



**MINISTÈRE
CHARGÉ DE LA MER
ET DE LA PÊCHE**

*Liberté
Égalité
Fraternité*

DIRECTION GENERALE DES AFFAIRES MARITIMES DE LA PÊCHE ET
DE L'AQUACULTURE

SOUS-DIRECTION DE LA TRANSFORMATION NUMÉRIQUE

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES
(CCTP)

LOT N° 6 : PLATEFORME ET INFRASTRUCTURE DONNÉES

**FOURNITURE DE PRESTATIONS DE VALORISATION
DES DONNEES**

Table des matières

ARTICLE VIII - LOT N° 6 : Plateforme et infrastructure Donnée.....	4
VIII.1 PRESTATION L6-1 : CONCEPTION ET INGÉNIERIE DE PLATEFORME.....	4
VIII.1.1 UO 6.1.1 - DÉFINITION ARCHITECTURE PLATEFORME DE DONNÉES.....	4
VIII.1.2 UO 6.1.2 - AUDIT ARCHITECTURE.....	6
VIII.1.3 UO 6.1.3 - DÉVELOPPEMENT DE COMPOSANTS SPÉCIFIQUES.....	9
VIII.1.4 UO 6.1.4 - PILOTAGE PROJET INGÉNIERIE PLATEFORME.....	11
VIII.1.5 UO 6.1.5 - RÉDACTION CAS DE TESTS VALIDATION PRODUIT.....	14
VIII.1.6 UO 6.1.6 - EXÉCUTION CAMPAGNES VALIDATION PRODUIT.....	17
VIII.1.7 UO 6.1.7 - SPRINT AGILE PLATEFORME.....	20
VIII.2 PRESTATION L6-2 : DÉPLOIEMENT ET ADMINISTRATION DE PLATEFORME.....	24
VIII.2.1 UO 6.2.1 - DÉFINITION ET MISE EN ŒUVRE ARCHITECTURE CIBLE.....	24
VIII.2.2 UO 6.2.2 - ADMINISTRATION ET MAINTENANCE DE PLATEFORME.....	28
VIII.2.3 UO 6.2.3 - MIGRATION DE DONNÉES ET DE SYSTÈMES.....	31
VIII.2.4 UO 6.2.4 - OPTIMISATION ET PERFORMANCE DE PLATEFORME.....	34
VIII.3 PRESTATION L6-3 : SÉCURITÉ ET CONFORMITÉ DE PLATEFORME.....	38
VIII.3.1 UO 6.3.1 - AUDIT DE SÉCURITÉ ET CONFORMITÉ.....	38
VIII.3.2 UO 6.3.2 - IMPLÉMENTATION DE MESURES DE SÉCURITÉ.....	42
VIII.3.3 UO 6.3.3 - GESTION DES IDENTITÉS ET DES ACCÈS.....	45
VIII.3.4 UO 6.3.4 - MONITORING ET GESTION DES INCIDENTS DE SÉCURITÉ....	49
VIII.4 PRESTATION L6-4 : SUPERVISION ET MONITORING DE PLATEFORME.....	53
VIII.4.1 UO 6.4.1 - CONCEPTION DE L'ARCHITECTURE DE SUPERVISION.....	53
VIII.4.2 UO 6.4.2 - IMPLÉMENTATION DES OUTILS DE MONITORING.....	57
VIII.4.3 UO 6.4.3 - OPTIMISATION DES PERFORMANCES ET DE LA DISPONIBILITÉ	61
VIII.4.4 UO 6.4.4 - REPORTING ET ALERTING AVANCÉ.....	64
VIII.4.5 UO 6.4.5 - SUIVI PERFORMANCE PRODUIT PLATEFORME.....	68
VIII.5 PRESTATION L6-5 : GOUVERNANCE TECHNIQUE DE PLATEFORME.....	72
VIII.5.1 UO 6.5.1 - DÉFINITION DES POLITIQUES DE GOUVERNANCE TECHNIQUE	72
VIII.5.2 UO 6.5.2 - MISE EN PLACE DES PROCESSUS DE VALIDATION ET CONFORMITÉ.....	76
VIII.5.3 UO 6.5.3 - GESTION DU CATALOGUE DE SERVICES TECHNIQUES.....	80

VIII.5.4 UO 6.5.4 - ACCOMPAGNEMENT À L'ADOPTION DES STANDARDS TECHNIQUES.....	84
VIII.6 PRESTATION L6-6 : EXPLOITATION ET SUPPORT DE PLATEFORME.....	88
VIII.6.1 UO 6.6.1 - EXPLOITATION COURANTE DE LA PLATEFORME.....	88
VIII.6.2 UO 6.6.2 - MAINTENANCE CORRECTIVE ET ÉVOLUTIVE.....	92
VIII.6.3 UO 6.6.3 - SUPPORT UTILISATEURS ET FORMATION.....	96
VIII.6.4 UO 6.6.4 - TRANSFERT DE COMPÉTENCES ET AUTONOMIE.....	100
VIII.6.5 UO 6.6.5 - ASTREINTES.....	104

ARTICLE VIII - LOT N° 6 : PLATEFORME ET INFRASTRUCTURE DONNÉE

Ce lot encadre la conception, le déploiement, la sécurisation, la supervision et l'exploitation des plateformes données (data lake, mesh, cloud, pipelines, outils d'orchestration). Il garantit la performance, la conformité et la disponibilité des infrastructures data, ainsi que leur gouvernance technique et évolutivité.

[Glossaire du lot6](#)

VIII.1 PRESTATION L6-1 : CONCEPTION ET INGÉNIERIE DE PLATEFORME

La Prestation L6-1 est axée sur le pilotage global et la définition de l'architecture de ces plateformes de données. En résumé, la Prestation L6-1 est fondamentale pour la mise en place et l'optimisation des fondations techniques des systèmes de données, en couvrant l'architecture, le développement de composants sur mesure, l'audit et le pilotage des projets d'ingénierie, garantissant ainsi une infrastructure data solide et adaptable.

VIII.1.1 UO 6.1.1 - DÉFINITION ARCHITECTURE PLATEFORME DE DONNÉES

OBJET

L'objet de cette UO est de concevoir et de formaliser l'architecture technique et fonctionnelle d'une plateforme de données évolutive et performante. Cette prestation vise à définir les composants clés (data lake, data warehouse, outils d'intégration, de gouvernance, de sécurité, etc.), leurs interactions, les standards techniques et les meilleures pratiques pour répondre aux besoins actuels et futurs en matière de gestion et de valorisation des données. Elle garantit l'alignement de l'infrastructure data avec les objectifs stratégiques de l'organisation.

CONTENU ET MODALITES D'EXECUTION

Cette UO est une activité de conception stratégique et de planification technique.

Contenu :

- **Analyse des besoins** : Recueil des exigences fonctionnelles et non fonctionnelles (performance, scalabilité, sécurité, coût, conformité) auprès des équipes métiers et IT.
- **État de l'art et choix technologiques** : Évaluation des technologies existantes sur le marché (cloud, open source, propriétaires) et recommandation des solutions adaptées aux besoins et à l'écosystème du bénéficiaire.
- Conception de l'architecture cible :
 - Définition de la topologie générale de la plateforme (on-premise, cloud, hybride).
 - Identification et spécification des couches et des composants (ingestion, stockage, traitement, exposition, gouvernance, sécurité, monitoring).
 - Définition des principes d'intégration des données et des flux.
 - Modélisation des données à haut niveau.
- **Définition des standards et bonnes pratiques** : Élaboration des règles d'ingénierie, de nommage, de sécurité et d'opérationnalisation.
- **Évaluation des risques et des coûts** : Identification des risques techniques et financiers liés à l'architecture proposée, et estimation budgétaire.
- **Feuille de route** : Proposition d'une feuille de route pour le déploiement progressif de l'architecture.

Modèle d'exécution :

- **Ateliers de co-construction** : Sessions interactives avec les parties prenantes (architectes, chefs de projet, experts métiers, DPO) pour valider les choix et les orientations.
- **Analyses comparatives (Proof of Concept - PoC si nécessaire)** : Réalisation d'études ciblées ou de PoC pour valider des choix technologiques critiques.
- **Veille technologique continue** : Intégration des dernières avancées et des retours d'expérience du marché.
- **Documentation collaborative** : Utilisation d'outils de documentation partagée pour la transparence et la traçabilité des décisions.

PROFIL(S) PRESENTI(S)

- Architecte Plateforme Cloud
- Architecte Data Mesh (maillage de données)
- Expert FinOps

- Architecte Big Data
- Expert Cybersécurité Cloud

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Environnements	1-2	3-5	>5
Sources de données	<10	10-50	>50
Utilisateurs	<100	100-1K	>1K
Volumes	<1TB	1-100TB	>100TB
Intégrations	<5	5-20	>20
Architecture	Monolithique	Microservices	Distribué, cloud-native

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	15 jours	30 jours	45 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Rapport d'analyse des besoins et matrice de maturité	1 semaine	2 semaines	2 semaines
Architecture Decision Records (ADR) et patterns	2 semaines	4 semaines	6 semaines
Spécifications techniques détaillées	3 semaines	6 semaines	8 semaines
PoC critiques et tests de validation	4 semaines	8 semaines	10 semaines
Feuille de route détaillée et estimation des coûts	4 semaines	8 semaines	12 semaines

VIII.1.2 UO 6.1.2 - AUDIT ARCHITECTURE

OBJET

L'objet de cette UO est de réaliser un audit approfondi de l'architecture existante de la plateforme de données. Cette prestation vise à évaluer la robustesse, la performance, la scalabilité, la sécurité, la conformité et la pertinence technologique de l'architecture actuelle. L'objectif est d'identifier les forces, les faiblesses, les risques et les opportunités d'amélioration afin de formuler des recommandations concrètes pour optimiser l'infrastructure data.

CONTENU ET MODALITES D'EXECUTION

Cette UO est une activité d'analyse critique et d'évaluation experte.

Contenu :

- **Collecte et analyse documentaire** : Examen des documents d'architecture, spécifications techniques, procédures d'exploitation, rapports d'incidents, etc.
- **Entretiens et ateliers** : Rencontres avec les équipes techniques (architectes, ingénieurs data, Ops, sécurité) et les utilisateurs clés pour comprendre les usages, les problématiques et les attentes.
- **Analyse technique et fonctionnelle** :
 - **Composants** : Évaluation des technologies utilisées (stockage, bases de données, ETL, outils de streaming, cloud services, outils de gouvernance, etc.) et de leur adéquation.
 - **Performance** : Analyse des goulots d'étranglement, des temps de traitement, de l'utilisation des ressources (CPU, RAM, stockage, réseau).
 - **Scalabilité** : Évaluation de la capacité de l'architecture à gérer une croissance des volumes de données et des utilisateurs.
 - **Sécurité** : Audit des mécanismes d'authentification, d'autorisation (IAM), de chiffrement, de journalisation et de conformité aux standards (ex: RGPD, SecNumCloud).
 - **Résilience et haute disponibilité** : Examen des dispositifs de sauvegarde, de restauration, de reprise après sinistre et des architectures redondantes.
 - **Gouvernance** : Analyse des processus de gestion des métadonnées, de qualité des données et de gestion des accès.
 - **Coût** : Évaluation de l'optimisation des coûts (notamment cloud).
- **Identification des écarts et des risques** : Confrontation de l'existant avec les bonnes pratiques de l'industrie et les objectifs du bénéficiaire.
- **Formulation de recommandations** : Proposition d'actions correctives et d'évolutions, avec priorisation et estimation des impacts (bénéfices/coûts/risques).

Modèle d'exécution :

- **Approche structurée** : Utilisation d'une méthodologie d'audit éprouvée (grilles d'évaluation, checklists).
- **Expertise multidisciplinaire** : Mobilisation d'experts en architecture data, sécurité, performance et exploitation.
- **Transparence** : Partage régulier des constats intermédiaires avec les équipes du bénéficiaire.
- **Objectivité** : Analyse neutre et indépendante de l'existant.

PROFIL(S) PRESSENTI(S)

- Auditeur Cloud
- Auditeur Sécurité
- Analyste FinOps
- Architecte Big Data / Ingénieur DataOps
- Ingénieur Observabilité

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Composants	<20	20-50	>50
Environnements	1-2	3-5	>5
Intégrations	<10	10-30	>30
Utilisateurs	<100	100-1K	>1K
Volumes de données	<1TB	1-100TB	>100TB
Architecture	Monolithique	Microservices	Distribué, cloud-native

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	15 jours	30 jours	60 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livraison(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Plan d'audit détaillé et grilles d'évaluation	1 semaine	1 semaine	1 semaine

Rapports d'audit par domaine et matrices de maturité	2 semaines	3 semaines	4 semaines
Rapport de synthèse et benchmarking	2 semaines	4 semaines	5 semaines
Plan de modernisation et de remédiation	2 semaines	4 semaines	6 semaines
Executive summary et présentation	3 jours	3 jours	3 jours

VIII.1.3 UO 6.1.3 - DÉVELOPPEMENT DE COMPOSANTS SPÉCIFIQUES

OBJET

L'UO a pour objet la conception, développement et déploiement de composants logiciels cloud-native spécialisés pour la plateforme de données, intégrant les patterns modernes (microservices, event-driven, serverless) et les meilleures pratiques (DevSecOps, observabilité, résilience). Cette prestation vise à développer des composants sur mesure robustes, sécurisés et performants, parfaitement intégrés à l'écosystème data moderne, avec une observabilité complète et une stratégie de déploiement automatisée.

CONTENU ET MODALITÉS D'EXÉCUTION

Méthodologies de développement :

- Modélisation centrée sur le domaine métier (Domain-Driven Design)
- Architecture claire et séparée par responsabilités (Clean Architecture)
- Développement piloté par les tests (Test-Driven Development)
- Spécifications exécutables et orientées comportement (Behavior-Driven Development)

Analyse et conception :

- Découverte et analyse : cas d'usage, récits utilisateurs, critères d'acceptation
- Architecture cloud-native : microservices, architecture orientée événements, serverless
- Conception centrée sur les APIs
- Patterns de résilience : coupe-circuit, réessai, isolation des composants, gestion des délais

Technologies et environnements (listes non exhaustives) :

- Développement back-end : Python (FastAPI), Java (Spring Boot), Typescript (node.js / NestJS), Go, Rust
- Traitement des données : Kafka, Spark, Flink, Airflow, Prefect
- Cloud-native : conteneurs Docker, Kubernetes, maillage de services, serverless
- APIs : REST, GraphQL, gRPC, WebSockets

Sécurité intégrée :

- Architecture Zero Trust : authentification continue, micro-segmentation
- Sécurité dans le cycle de développement (DevSecOps) : analyse statique et dynamique, vérification des dépendances et des conteneurs
- Standards et protocoles de sécurité : OAuth 2.0, OpenID Connect, JWT, mTLS

Observabilité intégrée :

- Trois piliers : métriques, journaux, traces
- Suivi applicatif et supervision avancée
- Tableaux de bord et indicateurs métier pour le pilotage

Modèle d'exécution :

- Développement agile : sprints de 2 à 4 semaines avec livraisons régulières
- Pratiques DevOps : intégration et déploiement continus, infrastructure automatisée
- Priorité cloud-native : conteneurs, orchestration, services managés
- Sécurité intégrée dès la conception
- Observabilité intégrée dès le développement

PROFIL(S) PRESSENTI(S)

- Développeur cloud-native
- Ingénieur sécurité DevSecOps
- Ingénieur fiabilité des systèmes (SRE)
- Architecte logiciel
- Data Engineer

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Fonctionnalités	1-3	4-10	>10
Intégrations	1-2	3-5	>5
APIs	1-3	4-8	>8
Volume de données	<1Go/j	1-100Go/j	>100Go/j
Utilisateurs	<100	100-1K	>1K

Architecture	Monolithique	Microservices	Distribuée, event-driven
--------------	--------------	---------------	--------------------------

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	4 semaines	12 semaines	24 semaines

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Récits utilisateurs et décisions d'architecture	5 jours	10 jours	10 jours
Spécifications techniques et conception des APIs	5 jours	15 jours	20 jours
Code source et tests automatisés	20 jours	40 jours	60 jours
Pipelines CI/CD et monitoring	20 jours	40 jours	60 jours
Tests de performance et documentation finale	20 jours	40 jours	60 jours

VIII.1.4 UO 6.1.4 - PILOTAGE PROJET INGÉNIERIE PLATEFORME

OBJET

L'UO a pour objet d'assurer le pilotage complet et structuré d'un projet d'ingénierie de plateforme de données moderne, en intégrant les méthodologies DevOps/DataOps et les pratiques cloud-native. Cette prestation vise à coordonner l'ensemble des activités, des ressources et des parties prenantes pour garantir l'atteinte des objectifs du projet dans le respect des délais, du budget, de la qualité, de la sécurité et de la performance. Elle couvre la planification agile, le suivi d'avancement en temps réel, la gestion proactive des risques, l'optimisation continue des coûts (FinOps), et la communication transparente basée sur l'observabilité. Elle nécessite des déplacements.

CONTENU ET MODALITÉS D'EXÉCUTION

Planification agile:

- Gestion de produit : Définition du périmètre avec approche centrée produit
- Planification des itérations : Organisation en sprints et grandes fonctionnalités
- Équipes transverses : Coordination des équipes DevOps/DataOps
- Planification FinOps : Estimation des ressources cloud et du budget prévisionnel

Observabilité du projet :

- Suivi des indicateurs de performance (équivalent métriques DORA) : délai de réalisation, cycle de traitement, fréquence de déploiement
- Tableaux de bord en temps réel pour le suivi projet
- Alertes intelligentes : notifications sur les écarts par rapport au plan

Suivi d'avancement :

- Cérémonies agiles : réunions quotidiennes, revues d'itérations, rétrospectives
- Suivi des objectifs et indicateurs techniques
- Reporting automatisé : tableaux de bord partagés avec les parties prenantes

Gestion FinOps intégrée :

- Suivi en temps réel : coûts cloud et consommation des ressources
- Optimisation continue : ajustement des tailles, instances réservées ou à la demande
- Alertes budgétaires : notifications sur les dépassements
- Reporting financier automatisé : tableaux de bord de coûts

Gestion proactive des risques :

- Évaluation des risques : identification des risques techniques, opérationnels et financiers
- Plans d'atténuation automatisés
- Suivi continu via indicateurs et métriques

Sécurité et conformité :

- Intégration des pratiques de sécurité dans le développement et l'exploitation
- Suivi continu de la conformité réglementaire (RGPD, SecNumCloud)
- Gestion des vulnérabilités et des incidents

Modèle d'exécution :

- Pilotage DevOps : collaboration renforcée entre développement et exploitation
- Automatisation maximale des processus
- Pilotage basé sur des données en temps réel
- Optimisation financière continue intégrée
- Sécurité intégrée à tous les processus

PROFIL(S) PRESSENTI(S)

- Chef de Projet Senior spécialisé en infrastructures cloud et data
- Product Owner technique avec expertise DevOps/DataOps
- Scrum Master / Coach Agile avec expertise cloud-native
- Expert FinOps pour le pilotage des coûts cloud
- Ingénieur SRE pour l'observabilité du projet

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Équipes	<5 personnes	5-15 personnes	>15 personnes
Environnements	1-2	3-5	>5
Technologies	Mono-cloud	Multi-cloud	Hybride, edge
Intégrations	<10	10-30	>30
Budget	<500K€	500K-2M€	>2M€
Durée	<6 mois	6-18 mois	>18 mois

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai maximal entre notification et début	3 jours	5 jours	7 jours
Durée maximale de réalisation	10 jours	15 jours	60 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Plan projet agile avec roadmap produit	1 semaine	2 semaines	2 semaines
Tableaux de bord d'observabilité du projet	5 jours	5 jours	5 jours
Comptes-rendus de cérémonies agiles	2 jours	2 jours	2 jours

Tableaux de bord temps réel de suivi	Continu	Continu	Continu
Registre des risques automatisé	Temps réel	Temps réel	Temps réel
Rapports FinOps et optimisation	Hebdomadaire	Hebdomadaire	Hebdomadaire
Documentation des pratiques DevOps	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Bilan de performance et recommandations	Fin de projet	Fin de projet	Fin de projet

VIII.1.5 UO 6.1.5 - RÉDACTION CAS DE TESTS VALIDATION PRODUIT

OBJET

L'UO a pour objet de concevoir et de rédiger des scénarios et des cas de tests complets pour valider la performance, la robustesse, la sécurité et la conformité de l'ensemble des produits et composants de la plateforme de données. Cette prestation vise à garantir que les solutions data (pipelines ETL/ELT, APIs, modèles ML/IA, tableaux de bord, infrastructure) répondent aux exigences fonctionnelles, non-fonctionnelles, de sécurité et de conformité réglementaire définies. Cette prestation couvre l'assurance qualité complète des produits data modernes, incluant les tests d'infrastructure as code, de sécurité, de performance des systèmes distribués, de qualité des données, et de conformité réglementaire.

CONTENU ET MODALITÉS D'EXÉCUTION

Stratégie de tests complète :

- Tests unitaires et d'intégration : validation des composants individuels et de leur intégration
- Tests de performance et de montée en charge : tests de charge, de stress et de volume
- Tests de sécurité : identification des vulnérabilités, contrôle des accès, chiffrement
- Tests de conformité : respect du RGPD, SecNumCloud, recommandations ANSSI
- Tests de résilience : ingénierie du chaos, reprise après sinistre

Tests d'infrastructure et DevOps :

- Infrastructure automatisée : tests des modèles Terraform, ARM, CloudFormation, Helm
- Déploiements automatisés : validation des chaînes d'intégration et de livraison continues (CI/CD)
- Gestion des configurations : tests des paramètres et environnements

Tests de sécurité spécialisés :

- Tests de vulnérabilité : analyse statique et dynamique du code, vérification des dépendances
- Tests de contrôle d'accès : gestion des identités, rôle et permissions
- Tests de chiffrement : vérification des données en transit et au repos
- Tests de conformité : vérification du respect des exigences réglementaires

Tests de qualité des données :

- Règles de qualité : complétude, exactitude, cohérence et actualité des données
- Gouvernance des données : respect des règles métier et réglementaires
- Traçabilité : suivi complet des transformations de données

Tests de résilience :

- Tolérance aux pannes : vérification de la robustesse face aux défaillances
- Reprise après sinistre : tests de sauvegarde et restauration
- Ingénierie du chaos : tests de résistance aux défaillances majeures

Automatisation des tests :

- Automatisation : scripts et tests intégrés aux chaînes d'intégration et de livraison
- Validation continue : exécution des tests de manière continue
- Orchestration : coordination des campagnes de tests

Modèle d'exécution :

- Développement piloté par les tests : tests conçus avant ou pendant le développement
- Tests intégrés en amont : intégration dès les premières phases du projet
- Validation continue : tests itératifs et adaptatifs
- Collaboration transverse : travail conjoint avec les équipes de développement, sécurité et infrastructure

PROFIL(S) PRESSENTI(S)

- Ingénieur Test Senior spécialisé en plateformes data et cloud
- Expert en tests de sécurité et conformité (RGPD, SecNumCloud)
- Ingénieur Test DevOps/DataOps (automatisation, CI/CD)
- Expert qualité des données et gouvernance

- Ingénieur Fiabilité des Systèmes

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Types de tests	Fonctionnels uniquement	Performance et sécurité	Conformité, résilience, chaos
Composants	<10	10-50	>50
Intégrations	<5	5-20	>20
Environnements	1-2	3-5	>5
Automatisation	Basique	Avancée	Complète avec ML
Conformité	Standards	RGPD	Multi-réglementaire

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	10 jours	15 jours	20 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Stratégie et plan de validation complet	3 jours	5 jours	7 jours
Matrice de traçabilité exigences-tests	2 jours	3 jours	5 jours
Cas de tests fonctionnels détaillés	7 jours	10 jours	12 jours
Cas de tests de sécurité et conformité	5 jours	8 jours	10 jours
Cas de tests de performance et scalabilité	5 jours	8 jours	10 jours
Cas de tests d'infrastructure et DevOps	4 jours	6 jours	8 jours
Cas de tests de qualité des	4 jours	6 jours	8 jours

données			
Cas de tests de résilience	6 jours	8 jours	10 jours
Scripts de tests automatisés	5 jours	10 jours	15 jours
Métriques et KPIs de qualité	3 jours	5 jours	7 jours

VIII.1.6 UO 6.1.6 - EXÉCUTION CAMPAGNES VALIDATION PRODUIT

OBJET

L'UO a pour objet d'exécuter les campagnes de tests de validation complètes pour l'ensemble des produits et composants de la plateforme de données, en s'appuyant sur les cas de tests définis dans l'UO 6.1.5. Cette prestation vise à évaluer objectivement la performance, la robustesse, la sécurité et la conformité de tous les produits data (pipelines ETL/ELT, APIs, modèles ML/IA, tableaux de bord, infrastructure) avant leur mise en production. Cette prestation implique l'exécution rigoureuse de tous types de tests, l'analyse des résultats avec observabilité moderne, l'identification des anomalies, et la validation de la conformité réglementaire.

CONTENU ET MODALITÉS D'EXÉCUTION

Environnements de test cloud-native :

- **Infrastructure as Code** : Provisionnement automatisé des environnements
- **Environnements éphémères** : Création à la demande avec nettoyage automatique
- **Jeux de données** : Données synthétiques, anonymisées, masquées
- **Configuration management** : Gestion des configurations via code

Observabilité des tests :

- **Monitoring temps réel** : Métriques de performance pendant l'exécution
- **Logging centralisé** : Agrégation des logs de tests
- **Tracing distribué** : Suivi des transactions end-to-end
- **Alerting intelligent** : Notifications sur les échecs et anomalies

Exécution automatisée :

- **CI/CD Integration** : Tests automatisés dans les pipelines
- **Orchestration** : Coordination des campagnes via Kubernetes
- **Parallel execution** : Exécution parallèle pour optimiser les délais
- **Retry mechanisms** : Gestion intelligente des échecs temporaires

Tests spécialisés :

- **Security testing** : Penetration testing, vulnerability scanning
- **Performance testing** : Load testing, stress testing, chaos engineering
- **Compliance testing** : Validation RGPD, SecNumCloud, ANSSI
- **Data quality testing** : Validation des règles de qualité des données

Analyse avancée des résultats :

- **Metrics analysis** : Comparaison aux SLA/SLO définis
- **Trend analysis** : Identification des tendances et dégradations
- **Root cause analysis** : Investigation automatisée des échecs
- **Performance profiling** : Analyse détaillée des goulots d'étranglement

Gestion intelligente des anomalies :

- **Automated detection** : Détection automatique des anomalies
- **Classification** : Catégorisation par criticité et impact
- **Escalade** : Processus d'escalade automatisé
- **Tracking** : Suivi du cycle de vie des anomalies

Modèle d'exécution :

- **DevOps/DataOps continuous** : Exécution automatisée en continu
- **Shift-left approach** : Tests dès les premières phases
- **Observability-driven** : Surveillance temps réel de l'exécution
- **Automatisation-first** : Automatisation maximale des processus

- **Orienté retour d'expérience utilisateur** : Amélioration continue basée sur les résultats

PROFIL(S) PRESSENTI(S)

- Ingénieur Test Senior spécialisé en plateformes data et cloud
- Expert en tests de sécurité et conformité (RGPD, SecNumCloud)
- Ingénieur Test DevOps/DataOps (automatisation, CI/CD)
- Expert qualité des données et gouvernance
- Ingénieur SRE pour l'observabilité des tests

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Types de tests	Fonctionnels automatisés	Performance et sécurité	Conformité, résilience, chaos
Composants	<10	10-50	>50
Intégrations	<5	5-20	>20
Environnements	1-2	3-5	>5
Automatisation	Basique	Avancée	Complète avec ML
Conformité	Standards	RGPD	Multi-réglementaire

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	10 jours	15 jours	20 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Configuration des environnements de test et observabilité	3 jours	3 jours	3 jours
Rapports d'exécution détaillés par type de test	1 jour	1 jour	1 jour
Rapports de tests de sécurité et	1 jour	2 jours	2 jours

conformité			
Rapports de tests d'infrastructure et DevOps	1 jour	1 jour	1 jour
Rapports de tests de qualité des données	1 jour	1 jour	1 jour
Rapports de tests de résilience et chaos engineering	1 jour	1 jour	2 jours
Base de données des anomalies avec classification	Temps réel	Temps réel	Temps réel
Tableaux de bord temps réel de suivi qualité et performance	Continu	Continu	Continu
Métriques d'observabilité et KPIs de performance	Temps réel	Temps réel	Temps réel
Attestations de conformité réglementaire	-	3 jours	3 jours
Rapport de synthèse de validation finale	3 jours	3 jours	3 jours
Documentation des environnements et configurations	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau

VIII.1.7 UO 6.1.7 - SPRINT AGILE PLATEFORME

OBJET

L'objet de cette UO est de réaliser des travaux spécifiques sous forme de sprints agiles, en adaptant leur dimensionnement multifactoriel (valeur, complexité, risque, dépendances) aux besoins des projets data et IA avancés. Cette prestation vise à fournir une méthodologie de travail moderne, data-driven et outcome-focused, permettant une livraison continue de valeur, une adaptation temps réel aux changements et une collaboration DevSecOps entre les équipes.

Cette UO est une activité de delivery agile et d'exécution technique DevSecOps.

CONTENU ET MODALITÉS D'EXÉCUTION

Framework de dimensionnement des sprints :

- **Sprint XS (eXtra Small)** : 2-3 jours, traitement d'anomalies critiques, spikes (démonstrateurs) techniques, proof of concepts rapides
- **Sprint S (Small)** : 1 semaine, features atomiques, traitement d'anomalies, optimisations ponctuelles, configuration changes
- **Sprint M (Medium)** : 2 semaines, features complètes, intégrations standards, refactorisation modérée, nouvelles sources de données
- **Sprint L (Large)** : 3 semaines, epics complexes, migrations majeures, nouvelles capacités plateforme, intégrations complexes
- **Sprint XL (eXtra Large)** : 4 semaines, transformations architecturales, projets de recherche, POCs étendus

Critères de dimensionnement multifactoriels :

- **Valeur métier** : Impact sur les objectifs métier (High/Medium/Low)
- **Complexité technique** : Complexité technique (Simple/Moderate/Complex)
- **Niveau de risque** : Niveau de risque (Low/Medium/High)
- **Dépendances** : Nombre et criticité des dépendances
- **Capacité de l'équipe** : Capacité et expertise de l'équipe
- **Incertitude** : Niveau d'incertitude

Sprint Planning:

- **Capacity planning** avec vélocité de l'équipe
- **Story point estimation** avec planning poker et relative sizing
- **Risk assessment** et mitigation planning avec ROAM
- **Definition of Ready** et Definition of Done clairs
- **Sprint objectifs** orientés valeur métier

Sprint d'innovation :

- Hackathons d'exploration des besoins
- Apprentissage
- Traitement du reste à faire

Exécution DevOps intégrée :

- **Application du cadre SAFe**
- **Réalisation de Features** : découpées en User Stories, mesure de la valeur

- **Continuous Integration/Continuous Deployment (CI/CD)**
- **Infrastructure as Code (IaC)** et GitOps
- **Tests automatisés** (unit, integration, fonctionnel, sécurité)
- **Mesure du niveau de qualité du code**
- **Feature flags** et déploiement progressif
- **Monitoring** et observabilité en temps réel

PROFIL(S) PRESSENTI(S)

- Data Engineer / Développeur Data (Lead technique) certifiés SAFe for teams
- Scrum Master certifié SAFe Scrum Master
- Product Owner Data
- Architecte Data
- Ingénieur DevOps / SRE

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Unité	XS	S	M	L	XL
Sprint	Hotfix/Spike	Feature simple	Feature complète	Epic complexe	Transformation
Valeur métier	Critique	Élevée	Moyenne	Élevée	Stratégique
Risques techniques	Très faible	Faible	Moyen	Élevé	Très élevé
Effort équipe	1-2 personnes	2-3 personnes	3-5 personnes	5-7 personnes	7+ personnes
Dependences	Aucune	Minimales	Modérées	Nombreuses	Critiques
Incertitude	Très faible	Faible	Moyenne	Élevée	Très élevée

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	XS	S	M	L	XL
Délai applicable	15 jours				

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise
Sprint planning artifacts (capacité, vitesse, objectifs)	Début de sprint
Definition of Ready/Done, checklist	Début de sprint
Backlog de sprint avec story points et critères d'acceptation	En début de chaque sprint
CI/CD pipeline configuration	J+1 du sprint
Cas de tests automatisés	En continu
Code source versionné avec Revue de code et des objectifs qualité et sécurité	À la fin de chaque sprint
Infrastructure as Code (IaC), scripts	À la fin de chaque sprint
Composants déployés avec monitoring et alerting	À la fin de chaque sprint
Résultats de tests de Performance et de sécurité	À la fin de chaque sprint
Documentation technique auto-générée et à jour	Au fil de l'eau
Tableau de bord de suivi des sprint	Temps réel
Compte rendu de démonstration et de rétrospective	1 jour après la revue
Compte-rendu de revue avec les mesures d'impact métier	1 jour ouvré après la revue
Compte-rendu de rétrospective avec plan d'actions d'amélioration	1 jour ouvré après la rétrospective

VIII.2 PRESTATION L6-2 : DÉPLOIEMENT ET ADMINISTRATION DE PLATEFORME

La Prestation L6-2 est dédiée à la mise en œuvre concrète et à la gestion opérationnelle des plateformes de données. En somme, la Prestation L6-2 est cruciale pour l'opérationnalisation des plateformes de données, en couvrant le déploiement des architectures définies, l'intégration des outils d'orchestration, l'harmonisation des environnements de développement à production, et la mise en place de processus CI/CD pour une livraison agile et fiable.

VIII.2.1 UO 6.2.1 - DÉFINITION ET MISE EN ŒUVRE ARCHITECTURE CIBLE

OBJET

L'UO a pour objet de concevoir, définir en détail et déployer l'architecture technique cible d'une plateforme de données moderne cloud-native, capable de supporter les paradigmes actuels (Data Lake, Lakehouse, Data Mesh, Dataspaces) dans des environnements mono-cloud, multi-cloud ou hybrides. Cette prestation vise à traduire les besoins stratégiques et fonctionnels en une infrastructure opérationnelle, performante, sécurisée, conforme et optimisée financièrement, en intégrant les meilleures pratiques DevOps/DataOps, GitOps, FinOps et de sécurité cloud-native. Cette UO intègre les pratiques modernes de déploiement continu, d'observabilité, de conformité réglementaire (RGPD, SecNumCloud, ANSSI), et d'optimisation des coûts cloud pour garantir une plateforme robuste et évolutive.

CONTENU ET MODALITÉS D'EXÉCUTION

Analyse des besoins et alignement stratégique cloud-native :

- **Collaboration architecture** : Travail avec les équipes architecture pour traduire les décisions en plan de déploiement multi-environnements
- **Stratégies de migration** : Définition des approches de migration et d'évolutivité
- **Évaluation comparative** : Analyse des coûts et performances cross-cloud

Sélection et configuration des technologies cloud-native :

- **Services cloud managés** : Choix et paramétrage optimisés pour chaque composant
- **Outils open-source** : Intégration des solutions communautaires
- **Évaluation TCO** : Comparaison AWS vs Azure vs GCP

Conception détaillée de l'infrastructure cloud-native :

- **Architectures réseau** : VPC, subnets, security groups, zones de disponibilité
- **Stratégies multi-cloud/hybrides** : Interconnexions et portabilité
- **Politiques IAM granulaires** : Chiffrement end-to-end et conformité réglementaire
- **Auto-scaling et load balancing** : Optimisation des performances et coûts
- **Architecture de reprise après sinistre** : Backup automatisé et RTO/RPO optimisés

Déploiement GitOps et Infrastructure as Code :

- **Outils** : Terraform, Pulumi, CDK, Helm, ArgoCD
- **Pipelines CI/CD** : Déploiement reproductible, versionné et auditable
- **Stratégies de déploiement** : Blue-green, canary, rolling deployments

Observabilité three pillars :

- **Monitoring** : Prometheus/Grafana avec métriques métiers
- **Logging** : ELK/Loki avec agrégation centralisée
- **Tracing** : Jaeger/Zipkin pour le suivi distribué
- **Alerting intelligent** : Notifications prédictives et escalade automatique

Mise en place des couches de données optimisées :

- **Formats modernes** : Delta Lake, Iceberg, Hudi avec partitioning intelligent
- **Lifecycle management** : Automatisation des politiques de rétention
- **Optimisation des accès** : Indexation et compression adaptatives

Intégration des services avec orchestration :

- **Kubernetes** : Déploiement et configuration des workloads
- **Service mesh** : Istio pour la communication sécurisée
- **Gouvernance cloud-native** : Intégration des outils de gouvernance

Sécurité cloud-native :

- **Contrôles de sécurité** : RBAC, network policies, pod security standards
- **Scanning de vulnérabilités** : Intégration continue dans les pipelines
- **Conformité continue** : Validation automatique des standards

Configuration FinOps et optimisation des coûts :

- **Monitoring des coûts** : Tableaux de bord temps réel et alerting budgétaire
- **Ajustement de taille automatique** : Optimisation des ressources
- **Recommandations d'optimisation** : IA pour l'optimisation prédictive

Tests d'intégration, performance et résilience :

- **Tests de charge** : Validation des performances sous stress
- **Chaos engineering** : Tests de résilience et identification des faiblesses
- **Reprise après sinistre** : Validation des procédures de récupération

Modèle d'exécution :

- **GitOps et Infrastructure as Code** : Déploiement entièrement automatisé avec versioning
- **Stratégies de déploiement avancées** : Blue-green, canary avec validation automatique
- **DevOps/DataOps/FinOps** : Équipes cross-fonctionnelles avec responsabilités partagées
- **Sécurité et conformité by design** : Intégration des contrôles dès le déploiement

PROFIL(S) PRESENTI(S)

- Architecte Cloud Data Senior (certification AWS/Azure/GCP)
- Ingénieur DataOps/MLOps Senior (expertise Kubernetes, GitOps)
- Expert Sécurité Cloud et Conformité (SecNumCloud, ANSSI)
- Ingénieur SRE pour l'observabilité
- Expert FinOps pour l'optimisation des coûts cloud

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Environnements	1-2	3-5	>5
Sources de données	<10	10-50	>50
Utilisateurs	<100	100-1K	>1K
Volumes	<1TB	1-100TB	>100TB
Intégrations	<5	5-20	>20
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	10 jours	15 jours	20 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Dossier d'Architecture Technique Détaillée cloud-native	2 semaines	3 semaines	4 semaines
Repository GitOps avec scripts IaC complets	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Configuration de l'observabilité (monitoring, logging, tracing)	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Documentation de sécurité et conformité réglementaire	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
Configuration FinOps et tableaux de bord de coûts	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Documentation complète d'installation, configuration et opération	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Rapports de tests complets (intégration, performance, sécurité, résilience)	Après chaque phase	Après chaque phase	Après chaque phase
Runbooks et procédures d'incident response	Avant production	Avant production	Avant production
Plan et procédures de reprise après sinistre testés	Avant production	Avant production	Avant production
Procès-verbal de recette technique de la plateforme	Fin de mise en œuvre	Fin de mise en œuvre	Fin de mise en œuvre

VIII.2.2 UO 6.2.2 - ADMINISTRATION ET MAINTENANCE DE PLATEFORME

OBJET

L'UO a pour objet d'assurer l'administration quotidienne et la maintenance préventive et corrective d'une plateforme de données cloud-native en production, selon les principes SRE (Site Reliability Engineering). Cette prestation couvre l'observabilité complète (monitoring, logging, tracing), la gestion automatisée des ressources, l'optimisation FinOps, la sécurité continue, la résolution d'incidents, et l'amélioration continue de la plateforme pour garantir sa disponibilité, performance, sécurité et conformité réglementaire. Cette UO intègre les pratiques modernes d'administration cloud-native, incluant l'observabilité three pillars, le chaos engineering, l'optimisation FinOps, la compliance as code, et la gestion multi-cloud/hybride pour assurer une plateforme robuste et optimisée.

CONTENU ET MODALITÉS D'EXÉCUTION

Observabilité et monitoring avancés :

- **Three pillars** : Metrics (Prometheus/Grafana), Logs (ELK/Loki), Traces (Jaeger/Zipkin)
- **Alerting intelligent** : Notifications prédictives et escalade automatique

- **Tableaux de bord temps réel** : Métriques métiers et techniques

Gestion des SLI/SLO :

- **Service Level Indicators** : Définition et monitoring des indicateurs clés
- **Service Level Objectives** : Objectifs de performance et disponibilité

Gestion automatisée des ressources et optimisation FinOps :

- **Auto-scaling intelligent** : Adaptation automatique aux charges
- **Ajustement de taille automatique** : Optimisation continue des ressources
- **Monitoring des coûts** : Suivi temps réel et alerting budgétaire
- **Recommandations d'optimisation** : IA pour l'optimisation prédictive

Administration GitOps :

- **Infrastructure as Code** : Gestion versionnée de l'infrastructure
- **Rollback automatique** : Retour en arrière en cas de problème
- **Audit trail complet** : Traçabilité de tous les changements

Maintenance préventive automatisée :

- **Mises à jour automatisées** : Patches de sécurité et mises à jour système
- **Tests automatisés** : Validation des mises à jour avant déploiement
- **Pipelines CI/CD** : Intégration continue des maintenances

Chaos engineering et tests de résilience :

- **Tests de chaos réguliers** : Validation de la robustesse
- Identification des points de défaillance : Amélioration proactive
- **Tests de reprise après sinistre** : Validation des procédures de récupération

Gestion avancée des incidents :

- **Diagnostic automatisé** : Identification rapide des causes
- **Résolution guidée par l'IA** : Assistance intelligente à la résolution
- **Post-mortems sans blâme** : Amélioration continue des processus

Sauvegarde et reprise après sinistre automatisés :

- **Stratégies de backup** : Automatisation complète des sauvegardes
- Tests réguliers de restauration : Validation de l'intégrité
- **RTO/RPO optimisés** : Objectifs de récupération ambitieux

Sécurité et conformité continues :

- **IAM automatisé** : Gestion des accès et permissions
- **Scanning continu** : Détection des vulnérabilités
- **Compliance as code** : Validation automatique de la conformité

- **Monitoring réglementaire** : Suivi RGPD, SecNumCloud, ANSSI

Gestion multi-cloud et hybride :

- **Administration unifiée** : Gestion centralisée des ressources
- **Optimisation cross-cloud** : Optimisation des coûts multi-cloud
- **Portabilité** : Gestion de la portabilité des workloads

Modèle d'exécution :

- **Support selon SLA** : Disponibilité selon les SLO avec monitoring des error budgets
- **Approche SRE proactive** : Anticipation par l'observabilité et le chaos engineering
- **Collaboration DevOps/DataOps/FinOps** : Intégration complète des équipes
- **Amélioration continue** : Optimisation basée sur les métriques et les retour d'expérience utilisateur

PROFIL(S) PRESENTI(S)

- Ingénieur SRE spécialisé plateformes data
- Administrateur Cloud (certification AWS/Azure/GCP)
- Ingénieur DataOps/MLOps Senior (expertise Kubernetes, observabilité)
- Expert FinOps pour l'optimisation des coûts cloud
- Spécialiste Sécurité Cloud et Conformité

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Composants	<20	20-100	>100
Environnements	1-2	3-5	>5
Utilisateurs	<100	100-1K	>1K
Volumes de données	<1TB	1-100TB	>100TB
Intégrations	<10	10-50	>50
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	--	Prestation continue	Prestation continue

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise
Tableaux de bord d'observabilité temps réel (SLI/SLO, métriques métiers)	Mise à jour continue
Rapports FinOps et optimisation des coûts	Hebdomadaire
Rapports d'incidents avec post-mortems et actions d'amélioration	48h après résolution
Rapports de chaos engineering et tests de résilience	Mensuel
Rapports de maintenance automatisée et mises à jour	Hebdomadaire
Rapports de conformité et sécurité continue	Hebdomadaire
Documentation as code mise à jour automatiquement	Mise à jour continue
Bilan de disponibilité avec métriques SRE (uptime, MTTR, MTBF)	Mensuel
Rapports d'optimisation et recommandations d'amélioration	Mensuel
Tableaux de bord exécutifs avec KPIs métiers	Temps réel

VIII.2.3 UO 6.2.3 - MIGRATION DE DONNÉES ET DE SYSTÈMES

OBJET

L'UO a pour objet de planifier, concevoir et exécuter la migration de données et de systèmes existants vers la nouvelle plateforme de données cloud-native, en utilisant des stratégies de migration modernes (zero-downtime, blue-green, strangler fig). Cette prestation couvre l'analyse des systèmes sources, la définition des stratégies de migration avancées, la transformation des données avec observabilité complète, et la validation de l'intégrité avec conformité réglementaire pour assurer une transition fluide, sécurisée et conforme. Cette UO intègre les pratiques modernes de migration cloud-native, incluant la synchronisation en temps réel, l'automatisation complète, l'observabilité des migrations, la sécurité continue, et la conformité réglementaire (RGPD, SecNumCloud) pour garantir une migration robuste et optimisée.

CONTENU ET MODALITÉS D'EXÉCUTION

Analyse approfondie des systèmes sources :

- **Inventaire automatisé** : Découverte et catalogage des systèmes existants
- **Analyse des dépendances** : Cartographie des interdépendances
- **Profilage des données** : Analyse de la qualité et des volumes
- **Cartographie des flux** : Mapping des flux de données actuels

Définition de stratégies de migration cloud-native :

- **Stratégies zero-downtime** : Migration sans interruption de service
- **Blue-green deployment** : Basculement sécurisé entre environnements
- **Strangler fig pattern** : Migration progressive par composants
- **Plans de rollback automatisé** : Procédures de retour en arrière

Évaluation et sélection des outils de migration :

- **Outils cloud-native** : AWS DMS, Azure Data Factory, GCP Dataflow
- **Solutions open-source** : Apache NiFi, Airbyte, Debezium
- **Évaluation comparative** : Performance, coûts, et fonctionnalités

Conception des processus de transformation avancés :

- **Règles de transformation** : Définition avec validation automatique
- **Mappings intelligents** : Correspondances automatisées
- **Nettoyage automatisé** : Amélioration de la qualité des données
- **Enrichissement** : Ajout de métadonnées et contexte

Développement d'outils de migration automatisés :

- **Pipelines ETL/ELT** : Développement cloud-native avec CI/CD
- **Monitoring intégré** : Observabilité des processus de migration
- **Gestion des erreurs** : Reprise automatique et gestion des échecs

Observabilité des migrations :

- **Monitoring temps réel** : Métriques de progression et performance
- **Alerting intelligent** : Notifications sur les anomalies
- **Tableaux de bord de progression** : Suivi visuel de l'avancement
- **Métriques de qualité** : Validation continue des données

Sécurité et conformité :

- **Chiffrement end-to-end** : Protection des données en transit et au repos
- **Anonymisation/pseudonymisation** : Respect de la vie privée
- **Audit trail complet** : Traçabilité de toutes les opérations
- **Validation RGPD** : Conformité réglementaire continue

Exécution avec synchronisation continue :

- **Réplication temps réel** : Synchronisation des données
- **Validation continue** : Vérification de l'intégrité
- **Basculement automatisé** : Migration selon les stratégies définies

Validation et contrôle qualité automatisés :

- **Vérification d'intégrité** : Validation automatique des données
- **Tests de performance** : Validation des performances
- **Tests de conformité** : Vérification réglementaire

Gestion des rollbacks et reprise après sinistre :

- **Procédures automatisées** : Rollback intelligent en cas de problème
- Tests de reprise après sinistre : Validation des procédures
- **Plans de contingence** : RTO/RPO optimisés

Modèle d'exécution :

- **DevOps/DataOps par phases** : Migration progressive avec CI/CD
- **Observabilité continue** : Monitoring temps réel et validation automatique
- **Gestion proactive des risques** : Identification et mitigation automatisées
- **Collaboration cross-fonctionnelle** : Implication de toutes les parties prenantes

PROFIL(S) PRESENTI(S)

- Ingénieur DataOps/MLOps Senior (expertise pipelines, observabilité)
- Expert Migration Cloud (certification AWS/Azure/GCP)
- Spécialiste Sécurité et Conformité des migrations
- Expert Qualité des Données et Gouvernance
- Ingénieur SRE pour l'observabilité des migrations

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Sources de données	<5	5-20	>20
Volume de données	<1TB	1-100TB	>100TB
Systèmes sources	<3	3-10	>10
Downtime acceptable	>24h	1-24h	Zero-downtime
Conformité	Standards	RGPD	Multi-réglementaire
Architecture cible	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	30 jours	45 jours	60 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Plan de migration détaillé avec stratégies cloud-native	1 semaine	2 semaines	3 semaines
Analyse complète des systèmes sources avec profilage automatisé	2 semaines	3 semaines	4 semaines
Évaluation et sélection des outils de migration	3 jours	1 semaine	2 semaines
Configuration de l'observabilité et monitoring des migrations	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Pipelines de migration automatisés avec CI/CD	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Documentation de sécurité et conformité des migrations	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Rapports de validation automatisée et contrôle qualité	Temps réel	Temps réel	Temps réel
Plans et procédures de rollback testés	Avant chaque phase	Avant chaque phase	Avant chaque phase
Tableaux de bord de monitoring et métriques de migration	Temps réel	Temps réel	Temps réel
Documentation complète et guides de formation	Fin de migration	Fin de migration	Fin de migration
Procès-verbal de recette de la migration	Fin de prestation	Fin de prestation	Fin de prestation

VIII.2.4 UO 6.2.4 - OPTIMISATION ET PERFORMANCE DE PLATEFORME

OBJET

L'UO a pour objet d'analyser, optimiser et améliorer les performances d'une plateforme de données cloud-native en production, en intégrant les pratiques modernes d'optimisation automatisée, FinOps,

et observabilité. Cette prestation couvre l'identification des goulots d'étranglement via l'observabilité avancée, l'optimisation des ressources cloud avec auto-scaling intelligent, l'amélioration des temps de réponse, l'optimisation des coûts, et la mise en place de mécanismes d'optimisation continue basés sur l'IA pour maintenir des performances optimales et des coûts maîtrisés. Cette UO intègre les pratiques modernes d'optimisation cloud-native, incluant l'auto-tuning, l'optimisation FinOps, l'observabilité three pillars, l'optimisation des architectures serverless/microservices, et l'utilisation de l'IA pour l'optimisation prédictive et automatisée.

CONTENU ET MODALITÉS D'EXÉCUTION

Analyse de performance avec observabilité avancée :

- **Three pillars** : Metrics (Prometheus), Logs (ELK), Traces (Jaeger)
- **IA/ML pour l'analyse** : Détection automatique des goulots d'étranglement
- **Analyse prédictive** : Anticipation des problèmes de performance
- **Profiling distribué** : Analyse détaillée des performances

Optimisation FinOps et gestion des coûts :

- **Analyse des coûts cloud** : Identification des optimisations possibles
- **Ajustement de taille automatique** : Ajustement intelligent des ressources
- **Optimisation des instances** : Spot/preemptible, instances réservées, instances à la demande
- **Recommandations d'économies** : IA pour l'optimisation prédictive

Optimisation des requêtes et traitements cloud-native :

- **Requêtes distribuées** : Optimisation des requêtes SQL/NoSQL
- **Jobs Spark/Kubernetes** : Tuning des workloads de traitement
- **Pipelines de données** : Optimisation des flux ETL/ELT
- **Auto-tuning** : Optimisation automatisée basée sur l'IA

Optimisation de l'infrastructure cloud-native :

- **Auto-scaling intelligent** : Adaptation proactive aux charges
- **Load balancing optimisé** : Distribution intelligente du trafic
- **Configurations Kubernetes** : Tuning des clusters et workloads
- **Services cloud managés** : Optimisation des configurations

Mécanismes de cache avancés :

- **Cache distribué** : Redis Cluster, Memcached optimisés
- **Cache intelligent** : Stratégies basées sur l'IA
- **Patterns d'accès** : Optimisation des stratégies de cache
- **Invalidation intelligente** : Gestion automatique du cache

Optimisation du stockage cloud-native :

- **Partitioning intelligent** : Stratégies adaptatives
- **Indexation automatique** : Création et maintenance automatisées
- **Compression adaptative** : Optimisation selon les patterns d'usage
- **Lifecycle management** : Gestion automatique du cycle de vie

Optimisation des architectures modernes :

- **Microservices** : Optimisation des communications inter-services
- **Fonctions serverless** : Tuning des fonctions Lambda/Azure Functions
- **Event-driven architectures** : Optimisation des flux d'événements
- **Service mesh** : Optimisation d'Istio pour réduire la latence

Surveillance et monitoring continu avec IA :

- **Observabilité avancée** : Monitoring prédictif et intelligent
- **Détection d'anomalies** : IA pour identifier les dégradations
- **Alerting prédictif** : Notifications avant les problèmes
- **Optimisation automatique** : Ajustements basés sur les patterns

Auto-tuning et optimisation automatisée :

- **Bases de données** : Auto-tuning des paramètres
- **Clusters Kubernetes** : Optimisation automatique des ressources
- **Pipelines de données** : Ajustement automatique des configurations
- **Apprentissage continu** : Amélioration basée sur l'historique

Tests de charge et chaos engineering :

- **Tests de performance** : Validation sous charge réelle
- **Chaos engineering** : Identification des faiblesses
- **Tests de stress** : Validation des limites
- Validation des optimisations : Mesure de l'impact

Modèle d'exécution :

- **DevOps/DataOps itératif** : Optimisation continue avec CI/CD
- **SLI/SLO et error budgets** : Validation quantifiée des améliorations
- Collaboration cross-fonctionnelle : Optimisation holistique
- **Amélioration continue basée sur l'IA** : Apprentissage et adaptation automatiques

PROFIL(S) PRESENTI(S)

- Expert Performance Cloud-Native Senior (certification AWS/Azure/GCP)
- Ingénieur SRE spécialisé optimisation
- Architecte Data Senior (expertise cloud, microservices, serverless)
- Expert FinOps pour l'optimisation des coûts cloud
- Spécialiste IA/ML pour l'optimisation automatisée

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Composants	<20	20-100	>100
Utilisateurs	<100	100-1K	>1K
Volume de données	<1TB	1-100TB	>100TB
Requêtes/jour	<1M	1-100M	>100M
Latence requise	>1s	100ms-1s	<100ms
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	--	30 jours	40 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Rapport d'analyse de performance avec observabilité avancée	3 jours	1 semaine	2 semaines
Analyse FinOps et recommandations d'optimisation des coûts	3 jours	1 semaine	1 semaine
Plan d'optimisation détaillé cloud-native avec auto-tuning	1 semaine	2 semaines	3 semaines
Configuration de l'observabilité et	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau

monitoring prédictif			
Optimisations implémentées avec auto-scaling et auto-tuning	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Tableaux de bord de performance et métriques SRE temps réel	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Rapports de tests de charge, chaos engineering et validation	Après chaque phase	Après chaque phase	Après chaque phase
Configuration des systèmes d'optimisation automatisée	Au fil de l'eau	Au fil de l'eau	Au fil de l'eau
Documentation d'optimisation cloud-native et guides d'auto-tuning	Fin de prestation	Fin de prestation	Fin de prestation
Rapport final avec métriques SRE et recommandations FinOps	Fin de prestation	Fin de prestation	Fin de prestation

VIII.3 PRESTATION L6-3 : SÉCURITÉ ET CONFORMITÉ DE PLATEFORME

La Prestation L6-3 est entièrement dédiée à la sécurité et à la conformité des infrastructures data. Elle vise à mettre en place des mesures robustes pour protéger les données et les systèmes, tout en assurant le respect des normes et réglementations en vigueur. En résumé, la Prestation L6-3 est essentielle pour bâtir et maintenir une plateforme de données hautement sécurisée et conforme aux exigences réglementaires, en mettant l'accent sur la gestion des accès, le chiffrement des données et l'auditabilité des activités.

VIII.3.1 UO 6.3.1 - AUDIT DE SÉCURITÉ ET CONFORMITÉ

OBJET

L'UO a pour objet de réaliser un audit complet de la sécurité et de la conformité d'une plateforme de données cloud-native, en évaluant les mesures de protection modernes, l'alignement avec les réglementations et standards cloud (RGPD, SecNumCloud, ANSSI, SOC2, ISO 27017), et l'identification des vulnérabilités dans les architectures distribuées. Cette prestation vise à garantir que la plateforme respecte les standards de sécurité cloud-native, les exigences réglementaires, et les meilleures pratiques DevSecOps. Cette UO intègre les pratiques modernes d'audit de sécurité cloud-

native, incluant l'audit des pipelines CI/CD, la sécurité des conteneurs, l'audit automatisé continu, et la conformité aux standards cloud français et européens pour garantir une sécurité robuste et une conformité réglementaire complète.

CONTENU ET MODALITÉS D'EXÉCUTION

Audit de sécurité technique cloud-native :

- Évaluation des mesures de sécurité cloud: gestion des identités et des accès (IAM), chiffrement de bout en bout, sécurité réseau, sécurité des conteneurs et de Kubernetes
- Authentification avancée : multi-facteur, architecture Zero Trust
- Sécurité des architectures : microservices, serverless, service mesh

Audit de conformité réglementaire étendu :

- Standards français et européens : RGPD, SecNumCloud, ANSSI, SOC2, ISO 27017/27018
- Conformité sectorielle : PCI-DSS, directives métier
- Validation automatisée : Conformité « as code » (Compliance as code) et monitoring continu

Audit DevSecOps et CI/CD :

- Sécurité des pipelines : Scanning automatisé, security as code
- Gestion des secrets : Rotation automatique, vault management
- Tests de sécurité : Intégration continue des contrôles

Audit de sécurité des conteneurs et orchestration :

- Sécurité Kubernetes : RBAC, network policies, pod security standards
- Sécurité des conteneurs : Image scanning, runtime protection
- Service mesh : Istio security, mTLS, traffic policies

Évaluation des politiques et procédures cloud :

- Politiques de sécurité : Cloud security frameworks, procédures de réponse aux incidents
- Reprise après sinistre : Plans de continuité, tests de récupération
- Gouvernance des identités : IAM cloud, privilèges minimaux

Tests de pénétration cloud-native :

- Architectures distribuées : Tests spécialisés cloud, microservices, APIs
- Outils modernes : Cloud-specific penetration testing
- Simulation d'attaques : Advanced persistent threats, cloud breaches

Audit des accès et permissions cloud :

- IAM cloud : Gestion des identités fédérées, RBAC granulaire
- Gouvernance des accès : Certification, revue des privilèges
- Accès multi-cloud : Gestion unifiée des identités

Évaluation de la gouvernance des données cloud :

- Classification automatisée : Data discovery, labeling automatique
- Protection des données : Chiffrement, anonymisation, pseudonymisation
- Traçabilité RGPD : Audit trail, droit à l'oubli, portabilité

Audit de sécurité automatisé et continu :

- Outils de scanning et gestion des vulnérabilités
- Monitoring de sécurité : SIEM cloud, détection d'anomalies
- Réponse automatique : SOAR, réponse à incident automatisée

Audit de la résilience et reprise après sinistre :

- Stratégies de sauvegarde : Cloud backup, réplication inter-régions
- Plans de continuité : Gestion de crise
- Cyber-résilience : Recovery from cyberattacks, tests de reprise après attaque

Modèle d'exécution :

- Application de cadres de sécurité cloud reconnus : NIST, recommandations AWS, Azure, OVH et ECO
- Tests automatisés : Outils cloud-native, scanning continu
- Collaboration DevSecOps : Approche intégrée sécurité-développement-opérations
- Confidentialité renforcée : Chiffrement des données d'audit, accès sécurisés

PROFIL(S) PRESSENTI(S)

- Auditeur Sécurité Cloud Senior (certification CISSP, CISM, CISSP)
- Expert Conformité Cloud et Réglementaire (SecNumCloud, ANSSI, RGPD)
- Spécialiste Tests de Pénétration Cloud-Native (OSCP, CEH)
- Expert DevSecOps et Security as Code
- Spécialiste Sécurité Kubernetes et Conteneurs (CKS)

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Composants auditable	<50	50-200	>200
Environnements	1-2	3-5	>5
Standards de conformité	<3	3-7	>7
Utilisateurs	<500	500-5K	>5K

Intégrations	<10	10-50	>50
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	15 jours	25 jours	35 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livraison(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Plan d'audit détaillé cloud-native	3 jours	1 semaine	1 semaine
Rapport d'audit de sécurité technique cloud-native	1 semaine	2 semaines	3 semaines
Rapport d'audit de conformité réglementaire étendu	2 semaines	3 semaines	4 semaines
Rapport d'audit DevSecOps et CI/CD	1 semaine	2 semaines	3 semaines
Rapport d'audit sécurité conteneurs et Kubernetes	1 semaine	2 semaines	3 semaines
Rapport de tests de pénétration cloud-native	2 semaines	3 semaines	4 semaines
Rapport d'audit automatisé et monitoring de sécurité	1 semaine	2 semaines	2 semaines
Évaluation de la résilience et reprise après sinistre	1 semaine	2 semaines	3 semaines
Rapport d'audit consolidé avec scoring et roadmap	Fin de prestation	Fin de prestation	Fin de prestation
Plan d'action priorisé pour la remédiation	Fin de prestation	Fin de prestation	Fin de prestation
Recommandations d'outils de sécurité cloud-native	Fin de prestation	Fin de prestation	Fin de prestation

VIII.3.2 UO 6.3.2 - IMPLÉMENTATION DE MESURES DE SÉCURITÉ

OBJET

L'UO a pour objet de concevoir et d'implémenter des mesures de sécurité cloud-native techniques et organisationnelles pour protéger une plateforme de données distribuée contre les menaces modernes. Cette prestation couvre la mise en place de contrôles de sécurité Zero Trust, la configuration d'outils de protection cloud-native, l'implémentation de security as code, et l'établissement de procédures DevSecOps pour assurer la confidentialité, l'intégrité, la disponibilité, et la conformité réglementaire des données. Cette UO intègre les pratiques modernes de sécurité cloud-native, incluant la sécurité des conteneurs, l'automatisation de la sécurité, la conformité continue, et la protection des architectures distribuées pour garantir une sécurité robuste et adaptée aux enjeux contemporains.

CONTENU ET MODALITÉS D'EXÉCUTION

Conception des mesures de sécurité cloud-native :

- **Contrôles Zero Trust** : Never trust, always verify, least privilege access
- **Sécurité des microservices** : Service-to-service authentication, API security
- **Protection des APIs** : Rate limiting, authentication, authorization
- **Architectures distribuées** : Security by design, defense in depth

Implémentation des contrôles d'accès cloud :

- **IAM cloud avancé** : Role-based access control, attribute-based access control
- **Authentification multi-facteur** : Adaptive authentication, passwordless
- **RBAC granulaire** : Fine-grained permissions, just-in-time access
- **Identités fédérées** : Cross-cloud identity management, SSO

Configuration des outils de sécurité cloud-native :

- **Protection périmétrique** : WAF cloud, CASB, cloud firewalls
- **Détection et réponse** : SIEM cloud, EDR, analytiques comportementaux
- **Sécurité des conteneurs** : Image scanning, runtime protection
- **Service mesh security** : Istio, Linkerd, traffic encryption

Implémentation de la sécurité des conteneurs et Kubernetes :

- **Pod security standards** : Security contexts, admission controllers
- **Network policies** : Microsegmentation, traffic isolation
- **Admission controllers** : Policy enforcement, compliance validation
- **Image scanning** : Vulnerability assessment, compliance checking

Mise en place du chiffrement avancé :

- **Chiffrement end-to-end** : Data in transit, data at rest, data in use
- **Gestion des clés** : Cloud KMS, key rotation, HSM integration
- **Chiffrement automatique** : Transparent encryption, field-level encryption
- **Rotation automatique** : Key lifecycle management, automated renewal

Implémentation DevSecOps et security as code :

- **Pipelines CI/CD sécurisés** : Security gates, automated testing
- **Scanning automatisé** : SAST, DAST, dependency scanning
- **Policy as code** : Infrastructure security policies, compliance automatisisation
- **Tests de sécurité** : Automated security testing, penetration testing

Établissement de procédures de sécurité cloud :

- **Réponse à incident**: Automated response, playbook execution
- **Reprise après sinistre** : Cloud backup, cross-region replication
- **Gestion des vulnérabilités** : Automated patching, vulnerability management
- **Orchestration** : SOAR integration, workflow automation

Implémentation de la conformité automatisée :

- **Compliance as code** : Automated compliance checking, policy enforcement
- **Monitoring continu** : Real-time compliance monitoring, alerting
- **Reporting automatisé** : Tableaux de bord de conformité, audit reports
- **Standards** : RGPD, SecNumCloud, SOC2, ISO 27017

Formation et sensibilisation DevSecOps :

- **Sécurité cloud-native** : Best practices, threat awareness
- **DevSecOps practices** : Secure coding, security testing
- **Réponse à incident**: Crisis management, communication protocols
- **Compliance** : Regulatory requirements, privacy protection

Tests et validation automatisés :

- **Tests de sécurité** : Automated penetration testing, vulnerability scanning
- **Chaos engineering** : Security chaos testing, resilience validation
- **Validation continue** : Continuous security assessment, monitoring
- **Monitoring** : Real-time security monitoring, threat detection

Modèle d'exécution :

- **DevSecOps par phases** : Intégration CI/CD, tests automatisés, retour d'expérience utilisateur continu
- **Validation automatisée** : Monitoring temps réel, alerting intelligent
- **Collaboration cross-fonctionnelle** : Sécurité holistique, responsabilités partagées
- **Amélioration continue** : Adaptation automatique, threat intelligence

PROFIL(S) PRESENTI(S)

- Ingénieur Sécurité Cloud-Native Senior (certification CISSP, CCSP)
- Architecte Sécurité Cloud et Zero Trust
- Expert DevSecOps et Security as Code
- Spécialiste Sécurité Kubernetes et Conteneurs (CKS)
- Expert Cryptographie et Gestion des Clés Cloud

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Composants sécurisés	<50	50-200	>200
Environnements	1-2	3-5	>5
Mesures de sécurité	<20	20-100	>100
Intégrations	<10	10-50	>50
Standards de conformité	<3	3-7	>7
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	25 jours	35 jours	45 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Plan d'implémentation sécurité cloud-native	3 jours	1 semaine	1 semaine
Configuration IAM cloud et contrôles d'accès avancés	2 semaines	3 semaines	4 semaines
Configuration des outils de sécurité cloud-native	3 semaines	4 semaines	5 semaines
Implémentation sécurité conteneurs et Kubernetes	2 semaines	3 semaines	4 semaines

Implémentation chiffrement avancé et gestion des clés	2 semaines	3 semaines	4 semaines
Intégration DevSecOps et security as code	3 semaines	4 semaines	5 semaines
Configuration compliance automatisée et monitoring	3 semaines	4 semaines	5 semaines
Procédures de sécurité cloud et incident response	3 semaines	5 semaines	6 semaines
Tests de sécurité automatisés et chaos engineering	3 semaines	5 semaines	6 semaines
Documentation as code et guides de sécurité	Fin de prestation	Fin de prestation	Fin de prestation
Rapport de validation et certification de sécurité	Fin de prestation	Fin de prestation	Fin de prestation

VIII.3.3 UO 6.3.3 - GESTION DES IDENTITÉS ET DES ACCÈS

OBJET

L'UO a pour objet de concevoir et d'implémenter un système de gestion des identités et des accès (IAM) cloud-native pour une plateforme de données distribuée, permettant de contrôler et de sécuriser l'accès aux ressources selon les principes Zero Trust, moindre privilège, et just-in-time access. Cette prestation couvre la mise en place de mécanismes d'authentification moderne, d'autorisation granulaire, de gestion des identités de service, et de traçabilité complète des accès dans des environnements multi-cloud et hybrides. Cette UO intègre les pratiques modernes d'IAM cloud-native, incluant la gestion des identités de workload, l'IAM as Code, l'authentification adaptative, et l'intégration avec les architectures Zero Trust pour garantir une sécurité d'accès robuste et évolutive.

CONTENU ET MODALITÉS D'EXÉCUTION

Conception de l'architecture IAM cloud-native

- Architecture Zero Trust avec validation continue.
- Identités humaines : Gestion du cycle de vie des utilisateurs et gestion des accès basée sur les rôles.
- Identités de service : Comptes de service et identités de workloads.
- Environnements multi-cloud : Identité fédérée et accès inter-cloud.

Implémentation de l'authentification :

- Authentification adaptative : Authentification basée sur le risque et accès contextuel.
- MFA avancé : Authentification biométrique et tokens matériels.
- Authentification sans mot de passe : FIDO2, WebAuthn, certificats numériques.
- SSO cloud : Authentification unique et fédérée.
- Fédération multi-cloud : Fédération d'identités cross-cloud.

Gestion des autorisations avancées :

- RBAC/ABAC granulaires : Permissions fines et accès basé sur les attributs.
- Policy as Code : Gestion des politiques d'accès via Infrastructure as Code.
- Autorisation contextuelle : Accès basé sur localisation, temps et dispositif.
- Accès Just-in-time : Accès temporaire avec workflows d'approbation.
- Élévation de privilèges : Escalade temporaire des privilèges.

Gestion des identités de service et workload :

- Comptes de service : Comptes Kubernetes, identités de services cloud.
- Identités de pods : Fédération d'identité pour workloads et accès containerisé.
- Fédération d'identités pour workloads : Authentification inter-cloud.
- Rotation automatique : Rotation automatique des identifiants et gestion des secrets.

Provisioning et gestion du cycle de vie automatisés

- IAM as Code : Gestion des identités via Infrastructure as Code.
- Intégration HR/SIRH : Provisioning automatique des utilisateurs et attribution des rôles.
- Auto-provisioning : Provisioning automatique basé sur les rôles.
- Déprovisionnement intelligent : Suppression automatisée des accès et détection des comptes orphelins.

Audit et traçabilité avancés

- Logging centralisé : Suivi centralisé des accès et audits.
- Audit trail immuable : audit logs infalsifiables, intégration blockchain.
- Analytique comportementale : Analyse du comportement utilisateur et détection d'anomalies.
- Détection d'anomalies : Détection pilotée par IA et scoring des risques.

Gestion des privilèges cloud-native

- PAM cloud : Gestion des accès privilégiés et sessions.
- Accès temporaire : Accès privilégié Just-in-time, sessions limitées dans le temps.
- Enregistrement des sessions : Audit des sessions privilégiées.
- Procédures Break-glass : Accès d'urgence avec workflows d'approbation.

IAM as Code et automatisation

- Politiques versionnées : Gestion versionnée des politiques et suivi des changements.
- Déploiement automatisé : Déploiement automatisé des politiques avec rollback possible.
- Tests de politiques : Validation des politiques et frameworks de tests.
- Intégration CI/CD : Intégration continue pour la gestion des changements d'accès.

Intégration avec l'écosystème cloud

- Services cloud natifs : Intégration AWS IAM, Azure AD, GCP IAM, ECO...
- Annuaire hybrides : Intégration Active Directory et LDAP.
- Systèmes existants : Intégration des systèmes existants et support de migration.

Gouvernance et conformité IAM

- Contrôles automatisés : Vérification automatique de conformité et application des politiques.
- Certification des accès : Revue périodique et certification des accès.
- Reporting réglementaire : Conformité RGPD, SOX.
- Audit automatisé : Suivi automatisé des accès et conformité.

Modèle d'exécution

- DevSecOps par phases : IAM as Code, tests automatisés, déploiement continu.
- Validation automatisée : Tests des politiques, validation des accès et monitoring.
- Collaboration cross-fonctionnelle : Gouvernance holistique et responsabilités partagées.
- Zero Trust by design : Vérification continue et accès contextuel.

PROFIL(S) PRESSENTI(S)

- Architecte IAM Cloud-Native Senior (certification CISSP, SABSA)
- Spécialiste IAM as Code et Automatisation
- Expert Identités de Service et Workload (Kubernetes, Service Mesh)
- Spécialiste PAM Cloud et Privilege Management
- Expert Analytics IAM et Détection d'Anomalies

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Identities gérées	<1K	1K-10K	>10K

Systèmes intégrés	<5	5-20	>20
Politiques d'accès	<50	50-500	>500
Environnements	1-2	3-5	>5
Standards de conformité	<3	3-7	>7
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	30 jours	40 jours	50 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livraison(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Architecture IAM cloud-native et Zero Trust	1 semaine	2 semaines	2 semaines
Configuration authentification moderne et adaptative	2 semaines	3 semaines	4 semaines
Politiques d'autorisation avancées et policy as code	3 semaines	4 semaines	5 semaines
Gestion des identités de service et workload	2 semaines	3 semaines	4 semaines
Processus de provisioning automatisé et IAM as Code	3 semaines	4 semaines	5 semaines
Configuration audit avancé et analytiques comportementaux	3 semaines	4 semaines	5 semaines
Solution PAM cloud-native et privilege management	4 semaines	5 semaines	6 semaines
Intégration CI/CD et automatisation IAM	4 semaines	5 semaines	6 semaines
Contrôles de conformité automatisés et reporting	4 semaines	5 semaines	6 semaines
Documentation as code et guides d'administration	Fin de prestation	Fin de prestation	Fin de prestation

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Rapport de validation et certification IAM	Fin de prestation	Fin de prestation	Fin de prestation

VIII.3.4 UO 6.3.4 - MONITORING ET GESTION DES INCIDENTS DE SÉCURITÉ

OBJET

L'UO a pour objet de mettre en place un système de monitoring de sécurité cloud-native et de gestion automatisée des incidents pour une plateforme de données distribuée, permettant de détecter, d'analyser, et de répondre automatiquement aux menaces modernes. Cette prestation couvre la mise en place d'outils de surveillance avancés (SIEM/SOAR cloud-native), l'automatisation de la réponse aux incidents, l'IA pour la détection d'anomalies, et la formation des équipes aux pratiques de cybersécurité moderne. Cette UO intègre les pratiques modernes de cybersécurité, incluant l'automatisation SOAR, l'IA/ML pour la détection, le threat hunting avancé, et le monitoring de sécurité des architectures cloud-native pour garantir une protection proactive et une réponse rapide aux cybermenaces.

CONTENU ET MODALITÉS D'EXÉCUTION

Mise en place du monitoring de sécurité cloud-native :

- SIEM/SOAR cloud : gestion des informations et événements de sécurité cloud-native
- Monitoring des conteneurs : surveillance de la sécurité des conteneurs, runtime protection
- Sécurité Kubernetes : monitoring de la sécurité des pods, mise en œuvre des politiques réseau
- Architectures distribuées : sécurité des microservices, surveillance du Service Mesh

Définition des règles de détection avancées :

- Règles basées sur l'IA/ML : apprentissage automatique appliqué à la détection de menaces
- Détection comportementale : analyse du comportement des utilisateurs et entités (UEBA – User and Entity Behavior Analytics)
- Chasse aux menaces automatisée (Automated threat hunting), détection proactive
- Signatures cloud : signatures de menaces spécifiques au cloud (Cloud-specific

threat signatures), modèles d'attaque (attack patterns)

Automatisation SOAR et orchestration :

- Playbooks automatisés : scénarios de réponse aux incidents automatisés
- Réponse orchestrée : coordination de la réponse entre outils de sécurité
- Intégration d'outils : intégration des solutions de sécurité, automatisation des workflows
- Réaction automatique : réponse automatique aux menaces, confinement

Gestion automatisée des alertes et incidents :

- Triage automatisé : tri des alertes automatisé par IA, hiérarchisation des priorités
- Escalade intelligente : escalade intelligente selon la gravité et le contexte
- Corrélation d'événements : corrélation des événements de sécurité, reconnaissance de schémas (pattern recognition)
- Réduction des faux positifs : ajustement des alertes pour limiter les faux positifs

Réponse aux incidents automatisée :

- Confinement automatique : confinement automatisé des menaces
- Isolation intelligente : isolation intelligente en fonction de l'analyse de la menace
- Éradication orchestrée : éradication coordonnée des menaces, remédiation
- Récupération assistée : récupération assistée par IA, procédures de restauration

Threat hunting et intelligence :

- Threat hunting proactif : chasse proactive aux menaces, investigation guidée par hypothèses
- Flux de renseignement sur les menaces : intégration de flux externes de renseignement sur les menaces (threat intelligence feeds)
- Analyse prédictive : analyse prédictive des menaces, évaluation des risques
- Veille automatisée : collecte automatisée de renseignements sur les menaces

Analyse forensique cloud-native :

- Investigation cloud : outils de forensic cloud, collecte de preuves
- Forensics automatisé : analyse forensique automatisée, extraction d'artefacts
- Reconstruction de timeline : reconstitution chronologique d'incident, analyse du chemin d'attaque
- Artefacts distribués : analyse d'artefacts distribués, corrélation inter-systèmes

Monitoring DevSecOps et CI/CD :

- Sécurité des pipelines : surveillance de la sécurité des pipelines CI/CD
- Détection continue : détection continue des vulnérabilités, analyses de

sécurité continues

- Monitoring des déploiements : surveillance de la sécurité des déploiements, suivi des changements

Reporting et communication avancés :

- Tableaux de bord temps réel : suivi de la sécurité en temps réel, reporting exécutif
- Rapports automatisés : rapports d'incident automatisés, reporting conformité
- Communication proactive : communication proactive avec les parties prenantes, notifications d'alerte
- Métriques de cybersécurité : indicateurs et tendances de sécurité (métriques de sécurité, KPIs, analyse des tendances)

Formation et sensibilisation :

- Threat hunting : formation aux techniques avancées de chasse aux menaces, entraînement à l'utilisation des outils
- Simulation d'incidents : exercices de simulation d'incidents, exercices sur table
- Cyber-résilience : formation à la cyber-résilience, gestion de crise
- Menaces émergentes : sensibilisation aux menaces émergentes, entraînement aux techniques d'attaque

Modèle d'exécution :

- Surveillance automatisée 24/7 : monitoring continu, détection par IA
- Réponse orchestrée : réponse automatisée, escalade intelligente
- Collaboration DevSecOps : opérations de sécurité intégrées, responsabilité partagée
- Threat intelligence proactive : renseignement sur les menaces proactif, défense adaptative

PROFIL(S) PRESSENTI(S)

- Analyste SOC Senior et Expert SOAR (certification GCIH, GCFA)
- Expert Threat Hunting et Intelligence (GIAC, SANS)
- Spécialiste IA/ML pour la Cybersécurité
- Expert Sécurité Cloud et Conteneurs (CKS, CCSP)
- Consultant Cyber-Résilience et Gestion de Crise

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Sources de logs	<100	100-1K	>1K
Événements/jour	<1M	1M-100M	>100M

Règles de détection	<100	100-1K	>1K
Intégrations SOAR	<10	10-50	>50
Environnements	1-2	3-5	>5
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	Implémentation 20 jours puis prestation continue	Implémentation 30 jours puis prestation continue	Implémentation 45 jours puis prestation continue

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrible(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Configuration monitoring sécurité cloud-native et SIEM/SOAR	2 semaines	3 semaines	4 semaines
Règles de détection avancées et modèles IA/ML	1 semaine	2 semaines	3 semaines
Configuration automatisation SOAR et playbooks	3 semaines	4 semaines	5 semaines
Procédures de gestion automatisée des incidents	3 semaines	4 semaines	5 semaines
Playbooks de réponse orchestrée aux incidents	3 semaines	4 semaines	6 semaines
Configuration threat hunting et intelligence	2 semaines	3 semaines	4 semaines
Configuration outils d'analyse forensique cloud	3 semaines	4 semaines	5 semaines
Monitoring	2 semaines	3 semaines	3 semaines

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
DevSecOps et sécurité CI/CD			
Tableaux de bord temps réel et rapports automatisés	Continu	Continu	Continu
Métriques de cybersécurité et KPIs (MTTR, MTDD)	Mensuel	Mensuel	Mensuel
Documentation complète et guides opérationnels	Fin d'implémentation	Fin d'implémentation	Fin d'implémentation

VIII.4 PRESTATION L6-4 : SUPERVISION ET MONITORING DE PLATEFORME

La Prestation L6-4 est axée sur la garantie de la performance, de la disponibilité et de la robustesse opérationnelle des plateformes de données. En somme, la Prestation L6-4 est essentielle pour maintenir une plateforme de données performante, fiable et disponible en permanence, grâce à une supervision proactive, des architectures résilientes et une optimisation continue des traitements.

VIII.4.1 UO 6.4.1 - CONCEPTION DE L'ARCHITECTURE DE SUPERVISION

OBJET

L'UO a pour objet de concevoir une architecture d'observabilité cloud-native complète pour une plateforme de données distribuée, intégrant les trois piliers modernes (metrics, logs, traces) pour surveiller en temps réel les performances, la disponibilité, et la santé des systèmes. Cette prestation couvre la définition des métriques SLI/SLO, la conception de tableaux de bord intelligents,

l'établissement de processus d'alerting automatisés, et l'intégration d'IA pour l'analyse prédictive et l'observabilité proactive. Cette UO intègre les pratiques modernes d'observabilité cloud-native, incluant la supervision des conteneurs, l'observabilité des microservices, l'intégration OpenTelemetry, et l'analyse prédictive pour garantir une supervision efficace et proactive des architectures distribuées.

CONTENU ET MODALITÉS D'EXÉCUTION

Analyse des besoins d'observabilité cloud-native :

- **Composants distribués** : Identification des microservices, conteneurs, et services cloud
- **SLI/SLO** : Définition des Service Level Indicators et Objectives
- **Exigences de disponibilité** : Requirements cloud et résilience
- **Observabilité microservices** : Besoins spécifiques aux architectures distribuées

Conception de l'architecture d'observabilité moderne :

- **Trois piliers** : Architecture basée sur metrics, logs, traces
- **Outils cloud-native** : Prometheus, Grafana, Jaeger, Loki
- **OpenTelemetry** : Intégration pour l'instrumentation standardisée
- **Corrélation multi-sources** : Liaison des métriques, logs et traces

Définition des métriques et SLI/SLO :

- **Service Level Indicators** : Métriques de performance critiques
- **Service Level Objectives** : Objectifs de disponibilité et performance
- **Error Budgets** : Gestion des budgets d'erreur selon SRE
- **Métriques cloud-native** : Adaptées aux architectures distribuées

Architecture de tracing distribué :

- **Système de tracing** : Conception pour microservices
- **Corrélation des traces** : Suivi des requêtes distribuées
- **Analyse des performances** : Identification des goulots d'étranglement
- **OpenTelemetry** : Instrumentation automatique et manuelle

Conception des tableaux de bord intelligents :

- **Tableaux de bord adaptatifs** : Visualisations dynamiques selon le contexte
- **Drill-down automatique** : Navigation intelligente dans les données
- **Corrélation multi-sources** : Intégration metrics, logs, traces
- **Profils utilisateurs** : SRE, DevOps, métier, direction

Définition des seuils et alerting intelligent :

- **Alertes basées sur SLO** : Notifications selon les objectifs de service
- **Alerting adaptatif** : Machine learning pour réduire les faux positifs
- **Corrélation multi-sources** : Alertes contextuelles
- **Escalade automatique** : Workflows d'escalade intelligents

Architecture de stockage des métriques cloud-native :

- **Solutions time-series** : Prometheus, InfluxDB, TimescaleDB
- **Rétention intelligente** : Politiques de rétention adaptatives
- **Archivage automatisé** : Stockage long terme optimisé
- **Compression** : Optimisation des coûts de stockage

Observabilité des conteneurs et Kubernetes :

- **Supervision des pods** : Monitoring des workloads Kubernetes
- **Services et ingress** : Observabilité des services exposés
- **Monitoring des ressources** : CPU, mémoire, réseau, stockage
- **Observabilité des workloads** : Applications containerisées

Intégration IA/ML pour l'observabilité :

- **Analyse prédictive** : Prédiction des problèmes de performance
- **Détection d'anomalies** : Identification automatique des comportements anormaux
- **Recommandations** : Suggestions d'optimisation automatisées
- **Apprentissage continu** : Amélioration des modèles de prédiction

Intégration écosystème cloud et DevOps :

- **Outils cloud-native** : Intégration avec les services cloud managés
- **Supervision CI/CD** : Monitoring des pipelines de déploiement
- **Observabilité des déploiements** : Suivi des releases et rollbacks
- **GitOps** : Intégration avec les workflows GitOps

Modèle d'exécution :

- **Approche SRE** : Collaboration avec équipes SRE, DevOps, développement
- **Méthodologie cloud-native** : Conception itérative avec validation continue
- **Standards modernes** : OpenTelemetry, SRE practices, observabilité cloud
- **Évolutivité auto-scalable** : Architecture adaptative aux charges

PROFIL(S) PRESENTI(S)

- Architecte Observabilité Cloud-Native Senior (certification SRE, CKA)

- Expert SRE / DevOps
- Expert OpenTelemetry et Tracing Distribué
- Consultant Performance et Optimisation Cloud
- Spécialiste IA/ML pour l'Observabilité

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Composants à surveiller	<50	50-200	>200
Microservices	<10	10-50	>50
Environnements	1-2	3-5	>5
Métriques collectées	<1K	1K-10K	>10K
Utilisateurs	<100	100-1K	>1K
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	20 jours	30 jours	40 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Analyse des besoins d'observabilité cloud-native	3 jours	1 semaine	1 semaine
Architecture technique d'observabilité moderne	2 semaines	3 semaines	4 semaines
Catalogue des métriques, SLI/SLO et Error Budgets	1 semaine	2 semaines	3 semaines
Architecture de tracing distribué et OpenTelemetry	2 semaines	3 semaines	4 semaines
Maquettes des tableaux de bord intelligents	2 semaines	3 semaines	4 semaines

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
Spécifications de l'alerting intelligent et ML	3 semaines	4 semaines	5 semaines
Architecture de stockage time-series et rétention	2 semaines	3 semaines	4 semaines
Spécifications observabilité Kubernetes et conteneurs	2 semaines	3 semaines	3 semaines
Architecture IA/ML pour l'analyse prédictive	3 semaines	4 semaines	5 semaines
Plan d'intégration écosystème cloud et DevOps	2 semaines	3 semaines	4 semaines
Documentation d'architecture complète et runbooks	Fin de prestation	Fin de prestation	Fin de prestation

VIII.4.2 UO 6.4.2 - IMPLÉMENTATION DES OUTILS DE MONITORING

OBJET

L'UO a pour objet d'implémenter et de configurer une stack d'observabilité cloud-native complète pour une plateforme de données distribuée, intégrant les trois piliers modernes (metrics, logs, traces) avec automatisation Infrastructure as Code. Cette prestation couvre le déploiement automatisé des solutions d'observabilité, leur configuration via GitOps, l'intégration avec les architectures cloud-native, et la mise en place d'une surveillance auto-adaptative et intelligente. Cette UO intègre les pratiques modernes d'implémentation d'observabilité, incluant l'Infrastructure as Code, le déploiement automatisé, l'observabilité des conteneurs, et l'intégration avec les écosystèmes cloud pour garantir une surveillance efficace et évolutive.

CONTENU ET MODALITÉS D'EXÉCUTION

Déploiement automatisé des outils d'observabilité :

- **Infrastructure as Code** : Terraform, Helm pour déploiement reproductible
- **Solutions cloud-native** : Prometheus, Grafana, Jaeger, Loki, OpenTelemetry
- **Configuration GitOps** : Déploiement déclaratif avec ArgoCD/Flux
- **Versioning** : Gestion des versions et rollback automatique

Configuration des agents de collecte cloud-native :

- **Agents automatisés** : Prometheus exporters, OpenTelemetry collectors
- **Fluent Bit/Fluentd** : Collecte de logs distribuée
- **Déploiement Kubernetes** : DaemonSets et sidecar containers
- **Auto-discovery** : Découverte automatique des services

Configuration des sources de données distribuées :

- **Services cloud** : Intégration avec AWS CloudWatch, Azure Monitor, GCP Monitoring
- **Microservices** : Instrumentation automatique et manuelle
- **Bases de données** : Monitoring des performances et métriques
- **Service discovery** : Découverte automatique des endpoints

Implémentation du tracing distribué :

- **Jaeger/Zipkin** : Déploiement et configuration du tracing
- **OpenTelemetry** : Configuration des collectors et exporters
- **Instrumentation** : Automatique et manuelle des applications
- **Corrélation** : Liaison traces, logs, et métriques

Création des tableaux de bord intelligents :

- **Grafana** : Développement de tableaux de bord avec templates
- **Templates automatisés** : Génération automatique selon les services
- **Drill-down dynamique** : Navigation contextuelle dans les données
- **Visualisations adaptatives** : Adaptation selon les rôles utilisateurs

Configuration de l'alerting intelligent :

- **AlertManager** : Configuration des règles d'alerte
- **Règles basées sur SLO** : Alertes selon les objectifs de service
- **ML et réduction faux positifs** : Algorithmes d'apprentissage
- **Notifications modernes** : Tchap, Webconf, PagerDuty, webhooks

Implémentation de l'observabilité Kubernetes :

- **Monitoring des clusters** : Métriques des nodes, pods, services
- **Workloads** : Surveillance des déploiements et statefulsets
- **Ingress et services** : Monitoring du trafic réseau
- **Métriques spécialisées** : Resource quotas, HPA, VPA

Configuration de l'auto-scaling et auto-healing :

- **HPA/VPA** : Auto-scaling basé sur les métriques custom
- **Auto-scaling monitoring** : Scaling des outils de surveillance

- **Self-healing** : Redémarrage automatique des composants défectueux
- **Circuit breakers** : Protection contre les surcharges

Intégration écosystème cloud et DevOps :

- **Services cloud managés** : Intégration native avec les clouds
- **Pipelines CI/CD** : Monitoring des déploiements et builds
- **GitOps** : Intégration avec les workflows de déploiement
- **Outils DevOps** : Jenkins, GitLab CI, GitHub Actions

Implémentation de la rétention et archivage intelligents :

- **Politiques de rétention** : Configuration automatisée par criticité
- **Compression** : Optimisation du stockage des métriques
- **Archivage cloud** : Stockage long terme S3, Azure Blob, GCS
- **Lifecycle management** : Gestion automatique du cycle de vie

Tests automatisés et validation continue :

- **Tests d'observabilité** : Validation des métriques et alertes
- **Synthetic monitoring** : Tests proactifs des services
- **Chaos engineering** : Tests de résilience du monitoring
- **Health checks** : Surveillance de la santé du système de monitoring

Modèle d'exécution :

- **GitOps automatisé** : Déploiement via pipelines CI/CD et IaC
- **Tests continus** : Validation automatique avec rollback
- **Collaboration DevOps/SRE** : Intégration dans les workflows existants
- **Sécurité by design** : Chiffrement, authentification, audit trail

PROFIL(S) PRESSENTI(S)

- Ingénieur SRE/DevOps Cloud-Native Senior (certification CKA, CKAD)
- Expert Infrastructure as Code et GitOps (Terraform, Helm)
- Spécialiste Observabilité Kubernetes et Conteneurs
- Expert Outils Cloud-Native (Prometheus, Grafana, Jaeger)
- Spécialiste OpenTelemetry et Tracing Distribué

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Outils à déployer	<10	10-30	>30

Sources de données	<50	50-200	>200
Environnements	1-2	3-5	>5
Intégrations	<10	10-50	>50
Agents de collecte	<100	100-1K	>1K
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	25 jours	35 jours	45 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Déploiement automatisé des outils d'observabilité	1 semaine	2 semaines	3 semaines
Configuration automatisée des agents de collecte	2 semaines	3 semaines	4 semaines
Configuration des sources de données et service discovery	2 semaines	3 semaines	3 semaines
Implémentation du tracing distribué et OpenTelemetry	3 semaines	4 semaines	5 semaines
Tableaux de bord intelligents et adaptatifs	3 semaines	4 semaines	5 semaines
Configuration de l'alerting intelligent et ML	3 semaines	4 semaines	5 semaines
Observabilité Kubernetes et monitoring des workloads	2 semaines	3 semaines	4 semaines
Configuration auto-scaling et auto-healing	3 semaines	4 semaines	5 semaines
Intégrations écosystème cloud et DevOps	4 semaines	5 semaines	6 semaines
Rétention intelligente et	2 semaines	3 semaines	4 semaines

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
archivage automatisé			
Tests automatisés et validation continue	4 semaines	5 semaines	6 semaines
Documentation as code et runbooks interactifs	Fin de prestation	Fin de prestation	Fin de prestation

VIII.4.3 UO 6.4.3 - OPTIMISATION DES PERFORMANCES ET DE LA DISPONIBILITÉ

OBJET

L'UO a pour objet d'optimiser les performances, la disponibilité, et les coûts d'une plateforme de données cloud-native en utilisant l'analyse prédictive, l'auto-optimisation, et les pratiques FinOps. Cette prestation couvre l'analyse intelligente des métriques, l'identification automatisée des goulots d'étranglement, la mise en place d'auto-scaling intelligent, l'optimisation des coûts cloud, et l'implémentation de mécanismes d'auto-healing pour assurer un service optimal et économique. Cette UO intègre les pratiques modernes d'optimisation cloud-native, incluant l'auto-optimisation basée sur l'IA, l'optimisation des conteneurs et microservices, le FinOps, et l'optimisation continue pour garantir des performances optimales et une maîtrise des coûts.

CONTENU ET MODALITÉS D'EXÉCUTION

Analyse intelligente des performances :

- **IA/ML pour l'analyse** : Identification automatique des patterns de performance
- **Prédiction des goulots** : Anticipation des problèmes de performance
- **Analyse des tendances** : Étude des patterns de charge et d'utilisation
- **Corrélation multi-sources** : Analyse holistique des métriques

Identification automatisée des goulots d'étranglement :

- **Analyse temps réel** : Détection en continu des points de congestion
- **Composants distribués** : Analyse des microservices et conteneurs
- **Corrélation automatique** : Liaison des métriques multi-sources
- **Priorisation intelligente** : Classification par impact métier

Optimisation intelligente des ressources cloud :

- **Auto-tuning** : Ajustement automatique des configurations
- **Ajustement de taille** : Optimisation automatique des tailles d'instances
- **Optimisation Kubernetes** : Tuning des ressources pods et nodes
- **Serverless optimization** : Optimisation des fonctions cloud

Optimisation FinOps et gestion des coûts :

- **Analyse des coûts** : Monitoring en temps réel des dépenses cloud
- **Instances réservées** : Optimisation des commitments cloud
- **Instances à la demande** : Utilisation intelligente des instances préemptibles
- **Recommandations automatisées** : Suggestions d'économies basées sur l'IA

Amélioration de la disponibilité cloud-native :

- **Haute disponibilité** : Implémentation multi-zones et multi-régions
- **Auto-healing** : Récupération automatique des pannes
- **Circuit breakers** : Protection contre les cascades de pannes
- **Résilience microservices** : Patterns de résilience distribués

Optimisation des requêtes et traitements:

- **Requêtes distribuées** : Optimisation des requêtes
- **Pipelines de données** : Amélioration des performances ETL/ELT
- **Cache intelligent** : Stratégies de cache adaptatif
- **Accélération** : Optimisation des traitements critiques

Auto-scaling intelligent et prédictif :

- **HPA/VPA avancés** : Auto-scaling basé sur métriques custom
- **Scaling prédictif** : Anticipation des besoins de ressources
- **Multi-métriques** : Scaling basé sur plusieurs indicateurs
- **Scaling cross-services** : Coordination du scaling distribué

Optimisation des conteneurs et Kubernetes :

- **Ressources pods** : Optimisation des requests et limits
- **Workloads tuning** : Amélioration des performances applicatives
- **Images optimization** : Optimisation de la taille et sécurité
- **Réseau** : Optimisation des communications inter-pods

Optimisation des architectures serverless :

- **Fonctions cloud** : Tuning Lambda, Azure Functions, Cloud Functions
- **Cold starts** : Réduction des temps de démarrage
- **Concurrence** : Gestion intelligente de la concurrence

- **Memory optimization** : Optimisation de l'allocation mémoire

Tests de charge cloud-native et chaos engineering :

- **Tests distribués** : Validation des performances sous charge
- **Chaos engineering** : Tests de résilience et identification des faiblesses
- **Validation SLO** : Vérification des objectifs de service
- **Load testing** : Tests de montée en charge automatisés

Monitoring continu et auto-optimisation :

- **Boucles d'optimisation** : Amélioration continue automatisée
- **Alerting prédictif** : Notifications avant les problèmes
- **Feedback loops** : Apprentissage continu des optimisations
- **Recommandations IA** : Suggestions d'amélioration automatisées

Modèle d'exécution :

- **Approche SRE** : Optimisation basée sur SLI/SLO et Error Budgets
- **Auto-optimisation** : Amélioration continue automatisée
- **Collaboration DevOps/FinOps** : Optimisation holistique performance/coûts
- **Amélioration intelligente** : Apprentissage machine et adaptation

PROFIL(S) PRESSENTI(S)

- Expert Performance Cloud-Native et SRE (certification CKA, AWS/Azure)
- Spécialiste FinOps et Optimisation des Coûts Cloud
- Expert Optimisation Kubernetes et Conteneurs
- Spécialiste IA/ML pour l'Optimisation et l'Auto-tuning
- Spécialiste Chaos Engineering et Tests de Performance

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Composants à optimiser	<50	50-200	>200
Métriques analysées	<1K	1K-10K	>10K
Environnements	1-2	3-5	>5
Utilisateurs	<1K	1K-10K	>10K
Volume de données	<10TB	10TB-1PB	>1PB
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	30 jours	40 jours	50 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Analyse intelligente des performances et diagnostic IA	1 semaine	2 semaines	3 semaines
Identification automatisée des goulots d'étranglement	2 semaines	3 semaines	3 semaines
Plan d'optimisation cloud-native et FinOps	2 semaines	3 semaines	4 semaines
Analyse et optimisation des coûts cloud (FinOps)	2 semaines	3 semaines	4 semaines
Implémentation haute disponibilité et auto-healing	4 semaines	5 semaines	6 semaines
Optimisation des requêtes et traitements distribués	3 semaines	4 semaines	5 semaines
Configuration auto-scaling intelligent et prédictif	3 semaines	4 semaines	5 semaines
Optimisation conteneurs, Kubernetes et serverless	4 semaines	5 semaines	6 semaines
Tests de charge cloud-native et chaos engineering	5 semaines	6 semaines	7 semaines
Implémentation monitoring continu et auto-optimisation	4 semaines	5 semaines	6 semaines
Documentation et recommandations intelligentes	Fin de prestation	Fin de prestation	Fin de prestation

VIII.4.4 UO 6.4.4 - REPORTING ET ALERTING AVANCÉ

OBJET

L'UO a pour objet de mettre en place un système de reporting et d'alerting intelligent cloud-native pour une plateforme de données distribuée, intégrant l'IA/ML pour l'analyse prédictive, l'auto-remediation, et l'observabilité moderne. Cette prestation couvre la création de rapports temps réel adaptatifs, la configuration d'alertes intelligentes basées sur les SLO, l'implémentation d'auto-remediation, et l'établissement de tableaux de bord exécutifs avec analytics avancés pour fournir une visibilité complète et proactive. Cette UO intègre les pratiques modernes de reporting et alerting, incluant l'intelligence artificielle pour la prédiction, l'auto-remediation automatisée, le streaming analytics, et l'intégration avec les écosystèmes cloud-native pour garantir une observabilité intelligente et proactive.

CONTENU ET MODALITÉS D'EXÉCUTION

Conception des rapports intelligents temps réel :

- **Streaming analytics** : Rapports en temps réel avec traitement continu
- **Rapports adaptatifs** : Génération automatique selon le contexte
- **Corrélation automatique** : Intégration multi-sources de données
- **Insights IA** : Génération automatique d'analyses et recommandations

Configuration des alertes intelligentes et prédictives :

- **Alerting basé sur SLO/SLI** : Notifications selon les objectifs de service
- **Alertes prédictives ML** : Prédiction des problèmes avant qu'ils surviennent
- **Réduction faux positifs** : Algorithmes d'apprentissage pour filtrer
- **Corrélation multi-sources** : Alertes contextuelles et intelligentes

Création de tableaux de bord exécutifs intelligents :

- **Tableaux de bord adaptatifs** : Visualisations qui s'adaptent au contexte
- **Drill-down automatique** : Navigation intelligente dans les données
- **Analytics prédictifs** : Tendances et prédictions automatisées
- **Recommandations** : Suggestions d'actions basées sur l'IA

Implémentation de l'auto-remediation et runbooks automatisés :

- **Actions automatiques** : Résolution automatique des incidents courants
- **Runbooks intelligents** : Procédures adaptatives selon le contexte
- **Orchestration** : Coordination automatique des actions de résolution
- **Escalade intelligente** : Escalade automatique selon la criticité

Mise en place de notifications intelligentes multi-canal :

- **Notifications contextuelles** : Messages adaptés au destinataire et contexte

- **Escalade automatique** : Progression intelligente selon la réponse
- **Intégration moderne** : Tchap, Webconf, PagerDuty, webhooks
- **Personnalisation** : Préférences utilisateur et filtrage intelligent

Automatisation du reporting avancé :

- **Génération automatique** : Rapports périodiques avec insights IA
- **Distribution intelligente** : Envoi automatique aux bonnes personnes
- **Personnalisation automatique** : Adaptation selon les rôles et besoins
- **Scheduling adaptatif** : Fréquence adaptée à la criticité

Alerting prédictif et analyse d'anomalies :

- **IA/ML pour alerting** : Détection d'anomalies basée sur l'apprentissage
- **Prédiction de pannes** : Anticipation des défaillances système
- **Recommandations** : Suggestions d'actions préventives
- **Apprentissage continu** : Amélioration des modèles de prédiction

Reporting de conformité et SLO automatisé :

- **Rapports de conformité** : Génération automatique pour audits
- **Tracking SLO/Error Budgets** : Suivi automatique des objectifs
- **Reporting réglementaire** : Conformité RGPD, SOX, autres standards
- **Audit trail** : Traçabilité complète des actions et décisions

Intégration streaming analytics et temps réel :

- **Reporting temps réel** : Tableaux de bord et métriques en continu
- **Streaming des métriques** : Flux de données en temps réel
- **Analytics en continu** : Traitement et analyse en streaming
- **Event-driven reporting** : Rapports déclenchés par événements

Intégration écosystème cloud et ITSM :

- **Outils cloud-native** : Intégration avec services cloud managés
- **Systèmes ITSM** : ServiceNow, Jira Service Management
- **Orchestration workflows** : Coordination avec les processus ITIL
- **APIs modernes** : Intégrations via REST, GraphQL, webhooks

Analytics avancés et intelligence artificielle :

- **Analytics prédictifs** : Prédiction des tendances et problèmes
- **Recommandations automatisées** : Suggestions d'optimisation IA
- **Insights automatiques** : Découverte automatique de patterns
- **Apprentissage machine** : Amélioration continue des analyses

Modèle d'exécution :

- **Approche SRE** : Reporting basé sur SLI/SLO et observabilité moderne
- **Configuration intelligente** : Auto-tuning et adaptation continue
- **Tests automatisés** : Validation des alertes et rapports
- **Formation SRE** : Accompagnement aux pratiques d'observabilité

PROFIL(S) PRESSENTI(S)

- Spécialiste Reporting Intelligent et Analytics (BI/ML)
- Expert SRE et Observabilité Cloud-Native
- Spécialiste IA/ML pour l'Alerting et la Prédiction
- Spécialiste Streaming Analytics et Temps Réel
- Expert Intégration Cloud et ITSM

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Rapports à générer	<50	50-200	>200
Alertes configurées	<100	100-1K	>1K
Sources de données	<20	20-100	>100
Utilisateurs	<100	100-1K	>1K
Intégrations	<10	10-50	>50
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	25 jours	35 jours	45 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Rapports intelligents temps réel	2 semaines	3 semaines	4 semaines

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
et streaming analytics			
Configuration alertes intelligentes et prédictives	3 semaines	4 semaines	5 semaines
Tableaux de bord exécutifs avec analytics avancés	3 semaines	4 semaines	5 semaines
Implémentation auto-remediation et runbooks automatisés	3 semaines	4 semaines	5 semaines
Configuration notifications intelligentes multi-canal	2 semaines	3 semaines	3 semaines
Automatisation reporting avancé avec insights IA	4 semaines	5 semaines	6 semaines
Configuration alerting prédictif et détection d'anomalies	4 semaines	5 semaines	6 semaines
Reporting conformité et SLO automatisé	3 semaines	4 semaines	5 semaines
Intégration streaming analytics et temps réel	2 semaines	3 semaines	4 semaines
Intégrations écosystème cloud et ITSM	3 semaines	4 semaines	5 semaines
Analytics avancés et recommandations IA	4 semaines	5 semaines	6 semaines
Documentation interactive et guides SRE	Fin de prestation	Fin de prestation	Fin de prestation

VIII.4.5 UO 6.4.5 - SUIVI PERFORMANCE PRODUIT PLATEFORME

OBJET

L'objet de cette UO est de mettre en place et d'opérer un cadre de suivi de la performance des produits infrastructure. Cette prestation vise à mesurer l'impact réel des produits sur les utilisateurs et l'organisation avec des métriques avancées et des analytiques comportementaux, à identifier les opportunités d'amélioration par l'expérimentation continue et à fournir les analyses nécessaires pour orienter les décisions produit et les stratégies d'évolution basées sur des données probantes.

Cette UO est une démarche analytique et de reporting, cruciale pour la gestion de produit basée sur les données et l'optimisation continue de la valeur.

CONTENU ET MODALITÉS D'EXÉCUTION

Analyse et cadrage

L'objectif de cette phase est de cadrer la **performance métier et produit** à suivre, en alignement avec les **objectifs stratégiques** et les **résultats clés (OKR)** définis avec la direction produit et les métiers.

- Identification des **objectifs stratégiques** associés au produit (valeur d'usage, impact métier, performance économique, efficacité opérationnelle).
- Définition des **KPI mesurables et actionnables** : adoption, satisfaction, efficacité, qualité, coûts, productivité.
- Définition des **OKR trimestriels ou semestriels** pour l'équipe produit d'ingénierie, en cohérence avec la roadmap.
- Traduction des objectifs métier en **indicateurs d'ingénierie et d'exploitation** (livraison de valeur, vitesse, fiabilité, disponibilité).
- Cartographie des sources de données nécessaires au suivi (produit, usage, analytics, outils internes).
- Définition du **cadre de gouvernance de la performance produit** : fréquence de mesure, rôles, responsabilités.

Cette phase établit les bases du **pilotage orienté valeur** et de la mesure d'impact des activités d'ingénierie.

Mise en place du dispositif de mesure

L'équipe met en œuvre les mécanismes de **collecte, consolidation et visualisation** des données de performance produit.

- Intégration des **sources de données clés** : logs d'usage, analytics produit, tickets, incidents, données financières, satisfaction utilisateur.
- Mise en place de **pipelines de collecte et d'agrégation** (automatisation, API, intégration avec DataOps).
- Construction de **tableaux de bord de suivi des OKR/KPI**, avec une vue synthétique par périmètre produit.
- Mise en œuvre d'indicateurs combinés :
 - **Valeur métier** : taux d'adoption, volume d'utilisation, impact opérationnel.
 - **Valeur délivrée** : user stories livrées, délais, vitesse, ROI perçu.
 - **Efficacité produit** : réduction du temps de traitement, fiabilité, réduction d'incidents.
 - **Coûts et ressources** : coûts d'exploitation, efficacité de la chaîne de delivery.
- Intégration des métriques dans un environnement analytique moderne (Power BI, Metabase, Digidash, Tableau).

- Automatisation des extractions et calculs pour assurer la **traçabilité et la fiabilité** des données de performance.

Analyse de la performance et alignement sur les OKR

L'équipe produit d'ingénierie réalise une **analyse régulière des performances** pour vérifier l'alignement avec les OKR et identifier les écarts.

- Mesure continue des **résultats clés (KR)** et de leur avancement.
- Identification des **écarts entre valeur prévue et valeur réalisée**, avec analyse de causes.
- Suivi des **indicateurs de santé produit** : satisfaction utilisateurs internes, qualité, dette technique, stabilité.
- Analyse de la **performance économique** : coûts d'exploitation vs bénéfices métier.
- Évaluation de la **création de valeur par les releases** ou évolutions déployées.
- Corrélation entre **effort d'ingénierie et impact business** pour prioriser les futures itérations.
- Consolidation des résultats dans un reporting d'équipe ou comité produit.

Cette phase permet de piloter la performance selon une logique **"outcome over output"** — mesurer la valeur délivrée, pas seulement les livrables.

Amélioration continue et pilotage par la valeur

Sur la base des analyses précédentes, l'équipe met en œuvre une démarche d'**amélioration continue orientée résultats**.

- Revue périodique des OKR avec ajustement des cibles et indicateurs.
- Mise en œuvre d'**actions correctives ou d'optimisation** sur les produits ou processus.
- Utilisation de **modèles de causalité** (impact mapping, value stream mapping) pour identifier les leviers d'amélioration.
- Expérimentations contrôlées (tests A/B, hypothèses produit) pour valider les impacts métier.
- Priorisation des évolutions en fonction du **rapport valeur / effort / risque**.
- Documentation systématique des apprentissages et décisions pour enrichir la gouvernance produit.

Cette démarche renforce la **maturité produit** et permet d'inscrire la performance dans un cycle agile d'adaptation et de progression continue.

Modèle d'exécution

Thème	Modalités
Périmètre	Produits et plateformes à forte composante d'ingénierie (API, data products, plateformes d'échange, outils internes).
Objectif	Piloter la performance métier et produit en alignement avec les OKR globaux et les objectifs de valeur délivrée.
Méthodologie	Approche data-driven et OKR , avec revue mensuelle et synchronisation continue avec les parties prenantes.
Outils	Tableau de bord (Power BI, Metabase, Grafana, Digdash),

Thème	Modalités
	collectes automatisées, intégrations aux outils DevOps et analytics.
Qualité / Sécurité	Données de performance anonymisées, gouvernance des accès, traçabilité des mesures.
Livrables	Tableau de bord de suivi des OKR/KPI + Rapport de performance produit + Plan d'amélioration.
Critères d'acceptation	100 % des OKR suivis et mis à jour, indicateurs validés par les parties prenantes, actions d'amélioration tracées et priorisées.

PROFIL(S) PRESENTI(S)

- Responsable croissance produit (certifié Reforge, GrowthHackers)
- Data Scientist / Data Engineer spécialisé en analytique
- Analyste produit senior (expert plateformes analytiques)
- Expert en analytique comportementale
- Product Owner / Chef de projet produit

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Critère	Analytics basiques	Multi-product tracking	Enterprise-scale analytics
--	--	A/B testing simple	Advanced experimentation
--	--	--	Analyses par ML

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	5 jours	7 jours	10 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de
-------------	------------------

	remise
Framework de métriques produit moderne (North Star, HEART, PLG)	7 jours
Spécification technique de l'instrumentation analytics	10 jours
Tableaux de bord interactifs temps réel avec alerting	20 à 30 jours
Rapports d'analyse avancée par ML et recommandations	Hebdomadaire
Résultats d'expérimentations A/B	Continu
Compte rendu des ateliers avec actions priorisées	24 heures
Documentation complète de l'architecture analytics	Au fil de l'eau
Compte rendu ROI et mesure d'impact métier	Mensuel
Analyse de cohorte et de rétention	Bi-hebdomadaire
Analyse comparative (benchmark) et enseignements issus de l'analyse de marché	Trimestriel

VIII.5 PRESTATION L6-5 : GOUVERNANCE TECHNIQUE DE PLATEFORME

La Prestation L6-5 est dédiée à l'établissement d'une gouvernance technique solide et à la mise en place des outils facilitant la gestion et l'exploitation des données et de la plateforme. En somme, la Prestation L6-5 est fondamentale pour instaurer un cadre de gestion et d'exploitation structuré de la plateforme de données, en favorisant la transparence, la responsabilité et la capacité d'évolution future.

VIII.5.1 UO 6.5.1 - DÉFINITION DES POLITIQUES DE GOUVERNANCE TECHNIQUE

OBJET

L'UO a pour objet de définir les politiques de gouvernance technique cloud-native pour une plateforme de données distribuée, établissant les règles automatisées, standards as code, et processus DevOps nécessaires pour assurer une gestion cohérente, sécurisée, et économique de l'infrastructure moderne. Cette prestation couvre la définition des politiques d'architecture cloud-native, de sécurité by design, de performance SRE, de conformité automatisée, et de FinOps pour garantir la qualité, la pérennité, et la maîtrise des coûts de la plateforme. Cette UO intègre les

pratiques modernes de gouvernance, incluant Policy as Code, GitOps, gouvernance des conteneurs, FinOps, et gouvernance automatisée pour garantir une gestion efficace et évolutive des architectures cloud-native.

CONTENU ET MODALITÉS D'EXÉCUTION

Définition des politiques d'architecture cloud-native :

- **Standards d'architecture distribuée** : Établissement des patterns microservices et architectures cloud-native
- **Règles de développement** : Standards de développement cloud-native et bonnes pratiques
- **Gouvernance des conteneurs** : Politiques de sécurité et gestion des workloads Kubernetes
- **Patterns de conception** : Architecture patterns pour la résilience et l'évolutivité

Politiques de sécurité by design et Zero Trust :

- **Sécurité cloud-native** : Définition des règles de sécurité distribuée et Zero Trust
- **Standards de chiffrement** : Politiques de chiffrement end-to-end et gestion des clés
- **Security as Code** : Automatisation des contrôles de sécurité et validation continue
- **Politiques Zero Trust** : Implémentation des principes de confiance zéro

Standards SRE et observabilité :

- **SLI/SLO et Error Budgets** : Établissement des indicateurs de fiabilité et objectifs de service
- **Objectifs de fiabilité** : Définition des standards de disponibilité et performance
- **Métriques d'observabilité** : Standards de monitoring, logging, et tracing distribué
- **Pratiques SRE** : Intégration des pratiques Site Reliability Engineering

Politiques FinOps et gouvernance des coûts :

- **Optimisation des coûts cloud** : Définition des règles d'optimisation financière
- **Budgets automatisés** : Politiques de gestion automatique des budgets
- **Alerting financier** : Notifications et contrôles des dépassements
- **Gouvernance des ressources** : Optimisation et ajustement de taille automatisé

Politiques de gestion des données cloud-native :

- **Stockage cloud** : Définition des règles de stockage distribué et multi-cloud
- **Sauvegarde automatisée** : Politiques de backup et reprise après sinistre
- **Archivage intelligent** : Stratégies d'archivage basées sur l'IA et les politiques
- **Rétention basée sur les politiques** : Gestion automatique du cycle de vie

Standards DevOps et GitOps :

- **Processus CI/CD** : Établissement des pipelines de déploiement automatisé

- **Infrastructure as Code** : Standards Terraform, Ansible, et automatisation
- **Policy as Code** : Définition des politiques en mode code et versioning
- **Déploiement automatisé** : Workflows GitOps et validation continue

Gouvernance des conteneurs et Kubernetes :

- **Sécurité des pods** : Définition des politiques de sécurité Kubernetes
- **Gestion des ressources** : Standards de ressource quotas et limits
- **Networking** : Politiques de réseau et service mesh
- **Conformité Kubernetes** : Standards de déploiement et gouvernance

Politiques de conformité automatisée :

- **Conformité as code** : Définition des règles de conformité automatisées
- **Audit automatisé** : Processus d'audit continu et validation
- **Reporting de compliance** : Génération automatique de rapports
- **Gouvernance réglementaire** : Conformité RGPD, SOX, et standards sectoriels

Gouvernance multi-cloud et hybride :

- **Gestion multi-cloud** : Politiques de gestion cross-cloud et interopérabilité
- **Standards d'interopérabilité** : Définition des standards de portabilité
- **Gouvernance des architectures hybrides** : Politiques on-premise et cloud
- **Orchestration multi-environnements** : Coordination des déploiements

Processus de validation automatisée :

- **Workflows GitOps** : Mise en place de processus de validation automatique
- **Validation automatique** : Contrôles automatisés des changements
- **Approbation basée sur les politiques** : Workflows d'approbation intelligents
- **Gates de qualité** : Points de contrôle automatisés dans les pipelines

Gouvernance de l'observabilité et monitoring :

- **Politiques de monitoring** : Standards de surveillance et alerting
- **Alerting intelligent** : Définition des règles d'alerte basées sur l'IA
- **Logging centralisé** : Politiques de collecte et analyse des logs
- **Gouvernance des données d'observabilité** : Gestion des métriques et traces

Modèle d'exécution :

- **Approche DevOps collaborative** : Travail intégré avec équipes DevOps, SRE, sécurité
- **Méthodologie GitOps** : Définition des politiques en mode code avec versioning
- **Alignement cloud-native** : Cohérence avec stratégies cloud et transformation numérique
- **Évolutivité auto-adaptative** : Politiques capables d'évoluer automatiquement

PROFIL(S) PRESSENTI(S)

- Architecte Gouvernance Cloud-Native Senior (certification cloud, TOGAF)
- Expert Sécurité Cloud et Zero Trust (CISSP, CCSP)
- Spécialiste Policy as Code et GitOps
- Expert FinOps et Gouvernance des Coûts Cloud
- Expert SRE et Gouvernance de l'Observabilité

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Nombre de politiques	<20	20-50	>50
Environnements	1-2	3-5	>5
Services à gouverner	<50	50-200	>200
Équipes impactées	<10	10-50	>50
Intégrations	<10	10-30	>30
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	30 jours	40 jours	50 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Politiques d'architecture cloud-native et microservices	2 semaines	3 semaines	3 semaines
Politiques de sécurité by design et Zero Trust	3 semaines	4 semaines	4 semaines
Standards SRE, SLI/SLO et observabilité	2 semaines	3 semaines	3 semaines
Politiques FinOps et gouvernance des coûts cloud	2 semaines	3 semaines	4 semaines

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
Politiques de gestion des données cloud-native	3 semaines	4 semaines	4 semaines
Standards DevOps, GitOps et Policy as Code	3 semaines	4 semaines	5 semaines
Gouvernance des conteneurs et Kubernetes	3 semaines	4 semaines	4 semaines
Politiques de conformité automatisée et audit	4 semaines	5 semaines	5 semaines
Gouvernance multi-cloud et architectures hybrides	4 semaines	5 semaines	5 semaines
Processus de validation automatisée et GitOps	4 semaines	5 semaines	6 semaines
Gouvernance de l'observabilité et monitoring	2 semaines	3 semaines	4 semaines
Documentation as code et guides de gouvernance	Fin de prestation	Fin de prestation	Fin de prestation

VIII.5.2 UO 6.5.2 - MISE EN PLACE DES PROCESSUS DE VALIDATION ET CONFORMITÉ

OBJET

L'UO a pour objet de mettre en place les processus de validation et de conformité automatisés cloud-native pour une plateforme de données distribuée, permettant d'assurer le respect continu des politiques, standards techniques, et exigences réglementaires via des contrôles shift-left et DevSecOps. Cette prestation couvre l'établissement de workflows GitOps de validation, la mise en place de contrôles automatisés intégrés, l'implémentation de compliance as code, et la validation continue pour garantir la conformité, la sécurité, et la qualité de la plateforme. Cette UO intègre les pratiques modernes de validation, incluant DevSecOps, compliance as code, validation des conteneurs, shift-left security, et conformité continue pour garantir une validation efficace et automatisée des architectures cloud-native.

CONTENU ET MODALITÉS D'EXÉCUTION

Conception des workflows GitOps de validation :

- **Processus de validation automatisée** : Définition des workflows de validation des changements cloud-native
- **Déploiements cloud-native** : Validation automatique des déploiements et évolutions
- **Pipelines CI/CD** : Intégration de gates de qualité et contrôles automatisés
- **Validation continue** : Processus de validation en continu et feedback loops

Mise en place des contrôles automatisés cloud-native :

- **Outils de validation** : Implémentation SonarQube, Snyk, Trivy pour la qualité et sécurité
- **Scanning de sécurité** : Contrôles automatisés de vulnérabilités et conformité
- **Contrôles de conformité** : Intégration dans les pipelines de déploiement
- **Validation automatique** : Contrôles en temps réel et validation continue

Validation et sécurité des conteneurs :

- **Scanning d'images** : Implémentation de contrôles de sécurité des images Docker
- **Validation des configurations Kubernetes** : Contrôles des manifests et politiques
- **Contrôles de sécurité des pods** : Validation des workloads et configurations
- **Compliance des workloads** : Conformité des déploiements Kubernetes

Processus d'audit automatisé et reporting continu :

- **Audit as code** : Établissement d'audit automatisé et programmable
- **Génération automatique** : Rapports de conformité en temps réel
- **Tableaux de bord de compliance** : Visualisation continue de la conformité
- **Suivi en temps réel** : Monitoring des écarts et non-conformités

Compliance as code et Policy as Code :

- **Politiques de conformité automatisées** : Implémentation de règles programmables
- **Validation des configurations cloud** : Contrôles automatisés des ressources
- **Enforcement automatique** : Application automatique des règles de conformité
- **Versioning des politiques** : Gestion des versions et évolution des règles

Intégration DevSecOps et shift-left :

- **Outils de développement** : Configuration d'intégrations avec IDE et outils dev
- **Validation de sécurité précoce** : Contrôles de sécurité dès le développement
- **Contrôles de qualité intégrés** : Validation continue dans les workflows
- **Retour d'expérience utilisateur rapide** : Retours immédiats aux développeurs

Validation FinOps et gouvernance des coûts :

- **Contrôles automatisés des coûts** : Validation des budgets et optimisation
- **Validation des budgets** : Contrôles automatiques des dépassements

- **Alerting sur les dépassements** : Notifications automatiques et escalade
- **Optimisation continue** : Recommandations automatisées d'économies

Gestion automatisée des exceptions et remédiation :

- **Workflows automatisés** : Gestion programmable des exceptions et dérogations
- **Auto-remediation** : Correction automatique des non-conformités
- **Plans de correction automatiques** : Actions de remédiation programmées
- **Escalade intelligente** : Processus d'escalade basés sur la criticité

Validation multi-cloud et hybride :

- **Architectures multi-cloud** : Processus de validation cross-cloud
- **Conformité cross-platform** : Standards de validation inter-plateformes
- **Standards d'interopérabilité** : Validation de la portabilité et compatibilité
- **Gouvernance distribuée** : Coordination des validations multi-environnements

Formation DevSecOps et sensibilisation :

- **Pratiques de validation moderne** : Formation aux workflows automatisés
- **DevSecOps** : Sensibilisation aux pratiques de sécurité intégrée
- Sensibilisation à la conformité continue : Culture de la validation continue
- **Adoption des outils** : Formation aux outils de validation et contrôle

Monitoring intelligent et amélioration continue :

- **Monitoring des processus avec IA** : Surveillance intelligente des workflows
- **Métriques de qualité** : Indicateurs de performance des validations
- **Amélioration continue automatisée** : Optimisation basée sur les données
- **Apprentissage machine** : Amélioration des processus par l'IA

Modèle d'exécution :

- **Approche DevSecOps** : Mise en place progressive avec validation précoce
- **Automatisation complète** : Privilégier l'automatisation totale des contrôles
- **Intégration cloud-native** : Intégration native dans les workflows cloud
- **Amélioration continue intelligente** : Mécanismes d'apprentissage et adaptation

PROFIL(S) PRESENTI(S)

- Expert DevSecOps et Validation Automatisée (certification DevSecOps)
- Spécialiste Compliance as Code et Policy as Code
- Expert Validation Kubernetes et Sécurité des Conteneurs
- Ingénieur Automatisation et Pipelines CI/CD

- Spécialiste FinOps et Validation des Coûts

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Processus de validation	<10	10-30	>30
Contrôles automatisés	<50	50-200	>200
Environnements	1-2	3-5	>5
Intégrations	<10	10-50	>50
Équipes impactées	<10	10-50	>50
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	35 jours	45 jours	55 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Workflows GitOps de validation et gates de qualité	3 semaines	4 semaines	4 semaines
Contrôles automatisés cloud-native et scanning	4 semaines	5 semaines	5 semaines
Validation et sécurité des conteneurs Kubernetes	3 semaines	4 semaines	5 semaines
Processus d'audit automatisé et tableaux de bord compliance	3 semaines	4 semaines	4 semaines
Compliance as code et Policy as Code	4 semaines	5 semaines	6 semaines
Intégrations DevSecOps et shift-left security	5 semaines	6 semaines	6 semaines
Validation FinOps et contrôles	4 semaines	5 semaines	5 semaines

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
des coûts			
Gestion automatisée des exceptions et auto-remediation	5 semaines	6 semaines	6 semaines
Validation multi-cloud et conformité hybride	4 semaines	5 semaines	6 semaines
Formation DevSecOps et sensibilisation moderne	5 semaines	6 semaines	7 semaines
Monitoring intelligent et amélioration continue	6 semaines	7 semaines	7 semaines
Documentation as code et runbooks de validation	Fin de prestation	Fin de prestation	Fin de prestation

VIII.5.3 UO 6.5.3 - GESTION DU CATALOGUE DE SERVICES TECHNIQUES

OBJET

L'UO a pour objet de mettre en place et gérer un catalogue de services techniques cloud-native intelligent pour une plateforme de données distribuée, permettant la découverte automatique, la documentation dynamique, et la gouvernance complète des services, APIs, et microservices. Cette prestation couvre la création d'un service registry moderne, la définition de standards de documentation as code, l'implémentation de découverte automatique, et la mise en place de processus de gestion du cycle de vie automatisés pour faciliter l'observabilité, l'utilisation, et la gouvernance des architectures distribuées. Cette UO intègre les pratiques modernes de catalogage, incluant service mesh, découverte automatique, API management cloud-native, observabilité des services, et catalogage multi-cloud pour garantir une gestion efficace et évolutive des services distribués.

CONTENU ET MODALITÉS D'EXÉCUTION

Conception du service registry cloud-native :

- **Architecture de catalogage distribuée** : Définition d'une architecture de service registry moderne
- **Métadonnées enrichies** : Structure de données complète pour les services
- **Classification automatique** : Taxonomie intelligente et catégorisation automatisée

- **Intégration avec les service mesh** : Connexion native avec Istio, Linkerd, Consul

Découverte automatique et inventaire intelligent :

- **Découverte automatique** : Implémentation de découverte des services Kubernetes, Consul, Istio
- **Catalogage automatisé** : Référencement automatique des nouveaux services
- **Synchronisation en temps réel** : Mise à jour continue du catalogue
- **Détection des changements** : Monitoring des évolutions et modifications

Catalogage des microservices et APIs :

- **Référencement automatique** : Catalogage automatisé des microservices déployés
- **Documentation des APIs** : Intégration OpenAPI/Swagger et génération automatique
- **Mapping des dépendances** : Cartographie automatique des relations inter-services
- **Versioning des APIs** : Gestion des versions et compatibilité

Documentation as code et standards automatisés :

- **Génération automatique** : Documentation générée depuis le code et les déploiements
- **Templates versionnés** : Standards de documentation avec versioning Git
- **Documentation intégrée** : Intégration dans les pipelines CI/CD
- **Mise à jour automatique** : Synchronisation avec les changements de code

Définition des SLI/SLO et observabilité :

- **Service Level Indicators** : Établissement d'indicateurs de performance automatisés
- **SLO automatisés** : Objectifs de service avec monitoring continu
- **Métriques d'observabilité** : Intégration avec les systèmes de monitoring
- **Monitoring de la santé** : Surveillance continue de l'état des services

Gestion du service mesh et networking :

- **Configurations Istio/Linkerd** : Catalogage des politiques de service mesh
- **Politiques de trafic** : Documentation des règles de routage et load balancing
- **Gouvernance du réseau** : Gestion des politiques de sécurité réseau
- **Observabilité du mesh** : Monitoring des communications inter-services

Processus de gestion du cycle de vie automatisé :

- **Workflows GitOps** : Gestion automatisée via pipelines de déploiement
- **Déploiement automatisé** : Intégration avec les processus de déploiement
- **Versioning intelligent** : Gestion automatique des versions et compatibilité
- **Dépréciation contrôlée** : Processus automatisé de fin de vie des services

Catalogage multi-cloud et hybride :

- **Services cross-cloud** : Référencement des services distribués multi-cloud
- **Mapping des architectures hybrides** : Cartographie des déploiements hybrides
- **Gouvernance multi-environnements** : Standards cross-platform et interopérabilité
- **Fédération des catalogues** : Agrégation des catalogues distribués

Interface intelligente et recherche avancée :

- **Portail avec recherche sémantique** : Interface utilisateur avec recherche intelligente
- **Recommandations IA** : Suggestions automatiques basées sur l'usage
- **Visualisation des topologies** : Cartographie interactive des architectures
- **Analytics d'usage** : Métriques d'utilisation et adoption des services

Intégration DevOps et observabilité :

- **Outils cloud-native** : Configuration d'intégrations avec l'écosystème cloud
- **Pipelines CI/CD** : Intégration avec les workflows de déploiement
- **Monitoring automatisé** : Connexion avec les systèmes d'observabilité
- **Alerting automatisé** : Notifications sur les changements et problèmes

Gouvernance des APIs et sécurité :

- **Politiques de sécurité** : Catalogage des règles de sécurité des APIs
- **Gestion des accès** : Documentation des politiques d'authentification
- **Rate limiting** : Gestion des quotas et limitations d'usage
- **Conformité des APIs** : Validation des standards et bonnes pratiques

Modèle d'exécution :

- **Approche cloud-native** : Travail intégré avec équipes DevOps, SRE, développement
- **Méthodologie GitOps** : Construction automatique via découverte et synchronisation
- **Automatisation complète** : Privilégier l'automatisation totale
- **Adoption cloud-native** : Déploiement par microservices avec intégration native

PROFIL(S) PRESSENTI(S)

- Architecte Services Cloud-Native et API Management (certification cloud)
- Expert Service Mesh et Découverte Automatique (Istio, Consul)
- Consultant Documentation as Code et Automatisation
- Expert Gouvernance des Services et Observabilité
- Expert DevOps et Intégration CI/CD

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Services à cataloguer	<50	50-200	>200
APIs et microservices	<20	20-100	>100
Environnements	1-2	3-5	>5
Intégrations	<10	10-30	>30
Utilisateurs	<100	100-1K	>1K
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	30 jours	40 jours	50 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Architecture service registry cloud-native et métadonnées	2 semaines	3 semaines	3 semaines
Découverte automatique et inventaire intelligent	3 semaines	4 semaines	4 semaines
Catalogage microservices, APIs et dépendances	2 semaines	3 semaines	4 semaines
Documentation as code et templates automatisés	2 semaines	3 semaines	3 semaines
SLI/SLO et métriques d'observabilité des services	3 semaines	4 semaines	4 semaines
Catalogage service mesh et politiques networking	3 semaines	4 semaines	5 semaines
Processus GitOps de gestion du cycle de vie	4 semaines	5 semaines	5 semaines
Catalogage multi-cloud et	3 semaines	4 semaines	4 semaines

architectures hybrides			
Interface intelligente et recherche sémantique	4 semaines	5 semaines	6 semaines
Intégrations DevOps et observabilité automatisée	4 semaines	5 semaines	5 semaines
Gouvernance APIs et sécurité des services	2 semaines	3 semaines	4 semaines
Documentation cloud-native et formation	Fin de prestation	Fin de prestation	Fin de prestation

VIII.5.4 UO 6.5.4 - ACCOMPAGNEMENT À L'ADOPTION DES STANDARDS TECHNIQUES

OBJET

L'UO a pour objet d'accompagner les équipes dans l'adoption des standards techniques cloud-native et des pratiques modernes pour la plateforme de données distribuée, en facilitant la transformation culturelle vers DevOps/SRE, en formant aux technologies cloud-native, et en assurant le suivi de la mise en œuvre avec des méthodes agiles. Cette prestation couvre l'élaboration de plans d'accompagnement adaptatifs, la formation immersive aux pratiques modernes, et la mise en place de mécanismes de support continu pour garantir une adoption réussie et durable des standards cloud-native, DevOps, et SRE. Cette UO intègre les méthodologies modernes d'accompagnement, incluant transformation agile, formation avec mise en pratique, coaching DevOps, mentoring SRE, et adoption progressive des pratiques cloud-native pour garantir une transformation efficace et durable.

CONTENU ET MODALITÉS D'EXÉCUTION

Élaboration du plan d'accompagnement agile :

- **Stratégie d'adoption progressive** : Définition d'une feuille de route cloud-native avec méthodologie agile
- **Sprints d'adoption** : Planification par itérations avec objectifs mesurables
- **Mécanismes de retours d'expérience continus** : Mécanismes de retour et ajustement permanent
- **Jalons de transformation** : Points de contrôle et validation des acquis

Analyse des impacts et transformation culturelle :

- **Impacts DevOps/SRE** : Évaluation des changements organisationnels et techniques
- **Résistances aux changements** : Identification des freins à l'adoption cloud-native

- **Actions de transformation culturelle** : Stratégies de conduite du changement
- **Accompagnement au mindset** : Evolution vers les cultures DevOps et SRE

Formation immersive aux pratiques cloud-native :

- **Formations avec mise en pratique** : Sessions pratiques sur environnements réels
- **DevOps et SRE** : Formation aux pratiques de développement et fiabilité
- **Kubernetes** : Formation approfondie aux conteneurs et orchestration
- **Infrastructure as Code** : Apprentissage Terraform, Ansible, et automatisation

Coaching DevOps et mentoring SRE :

- **Accompagnement personnalisé** : Coaching individuel aux pratiques DevOps
- **Coaching SRE** : Mentoring sur l'observabilité et la fiabilité
- **Mentoring sur l'observabilité** : Accompagnement aux pratiques de monitoring
- **Pratiques de fiabilité** : Formation aux Error Budgets et SLI/SLO

Création de supports pédagogiques interactifs :

- **Labs pratiques** : Développement d'environnements de formation avec mise en pratique
- **Tutoriels interactifs** : Guides pratiques et exercices dirigés
- **Documentation as code** : Documentation versionnée et collaborative
- **Environnements de formation cloud** : Plateformes d'apprentissage dédiées

Formation aux outils cloud-native :

- **Sessions spécialisées Kubernetes** : Formation approfondie à l'orchestration
- **Terraform et Infrastructure as Code** : Automatisation et provisioning
- **GitOps et déploiement** : Workflows de déploiement automatisé
- **Outils de monitoring et sécurité** : Formation aux outils d'observabilité et sécurité

Mise en place d'un support technique expert :

- **Centre d'excellence cloud-native** : Établissement d'un CoE pour l'accompagnement
- **Support DevOps** : Assistance technique aux pratiques de développement
- **Assistance SRE** : Support pour l'application des standards de fiabilité
- **Helpdesk spécialisé** : Support technique dédié aux technologies cloud

Accompagnement à l'automatisation :

- **Pratiques d'automatisation** : Formation aux workflows automatisés
- **CI/CD et pipelines** : Implémentation de chaînes de déploiement
- **Infrastructure as Code** : Automatisation du provisioning et configuration
- **Policy as Code** : Automatisation de la gouvernance et conformité

Pilotage agile de l'adoption :

- **Métriques DevOps (DORA)** : Suivi avec indicateurs de performance DevOps
- **Indicateurs SRE** : Monitoring des SLI/SLO et Error Budgets
- **Tableaux de bord d'adoption** : Visualisation des progrès et adoption
- **Amélioration continue** : Optimisation basée sur les métriques et les retours d'expérience utilisateur

Transformation de la culture technique :

- **Sensibilisation aux pratiques modernes** : Actions de promotion des standards cloud-native
- **Promotion de la culture DevOps** : Évangélisation des pratiques collaboratives
- **Adoption des mindsets cloud-native** : Transformation vers les mentalités modernes
- **Communautés de pratiques** : Création de groupes d'échange et partage

Communication et évangélisation :

- **Actions de communication** : Mise en place d'actions sur les bénéfices cloud-native
- **Communautés de pratiques** : Animation de groupes d'échange et retours d'expérience
- **Partage d'expériences** : Organisation de sessions de partage et capitalisation
- **Évangélisation interne** : Promotion des succès et bonnes pratiques

Capitalisation et amélioration continue :

- **Collecte de retours d'expérience** : Mécanismes de retours d'expérience utilisateur et apprentissage
- **Amélioration des standards** : Évolution basée sur les retours terrain
- **Évolution des pratiques** : Adaptation selon les apprentissages et innovations
- **Optimisation continue** : Amélioration permanente des méthodes d'accompagnement

Modèle d'exécution :

- **Approche agile et adaptative** : Déploiement par sprints avec adaptation continue
- **Accompagnement personnalisé** : Adaptation selon les profils techniques et besoins
- **Méthodes pédagogiques modernes** : Formation immersive, labs pratiques, apprentissage par la pratique
- **Amélioration continue** : Ajustement basé sur les métriques et les retours d'expérience utilisateur

PROFIL(S) PRESSENTI(S)

- Consultant Transformation Cloud-Native et DevOps (certification cloud, DevOps)
- Formateur Expert Cloud-Native et SRE (CKA, SRE)
- Coach DevOps et Mentor SRE
- Formateur Sécurité Cloud et DevSecOps

- Expert Accompagnement Automatisation et GitOps

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Équipes à accompagner	<10	10-50	>50
Technologies à adopter	<5	5-15	>15
Environnements	1-2	3-5	>5
Changements culturels	Mineurs	Modérés	Majeurs
Résistances attendues	Faibles	Moyennes	Élevées
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	40 jours	50 jours	60 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Plan d'accompagnement agile et stratégie cloud-native	2 semaines	3 semaines	3 semaines
Analyse impacts transformation et plan changement culturel	3 semaines	4 semaines	4 semaines
Programme formation cloud-native et sessions de mise en pratique	5 semaines	6 semaines	6 semaines
Coaching DevOps et mentoring SRE personnalisés	5 semaines	6 semaines	7 semaines
Labs pratiques et documentation interactive	4 semaines	5 semaines	5 semaines
Formation spécialisée outils cloud-native	4 semaines	5 semaines	6 semaines
Centre d'excellence cloud-native	3 semaines	4 semaines	5 semaines

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
opérationnel			
Accompagnement automatisation et CI/CD	5 semaines	6 semaines	6 semaines
Tableaux de bord adoption avec métriques DORA/SRE	4 semaines	5 semaines	5 semaines
Actions transformation culture technique	6 semaines	7 semaines	7 semaines
Communication et communautés de pratiques	6 semaines	7 semaines	8 semaines
Rapport capitalisation et plan d'évolution	Fin de prestation	Fin de prestation	Fin de prestation

VIII.6 PRESTATION L6-6 : EXPLOITATION ET SUPPORT DE PLATEFORME

Cette prestation est dédiée à l'exploitation courante et au Maintien en Condition Opérationnelle (MCO) des environnements et systèmes de données. Son objectif est de garantir la disponibilité, la performance et la stabilité des infrastructures et applications data.

Elle couvre les opérations quotidiennes d'exploitation (installation, supervision), le traitement rapide et efficace des incidents, la réalisation d'évolutions mineures pour maintenir les systèmes à jour et optimisés, ainsi que l'accompagnement aux migrations d'environnements (cloud, on-premise, hybride). Enfin, elle intègre la gestion des carnets de tickets et les astreintes, assurant une réactivité constante face aux imprévus et aux besoins opérationnels

VIII.6.1 UO 6.6.1 - EXPLOITATION COURANTE DE LA PLATEFORME

OBJET

L'UO a pour objet d'assurer l'exploitation courante cloud-native d'une plateforme de données distribuée, garantissant son fonctionnement autonome, la haute disponibilité des services, et les performances optimales via l'automatisation, l'auto-healing, et les pratiques SRE. Cette prestation couvre l'observabilité moderne, la maintenance automatisée, la gestion intelligente des incidents, l'auto-scaling, et l'optimisation continue pour assurer un niveau de service élevé et une fiabilité exceptionnelle dans un environnement cloud complexe. Cette UO intègre les pratiques modernes d'exploitation, incluant SRE, auto-healing, observabilité cloud-native, FinOps, et exploitation automatisée pour garantir une gestion efficace et évolutive des architectures distribuées. L'installation doit être automatisée et utilise la chaîne CI/CD du bénéficiaire pour exécuter les traitements. La supervision s'effectue en heures ouvrées de 8H00 à 18H00.

CONTENU ET MODALITÉS D'EXÉCUTION

Observabilité et monitoring cloud-native :

- **Supervision en temps réel** : Monitoring avec les trois piliers (metrics, logs, traces)
- **SLI/SLO et Error Budgets** : Établissement d'indicateurs de fiabilité et objectifs de service
- **Alerting intelligent** : Notifications prédictives et escalade automatique
- **Tableaux de bord adaptatifs** : Visualisation intelligente et analytics en temps réel

Maintenance automatisée et auto-healing :

- **Planification automatique** : Maintenance prédictive basée sur l'IA
- **Auto-remediation** : Correction automatique des problèmes courants
- **Maintenance prédictive** : Prévention des pannes par analyse des patterns
- **Healing automatique** : Restauration automatique des services défaillants

Gestion intelligente des incidents SRE :

- **Traitement automatisé** : Diagnostic IA et résolution automatique
- **Escalade intelligente** : Routage automatique selon la criticité
- **Post-mortem automatisés** : Analyse sans blame et amélioration continue
- **Gestion des crises** : Coordination automatisée des équipes

Auto-scaling et optimisation des ressources :

- **Scaling automatique** : Horizontal et vertical selon la demande
- **Optimisation Kubernetes** : Gestion intelligente des workloads
- **Gestion de la capacité** : Prédiction et provisioning automatique
- **Ajustement de taille** : Optimisation continue des ressources

Optimisation continue des performances :

- **Analyse automatisée** : Identification IA des goulots d'étranglement

- **Optimisation prédictive** : Amélioration basée sur les patterns d'usage
- **Tuning automatique** : Ajustement continu des paramètres
- **Benchmarking** : Comparaison et validation des performances

Exploitation Kubernetes et conteneurs :

- **Administration automatisée** : Gestion des clusters et workloads
- **Networking** : Configuration et optimisation des réseaux
- **Sécurité des conteneurs** : Monitoring et protection en temps réel
- **Lifecycle management** : Gestion automatique du cycle de vie

Gestion automatisée des sauvegardes cloud :

- **Sauvegardes cross-region** : Protection distribuée et automatisée
- **Tests de restauration** : Validation automatique de l'intégrité
- **Reprise après sinistre** : Orchestration automatique de la reprise
- **Archivage intelligent** : Gestion automatique du cycle de vie

FinOps et optimisation des coûts :

- **Monitoring des coûts** : Surveillance en temps réel des dépenses
- **Optimisation automatique** : Recommandations et actions automatisées
- **Alerting budgétaire** : Notifications et contrôles des dépassements
- **Recommandations IA** : Suggestions d'économies basées sur l'usage

Administration cloud-native des données :

- **Maintenance automatisée** : Gestion des bases de données cloud
- **Optimisation des requêtes** : Amélioration automatique des performances
- **Gestion intelligente** : Stockage adaptatif et optimisation
- **Monitoring des données** : Surveillance de la qualité et intégrité

Déploiement automatisé et GitOps :

- **Déploiement continu** : Workflows GitOps et automatisation
- **Rollback automatique** : Retour en arrière intelligent en cas d'erreur
- **Gestion des versions** : Infrastructure as Code et versioning
- **Validation continue** : Tests automatisés et gates de qualité

Chaos engineering et tests de résilience :

- **Tests automatisés** : Validation continue de la robustesse
- **Chaos engineering** : Injection contrôlée de pannes
- **Validation de résilience** : Tests de résistance et récupération
- **Amélioration continue** : Renforcement basé sur les résultats

Reporting intelligent et analytics :

- **Tableaux de bord adaptatifs** : Visualisation intelligente et personnalisée
- **Reporting automatisé** : Génération automatique de rapports
- **Analytics prédictifs** : Insights IA sur les tendances
- **Métriques DORA** : Indicateurs de performance DevOps

Modèle d'exécution :

- **Surveillance 24/7** : Monitoring automatisé avec IA et intervention humaine si nécessaire
- **Approche SRE et proactive** : Maintenance prédictive et prévention par l'IA
- **Processus automatisés** : Infrastructure as Code et workflows GitOps
- **Amélioration continue** : Optimisation basée sur les métriques et les retours

PROFIL(S) PRESSENTI(S)

- Expert SRE et Exploitation Cloud-Native (certification SRE, CKA)
- Spécialiste Kubernetes et Administration Conteneurs
- Spécialiste FinOps et Optimisation des Coûts Cloud
- Ingénieur Automatisation et Infrastructure as Code
- Expert Observabilité et Monitoring Cloud-Native

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Services à exploiter	<50	50-200	>200
Environnements	1-2	3-5	>5
Utilisateurs	<1K	1K-10K	>10K
Intégrations	<10	10-50	>50
Données (TB)	<10	10-100	>100
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	Setup 20 jours puis continu	Setup 30 jours puis continu	Setup 45 jours puis continu

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Runbooks SRE et procédures automatisées	2 semaines	3 semaines	3 semaines
Observabilité cloud-native opérationnelle	1 semaine	2 semaines	2 semaines
Auto-healing et maintenance prédictive	3 semaines	4 semaines	4 semaines
Gestion intelligente des incidents SRE	1 semaine	2 semaines	2 semaines
Auto-scaling et optimisation des ressources	2 semaines	3 semaines	3 semaines
Exploitation Kubernetes automatisée	2 semaines	3 semaines	3 semaines
Sauvegardes cloud et reprise après sinistre	3 semaines	4 semaines	4 semaines
FinOps et monitoring des coûts	1 semaine	2 semaines	3 semaines
Administration cloud-native des données	3 semaines	4 semaines	4 semaines
GitOps et déploiement automatisé	2 semaines	3 semaines	4 semaines
Chaos engineering et tests de résilience	4 semaines	5 semaines	5 semaines
Tableaux de bord intelligents et analytics	4 semaines	5 semaines	5 semaines
Rapports SRE et métriques DORA	Mensuellement	Mensuellement	Mensuellement
Documentation as code et knowledge base	En continu	En continu	En continu

VIII.6.2 UO 6.6.2 - MAINTENANCE CORRECTIVE ET ÉVOLUTIVE

OBJET

L'UO a pour objet la correction complète des incidents de fonctionnement affectant tout développement opéré au titre d'un projet du présent marché.

La correction s'entend du rétablissement intégral de l'usage normal du développement.

CONTENU ET MODALITÉS D'EXÉCUTION

PÉRIODE DE MAINTENANCE

La période de maintenance qui définit la couverture temporelle du service de maintenance que le titulaire doit assurer aux conditions du marché couvre les jours ouvrés du bénéficiaire et court du lundi au vendredi, de 8h00 à 18h00.

MODALITÉS DE DÉCLENCHEMENT ET D'EXÉCUTION

Le signalement est opéré par un représentant de l'administration au moyen d'un message électronique adressé au titulaire. La détermination du niveau de criticité appartient exclusivement à l'administration. Toutefois, avec l'accord du bénéficiaire, le niveau de criticité peut être révisé à tout moment. De la même façon, l'administration peut, s'il le souhaite, allonger les délais de résolution fixés. La révision du niveau de criticité et l'allongement des délais sont portés à la connaissance du titulaire par tout moyen permettant de donner date et heure certaines.

Les signalements peuvent être opérés 24h/24 mais les délais ne courent qu'à l'intérieur de la période de maintenance ainsi qu'il est dit ci-après à l'article III.5.1.4.

Le suivi des opérations de maintenance est transcrit dans un journal horodaté qui :

- revêt impérativement la forme d'un fichier électronique compatible avec la norme ISO 26300 - 2006 (Open Document) ;
- contient au minimum les éléments suivants :
 - numéro de dossier ;
 - développement concerné ;
 - date et heure de signalement ;
 - date et heure de remise en état ;
 - description de l'incident ;
 - solution apportée.

L'administration a la faculté de dispenser le titulaire de la tenue du journal horodaté. La dispense revêt la forme d'un avis écrit et exprès adressé au titulaire par tout moyen permettant de donner date et heure certaines. En l'absence de cet avis, le titulaire tient à jour le journal horodaté qui est remis à l'administration à la demande de ce dernier.

MODALITÉS DE COMMANDE

L'UO 6.6.2 s'exécute sur la base de tickets utilisables unitairement par incident.

Ainsi qu'il est indiqué au CCAP, l'administration qui entend recourir à l'UO 6.6.2 doit avoir, préalablement à toute demande d'intervention adressée au titulaire, notifié une commande de carnet de tickets audit titulaire. Le choix du type de carnet commandé (carnet de 5 tickets ; carnet de 10 tickets ; carnet de 15 tickets) est laissé à la libre appréciation de l'administration.

Les travaux effectués au titre de l'UO se voient appliquer la garantie contractuelle prévue au marché.

PROFIL(S) PRESSENTI(S)

- **Ingénieur Support L2/L3** (principal)
- **Ingénieur SRE (Site Reliability Engineer)**
- **Expert Sécurité** (pour incidents sécurité)
- **Architecte Data** (pour incidents complexes)

TYPOLOGIE DES INCIDENTS ET DÉLAIS DE RÉOLUTION

NIVEAU DE CRITICITÉ	DÉFINITION	DÉLAI DE CORRECTION	SLO CIBLE
CRITIQUE	Incident de sécurité majeur, perte de données, indisponibilité totale du service	2 heures ouvrées	99.9%
BLOQUANT	Incident rendant impossible l'utilisation normale d'un développement de façon rédhibitoire et non contournable	4 heures ouvrées	99.5%

MAJEUR	Incident entravant l'utilisation sans l'interdire, contournement possible	1 jour ouvré	99%
MINEUR	Incident n'impactant pas significativement l'usage	3 jours ouvrés	95%

PRÉCISIONS SUR LES DÉLAIS

Les délais se décomptent à l'intérieur de la période de maintenance précisée ci-avant à l'article VIII.6.6.2.

- Pour les délais exprimés en heures, ils se décomptent d'heure à heure.

Exemples :

- Un incident bloquant est signalé le 15 avril 2019 à 5h00. La correction doit intervenir au plus tard le 15 avril 2019 à 12h00 (le délai de 4 heures ouvrées se décompte à partir de l'heure d'ouverture de la période de maintenance).
- Un incident bloquant est signalé le 19 avril 2019 à 17h00. La correction doit intervenir au plus tard le 23 avril 2019 à 11h00 (les 20, 21 et 22 avril 2019 ne sont pas des jours ouvrés).

- Pour les délais exprimés en jours, par dérogation à l'article 3.2 du CCAG-TIC, le délai se décompte de jour à jour et d'heure à heure.

Exemples :

- Un incident majeur est signalé le 15 avril 2019 à 5h00. La correction doit intervenir au plus tard le 17 avril 2019 à 8h00 (le délai de 2 jours ouvrés se décompte à partir du 15 avril 2019 – 8 heures [heure d'ouverture de la période de maintenance] et s'achève 2 jours plus tard le 17 avril 2019 à 8 heures).
- Un incident mineur est signalé le 7 mai 2019 à 12h00. La correction doit intervenir au plus tard le 15 mai 2019 à 12h00 (les 8, 11 et 12 mai 2019 ne sont pas des jours ouvrés).

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livraison	Délai maximal de remise à partir du signalement			
	CRITIQUE	BLOQUANT	MAJEUR	MINEUR
Correctif opérationnel sur l'environnement concerné	2 heures	4 heures	1 jour	3 jours
Rapport d'intervention détaillé	4 heures	6 heures	2 jours	5 jours

Journal horodaté des interventions (NOTA : l'administration a la faculté de dispenser le titulaire de la tenue de ce livrable)	Sur demande du bénéficiaire
---	-----------------------------

MODALITÉS DE COMMANDE

L'UO 6.6.2 s'exécute sur la base de tickets utilisables unitairement par incident.

Ainsi qu'il est indiqué au CCAP, l'administration qui entend recourir à l'UO 6.6.2 doit avoir, préalablement à toute demande d'intervention adressée au titulaire, notifié une commande de carnet de tickets audit titulaire. Le choix du type de carnet commandé (carnet de 5 tickets ; carnet de 10 tickets ; carnet de 15 tickets) est laissé à la libre appréciation de l'administration.

VIII.6.3 UO 6.6.3 - SUPPORT UTILISATEURS ET FORMATION

OBJET

L'UO a pour objet d'assurer le support intelligent aux utilisateurs et la formation cloud-native sur l'utilisation d'une plateforme de données distribuée, garantissant une adoption réussie des pratiques modernes, une utilisation optimale des outils cloud-native, et une montée en compétences DevOps/SRE des équipes. Cette prestation couvre l'assistance technique automatisée, la résolution intelligente des problèmes, la formation immersive aux outils et processus cloud-native, et l'accompagnement dans la transformation vers les pratiques modernes. Cette UO intègre les pratiques modernes de support, incluant support automatisé avec IA, formation de mise en pratique cloud-native, accompagnement DevOps/SRE, et support multi-canal intelligent pour garantir une adoption efficace des technologies et pratiques modernes.

CONTENU ET MODALITÉS D'EXÉCUTION

Support technique intelligent et automatisé :

- **Assistance avec chatbots IA** : Support automatisé de premier niveau
- **Résolution automatique** : Traitement automatique des problèmes courants
- **Support outils cloud-native** : Assistance spécialisée sur les technologies modernes
- **Escalade intelligente** : Routage automatique vers les experts appropriés

Formation immersive cloud-native :

- **Sessions de mise en pratique** : Formation pratique sur environnements réels
- **Kubernetes et DevOps** : Formation approfondie aux technologies modernes

- **SRE et observabilité** : Apprentissage des pratiques de fiabilité
- **Infrastructure as Code** : Formation aux outils d'automatisation

Formation DevOps et SRE spécialisée :

- **Pratiques DevOps** : Formation aux méthodologies de développement
- **SRE et observabilité** : Apprentissage de la gestion de la fiabilité
- **Transformation culturelle** : Accompagnement au changement de mindset
- **Coaching personnalisé** : Mentoring individuel sur les pratiques

Documentation interactive et knowledge base :

- **Guides interactifs** : Documentation dynamique et searchable
- **Tutoriels vidéo** : Contenus multimédias et démonstrations
- **Documentation as code** : Documentation versionnée et collaborative
- **Base de connaissances IA** : Repository intelligent avec recherche sémantique

Accompagnement à l'adoption cloud-native :

- **Transformation DevOps** : Assistance dans l'évolution des pratiques
- **Coaching SRE** : Mentoring sur les pratiques de fiabilité
- **Mentoring outils cloud** : Accompagnement sur les technologies modernes
- **Accompagnement culturel** : Support dans la transformation des équipes

Gestion intelligente des demandes :

- **Traitement automatisé avec IA** : Classification et routage automatique
- **Priorisation intelligente** : Tri automatique selon la criticité
- **Routing automatique** : Affectation automatique aux experts
- **Suivi en temps réel** : Monitoring et analytics des demandes

Support spécialisé Kubernetes et conteneurs :

- **Administration Kubernetes** : Assistance sur la gestion des clusters
- **Résolution de problèmes conteneurs** : Support sur les problèmes de workloads
- **Support workloads** : Assistance sur les applications cloud-native
- **Optimisation** : Conseils sur les performances et ressources

Amélioration continue de l'expérience :

- **Collecte automatisée** : Retours d'expérience utilisateur automatisés automatique et analytics
- **Analyse IA des besoins** : Identification intelligente des améliorations
- **Recommandations intelligentes** : Suggestions automatiques d'optimisation
- **Optimisation continue** : Amélioration permanente de l'expérience

Formation aux outils cloud-native :

- **Sessions spécialisées** : Formation approfondie aux technologies
- **Terraform et GitOps** : Apprentissage de l'Infrastructure as Code
- **Monitoring et sécurité** : Formation aux outils d'observabilité
- **Outils de développement** : Formation aux plateformes modernes

Formation des champions internes :

- **Référents DevOps/SRE** : Formation de leaders techniques
- **Centres d'excellence** : Création de communautés d'expertise
- **Communautés de pratiques** : Animation de groupes d'échange
- **Certification interne** : Programmes de validation des compétences

Support FinOps et optimisation :

- **Optimisation des coûts** : Assistance sur la gestion financière
- **Pratiques FinOps** : Formation aux méthodologies d'optimisation
- **Outils de gestion budgétaire** : Support sur les plateformes financières
- **Monitoring des coûts** : Assistance sur le suivi des dépenses

Évaluation et analytics avancés :

- **Métriques DORA** : Mesure de l'adoption des pratiques DevOps
- **Analytics de satisfaction** : Mesure de l'expérience utilisateur
- **Insights IA** : Analyse intelligente de l'utilisation
- **Reporting automatisé** : Génération automatique de rapports

Modèle d'exécution :

- **Support omni-canal** : Assistance via chatbots IA, vidéo, et experts humains
- **Formation adaptative** : Parcours personnalisés et certification progressive
- **Approche DevOps** : Support intégré dans les workflows modernes
- **Amélioration continue** : Évolution basée sur les analytics et les retours d'expérience utilisateur

PROFIL(S) PRESSENTI(S)

- Expert Support Cloud-Native et DevOps (certification cloud, DevOps)
- Formateur Spécialisé Cloud-Native et SRE (CKA, SRE)
- Expert Support Automatisé et IA
- Consultant Accompagnement Transformation Cloud
- Formateur FinOps et Optimisation des Coûts

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Utilisateurs à supporter	<100	100-1K	>1K
Demandes par mois	<500	500-5K	>5K
Technologies à former	<5	5-15	>15
Équipes à accompagner	<10	10-50	>50
Langues de support	1	2-3	>3
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	Setup 10 jours puis continu	Setup 20 jours puis continu	Setup 30 jours puis continu

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Support intelligent et automatisé opérationnel	1 semaine	2 semaines	2 semaines
Programme de formation cloud-native développé	2 semaines	3 semaines	3 semaines
Formation DevOps et SRE spécialisée	3 semaines	4 semaines	4 semaines
Documentation interactive et knowledge base	2 semaines	3 semaines	3 semaines
Accompagnement transformation cloud-native	2 semaines	3 semaines	3 semaines
Gestion intelligente des demandes avec IA	1 semaine	2 semaines	2 semaines
Support spécialisé Kubernetes et conteneurs	3 semaines	4 semaines	4 semaines

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
Formation outils cloud-native et DevOps	2 semaines	3 semaines	4 semaines
Formation des champions et centres d'excellence	4 semaines	5 semaines	5 semaines
Support FinOps et optimisation des coûts	2 semaines	3 semaines	3 semaines
Sessions de formation de mise en pratique organisées	3 semaines	4 semaines	4 semaines
Analytics avancés et métriques d'adoption	3 semaines	4 semaines	4 semaines
Rapports intelligents et insights IA	Mensuellement	Mensuellement	Mensuellement
Évaluation continue et recommandations	En continu	En continu	En continu

VIII.6.4 UO 6.6.4 - TRANSFERT DE COMPÉTENCES ET AUTONOMIE

OBJET

L'UO a pour objet d'assurer le transfert complet de compétences cloud-native et l'autonomisation des équipes internes pour la gestion d'une plateforme de données distribuée, garantissant la continuité opérationnelle SRE et la capacité d'évolution autonome sur les technologies modernes. Cette prestation couvre la formation immersive aux pratiques cloud-native, le transfert des connaissances DevOps/SRE, l'accompagnement vers l'autonomie technique et culturelle, et la mise en place des conditions pour une gestion interne experte et évolutive. Cette UO intègre les pratiques modernes de transfert, incluant formation avec mise en pratique cloud-native, coaching DevOps/SRE, autonomisation sur Kubernetes, transfert FinOps, et développement de centres d'excellence pour garantir une autonomie complète et durable. Elle nécessite des déplacements.

CONTENU ET MODALITÉS D'EXÉCUTION

Formation technique cloud-native immersive :

- **Architecture cloud-native** : Formation approfondie sur les architectures distribuées
- **Kubernetes et microservices** : Maîtrise de l'orchestration et des patterns

- **Infrastructure as Code** : Apprentissage de l'automatisation complète
- **Technologies distribuées** : Formation sur les systèmes complexes avec labs pratiques

Transfert des compétences DevOps/SRE :

- **Savoir-faire DevOps** : Transmission des pratiques de développement
- **Pratiques SRE** : Formation à la gestion de la fiabilité
- **Observabilité et auto-healing** : Maîtrise du monitoring et de l'auto-remediation
- **Gestion des incidents** : Formation aux processus de résolution avec coaching

Autonomisation Kubernetes et conteneurs :

- **Administration Kubernetes** : Formation experte sur la gestion des clusters
- **Orchestration avancée** : Maîtrise des workloads et du networking
- **Sécurité des conteneurs** : Formation à la protection des applications
- **Résolution de problèmes avancé** : Diagnostic et résolution des problèmes complexes

Accompagnement transformation culturelle :

- **Coaching vers l'autonomie DevOps** : Développement des pratiques collaboratives
- **Mentoring SRE** : Accompagnement vers la culture de fiabilité
- **Culture cloud-native** : Transformation des mindsets et pratiques
- **Transformation des mindsets** : Évolution vers les mentalités modernes

Documentation as code et knowledge base :

- **Documentation interactive** : Création de guides dynamiques et versionnés
- **Runbooks automatisés** : Procédures exécutables et maintenues
- **Base de connaissances intelligente** : Repository searchable et évolutif
- **Guides de bonnes pratiques** : Standards et recommandations versionnés

Formation FinOps et optimisation :

- **Compétences d'optimisation** : Transfert des pratiques de gestion des coûts
- **Pratiques FinOps** : Formation aux méthodologies financières cloud
- **Gestion budgétaire cloud** : Maîtrise des outils de contrôle des coûts
- **Monitoring financier** : Formation au suivi et à l'optimisation

Formation aux outils cloud-native :

- **Outils de monitoring** : Maîtrise des plateformes d'observabilité
- **GitOps et Infrastructure as Code** : Formation aux workflows automatisés
- **Sécurité cloud** : Formation aux outils et pratiques de protection
- **Plateformes de développement** : Maîtrise des environnements modernes

Mise en place de centres d'excellence :

- **Centres d'expertise cloud-native** : Création de communautés d'experts
- **Communautés de pratiques** : Animation de groupes d'échange
- **Programmes de certification** : Développement de parcours de validation
- **Knowledge sharing** : Mise en place de mécanismes de partage

Processus d'autonomie et gouvernance :

- **Processus SRE** : Définition des workflows de fiabilité
- **Workflows GitOps** : Mise en place des processus automatisés
- **Gouvernance cloud-native** : Établissement des règles et standards
- **Mécanismes d'amélioration** : Processus d'évolution continue

Transfert de l'observabilité moderne :

- **Trois piliers** : Formation sur metrics, logs, et traces
- **SLI/SLO et Error Budgets** : Maîtrise des indicateurs de fiabilité
- **Monitoring intelligent** : Formation aux outils d'observabilité avancés
- **Analytics prédictifs** : Formation à l'analyse des tendances

Évaluation et certification :

- **Compétences cloud-native** : Évaluation des acquis techniques
- **Certification interne** : Programmes de validation des compétences
- **Validation pratique** : Tests sur environnements réels
- **Plans de développement** : Plans personnalisés d'évolution

Plan de montée en compétences évolutif :

- **Feuille de route de développement** : Stratégie d'évolution des compétences cloud-native
- **Parcours de certification** : Programmes de validation progressive
- **Stratégie d'évolution** : Plans d'adaptation aux nouvelles technologies
- **Formation continue** : Mécanismes de mise à jour des compétences

Modèle d'exécution :

- **Approche immersive** : Transfert par la pratique avec environnements réels
- **Formation adaptative** : Apprentissage adapté aux profils et personnalisé
- **Évaluation continue** : Validation basée sur les métriques et les retours d'expérience utilisateur
- **Autonomisation progressive** : Passage graduel avec validation et mentoring

PROFIL(S) PRESSENTI(S)

- Expert Formateur Cloud-Native Senior (certification cloud, CKA, SRE)
- Spécialiste Transfert DevOps et SRE (certification DevOps)
- Consultant Transformation Culturelle Cloud-Native
- Spécialiste Documentation as Code et Knowledge Management
- Expert FinOps et Optimisation des Coûts Cloud

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Moyen	Complexe
Équipes à former	<10	10-50	>50
Technologies à transférer	<5	5-15	>15
Environnements	1-2	3-5	>5
Processus à automatiser	<10	10-30	>30
Changements culturels	Mineurs	Modérés	Majeurs
Architecture	Mono-cloud	Multi-cloud	Hybride, edge

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Moyen	Complexe
Délai applicable	60 jours	75 jours	90 jours

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrable(s)	Délai maximal de remise à partir du premier jour d'exécution		
	Simple	Moyen	Complexe
Plan de transfert cloud-native et feuille de route	5 jours	10 jours	10 jours
Programme de formation immersive développé	10 jours	15 jours	15 jours
Formation DevOps/SRE et coaching réalisés	30 jours	40 jours	40 jours
Automatisation Kubernetes et conteneurs	30 jours	40 jours	40 jours

Accompagnement transformation culturelle	40 jours	40 jours	40 jours
Documentation as code et knowledge base	35 jours	40 jours	40 jours
Formation FinOps et optimisation des coûts	25 jours	35 jours	35 jours
Formation outils cloud-native complète	30 jours	40 jours	40 jours
Centres d'excellence et communautés créés	30 jours	40 jours	40 jours
Processus SRE et gouvernance cloud-native	20 jours	30 jours	30 jours
Transfert observabilité moderne	25 jours	35 jours	40 jours
Évaluation et certification cloud-native	30 jours	40 jours	40 jours
Plan évolutif de montée en compétences	Fin de prestation	Fin de prestation	Fin de prestation
Validation autonomie et handover complet	Fin de prestation	Fin de prestation	Fin de prestation

VIII.6.5 UO 6.6.5 - ASTREINTES

OBJET

Astreinte pour la supervision et le traitement des incidents des systèmes d'information et infrastructures techniques.

CONTENU ET MODALITÉS D'EXÉCUTION

Périmètre de couverture :

- Supervision des infrastructures et systèmes d'information
- Monitoring des services et applications métier
- Surveillance des performances et disponibilité des systèmes
- Vérification des processus de sauvegarde et sécurité
- Supervision des interfaces et flux de données
- Traitement d'incidents

Plages horaires :

- **Simple** : 19h30 - 23h00
- **Complexe** : 16h15 - 7h30

Modalités d'intervention :

- Accès à distance aux environnements via VPN
- Diagnostic et résolution des incidents selon procédures établies
- Escalade vers l'équipe de jour si intervention complexe nécessaire
- Coordination avec les équipes métier et techniques
- Retour d'expérience systématique après chaque intervention
- Application des fiches réflexes et procédures documentées

PROFIL(S) PRESSENTI(S)

- Exploitant de Systèmes d'Information
- Technicien d'Exploitation
- Administrateur Systèmes
- Technicien Support

DÉTERMINATION DU NIVEAU DE COMPLEXITÉ

Complexité	Simple	Complexe
Astreinte de 19h30 à 23h	Si oui	-
Astreinte étendue de 16h15 à 7h30	-	Si oui

DÉLAIS D'EXÉCUTION DES PRESTATIONS

Complexité	Simple	Complexe
Délai applicable	19h30-23h00	H24 (16h15-7h30)

LIVRABLE(S) ET DÉLAIS ASSOCIÉS

Livrible(s)	Délai maximal de remise à partir du premier jour d'exécution de la prestation	
	Simple	Complexe
CR d'intervention en astreinte	24 heures	
Fiche réflexe actualisée	5 jours	
Fiche retour d'expérience	3 jours	

