsi que le traitement des demandes d'autorisation, de blocage ou d'exception conformément aux règles définies par l'OPCO-SANTE.

5.3.3.5 Protection de la messagerie (antispam)

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles et de sécurité de la solution de protection de la messagerie électronique de l'OPCO-SANTE.

La solution repose sur un service centralisé en mode SaaS, interconnecté avec la plateforme de messagerie de l'OPCO-SANTE, permettant d'assurer le contrôle et le filtrage des flux de messagerie entrants et sortants.

Le Titulaire assure notamment l'administration des politiques de protection et de filtrage, la gestion des règles, listes d'autorisation et de blocage, quarantaines et exceptions, ainsi que le traitement des demandes et incidents liés au fonctionnement de la solution.

La solution contribue notamment à la protection contre le spam, le phishing, les contenus malveillants et, plus généralement, les menaces véhiculées par la messagerie électronique.

5.3.3.6 Gestion des accès à privilèges (PAM / bastion)

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles et de sécurité de la solution de gestion des accès à privilèges (PAM) et du bastion d'administration.

Le Titulaire assure notamment la gestion des ressources et comptes administrés par la solution, des politiques d'accès, des habilitations et des mécanismes permettant le contrôle, la traçabilité et l'enregistrement des sessions d'administration.

Il accompagne également l'OPCO-SANTE dans l'intégration de nouveaux équipements, systèmes ou comptes nécessitant d'être administrés au travers du bastion.

5.3.3.7 Authentification multifacteur (MFA)

Assurer l'exploitation, l'administration, la supervision et le maintien en conditions opérationnelles et de sécurité de la solution d'authentification multifacteur (MFA).

Le Titulaire assure la gestion des configurations et politiques d'authentification relevant de son périmètre ainsi que l'intégration des systèmes et applications nécessitant le recours à une authentification renforcée.

Il contribue également au diagnostic et au traitement des incidents liés au fonctionnement du service MFA et à son intégration avec le Système d'Information de l'OPCO-SANTE

5.3.3.8 Landing Zone Azure

Assurer l'exploitation, l'administration et le maintien en conditions opérationnelles et de sécurité des composants de la Landing Zone Azure relevant du périmètre de la prestation.

La prestation couvre notamment les mécanismes de connectivité sécurisée entre Azure et le Système d'Information de l'OPCO-SANTE, ainsi que l'administration des configurations, politiques et règles de sécurité communes nécessaires à l'hébergement sécurisé des ressources dans Azure.

Le Titulaire accompagne également l'OPCO-SANTE dans les évolutions de la Landing Zone ayant un impact sur les composants réseau et sécurité relevant de son périmètre.

5.3.3.9 Gestion opérationnelle des certificats

Assurer la gestion opérationnelle des certificats numériques utilisés par les équipements, applications et solutions relevant du périmètre de la prestation.

Le Titulaire assure notamment l'inventaire et le suivi des certificats déployés, la surveillance de leur date d'expiration, l'anticipation des renouvellements ainsi que leur installation, leur remplacement et leur configuration sur les composants concernés.

L'émission et la fourniture des certificats restent sous la responsabilité de l'OPCO-SANTE ou des autorités de certification désignées par celui-ci. Le Titulaire assure la coordination nécessaire avec les différents intervenants afin de garantir leur renouvellement et leur déploiement avant expiration.

5.3.3.10 Administration de la solution EDR

Assurer l'exploitation, l'administration et le maintien en conditions opérationnelles et de sécurité de la solution EDR déployée sur le Système d'Information de l'OPCO-SANTE.

La prestation comprend notamment le déploiement et le maintien en condition des agents, la gestion des configurations et des politiques de protection, le suivi de la couverture et de l'état de santé des agents ainsi que la gestion des exclusions.

Les activités de surveillance des événements de sécurité, d'analyse des alertes et de réponse aux incidents relèvent du périmètre SOC. Le Titulaire assure à ce titre la coordination nécessaire avec le SOC et met à sa disposition les accès et droits nécessaires à l'exercice de ses missions.

Toute modification ou exclusion susceptible de réduire durablement la couverture de détection ou de protection est soumise à validation selon les modalités définies par l'OPCO-SANTE.

5.3.4 Infogérance SOC

5.3.4.1 Périmètre et principes du SOC

Le Titulaire assure une prestation de **Security Operations Center (SOC)** destinée à assurer la surveillance de sécurité du Système d'Information du Pouvoir adjudicateur, la détection des menaces, leur qualification et leur investigation.

Les activités du SOC s'exercent selon deux modalités complémentaires :

- **La détection et le traitement des événements et incidents de sécurité**, résultant notamment des mécanismes de surveillance, de corrélation, des cas d'usage de détection, de la Threat Intelligence, du Threat Hunting ou de toute autre capacité de détection mise en œuvre dans le cadre de la prestation ;
- **La prise en charge de demandes d'investigation ou de levée de doute**, formulées par le Pouvoir adjudicateur ou par les équipes d'infogérance, lorsqu'une situation nécessite une analyse ou une qualification de sécurité sans qu'un incident de sécurité soit préalablement caractérisé.

Une demande d'investigation peut conduire, lorsque les analyses mettent en évidence une menace, une compromission ou un risque significatif, à l'ouverture d'un incident de sécurité et à l'application du processus de gestion des incidents défini au présent CCTP.

Le SOC prend en compte l'ensemble des sources pertinentes nécessaires à la surveillance du Système d'Information. Selon leur présence dans le système d'information, ce périmètre comprend notamment :

- les identités et services d'authentification ;
- les postes de travail ;

- les serveurs ;
- les annuaires ;
- Microsoft 365 ;
- Microsoft Azure et les environnements Cloud ;
- les équipements réseau ;
- les pare-feu ;
- les équipements et solutions de sécurité ;
- les WAF ;
- les solutions EDR/XDR ;
- les solutions de messagerie ;
- les proxies ;
- les VPN ;
- les bastions ;
- les systèmes d'exploitation ;
- les applications et services exposés ;
- les journaux applicatifs présentant un intérêt en matière de sécurité ;
- les solutions de gestion des vulnérabilités ;
- et plus généralement toute source pertinente au regard des risques et scénarios de menace.

Le périmètre des sources supervisées est formalisé dans un **référentiel des sources SOC**, maintenu à jour pendant toute la durée du marché.

Pour chaque source sont notamment identifiés :

- le système ou service concerné ;
- son niveau de criticité ;
- la nature des données collectées ;
- le mode de collecte ;
- la volumétrie ;
- les cas d'usage exploitant la source ;
- l'état de la collecte ;
- la durée de conservation ;
- les éventuelles limitations connues.

Le Titulaire précise également sa capacité à intervenir sur différents écosystèmes technologiques et constructeurs, notamment Microsoft, Cisco, Fortinet, Palo Alto Networks ou technologies équivalentes.
Le Pouvoir adjudicateur recherche une capacité SOC **transverse et multi-technologies**, permettant d'assurer les prestations de surveillance, de qualification et d'investigation indépendamment d'un constructeur ou d'une plateforme particulière.

5.3.4.2 Demandes d'investigation et levées de doute

En complément de la détection et du traitement des incidents de sécurité, le SOC assure la prise en charge des demandes ponctuelles d'investigation, d'analyse et de qualification de sécurité formulées par l'équipe d'infogérance ou par le Pouvoir adjudicateur. Ces demandes peuvent notamment porter sur :

- la réputation et le niveau de confiance d'une URL, d'un domaine ou d'une adresse IP ;
- l'analyse d'un fichier ou d'un artefact suspect ;
- la qualification d'un indicateur de compromission ;
- l'analyse d'un courriel, d'un expéditeur ou d'un comportement suspect ;
- la recherche d'éléments de compromission ou de signaux faibles dans les sources disponibles ;
- la réalisation d'une recherche ponctuelle de Threat Intelligence ;
- l'émission d'un avis de sécurité préalable à une opération technique, notamment une mise en liste blanche, une autorisation ou un déblocage.

Le SOC restitue le résultat de son analyse sous une forme exploitable, comprenant a minima les éléments analysés, les constats, le niveau de risque identifié et la recommandation associée.

Lorsque l'analyse conclut à la nécessité d'une action technique sur une solution ou un équipement relevant de l'infogérance Réseau / Sécurité, le SOC transmet les éléments nécessaires à l'infogérant concerné afin de permettre la réalisation de l'action, conformément aux processus de coordination et aux responsabilités définis dans le présent CCTP ou lors de la phase d'initialisation.

Le SOC demeure responsable de l'analyse et de la qualification de sécurité ; l'infogérant Réseau / Sécurité demeure responsable de la mise en œuvre technique lorsqu'elle relève de son périmètre.

5.3.4.3 Gestion du SIEM

Pendant toute la durée du marché, le Titulaire assure l'exploitation, l'administration, la supervision ainsi que le maintien en conditions opérationnelles et de sécurité du SIEM et de ses composants associés. À ce titre, le Titulaire assure notamment :

- l'administration et la configuration de la solution ;
- le maintien en conditions opérationnelles (MCO) et le maintien en conditions de sécurité (MCS) ;
- la gestion des correctifs, mises à jour, évolutions et montées de version ;
- la supervision technique de la plateforme, de ses composants et des mécanismes de collecte associés ;
- l'intégration, la modification et le retrait des sources de journaux en fonction des évolutions du périmètre ;

- la configuration et le maintien des collecteurs, connecteurs, agents ou autres composants nécessaires à la collecte des événements ;
- la normalisation, l'enrichissement et le traitement des événements collectés ;
- la gestion et le maintien des politiques de rétention et d'archivage définies ;
- le suivi des capacités, des performances et de la volumétrie ;
- l'identification et le traitement des incidents et anomalies susceptibles d'affecter le fonctionnement du SIEM ou la capacité de détection du SOC ;
- le maintien à jour de la documentation technique et d'exploitation.

Le Titulaire veille en particulier au bon fonctionnement de la chaîne de collecte et à l'absence d'angle mort susceptible d'altérer la capacité de surveillance du SOC. Il assure à ce titre la détection et le traitement des anomalies telles qu'une interruption de collecte, une source devenue silencieuse, une baisse anormale de volumétrie, un retard d'ingestion ou une défaillance d'un composant de collecte.

Le Titulaire assure également la gestion, la documentation, le maintien à jour et le versionnage des règles de détection, des règles de corrélation et des cas d'usage appliqués à l'environnement du Pouvoir adjudicateur.

Ces éléments sont maintenus et adaptés tout au long de la prestation afin de prendre en compte notamment :

- les évolutions du Système d'Information ;
- l'intégration ou le retrait de sources ;
- l'évolution des menaces et des techniques d'attaque ;
- les enseignements issus des alertes, incidents et investigations ;
- les demandes du Pouvoir adjudicateur ;
- les actions d'amélioration continue du dispositif SOC.

Le Pouvoir adjudicateur dispose d'une visibilité sur les règles, corrélations et cas d'usage appliqués à son environnement et peut demander au Titulaire leur analyse, leur adaptation, leur évolution ou la création de nouveaux cas d'usage.

Les règles, corrélations, configurations et cas d'usage développés ou adaptés spécifiquement pour le périmètre du Pouvoir adjudicateur doivent être documentés et maintenus dans des conditions permettant leur restitution dans le cadre de la réversibilité et, dans la mesure du possible, leur réexploitation ou leur transposition vers une autre solution.

5.3.4.4 Cas d'usage et détection des menaces

Le Titulaire assure, pendant toute la durée de la prestation, le maintien et l'évolution des capacités de détection du SOC. Celles-ci ne doivent pas reposer exclusivement sur les règles génériques ou les contenus standards fournis par les éditeurs des solutions utilisées.

Le Titulaire met en œuvre une démarche de **Detection Engineering** permettant de concevoir, tester, déployer, maintenir et améliorer les règles de détection et cas d'usage applicables au Système d'Information du Pouvoir adjudicateur.

Les cas d'usage sont adaptés au contexte, aux actifs, aux risques et aux menaces susceptibles d'affecter le Pouvoir adjudicateur. Ils sont alimentés notamment par les évolutions du Système d'Information, les incidents et investigations réalisés, la Threat Intelligence, les résultats des activités de Threat Hunting, les vulnérabilités identifiées ainsi que l'évolution des techniques d'attaque.

Chaque cas d'usage doit être documenté de manière à permettre d'identifier son objectif, le scénario de menace couvert, les sources de données nécessaires, la logique de détection, le niveau de criticité associé, les modalités d'investigation et d'escalade ainsi que les évolutions apportées au cours de son cycle de vie.

Le Titulaire maintient un **catalogue des cas d'usage SOC** accessible au Pouvoir adjudicateur et assure leur suivi tout au long de la prestation.

Il évalue périodiquement la couverture de détection afin d'identifier les scénarios correctement couverts, ceux présentant une couverture partielle ainsi que les éventuels angles morts nécessitant la mise en œuvre de nouvelles capacités de surveillance.

Cette analyse peut notamment s'appuyer sur le référentiel **MITRE ATT&CK**, contextualisé au regard de l'environnement et des risques du Pouvoir adjudicateur.

Les résultats des revues de couverture contribuent à la définition et à la priorisation des évolutions du dispositif de détection dans le cadre de l'amélioration continue du SOC.

Les règles et cas d'usage développés ou adaptés spécifiquement au périmètre du Pouvoir adjudicateur sont documentés et conservés dans des conditions permettant leur restitution dans le cadre de la réversibilité.

5.3.4.5 Détection et suivi des vulnérabilités

Le Titulaire assure la détection, la contextualisation, la qualification, la priorisation et le suivi des vulnérabilités susceptibles d'affecter les actifs, équipements, systèmes, applications et composants intégrés au périmètre de surveillance du SOC, y compris lorsque leur exploitation ou leur remédiation relève d'un autre prestataire ou exploitant.

La couverture attendue porte sur les niveaux suivants :

- **Services et solutions exploités :** détection des vulnérabilités affectant les solutions et services du périmètre, notamment les solutions de sécurité, proxy, WAF, bastion, MFA et autres composants exploités dans le cadre de la prestation ;
- **Systèmes d'exploitation :** détection des vulnérabilités et des correctifs de sécurité manquants affectant les systèmes d'exploitation des équipements, serveurs et composants relevant du périmètre ;

- **Composants d'infrastructure :** détection des vulnérabilités affectant les versions logicielles, systèmes embarqués et firmwares des équipements d'infrastructure, notamment les pare-feu, commutateurs, équipements réseau et autres composants techniques ;
- **Composants applicatifs et bibliothèques logicielles :** détection des vulnérabilités affectant les composants applicatifs et bibliothèques logicielles utilisés par les applications du périmètre, par exemple les versions Java, .NET, PHP, Node.js ou des bibliothèques telles que Log4j.

Une attention particulière est portée aux applications et logiciels métiers critiques du Système d'Information. A ce titre, lorsque les applications et logiciels métiers produisent des journaux ou événements exploitables à des fins de sécurité, et sous réserve de faisabilité technique, ceux-ci sont intégrés au dispositif SOC afin de contribuer à la détection de comportements anormaux, de tentatives d'exploitation ou d'indices de compromission

À titre d'exemple, lorsqu'une vulnérabilité critique affecte une bibliothèque ou un composant largement utilisé, tel que Log4j, le dispositif doit permettre de rechercher sa présence dans le périmètre, d'identifier les applications ou services potentiellement concernés et d'en apprécier l'exposition réelle

La prestation ne doit pas se limiter à la production ou à la transmission d'une liste de vulnérabilités.

Le Titulaire contextualise les résultats au regard de l'environnement réel du Pouvoir adjudicateur afin de déterminer notamment la présence effective du composant vulnérable, sa version, l'utilisation de la fonctionnalité concernée, son niveau d'exposition, la criticité de l'actif ou de l'application, l'existence d'un exploit disponible ou d'une exploitation active connue, ainsi que les éventuelles mesures compensatoires déjà en place.

La contextualisation doit permettre de distinguer une vulnérabilité théoriquement applicable d'une vulnérabilité réellement pertinente et actionnable au regard du contexte du Système d'Information, puis d'en déterminer le niveau de priorité et les recommandations de traitement appropriées.

La détection, la contextualisation et la priorisation des vulnérabilités relèvent du SOC.

La mise en œuvre des mesures de remédiation relève de l'exploitant en charge du MCO/MCS du composant concerné, qu'il s'agisse des équipes d'infogérance SOC, réseau/sécurité, système ou de tout autre exploitant tiers responsable du périmètre.

L'état des vulnérabilités, leur niveau de priorité, les actions de remédiation engagées ainsi que les éventuels retards, difficultés ou impossibilités de traitement sont intégrés au reporting de la prestation.

5.3.4.6 Surveillance de la surface d'attaque interne et externe

Le Titulaire assure une surveillance continue de la **surface d'attaque interne et externe** du Pouvoir adjudicateur afin d'identifier les expositions, évolutions ou configurations susceptibles d'accroître le niveau de risque du Système d'Information.

Cette surveillance concerne :

- Externe : Les actifs et services **exposés** sur Internet, les domaines et sous-domaines, les certificats, les nouveaux points d'exposition, les configurations présentant un risque, les actifs inconnus ou insuffisamment référencés ainsi que les modifications significatives de la surface d'exposition.
- Interne : Les actifs, services ou composants présents sur le périmètre **interne** et susceptibles de constituer une exposition ou un angle mort de sécurité.

Les informations détectées sont qualifiées et contextualisées au regard du Système d'Information, de la criticité des actifs et des informations détenues par le SOC. La prestation ne doit pas se limiter à produire un inventaire brut des actifs ou expositions identifiés.

Toute exposition présentant un risque significatif fait l'objet d'une analyse permettant d'en apprécier la réalité, la criticité et les mesures de traitement nécessaires. Lorsque la situation le justifie, elle donne lieu à une notification au Pouvoir adjudicateur, à une recommandation de remédiation et à la **création d'un incident de sécurité**, traité conformément au processus de gestion des événements et incidents de sécurité défini au présent CCTP.

Les résultats de cette surveillance alimentent les autres activités du SOC, notamment la gestion des vulnérabilités, la Threat Intelligence, les mécanismes de détection et les activités de Threat Hunting.

5.3.4.7 Surveillance du Dark Web

Le Titulaire assure une capacité de surveillance des sources spécialisées du **Dark Web** et, plus largement, des espaces susceptibles de faire apparaître des informations pouvant concerner le Pouvoir adjudicateur ou révéler une compromission, une fuite de données ou la préparation d'une attaque.

Cette surveillance porte notamment sur les domaines et marques surveillés, les adresses de messagerie, les identifiants compromis, les données ou documents divulgués, les mentions du Pouvoir adjudicateur, les accès à son Système d'Information susceptibles d'être proposés à la vente ainsi que tout autre signal présentant un intérêt en matière de sécurité.

Les informations collectées font l'objet d'une **qualification et d'une contextualisation préalables** afin de limiter les faux positifs, le bruit et les notifications dépourvues de caractère opérationnel.

Lorsqu'une information est jugée pertinente, le Titulaire en évalue la portée et les conséquences potentielles pour le Pouvoir adjudicateur et engage, selon la situation, les actions nécessaires.

Ces informations peuvent notamment conduire à l'ouverture d'une investigation, à une recherche d'indicateurs de compromission dans le Système d'Information, à l'évolution d'un cas d'usage de détection, au déclenchement d'une activité de Threat Hunting ou à la notification d'une menace ou d'une exposition au Pouvoir adjudicateur.

Les résultats issus de cette surveillance sont ainsi intégrés aux capacités de Threat Intelligence et contribuent à l'amélioration continue du dispositif SOC.

5.3.4.8 Threat Intelligence

Le Titulaire assure, pendant toute la durée de la prestation, une capacité de **Threat Intelligence** permettant d'identifier, de collecter, de qualifier et de contextualiser les informations relatives aux menaces susceptibles d'affecter le Pouvoir adjudicateur.

Cette capacité couvre les dimensions stratégique, tactique, opérationnelle et technique de la menace et doit permettre d'apporter au SOC des informations directement exploitables dans le cadre de ses activités de surveillance, d'investigation et d'amélioration continue.

Le Titulaire assure notamment :

- le suivi des menaces, campagnes, groupes d'attaquants, tactiques, techniques et procédures susceptibles de concerner le Pouvoir adjudicateur ;
- l'identification et la qualification des menaces émergentes ou des campagnes nécessitant une vigilance particulière ;
- la collecte et l'exploitation des indicateurs de compromission et autres marqueurs techniques pertinents ;
- la contextualisation des renseignements collectés au regard du Système d'Information, des technologies utilisées, du secteur d'activité et de l'exposition du Pouvoir adjudicateur ;
- l'enrichissement des alertes et investigations du SOC à partir de ces informations ;
- l'exploitation de ces renseignements pour la création ou l'évolution des règles de détection et des cas d'usage ;
- leur prise en compte dans la priorisation des vulnérabilités et des expositions identifiées ;
- leur utilisation pour orienter les activités de Threat Hunting.

La prestation ne doit pas se limiter à la mise à disposition de flux d'indicateurs ou de publications génériques. Le Titulaire analyse la pertinence des informations collectées au regard du contexte du Pouvoir adjudicateur et en détermine les éventuelles actions à engager.

Lorsqu'une information révèle une menace présentant un risque significatif pour le Système d'Information, le Titulaire procède aux investigations nécessaires et, lorsque la situation le justifie, déclenche le processus de gestion des événements et incidents de sécurité défini au présent CCTP.

Le Titulaire informe également le Pouvoir adjudicateur des menaces, campagnes ou évolutions significatives susceptibles d'avoir un impact sur son environnement et formule, lorsque nécessaire, les recommandations de surveillance, de protection ou de remédiation associées.

Les enseignements issus des investigations, incidents de sécurité, campagnes de Threat Hunting et interventions CERT/CSIRT sont réexploités afin d'enrichir la connaissance de la menace et d'améliorer les capacités de détection du SOC.

5.3.4.9 Threat Hunting

Le Titulaire assure, pendant toute la durée de la prestation, des activités régulières de **Threat Hunting** destinées à rechercher de manière proactive des comportements suspects, techniques d'attaque ou traces de compromission qui ne seraient pas identifiés par les mécanismes de détection existants.

Les activités de Threat Hunting font l'objet de campagnes planifiées, complétées, lorsque nécessaire, par des recherches spécifiques pouvant être déclenchées à la suite d'un incident, d'une menace identifiée par la Threat Intelligence, d'une vulnérabilité critique ou de tout autre élément justifiant une investigation proactive

Lorsqu'une activité de Threat Hunting met en évidence un comportement suspect, une trace de compromission ou un risque significatif, le Titulaire poursuit les investigations et déclenche, lorsque nécessaire, le processus de gestion des événements et incidents de sécurité.

Chaque activité fait l'objet d'une traçabilité précisant a minima :

- l'hypothèse recherchée ;
- le périmètre concerné ;
- les sources et données exploitées ;
- les recherches et investigations réalisées ;
- les résultats et conclusions ;
- les éventuelles actions ou évolutions recommandées.

Le Titulaire exploite systématiquement les enseignements issus du Threat Hunting pour améliorer le dispositif SOC. Les résultats peuvent notamment conduire à la création ou à l'évolution de règles de détection et de cas d'usage, à l'adaptation des procédures d'investigation, à l'évolution des sources de données exploitées ou à l'enrichissement de la Threat Intelligence.

Les activités réalisées, leurs principaux résultats ainsi que les évolutions du dispositif qui en découlent sont intégrés au reporting de la prestation.

La fréquence minimale de réalisation des campagnes ainsi que les délais associés sont définies dans le chapitre : ***7.2.5 SLA – Activités récurrentes du SOC.***

5.3.4.10 CERT/CSIRT – Réponse à incident (à déclenchement)

En complément des capacités courantes de qualification, d'investigation et de traitement assurées par le SOC et les équipes d'infogérance, le Titulaire met à disposition une capacité **CERT/CSIRT mobilisable** pour les incidents nécessitant des compétences ou des moyens spécialisés.

Cette prestation est **activable à la demande du Pouvoir adjudicateur** et fait l'objet d'une tarification spécifique conformément aux dispositions prévues au BPU.

Le recours au CERT/CSIRT intervient notamment lorsque la nature, l'ampleur ou la complexité d'un incident nécessite des capacités d'investigation approfondie, d'analyse forensic, d'analyse de compromission, de recherche d'indicateurs de compromission, d'analyse de malware lorsque nécessaire, de confinement ou d'accompagnement technique à la remédiation et au rétablissement.

Le déclenchement du CERT/CSIRT ne doit pas entraîner de rupture dans la prise en charge de l'incident. Le Titulaire assure la transmission des informations, investigations et éléments de contexte déjà disponibles ainsi que la coordination entre le SOC, le CERT/CSIRT, les équipes d'infogérance et, le cas échéant, les autres intervenants mobilisés.

Les actions de confinement, de remédiation ou de modification du Système d'Information sont réalisées conformément aux responsabilités définies au marché et à la matrice des actions autorisées.

Les interventions du CERT/CSIRT font l'objet d'une traçabilité et d'un retour d'expérience. Les enseignements issus des investigations sont réinjectés dans les activités récurrentes du SOC et peuvent notamment conduire à l'évolution des cas d'usage et règles de détection, des procédures d'investigation, des activités de Threat Hunting, de la Threat Intelligence ou des mécanismes de réponse.

5.3.4.11 Amélioration continue du SOC

Le Titulaire assure une amélioration continue des capacités de surveillance et de détection.

Le Titulaire propose régulièrement :

- de nouveaux cas d'usage ;
- l'amélioration des règles existantes ;
- la suppression des règles devenues inutiles ;
- l'amélioration des sources ;

- la réduction des faux positifs ;
- l'automatisation des investigations ;
- l'amélioration des procédures de réponse.

Le SOC ne doit donc pas être considéré comme un dispositif figé à l'issue de la phase d'initialisation.

5.3.5 Continuité d'activité (PCA/PRA)

L'OPCO-SANTE souhaite mettre en place un plan de bascule PRA qui couvre, à minima, les dysfonctionnements suivants. Le titulaire devra être capable d'assurer l'ensemble des scénarios de PRA ci-dessous et des tests associés. Le titulaire pourra proposer tout test supplémentaire qu'il considère comme nécessaire compte tenu de l'architecture existante.

Un test PRA complet consiste à effectuer à minima chacun des tests de scénarios suivants. Ce périmètre et les scénarios pourront évoluer au besoin durant le marché avec accord des deux parties.

Scénario d'incident	Scénario de secours	Validation des services associés
Coupure d'une FON entre les DC	- Fonctionnement sur une seule FON	- Validation de l'ensemble des services rendus par la FON (réplication, services Actif/Actif, accès aux ESX, …)
Coupure internet ou Firewall HS DC de PROD	- Bascule automatique vers le firewall de PRA - Bascule automatique des VPN client, IPSEC vers le firewall PRA - Flux de production (métier) passe par FON du DC PRA vers DC PROD	- Validation de l'accès internet via le site de PRA - Validation des VPNs IPSec des sites et partenaires sur firewall PRA - Validation des accès au SI (prod) via firewall PRA et FON - Validation des VPNs clients sur firewall PRA
Perte d'un membre du stack de switchs DC	- Bascule automatique sur le membre secondaire (Service sur 1 switch / 1 FON)	- Validation de l'ensemble des services rendus par le switch (réplication, services Actif/Actif, accès aux ESX, …)
Perte du firewall du lien internet primaire à Levallois	- Bascule automatique sur le firewall secondaire - Bascule automatique sur le firewall secondaire du VPN IPSEC Levallois vers DC	- Validation de l'accès internet via la liaison internet secondaire - Validation de l'ensemble des services d'accès via le firewall secondaire et le lien internet secondaire
Perte d'un membre du stack de switchs Levallois interco	- Bascule automatique sur le membre secondaire (Service sur 1 seul switch)	- Validation de l'ensemble des services d'accès via le membre secondaire et le lien internet secondaire

Perte d'un membre d'un switch Levallois user	- Bascule manuelle sur le switch secondaire	- Validation de l'ensemble des services d'accès via le secours
Perte du firewall du lien internet primaire à Malakoff	- Bascule automatique sur le firewall secondaire - Bascule automatique sur le firewall secondaire du VPN IPSEC Malakoff vers DC	- Validation de l'accès internet via la liaison internet secondaire - Validation de l'ensemble des services d'accès via le firewall secondaire et le lien internet secondaire
Perte d'un membre du stack de switchs LAN Malakoff	- Bascule automatique sur le membre secondaire (Service sur 1 seul switch)	- Validation de l'ensemble des services d'accès via le membre secondaire et le lien internet secondaire
Perte du firewall du lien internet primaire à PACA	- Bascule automatique sur le firewall secondaire - Bascule automatique sur le firewall secondaire du VPN IPSEC Malakoff vers DC	- Validation de l'accès internet via la liaison internet secondaire - Validation de l'ensemble des services d'accès via le firewall secondaire et le lien internet secondaire
Perte d'un membre du stack de switchs PACA LAN	- Bascule automatique sur le membre secondaire (Service sur 1 seul switch)	- Validation de l'ensemble des services d'accès via le membre secondaire et le lien internet secondaire

L'ensemble de ces scénarios sont considérés comme des demandes standard définies au catalogue de services et doivent être testé à la demande du Pouvoir adjudicateur.

La planification et réalisation sont à convenir entre les deux parties

Le titulaire devra également être disponible entre 3 jours par an afin de participer aux tests réguliers du PRA Système et Infrastructure en tant que contributeur.

Les modalités d'intervention sont décrites dans le chapitre : ***6.1.1 Modalités d'intervention***

5.3.6 Prestations complémentaires

Les prestations définies dans ce paragraphe feront l'objet de bon de commande spécifique.

Projets sur périmètre infogéré

l'OPCO-SANTE pourra demander des prestations complémentaires au gré des besoins et/ou projets. Les coûts de prestations devront respecter les UOs des profils indiqués dans l'offre.

Le Titulaire indique dans son offre technique la décomposition des profils d'intervenant pour la réalisation des prestations et des unités d'œuvre du présent marché.

Ces profils devront impérativement respecter la nomenclature CIGREF (Nomenclature RH - Cigref).

Réalisation d'audits

Le titulaire pourra potentiellement être sollicité à la demande pour effectuer des prestations complémentaires d'audit telles que :

- Audit de couverture WI-FI d'un site
- Audit de performance
- Audit des configurations
- Audit de sécurité et tests d'intrusion

Accompagnement et conseil en cybersécurité

En complément des prestations d'exploitation opérationnelle du SOC, le Titulaire devra être en mesure de proposer, à la demande du Pouvoir adjudicateur, des prestations d'accompagnement, d'expertise et de conseil portant notamment sur :

- la gouvernance de la cybersécurité ;
- l'évolution de l'architecture de sécurité ;
- l'évolution et l'optimisation du dispositif SOC ;
- l'accompagnement à la définition de feuilles de route de sécurité ;
- l'analyse des risques et l'identification des axes d'amélioration ;
- l'accompagnement à la prise en compte des évolutions réglementaires et normatives applicables.

Une attention particulière sera portée à sa capacité à accompagner le Pouvoir adjudicateur dans la prise en compte des exigences issues de la directive **NIS2** et, plus largement, dans l'adaptation de son dispositif de cybersécurité aux évolutions réglementaires, organisationnelles et technologiques.

Assistance aux démarches post-incident de cybersécurité

En complément des prestations de détection, d'investigation et de traitement des incidents de sécurité prévues dans le cadre du SOC, le Pouvoir adjudicateur pourra solliciter le Titulaire pour des prestations complémentaires d'assistance consécutives à un incident de cybersécurité. Ces prestations pourront notamment concerner l'accompagnement du Pouvoir adjudicateur dans le cadre :

- d'une notification ou d'une démarche auprès de la CNIL ;
- d'un dépôt de plainte auprès des services compétents ;
- d'une déclaration de sinistre et des échanges avec l'assureur cyber ;
- de toute autre démarche administrative, réglementaire ou judiciaire nécessitant la production d'éléments techniques relatifs à l'incident.

À ce titre, le Titulaire pourra notamment être chargé de collecter et préserver les éléments techniques utiles, de reconstituer la chronologie de l'incident, de documenter les impacts et actions de remédiation, de produire les éléments nécessaires aux démarches engagées et d'apporter son expertise technique lors des échanges avec les autorités, assureurs ou experts mandatés.

Le Titulaire devra être en mesure de mobiliser les compétences nécessaires dans des délais compatibles avec les contraintes applicables.

Acquisition de logiciels et de matériels

Concernant l'acquisition des logiciels, matériels et licences liés au périmètre d'infogérance, l'OPCO-SANTE pourra, solliciter le Titulaire pour réaliser de telles acquisitions. Ces dernières feront l'objet d'un chiffrage spécifique et seront commandées conformément aux modalités prévues dans le marché.

6 Gouvernance et organisation

6.1 Organisation

6.1.1 Modalités d'intervention

Le Titulaire réalise principalement les interventions à distance, de manière sécurisée, au moyen des outils et dispositifs d'accès mis à disposition ou validés par le Pouvoir adjudicateur.

Il se conforme aux exigences de sécurité, de contrôle d'accès, d'authentification et de traçabilité définies par le Pouvoir adjudicateur. Les accès au Système d'Information doivent être strictement limités aux besoins de la prestation et aux personnels dûment autorisés.

Le Titulaire décrit dans son mémoire technique les mesures mises en œuvre pour sécuriser les centres d'opérations ou locaux depuis lesquels ses équipes sont susceptibles d'intervenir à distance sur le Système d'Information du Pouvoir adjudicateur. Ces mesures couvrent notamment :

- la gestion et le contrôle des accès physiques aux locaux ;
- les dispositions applicables aux personnels externes intervenant sur les sites du Titulaire ;
- la surveillance et la sécurisation des zones depuis lesquelles les interventions sont réalisées ;
- la continuité des services essentiels, notamment l'alimentation électrique, la climatisation et les télécommunications ;
- la protection contre les principaux risques physiques, notamment les incendies et dégâts des eaux ;
- les dispositifs de continuité et de reprise d'activité nécessaires au maintien du service.

Le Pouvoir adjudicateur se réserve la possibilité de demander des interventions physiques sur ses sites régionaux ou dans ses datacenters situés en Île-de-France lorsque la nature de l'intervention le nécessite.

Ces interventions font l'objet d'un cadrage préalable avec le Pouvoir adjudicateur et, lorsqu'elles ne sont pas incluses dans les prestations forfaitaires du marché, d'un chiffrage conformément aux unités d'œuvre prévues dans l'annexe financière.

Des interventions sur site pourront notamment être requises lors des phases d'initialisation, d'intégration, de changement majeur, de traitement d'incident ou pour toute opération nécessitant une présence physique.

6.1.2 Gestion et stockage de la documentation

Le Pouvoir adjudicateur met à disposition du Titulaire un **espace documentaire sécurisé** destiné au stockage et au partage de l'ensemble de la documentation relative à la prestation.

Cet espace constitue le **référentiel documentaire de référence** du marché. Le Titulaire est tenu de l'utiliser pour le stockage, la consultation, la mise à jour et le partage des documents produits ou utilisés dans le cadre de la prestation.

Les modalités d'organisation de cet espace, les droits d'accès, les règles de classement, de nommage, de versionnage, de validation et d'archivage sont définies lors de la phase d'initialisation.

Sauf nécessité technique dûment justifiée, la documentation du Pouvoir adjudicateur ne doit pas être stockée, copiée ou conservée dans les espaces documentaires, outils collaboratifs ou systèmes internes du Titulaire ou de ses éventuels sous-traitants.

Toute nécessité de conserver temporairement une copie en dehors de l'espace mis à disposition par le Pouvoir adjudicateur doit être préalablement portée à sa connaissance et limitée au strict besoin nécessaire à l'exécution de la prestation.

Ces copies doivent être protégées conformément aux exigences de sécurité du marché, maintenues à jour lorsqu'elles restent nécessaires et supprimées dès que leur conservation n'est plus justifiée.

En aucun cas un espace documentaire du Titulaire ou d'un tiers ne peut se substituer au référentiel documentaire mis à disposition par le Pouvoir adjudicateur.

6.1.3 Plages de services

Le Pouvoir adjudicateur définit les plages de services comme suit :

- HO : 8h-19h
- HNO Semaine : 19h-8h
- HNO Weekend : du vendredi 19h au lundi 8h

6.1.3.1 Supervision et qualification initiale

Le Titulaire assure la supervision de l'ensemble du périmètre du marché 24 heures sur 24 et 7 jours sur 7, 365 jours par an.

Cette organisation devra permettre de détecter, identifier et qualifier tout événement ou alerte pertinent sur l'ensemble du périmètre

Le Titulaire décrira l'organisation humaine et technique mise en œuvre pour assurer cette surveillance, en distinguant notamment le fonctionnement en heures ouvrées et hors heures ouvrées, les niveaux d'analyse disponibles, les mécanismes d'astreinte et les modalités d'escalade.

6.1.4 Organisation opérationnelle de l'infogérance

Le Titulaire décrit l'organisation mise en œuvre pour assurer le fonctionnement de :

6.1.4.1 Infogérance réseau sécurité

- les niveaux d'analystes mobilisés ;
- les modalités de fonctionnement N1/N2/N3 ;
- les dispositifs d'astreinte ou de présence permanente ;
- les modalités d'escalade ;
- les compétences spécialisées disponibles ;
- les responsabilités respectives des différentes équipes ;

6.1.4.2 Infogérance SOC

- les niveaux d'analystes mobilisés ;
- les modalités de fonctionnement N1/N2/N3 ;
- les dispositifs d'astreinte ou de présence permanente ;
- les modalités d'escalade ;
- les compétences spécialisées disponibles ;
- les responsabilités respectives des différentes équipes ;
- les interactions avec ses capacités CERT/CSIRT, Threat Intelligence et Threat Hunting.

Le Titulaire précise les activités réalisées directement par ses équipes et celles éventuellement confiées à des partenaires ou sous-traitants.

Le dispositif doit rechercher une **continuité opérationnelle maximale entre la détection, l'investigation et la remédiation**, afin de limiter les changements d'interlocuteurs et de ne pas transférer au Pouvoir adjudicateur la coordination entre les différentes composantes du service.

6.1.4.3 Articulation SOC / Infogérance

L'articulation entre le SOC et les activités d'infogérance réseau et sécurité constitue un élément central du service attendu par le Pouvoir adjudicateur.

L'organisation proposée devra permettre qu'une détection nécessitant une investigation, une expertise complémentaire ou une action technique soit prise en charge par les équipes compétentes sans que le Pouvoir adjudicateur ait à assurer lui-même la coordination entre le SOC, les équipes d'exploitation et les différentes expertises mobilisées par le Titulaire.

Le Titulaire assure ainsi une continuité opérationnelle entre les activités de détection, d'analyse, d'investigation et de remédiation.

Il précisera les modalités d'articulation et d'interaction entre les différentes capacités susceptibles d'être mobilisées dans le cadre de la prestation, notamment les fonctions SOC, CERT/CSIRT, Threat Intelligence, Threat Hunting, intégration et infogérance.

Cette organisation devra notamment préciser :

- les rôles et responsabilités de chaque équipe ;
- les modalités de sollicitation et de mobilisation des différentes expertises ;
- les circuits d'escalade fonctionnels et techniques ;
- les modalités de coordination entre les équipes SOC et les équipes d'exploitation ;
- les conditions de transfert d'une alerte ou d'un incident entre les différents niveaux et domaines d'expertise ;
- les modalités de suivi jusqu'à la résolution ou au rétablissement du service.

Une **matrice des actions autorisées** est définie et validée pendant la phase d'initialisation. Elle distingue notamment :

- les actions pouvant être exécutées automatiquement ;
- les actions pouvant être réalisées directement par le Titulaire ;
- les actions nécessitant une validation préalable du Pouvoir adjudicateur.

Le Titulaire formalise cette organisation et les circuits opérationnels associés dans le **PAQ et le PAS**, en décrivant notamment le passage de la détection à l'investigation puis, lorsque nécessaire, à la remédiation ou à l'action technique.

L'organisation retenue devra permettre de limiter les ruptures de prise en charge entre les différentes équipes et d'assurer une traçabilité complète des actions réalisées tout au long du traitement.

6.1.5 Support et niveaux de prise en charge

Le Titulaire met en place une organisation de support permettant d'assurer la prise en charge des différentes sollicitations relevant du périmètre du marché, notamment les incidents, demandes, alertes, opérations et sollicitations techniques.

Cette organisation repose sur plusieurs niveaux de prise en charge permettant de mobiliser les compétences adaptées à la nature, à la criticité et à la complexité de la sollicitation.

Les niveaux de support décrits ci-dessous constituent des niveaux de compétence et de responsabilité. Ils ne doivent pas être interprétés comme imposant un traitement strictement séquentiel lorsque la situation nécessite la mobilisation immédiate d'un niveau d'expertise supérieur.

Niveau 1 – Prise en charge initiale

Le niveau 1 assure la réception, l'enregistrement et la qualification initiale des sollicitations relevant du périmètre du marché.

Il assure notamment :

- la réception ou la prise en compte de la sollicitation ;
- son enregistrement et sa traçabilité dans l'outil ITSM ;

- la collecte des informations nécessaires à son traitement ;
- la qualification, la catégorisation et la priorisation ;
- la réalisation des premiers diagnostics ;
- l'application des procédures et solutions documentées dans la base de connaissances ;
- le traitement des sollicitations relevant de son niveau de compétence ;
- l'escalade vers le niveau approprié lorsque la sollicitation nécessite une expertise complémentaire.

Le niveau 1 veille à la qualité et à l'exhaustivité des informations transmises lors de toute escalade.

Niveau 2 – Expertise technique

Le niveau 2 assure la prise en charge des sollicitations nécessitant une expertise technique approfondie ou ne pouvant être traitées par le niveau 1.

Il assure notamment :

- l'analyse technique approfondie ;
- l'exploitation des journaux, alertes, événements et données de supervision disponibles ;
- l'identification des composants, équipements ou services concernés ;
- la recherche et la mise en œuvre de solutions de correction ou de contournement ;
- la réalisation des actions techniques relevant de son périmètre ;
- la coordination avec les autres équipes techniques lorsque nécessaire ;
- l'enrichissement des informations et de la documentation associées ;
- l'escalade vers le niveau 3 lorsque la situation nécessite une expertise avancée ou spécialisée.

Niveau 3 – Expertise avancée

Le niveau 3 constitue le niveau d'expertise le plus élevé mobilisable par le Titulaire dans le cadre de la prestation.

Il intervient notamment lorsqu'une sollicitation nécessite :

- une expertise approfondie sur un composant, une architecture ou une technologie ;
- une analyse technique complexe ;
- des compétences spécialisées ;
- la conception ou la mise en œuvre d'une correction spécifique ;
- la mobilisation ou la coordination d'un éditeur, constructeur, intégrateur ou fournisseur tiers.

6.1.6 Organisation des escalades

Le Titulaire met en place et maintient un dispositif formalisé d'escalade permettant de mobiliser les compétences et niveaux de responsabilité adaptés à la nature, à la criticité et à la complexité des sollicitations.

Les circuits d'escalade doivent permettre d'éviter tout retard de traitement lié à une succession inutile des niveaux de support.

L'escalade vers un niveau supérieur est réalisée dès lors que :

- le niveau de compétence requis dépasse celui de l'intervenant initialement mobilisé ;
- la complexité technique nécessite une expertise complémentaire ;
- la criticité ou l'impact de la situation justifie la mobilisation immédiate de ressources supplémentaires ;
- le traitement nécessite l'intervention d'un éditeur, constructeur, opérateur, intégrateur ou autre tiers ;
- le risque de non-respect d'un engagement de service est identifié.

L'escalade doit être déclenchée en fonction des besoins de la situation et ne doit pas être conditionnée à l'expiration préalable des délais contractuels.

Lorsque la situation le justifie, notamment pour les incidents critiques ou majeurs, le Titulaire privilégie la mobilisation parallèle des différents niveaux de compétence nécessaires plutôt qu'un traitement successif N1, N2 puis N3.

Les escalades techniques n'interrompent pas le traitement de la sollicitation et ne suspendent ni ne réinitialisent les délais associés aux engagements de service.

Lorsqu'un éditeur, constructeur, opérateur, intégrateur ou autre tiers doit être sollicité, le Titulaire demeure responsable du pilotage de la sollicitation relevant de son périmètre et assure le suivi des actions jusqu'à leur achèvement.

Le Titulaire formalise durant la phase d'initialisation les circuits d'escalade applicables au marché, notamment les interlocuteurs, moyens de contact, niveaux de responsabilité et modalités de mobilisation en HO et, lorsque requis, en HNO.

6.1.7 Référents opérationnels

Le Titulaire désigne, pour toute la durée du marché, des référents opérationnels clairement identifiés constituant les interlocuteurs privilégiés du Pouvoir adjudicateur pour le suivi courant de la prestation. Le dispositif comprend a minima :

- **Un Service Delivery Manager (SDM)**, ou fonction équivalente, chargé du pilotage opérationnel de la prestation, du suivi des engagements, de la coordination des équipes du Titulaire et de la bonne prise en compte des sollicitations du Pouvoir adjudicateur ;
- **Un référent technique** disposant d’un niveau d’expertise N3 ou équivalent, chargé d’assurer la coordination technique de la prestation, notamment avec les équipes de support et les différents experts intervenant sur le périmètre du marché.

Le référent technique constitue un point d'entrée privilégié pour les sujets nécessitant une coordination transverse, une expertise approfondie ou la mobilisation de plusieurs intervenants. Il veille notamment à la bonne articulation entre les différents niveaux de support, à la mobilisation des expertises nécessaires et au suivi des sujets techniques présentant un caractère complexe, transverse ou sensible.

Le SDM et le référent technique participent aux instances de pilotage les concernant. Le référent technique participe notamment au Comité Technique (COTECH) afin de contribuer au suivi des sujets techniques, des actions en cours, des risques et des évolutions du périmètre.

Continuité et suppléance

Le Titulaire garantit la continuité du dispositif de référents opérationnels pendant toute la durée du marché.

L'organisation mise en place ne doit pas reposer exclusivement sur la disponibilité d'une personne identifiée. Le Titulaire prévoit en conséquence les dispositifs de suppléance nécessaires afin d'assurer la continuité du pilotage opérationnel et technique, notamment pendant les périodes d'absence, de congé ou d'indisponibilité des référents principaux.

Les suppléants doivent disposer d'un niveau de connaissance suffisant du contexte, du périmètre, des sujets en cours et des engagements contractuels afin de permettre une reprise effective des responsabilités sans dégradation de la qualité de service.

Le dispositif doit également permettre la **mobilisation en heures non ouvrées (HNO)** en cas d'incident majeur, critique ou de situation de crise.

Le Titulaire précise dans son mémoire technique l'organisation proposée, les rôles respectifs de ces référents ainsi que leurs modalités d'interaction avec les autres équipes mobilisées dans le cadre du marché.

6.1.8 Référent commercial

Le Titulaire désigne un **référent commercial** chargé d'assurer le suivi contractuel et commercial de la prestation. Il constitue l'interlocuteur privilégié du Pouvoir adjudicateur pour les sujets relatifs au marché, notamment le suivi des engagements, les demandes de devis, les évolutions de périmètre, les prestations complémentaires et, plus généralement, toute question nécessitant une coordination commerciale ou contractuelle.

Le référent commercial veille à la bonne prise en compte des sollicitations du Pouvoir adjudicateur et assure, lorsque nécessaire, la coordination avec les équipes opérationnelles et techniques du Titulaire.

6.2 Processus et principes de gestion

6.2.1 Gestion de la supervision

6.2.1.1 Principes généraux

La supervision a pour objectifs :

- de détecter au plus tôt les dysfonctionnements et dégradations susceptibles d'affecter les services ;
- d'identifier les situations pouvant conduire à une indisponibilité ;
- de permettre une prise en charge proactive des incidents, lorsque cela est possible avant tout signalement utilisateur ;
- de surveiller la disponibilité, les performances et le bon fonctionnement des composants supervisés ;
- d'assurer la remontée et le traitement des événements techniques ;
- d'assurer la traçabilité des alertes et des actions réalisées ;
- de fournir les données nécessaires au suivi de la qualité et de la disponibilité des services ;
- de contribuer à l'amélioration continue de l'exploitation.

Le Titulaire assure la surveillance permanente des outils de supervision et garantit la continuité du dispositif de supervision pendant toute la durée du marché.

6.2.1.2 Périmètre et référentiel de supervision

Le Titulaire s'assure que tout composant entrant dans le périmètre d'exploitation fait l'objet d'une supervision adaptée. Le périmètre de supervision est défini et maintenu dans un référentiel partagé entre le Titulaire et le Pouvoir adjudicateur.

Le Pouvoir adjudicateur souhaite que le Titulaire constitue (lors de l'initialisation du marché) et maintienne un référentiel de supervision décrivant l'ensemble des éléments supervisés. Pour chaque composant ou service, ce référentiel précise a minima :

- l'élément supervisé ;
- les contrôles et métriques associés ;
- les seuils d'alerte ;
- les périodes de supervision ;
- les règles de corrélation éventuelles ;
- les actions automatiques éventuelles ;
- les consignes de traitement ;
- les règles d'escalade ;
- les groupes ou équipes devant être sollicités ;
- les éventuelles dépendances avec d'autres composants.

Le référentiel est tenu à jour par le Titulaire pendant toute la durée du marché et mise à disposition du Pouvoir adjudicateur.

Toute modification significative de l'environnement technique doit donner lieu à une vérification et, si nécessaire, à une adaptation de la supervision correspondante.

6.2.1.3 Mise sous supervision

Tout nouveau composant entrant dans le périmètre de la prestation doit être intégré au dispositif de supervision. La mise sous supervision comprend notamment :

- l'identification des contrôles nécessaires ;
- la configuration des métriques ;
- la définition des seuils ;
- la définition des règles d'alerte ;
- la configuration des destinataires et règles d'escalade ;
- la définition ou mise à jour des consignes de traitement ;
- la réalisation des tests de bon fonctionnement ;
- la mise à jour du référentiel de supervision.

La mise en production d'un nouveau composant relevant du périmètre ne peut être considérée comme complètement achevée tant que les dispositifs de supervision nécessaires à son exploitation ne sont pas opérationnels.

6.2.1.4 Classification des événements

Les événements remontés par les outils de supervision font l'objet d'une classification permettant d'adapter leur traitement selon les niveaux suivants :

Niveau	Nature	Traitement attendu
Information	Événement ne nécessitant pas d'action immédiate	Traçabilité / analyse si nécessaire
Avertissement	Dégradation ou dépassement d'un seuil pouvant conduire à un incident	Analyse et action préventive
Majeur	Dysfonctionnement avéré affectant un composant ou un service	Qualification et prise en charge
Critique	Indisponibilité ou dégradation majeure d'un service critique	Prise en charge immédiate et processus incident

La criticité technique de l'alerte ne détermine pas à elle seule la priorité de l'incident.

Le Titulaire analyse l'impact de l'événement sur les services afin de déterminer la priorité de l'incident conformément à la matrice de priorité définie dans le processus de gestion des incidents.

6.2.1.5 Traitement des alertes de supervision et sécurité

Le Titulaire assure une surveillance permanente des alertes générées par les outils de supervision liés au périmètre réseau/sécurité et SOC

- Toute alerte nécessitant une action fait l'objet d'une qualification permettant :
- de confirmer la réalité de l'événement ;
- d'identifier le composant concerné ;
- d'évaluer son impact ;
- d'identifier les éventuels événements associés ;
- de déterminer les actions à engager ;
- de déclencher, lorsque nécessaire, le processus de gestion des incidents.

Le Titulaire applique les consignes et procédures définies pour les événements connus.

Lorsqu'une alerte correspond à un incident avéré, le Titulaire crée ou fait créer automatiquement un ticket d'incident dans l'outil ITSM et applique les dispositions prévues au chapitre relatif à la gestion des incidents.

Le traitement est alors soumis aux SLA correspondant à la priorité de l'incident.

Les alertes non pertinentes sont clôturées et capitalisées afin d'améliorer les mécanismes de détection.

6.2.1.6 Corrélation et prévention des incidents multiples

Le Titulaire met en œuvre les mécanismes permettant, dans la mesure des capacités des outils, de corréler les événements provenant d'une même cause.

L'objectif est notamment :

- d'éviter la création d'un nombre excessif d'incidents pour une même cause ;
- d'identifier les dépendances entre composants ;
- de faciliter l'identification du composant à l'origine du dysfonctionnement ;
- de réduire le bruit généré par la supervision ;
- de faciliter le diagnostic des équipes d'exploitation.

Lorsqu'un même événement affecte plusieurs composants ou services, le Titulaire privilégie la création d'un incident principal auquel sont rattachés les événements ou incidents associés, lorsque cette organisation est pertinente.

6.2.1.7 Supervision proactive

Le Titulaire ne limite pas son activité à la seule réaction aux seuils critiques.

Il analyse les événements et tendances permettant d'anticiper une dégradation du service.

Une attention particulière est portée notamment :

- à l'évolution des capacités ;
- à la saturation progressive des ressources ;
- aux dégradations de performance ;
- aux erreurs récurrentes ;
- aux échecs de traitements ;
- aux anomalies de sauvegarde ;
- aux expirations de certificats ;
- aux comportements inhabituels des composants supervisés.

Lorsqu'une évolution permet d'anticiper un incident, le Titulaire engage les actions relevant de son périmètre ou alerte le Pouvoir adjudicateur et formule les préconisations nécessaires.

6.2.1.8 Gestion des faux positifs et des alertes récurrentes

Le Titulaire assure l'analyse régulière de la pertinence des alertes générées.

Les faux positifs, alertes non pertinentes ou alertes répétitives sans action associée doivent faire l'objet d'une analyse.

Le Titulaire propose les adaptations nécessaires :

- modification des seuils ;
- modification des règles de déclenchement ;
- mise en place de temporisations ;
- amélioration des mécanismes de corrélation ;
- modification des procédures de traitement ;
- automatisation des actions lorsque cela est pertinent.

Toute modification susceptible de réduire le niveau de détection d'un service critique est soumise à validation préalable du Pouvoir adjudicateur.

6.2.1.9 Consignes de supervision

Les événements nécessitant une intervention récurrente font l'objet de consignes documentées.

Ces consignes précisent notamment :

- la signification de l'alerte ;
- les contrôles à effectuer ;
- les premières actions à réaliser ;
- les conditions d'ouverture d'un incident ;
- les règles de qualification et de priorité ;
- les éventuelles actions de rétablissement autorisées ;
- les critères d'escalade N1/N2/N3 ;
- les équipes à contacter ;

- les éléments à collecter pour faciliter le diagnostic.

Le Titulaire assure la mise à jour de ces consignes en fonction des incidents rencontrés et des retours d'expérience.

6.2.1.10 Amélioration continue

Le Titulaire procède régulièrement à une revue de la qualité et de la couverture de la supervision. Cette revue a notamment pour objectifs :

- d'identifier les composants insuffisamment supervisés ;
- d'identifier les contrôles devenus obsolètes ;
- d'améliorer la pertinence des seuils ;
- de réduire le nombre de faux positifs ;
- d'améliorer les mécanismes de corrélation ;
- d'identifier les possibilités d'automatisation ;
- d'améliorer la détection précoce des incidents ;
- de capitaliser sur les incidents et problèmes rencontrés.

Les incidents majeurs et les analyses de problèmes donnent systématiquement lieu à une vérification de la pertinence du dispositif de supervision.

Lorsque l'analyse d'un incident démontre qu'une détection plus précoce aurait été possible, le Titulaire propose les évolutions nécessaires afin d'éviter la répétition de cette situation.

6.2.2 Gestion des incidents

6.2.2.1 Principes généraux

Le Titulaire assure la gestion des incidents affectant les services et composants relevant du périmètre de la prestation, conformément aux bonnes pratiques ITIL.

La gestion des incidents a pour objectif de rétablir le service nominal dans les meilleurs délais, de limiter l'impact sur les utilisateurs et les activités du Pouvoir adjudicateur et d'assurer une communication adaptée pendant toute la durée de l'incident.

Le Titulaire assure notamment :

- la détection et/ou la prise en compte des incidents
- l'enregistrement et la traçabilité de chaque incident dans l'outil ITSM
- la qualification et la catégorisation
- l'évaluation de l'impact, de l'urgence et de la criticité
- la priorisation des incidents
- le diagnostic et la mise en œuvre des actions de résolution ou de contournement
- les escalades fonctionnelles, techniques et hiérarchiques nécessaires
- l'information régulière des parties prenantes
- la vérification du rétablissement du service

- la clôture documentée de l'incident
- la capitalisation des connaissances et le retour d'expérience

L'escalade d'un incident entre les niveaux N1, N2 et N3, ou sa transmission à un sous-traitant n'interrompt pas et ne réinitialise pas le calcul des délais contractuels.

6.2.2.2 Niveaux de prise en charge

Le dispositif de gestion des incidents repose sur plusieurs niveaux de prise en charge permettant une mobilisation progressive des compétences nécessaires à leur résolution, en fonction de la nature et de la complexité de l'incident.

Le premier niveau assure notamment la réception ou la détection de l'incident, son enregistrement, sa qualification, les premiers diagnostics et l'application des procédures et solutions documentées.

Lorsque l'incident ne peut être résolu à ce niveau, il est escaladé vers les niveaux d'expertise appropriés, y compris, lorsque nécessaire, vers les constructeurs, éditeurs ou partenaires du Titulaire.

L'escalade doit être réalisée en fonction de la complexité de l'incident, du niveau d'expertise requis et de la nécessité d'accélérer le rétablissement du service. Elle ne doit pas être conditionnée uniquement à l'expiration des délais de traitement.

L'escalade vers un niveau supérieur ne décharge pas le niveau ayant initialement pris en charge l'incident de ses obligations de suivi, de coordination et de transmission des informations nécessaires à la poursuite du traitement.

Le passage d'un niveau de support à un autre ne doit entraîner aucune interruption dans le traitement de l'incident ni remettre à zéro les engagements de service associés à celui-ci.

Le Titulaire organise ses niveaux de support de manière à respecter les engagements de prise en charge et de résolution définis au présent CCTP.

Escalade N1 / N2 / N3

L'escalade doit être réalisée en fonction de la complexité de l'incident et non uniquement à l'expiration des délais de traitement.

Pour les incidents P1 et P2, le Titulaire privilégie une mobilisation parallèle des compétences lorsque celle-ci est susceptible de réduire le délai de rétablissement.

L'escalade vers un niveau supérieur ne décharge pas le niveau ayant initialement pris en charge l'incident de ses obligations de suivi et de transmission des informations.

L'escalade entre les différents niveaux de support ne doit pas interrompre le traitement de l'incident ni remettre à zéro les engagements de service associés à celui-ci.

Le Titulaire reste responsable du pilotage de l'incident lorsque l'intervention d'un tiers est nécessaire et assure le suivi des actions jusqu'au rétablissement du service.

Gestion de crise et incidents critiques

Lorsqu'un incident présente un impact majeur, durable ou susceptible d'affecter significativement la continuité des activités, le Titulaire doit être en capacité d'activer ou de participer au dispositif de gestion de crise du Pouvoir adjudicateur.

Le Titulaire mettra à disposition du Pouvoir adjudicateur un responsable disposant de l'autorité et des compétences nécessaires pour coordonner ses différents intervenants. Celui-ci assure notamment sur son périmètre :

- la coordination des équipes techniques ;
- la centralisation des informations ;
- la tenue de la chronologie des événements et des actions entreprises ;
- le suivi des décisions et actions ;
- la coordination avec les éditeurs, constructeurs et prestataires tiers ;

De plus, il participera à :

- la production de points de situation réguliers ;
- l'estimation, lorsque cela est possible, du délai de rétablissement ;
- la préparation des éléments nécessaires à la communication auprès des parties prenantes.

6.2.2.3 Qualification et priorisation

Chaque incident fait l'objet d'une qualification permettant de déterminer son niveau de priorité. Elle est déterminée notamment en fonction :

- de l'impact sur les utilisateurs et les activités ;
- du nombre d'utilisateurs ou de services affectés ;
- de la criticité du service concerné ;
- de l'urgence de la situation ;
- de l'existence ou non d'une solution de contournement ;
- des risques opérationnels, techniques ou de sécurité associée.

La priorité d'un incident dépend de deux paramètres : la criticité et la sévérité de l'incident, autrement dit :

- Priorité = Criticité x Sévérité.

3 niveaux de priorités sont attendus :

- **P1 – Critique :** indisponibilité totale ou dégradation majeure d'un service critique, sans solution de contournement acceptable.

- **P2 – Majeur :** dégradation importante d'un service ou indisponibilité affectant significativement son fonctionnement, avec impact métier significatif.
- **P3 – Mineur :** incident à faible impact ne compromettant pas le fonctionnement général du service.

Les délais de prise en charge, de diagnostic, de rétablissement et, le cas échéant, de résolution associée à chaque priorité sont définis dans les engagements de niveaux de service (SLA) du marché.

La priorité d'un incident peut être réévaluée pendant son traitement en fonction de l'évolution de son impact.

Criticité

La **criticité** signifie l'urgence de traitement de l'incident déterminée par le périmètre. Une liste des différents périmètres de l'infogérance sera fournie au début du marché indiquant le niveau de criticité de chaque périmètre. Ces périmètres sont amenés à évoluer durant le marché avec l'accord des deux parties.

Sévérité

La **sévérité** signifie l'impact que peut avoir l'incident sur le métier en fonction du service, de l'application ou du matériel impacté et de la taille ou le type de population concernée.

Les niveaux de sévérité sont définis ainsi :

- Sévérité 1 : impact important, plus de 51 utilisateurs concernés
- Sévérité 2 : impact significatif, de 11 à 50 utilisateurs concernés
- Sévérité 3 : impact limité, de 1 à 10 utilisateurs concernés

Une liste d'utilisateurs VIP (COMEX, CODIR, etc) d'environ 10 personnes sera communiquée au début du marché. En cas d'incident impliquant ce groupe d'utilisateurs, le niveau de sévérité sera automatiquement réévalué du niveau 3 au niveau 2. Cette liste pourra être amenée à évoluer durant le marché avec l'accord des deux parties.

Matrice de qualification des niveaux de priorité

	Sévérité 1	Sévérité 2	Sévérité 3
Criticité 1	P1	P1	P2
Criticité 2	P1	P2	P3
Criticité 3	P2	P3	P3

Le Pouvoir adjudicateur se réserve la possibilité de demander une modification de la priorité lorsque son appréciation de l'impact métier diffère de celle du Titulaire.
La priorité peut également être réévaluée pendant le traitement de l'incident en fonction de l'évolution de son impact.

6.2.2.4 Événements et incidents de sécurité

Les événements et incidents de sécurité détectés ou qualifiés par le SOC font l'objet d'une classification spécifique selon leur niveau de sévérité :

- **S1 – Critique** : incident de sécurité avéré ou fortement probable présentant un impact majeur, une compromission significative, un risque important de propagation ou affectant un actif particulièrement critique ;
- **S2 – Majeur** : incident ou événement de sécurité présentant un risque significatif nécessitant une investigation et, le cas échéant, des mesures de confinement ou de remédiation rapides ;
- **S3 – Mineur** : événement ou incident de sécurité présentant un impact ou un risque limité et ne nécessitant pas d'intervention immédiate.

Cette classification permet de caractériser le niveau de risque cyber et est distincte de la priorité opérationnelle **P1, P2 ou P3**, laquelle détermine la mobilisation des équipes d'exploitation, la plage d'intervention et les SLA applicables.
Lorsqu'un événement de sécurité nécessite l'ouverture d'un incident, celui-ci est enregistré dans l'outil ITSM et traité selon les principes suivants :

Sévérité sécurité	**Situation**	**Priorité opérationnelle associée**
S1 – Critique	Compromission avérée ou fortement probable, impact majeur, propagation ou risque immédiat	**P1**
S2 – Majeur	Risque significatif nécessitant une investigation et/ou une action rapide	**P1 lorsque l'intervention technique ne peut être différée sans accroître le risque** ; à défaut, priorité définie selon impact et urgence
S3 – Mineur	Risque limité, événement sans impact immédiat ou action pouvant être planifiée	**P2 ou P3** selon impact et urgence

Lorsque le SOC et l'équipe chargée de la remédiation utilisent le même outil ITSM, le traitement est réalisé, sauf nécessité particulière, au travers d'un incident unique.
Le SOC demeure responsable de la qualification et de l'investigation de sécurité. Les équipes d'exploitation assurent les actions techniques de confinement, de remédiation et de rétablissement relevant de leur périmètre.
Lorsque l'intervention d'un autre prestataire ou d'une équipe utilisant un outil ITSM distinct est nécessaire, le Titulaire assure la coordination et la traçabilité entre les tickets correspondants.

6.2.2.5 Clôture des incidents

Un incident ne peut être considéré comme résolu sur la seule base de la disparition de l'alerte technique. Avant clôture, le Titulaire s'assure :

- du rétablissement effectif du service ;
- de la vérification du fonctionnement des composants concernés ;
- de la documentation des actions réalisées ;
- de l'identification de la solution définitive ou du contournement mis en œuvre ;
- de la mise à jour de la base de connaissances lorsque cela est pertinent.

La clôture de l'incident est tracée dans l'outil ITSM.

6.2.2.6 Rétablissement et résolution

Le rétablissement du service constitue l'objectif prioritaire de la gestion d'un incident. Lorsqu'une solution de contournement permet de restaurer le service, l'incident peut être considéré comme rétabli, sous réserve de validation de l'efficacité du contournement.
Il ne peut toutefois être considéré comme définitivement résolu lorsque :

- le contournement présente un caractère temporaire ;
- la cause du dysfonctionnement demeure active ;
- le risque de récurrence demeure significatif ;
- une action corrective complémentaire reste nécessaire.

Le Titulaire poursuit alors les investigations dans le cadre de l'incident ou, lorsque cela est pertinent, dans le cadre du processus de gestion des problèmes.

6.2.2.7 Retour d'expérience et capitalisation (REX)

Les incidents critiques (P1), récurrents ou présentant un intérêt particulier font l'objet d'une analyse a posteriori. Pour ces incidents, le Titulaire produit un rapport d'incident / retour d'expérience (REX) dans le délai défini par le marché.
Ce rapport comprend à minima :

- la description de l'incident ;
- son impact et sa durée ;
- la chronologie détaillée des événements ;
- les systèmes et services concernés ;
- les actions de diagnostic réalisées ;
- les mesures de contournement mises en œuvre ;
- les actions ayant permis le rétablissement ;
- l'analyse de la cause racine, lorsqu'elle est identifiée ;
- les difficultés rencontrées pendant le traitement ;
- les actions correctives et préventives proposées ;
- les responsables et échéances associés à ces actions.

Lorsque la cause racine ne peut être identifiée immédiatement, le Titulaire ouvre ou alimente un problème au sens ITIL afin d'en poursuivre l'analyse indépendamment de la clôture de l'incident.

6.2.2.8 Gestion des problèmes et prévention de la récurrence

Le Titulaire contribue à la gestion des problèmes afin de réduire le nombre et l'impact des incidents récurrents.
Les incidents présentant des caractéristiques similaires doivent pouvoir être rapprochés afin d'identifier les tendances et causes communes. Le Titulaire assure notamment :

- l'identification des incidents récurrents ;
- la proposition d'ouverture de problèmes ;
- la réalisation ou la contribution aux analyses de causes racines ;
- l'identification des solutions de contournement ;
- la proposition d'actions correctives ou préventives ;
- le suivi des actions issues des analyses de problèmes ;
- L'alimentation de la base des erreurs connues et de la base de connaissances.

6.2.3 Gestion des demandes

6.2.3.1 Principes généraux

Le Titulaire assure la gestion des demandes de service relevant du périmètre de la prestation conformément aux bonnes pratiques ITIL.

Une demande de service correspond à une sollicitation du Pouvoir adjudicateur ne résultant pas d'une interruption ou d'une dégradation non planifiée d'un service.

La gestion des demandes a notamment pour objectifs :

- d'assurer une prise en charge homogène et traçable des demandes ;
- de standardiser et d'industrialiser les opérations récurrentes ;
- de garantir des délais de prise en charge et d'exécution adaptés à la nature des demandes ;
- d'assurer la traçabilité des actions réalisées ;
- de maîtriser les demandes nécessitant une charge ou une expertise particulière ;
- de permettre au Pouvoir adjudicateur de maîtriser les coûts et les délais associés aux demandes non standardisées.

Toute demande est enregistrée et suivie dans l'outil ITSM mis à disposition dans le cadre du marché.

6.2.3.2 Catalogue de services

Le Titulaire prend en charge les demandes standardisées définies dans le catalogue de services.

Le catalogue constitue le référentiel des prestations récurrentes pouvant être commandées dans le cadre de la prestation.

Le catalogue de services sur l'ensemble du périmètre sera consolidé et validé lors de la phase d'initialisation sans impact financier puis sera maintenu à jour pendant toute la durée du marché.

Le Titulaire est force de proposition pour son enrichissement, notamment lorsque des demandes initialement non standardisées deviennent suffisamment récurrentes et maîtrisées pour faire l'objet d'une procédure standard.

Toute évolution du catalogue ou des SLA associés est soumise à validation préalable du Pouvoir adjudicateur.

6.2.3.3 Classification des demandes

Les demandes sont réparties en deux catégories.

Demandes standardisées

Une demande standardisée correspond à une opération :

- identifiée dans le catalogue de services ;
- disposant d'une procédure connue et maîtrisée ;
- reproductible ;
- dont les prérequis sont identifiés ;
- dont la charge de réalisation est connue ;
- et dont la charge totale nécessaire à son exécution est maitrisée

Ces demandes sont réalisées dans le cadre de la prestation d'infogérance et sont soumises aux SLA définis dans le catalogue de services.

En fonction de son impact et de son périmètre, une demande pourra nécessiter la validation du N3. Ces demandes seront définies et convenues pendant la phase d'initialisation entre le Titulaire et le Pouvoir adjudicateur.

Les demandes standard ne nécessitent pas l'établissement d'un devis spécifique.

Demandes nécessitant une prestation spécifique

Toute demande non standard fera obligatoirement l'objet d'un chiffrage spécifique préalable. Il en est de même lorsqu'une demande, indépendamment de sa charge estimée :

- ne figure pas au catalogue de services ;
- nécessite une étude ou une expertise particulière ;

- présente une complexité ne permettant pas l'application d'une procédure standardisée ;
- nécessite la mobilisation exceptionnelle de plusieurs compétences ;
- ou entraîne une modification significative de l'environnement technique.

Dans ce cas, le Titulaire ne peut engager les travaux de réalisation sans validation préalable du Pouvoir adjudicateur.

Le chiffrage est établi sur la base des Unités d'Œuvre (UO) applicables à la prestation concernée et des tarifs unitaires définis au BPU.

Lorsque la demande ne correspond pas directement à une prestation standard du catalogue, le Titulaire précise les UO mobilisées, les quantités estimées ainsi que les éventuelles hypothèses retenues pour établir son devis.

6.2.3.4 Qualification et priorisation

À réception d'une demande, le Titulaire procède à sa qualification.

Il vérifie notamment :

- la nature de la demande ;
- son appartenance au catalogue ;
- la complétude des informations ;
- les prérequis ;
- les autorisations nécessaires ;
- la procédure applicable ;
- la charge prévisionnelle de réalisation.

Lorsque la demande est standardisée, son exécution est engagée conformément au SLA applicable.

Lorsque la demande n'est pas standard ou nécessite une prestation spécifique, il en informe le Pouvoir adjudicateur et engage la procédure de chiffrage.

Le Titulaire ne peut procéder artificiellement au découpage d'une même demande en plusieurs demandes unitaires afin de maintenir les SLA.

L'appréciation de la charge porte sur l'ensemble des travaux nécessaires à l'atteinte du résultat demandé.

Gestion des changements associés aux demandes

Certaines demandes peuvent nécessiter une modification du Système d'Information pour être satisfaites.

Lorsqu'une demande implique une modification de configuration, d'équipement, de logiciel, de règle ou de service relevant de son périmètre, le Titulaire assure notamment :

- l'identification des demandes nécessitant l'ouverture d'un changement ;
- la qualification de la nature et du niveau de risque du changement ;
- la proposition ou l'ouverture du changement associé dans l'outil ITSM ;
- l'analyse des impacts et des éventuelles dépendances ;
- la préparation des modalités de mise en œuvre et, lorsque nécessaire, du plan de retour arrière ;
- la soumission du changement aux validations requises ;
- la planification et la coordination de sa mise en œuvre ;
- le suivi du changement jusqu'à sa réalisation et à la vérification du bon fonctionnement du service ;
- le maintien du lien entre la demande initiale et le changement associé afin d'assurer la traçabilité complète du traitement.

Les modalités détaillées de gestion des changements seront définies et formalisées lors de la phase d'initialisation, en déclinaison du processus de gestion des demandes.

Cette phase permettra notamment de définir les différentes catégories de changements, les niveaux de validation associés, les circuits de décision, les exigences de traçabilité, les modalités de planification ainsi que les conditions de recours à des procédures accélérées pour les changements urgents.

Le recours au processus de gestion des changements doit rester proportionné à la nature et au niveau de risque de la modification envisagée. Les opérations récurrentes, maîtrisées et préalablement autorisées peuvent notamment relever du processus de changement standard.

6.2.3.5 Chiffrage des demandes spécifiques

Pour toute demande nécessitant un chiffrage, le Titulaire le transmet au Pouvoir adjudicateur. Il comprend a minima :

- la description et la compréhension du besoin ;
- le périmètre de l'intervention ;
- les hypothèses et prérequis ;
- les travaux à réaliser ;
- les profils ou compétences nécessaires ;
- la charge estimée, exprimée en jours/homme ;
- le délai prévisionnel de réalisation ;
- la date prévisionnelle de démarrage ;
- les éventuelles contraintes techniques ;
- les risques identifiés ;
- les éventuelles indisponibilités ou interruptions de service nécessaires ;
- le coût de la prestation, établi conformément aux prix prévus au marché.

Lorsque plusieurs solutions sont envisageables, le Titulaire présente les différentes options et leurs impacts respectifs lorsque cela est pertinent.

Validation et engagement des travaux

Aucune prestation spécifique ne peut être engagée sans validation explicite du devis par le Pouvoir adjudicateur. La validation porte notamment sur :

- le périmètre ;
- la charge ;
- le coût ;
- le calendrier ;
- les livrables ou résultats attendus.

La validation du devis constitue le point de départ de l'engagement de réalisation correspondant.

Le Titulaire ne peut facturer une charge supérieure au montant validé sans accord préalable du Pouvoir adjudicateur.

Lorsqu'un dépassement devient prévisible en cours de réalisation, le Titulaire suspend les travaux concernés, sauf nécessité opérationnelle ou accord contraire, et transmet un chiffrage complémentaire pour validation.

6.2.3.6 Exécution des demandes spécifiques

Après validation du devis, le Titulaire réalise la demande conformément aux engagements approuvés.

Le suivi de la demande est assuré dans l'outil ITSM ou dans l'outil de suivi de projet convenu avec le Pouvoir adjudicateur. Le Titulaire assure la traçabilité :

- de la date de validation ;
- du démarrage des travaux ;
- des actions réalisées ;
- des éventuelles difficultés ;
- des modifications de planning ;
- de la date de réalisation ;
- de la validation du résultat.

Tout retard prévisible doit être signalé sans attendre l'échéance contractuelle.

6.2.3.7 Clôture des demandes

Une demande ne peut être clôturée qu'après :

- réalisation des actions demandées ;
- vérification de leur bonne exécution ;

- Si demandé, renseignement des actions réalisées dans l'outil ITSM ;
- production des éventuels livrables ;
- mise à jour de la documentation lorsque nécessaire.

Pour les demandes spécifiques, la clôture intervient après validation du résultat par le Pouvoir adjudicateur et la signature d'un PV de livraison.

6.2.3.8 Capitalisation et industrialisation

Le Titulaire analyse régulièrement les demandes reçues afin d'identifier les opérations pouvant être standardisées, automatisées ou intégrées au catalogue.

Une attention particulière est portée :

- aux demandes récurrentes ;
- aux demandes nécessitant régulièrement un chiffrage similaire ;
- aux opérations présentant un potentiel d'automatisation ;
- aux demandes dont les délais de réalisation pourraient être réduits par une amélioration des procédures.

Le Titulaire propose au Pouvoir adjudicateur les évolutions du catalogue permettant d'améliorer la qualité, les délais ou l'efficacité de la prestation.

L'intégration d'une nouvelle demande au catalogue et la définition du SLA correspondant sont soumises à validation du Pouvoir adjudicateur.

6.2.4 Patch Management – Gestion des correctifs

Le Titulaire met en œuvre un processus de Patch Management permettant d'assurer une gestion régulière, maîtrisée et traçable des versions et correctifs applicables aux équipements, logiciels, firmwares et composants relevant de son périmètre.

Ce processus vise à maintenir les composants dans un état stable, supporté et sécurisé et s'inscrit dans une démarche à la fois préventive, planifiée et corrective.

Il s'appuie notamment sur une **veille technique et éditeur continue**, sur le suivi des vulnérabilités et des cycles de vie des produits, ainsi que sur le plan annuel de maintenance prévisionnel défini pour le périmètre.

6.2.4.1 Veille et identification des correctifs

Le Titulaire assure une veille continue portant notamment sur :

- les nouvelles versions et correctifs disponibles ;
- les bulletins de sécurité et recommandations des constructeurs et éditeurs ;
- les vulnérabilités identifiées par le SOC, les outils de détection, les éditeurs, le CERT-FR ou toute autre source pertinente ;
- les fins de support, fins de maintenance et situations d'obsolescence ;

- les évolutions susceptibles d'affecter la stabilité, la sécurité ou la compatibilité des composants exploités.

Les versions, correctifs et évolutions identifiées font l'objet d'une analyse permettant de déterminer leur applicabilité au contexte du Pouvoir adjudicateur.

6.2.4.2 Maintenance préventive et planifiée

Le Patch Management s'inscrit dans une démarche proactive et ne doit pas reposer uniquement sur la survenance d'un incident ou l'identification d'une vulnérabilité.

Le Titulaire met en œuvre un plan annuel de maintenance prévisionnel couvrant les équipements, logiciels et composants relevant de son périmètre et propose une fréquence de maintenance adaptée aux différentes technologies concernées.

Ce plan intègre notamment :

- les campagnes régulières d'application des correctifs ;
- les montées de version nécessaires au maintien dans des versions supportées et recommandées ;
- les opérations permettant de prévenir l'obsolescence ;
- les évolutions rendues nécessaires par les recommandations des constructeurs et éditeurs ;
- les contraintes de compatibilité, de dépendance et de disponibilité associées aux opérations prévues.

Le plan annuel de maintenance est actualisé en fonction des évolutions du périmètre, des recommandations des constructeurs et éditeurs, des risques identifiés et des contraintes d'exploitation.

6.2.4.3 Maintien des niveaux de version

Le Titulaire veille à maintenir les équipements et solutions dans des versions supportées, stables et recommandées par les éditeurs ou constructeurs.

Sauf contrainte technique dûment justifiée et validée par le Pouvoir adjudicateur, les composants exploités ne doivent pas présenter un retard supérieur à :

- une (1) version majeure par rapport à la version stable recommandée par l'éditeur ;
- deux (2) versions mineures au sein d'une même branche majeure supportée.

Lorsqu'un dépassement de ces seuils est identifié, le Titulaire propose un plan de mise à niveau précisant les risques, prérequis, impacts et calendrier de réalisation.

6.2.4.4 Fins de support et de l'obsolescence

Le processus de Patch Management intègre le suivi des cycles de vie des équipements, logiciels, firmwares et composants relevant du périmètre du Titulaire.

À ce titre, le Titulaire assure notamment le suivi :

- des dates de fin de support ;
- des fins de maintenance ;
- des fins de vie annoncées par les constructeurs et éditeurs ;
- des versions ne bénéficiant plus de correctifs de sécurité ;
- des dépendances ou incompatibilités susceptibles de contraindre les évolutions futures.

Le Titulaire informe le Pouvoir adjudicateur suffisamment en amont de toute échéance susceptible d'affecter le maintien en conditions opérationnelles ou de sécurité et propose les actions nécessaires de mise à niveau, migration, renouvellement ou remplacement.

Les seuils de notification, niveaux d'alerte, délais d'anticipation et modalités de suivi associés sont définis et validés avec le Pouvoir adjudicateur lors de cette phase, puis ajustés si nécessaire pendant la durée du marché.

6.2.4.5 Analyse et qualification

Avant toute mise en œuvre, le Titulaire analyse notamment :

- la criticité et l'urgence du correctif ou de la montée de version ;
- sa stabilité et les recommandations de l'éditeur ou du constructeur ;
- sa compatibilité avec les équipements, logiciels et dépendances existantes ;
- les risques de régression ;
- les prérequis techniques éventuels ;
- les impacts sur la disponibilité des services ;
- les modalités de sauvegarde et de retour arrière nécessaires.

Le choix d'une version ou d'un correctif à déployer ne doit pas résulter de sa seule disponibilité, mais d'une analyse de son intérêt, de sa stabilité et de ses impacts sur l'environnement concerné.

6.2.4.6 Classification des correctifs

À l'issue de l'analyse, les correctifs sont classés selon leur niveau de criticité afin d'adapter leur priorité et leurs modalités de traitement.

P1- Critique

Relèvent notamment de cette catégorie les correctifs répondant :

- à une vulnérabilité critique ;

- à une vulnérabilité activement exploitée ;
- à une vulnérabilité présentant un niveau de risque élevé au regard de l'exposition du composant concerné ;
- à un bulletin de sécurité nécessitant une action prioritaire ;
- à une demande expresse du Pouvoir adjudicateur justifiée par le niveau de risque.

P2- Majeur

Correctif de sécurité, de stabilité ou de fiabilité présentant un risque significatif pour le Système d'Information, sans nécessiter pour autant un traitement immédiat.

P3- Mineur

Correctif de maintenance, de stabilité ou de sécurité présentant un niveau de risque limité et pouvant être intégré aux campagnes de maintenance planifiées.

La classification tient notamment compte, lorsque ces éléments sont disponibles :

- de la criticité publiée par l'éditeur ou le constructeur ;
- du score CVSS ;
- de l'exposition du composant ;
- de l'existence d'un exploit connu ou d'une exploitation active ;
- de la criticité du service ou du composant concerné ;
- de l'existence de mesures compensatoires ;
- des recommandations des organismes de référence ou autorités compétentes.

La classification retenue doit tenir compte du contexte propre au Système d'Information et ne saurait reposer uniquement sur la criticité générique publiée par l'éditeur.

Le Pouvoir adjudicateur peut demander la reclassification d'un correctif lorsque le risque métier, opérationnel ou de sécurité le justifie.

6.2.4.7 Gestion corrective et urgente

Lorsqu'un incident, une vulnérabilité critique, une alerte de sécurité ou un risque significatif nécessite une remédiation rapide, le Titulaire met en œuvre un traitement adapté au niveau d'urgence. Les actions peuvent notamment comprendre :

- l'application accélérée d'un correctif ;
- une montée ou une descente de version ;
- une modification de configuration ;
- la mise en œuvre d'une mesure compensatoire ;
- toute autre action permettant de supprimer ou de réduire le risque identifié.

Le caractère urgent d'un correctif ne dispense pas le Titulaire d'évaluer les risques liés à son déploiement et de prévoir les mesures de sécurisation adaptées à la situation.

6.2.4.8 Gestion des exceptions et mesures compensatoires

Lorsqu'un correctif ne peut être déployé dans les délais prévus en raison d'une incompatibilité, d'un risque de régression, d'une contrainte d'exploitation ou de toute autre contrainte technique dûment justifiée, le Titulaire documente l'exception.

Cette documentation précise notamment :

- la raison du report ;
- le risque associé ;
- les composants concernés ;
- les mesures compensatoires proposées ;
- la durée prévisionnelle de l'exception ;
- la date cible de mise en conformité.

Les mesures compensatoires peuvent notamment comprendre :

- la restriction des flux ;
- le durcissement de la configuration ;
- la désactivation temporaire d'une fonctionnalité ;
- le renforcement de la supervision ;
- la segmentation ;
- la mise en œuvre de mesures de filtrage complémentaires ;
- la limitation des accès.

Les mesures retenues doivent être adaptées au risque identifié et permettre de réduire l'exposition du composant dans l'attente de sa mise en conformité.

Toute exception aux délais de patching applicables doit être documentée et soumise à validation du Pouvoir adjudicateur.

Une exception ne constitue pas une dérogation permanente. Le Titulaire maintient le suivi du correctif concerné jusqu'à sa mise en œuvre, son remplacement par une solution définitive ou la disparition dûment justifiée du risque associé.

6.2.4.9 Préparation, déploiement et retour arrière

Les opérations de patching sont préparées de manière à limiter les risques de régression ou d'interruption de service.

Le Titulaire prévoit, lorsque cela est pertinent :

- les tests préalables ;
- la vérification des sauvegardes ;
- la définition d'un plan de retour arrière ;
- les contrôles post-déploiement nécessaires à la vérification du bon fonctionnement des composants et services concernés.

À l'issue de l'intervention, le Titulaire vérifie le bon fonctionnement des composants et services concernés et assure la traçabilité des opérations réalisées et des éventuels écarts constatés.

6.2.4.10 Articulation avec les autres processus

Le Patch Management s'articule notamment avec :

- la gestion des vulnérabilités et les alertes remontées par le SOC ;
- la gestion des incidents lorsqu'un correctif est nécessaire au rétablissement ou à la sécurisation du service ;
- la gestion des demandes et changements pour la validation et la planification des opérations ;
- le plan annuel de maintenance prévisionnel.

Le Titulaire assure la traçabilité des correctifs appliqués, différés ou non applicables ainsi que des exceptions, décisions, mesures compensatoires et risques associés.

6.2.4.11 Suivi et gouvernance du Patch Management

Le Patch Management fait l'objet d'un suivi dans les instances de gouvernance.

Le comité opérationnel présente notamment :

- les campagnes réalisées ;
- les campagnes à venir ;
- les correctifs critiques ;
- les échecs ;
- les composants non conformes ;
- les exceptions ;
- les risques identifiés.

Le COPIL présente notamment :

- l'évolution du taux de conformité ;
- les dépassements de SLA ;
- les principales exceptions ;
- les risques significatifs ;

Les écarts récurrents donnent lieu à un plan d'amélioration

6.2.5 Gestion de la documentation et de la connaissance

Le Titulaire met en œuvre une gestion structurée de la documentation et de la connaissance permettant de garantir la disponibilité, la fiabilité, l'actualisation et la transmission des informations nécessaires à l'exploitation du périmètre.

La documentation constitue un élément à part entière de la prestation et doit être maintenue à jour pendant toute la durée du marché.

Le Titulaire assure notamment :

- la création et la mise à jour de la documentation technique et d'exploitation relevant de son périmètre ;
- la mise à jour des procédures, modes opératoires et consignes nécessaires à l'exploitation courante ;
- la capitalisation des diagnostics, solutions de contournement, erreurs connues et méthodes de résolution issues du traitement des incidents et problèmes ;
- la documentation des changements, mises à jour, évolutions d'architecture et opérations significatives réalisées ;
- la mise à jour des référentiels techniques, inventaires, schémas et informations de configuration relevant de son périmètre ;
- l'alimentation et le maintien de la base de connaissances ;
- la mise à disposition des informations nécessaires aux autres intervenants autorisés par le Pouvoir adjudicateur.

6.2.5.1 Mise à jour de la documentation

Toute opération entraînant une modification durable de l'environnement technique, d'une configuration, d'une architecture, d'une procédure ou d'un mode opératoire doit donner lieu, lorsque nécessaire, à une mise à jour de la documentation associée.

La mise à jour documentaire fait partie intégrante de la prestation et ne doit pas être considérée comme une action facultative ou distincte de l'opération réalisée.

Le Titulaire veille notamment à éviter la conservation de procédures obsolètes ou contradictoires susceptibles de compromettre la qualité de l'exploitation.

6.2.5.2 Capitalisation de la connaissance

Le Titulaire organise la capitalisation des connaissances acquises au cours de la prestation afin de limiter la dépendance aux connaissances individuelles des intervenants.

Les éléments présentant un intérêt pour le traitement d'événements futurs sont intégrés dans la base de connaissances et mis à disposition des équipes concernées.

Cette capitalisation porte notamment sur :

- les incidents significatifs ou récurrents ;
- les problèmes et causes racines identifiés ;
- les solutions de contournement ;
- les erreurs connues ;
- les procédures de diagnostic et de résolution ;

- les spécificités techniques du périmètre ;
- les retours d'expérience issus des opérations ou changements réalisés.

6.2.5.3 Validation de la documentation

Toute création d'un nouveau document ou modification significative d'un document existant fait obligatoirement l'objet d'une étape de révision avant sa mise en application ou sa publication définitive.

Le Titulaire assure la préparation et la revue initiale du document et le soumet au Pouvoir adjudicateur pour validation.

La documentation ne peut être considérée comme approuvée tant que cette validation n'a pas été formalisée par le Pouvoir adjudicateur.

Le processus de validation permet notamment de vérifier :

- la conformité du contenu avec l'environnement effectivement exploité ;
- la cohérence avec les autres documents et référentiels existants ;
- le niveau de détail et la qualité des informations fournies ;
- la prise en compte des exigences techniques, organisationnelles et de sécurité applicables ;
- l'identification correcte de la version et de la date de mise à jour.

En cas de demande de correction ou de complément formulée par le Pouvoir adjudicateur, le Titulaire met à jour le document et le soumet à nouveau à validation.

Les modalités détaillées de revue, d'approbation et de gestion des versions documentaires sont définies lors de la phase d'initialisation.

6.2.5.4 Référentiel documentaire

Le Titulaire met en place et maintient un référentiel permettant d'assurer le suivi consolidé de la documentation relevant de la prestation.

Ce référentiel constitue la source de référence permettant d'identifier les documents existants, leur état d'avancement, leur version et leur emplacement.

Il comporte à minima, pour chaque document :

- le domaine ou périmètre technique concerné ;
- le type de document (DAT , DEX , FEX , etc. …) ;
- le titre du document ;
- une description ou un objet synthétique ;
- la version en vigueur ;
- le statut du document ;
- la date de création ;
- la date de dernière mise à jour ;

- la date de dernière validation ;
- l'auteur ou responsable de la mise à jour ;
- le valideur ;
- l'emplacement ou le lien d'accès au document ;
- les éventuels documents ou référentiels associés ;
- la prochaine date de revue lorsque celle-ci est applicable.

Les statuts utilisés permettent notamment de distinguer les documents en cours de rédaction, en cours de révision, soumis à validation, validés et obsolètes ou archivés.

Le Titulaire maintient ce référentiel à jour pendant toute la durée de la prestation et s'assure de sa cohérence avec les documents effectivement disponibles.

Les modalités de structuration, de stockage et de gestion du référentiel documentaire sont définies avec le Pouvoir adjudicateur lors de la phase d'initialisation.

6.2.5.5 Qualité et accessibilité de la documentation

La documentation produite ou mise à jour par le Titulaire doit être exploitable, structurée, compréhensible et suffisamment détaillée pour permettre son utilisation par un intervenant disposant des compétences adaptées.

Elle est conservée dans les espaces ou outils définis avec le Pouvoir adjudicateur et demeure accessible à celui-ci pendant toute la durée du marché.

Les formats, règles de nommage, niveaux de détail attendus, modalités de validation et outils de gestion documentaire sont précisés lors de la phase d'initialisation.

6.2.5.6 Transmission et réversibilité

Le Titulaire veille à ce que la connaissance nécessaire à l'exploitation ne repose pas exclusivement sur ses propres équipes ou outils.

Les documents, procédures, bases de connaissances et éléments techniques produits dans le cadre de la prestation doivent pouvoir être transmis et exploités dans le cadre d'un changement d'intervenant ou d'une opération de réversibilité.

Le Titulaire contribue, lorsque nécessaire, au transfert de connaissances vers le Pouvoir adjudicateur ou tout tiers désigné par celui-ci.

6.2.6 Amélioration continue

Le Titulaire inscrit l'ensemble des processus de la prestation dans une démarche d'amélioration continue.

À ce titre, il analyse périodiquement leur fonctionnement, leur efficacité et leur adéquation avec les besoins du Pouvoir adjudicateur afin d'identifier les éventuels ajustements ou actions d'amélioration nécessaires pendant la durée du marché.

Cette analyse peut notamment s'appuyer sur :

- les incidents, problèmes et récurrences constatés ;
- les écarts aux engagements de service ;
- les retours d'expérience issus des opérations réalisées ;
- les indicateurs et tendances observés dans le cadre du reporting ;
- les évolutions du périmètre, des technologies ou des risques ;
- les recommandations des constructeurs, éditeurs ou organismes de référence.

Le Titulaire propose au Pouvoir adjudicateur les actions d'amélioration identifiées et, après validation, assure leur mise en œuvre et leur suivi.

Les évolutions significatives apportées aux processus, procédures ou modes opératoires sont documentées et intégrées à la documentation de la prestation.

6.3 Gouvernance et pilotage

Le Titulaire met en place un dispositif de gouvernance permettant d'assurer le suivi opérationnel, contractuel et stratégique des prestations d'infogérance Réseau, Sécurité et SOC.

Ce dispositif repose sur des instances de pilotage, des reportings périodiques et des indicateurs permettant d'évaluer la qualité de service, de suivre les engagements contractuels, d'anticiper les risques et de piloter les actions d'amélioration continue.

Le Titulaire est responsable de la préparation, de l'animation et du suivi des instances de gouvernance. Il assure la production des supports, tableaux de bord et comptes rendus associés.

Les modalités de fonctionnement, les participants et les supports de gouvernance sont précisés et validés avec le Pouvoir adjudicateur lors de la phase d'initialisation, dans le respect des exigences du présent CCTP.

6.4 Instances de pilotage

La gouvernance de la prestation s'articule autour de trois instances complémentaires, correspondant à différents niveaux de pilotage.

6.4.1 Comité technique (COTECH)

Le COTECH constitue l'instance de suivi opérationnel de la prestation. Il permet de faire le point sur les activités réalisées et en cours, d'identifier les difficultés rencontrées, de coordonner les interventions et de suivre les actions nécessaires au bon fonctionnement des services.

Il réunit les interlocuteurs opérationnels et techniques du Titulaire et du Pouvoir adjudicateur.

Les sujets abordés comprennent notamment :

Infogérance Réseau et Sécurité

- le suivi des incidents, demandes et problèmes ;
- les incidents significatifs et leurs actions correctives ;
- le suivi des changements et des opérations planifiées ;
- l'état de la supervision et de la disponibilité des services ;
- les performances, capacités et éventuelles dégradations ;
- le suivi des correctifs, versions et opérations de maintenance ;
- les difficultés opérationnelles et points de blocage ;
- l'avancement des plans d'action et des opérations à venir.

Infogérance SOC

- le suivi des alertes et événements de sécurité significatifs ;
- les incidents de sécurité et investigations en cours ;
- les vulnérabilités identifiées et les actions de remédiation ;
- l'état de la collecte et de la supervision des sources ;
- les anomalies de fonctionnement des outils SOC ;
- les campagnes de Threat Hunting et leurs résultats ;
- les évolutions et ajustements des cas d'usage de détection ;
- les actions opérationnelles en cours ou à planifier.

Le COTECH permet également de suivre les écarts opérationnels par rapport aux engagements de service et de définir les actions correctives nécessaires.

6.4.2 Comité de pilotage (COPIL)

Le COPIL constitue l'instance de suivi de la performance globale et de la bonne exécution du marché.

Il permet d'évaluer la qualité des prestations, d'examiner le respect des engagements contractuels, de suivre les risques et de procéder aux arbitrages relevant de son niveau de responsabilité.

Le COPIL s'appuie sur les indicateurs et reportings consolidés produits par le Titulaire.

Les sujets abordés comprennent notamment :

Infogérance Réseau et Sécurité

- la synthèse de la qualité et de la continuité des services ;
- le bilan des incidents majeurs et des problèmes récurrents ;
- le respect des engagements de service (SLA) ;
- l'évolution de la volumétrie des incidents et demandes ;
- la disponibilité, la capacité et la performance des infrastructures ;

- le bilan des changements et des opérations de maintenance ;
- le suivi des plans d'amélioration et des risques opérationnels ;
- le suivi des volumes contractuels, des consommations et des prestations complémentaires ;
- les éventuels écarts contractuels et les mesures correctives associées.

Infogérance SOC

- le bilan de l'activité et des incidents de sécurité ;
- l'évolution des menaces et des risques identifiés ;
- la performance opérationnelle du SOC et le respect des SLA ;
- l'efficacité et l'évolution de la couverture de détection ;
- le suivi des vulnérabilités significatives et de leur remédiation ;
- l'évolution de la surface d'attaque et de l'exposition aux risques ;
- le bilan des activités de Threat Intelligence et de Threat Hunting ;
- le suivi des actions d'amélioration du dispositif SOC.

Le COPIL examine également les éléments contractuels et financiers de la prestation, notamment les éventuels dépassements de volumétrie, les prestations sur devis et les évolutions du périmètre.

Il valide les plans d'action et les orientations relevant de ses attributions, dans les limites des dispositions contractuelles applicables au marché.

6.4.3 Comité stratégique (COSTRAT)

Le COSTRAT constitue l'instance de gouvernance stratégique de la prestation.

Il permet de disposer d'une vision globale de l'évolution des services, d'anticiper les besoins futurs, d'examiner les risques majeurs et de définir les orientations structurantes à moyen et long terme.

Les sujets abordés comprennent notamment :

Infogérance Réseau et Sécurité

- le bilan global de la prestation et de son évolution ;
- les évolutions du périmètre et des besoins du Pouvoir adjudicateur ;
- les risques majeurs relatifs à la disponibilité et à la sécurité des infrastructures ;
- les enjeux d'obsolescence et les trajectoires technologiques ;
- les projets et évolutions structurantes ;
- les orientations et opportunités d'amélioration continue.

Infogérance SOC

- l'évolution du contexte de menace et de la posture de cybersécurité ;
- la maturité et la performance globale du dispositif SOC ;

- l'évolution de la couverture et des capacités de détection ;
- les risques cyber majeurs et les besoins de renforcement du dispositif ;
- les évolutions technologiques et fonctionnelles des outils SOC ;
- les orientations de la feuille de route cybersécurité.

Le COSTRAT permet de partager les perspectives d'évolution, de définir les priorités stratégiques et de préparer les arbitrages nécessaires.

6.5 Modalités communes aux instances

Les fréquences des différentes instances sont définies au chapitre : **9.2.1 *SLA – Gouvernance et pilotage.***

Pour chaque instance, le Titulaire assure :

- la préparation de l'ordre du jour et des supports de présentation ;
- la consolidation et l'analyse des informations nécessaires ;
- l'animation des échanges ;
- la rédaction et la diffusion du compte rendu ;
- le suivi des décisions et des actions engagées.

Les comptes rendus précisent notamment les décisions prises, les actions à réaliser, les responsables désignés et les échéances associées.

Le Titulaire tient à jour un plan d'action consolidé, partagé avec le Pouvoir adjudicateur, permettant d'assurer la traçabilité et le suivi des actions jusqu'à leur clôture.

Des réunions exceptionnelles peuvent être organisées à la demande du Pouvoir adjudicateur lorsque la situation opérationnelle, contractuelle ou sécuritaire le justifie.

6.6 Reporting et indicateurs

Le Titulaire assure la production et la mise à disposition des reportings nécessaires au suivi de la prestation, à l'évaluation de sa performance et au contrôle du respect des engagements contractuels.

Les informations présentées doivent être fiables, actualisées, exploitables et adaptées au niveau de pilotage concerné.

Les reportings couvrent l'ensemble du périmètre Réseau, Sécurité et SOC. Ils permettent de disposer d'une vision consolidée de la prestation tout en distinguant les activités et indicateurs propres à chaque domaine.

6.6.1 Météo quotidienne des services

Le Titulaire fournit chaque jour ouvré une météo des services présentant une synthèse de l'état opérationnel du périmètre infogéré.

Cette météo a pour objectif d'informer le Pouvoir adjudicateur de l'état des services, des événements significatifs survenus depuis la précédente communication et des situations nécessitant une attention ou une intervention particulière.

Elle comprend notamment :

Infogérance Réseau et Sécurité

- l'état de disponibilité des principaux services et infrastructures ;
- les incidents P1/P2 en cours ou survenus depuis la précédente météo ;
- les incidents significatifs non résolus et les dégradations connues ;
- les opérations significatives réalisées ou programmées ;
- les anomalies de supervision et les éventuelles pertes de visibilité ;
- les risques opérationnels identifiés et les actions en cours ;
- les points nécessitant une intervention ou une décision du Pouvoir adjudicateur.

Infogérance SOC

- les événements et incidents de sécurité significatifs, notamment S1/S2 ;
- les événements majeurs survenus depuis la précédente météo ;
- les nouvelles vulnérabilités critiques affectant potentiellement le périmètre ;
- les anomalies significatives de collecte ou de fonctionnement du dispositif SOC ;
- les nouvelles expositions ou menaces nécessitant une vigilance particulière ;
- les actions de sécurité nécessitant une attention du Pouvoir adjudicateur.

La météo quotidienne est mise à disposition avant le début de la plage de service définie par le Pouvoir adjudicateur, selon les modalités et l'horaire validés lors de la phase d'initialisation.

Elle est présentée sous une forme synthétique permettant d'identifier rapidement l'état général des services, les situations dégradées et les actions prioritaires.

6.6.2 Tableaux de bord et indicateurs de performance (KPI)

Le Titulaire met à disposition du Pouvoir adjudicateur des tableaux de bord permettant de suivre l'activité, la qualité de service et la performance des prestations.

Les indicateurs couvrent notamment les domaines suivants :

Domaine	**Principaux indicateurs attendus**
Gestion des incidents	Volumétrie et répartition par priorité, délais de prise en charge et de résolution, respect des SLA, incidents récurrents
Gestion des demandes	Volumétrie et typologie, délais de traitement, respect des SLA, suivi des volumes contractuels et des prestations sur devis

Supervision et disponibilité	Disponibilité des services, alertes significatives, incidents détectés par la supervision, pertes de supervision, capacité et performance
Gestion des changements	Nombre et nature des changements, taux de réussite, changements ayant généré des incidents
MCO / MCS	État des versions, conformité des composants, suivi des correctifs et des opérations de maintenance
Activité SOC	Volumétrie des alertes et événements de sécurité, répartition par criticité, incidents détectés et traités, investigations réalisées
Performance SOC	Délais de qualification et de traitement, respect des SLA, couverture de détection, état de la collecte, faux positifs
Vulnérabilités	Nombre et criticité des vulnérabilités, évolution du stock, délais et état d'avancement des remédiations
Amélioration continue	Actions engagées, avancement des plans d'amélioration, principales évolutions et résultats obtenus

Ces indicateurs constituent le socle minimal du reporting attendu. Ils peuvent être complétés par des indicateurs spécifiques aux activités ou aux outils mis en œuvre, en fonction des besoins de pilotage identifiés.

Les indicateurs associés aux engagements contractuels doivent permettre de vérifier le respect des objectifs définis au chapitre « Engagements de service (SLA) ».

Le Titulaire veille à la cohérence entre les données issues des différents outils de ticketing, de supervision et du SOC.

Les modalités de calcul, les sources de données et les règles de consolidation sont documentées et validées avec le Pouvoir adjudicateur lors de la phase d'initialisation.

Les tableaux de bord et reportings sont mis à disposition du Pouvoir adjudicateur selon des modalités définies lors de la phase d'initialisation.

Ils doivent permettre la consultation des résultats historiques et leur export dans des formats courants et exploitables.

6.7 Phase d’initialisation

La phase d’initialisation a pour objectif de permettre au Titulaire de prendre en charge le périmètre de la prestation dans des conditions maîtrisées, en assurant la continuité de service, l’appropriation de l’environnement existant et la mise en place des dispositifs nouveaux prévus au marché.

Cette phase recouvre deux situations distinctes :

- pour le périmètre **Infogérance Réseau et Sécurité**, il s'agit principalement d'une **reprise de l'existant**, le service étant déjà opéré. La phase d'initialisation devra permettre au Titulaire de reprendre les activités, de consolider sa connaissance de l'environnement, d'actualiser le périmètre technique et documentaire et de s'assurer de sa capacité à assurer le service en régime nominal sans rupture de service ;
- pour le périmètre **SOC**, il s'agit d'une **phase de construction et de mise en service d'un nouveau dispositif**, comprenant notamment la définition de l'organisation technique et opérationnelle , l'intégration des sources de données, la mise en œuvre des cas d'usage de détection, la définition des procédures de traitement et d'escalade ainsi que la préparation du passage en exploitation.

Le Titulaire devra adapter son organisation, son planning et les ressources mobilisées à ces deux situations.

6.7.1 Organisation et ressources mobilisées

Le Titulaire met en place, dès le démarrage du marché, une organisation dédiée à la phase d'initialisation disposant des compétences et des moyens nécessaires à la reprise du périmètre existant et à la construction du dispositif SOC.

Le Titulaire désigne a minima les ressources suivantes :

- **Un Chef de projet (Transition Manager)**, chargé du pilotage global de la phase d'initialisation, de la coordination des différentes parties prenantes, du suivi du planning, des risques, des actions et des livrables associés jusqu'à la mise en exploitation;
- **Un Responsable de service ou Service Delivery Manager**, garant de la mise en place du dispositif de gouvernance, des processus de gestion de service, des indicateurs, des SLA et des modalités de fonctionnement en régime nominal ;
- **Un référent technique Réseau et Sécurité**, chargé notamment de la reprise de connaissance de l'environnement existant, de la validation du périmètre, de la revue des architectures, configurations, procédures et documentations et de l'identification des éventuels écarts ou risques de reprise ;
- **Un référent SOC**, disposant de l'expertise nécessaire pour piloter la conception et la mise en œuvre du dispositif de supervision de sécurité, des règles de détection, des procédures opérationnelles et des modalités d'escalade ;
- **Les experts techniques nécessaires**, mobilisés selon les technologies, solutions et domaines concernés afin d'assurer les opérations de transfert de connaissances, de revue documentaire, d'intégration, de paramétrage et de validation ;

Le Titulaire veille à assurer une passation suffisante entre les ressources mobilisées pendant la phase d'initialisation et celles qui assureront ensuite l'exploitation courante du service.

6.7.2 Reprise du périmètre Infogérance Réseau et Sécurité

Pour le périmètre Réseau et Sécurité, le Titulaire devra organiser la reprise des activités existantes en garantissant la continuité des services. Cette reprise comprend notamment :

- la prise de connaissance des architectures, équipements, configurations et flux ;
- la revue et l'appropriation de la documentation existante ;
- l'identification et la validation des équipements et solutions inclus dans le périmètre ;
- l'actualisation de l'inventaire et des référentiels techniques ;
- la revue des procédures d'exploitation, de supervision, de sauvegarde, de gestion des incidents, des changements et des vulnérabilités ;
- la reprise des outils, accès, comptes techniques et mécanismes d'administration nécessaires à l'exploitation ;
- l'identification des écarts, risques, obsolescences ou insuffisances documentaires ;
- la formalisation, le cas échéant, d'un plan d'actions de mise à niveau.

La reprise ne devra entraîner aucune interruption ou dégradation évitable du service.

Le Titulaire est tenu de signaler au Pouvoir adjudicateur tout écart constaté entre le périmètre contractuel, l'inventaire documentaire disponible et la réalité technique observée lors de la phase d'initialisation.

6.7.3 Construction et mise en service du SOC

Le Pouvoir adjudicateur ne disposant pas actuellement d'un SOC, le Titulaire assure, dans le cadre de la phase d'initialisation, la **conception, la construction, le déploiement et la mise en service du dispositif SOC**.

Cette phase doit permettre de définir conjointement avec le Pouvoir adjudicateur **l'architecture technique cible du SOC, son organisation opérationnelle, ainsi que le modèle de fourniture, d'hébergement, d'acquisition et d'exploitation des outils et services associés**, préalablement à leur mise en œuvre.

La mise en œuvre du SOC pourra être réalisée de manière progressive afin de permettre une montée en puissance maîtrisée du dispositif, notamment au regard de l'intégration successive des sources, des cas d'usage et des capacités de détection.

Il précisera notamment les modalités d'articulation et d'interaction entre les différentes capacités mobilisées dans le cadre de la prestation, notamment les fonctions SOC, CERT/CSIRT, Threat Intelligence, Threat Hunting, intégration et infogérance.

Le passage en exploitation nominale intervient après réalisation des travaux prévus, validation des livrables et tests attendus, et **signature du procès-verbal de validation de la phase d'initialisation par le Pouvoir adjudicateur**.

6.7.3.1 SIEM

La solution SIEM étant identifiée dans l'offre du candidat, la phase d'initialisation a pour objet d'en confirmer l'architecture, le dimensionnement et les modalités de mise en œuvre.

Le Titulaire assure notamment :

- la finalisation de l'architecture technique cible ;
- la confirmation ou l'ajustement du dimensionnement ;
- la souscription ou l'acquisition de la solution pour le compte du Pouvoir Adjudicateur ;
- le déploiement et le paramétrage des composants nécessaires ;
- l'intégration des sources et la configuration des mécanismes de collecte et de conservation ;
- la mise en œuvre des premiers cas d'usage et règles de détection ;
- la définition des procédures opérationnelles, d'escalade et de traitement ;
- la réalisation des tests nécessaires ;
- la validation du dispositif avant passage en exploitation nominale.

Dimensionnement

La volumétrie exacte des événements de sécurité à collecter n'est pas connue à la date de publication du marché.

Pour le dimensionnement et le chiffrage de la solution SIEM, le candidat retient une volumétrie de référence de **50 Go de journaux ingérés par jour.**

Le candidat précise le dimensionnement technique et le modèle de licence ou de souscription correspondant à cette volumétrie, ainsi que les capacités de conservation associées.

Cette volumétrie constitue la base de dimensionnement à prendre en compte dans l'offre, indépendamment de l'estimation que le candidat pourrait établir à partir du périmètre du Système d'Information décrit dans le présent CCTP.

Si le candidat estime que cette volumétrie présente un écart significatif avec le dimensionnement qu'il juge adapté au regard des informations de sizing fournies dans le CCTP et ses annexes, il peut le préciser et le justifier dans sa réponse technique.

Il indique alors la volumétrie qu'il estime adaptée, les hypothèses et éléments techniques ayant conduit à cette estimation ainsi que, à titre informatif, les conséquences éventuelles sur le dimensionnement et le coût de la solution.

Cette estimation alternative ne se substitue pas à la volumétrie de référence retenue pour le chiffrage de l'offre.

La volumétrie réelle est mesurée pendant la phase d'initialisation. Le dimensionnement pourra, le cas échéant, être ajusté selon les modalités et prix prévus au marché.

6.7.3.2 Détection et au suivi des vulnérabilités

Dans le cadre du dispositif SOC, le Titulaire met en œuvre les moyens et outillages nécessaires à la détection, à la qualification et au suivi des vulnérabilités sur les différents niveaux de couverture définies au présent CCTP.

Le candidat décrit dans son offre le dispositif proposé en s'appuyant, lorsque cela est pertinent, sur les outils déjà présents dans le Système d'Information et sur les composants de la chaîne SOC.

Il identifie les éventuelles capacités complémentaires nécessaires pour atteindre le niveau de couverture attendu et précise, pour chacune d'elles :

- la fonction couverte ;
- la solution ou le service proposé ;
- son mode de fourniture et d'hébergement ;
- ses modalités d'intégration avec le SOC et le SIEM ;
- les éventuels prérequis ;
- les coûts associés compris dans le forfait.

Le dispositif proposé doit permettre de couvrir les exigences de détection et de suivi des vulnérabilités définies au présent CCTP.

6.7.4 Gouvernance spécifique

Pendant la phase d'initialisation, une gouvernance renforcée est mise en place.

Elle comprend a minima :

- une réunion de lancement ;
- des points de suivi réguliers adaptés au rythme de la transition ;
- un suivi formalisé du planning, des actions, des risques et des décisions ;
- un suivi distinct des travaux de reprise Réseau/Sécurité et des travaux de construction du SOC ;
- une revue de fin de phase permettant de constater la capacité du Titulaire à assurer les services concernés en régime nominal.

La fréquence des points de suivi pourra être adaptée par le Pouvoir adjudicateur en fonction de l'avancement, des risques identifiés ou des difficultés rencontrées.

La fin de la phase d'initialisation pourra être prononcée de manière différenciée entre le périmètre **Infogérance Réseau et Sécurité** et le périmètre **SOC**, lorsque leur niveau de maturité ou leur calendrier de mise en service le justifie.

Elle reste, dans tous les cas, soumise à la validation expresse du Pouvoir adjudicateur sur la base des critères, livrables et conditions de passage en régime nominal définis au marché. Le seul écoulement de la durée prévisionnelle de la phase d'initialisation ne saurait valoir validation de celle-ci. La clôture de la phase d'initialisation est conditionnée à la validation expresse du Pouvoir adjudicateur, matérialisée par la signature d'un procès-verbal de fin d'initialisation attestant de la réalisation des travaux, de la remise des livrables attendus et de l'aptitude du Titulaire à assurer le service en régime nominal.

6.7.5 Validation de la phase d'initialisation

Le passage en exploitation intervient après validation des travaux et livrables attendus et **signature du procès-verbal de validation de la phase d'initialisation par le Pouvoir adjudicateur**.

Le seul écoulement de la durée prévisionnelle de la phase d'initialisation ne saurait valoir validation de celle-ci.

6.8 Réversibilité

A la fin du marché, ou en cas de rupture anticipée du marché, il est demandé au Titulaire de s'engager à restituer l'ensemble des données et compétences qui permettront d'assurer une transition fluide vers un nouveau prestataire ou vers les ressources internes du Pouvoir adjudicateur.

Le Titulaire doit fournir un plan de réversibilité qui détaille une méthode claire décrivant l'ensemble des étapes du transfert avant la signature du contrat, accompagné d'un calendrier précis qui fixe la durée de la réversibilité et les jalons clés à respecter.

Le Titulaire doit fournir par ailleurs un inventaire complet des matériels, logiciels, configurations, données, règles, cas d'usage historiques, scripts, comptes, contrats de licence et accès utilisés, ainsi que les dépendances vis-à-vis de ses propres outils. Il doit aussi restituer toutes les données en sa possession qui appartiennent au Pouvoir adjudicateur, dans un format standard, lisible et exploitable.

Il doit prouver qu'il a bien supprimé, de manière sécurisée, toutes les données dans ses propres systèmes qui appartiennent au Pouvoir Adjudicateur après le transfert.

Concernant la documentation technique, le Titulaire s'engage à restituer les plans techniques, les codes d'administration, clés de sécurité, procédures d'exploitation, modes opératoires qui permettent de gérer la prestation.

En termes de transfert de compétences, le Titulaire doit s'engager à travailler en coactivité sur la période avec le nouveau prestataire ou les équipes internes du Pouvoir Adjudicateur afin d'assurer la continuité de service. Lors de cette période, le Titulaire forme et accompagne les équipes qui reprennent la main pour expliquer les particularités de la prestation.

La continuité de service doit être assurée normalement par le Titulaire, des pénalités financières sont prévues si le Titulaire bloque ou retarde le transfert.

7 Engagements de service (SLA)

7.1 Définitions des différents délais

Afin d'éviter toute ambiguïté dans la mesure des niveaux de service, les notions suivantes sont distinguées.

7.1.1 Délai de prise en charge

Durée entre la détection ou le signalement de l'incident et le début effectif de son traitement par le Titulaire.

La simple création automatique d'un ticket ne constitue pas une prise en charge. Celle-ci doit correspondre au début effectif des opérations de qualification ou de diagnostic.

7.1.2 Délai de qualification

Durée nécessaire pour confirmer l'incident, déterminer son impact, son niveau de priorité et identifier les premiers composants ou services susceptibles d'être concernés.

7.1.3 Délai de rétablissement

Durée entre la détection ou le signalement de l'incident et le retour du service à un niveau de fonctionnement permettant son utilisation dans des conditions acceptables.

Le rétablissement peut résulter :

- d'une correction définitive ;
- de la mise en œuvre d'une solution de contournement ;
- d'une restauration ;
- d'un retour arrière ;
- ou de toute autre mesure permettant le rétablissement du service.

7.1.4 Délai de résolution

Durée nécessaire pour apporter une solution définitive à l'incident lorsque le rétablissement a été obtenu au moyen d'une solution temporaire.

Le rétablissement du service ne dispense donc pas le Titulaire de poursuivre les investigations nécessaires à la résolution définitive lorsque celle-ci est nécessaire.

7.2 Niveaux et engagements de service (SLA)

7.2.1 Principes généraux

Le Titulaire est soumis aux engagements de niveaux de service définis dans le présent chapitre.

Les engagements sont mesurés à partir des données issues de l'outil ITSM, des outils de supervision, des outils de communication et des différents livrables produits dans le cadre de la prestation.

Sauf disposition contraire :

- Les délais associés aux incidents P1 sont calculés 24h/24 et 7j/7 ;
- Les délais associés aux incidents P2 et P3 et aux demandes de service sont calculés en heures ou jours ouvrés ;
- Le transfert d'un ticket entre les niveaux N1, N2 et N3 ne suspend ni ne réinitialise les SLA ;
- L'intervention d'un éditeur, constructeur ou prestataire tiers ne suspend pas automatiquement les SLA ;
- Toute suspension d'un SLA doit être justifiée, documentée dans l'outil ITSM et validée par le Pouvoir adjudicateur.

7.2.2 Mesure du rétablissement

Les délais associés aux engagements de service sont mesurés à partir de l'événement déclencheur correspondant à la nature de la prestation.
Sauf mention contraire, les délais indiqués ne sont pas cumulatifs

Le délai de rétablissement est calculé entre :
T0 : détection de l'incident par la supervision ou signalement de l'incident
et
T1 : retour du service à un niveau de fonctionnement acceptable.

Le rétablissement peut résulter d'une correction définitive ou d'une solution de contournement validée.

Lorsqu'une solution de contournement est utilisée, le Titulaire poursuit les actions nécessaires à la résolution définitive dans le cadre de l'incident ou du processus de gestion des problèmes.

7.2.3 SLA – Supervision 24/7

La supervision est assurée 24h/24 et 7j/7 sur les composants définis dans le référentiel de supervision.

Engagement	SLA
Prise en compte d'une alerte	≤ 15 min
Qualification d'une alerte	≤ 15 min
Création de l'incident associé	≤ 15 min après qualification
Perte de supervision d'un composant : détection	≤ 15 min
Perte de supervision : prise en charge	≤ 15 min
Rétablissement de la supervision d'un composant	≤ 2 h
Intégration d'un nouveau composant à la supervision	≤ 3 jours ouvrés après fourniture des prérequis
Mise à jour d'une règle ou d'un seuil	≤ 1 jours ouvrés
Correction d'une alerte identifiée comme faux positif	≤ 3 jours ouvrés

Une alerte conduisant à la qualification d'un incident est ensuite soumise aux SLA du processus de gestion des incidents.

7.2.4 SLA – Gestion des incidents

Engagement	P1 – Critique	P2 – Majeur	P3 – Mineur
Plage surveillance et qualification	24/7	24/7	24/7
Prise en charge	≤ 15 min	≤ 15 min	≤ 15 min
Qualification initiale	≤ 30 min	≤ 30 min	≤ 30 min
Escalade N2 si nécessaire	≤ 45 min	≤ 1 h	≤ 4 h
Escalade N3 si nécessaire	≤ 2 h	≤ 4 h	≤ 8 h
Plage de rétablissement	24/7	HO	HO
Objectif de rétablissement	≤ 4 h	≤ 8 h	≤ 2 jours ouvrés
Ouverture cellule de crise	≤ 4 h	Selon criticité / évolution	Non
Incident Manager	Si cellule crise	Si nécessaire	Non
Fréquence d'information cellule de crise	Toutes les 2 h	Toutes les 4 h	Selon nécessité
REX	Obligatoire	Selon critères définis au CCTP	Sur demande

7.2.5 SLA – Gestion des événements de sécurité par le SOC

Engagement	P1 – Critique	P2 – Majeur	P3 – Mineur
Plage surveillance et qualification	24/7	24/7	24/7

Engagement	P1 – Critique	P2 – Majeur	P3 – Mineur
Prise en charge	≤ 15 min	≤ 15 min	≤ 15 min
Qualification initiale	≤ 30 min	≤ 30 min	≤ 30 min
Escalade expertise SOC N2/N3	≤ 45 min	≤ 2 h	≤ 1 jour ouvré
Mobilisation des équipes de remédiation (ouverture ticket)	≤ 1 h	≤ 3 h	≤ 1 h
Ouverture / participation à une cellule de crise	≤ 2 h	Selon criticité / évolution	Non
Mobilisation du CERT/CSIRT après déclenchement	≤ 1 h	≤ 2 h	≤ 1 jour ouvré
Première restitution de l'investigation CERT/CSIRT	≤ 24 h après mobilisation	≤ 48 h après mobilisation	≤ 72 h après mobilisation
Rapport préliminaire d'investigation	≤ 3 jours ouvrés	≤ 5 jours ouvrés	≤ 7 jours ouvrés
Rapport final d'investigation	≤ 2 jours ouvrés après clôture des investigations	≤ 3 jours ouvrés après clôture des investigations	≤ 5 jours ouvrés après clôture des investigations

7.2.6 SLA – Activités récurrentes du SOC

En complément des engagements applicables au traitement des événements et incidents de sécurité, le Titulaire assure les activités récurrentes de Threat Intelligence et de Threat Hunting selon les fréquences minimales définies ci-dessous.

Activité	Engagement	Fréquence / délai
Threat Intelligence	Veille, collecte et qualification des informations relatives aux menaces susceptibles d'affecter le Système d'Information	Continue
Threat Intelligence	Analyse et contextualisation des menaces présentant un intérêt	Au fil de l'eau
Threat Intelligence	Prise en compte d'une menace critique identifiée comme directement applicable au Système d'Information	≤ 4 h après identification
Threat Intelligence	Restitution synthétique des menaces, tendances et évolutions significatives	Mensuelle
Threat Hunting	Réalisation d'une campagne planifiée de Threat Hunting	A minima 1 campagne par mois

Threat Hunting	Déclenchement d'une campagne complémentaire à la suite d'un incident, d'une menace identifiée, d'une vulnérabilité critique ou d'un signal justifiant une recherche proactive	Selon nécessité
Threat Hunting	Lancement d'une campagne demandée par le Pouvoir adjudicateur	≤ 1 jour ouvré après validation de la demande
Threat Hunting	Restitution des résultats d'une campagne	≤ 5 jours ouvrés après clôture de la campagne

Les enseignements issus des activités de Threat Intelligence et de Threat Hunting sont exploités, lorsque cela est pertinent, pour améliorer les règles de détection, les cas d'usage du SOC, les investigations et les mesures de protection du Système d'Information.

7.2.7 SLA – REX Incident

Engagement	**SLA**
Chronologie initiale après rétablissement	≤ 1 jour ouvré
REX préliminaire	≤ 2 jours ouvrés
REX définitif	≤ 5 jours ouvrés
Plan d'actions associé	Avec le REX définitif
Exécution du plan actions	≤ 2 jours ouvrés après validation du REX
Mise à jour base de connaissances	≤ 5 jours ouvrés après validation du REX

Le REX doit comporter à minima la chronologie, l'analyse des causes, les actions réalisées, les enseignements et les actions correctives ou préventives.

Chaque action issue d'un REX comporte obligatoirement un responsable, une échéance et un statut.

7.2.8 SLA – Gestion des demandes

7.2.8.1 Demande Standard

Chaque demande Standard dispose dans le catalogue d'un SLA d'exécution spécifique.
Les engagements généraux sont les suivants :

Engagement	**Demande Standard**
Prise en charge et Qualification initiale	SLA défini dans le catalogue

Engagement	Demande Standard
Réalisation	SLA défini dans le catalogue
SLA maximum par défaut	≤ 5 jours ouvrés
Information en cas de blocage	≤ 1 jour ouvré

Le catalogue peut prévoir des SLA plus contraignants pour certaines demandes courantes. Le SLA d'exécution débute lorsque la demande est complète et que les autorisations et prérequis nécessaires sont disponibles.

7.2.8.2 Demande chiffrée – Sur devis

Engagement	SLA
Prise en charge de la demande	≤ 4 h ouvrées
Qualification initiale	≤ 1 jour ouvré
Information sur la nécessité d'un devis	≤ 1 jour ouvré
Devis simple	≤ 2 jours ouvrés
Devis nécessitant une étude technique	≤ 5 jours ouvrés
Accusé de réception de la validation du devis	≤ 1 jour ouvré
Planification après validation	≤ 2 jours ouvrés
Réalisation	Selon délai contractuellement validé dans le devis

7.2.8.3 Démarrage des prestations et mobilisation des ressources

La transmission d'un devis, d'un chiffrage ou d'une proposition de profil ne saurait être considérée comme satisfaisant à elle seule à l'engagement de service lorsque la disponibilité effective des ressources proposées ne permet pas de réaliser la prestation dans les délais attendus. Le Titulaire garantit une capacité de mobilisation des ressources compatibles avec les besoins du Pouvoir adjudicateur et les engagements contractuels de la prestation.

Engagement	SLA
Démarrage de la prestation	≤ 15 jours ouvrés, sauf délai dérogatoire expressément validé ou convenu avec le Pouvoir adjudicateur
Réalisation	Selon le délai contractuellement validé dans le devis

Tout délai dérogatoire doit faire l'objet d'un accord préalable du Pouvoir adjudicateur. L'absence de ressources disponibles chez le Titulaire ne constitue pas, à elle seule, un motif de suspension ou de dépassement du SLA.

Lorsque les délais de mobilisation ou de réalisation proposés par le Titulaire ne sont pas compatibles avec les contraintes ou besoins du Pouvoir adjudicateur, celui-ci se réserve le droit de ne pas donner suite au devis ou à la proposition concernée et de faire réaliser la prestation par un autre prestataire.

7.2.9 SLA – Traitement des correctifs sécurité

Les délais sont calculés à compter de la date à laquelle le correctif est publié et identifié comme applicable au périmètre.

Niveau	**Analyse d'applicabilité**	**Planification**	**Déploiement maximum**
P1- Critique	≤ 1 jour ouvré	≤ 2 jours ouvrés	≤ 7 jours calendaires
P2- Majeur	≤ 3 jours ouvrés	≤ 5 jours ouvrés	≤ 30 jours calendaires
P3- Mineur	≤ 5 jours ouvrés	Selon cycle mensuel	≤ 60 jours calendaires

7.2.9.1 Vulnérabilité de sécurité activement exploitée

Les engagements définis dans la présente section concernent exclusivement les correctifs répondant à une vulnérabilité ou à un risque de sécurité

Pour une vulnérabilité critique activement exploitée ou explicitement identifiée comme urgente par le Pouvoir adjudicateur :

Engagement	**SLA**
Analyse initiale	≤ 4 h
Identification des composants exposés	≤ 8 h
Proposition d'une mesure de réduction du risque	≤ 24 h
Correctif ou mesure compensatoire	≤ 48 h lorsque techniquement possible
Déploiement définitif	Selon risque et validation du Pouvoir adjudicateur

Lorsqu'un correctif ne peut être appliqué dans le délai prévu, les dispositions relatives aux exceptions et mesures compensatoires définies dans le processus de Patch Management s'appliquent.

7.2.10SLA – Conformité des versions et maintenance préventive

Les correctifs de maintenance, correctifs de stabilité et montées de version ne relevant pas d'un traitement de sécurité urgent, sont pris en charge dans le cadre du plan annuel de maintenance prévisionnel. Le Titulaire assure le suivi du niveau de conformité des équipements, logiciels et composants relevant de son périmètre au regard :

- des versions supportées par les constructeurs et éditeurs ;
- des niveaux de versions cibles définis au présent CCTP ;
- des opérations prévues au plan annuel de maintenance ;
- des éventuelles exceptions validées par le Pouvoir adjudicateur.

Taux de conformité des versions

Le taux de conformité des versions correspond au rapport entre :

Nombre de composants respectant le niveau de version attendu / Nombre total de composants relevant du périmètre concerné.

Indicateur	**Objectif**	**Fréquence**
Composants respectant les niveaux de version attendus	**≥ 95 %**	Trimestriel
Composants en version non supportée sans dérogation validée	**0 %**	Trimestriel
Composants dépassant les seuils de version autorisés et non planifiée	**0 %**	Trimestriel
Opérations de maintenance réalisées dans l'échéance planifiée	**≥ 90 %**	Trimestriel

Les composants faisant l'objet d'une exception technique formalisée et validée par le Pouvoir adjudicateur sont identifiés séparément dans le reporting.

7.2.11 SLA – Gouvernance et pilotage

7.2.11.1 Météo quotidienne des services

Engagement	**SLA**
Production météo	Chaque jour ouvré
Disponibilité	Avant 9h
Exactitude / actualisation	Situation arrêtée au plus près de la production
Correction d'une information erronée significative	≤ 1 h après signalement

7.2.11.2 Comité technique (COTECH)

Engagement	**SLA**
Comité technique (COTECH)	Hebdomadaire
Mise à jour des données	Données arrêtées au plus tard à J-1
Compte rendu	≤ 1 jours ouvrés après le comité
Mise à jour du plan d'actions	≤ 1 jour ouvré après validation du CR

7.2.11.3 Comité de Pilotage (COPIL)

Engagement	**SLA**
Comité de Pilotage (COPIL)	Trimestriel
Transmission du support COPIL	J-3 ouvrés
Données du support	Trimestre précédent consolidé
Correction demandée sur le support	≤ 1 jour ouvré
Compte rendu COPIL	≤ 3 jours ouvrés
Plan d'actions actualisé	Avec le compte rendu

7.2.11.4 Comité stratégique (COSTRAT)

Engagement	**SLA**
Comité de Pilotage (COSTRAT)	Annuel
Transmission du support COSTRAT	J-7 ouvrés
Données du support	L'année en cours consolidé
Correction demandée sur le support	≤ 2 jour ouvré
Compte rendu COSTRAT	≤ 5 jours ouvrés
Plan d'actions actualisé	Avec le compte rendu

7.2.11.5 Base documentaire et de connaissances (KB)

Le Titulaire assure la tenue à jour de la documentation nécessaire à l'exploitation.

Engagement	**SLA**
Documentation après changement standard	≤ 2 jours ouvrés
Documentation après changement significatif	≤ 5 jours ouvrés
Mise à jour documentation après REX	≤ 5 jours ouvrés après validation REX
Création/mise à jour fiche KB	≤ 2 jours ouvrés

Engagement	SLA
Correction documentaire demandée	≤ 2 jours ouvrés
Revue générale documentaire	Au minimum annuelle

La documentation doit être stockée dans les espaces désignés par le Pouvoir adjudicateur et demeure accessible à celui-ci.

7.2.12 SLA – Phase d'initialisation

La phase d'initialisation débute à compter de la date de démarrage des prestations convenue entre les Parties.

Le Titulaire est soumis aux engagements suivants :

Engagement	SLA
Organisation de la réunion de lancement	≤ 10 jours ouvrés à compter de la date de démarrage des prestations
Présentation du planning prévisionnel d'initialisation	Lors de la réunion de lancement
Démarrage des ateliers techniques relatifs à l'infogérance réseau et sécurité	≤ 10 jours ouvrés après la réunion de lancement
Mise en œuvre opérationnelle de l'infogérance réseau et sécurité	≤ 2 mois après la réunion de lancement
Démarrage des ateliers techniques relatifs au SOC	≤ 10 jours ouvrés après la réunion de lancement
Mise en œuvre opérationnelle du SOC	≤ 4 mois après la réunion de lancement

Pour les engagements relatifs à la mise en œuvre opérationnelle de l'infogérance réseau et sécurité et du SOC, une période de tolérance maximale d'un mois calendaire est accordée au Titulaire au-delà du délai contractuel indiqué ci-dessus.

À l'issue de cette période de tolérance, tout dépassement non justifié par un retard imputable au Pouvoir adjudicateur ou par un événement expressément accepté par celui-ci est susceptible d'entraîner l'application des pénalités prévues au marché.

7.2.13 Mesure de la performance globale

En complément du respect unitaire des SLA, le Titulaire est soumis à des objectifs mensuels de qualité.

Indicateur	Objectif	Fréquence
Respect prise en charge P1, P2 et P3	**≥ 90 %**	Mensuel

Indicateur	Objectif	Fréquence
Respect rétablissement P1 et P2	**100 %**	Mensuel
Respect rétablissement P3	**≥ 95 %**	Mensuel
Respect prise en charge des demandes (Standard et chiffrée)	**≥ 95 %**	Mensuel
Respect réalisation des demandes (Standard et chiffrée)	**≥ 95 %**	Mensuel
Respect des délais de mobilisation des ressources et de démarrage des prestations	**≥ 95 %**	Trimestriel
Production météo dans les délais	**≥ 90 %**	Mensuel
Reporting / supports de gouvernance dans les délais	**≥ 90 %**	Trimestriel
REX P1 produits dans les délais	**≥ 95 %**	Trimestriel
Disponibilité des outils fournis pour la prestation	**≥ 99 %**	Mensuel

Les résultats sont présentés au COPIL et font l'objet d'une analyse des écarts

Tout écart significatif ou récurrent donne lieu à la mise en œuvre d'un plan d'amélioration soumis au Pouvoir adjudicateur.

8 Exigences techniques et de sécurité

8.1 Exigences techniques générales

Le Titulaire réalise les prestations en tenant compte de l'architecture, des standards, des contraintes techniques, opérationnelles, réglementaires et des règles d'exploitation du Système d'Information du Pouvoir adjudicateur. À ce titre, il doit notamment :

- garantir la compatibilité des solutions, équipements, logiciels et configurations proposés avec l'environnement existant ;
- respecter les standards techniques et règles d'architecture définis par le Pouvoir adjudicateur ;
- privilégier les versions maintenues et supportées par les éditeurs et constructeurs ;
- ne pas introduire, sans validation préalable, de composant susceptible de créer une dépendance technique, une incompatibilité ou une régression ;
- respecter les prérequis, recommandations et matrices de compatibilité des constructeurs et éditeurs ;
- limiter autant que possible les configurations spécifiques ou non standards susceptibles de complexifier l'exploitation ou les évolutions futures ;
- garantir la réversibilité des configurations, paramétrages et données nécessaires à l'exploitation ;
- maintenir une documentation technique suffisante permettant au Pouvoir adjudicateur ou à un tiers autorisé de reprendre l'exploitation des composants concernés.

Toute évolution susceptible d'avoir un impact significatif sur l'architecture, la sécurité, les performances, les flux, la disponibilité ou l'interopérabilité du Système d'Information est soumise à validation préalable du Pouvoir adjudicateur.

Le Titulaire doit également signaler toute obsolescence matérielle ou logicielle, fin de support constructeur ou éditeur, incompatibilité ou risque technique identifié sur le périmètre dont il assure l'exploitation.

8.2 Exigences liées à l'utilisation l'IA

L'utilisation de solutions ou de services reposant sur des technologies d'intelligence artificielle dans le cadre de l'exécution des prestations est soumise aux exigences du présent chapitre.

Le Pouvoir adjudicateur se réserve le droit de demander au Titulaire la liste des outils ou fonctionnalités d'intelligence artificielle utilisés dans le cadre de la prestation ainsi que leurs conditions d'utilisation.

Le Titulaire doit informer préalablement le Pouvoir adjudicateur de tout recours à une solution, un service ou une fonctionnalité reposant sur de l'intelligence artificielle dans le cadre de l'exécution des prestations. Cette information doit notamment préciser :

- la solution ou le service utilisé ;
- son éditeur ou fournisseur ;
- son mode de mise à disposition, notamment SaaS, service cloud, solution on-premise ou composant intégré à un outil existant ;
- la finalité et les usages envisagés dans le cadre de la prestation ;
- la nature des données susceptibles d'être transmises, analysées ou traitées ;
- les lieux d'hébergement et de traitement des données ;
- lorsque cela est applicable, les conditions d'hébergement, d'exécution ou de mise à disposition du modèle d'intelligence artificielle ;
- les éventuels sous-traitants ou fournisseurs tiers impliqués dans le traitement ;
- les conditions de conservation, de réutilisation ou d'utilisation des données aux fins d'entraînement ou d'amélioration des modèles.

Le recours à une telle solution est soumis à l'autorisation préalable du Pouvoir adjudicateur lorsque son utilisation implique la transmission, le traitement ou l'hébergement de données appartenant au Pouvoir adjudicateur. Sont notamment concernés :

- les configurations des équipements ;
- les journaux techniques ou de sécurité ;
- les adresses IP, noms de machines et informations d'architecture ;
- les règles de pare-feu et politiques de sécurité ;
- les scripts et codes spécifiques ;
- les données issues des outils de supervision ou du SOC ;
- les informations relatives aux vulnérabilités ou incidents de sécurité ;
- les identifiants, secrets, certificats, clés ou jetons d'authentification ;
- les données à caractère personnel ;
- plus généralement, toute information non publique relative au Système d'Information du Pouvoir adjudicateur.

Lorsque l'utilisation d'une solution d'intelligence artificielle est autorisée, le Titulaire doit garantir que :

- les données transmises ne sont pas utilisées pour entraîner ou améliorer des modèles accessibles à des tiers, sauf accord explicite du Pouvoir adjudicateur ;
- les conditions d'hébergement et de traitement des données sont compatibles avec les exigences contractuelles et réglementaires applicables ;
- les accès à la solution sont maîtrisés et tracés ;
- les résultats générés font systématiquement l'objet d'une validation humaine avant toute utilisation susceptible d'avoir un impact sur le Système d'Information ;

- aucune modification de production, règle de sécurité, configuration ou action de remédiation ne peut être exécutée de manière autonome par une intelligence artificielle sans mécanisme de contrôle et d'autorisation préalablement validé.

8.3 Exigences relatives aux services Cloud et aux données

Les services Cloud ou SaaS utilisés dans le cadre de la prestation et amenés à traiter ou stocker des données du Pouvoir adjudicateur doivent présenter un niveau de sécurité adapté à leur sensibilité.

Le candidat précise notamment la localisation des données et sauvegardes, les principaux sous-traitants techniques, les mécanismes de chiffrement et de contrôle des accès, ainsi que les modalités de restitution et de suppression des données.

Les données sont hébergées au sein de l'Union européenne ou de l'Espace économique européen sauf dérogation expressément acceptée par le Pouvoir adjudicateur.

Lorsqu'une qualification SecNumCloud est applicable à la solution ou au service proposé, le candidat l'indique dans son offre. À défaut, il présente les garanties de sécurité mises en œuvre permettant d'apprécier le niveau de protection offert.

L'absence de qualification SecNumCloud ne constitue pas à elle seule un motif de non-conformité, sauf disposition contraire prévue dans les pièces du marché.

8.4 Exigences de sécurité

Le Titulaire applique les règles de sécurité définies par le Pouvoir adjudicateur ainsi que les bonnes pratiques reconnues en matière de sécurité. Il adopte notamment les principes suivants :

- moindre privilège ;
- séparation des rôles ;
- limitation de l'exposition des services ;
- segmentation et cloisonnement ;
- traçabilité des actions d'administration ;
- utilisation de protocoles et mécanismes cryptographiques conformes à l'état de l'art.

Le Titulaire informe sans délai le Pouvoir adjudicateur de toute situation susceptible d'affecter la sécurité du Système d'Information, y compris lorsqu'elle résulte d'une erreur humaine, d'une mauvaise configuration, d'une vulnérabilité connue, d'un défaut d'un équipement ou logiciel ou d'une compromission réelle ou suspectée.

8.4.1 Authentification et gestion des accès

Les accès accordés au Titulaire sont strictement limités aux besoins nécessaires à l'exécution des prestations.

Les comptes utilisés par les intervenants doivent être nominatifs. L'utilisation de comptes génériques ou partagés pour les opérations d'administration est interdite, sauf impossibilité technique dûment justifiée et expressément validée par le Pouvoir adjudicateur.

Les accès d'administration doivent être réalisés :

- au travers des dispositifs d'administration sécurisée mis à disposition par le Pouvoir adjudicateur, notamment le bastion ;
- avec une authentification forte ou accès sécurisé (VPN) ;
- depuis des équipements maîtrisés et sécurisés ;
- au moyen de protocoles d'administration sécurisés ;
- avec une journalisation permettant d'identifier l'intervenant et les actions réalisées.
- Les droits attribués doivent respecter le principe du moindre privilège.
- Les comptes et habilitations ne doivent pas être transmis entre collaborateurs.

Le Titulaire est responsable de la gestion des arrivées, départs et changements d'affectation de ses collaborateurs et sous-traitants intervenant sur le marché.

Il doit informer le Pouvoir adjudicateur dans les meilleurs délais de toute modification nécessitant la création, la modification, la suspension ou la suppression d'un accès.

En cas de départ d'un intervenant ou de retrait de son habilitation sur le marché, le Titulaire demande sans délai la révocation de ses accès.

Toute compromission réelle ou suspectée d'un compte utilisé dans le cadre du marché doit être immédiatement signalée au Pouvoir adjudicateur.

8.4.2 Gestion des secrets et mots de passe

Les mots de passe, secrets, clés et autres éléments d'authentification utilisés dans le cadre de la prestation doivent être stockés et gérés de manière sécurisée, conformément aux dispositifs et exigences définis par le Pouvoir adjudicateur.

Lorsqu'un secret partagé ne peut pas être intégré aux dispositifs prévus par le Pouvoir adjudicateur, le Titulaire doit garantir son stockage dans une solution sécurisée conforme aux bonnes pratiques de sécurité, avec un accès limité aux seules personnes habilitées.

Les secrets et mots de passe ne doivent en aucun cas être stockés ou transmis en clair par des moyens non sécurisés.

8.4.3 Environnement technique du Titulaire

Le Titulaire doit maintenir à jour et en condition de sécurité les systèmes, postes de travail, outils, plateformes et services qu'il utilise pour accéder au Système d'Information du Pouvoir adjudicateur ou pour exécuter les prestations.

Il veille notamment à l'application régulière des correctifs de sécurité et à l'utilisation de versions maintenues par leurs éditeurs ou constructeurs.

Toute vulnérabilité critique affectant un outil, un équipement ou un service du Titulaire connecté au Système d'Information du Pouvoir adjudicateur ou susceptible d'en compromettre la sécurité doit faire l'objet d'une remédiation dans les meilleurs délais.

Lorsque cette vulnérabilité présente un risque pour le Pouvoir adjudicateur, le Titulaire doit l'en informer sans délai et préciser les mesures de protection ou de remédiation mises en œuvre**.**

8.4.4 Sécurité des sauvegardes

Lorsque le Titulaire administre, exploite ou intervient sur des mécanismes de sauvegarde entrant dans le périmètre du marché, il doit veiller à préserver leur confidentialité, leur intégrité et leur disponibilité.

Les sauvegardes contenant des informations du Pouvoir adjudicateur doivent bénéficier d'un niveau de protection adapté à la sensibilité des données qu'elles contiennent.

Le Titulaire doit notamment veiller à :

- limiter strictement les droits d'accès aux infrastructures et données de sauvegarde ;
- séparer autant que possible les droits d'administration des environnements de production et ceux des systèmes de sauvegarde ;
- protéger les accès d'administration par des mécanismes d'authentification forte lorsque la solution le permet ;
- garantir la traçabilité des opérations sensibles ;
- protéger les flux et données de sauvegarde par des mécanismes de chiffrement adaptés lorsque cela est techniquement pertinent ;
- mettre en œuvre, lorsque la solution le permet, des mécanismes permettant de réduire le risque de suppression ou d'altération des sauvegardes en cas de compromission du Système d'Information ;
- respecter les durées de conservation et politiques de sauvegarde définies par le Pouvoir adjudicateur.

Toute suppression massive, modification substantielle d'une politique de sauvegarde ou action susceptible d'altérer significativement la capacité de restauration doit faire l'objet d'une validation préalable du Pouvoir adjudicateur.

8.5 Exigences relatives aux sous-traitants

Le recours à des sous-traitants ne diminue en aucune manière la responsabilité du Titulaire quant au respect des obligations du marché.

Le Titulaire s'assure que tout sous-traitant intervenant directement ou indirectement sur le Système d'Information respecte un niveau de sécurité au moins équivalent à celui exigé du Titulaire. Les exigences relatives notamment :

- à la confidentialité ;
- aux habilitations ;
- à la gestion des accès ;
- à la traçabilité ;
- au traitement des incidents de sécurité ;
- à la protection des données ;
- à l'utilisation de l'intelligence artificielle ;
- et aux conditions d'intervention sur le Système d'Information

Le Titulaire demeure l'interlocuteur et le responsable contractuel du Pouvoir adjudicateur pour les prestations confiées à ses sous-traitants.

Il informe le Pouvoir adjudicateur de tout changement significatif de sous-traitant intervenant sur le périmètre technique ou ayant accès aux données ou infrastructures du Pouvoir adjudicateur, selon les modalités prévues par les pièces administratives du marché.

8.6 Conformité et réglementation

Le Titulaire réalise les prestations dans le respect de l'ensemble des dispositions légales et réglementaires qui lui sont applicables ainsi que de celles applicables au Pouvoir adjudicateur lorsqu'elles concernent directement les prestations réalisées.

Sont notamment concernés, selon leur applicabilité :

- le Règlement général sur la protection des données (RGPD) ;
- les dispositions nationales relatives à la protection des données personnelles ;
- les réglementations européennes et nationales applicables à la cybersécurité et à la résilience des systèmes d'information ;
- les obligations issues ou à venir de la transposition nationale de la directive européenne NIS2 ;
- les exigences applicables en matière de notification ou de gestion des incidents de sécurité.

À la date de rédaction du présent marché, la transposition française de la directive NIS2 demeure en cours. Le Titulaire devra prendre en compte les textes réglementaires applicables pendant toute la durée d'exécution du marché ainsi que leurs évolutions.

Le Titulaire devra être en mesure d'accompagner le Pouvoir adjudicateur dans l'application des exigences de cybersécurité qui concernent les prestations placées sous sa responsabilité.

Les pratiques du Titulaire doivent également s'inscrire dans les principes et bonnes pratiques reconnus par les référentiels de sécurité pertinents, notamment :

- les recommandations de l'ANSSI ;
- le Référentiel Cyber France (ReCyF), lorsqu'il est applicable ou pertinent ;
- les principes de l'ISO/IEC 27001 et standards associés ;
- les recommandations de sécurité des constructeurs et éditeurs.

La référence à ces normes et référentiels ne vaut pas obligation de certification du Titulaire sauf lorsque cette exigence est expressément prévue dans une autre pièce du marché.

Le Référentiel Cyber France publié par l'ANSSI depuis mars 2026 fournit notamment des mesures permettant d'anticiper les objectifs de sécurité associés à NIS2.

Le Titulaire informe le Pouvoir adjudicateur de toute évolution réglementaire dont il a connaissance et susceptible d'avoir un impact significatif sur les prestations ou sur le niveau de sécurité du périmètre exploité.

8.7 Confidentialité

Le Titulaire est tenu au respect des obligations de confidentialité applicables à l'ensemble des informations, données, documents, configurations, architectures et éléments dont il pourrait avoir connaissance dans le cadre de l'exécution du marché.

Les dispositions détaillées relatives à la confidentialité, à la protection des informations, aux obligations des intervenants ainsi qu'aux éventuels engagements spécifiques sont définies dans les pièces administratives et/ou l'annexe juridique du marché.

Le présent CCTP ne se substitue pas à ces dispositions.

D'un point de vue opérationnel, le Titulaire veille néanmoins à ce que les informations auxquelles ses collaborateurs ou sous-traitants ont accès ne soient utilisées que pour les besoins strictement nécessaires à l'exécution des prestations et ne soient communiquées à aucun tiers non autorisé.

9 Livrables attendus

Le présent marché distingue deux catégories de livrables :

- les éléments demandés au candidat dans le cadre de sa réponse à la consultation sont définies dans le document annexe intitulé Cadre de Réponse Technique (CRT) ;
- les livrables contractuels produits, complétés, actualisés et maintenus par le Titulaire pendant l'exécution du marché.

Cette distinction permet de différencier les éléments nécessaires à l'analyse des offres des documents opérationnels constituant les livrables d'exécution du marché.

9.1 Livrables contractuels pendant l'exécution du marché

Les livrables contractuels constituent les documents de référence nécessaires à l'initialisation, à l'exploitation, au pilotage, à la sécurité, à l'amélioration continue et à la réversibilité des prestations.

Ils sont élaborés, complétés ou repris à partir de la documentation existante et des éléments proposés par le Titulaire dans son offre.

Sauf disposition contraire, leur production, leur actualisation et leur maintien en condition opérationnelle documentaire sont compris dans les prestations du marché.

Les livrables sont transmis dans des formats standards, lisibles, exploitables et modifiables. Ils doivent permettre leur réutilisation par le Pouvoir adjudicateur et, le cas échéant, leur transmission à un tiers autorisé.

Le Titulaire assure pendant toute la durée du marché :

- la cohérence des différents documents ;
- leur actualisation à la suite des évolutions du périmètre, de l'architecture, des processus ou de l'organisation ;
- leur gestion de version ;
- leur traçabilité ;
- leur mise à disposition dans le référentiel documentaire défini avec le Pouvoir adjudicateur.

Les modalités détaillées de production, de validation, d'actualisation et de gestion documentaire sont précisées lors de la phase d'initialisation.

9.1.1 Livrables de la phase d'initialisation

La phase d'initialisation donne lieu à la production, à l'actualisation, à la consolidation ou à la validation des documents nécessaires au passage en exploitation nominale.

Selon la nature des documents et l'état de l'existant, le Titulaire assure leur création, leur reprise, leur mise à jour ou leur validation. Les livrables attendus comprennent notamment :

Livrable	**Périmètre**
Plan détaillé d'initialisation	Ensemble du marché
Planning détaillé, jalons, charges, ressources et responsabilités	Ensemble du marché
PAQ – Plan d'Assurance Qualité	Ensemble du marché
PAS – Plan d'Assurance Sécurité	Ensemble du marché
Convention de services	Ensemble du marché
Organisation opérationnelle et matrice RACI	Ensemble du marché
Matrice des contacts, escalades et astreintes HO/HNO	Ensemble du marché
Matrice des actions autorisées	SOC / Sécurité
Inventaire technique actualisé	Réseau / Sécurité
État initial des versions, niveaux de support, fins de support et obsolescences	Réseau / Sécurité
Référentiel documentaire	Ensemble du marché
DAT et schémas techniques actualisés ou constitués	Selon périmètre
DEX et procédures d'exploitation	Selon périmètre
Référentiel de supervision	Réseau / Sécurité
Consignes de supervision et d'escalade	Réseau / Sécurité
Référentiel des sources SOC	SOC
Catalogue initial des cas d'usage et règles de détection	SOC
Évaluation initiale de la couverture de détection	SOC
Processus de gestion des incidents et événements de sécurité	Ensemble du marché
Processus de gestion des incidents critiques et de crise	Ensemble du marché
Processus de gestion des demandes	Ensemble du marché
Procédures opérationnelles associées au catalogue de services	Ensemble du marché
Processus de gestion des changements	Ensemble du marché
Processus de gestion des problèmes	Ensemble du marché
Processus de Patch Management	Réseau / Sécurité
Processus de détection, qualification et suivi des vulnérabilités	SOC / Infogérance
Plan annuel de maintenance prévisionnel initial	Réseau / Sécurité
Modalités de gestion et de validation de la documentation	Ensemble du marché
Modèles définitifs de météo, COTECH, COPIL et COSTRAT	Ensemble du marché

Catalogue des KPI, SLA et modalités de mesure	Ensemble du marché
Base de connaissances initialisée ou reprise de la base existante	Ensemble du marché

Lorsque plusieurs documents peuvent utilement être regroupés au sein d'un même référentiel ou document maître, le Titulaire peut proposer leur consolidation, sous réserve de l'accord du Pouvoir adjudicateur et à condition que l'ensemble des informations attendues demeure clairement identifiable et exploitable.

Les livrables sont soumis à validation du Pouvoir adjudicateur selon les modalités définies dans le cadre de la gouvernance de la phase d'initialisation.

Lorsque des écarts, insuffisances documentaires, obsolescences ou risques sont identifiés lors de la reprise, le Titulaire les formalise et propose un plan d'actions précisant a minima les constats, les mesures recommandées, leur niveau de priorité, les responsables identifiés et les échéances associées.

La clôture de la phase d'initialisation est conditionnée à la réalisation des travaux prévus, à la remise et à la validation des livrables nécessaires au passage en exploitation nominale ainsi qu'à la signature du procès-verbal de validation de la phase d'initialisation.

Le seul écoulement de la durée prévisionnelle de la phase d'initialisation ne saurait valoir validation ou clôture de celle-ci.

9.1.2 Livrables récurrents en phase d'exploitation

Pendant toute la durée de la prestation, le Titulaire produit, actualise et maintient les livrables nécessaires au pilotage, à l'exploitation, à la sécurité et à l'amélioration continue du service.

Les livrables issus de la phase d'initialisation constituent le socle documentaire de référence et sont maintenus à jour pendant toute la durée du marché lorsque leur nature le nécessite.

9.1.2.1 Gouvernance et pilotage

Les principaux livrables de gouvernance comprennent notamment :

- la météo quotidienne des services ;
- les supports et comptes rendus de COTECH ;
- les supports et comptes rendus de COPIL ;
- les supports et comptes rendus de COSTRAT ;
- le suivi des risques, décisions, actions et points de blocage ;
- les tableaux de bord relatifs aux SLA et KPI ;
- les états de consommation des volumétries contractuelles ;
- les états de consommation des prestations complémentaires ou réalisées sur devis ;
- les plans d'amélioration du service et leur suivi.

Les fréquences et délais de remise de ces livrables sont définis dans les engagements de service et les dispositions relatives à la gouvernance du marché.

9.1.2.2 Exploitation Réseau et Sécurité

Le Titulaire produit et maintient notamment :

- les reportings d'incidents, demandes, problèmes et changements ;
- les indicateurs de disponibilité et de performance ;
- les rapports et tableaux de bord de supervision ;
- les analyses de capacité et de performance ;
- le suivi des versions ;
- le suivi des fins de support, fins de maintenance et obsolescences ;
- le plan annuel de maintenance prévisionnel et ses mises à jour ;
- les bilans des campagnes de correctifs et des montées de version ;
- le suivi des exceptions et des mesures compensatoires ;
- les référentiels, inventaires et documents techniques actualisés ;
- la base de connaissances et les fiches de résolution ;
- les DAT, DEX, schémas, procédures et modes opératoires actualisés lorsque les évolutions réalisées le nécessitent.

9.1.2.3 SOC

Le Titulaire produit et maintient notamment :

- les tableaux de bord et reportings SOC ;
- l'état des alertes et incidents de sécurité ;
- le référentiel des sources SOC ;
- le suivi des anomalies et pertes de collecte ;
- le catalogue des cas d'usage et règles de détection ;
- les résultats des revues de couverture de détection ;
- les rapports et informations de Threat Intelligence présentant un intérêt pour le Pouvoir adjudicateur ;
- les comptes rendus des campagnes de Threat Hunting ;
- les rapports de vulnérabilités et leur état de suivi ;
- les éléments de suivi de la surface d'attaque ;
- les informations pertinentes issues de la surveillance du Dark Web ;
- les recommandations de remédiation ;
- les plans d'amélioration continue du dispositif SOC.

Les référentiels SOC sont maintenus à jour afin de refléter les évolutions du périmètre supervisé, des sources collectées, des menaces identifiées et des mécanismes de détection mis en œuvre.

9.1.2.4 Incidents et retours d'expérience

Les incidents soumis aux dispositions prévues au processus de gestion des incidents donnent lieu, selon leur niveau de priorité et les critères définis au marché, à la production d'un REX contenant les éléments suivants :

- chronologie de l'incident ;
- rapport d'incident ;
- analyse de cause racine lorsque celle-ci peut être établie ;
- retour d'expérience (REX) ;
- plan d'actions correctives et préventives ;
- mise à jour des procédures concernées ;
- mise à jour des règles de supervision ;
- mise à jour des cas d'usage SOC lorsque nécessaire ;
- alimentation ou mise à jour de la base de connaissances.

La production de ces éléments ne dispense pas le Titulaire de mettre à jour les autres référentiels ou documents contractuels impactés par l'incident.

9.1.3 Livrables de réversibilité

La réversibilité donne lieu à la production, à l'actualisation et à la restitution de l'ensemble des éléments nécessaires à la reprise de la prestation par le Pouvoir adjudicateur ou par un tiers désigné par celui-ci.

Les livrables comprennent notamment :

- le plan détaillé de réversibilité actualisé et le planning et les jalons de transfert ;
- la matrice des responsabilités pendant la période de réversibilité ;
- l'inventaire technique complet du périmètre ;
- l'inventaire des comptes, accès et habilitations ;
- les configurations et sauvegardes de configurations ;
- les données et historiques relevant du Pouvoir adjudicateur ;
- les exports des outils de ticketing et de supervision lorsque nécessaires ;
- le référentiel des sources SOC ;
- les règles de corrélation et de détection et les cas d'usage SOC ;
- les tableaux de bord et configurations développés spécifiquement pour le Pouvoir adjudicateur ;
- la base de connaissances ;
- les informations relatives aux licences, abonnements, contrats et dépendances techniques ;
- les éléments permettant la reprise des services fournis ou hébergés par le Titulaire ;
- les supports de transfert de connaissances ;
- les comptes rendus des sessions de transfert ;
- le procès-verbal de réversibilité ou de transfert.

Le Titulaire assure la remise des éléments dans des formats standards, lisibles, exploitables et, lorsque leur nature le permet, modifiables, afin de permettre au Pouvoir adjudicateur ou au prestataire entrant d'en assurer la reprise, la maintenance et la réutilisation.

Il assure, pendant la période de réversibilité, la coopération, l'assistance et la transmission des connaissances nécessaires au maintien de la continuité du service.

La réversibilité ne saurait être considérée comme achevée du seul fait de la transmission documentaire. Elle est conditionnée à la remise des éléments prévus, à leur caractère exploitable et à la réalisation des opérations de transfert prévues au plan de réversibilité.

À l'issue de la réversibilité et après validation de la bonne restitution des données et éléments nécessaires à la reprise, le Titulaire procède, conformément aux dispositions contractuelles applicables, à la suppression des données du Pouvoir adjudicateur qui ne sont plus nécessaires à l'exécution de ses obligations et fournit, lorsque requis, les éléments attestant de cette suppression.

10 Annexe : Sites

Catégorie	Délégation	Adresse
Principal - Siège	ILE-DE-FRANCE - Levallois (Dpt 75-77-78-91-92-93-94-95)	31 rue Anatole France 92300 Levallois Perret
Région	RHONE-ALPES (Dpt 01-07-26-38-42-69-73-74)	Immeuble Le Président 74 bd du 11 Novembre CS 50039 69626 VILLEURBANNE CEDEX
Région	AUVERGNE (Dpt 03-15-43-63)	Immeuble @ Number One Parc Technologique de la Pardieu 9 allée Evariste Galois 63174 AUBIERE Cedex
Région	FRANCHE COMTE (Dpt 25-39-70-90)	Les Ilots des Montboucons 1 rue François-André Vincent 25000 BESANCON
Région	BOURGOGNE (Dpt 21-58-71-89)	59 avenue Roland Carraz CS 70141 21304 CHENOVE Cedex
Région	BRETAGNE (Dpt 22-29-35-56)	39 rue du Capitaine Maignan CS 64436 35044 RENNES CEDEX
Région	CENTRE (Dpt 18-28-36-37-41-45)	3/5 bd de Verdun 45007 ORLEANS CEDEX 1
Région	ALSACE (Dpt 67-68)	Espace Européen de l'Entreprise 19 avenue de l'Europe 67300 SCHILTIGHEIM
Région	LORRAINE (Dpt 54-55-57-88)	Médiaparc 2/4 rue Jacques Villermaux 54000 NANCY
Région	NORD-PAS-DE-CALAIS (Dpt 59-62)	Immeuble Grand Siecle 6 place Mendes France 59000 LILLE
Région	PICARDIE (Dpt 02-60-80)	11 rue Vanmarcke 80000 AMIENS
Principal - Région	ILE-DE-FRANCE - Malakoff (Dpt 75-77-78-91-92-93-94-95)	40 rue Gabriel Crié CS 70001 92247 MALAKOFF CEDEX
Région	BASSE-NORMANDIE (Dpt 14-50-61)	Résidence Wagram 48 avenue de l'Hippodrome 14000 CAEN
Région	HAUTE-NORMANDIE (Dpt 27-76)	52 rue Victor Hugo 27000 EVREUX
Région	AQUITAINE (Dpt 24-33-40-47-64)	Les Bureaux du Lac 1 Bât. 2 6 rue Théodore Blanc 33520 BRUGES
Région	LIMOUSIN (Dpt 19-23-87)	25 bd Victor Hugo 87000 LIMOGES
Région	LANGUEDOC-ROUSSILLON (Dpt 11-30-34-48-66)	420 allée Henri II de Montmorency 34000 MONTPELLIER
Région	MIDI-PYRENEES (Dpt 09-12-31-32-46-65-81-82)	Les Berges du Lac Bât. B Rue du Colombier BP 47694 31676 LABEGE CEDEX
Principal - Région	P.A.C.A.C. (Dpt 04-05-06-13-20-83-84)	Tour Méditerranée 65 avenue Jules Cantini 13298 MARSEILLE CEDEX 20
Région	PAYS DE LA LOIRE (Dpt 44-49-53-72-85)	1 rue MargueriteThibert CS 30225 44202 NANTES CEDEX 2
Région	ILE DE LA REUNION	7 boulevard du Chaudron IMMEUBLE TRITON CS 61034 97495 STE CLOTILDE CEDEX

10.1 Hors périmètre

Catégorie	Délégation	Adresse
Région	GUADELOUPE	Zone Artisanale de Dugazon de Bourgogne 97139 LES ABIMES
Région	GUYANE	Résidence MAN'CIA 1897 route de Montjoly 97354 REMIRE-MONTJOLY
Région	MARTINIQUE	1490 chemin du Glyceria Immeuble le Glyceria 97232 LAMENTIN