Confidentiel

RGPD chez Adler Technologies

Contrôlé par		Interne	X	Libre	

Historique des modifications

N°	Version	Date	Auteur	Objet
1	2.1	01/12/2017	SJH	Création
2	2.2	04/12/2018	SJH	Mise à jour pour XT-Time en mode SaaS
3	2.3	17/07/2019	SJH	Mise à jour XT-ERP
4	2.4	28/08/2019	SJH	Localisation des serveurs
5	3.0	27/05/2025	SJH	Adaptation pour LPM
6	3.1	01/07/2025	SJH	Ajouter une politique de sécurité
7	4.0	10/07/2025	SJH	Récriture du contrat
8	4.1	31/08/2025	SJH	Intégrer l'enregistrement des appels téléphonique. Article 21 / Annexe 1 – Traitement 5
9				
10				
11				
12				
13				
14				
15				

Table des matières

Conformément au Règlement Général sur la Protection des Données (RGPD)

Entre :

- **Adler Technologies**, SARL, au capital de 100 000 euros, immatriculée au RCS de Créteil sous le numéro 445 336 894 00016, dont le siège social est situé 126 Rue de Brie – 94 000 Créteil, représentée par Sam JARRAH en qualité de gérant, ci-après dénommée "**Le Sous-traitant-éditeur**" ou "**le Sous-traitant**"

Et :

- **Les clients d'Adler Technologies**, ci-après dénommée "**le Client**" ou "**le Responsable de traitement**"

Ci-après dénommées individuellement "**Partie**" et collectivement "**Parties**"

ARTICLE 1 - OBJET ET CHAMP D'APPLICATION

Le présent contrat a pour objet de définir les conditions dans lesquelles Le Sous-traitant-éditeur, agissant en qualité de sous-traitant au sens de l'article 28 du RGPD, traite des données à caractère personnel pour le compte du Client, responsable de traitement, dans le cadre de l'utilisation des logiciels :

- **XT-Time** : solution GTA, de **G**estion des **T**emps de présence et des **A**ctivités, avec ou sans géolocalisation, et des absences. De contrôle d'accès, et 20 aines de modules optionnelles tel que la gestion des droits CP, RTT, CET, interface paie, calcul des heures majorées, ...
- **XT-ERP** : solution ERP spécialisée dans la planification des ressources, circuit achat, vente, gestion à l'affaire, gestion des interventions sur le terrain, et une 20 aines de modules optionnelles telles que dématérialisation des factures, gestion des fluides, gestion de la signatures électroniques, gestion helpdesk, ...
- **XT-Talk** : est une *application* mobile disponible sur *l'App Store*. Elle fait office de pointeuse mobile pour **XT-Time** et constitue un outil complet de gestion et de pilotage des interventions terrain pour **XT-ERP**.

Le Sous-traitant-éditeur utilise par ailleurs un système **d'helpdesk interne**, intégré à XT-ERP pour assurer la traçabilité des demandes RGPD et garantir le respect des obligations de conformité.
Le présent contrat s'applique selon les modalités de commercialisation suivantes :

- **Mode SaaS** : hébergement et exploitation par Le Sous-traitant-éditeur
- **Mode Licence** : installation sur l'infrastructure du Client

---

ARTICLE 2 - DÉFINITIONS

Au sens du présent contrat, les termes suivants ont la signification qui leur est donnée ci-après :
Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable au sens de l'article 4.1 du RGPD.
Traitement : toute opération effectuée sur des données à caractère personnel au sens de l'article 4.2 du RGPD.
Responsable de traitement : la personne physique ou morale qui détermine les finalités et les moyens du traitement au sens de l'article 4.7 du RGPD.
Sous-traitant : la personne physique ou morale qui traite des données à caractère personnel pour le compte du responsable de traitement au sens de l'article 4.8 du RGPD.
Violation de données : violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données à caractère personnel au sens de l'article 4.12 du RGPD.

ARTICLE 3 - DESCRIPTION DES TRAITEMENTS

3.1 Finalités des traitements

Les traitements de données réalisés par Le Sous-traitant-éditeur pour le compte du Client ont pour finalités :
Pour XT-Time :

- Gestion des temps de présence et d'absences des salariés, contrôle d'accès, suivi des activités
- Suivi des heures de travail, traçabilité des accès physique aux locaux du client
- Contrôle des pointages quotidiens
- Géolocalisation des pointages (si activée)

- Génération de rapports de présence et des absences ainsi que les rapports d'accès
- Calcul des heures supplémentaires, CP, RTT, CET, … (si activée)
- Interface paie, import des absences, import fichier du personnel, … (si activée)

Pour XT-ERP :

- Circuit achat, vente, Helpdesk, dématérialisation des factures
- Gestion à l'affaire, Gestion des interventions techniques
- Planification des ressources
- Suivi de la géolocalisation des techniciens
- Gestion des clients, fournisseurs et contacts
- Reporting d'activité
- Et bien d'autres modules

3.2 Catégories de données traitées

Données d'identification :

- Nom, prénom, numéro d'employé/identifiant, coordonnées professionnelles, et personnelles, photographie (pour reconnaissance biométrique si applicable), identifiant paie, identifiant RH, d'autres données peuvent être ajoutées ou personnalisées par le client

Données de géolocalisation (si activé):

- Coordonnées GPS des pointages, adresses des interventions, trajets et déplacements

Données professionnelles :

- Horaires de travail
- Temps de présence
- Absences
- CP, RTT, CET, (si activé)
- Compétences et qualifications (si activé)
- Historique des interventions (si activé)
- Traçabilité d'accès (si activé)

Données techniques :

- Logs de connexion, adresses IP (si mode licence), identifiants des lecteurs de badge ou d'accès, identifiants des terminaux fixes et mobiles, smartphone, tablette (si utilisation de XT-Talk)

3.3 Catégories de personnes concernées

- Salariés du Client
- Techniciens et intervenants
- Clients finaux du Client (contacts)
- Utilisateurs des applications

ARTICLE 4 - OBLIGATIONS DU SOUS-TRAITANT

4.1 Obligations générales

Le Sous-traitant-éditeur s'engage à :

- Ne traiter les données à caractère personnel que sur instruction documentée du Client
- Garantir la confidentialité des données traitées
- Mettre en place les mesures techniques et organisationnelles appropriées
- Ne pas transférer les données vers un pays tiers sans autorisation
- Assister le Client dans le respect de ses obligations
- Supprimer ou restituer les données à l'issue du contrat

4.2 Instructions de traitement

Le Sous-traitant-éditeur ne traite les données à caractère personnel que sur instructions documentées du Client, y compris en ce qui concerne les transferts vers un pays tiers ou une organisation internationale.
Les instructions initiales sont définies dans le présent contrat et dans la documentation technique des logiciels. Toute instruction supplémentaire doit faire l'objet d'un avenant écrit.

Les engagements du Sous-traitant-éditeur au titre du présent contrat sont subordonnés à la fourniture, par le Client, d'instructions claires, documentées et conformes au RGPD. En l'absence ou en cas d'insuffisance de telles instructions, le Sous-traitant-éditeur ne saurait être tenu responsable des écarts de conformité constatés lors d'un audit, d'un contrôle ou d'une procédure, et pourra suspendre le traitement jusqu'à obtention d'instructions appropriées. Cette subordination vise à éviter toute non-conformité factuelle imputable au Responsable de traitement et à limiter les risques de sanctions pour les Parties.

4.3 Confidentialité

Le Sous-traitant-éditeur garantit que les personnes autorisées à traiter les données à caractère personnel sont soumises à une obligation légale appropriée de confidentialité.

ARTICLE 5 - MESURES DE SÉCURITÉ

Voir : ANNEXE 2 : mesures de sécurités détaillées

ARTICLE 6 - SOUS-TRAITANCE ULTÉRIEURE

6.1 Autorisation de sous-traitance

Le Client autorise Le Sous-traitant-éditeur à faire appel à des sous-traitants ultérieurs selon les conditions définies au présent article.

6.2 Sous-traitants autorisés

Hébergeurs :

- Voir ANNEXE 4 - LISTE DES SOUS-TRAITANTS AUTORISÉS

6.3 Obligations relatives aux sous-traitants

Le Sous-traitant-éditeur s'engage à :

- Choisir des sous-traitants qui sont au respect du RGPD
- Informer le Client de tout changement de sous-traitant
- Demeurer pleinement responsable vis-à-vis du Client

ARTICLE 7 - TRANSFERTS INTERNATIONAUX

7.1 Principe

Les données à caractère personnel sont traitées exclusivement au sein de l'Union européenne, sauf autorisation expresse du Client.

7.2 Transferts autorisés

En cas de transfert vers un pays tiers, Le Sous-traitant-éditeur s'engage à :

- Vérifier l'existence d'une décision d'adéquation
- Mettre en place les garanties appropriées (clauses contractuelles types)

- Informer le Client de tout transfert
- Documenter les transferts effectués

ARTICLE 8 - DROITS DES PERSONNES CONCERNÉES

8.1 Assistance au responsable de traitement

Le Sous-traitant-éditeur assiste le Client dans le respect des droits des personnes concernées :

- **Droit d'accès** : fourniture des données dans un délai de 48h
- **Droit de rectification** : correction des données inexactes
- **Droit à l'effacement** : suppression définitive des données
- **Droit à la limitation** : blocage temporaire du traitement
- **Droit à la portabilité** : export dans un format structuré
- **Droit d'opposition** : arrêt du traitement pour motifs légitimes

8.2 Modalités d'assistance

Le Sous-traitant-éditeur s'engage à :

- Répondre aux demandes dans un délai de 1 semaine
- Fournir les outils techniques nécessaires
- Documenter les actions réalisées via son système d'helpdesk interne
- Assurer la traçabilité complète des demandes RGPD
- Facturer les interventions complexes selon le tarif en vigueur

8.3 Traçabilité des demandes RGPD

Le Sous-traitant-éditeur utilise un système d'helpdesk interne pour :

- Enregistrer toutes les demandes d'exercice de droits
- Assurer le suivi des délais de réponse
- Documenter les actions réalisées
- Conserver la preuve de conformité
- Générer des rapports de conformité

ARTICLE 9 - ANALYSE D'IMPACT

Le Sous-traitant-éditeur assiste le Client dans la réalisation d'analyses d'impact relatives à la protection des données (AIPD) lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Cette assistance comprend :

- Fourniture de la documentation technique
- Description des mesures de sécurité
- Évaluation des risques techniques
- Propositions de mesures d'atténuation
- Facturer les interventions complexes selon le tarif en vigueur

---

ARTICLE 10 - NOTIFICATION DES VIOLATIONS

10.1 Obligation de notification

Le Sous-traitant-éditeur notifie au Client toute violation de données à caractère personnel dans les plus brefs délais après en avoir pris connaissance et au plus tard dans un délai de 72 heures.

10.2 Contenu de la notification

La notification contient au minimum :

- Description de la nature de la violation
- Catégories et nombre approximatif de personnes concernées
- Catégories et nombre approximatif d'enregistrements
- Conséquences probables de la violation
- Mesures prises ou envisagées pour remédier à la violation

10.3 Assistance complémentaire

Le Sous-traitant-éditeur assiste le Client dans :

- L'évaluation de l'obligation de notification à l'autorité de contrôle
- La rédaction de la notification aux personnes concernées
- La mise en place de mesures correctives
- La documentation de l'incident

ARTICLE 11 - CONTRÔLES ET AUDITS

11.1 Droit de contrôle

Le Client peut réaliser des audits et inspections pour vérifier le respect du présent contrat, moyennant un préavis de 15 jours.

11.2 Modalités des contrôles

Audits documentaires :

- Fourniture des procédures
- Fourniture des tableaux de bords de contrôle et de suivi
- Fourniture des statistiques

Audits sur site (mode SaaS uniquement) :

- Visite des locaux
- Entretiens avec le personnel
- Vérification des mesures de sécurité
- Frais d'audit à la charge du Client

ARTICLE 12 - DURÉE DE CONSERVATION

12.1 Principes généraux

Les données sont conservées uniquement pour la durée nécessaire aux finalités du traitement, sauf obligation légale de conservation plus longue.

12.2 Durées de conservation par catégorie

Les données sont conservées pour les durées suivantes, qui sont indicatives pour les cas non soumis à des obligations légales strictes et peuvent être ajustées sur instruction documentée du Client (dans la limite des exigences RGPD et des lois applicables). Les durées basées sur des obligations légales (telles que celles issues du Code du travail ou de la prescription commerciale) restent impératives et non indicatives :

- **Données de pointage*** : 5 ans (obligation légale, Article L.3171-1 du Code du travail)
- **Données de géolocalisation** : durée définie par le Client (indicative, max 1 an par défaut, conformément aux recommandations CNIL)
- **Données d'intervention*** : 10 ans (prescription commerciale, Article L.110-4 du Code de commerce)
- **Logs de sécurité** : 1 an (indicative, pour traçabilité)
- **Données de sauvegarde** : 30 jours (mode SaaS, indicative pour optimisation)
- **Traçabilité RGPD (helpdesk interne)** : 10 ans (indicative, pour preuve de conformité ; anciennement "sans délai", ajusté pour alignement CNIL)

12.3 Purge automatique

Le Sous-traitant-éditeur met en place des mécanismes de purge automatique selon les durées définies ci-dessus, par défaut et pour assurer la conformité RGPD, sauf instruction contraire documentée du Client. Les purges ne seront effectuées qu'à la demande expresse du Client pour les durées indicatives et non obligatoires, afin d'éviter toute suppression prématurée. En cas d'instruction de conservation prolongée, le Client assume la responsabilité de justifier cette dérogation auprès des autorités (e.g., CNIL), et Le Sous-traitant-éditeur pourra facturer des coûts supplémentaires d'hébergement.

ARTICLE 13 - RESTITUTION ET SUPPRESSION DES DONNÉES

13.1 À l'expiration du contrat

À l'expiration du contrat de service, Le Sous-traitant-éditeur :

- Restitue toutes les données au Client dans un format exploitable (soumis à facturation)
- Supprime définitivement toutes les copies
- Fournit une attestation de suppression
- Conserve les données 30 jours supplémentaires pour transition

13.2 Modalités de restitution

Mode SaaS :

- Export complet de la base de données
- Format DUMP, ou SQL, en clair ou chiffré, selon demande (soumis à facturation)
- Transmission sécurisée

Mode Licence :

- Assistance à la récupération des données
- Documentation de la structure des données
- Support pour la migration

ARTICLE 14 - RESPONSABILITÉ ET ASSURANCE

14.1 Responsabilité

Chaque partie est responsable du respect de ses obligations au titre de la réglementation sur la protection des données personnelles.

Le Sous-traitant-éditeur est responsable des dommages directs causés par un traitement contraire au RGPD qui lui est imputable et qui résulte d'une faute prouvée de sa part.

14.2 Limitation de responsabilité

La responsabilité de Le Sous-traitant-éditeur est limitée aux dommages directs et prévisibles imputables à une faute prouvée, conformément aux conditions générales de vente et dans le respect des dispositions d'ordre public du RGPD. Sont expressément exclus les dommages indirects ou consécutifs, tels que les pertes de données, de profits, d'exploitation ou d'opportunités, y compris ceux résultant d'une mauvaise configuration ou utilisation par le Client en mode Licence.
En tout état de cause, la responsabilité globale du Sous-traitant-éditeur au titre du présent contrat est plafonnée au montant total des sommes perçues par Le Sous-traitant-éditeur au titre du contrat de service principal au cours des dix-huit (18) mois précédant l'événement générateur de responsabilité.

14.3 Assurance

Le Sous-traitant-éditeur maintient une assurance responsabilité civile professionnelle couvrant les risques liés au traitement des données personnelles.

ARTICLE 15 - DISPOSITIONS PARTICULIÈRES SELON LE MODE DE DÉPLOIEMENT

15.1 Mode SaaS

Responsabilité du Sous-traitant-éditeur :

- Sécurité de l'infrastructure d'hébergement
- Mise à jour et maintenance des logiciels
- Sauvegardes et plan de reprise d'activité
- Surveillance de la sécurité
- Traçabilité RGPD via helpdesk interne

Responsabilité du Client :

- Gestion des comptes utilisateurs
- Configuration des paramètres de sécurité
- Formation des utilisateurs
- Respect des conditions d'utilisation
- Transmission des demandes RGPD

15.2 Mode Licence

Responsabilité du Sous-traitant-éditeur :

- Sécurité du logiciel fourni
- Correctifs de sécurité
- Documentation et formation
- Traçabilité RGPD via helpdesk interne

Responsabilité du Client :

- Sécurité de l'infrastructure
- Installation et configuration
- Sauvegardes et maintenance
- Mise en œuvre des mesures de sécurité
- Transmission des demandes RGPD

ARTICLE 16 - SYSTÈME DE TRAÇABILITÉ RGPD

16.1 Helpdesk interne de conformité

Le Sous-traitant-éditeur utilise un système d'helpdesk interne (intégré à XT-ERP) pour assurer la traçabilité et le suivi de toutes les demandes liées au RGPD, notamment :

Demandes d'exercice de droits :

- Enregistrement automatique de toute demande
- Attribution d'un numéro de ticket unique
- Suivi des délais de traitement (48h pour accusé de réception, 72h pour réponse)
- Traçabilité des actions réalisées
- Archivage des preuves de conformité

Gestion des violations de données :

- Enregistrement immédiat des incidents
- Suivi des notifications aux autorités et personnes concernées
- Documentation des mesures correctives
- Reporting de conformité

Intégration avec XT-ERP : Pour une traçabilité automatisée et optimisée, le système d'helpdesk interne est intégré à XT-ERP. Cela permet une synchronisation automatique des tickets RGPD avec les workflows du Client, facilitant l'enregistrement, le suivi et l'archivage des demandes directement dans l'environnement XT-ERP, tout en respectant les principes de minimisation et de sécurité des données.

16.2 Avantages pour le Client

Ce système, offert comme un service premium par Le Sous-traitant-éditeur, permet au Client de :

- Disposez de votre espace client en ligne pour déclarer des tickets d'incidents
- Obtenir un suivi transparent de ses demandes
- Bénéficier d'une traçabilité complète des actions
- Disposer de preuves documentées en cas de contrôle
- Profiter d'une intégration fluide avec XT-ERP pour une gestion automatisée, réduisant les efforts manuels et améliorant l'efficacité opérationnelle
- Et bientôt (à partir du 1er trimestre 2026) : Recevoir des rapports de conformité détaillés (gratuits pour les clients fidèles, définis comme ceux ayant un contrat actif depuis au moins 12 mois et un historique de paiement sans incident)

16.3 Confidentialité et sécurité

Le système de traçabilité respecte les principes suivants :

- Accès limité aux seules personnes habilitées
- Chiffrement des données de conformité
- Conservation sécurisée des preuves (3 ans)
- Audit trail complet et horodaté
- Sauvegardes régulières et sécurisées

Ce service premium est inclus dans les offres SaaS et Licence avancées, et peut faire l'objet d'options supplémentaires pour une personnalisation accrue. Le Sous-traitant-éditeur s'engage à maintenir et à évoluer ce système en ligne avec les meilleures pratiques RGPD, renforçant ainsi la valeur ajoutée pour ses clients fidèles.

ARTICLE 17 - FORMATION ET SENSIBILISATION

Le Sous-traitant-éditeur s'engage à :

- Former son personnel au RGPD et à la sécurité des données
- Sensibiliser les utilisateurs aux bonnes pratiques
- Fournir la documentation nécessaire

ARTICLE 18 - ÉVOLUTION RÉGLEMENTAIRE

Le Sous-traitant-éditeur s'engage à :

- Suivre l'évolution de la réglementation
- Adapter les mesures de sécurité si nécessaire
- Informer le Client des impacts sur les traitements
- Proposer les modifications contractuelles requises

ARTICLE 19 - ENTRÉE EN VIGUEUR ET DURÉE

Le présent contrat entre en vigueur à la date de sa signature et pour toute la durée du contrat de service principal.
Il peut être modifié par avenant signé des deux parties ou en cas d'évolution réglementaire majeure.

Afin d'assurer une mise en conformité progressive et transparente avec les dispositions du présent contrat, Le Sous-traitant-éditeur s'engage à respecter la feuille de route détaillée en
Annexe A : Feuille de Route Progressive vers la Conformité Intégrale RGPD
Cette annexe décrit les actions futures que Le Sous-traitant-éditeur doit engager pour atteindre un accord total avec les exigences du document, y compris les timelines associées (indiquées par trimestre de mise en route). Le Client peut consulter cette Annexe A pour suivre l'avancement des mesures, qui seront mises à jour annuellement ou en cas de besoin, sous réserve d'un avenant si des modifications substantielles sont requises. Le Sous-traitant-éditeur fournira des rapports trimestriels sur l'état d'avancement au Client sur demande documentée.

ARTICLE 20 - DROIT APPLICABLE ET JURIDICTION

Le présent contrat est soumis au droit français.
En cas de litige, après tentative de résolution amiable, les tribunaux de Créteil seront seuls compétents.

ARTICLE 21 - DISPOSITIONS RELATIVES À L'INTELLIGENCE ARTIFICIELLE

Conformément au Règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées sur l'intelligence artificielle (AI Act), entré en vigueur en 2024 et pleinement applicable à compter du 2 août 2026 (avec des exceptions pour les interdictions et obligations générales), les Parties s'engagent à respecter les obligations applicables en matière d'intelligence artificielle (IA), en complément des dispositions du RGPD.
Si les logiciels XT-Time ou XT-ERP impliquent des traitements basés sur l'intelligence artificielle (par exemple, dans XT-Time, optimisation des horaires d'un service en fonction de leur historique de pointages, ou tester l'authenticité d'un arrêt maladie, dans XT-ERP pour la planification automatisée des ressources, l'optimisation des tournées ou le suivi des interventions via des algorithmes d'apprentissage automatique :

- Aucun traitement IA classé à haut risque au sens de l'AI Act ne sera déployé sans une Analyse d'Impact relative à la Protection des Données (AIPD) préalable, conformément à l'article 35 du RGPD et aux exigences d'évaluation de conformité de l'AI Act. Le Client, en tant que Responsable de traitement, est tenu de réaliser ou de coordonner cette AIPD, avec l'assistance du Sous-traitant-éditeur sur demande documentée.
- Le Sous-traitant-éditeur assistera le Client dans le respect de ses obligations sous l'AI Act, notamment en fournissant les informations techniques nécessaires pour l'évaluation des risques, la transparence des systèmes IA et la mise en œuvre de mesures de mitigation (telles que la gestion des risques, la documentation des modèles IA et les audits de conformité).
- Les traitements IA seront limités aux finalités définies à l'Article 3 du présent contrat, respecteront les principes de minimisation des données, de transparence et de non-discrimination, et ne traiteront pas de données sensibles sans base juridique appropriée et mesures de sécurité renforcées.
- En cas de classification d'un traitement comme IA à haut risque ou interdit par l'AI Act, le Sous-traitant-éditeur informera immédiatement le Client et suspendra le traitement jusqu'à obtention d'instructions écrites confirmant la conformité. Toute modification liée à l'IA fera l'objet d'un avenant au présent contrat.
- Le Sous-traitant-éditeur s'engage à suivre l'évolution de l'AI Act et à adapter ses pratiques en conséquence, en informant le Client de tout impact potentiel sur les traitements.

Cette clause ne s'applique que si des fonctionnalités IA sont activées dans les logiciels, sur instruction du Client. Le Sous-traitant-éditeur demeure pleinement responsable de ses obligations en tant que fournisseur ou déployeur d'IA au sens de l'AI Act, dans la limite des instructions reçues.

L'éditeur informe également que certains appels téléphoniques peuvent être enregistrés et analysés par des outils d'IA, afin d'assurer le suivi qualité, la formation et l'optimisation des services. Ces enregistrements sont traités dans le respect du RGPD et des principes de proportionnalité.

Ce contrat a été établi en conformité avec le Règlement (UE) 2016/679 du 27 avril 2016 (RGPD) et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée.

ANNEXE 1 - REGISTRE DES TRAITEMENTS

Conformément à l'article 30 du RGPD

TRAITEMENT N°1 - XT-TIME (MODE SAAS)

1.1 Identification du traitement

Nom du traitement : *Gestion des temps de présence XT-Time (mode SaaS)*

Responsable de traitement : *Client utilisateur du logiciel*

Responsable du traitement chez le sous-traitant-éditeur : *Sam JARRAH*

1.2 Finalités du traitement

- *Gestion des temps de présence des salariés*
- *Suivi des heures de travail et absences*
- *Contrôle des pointages quotidiens*
- *Géolocalisation des pointages (optionnel)*
- *Génération de rapports de présence*
- *Calcul des heures supplémentaires, CP, RTT, CET, Interface paie, Import des absences, et bien d'autres modules (optionnel)*
- *Édition de tableaux de bord RH*

1.3 Base juridique

Côté Client (Responsable de traitement) :

- *Art. 6.1.b RGPD : Exécution du contrat de travail*
- *Art. 6.1.c RGPD : Respect d'obligations légales (Code du travail)*
- *Art. 6.1.f RGPD : Intérêt légitime pour la géolocalisation*

Côté Sous-traitant-éditeur :

- *Art. 6.1.f RGPD : Intérêt légitime pour la fourniture du service*

1.4 Catégories de données traitées

Données d'identification :

- *Nom, prénom*
- *Numéro d'employé/matricule*
- *Adresse email professionnelle*
- *Photographie (pour reconnaissance faciale si activée)*

Données de pointage :

- *Heures d'arrivée et de départ*
- *Temps de pause*
- *Heures de travail effectuées*
- *Statut présence/absence*
- *Historique des pointages*

Données de géolocalisation** (optionnel) **:

- *Coordonnées GPS du pointage*
- *Adresse du lieu de pointage*
- *Rayon de tolérance géographique*
- *Historique des localisations*

Données techniques :

- *Identifiant du terminal/badge*
- *Adresse IP de connexion*
- *Logs d'utilisation*
- *Horodatage des actions*

1.5 Catégories de personnes concernées

- *Salariés du Client*
- *Intérimaires et personnel temporaire*
- *Stagiaires et apprentis*
- *Consultants externes (si applicable)*

1.6 Destinataires des données

Destinataires internes :

- *Service RH du Client*
- *Managers et responsables d'équipe*
- *Service paie du Client*
- *Administrateurs système*

Destinataires externes :

- *Experts-comptables (pour la paie)*
- *Avocats (en cas de contentieux)*
- *Autorités de contrôle (sur demande)*
- *Juridictions compétentes (sur réquisition)*

1.7 Transferts vers des pays tiers

***Principe :** Aucun transfert vers des pays tiers*

***Hébergement :** Union européenne exclusivement (AWS EU)*

- ***Région principale et de backup :** EU-West-1 (Irlande) **Garanties :** AWS Data Processing Agreement (DPA) conforme RGPD*

1.8 Durées de conservation

Données de pointage : *5 ans (art. L3171-4 Code du travail)*
Données de géolocalisation : *1 an maximum (recommandation CNIL)*
Logs techniques : *1 an*
Sauvegardes : *30 jours*
Données supprimées : *Effacement définitif après expiration*

1.9 Mesures de sécurité

Mesures techniques (AWS) :

- *Chiffrement AES-256 au repos et en transit (AWS KMS)*
- *Serveurs virtuels sécurisés (Amazon EC2)*
- *Base de données chiffrée (Amazon Aurora)*
- *Sauvegardes automatiques chiffrées (AWS Backup)*
- *Monitoring de sécurité (GuardDuty, CloudTrail, CloudWatch)*
- *Firewall cloud (Security Groups, Network ACLs)*
- *Authentification multi-facteurs (AWS IAM)*
- *Détection des menaces (AWS GuardDuty)*

Mesures organisationnelles :

- *Politique de sécurité documentée*
- *Formation du personnel au cloud AWS*
- *Contrôle des accès via AWS IAM*
- *Procédures d'incident cloud*
- *Audits des configurations AWS*
- *Conformité certifications AWS (ISO 27001, SOC 2)*

1.10 Sous-traitants ultérieurs

Hébergeur cloud : *Amazon Web Services (AWS)*

- *Localisation : EU (Paris - eu-west-3) ou EU (Irlande - eu-west-1)*
- *Certification : ISO 27001, ISO 27017, ISO 27018, SOC 2, CISPE*
- *Services : Infrastructure cloud (EC2, Aurora, S3, etc.)*
- *Contrat : AWS Data Processing Agreement (DPA)*

Maintenances matérielles : *ASF sécurité*

- *Localisation : France*
- *Services : Installation et maintenances des lecteurs de badges et accès*
- *Accès : sur site du client*

TRAITEMENT N°2 - XT-TIME (MODE LICENCE)

2.1 Identification du traitement

Nom du traitement : *Gestion des temps de présence XT-Time (mode licence)*
Responsable de traitement : *Client utilisateur du logiciel*
Sous-traitant-éditeur : *Adler Technologies (pour le support et la maintenance)*
Date de création : *2003*
Responsable du traitement chez le sous-traitant-éditeur : *M. Stephan COFFIN*

2.2 Finalités du traitement
Identiques au mode SaaS *(voir traitement N°1)*

2.3 Base juridique
Identique au mode SaaS *(voir traitement N°1)*

2.4 Catégories de données traitées
Identiques au mode SaaS *(voir traitement N°1)*

2.5 Catégories de personnes concernées
Identiques au mode SaaS *(voir traitement N°1)*

2.6 Destinataires des données
Accès limité du sous-traitant-éditeur :

- *Équipe support technique (uniquement en cas d'intervention)*
- *Développeurs (pour résolution de bugs critiques)*
- *Responsable sécurité (pour audits)*

Autres destinataires : *Déterminés par le Client*

2.7 Transferts vers des pays tiers
Aucun transfert *par le sous-traitant-éditeur*
Support à distance : *Via AWS Systems Manager (région EU)*
Responsabilité du Client *pour son infrastructure si applicable*

2.8 Durées de conservation
Gestion par le Client *selon ses obligations légales*
Accès du sous-traitant-éditeur : *Limité à la durée d'intervention*
Logs d'intervention : *1 an chez le sous-traitant-éditeur*

2.9 Mesures de sécurité
Responsabilité partagée :

- ***Sous-traitant-éditeur :*** *Sécurité du logiciel, correctifs, formation, support AWS*

- ***Client :*** *accès au logiciel*

Mesures du sous-traitant :

- *Support via AWS Systems Manager (connexion sécurisée)*
- *Authentification AWS IAM pour les techniciens*
- *Logs des interventions dans AWS CloudTrail*
- *Chiffrement des sessions de support*
- *Accès temporaire uniquement*

2.10 Sous-traitants ultérieurs

Support technique : *Editeur*

- *Localisation : France*
- *Services: Support via AWS Systems Manager*
- *Accès : Temporaire et tracé via AWS CloudTrail*

Infrastructure AWS : *Amazon Web Services*

- *Localisation : EU (si support à distance via AWS)*
- *Services : Outils de support et monitoring*
- *Accès : Limité aux interventions autorisées*

TRAITEMENT N°3 - XT-ERP (MODE SAAS)

3.1 Identification du traitement

Nom du traitement : *Gestion des achats / ventes / interventions XT-ERP*

Responsable de traitement : *Client utilisateur du logiciel*

Sous-traitant-éditeur : *Adler technologies*

Responsable du traitement chez le sous-traitant-éditeur : *M. Ahamd WABBI*

3.2 Finalités du traitement

- *Gestion des interventions techniques*
- *Planification des interventions sur le terrain*
- *Suivi de la géolocalisation des techniciens*
- *Gestion des clients et contacts*
- *Facturation des prestations*
- *Reporting d'activité et performance*
- *Optimisation des tournées*

3.3 Base juridique

Côté Client (Responsable de traitement) :

- *Art. 6.1.b RGPD : Exécution de contrats commerciaux*

- *Art. 6.1.c RGPD : Respect d'obligations légales (facturation)*
- *Art. 6.1.f RGPD : Intérêt légitime pour la géolocalisation*

Côté Sous-traitant-éditeur :

- *Art. 6.1.f RGPD : Intérêt légitime pour la fourniture du service*

3.4 Catégories de données traitées

Données des techniciens :

- *Nom, prénom*
- *Coordonnées professionnelles*
- *Qualifications et compétences*
- *Planning d'intervention*
- *Géolocalisation en temps réel (optionnel)*

Données des clients finaux :

- *Raison sociale/nom*
- *Adresse d'intervention*
- *Coordonnées de contact*
- *Historique des interventions*
- *Informations techniques (équipements)*

Données d'intervention :

- *Nature de l'intervention*
- *Durée et horaires*
- *Matériel utilisé*
- *Comptes-rendus*
- *Photos/documents techniques*

Données de facturation :

- *Montants facturés*
- *Conditions de paiement*
- *Historique des paiements*
- *Données comptables*

3.5 Catégories de personnes concernées

- *Techniciens et intervenants du Client*
- *Clients finaux du Client*
- *Contacts des entreprises clientes*
- *Utilisateurs administratifs*

3.6 Destinataires des données

Destinataires internes :

- *Service commercial du Client*
- *Service technique du Client*
- *Service comptabilité du Client*

- *Direction du Client*

Destinataires externes :

- *Clients finaux (pour validation d'intervention)*
- *Experts-comptables*
- *Organismes de certification (si applicable)*
- *Autorités de contrôle (sur demande)*

3.7 Transferts vers des pays tiers

Principe : *Aucun transfert vers des pays tiers*

Hébergement : *Union européenne exclusivement (AWS EU)*

- ***Région principale et de backup :*** *EU-West-1 (Irlande)* ***Garanties :*** *AWS Data Processing Agreement (DPA) conforme RGPD*

3.8 Durées de conservation

Données d'intervention : *10 ans (prescription commerciale)*

Données de géolocalisation : *1 an maximum*

Données de facturation : *10 ans (obligations comptables)*

Logs techniques : *1 an*

Sauvegardes : *30 jours*

3.9 Mesures de sécurité

Identiques au traitement XT-Time SaaS *avec services AWS :*

- *Chiffrement AES-256 (AWS KMS)*
- *Serveurs Amazon EC2 sécurisés*
- *Base de données Amazon Aurora chiffrée*
- *Monitoring AWS (GuardDuty, CloudTrail, CloudWatch)*
- *Sauvegardes automatiques AWS Backup*
- *Firewall cloud (Security Groups)*
- *Authentification AWS IAM*

3.10 Sous-traitants ultérieurs

Identiques au traitement XT-Time SaaS *avec AWS :*

- ***Amazon Web Services*** *: Infrastructure cloud EU*
- ***Prestataires techniques*** *: Support via AWS Systems Manager*
- ***Certification*** *: ISO 27001, SOC 2, CISPE*

TRAITEMENT N°4 - HELPDESK INTERNE RGPD

4.1 Identification du traitement

Nom du traitement : *Système de traçabilité RGPD*
Responsable de traitement : *Editeur*
Finalité : *Gestion interne de la conformité RGPD*
Responsable du traitement : *M. Aimen Daghsen*

4.2 Finalités du traitement

- *Traçabilité des demandes d'exercice de droits*
- *Suivi des délais de traitement RGPD*
- *Documentation des actions de conformité*
- *Archivage des preuves de conformité*
- *Génération de rapports de conformité*
- *Gestion des violations de données*
- *Amélioration continue des processus*

4.3 Base juridique

Art. 6.1.f RGPD : *Intérêt légitime pour assurer la conformité réglementaire*

4.4 Catégories de données traitées

Données des demandeurs :

- *Nom, prénom*
- *Coordonnées (email, téléphone)*
- *Société d'appartenance*
- *Fonction/rôle*

Données de traitement :

- *Nature de la demande RGPD*
- *Date de réception*
- *Délais de traitement*
- *Actions réalisées*
- *Preuves d'exécution*
- *Correspondances échangées*

Données de suivi :

- *Numéro de ticket*
- *Statut de la demande*
- *Historique des actions*
- *Responsable du traitement*
- *Date de clôture*

4.5 Catégories de personnes concernées

- *Salariés des entreprises clientes*

- *Contacts des entreprises clientes*
- *Utilisateurs finaux des logiciels*
- *Responsables RGPD clients*

4.6 Destinataires des données

Destinataires internes :

- *Équipe conformité RGPD*
- *Direction juridique*
- *Responsables produits*
- *Équipes techniques (si nécessaire)*

Destinataires externes :

- *Clients (pour suivi de leurs demandes)*
- *Avocats spécialisés (si contentieux)*
- *Autorités de contrôle (sur demande)*

4.7 Transferts vers des pays tiers

Aucun transfert *vers des pays tiers*

Hébergement : *Amazon Web Services - Région EU (Irland)*

Données internes *: Traitées exclusivement en Union européenne*

4.8 Durées de conservation

Données de traçabilité : *3 ans (preuve de conformité)*

Correspondances : *3 ans*

Rapports de conformité : *3 ans*

Logs système : *1 an*

4.9 Mesures de sécurité

Mesures techniques AWS :

- *Chiffrement des données sensibles (AWS KMS)*
- *Accès limité aux personnes habilitées (AWS IAM)*
- *Authentification multi-facteurs (AWS MFA)*
- *Audit trail complet (AWS CloudTrail)*
- *Sauvegardes sécurisées (AWS Backup)*
- *Monitoring continu (AWS CloudWatch)*

Mesures organisationnelles :

- *Politique de confidentialité interne*
- *Formation des équipes AWS et RGPD*
- *Procédures documentées*
- *Contrôles d'accès réguliers via AWS IAM*

4.10 Sous-traitants ultérieurs

Hébergement : *Amazon Web Services (AWS)*

- *Localisation : EU-West-3 (Paris, France)*
- *Services : Infrastructure cloud (EC2, Aurora, S3)*
- *Certification : ISO 27001, SOC 2, CISPE*
- *Contrat : AWS Data Processing Agreement (DPA)*

SYNTHÈSE DES TRAITEMENTS

Traitement	*Mode*	*Finalité principale*	*Durée conservation*	*Transfert pays tiers*	*Hébergement*
XT-Time	*SaaS*	*Gestion temps présence*	*5 ans (pointages, absences)*	*Non*	*AWS EU (Irlande)*
XT-Time	*Licence*	*Gestion temps présence*	*Définie par client*	*Non*	*Client + support AWS*
XT-ERP	*SaaS*	*ERP*	*10 ans (commercial)*	*Non*	*AWS EU (Irlande)*

TRAITEMENT N°5 – ENREGISTREMENT ET TRAITEMENT DES APPELS TÉLÉPHONIQUES

1. Identification du traitement

- *Nom du traitement : Enregistrement et analyse des appels téléphoniques*
- *Responsable de traitement : Client utilisateur des services Adler Technologies*
- *Sous-traitant-éditeur : Adler Technologies*
- *Responsable du traitement chez le sous-traitant-éditeur : SJH*

2. Finalités du traitement

- *Assurer la preuve des échanges contractuels et commerciaux*
- *Améliorer la qualité du service rendu*
- *Former les collaborateurs internes*
- *Analyser les enregistrements via des outils d'**intelligence artificielle (IA)** afin d'optimiser les processus internes, améliorer la réactivité du support et développer des services innovants*

3. Base juridique

- *Art. 6.1.b RGPD : Exécution du contrat (preuve des échanges)*
- *Art. 6.1.f RGPD : Intérêt légitime (qualité, formation, innovation IA)*

- *Art. 6.1.a RGPD : Consentement explicite si l'enregistrement est utilisé pour des finalités marketing, de recherche ou de scoring avancé*

4. Catégories de données traitées

- *Données d'identification de l'interlocuteur (nom, prénom, fonction, coordonnées téléphoniques)*
- *Données de communication (contenu de l'appel, enregistrement vocal)*
- *Données techniques liées à l'appel (date, heure, durée, numéro appelant/appelé, métadonnées techniques)*
- *Données dérivées issues de l'IA (transcription, analyse sémantique, détection de mots-clés, scoring de satisfaction)*

5. Catégories de personnes concernées

- *Clients et prospects*
- *Fournisseurs et partenaires*
- *Collaborateurs du Client ou du Sous-traitant-éditeur (dans le cadre de la formation)*

6. Destinataires des données

- *Destinataires internes : Service support, service qualité, direction, collaborateurs en formation*
- *Destinataires externes : Sous-traitants techniques IA dûment encadrés contractuellement (art. 28 RGPD), autorités judiciaires en cas de litige*

7. Transferts vers des pays tiers

- *Principe : Aucun transfert hors UE*
- *Si recours exceptionnel à un outil IA externe : transfert uniquement encadré par des clauses contractuelles types (SCC) et avec information préalable du Client*

8. Durées de conservation

- *Enregistrements destinés à la qualité/formation :* ***6 mois maximum***
- *Enregistrements destinés à la preuve contractuelle :* ***jusqu'à 5 ans*** *(durée de prescription commerciale)*
- *Résultats anonymisés des analyses IA : conservation possible sans limite à des fins statistiques et de recherche*

9. Mesures de sécurité

- *Chiffrement AES-256 des fichiers audios*
- *Accès restreint aux personnes habilitées*
- *Journalisation et traçabilité des accès*
- *Stockage sécurisé dans l'UE (infrastructures AWS conformes RGPD)*
- *Procédure de purge automatique en fin de durée de conservation*

10. Sous-traitants ultérieurs

- *Hébergeur cloud pour traitement IA: Amazon Web Services (AWS – régions EU)*

- *Hébergeur cloud opérateur téléphonique : W3Tel - 1 Rue Terre Neuve bât G, 91940 Les Ulis*
- *Prestataires IA (si utilisés) : OpenAI, Mistral, Claude, Gemini soumis à clauses RGPD et AI Act*

CONTACTS
Responsable du registre : *Sam JARRAH (SJH) – responsable produit*
Email : *s.jarrah@xtime.fr*
Téléphone : *+33 6 03 07 04 95*

Ce registre est mis à jour régulièrement et tenu à disposition des autorités de contrôle conformément à l'article 30 du RGPD.

ANNEXE 2 - MESURES DE SÉCURITÉ DÉTAILLÉES

INFORMATIONS GÉNÉRALES

Sous-traitant-éditeur : *Adler Technologies*

Responsable sécurité : *M. Ahmad WABBI*

Infrastructure :

- ***Cloud Provider:*** *Amazon Web Services (AWS)*
- ***Région :*** *Europe (eu-west-3 - Paris) ou eu-west-1 (Irlande)*
- ***Serveurs :*** *Amazon EC2*
- ***Base de données :*** *Amazon Aurora*
- ***Localisation :*** *Union Européenne exclusivement*

Certifications AWS :

- *ISO 27001, ISO 27017, ISO 27018*
- *SOC 1, SOC 2, SOC 3*
- ***Certification CISPE*** *(Code of Conduct for Data Protection)*

Définitions et intérêts des briques sécuritaires utilisés

- ***AWS GuardDuty*** *est un service de détection des menaces*
  Il est conçu pour analyser en continu les événements de sécurité afin d'identifier des comportements malveillants, des accès non autorisés ou des activités suspectes dans un compte AWS.
- *Objectif principal :*
  Fournir une surveillance automatisée, intelligente et en temps quasi réel de la sécurité de l'environnement AWS, sans déployer d'agent sur les ressources.

- ***AWS Inspector*** *est un service de gestion des vulnérabilités automatisé qui analyse en continu les ressources AWS afin de détecter les failles de sécurité, les erreurs de configuration et les logiciels obsolètes.*
- *Objectif principal :*
  Identifier les vulnérabilités techniques (système, packages, configurations) présentes sur les machines EC2, les conteneurs Amazon ECR ou les images de machine virtuelle, pour prévenir les cyberattaques.

- **AWS CloudTrail** est un service de journalisation qui enregistre toutes les actions effectuées sur un compte AWS, qu'elles soient humaines (via la Console AWS, AWS CLI) ou automatisées (via les SDK, API, services AWS).
- *Objectif principal :*
  Tracer, auditer et analyser l'activité des utilisateurs, rôles, services et API dans l'environnement AWS, pour des besoins de sécurité, conformité, audit ou forensic.

- ***Amazon CloudWatch*** *est un service de surveillance et d'observabilité qui permet de collecter, visualiser, analyser et réagir aux métriques, logs et événements générés par votre infrastructure AWS (et vos applications on-premise si besoin).*
- *Objectif principal :*
  Offrir une vue centralisée et en temps réel de la santé, des performances et de l'activité des ressources AWS et des applications, pour permettre une détection proactive des incidents, une optimisation des performances, et une réaction rapide aux anomalies.

- ***VPC Flow Logs*** *est un service AWS permettant d'enregistrer les flux de trafic IP (entrant et sortant) associés aux interfaces réseau d'un VPC (Virtual Private Cloud). Il s'agit d'un outil d'observation réseau essentiel pour la sécurité, le diagnostic réseau et l'audit de conformité.*
- *Objectif principal :*
  Permettre à une entreprise d'enregistrer, analyser et auditer le trafic réseau au sein de son environnement AWS, notamment pour détecter des comportements anormaux, comprendre les pannes ou prouver la conformité.

Vision stratégique

L'utilisation combinée de ces cinq services permet de mettre en place une défense en profondeur ("defense-in-depth") qui couvre toutes les couches critiques de sécurité cloud : détection, prévention, supervision, traçabilité, et conformité.

1. Surveillance en continu des menaces – AWS GuardDuty

- *Détection comportementale des menaces (exfiltration, minage crypto, escalation de privilège, etc.)*
- *Basé sur des flux de renseignement et des modèles ML*
- *Aucune infrastructure à déployer, détection active dès activation*
- ***RGPD :*** *assure la détection des accès non autorisés à des données personnelles*

***Stratégie** : permet de surveiller en continu l'environnement AWS sans perturber la production, en gardant une traçabilité des menaces internes/externes.*

2. Détection des vulnérabilités système – AWS Inspector

- *Analyse automatique des failles de sécurité dans EC2, ECR*
- *Évalue les CVE, permissions excessives, configurations dangereuses*
- *Attribution de scores de risque*
- ***RGPD :** répond à l'exigence d'évaluation régulière des failles de sécurité (art. 32 du RGPD)*

***Stratégie :** permet d'anticiper les failles techniques avant qu'elles ne soient exploitées.*

3. Supervision & réactivité – AWS CloudWatch

- *Collecte de métriques système (CPU, RAM, erreurs)*
- *Surveillance de logs applicatifs et alertes automatiques*
- *Déclenchement d'actions correctives (auto-reboot, scaling, etc.)*
- ***RGPD :** utile pour documenter les mesures techniques de surveillance (plan de sécurité informatique)*

***Stratégie :** outil central pour une détection précoce d'incident, et réduction du temps de réaction (MTTR).*

4. Traçabilité des actions – AWS CloudTrail

- *Journalisation de toutes les actions d'administration AWS (API, console, CLI)*
- *Qui a fait quoi, quand, comment et depuis où*
- *Conservation dans un bucket sécurisé (S3)*
- ***RGPD :** couvre l'obligation de pouvoir auditer les accès et modifications aux données personnelles*

***Stratégie :** indispensable pour l'audit interne, la preuve de conformité, et les analyses post-incidents.*

5. Audit réseau – VPC Flow Logs

- *Journalisation de tous les flux réseau (IP source/destination, port, protocole, accept/reject)*
- *Suivi de la connectivité entre services, machines, internet*
- *Corrélation avec CloudWatch et GuardDuty*
- ***RGPD :** permet de démontrer l'absence d'exposition non intentionnelle de données sensibles*

Stratégie : *permet d'isoler les comportements suspects réseau, de détecter des fuites potentielles, ou de documenter les canaux réseau autorisés.*

Architecture combinée = Sécurité intégrée, visibilité complète

Couche	***Solution AWS***	***Rôle stratégique***
Prévention des failles	*AWS Inspector*	*Évite les vulnérabilités techniques avant qu'elles ne soient exploitées*
Détection comportementale	*AWS GuardDuty*	*Identifie les activités anormales ou malveillantes*
Surveillance opérationnelle	*AWS CloudWatch*	*Supervise la santé système & déclenche des actions*
Audit et conformité	*AWS CloudTrail*	*Trace toutes les actions humaines et machines*
Trafic réseau	*VPC Flow Logs*	*Journalise tous les flux IP, pour contrôle ou forensic*

Conformité RGPD – Article 32 et plus

L'ensemble de ces services couvre les 4 piliers exigés par le RGPD (article 32) :

Exigence RGPD	*Réponse AWS*
Confidentialité	*VPC Flow Logs + GuardDuty permettent de détecter toute fuite de données*
Intégrité	*CloudTrail trace les modifications sur les systèmes*
Disponibilité	*CloudWatch surveille la disponibilité des services critiques*
Résilience	*Intégration avec des workflows de remédiation automatique (via EventBridge + Lambda)*

Bonus : *la combinaison offre des preuves exploitables lors d'un contrôle CNIL ou d'un audit ISO 27001.*

En combinant ces cinq briques AWS, nous obtenons :

- *Une visibilité complète sur ce qui se passe dans notre cloud*
- *Une détection proactive des risques techniques ou comportementaux*
- *Une réponse rapide et documentée en cas d'incident*
- *Un socle RGPD solide, industrialisable et évolutif*

1. MODÈLE DE RESPONSABILITÉ PARTAGÉE AWS

1.1 Responsabilités AWS (Sécurité DU cloud)

1.1.1 Infrastructure physique

- ***Centres de données** sécurisés et certifiés*
- ***Sécurité physique** des serveurs*
- ***Redondance** et haute disponibilité*
- ***Climatisation** et alimentation électrique*
- ***Destruction sécurisée** des supports*

1.1.2 Services managés

- ***Hyperviseur** et isolation des instances*
- ***Réseau** infrastructure AWS*
- ***Sécurité** des services Aurora, EC2, S3*
- ***Mises à jour** de sécurité de l'infrastructure*
- ***Monitoring** infrastructure 24h/24*

1.2 Responsabilités de Le Sous-traitant-éditeur (Sécurité DANS le cloud)

1.2.1 Configuration des services

- ***Configuration** des instances EC2*
- ***Paramétrage** des bases de données Aurora*
- ***Gestion** des utilisateurs et accès*
- ***Configuration** des Security Groups*
- ***Chiffrement** des données*

1.2.2 Applications et données

- ***Sécurité** des applications*
- ***Gestion** des données personnelles*
- ***Sauvegarde** et récupération*
- ***Monitoring** applicatif*
- ***Mise à jour** des OS et applications*

2. SERVICES AWS UTILISÉS ET SÉCURITÉ

2.1 Amazon EC2 (Serveurs virtuels)

2.1.1 Configuration sécurisée

Instances EC2 :

- ***AMI*** *(Amazon Machine Image) officielles et à jour*
- ***Instance type*** *dimensionnée selon les besoins*
- ***Placement*** *dans un VPC privé*
- ***EBS*** *(Elastic Block Store) chiffré par défaut*
- ***Security Groups*** *configurés en mode restrictif*

Système d'exploitation :

- ***Ubuntu LTS*** *ou* ***Amazon Linux 2, ou Windows 2025*** *(support étendu)*
- ***Mises à jour*** *manuelle*
- ***Couple de supervision proactive AWS: AWS GuardDuty*** *+ AWS Inspector*
- ***Monitoring*** *: AWS CloudWatch*
- ***Logs****: AWS CloudTrail activé, VPC Flow logs activé*

2.1.2 Accès aux serveurs

AWS Systems Manager Session Manager :

- ***Connexion*** *RDP, SSH, uniquement à partir du réseau Adler*
- ***Accès*** *via console AWS, ou RDP*
- ***Traçabilité*** *voire* ***Logs*** *(paragraphe avant)*
- ***Pas de bastion host*** *nécessaire*
- ***Chiffrement*** *des sessions*

Alternative SSH (si nécessaire) :

- ***Clés SSH*** *uniques par utilisateur*
- ***Rotation*** *des clés tous les 6 mois*
- ***Connexion*** *via VPN uniquement*
- ***Disable*** *du password authentication*

2.2 Amazon Aurora (Base de données)

2.2.1 Sécurité de la base de données

Configuration Aurora :

- ***Chiffrement*** *au repos activé (AES-256)*
- ***Chiffrement*** *en transit (SSL/TLS)*
- ***Subnet group*** *privé uniquement*
- ***Backup*** *automatique activé (7 jours minimum)*
- ***Point-in-time recovery*** *activé*

Contrôle d'accès :

- ***Mots de passe*** *forts (MFA2)*
- ***Rotation*** *des mots de passe (tous les 3 mois)*

- ***Principe** du moindre privilège*
- ***Audit** des connexions activé*

2.2.2 Monitoring et alertes

AWS RDS Performance Insights :

- ***Surveillance** des performances*
- ***Détection** des requêtes anormales*
- ***Alertes** sur les pics d'activité*
- ***Historique** des performances*

AWS CloudWatch :

- ***Métriques** de base de données*
- ***Alertes** personnalisées*
- ***Logs** d'erreur collectés*
- ***Tableaux de bord** de monitoring*

2.3 Réseau et sécurité

2.3.1 Amazon VPC (Virtual Private Cloud)

Configuration réseau :

- ***VPC** dédié avec sous-réseaux privés*
- ***Internet Gateway** pour accès sortant uniquement*
- ***NAT Gateway** pour mise à jour des serveurs*
- ***Route tables** configurées de manière restrictive*
- ***Network ACLs** en plus des Security Groups*

Sous-réseaux :

- ***Subnet public** : Load Balancer uniquement*
- ***Subnet privé** : Serveurs d'application*
- ***Subnet privé** : Base de données*
- ***Availability Zones** multiples pour redondance*

2.3.2 AWS Security Groups (Firewall)

Configuration des Security Groups :

- ***Deny all** par défaut*
- ***Règles** entrantes restrictives*
- ***HTTPS** (port 443) depuis Internet uniquement*
- ***SSH** (port 22) depuis VPN uniquement*
- ***Base de données** (port 3306) depuis app uniquement*

2.4 Sauvegardes et récupération

2.4.1 AWS Backup

Configuration automatique :

- ***Plan de sauvegarde*** *quotidien*
- ***Retention*** *: 30 jours minimum*
- ***Sauvegarde*** *cross-region activée*
- ***Chiffrement*** *des sauvegardes*
- ***Test*** *de restauration mensuel*

Ressources sauvegardées :

- ***Volumes EBS*** *des serveurs EC2*
- ***Base de données*** *Aurora (automated backup)*
- ***Configuration*** *des Security Groups*
- ***Snapshots*** *des AMI personnalisées*

2.4.2 Stratégie de récupération

Objectifs :

- ***RTO*** *(Recovery Time Objective) : 4 heures*
- ***RPO*** *(Recovery Point Objective) : 1 heure*
- ***Sauvegarde*** *dans région secondaire*
- ***Test*** *de récupération trimestriel*

Procédure de récupération :

1. ***Évaluation*** *des dégâts*
2. ***Lancement*** *d'instances depuis backup*
3. ***Restauration*** *base de données*
4. ***Reconfiguration*** *des Security Groups*
5. ***Test*** *de fonctionnement*
6. ***Bascule*** *du trafic*

---

3. AUTHENTIFICATION ET ACCÈS

3.1 AWS IAM (Identity and Access Management)

3.1.1 Gestion des utilisateurs

Comptes AWS :

- ***Root account*** *sécurisé et non utilisé*
- ***Comptes IAM*** *individuels pour chaque utilisateur*
- ***MFA*** *obligatoire pour tous les accès*

- ***Rotation*** *des clés d'accès tous les 3 mois*
- ***Pas de clés*** *en dur dans le code*

Politiques d'accès :

- ***Principe*** *du moindre privilège*
- ***Groupes*** *par fonction (Admin, Developer, ReadOnly)*
- ***Politiques*** *personnalisées par besoin*
- ***Révision*** *annuelle des droits*
- ***Suppression*** *immédiate en cas de départ*

3.1.2 Authentification multi-facteurs (MFA)

Configuration MFA :

- ***Obligatoire*** *pour tous les utilisateurs AWS*
- ***Applications*** *supportées : Google Authenticator, Authy*
- ***Backup codes*** *sécurisés*
- ***Renouvellement*** *en cas de perte de device*
- ***Audit*** *des connexions sans MFA*

3.2 Accès aux applications

3.2.1 Application Load Balancer (ALB)

Configuration HTTPS :

- ***Certificat SSL*** *AWS Certificate Manager*
- ***Renouvellement*** *automatique*
- ***Redirection*** *HTTP vers HTTPS*
- ***HSTS*** *activé*
- ***Logs*** *d'accès dans CloudWatch*

3.2.2 Authentification applicative

Mécanismes d'authentification :

- ***JWT*** *tokens avec expiration*
- ***Session*** *timeout à 10 minutes, paramétrable par application et par client*
- ***Password policy*** *: 8 caractères minimum*
- ***Account lockout*** *: non limité*
- ***Audit*** *des connexions*

---

4. MONITORING ET SURVEILLANCE

4.1 AWS CloudWatch / Zabbix

4.1.1 Métriques surveillées

Serveurs EC2 :

- ***CPU** utilization > 80%*
- ***Memory** utilization > 80%*
- ***Disk** utilization > 80%*
- ***Network** errors*
- ***Status** check failures*

Base de données Aurora :

- ***CPU** utilization > 80%*
- ***Database** connections > 80%*
- ***Read/Write** latency*
- ***Storage** utilization*
- ***Backup** failures*

4.1.2 Alertes configurées

Notifications :

- ***Email** à l'équipe technique*
- ***Escalade** automatique si pas de réponse*

4.2 AWS CloudTrail

4.2.1 Audit des actions

Événements audités :

- ***Connexions** à la console AWS*
- ***Modifications** des Security Groups*
- ***Accès** aux instances EC2*
- ***Modifications** de la base de données*
- ***Création/suppression** de ressources*

4.2.2 Stockage des logs

Configuration :

- ***Stockage** dans S3 avec chiffrement*
- ***Retention** : 1 an minimum*
- ***Intégrité** vérifiée par AWS*
- ***Accès** limité aux administrateurs*
- ***Alertes** sur actions critiques*

4.3 AWS GuardDuty

4.3.1 Détection des menaces

Surveillance automatique :

- ***Activité*** *malveillante sur les instances*
- ***Reconnaissance*** *réseau*
- ***Compromission*** *d'instances*
- ***Communication*** *avec des botnets*
- ***Exfiltration*** *de données*

4.3.2 Réponse aux menaces

Actions automatiques :

- ***Isolation*** *de l'instance compromise*
- ***Notification*** *immédiate de l'équipe*
- ***Collecte*** *des preuves*
- ***Analyse*** *des logs*
- ***Recommandations*** *de remédiation*

---

5. CHIFFREMENT ET PROTECTION DES DONNÉES

5.1 Chiffrement au repos

5.1.1 Amazon EBS (Elastic Block Store)

Configuration :

- ***Chiffrement*** *par défaut activé*
- ***Clés KMS*** *gérées par AWS*
- ***Rotation*** *automatique des clés*
- ***Chiffrement*** *AES-256*
- ***Snapshots*** *chiffrés automatiquement*

5.1.2 Amazon Aurora

Chiffrement de la base :

- ***TDE*** *(Transparent Data Encryption)*
- ***Clés*** *gérées par AWS KMS*
- ***Backups*** *automatiquement chiffrés*
- ***Replicas*** *chiffrés*
- ***Logs*** *chiffrés*

5.2 Chiffrement en transit

5.2.1 Communications externes

HTTPS/TLS :

- ***TLS 1.2*** *minimum*
- ***Certificats*** *AWS Certificate Manager*

- ***Perfect Forward Secrecy*** *activé*
- ***HSTS*** *configuré*
- ***Redirection*** *HTTP vers HTTPS*

5.2.2 Communications internes

Chiffrement interne :

- ***SSL*** *entre application et base de données*
- ***VPC*** *pour isolation réseau*
- ***Security Groups*** *pour contrôle d'accès*
- ***Private subnets*** *pour les serveurs*

5.3 AWS Key Management Service (KMS)

5.3.1 Gestion des clés

Clés de chiffrement :

- ***Customer Master Keys*** *(CMK) par environnement*
- ***Rotation*** *automatique annuelle*
- ***Audit*** *de l'utilisation des clés*
- ***Permissions*** *granulaires*
- ***Backup*** *des clés*

---

6. GESTION DES INCIDENTS

6.1 Détection automatique

6.1.1 AWS Config

Surveillance de la configuration :

- ***Compliance*** *rules automatiques*
- ***Détection*** *des dérives de configuration*
- ***Alertes*** *sur modifications non autorisées*
- ***Historique*** *des configurations*
- ***Remédiation*** *automatique possible*

6.1.2 AWS Security Hub

Tableau de bord unifié :

- ***Findings*** *de sécurité centralisée*
- ***Intégration*** *GuardDuty, Inspector, Macie*
- ***Compliance*** *checks automatiques*
- ***Priorisation*** *des alertes*
- ***Workflows*** *de remédiation*

6.2 Procédure de réponse

6.2.1 Incident critique

Actions immédiates :

1. ***Isolation** de l'instance compromise*
2. ***Notification** équipe sécurité*
3. ***Collecte** des preuves (snapshots, logs)*
4. ***Analyse** de l'impact*
5. ***Communication** aux parties prenantes*

6.2.2 Remédiation

Étapes de remédiation :

1. ***Identification** de la cause racine*
2. ***Patch** des vulnérabilités*
3. ***Reconfiguration** des systèmes*
4. ***Test** de non-régression*
5. ***Mise en production** sécurisée*

---

7. CONFORMITÉ ET AUDIT

7.1 Conformité RGPD

7.1.1 Localisation des données

Contraintes géographiques :

- ***Région AWS** : EU (Paris) ou EU (Irlande)*
- ***Pas de transfert** hors Union Européenne*
- ***Data residency** garantie*
- ***Accord** de sous-traitance avec AWS*
- ***Certifications** AWS valides*

7.1.2 Droits des personnes

Mise en œuvre technique :

- ***Chiffrement** des données personnelles (chiffrement Aurora)*
- ***Pseudonymisation** quand possible*
- ***Accès** granulaire aux données*
- ***Suppression** sécurisée possible*
- ***Portabilité** des données*

7.2 Audit et reporting

7.2.1 AWS CloudTrail

Traçabilité complète :

- ***Tous*** *les accès AWS loggés*
- ***Intégrité*** *des logs garantie*
- ***Rétention*** *1 an minimum – pour les loges critiques*
- ***Accès*** *en lecture seule*
- ***Export*** *pour audit externe*

7.2.2 Rapports de conformité

Reporting mensuel :

- ***Incidents*** *de sécurité*
- ***Disponibilité*** *des services*
- ***Backup*** *status*
- ***Vulnérabilités*** *détectées*
- ***Actions*** *correctives*

---

8. PROCÉDURES OPÉRATIONNELLES

8.1 Déploiement sécurisé

8.1.2 CI/CD Pipeline

Pipeline de déploiement :

- ***Tests*** *de sécurité automatisés*
- ***Scan*** *des vulnérabilités*
- ***Validation*** *des configurations*
- ***Déploiement*** *progressif (test – demo- prod)*
- ***Monitoring*** *post-déploiement*

8.2 Maintenance préventive

8.2.1 Mises à jour

Patch management :

- ***AWS Systems Manager*** *Patch Manager*
- ***Maintenance windows*** *planifiées*
- ***Test*** *sur environnement de recette*
- ***Rollback*** *plan préparé*
- ***Monitoring*** *post-mise à jour*

8.2.2 Optimisation continue

Révision trimestrielle :

- ***Analyse*** *des coûts*

- ***Optimisation*** *des performances*
- ***Révision*** *des Security Groups*
- ***Mise à jour*** *des AMI*
- ***Formation*** *équipe sur nouveautés AWS – travail personnel*

ANNEXE 3 - PROCÉDURE DE GESTION DES INCIDENTS

---

1. DÉFINITIONS ET TYPES D'INCIDENTS

1.1 Définition d'un incident de sécurité

Un incident de sécurité est un événement qui compromet ou peut compromettre :

- ***Confidentialité** : Accès non autorisé aux données*
- ***Intégrité** : Modification non autorisée des données*
- ***Disponibilité** : Interruption des services*
- ***Traçabilité** : Perte des logs d'audit*

1.2 Types d'incidents

1.2.1 Incidents techniques

- ***Panne** serveur ou base de données*
- ***Surcharge** système ou réseau*
- ***Défaillance** des sauvegardes*
- ***Erreur** de configuration*
- ***Bug** critique applicatif*

1.2.2 Incidents de sécurité

- ***Tentative** d'intrusion détectée*
- ***Accès** non autorisé aux données*
- ***Malware** ou virus détecté*
- ***Phishing** ou ingénierie sociale*
- ***Perte** ou vol d'équipement*

1.2.3 Violations de données personnelles

- ***Accès** non autorisé aux données RGPD*
- ***Suppression** accidentelle ou malveillante*
- ***Divulgation** involontaire de données*
- ***Exfiltration** de données personnelles*
- ***Modification** non autorisée des données*

---

2. CLASSIFICATION ET PRIORISATION

2.1 Niveaux de criticité

2.1.1 Critique (P1)

Critères :

- *Service complètement indisponible*
- *Violation de données personnelles sensibles*
- *Perte de données critiques*
- *Compromission de la sécurité*

Exemples :

- *Panne complète AWS région*
- *Accès non autorisé à la base de données*
- *Suppression massive de données*
- *Attaque par ransomware*

Délais :

- ***Détection** : Immédiate (monitoring)*
- ***Réaction** : 1 heure*
- ***Escalade** : Immédiate*
- ***Résolution** : 4 heures maximum*

2.1.2 Élevé (P2)

Critères :

- *Service partiellement indisponible*
- *Dégradation significative des performances*
- *Violation mineure de données*
- *Risque de sécurité modéré*

Exemples :

- *Lenteur importante des applications*
- *Erreur de configuration Security Group*
- *Accès à des logs par utilisateur non autorisé*
- *Défaillance d'un service AWS*

Délais :

- ***Détection** : 1 heure*
- ***Réaction** : 2 heures*
- ***Escalade** : 4 heures*
- ***Résolution** : 24 heures maximum*

2.1.3 Moyen (P3)

Critères :

- *Dysfonctionnement mineur*
- *Impact limité sur les utilisateurs*
- *Risque potentiel de sécurité*

- *Problème de performance localisé*

Exemples :

- *Bug non bloquant dans l'application*
- *Alerte de monitoring non critique*
- *Problème de synchronisation des données*
- *Mise à jour de sécurité à appliquer*

Délais :

- ***Détection** : 8 heures*
- ***Réaction** : 8 heures*
- ***Escalade** : 72 heures*
- ***Résolution** : 1 semaine maximum*

2.1.4 Faible (P4)

Critères :

- *Problème cosmétique*
- *Amélioration de performance*
- *Demande d'évolution*
- *Problème documentaire*

Exemples :

- *Problème d'affichage mineur*
- *Optimisation des requêtes*
- *Mise à jour de documentation*
- *Formation utilisateur*

Délais :

- ***Détection** : Variable*
- ***Réaction** : 72 heures*
- ***Escalade** : Non applicable*
- ***Résolution** : 1 mois maximum*

2.2 Matrice de criticité

Impact	***Disponibilité***	***Données***	***Sécurité***	***Utilisateurs***	***Niveau***
Critique	*100% indisponible*	*Perte/violation*	*Compromission*	*Tous*	*P1*
Élevé	*> 50% indisponible*	*Accès non autorisé*	*Vulnérabilité*	*> 50%*	*P2*
Moyen	*< 50% indisponible*	*Problème intégrité*	*Risque potentiel*	*< 50%*	*P3*

Faible	*Performance*	*Problème mineur*	*Amélioration*	*Individuel*	*P4*

---

3. DÉTECTION ET SURVEILLANCE

3.1 Outils de surveillance AWS

3.1.1 Amazon CloudWatch

Métriques surveillées :

- ***CPU*** *des instances EC2 > 80%*
- ***Mémoire*** *des instances > 80%*
- ***Connexions*** *Aurora > 80% du maximum*
- ***Latence*** *des requêtes > 2 secondes*
- ***Erreurs*** *HTTP 5xx > 1%*

Alertes configurées :

- ***Email*** *: SJH / AWI / ADN*
- ***SMS*** *: en cours*
- ***Webhook*** *: Intégration avec l'helpdesk, en cours*
- ***Escalade*** *: Après 4 alertes consécutives*

3.1.2 AWS GuardDuty

Détection automatique :

- ***Reconnaissance*** *réseau*
- ***Compromission*** *d'instances*
- ***Exfiltration*** *de données*
- ***Communication*** *avec botnets*
- ***Crypto-mining*** *malveillant*

Actions automatiques :

- ***Isolation*** *de l'instance. En cours*
- ***Notification*** *immédiate équipe*
- ***Ticket*** *helpdesk automatique. En cours*
- ***Collecte*** *des preuves*

3.1.3 AWS CloudTrail

Événements audités :

- ***Connexions*** *à la console AWS*
- ***Modifications*** *des Security Groups*
- ***Accès*** *aux données sensibles*
- ***Changements*** *de configuration*
- ***Tentatives*** *d'accès échouées*

Alertes sur événements critiques :

- ***Root account** utilisé*
- ***MFA** désactivé*
- ***Suppression** de logs*
- ***Modification** des politiques IAM*
- ***Accès** depuis pays non autorisés*

3.2 Surveillance applicative

3.2.1 Monitoring interne

Logs applicatifs :

- ***Erreurs** de connexion base de données*
- ***Échecs** d'authentification répétés*
- ***Temps** de réponse anormaux*
- ***Exceptions** non gérées*
- ***Utilisations** anormales des API*

Indicateurs métier :

- ***Nombre** de pointages par jour*
- ***Connexions** utilisateurs*
- ***Requêtes** API par minute*
- ***Taille** des données échangées*
- ***Erreurs** de synchronisation*

3.2.2 Surveillance manuelle

Vérifications quotidiennes :

- ***Statut** des services AWS*
- ***Rapport** des sauvegardes*
- ***Logs** d'erreur applicatifs*
- ***Alertes** de sécurité*
- ***Utilisation** des ressources*

---

4. PROCÉDURE DE RÉPONSE AUX INCIDENTS

4.1 Détection et alerte

4.1.1 Sources de détection

Automatique :

- ***Alertes** CloudWatch*
- ***Findings** GuardDuty*
- ***Événements** CloudTrail*
- ***Monitoring** applicatif*

- ***Logs** d'erreur*

Manuelle :

- ***Signalement** utilisateur*
- ***Vérification** quotidienne*
- ***Rapport** client*
- ***Audit** de sécurité*
- ***Veille** technique*

4.1.2 Première alerte

Réception de l'alerte :

1. ***Notification** reçue (email, SMS, webhook)*
2. ***Vérification** de l'authenticité*
3. ***Évaluation** initiale de l'impact*
4. ***Création** d'un ticket helpdesk*
5. ***Notification** du responsable incident*

Informations à collecter :

- ***Horodatage** de l'événement*
- ***Source** de l'alerte*
- ***Services** impactés*
- ***Utilisateurs** concernés*
- ***Symptômes** observés*

4.2 Création du ticket incident

4.2.1 Helpdesk - Ticket d'incident

Informations obligatoires :

- ***Numéro** de ticket unique*
- ***Date/heure** de détection*
- ***Niveau** de criticité (P1 à P4)*
- ***Description** détaillée*
- ***Services** impactés*
- ***Responsable** assigné*
- ***Statut** initial : "Ouvert"*

Exemple de ticket :

Ticket #INC-2024-001
Date : 15/03/2024 10:30
Criticité : P1
Titre : Panne base de données Aurora
Description : Impossibilité de connexion à la base Aurora

Services : XT-Time, XT-ERP
Statut : Ouvert
Client impacté : Tous

4.2.2 Suivi dans l'helpdesk

Statuts possibles :

- ***Ouvert** : Incident détecté, en cours d'analyse*
- ***En cours** : Résolution en cours*
- ***Résolu** : Solution appliquée, en test*
- ***Fermé** : Incident résolu définitivement*
- ***Escaladé** : Transféré à un niveau supérieur*

Historique automatique :

- ***Toutes** les actions loggées*
- ***Horodatage** de chaque étape*
- ***Responsable** de chaque action*
- ***Commentaires** détaillés*
- ***Pièces** jointes (logs, captures)*

4.3 Équipe de réponse

4.3.1 Composition de l'équipe

***Responsable incident :** SCN*

- ***Coordination** générale*
- ***Décisions** techniques*
- ***Communication** interne/externe*
- ***Escalade** si nécessaire*

***Responsable technique :** ADN / AWI / SJH*

- ***Diagnostic** technique*
- ***Résolution** des problèmes*
- ***Liaison** avec AWS Support*
- ***Tests** de fonctionnement*

***Responsable communication :** SJH*

- ***Information** des utilisateurs*
- ***Communication** clients*
- ***Notification** RGPD si nécessaire*
- ***Reporting** direction*

4.3.2 Rôles et responsabilités

Pendant l'incident :

- ***Responsable incident** : Prend les décisions*

- ***Équipe technique*** *: Analyse et résout*
- ***Autres*** *: Évitent les interventions parasites*
- ***Direction*** *: Informée mais n'interfère pas*

Répartition des tâches :

- ***Investigation*** *: Équipe technique*
- ***Communication*** *: Responsable désigné*
- ***Documentation*** *: Mise à jour helpdesk*
- ***Décisions*** *: Responsable incident uniquement*

---

5. ACTIONS DE RÉSOLUTION

5.1 Analyse et diagnostic

5.1.1 Collecte d'informations

Logs et métriques :

- ***CloudWatch*** *: Métriques système*
- ***CloudTrail*** *: Logs d'audit*
- ***GuardDuty*** *: Alertes de sécurité*
- ***Logs*** *applicatifs*
- ***Témoignages*** *utilisateurs*

Outils de diagnostic :

- ***AWS System Manager*** *: Accès aux instances*
- ***AWS X-Ray*** *: Tracing des requêtes*
- ***RDS Performance Insights*** *: Diagnostic DB*
- ***VPC Flow Logs*** *: Analyse réseau*
- ***AWS Config*** *: Historique des configs*

5.1.2 Analyse des causes

Méthodologie :

1. ***Symptômes*** *: Qu'est-ce qui ne fonctionne pas ?*
2. ***Chronologie*** *: Quand cela a-t-il commencé ?*
3. ***Corrélation*** *: Quels changements récents ?*
4. ***Impact*** *: Qui/quoi est affecté ?*
5. ***Cause*** *: Pourquoi cela s'est-il produit ?*

Documentation dans l'helpdesk :

- ***Hypothèses*** *testées*
- ***Résultats*** *des tests*
- ***Causes*** *identifiées*
- ***Solutions*** *envisagées*

- ***Décision** finale*

5.2 Actions correctives

5.2.1 Mesures immédiates

Confinement :

- ***Isolation** des systèmes compromis*
- ***Arrêt** des services défaillants*
- ***Basculement** vers système de secours*
- ***Limitation** des accès utilisateurs*
- ***Sauvegarde** des preuves*

Exemples par type d'incident :

- ***Panne** : Redémarrage des services*
- ***Intrusion** : Isolation de l'instance*
- ***Malware** : Arrêt et scan antivirus*
- ***Violation** : Verrouillage des comptes*
- ***Erreur** : Rollback de la configuration*

5.2.2 Résolution définitive

Eradication :

- ***Suppression** de la cause racine*
- ***Correction** des vulnérabilités*
- ***Mise à jour** des systèmes*
- ***Renforcement** des sécurités*
- ***Validation** des correctifs*

Récupération :

- ***Restauration** des services*
- ***Validation** du fonctionnement*
- ***Test** de non-régression- manuel*
- ***Surveillance** renforcée*
- ***Retour** à la normale*

5.3 Utilisation des services AWS

5.3.1 AWS Support

Cas d'escalade vers AWS :

- ***Panne** infrastructure AWS*
- ***Problème** de performance AWS*
- ***Question** de sécurité AWS*
- ***Besoin** d'expertise technique*

- ***Incident** critique P1*

Procédure de contact :

1. ***Ouverture** cas AWS Support*
2. ***Liaison** avec ticket helpdesk interne*
3. ***Suivi** régulier des échanges*
4. ***Synchronisation** des actions*
5. ***Clôture** coordonnée*

5.3.2 Services AWS d'urgence

AWS Systems Manager :

- ***Accès** d'urgence aux instances*
- ***Exécution** de commandes à distance*
- ***Patch** management d'urgence*
- ***Collecte** de logs système*

AWS Config :

- ***Historique** des configurations*
- ***Compliance** rules activées*
- ***Remédiation** automatique*

---

6. COMMUNICATION ET NOTIFICATION

6.1 Communication interne

6.1.1 Notification immédiate

Incidents P1 (Critiques) :

- ***Direction** : Appel + Email immédiat*
- ***Équipe technique** : Appel + Email immédiat + WhatsApp*
- ***Équipe support** : Appel + Email immédiat + WhatsApp*
- ***Toute l'équipe** : Information générale*

Incidents P2 (Élevés) :

- ***Responsable technique** : Email + WhatsApp*
- ***Équipe technique** : Email + WhatsApp*
- ***Direction** : Email informatif*
- ***Support** : Mise à jour statut*

Canaux de communication :

- ***Téléphone** : Urgences uniquement*
- ***Email** : de la personne concernée*
- ***WhatsApp**: Message*
- ***Helpdesk** : Commentaires du ticket*

6.1.2 Points de situation

Fréquence selon criticité :

- ***P1** : Toutes les 30 minutes*
- ***P2** : Toutes les 2 heures*
- ***P3** : Hebdomadaire*
- ***P4** : Mensuel*

Contenu du point :

- ***Statut** actuel de l'incident*
- ***Actions** en cours*
- ***Prochaines** étapes*
- ***Estimation** de résolution*
- ***Impact** clients*

6.2 Communication externe

6.2.1 Notification clients

Incidents impactants :

- ***P1** : Notification < 1 heure*
- ***P2** : Notification < 2 heures*
- ***P3** : Notification < 1 semaine*
- ***P4** : Pas de notification (sauf demande)*

Canaux de notification :

- ***Email** : Contacts techniques clients*

Contenu de la notification :

- ***Nature** de l'incident*
- ***Services** impactés*
- ***Estimation** de résolution*
- ***Actions** en cours*
- ***Prochaine** mise à jour*

6.2.2 Modèles de communication

Notification initiale :

Objet : [INCIDENT] Problème technique sur [Service]
Cher client,
Nous rencontrons actuellement un problème technique sur [Service] qui peut impacter [Fonctionnalités].

Incident détecté : [Date/Heure]
Services impactés : [Liste]
Cause identifiée : [Cause ou "En cours d'investigation"]
Estimation résolution : [Délai]

Nos équipes travaillent activement à la résolution.
Prochaine mise à jour : [Heure]

Équipe technique [Entreprise]

Notification de résolution :

Objet : [RÉSOLU] Problème technique sur [Service]
Cher client,
Le problème technique sur [Service] est désormais résolu.

Incident résolu : [Date/Heure]
Durée d'impact : [Durée]
Cause : [Cause identifiée]
Solution appliquée : [Solution]

Tous les services fonctionnent normalement.
Un rapport d'incident détaillé suivra sous 48h.

Équipe technique [Entreprise]

---

7. VIOLATIONS DE DONNÉES PERSONNELLES

7.1 Évaluation de la violation

7.1.1 Critères d'évaluation

Type de données concernées :

- ***Données d'identification** : Nom, prénom, email*
- ***Données sensibles** : Localisation, biométrie*
- ***Données techniques** : Logs, adresses IP*
- ***Données professionnelles** : Horaires, interventions*

Nombre de personnes concernées :

- ***< 100** : Risque limité*

- ***100-1000*** *: Risque modéré*
- ***1000-10000*** *: Risque élevé*
- ***> 10000*** *: Risque critique*

Risque pour les droits et libertés :

- ***Faible*** *: Données pseudonymisées*
- ***Modéré*** *: Données professionnelles*
- ***Élevé*** *: Données sensibles*
- ***Critique*** *: Risque d'usurpation d'identité*

7.1.2 Matrice de risque RGPD

Données	***Personnes***	***Risque***	***Notification CNIL***	***Notification personnes***
Pseudonymisées	*< 100*	*Faible*	*Non*	*Non*
Professionnelles	*100-1000*	*Modéré*	*Oui*	*Non*
Sensibles	*> 1000*	*Élevé*	*Oui*	*Oui*
Identifiantes	*> 10000*	*Critique*	*Oui*	*Oui*

7.2 Procédure de notification

7.2.1 Notification à la CNIL

Délai : *72 heures maximum après prise de connaissance*

Procédure :

1. ***Évaluation*** *du risque (< 4 heures)*
2. ***Décision*** *de notification (< 8 heures)*
3. ***Préparation*** *du dossier (< 72 heures)*
4. ***Envoi*** *notification CNIL (< une semaine)*
5. ***Suivi*** *des échanges avec la CNIL*

Responsable : *SJH*

Suppléant : *AWI*

Outil : *Téléprocédure CNIL + helpdesk interne*

Contenu de la notification :

- ***Nature*** *de la violation*
- ***Catégories*** *de données concernées*
- ***Nombre*** *approximatif de personnes*
- ***Conséquences*** *probables*
- ***Mesures*** *prises ou envisagées*

7.2.2 Notification aux clients

Délai : *48 heures maximum*

Procédure :

1. ***Notification*** *<48 par email*
2. ***Appel*** *téléphonique si critique*
3. ***Réponse*** *aux questions clients*
4. ***Rapport*** *détaillé sous 72h*

Modèle de notification :

Objet : [URGENT] Violation de données personnelles
Cher client,
Nous vous informons qu'un incident de sécurité a affecté
Certaines données personnelles traitées par nos services.

Incident détecté : [Date/Heure]
Nature : [Description]
Données concernées : [Type et nombre]
Personnes impactées : [Nombre et catégories]
Mesures prises : [Actions correctives]

Nous avons immédiatement :
- Sécurisé les systèmes
- Notifié la CNIL
- Renforcé la surveillance

Un rapport détaillé suivra sous 48h.
Contact : [Email/Téléphone]

Direction [Entreprise]

7.2.3 Notification aux personnes concernées

Quand notifier :

- ***Risque élevé*** *pour les droits et libertés*
- ***Données sensibles*** *compromises*
- ***Risque*** *d'usurpation d'identité*
- ***Impossibilité*** *de réduire le risque*

Moyens de notification :

- ***Email** : Canal principal*
- ***Appel** : Si pas d'email*

Contenu :

- ***Nature** de la violation*
- ***Données** vous concernant*
- ***Risques** potentiels*
- ***Mesures** que nous prenons*
- ***Conseils** pour vous protéger*
- ***Contact** pour plus d'informations*

---

8. SUIVI ET CLÔTURE

8.1 Résolution et tests

8.1.1 Validation de la résolution

Tests fonctionnels :

- ***Redémarrage** des services si nécessaire*
- ***Vérification** des fonctionnalités*
- ***Tests** de performance*
- ***Validation** utilisateur*
- ***Monitoring** renforcé*

Tests de sécurité :

- ***Scan** de vulnérabilités*
- ***Vérification** des accès*
- ***Contrôle** des configurations*
- ***Audit** des logs*
- ***Test** de restauration*

8.1.2 Surveillance post-incident

Monitoring renforcé :

- ***Durée** : 48h minimum*
- ***Fréquence** : Toutes les 2 heures*
- ***Métriques** : Performances et sécurité*
- ***Alertes** : Seuils abaissés*
- ***Rapports** : Toutes les 8h*

Critères de normalisation :

- ***Stabilité** > 24h*
- ***Performances** normales*
- ***Pas d'alerte** de sécurité*
- ***Utilisateurs** satisfaits*

- ***Metrics*** *dans les normes*

8.2 Clôture du ticket

8.2.1 Helpdesk - Clôture

Informations de clôture :

- ***Date/heure*** *de résolution*
- ***Durée*** *totale de l'incident*
- ***Cause*** *racine identifiée*
- ***Solution*** *appliquée*
- ***Tests*** *effectués*
- ***Validation*** *utilisateur*

Statut final :

- ***Résolu*** *: Solution appliquée et validée*
- ***Fermé*** *: Incident complètement terminé*
- ***Archivé*** *: Après 30 jours sans réouverture*

8.2.2 Validation client

Confirmation de résolution :

- ***Email*** *de confirmation envoyé*
- ***Validation*** *par le client*
- ***Satisfaction*** *mesurée*
- ***Feedback*** *collecté*
- ***Amélioration*** *proposée*

8.3 Rapport d'incident

8.3.1 Rapport technique

Contenu :

- ***Résumé*** *exécutif*
- ***Chronologie*** *détaillée*
- ***Cause*** *racine*
- ***Impact*** *mesuré*
- ***Actions*** *correctives*
- ***Prévention*** *future*

Délai : *48h après résolution*

Diffusion : *Équipe technique + Direction*

Stockage : *Helpdesk + Archives*

8.3.2 Rapport client

Contenu :

- ***Description*** *de l'incident*
- ***Impact*** *sur les services*
- ***Actions*** *de résolution*

- ***Prévention*** *mise en place*
- ***Excuses*** *si nécessaire*

Délai : *48h après résolution*

Format : *HTML ou texte*

Diffusion : *Contacts clients impactés*

---

9. AMÉLIORATION CONTINUE

9.1 Retour d'expérience

9.1.1 Post-mortem

Réunion d'équipe :

- ***Délai*** *: 1 semaine après résolution*
- ***Participants*** *: Équipe de réponse*
- ***Durée*** *: 1 heure maximum*
- ***Animateur*** *: Responsable incident*

Questions analysées :

- ***Qu'est-ce qui a bien fonctionné ?***
- ***Qu'est-ce qui a mal fonctionné ?***
- ***Qu'est-ce qui aurait pu être mieux ?***
- ***Quelles améliorations proposer ?***
- ***Comment éviter la récurrence ?***

9.1.2 Actions d'amélioration

Types d'actions :

- ***Technique*** *: Monitoring, alertes, outils*
- ***Processus*** *: Procédures, formation*
- ***Organisationnel*** *: Équipe, responsabilités*
- ***Préventif*** *: renforcement, tests*

Suivi des actions :

- ***Responsable*** *: Assigné à chaque action*
- ***Délai*** *: Date limite définie*
- ***Statut*** *: Suivi dans l'helpdesk*
- ***Validation*** *: Tests et validation*
- ***Efficacité*** *: Mesure de l'amélioration*

9.2 Évolution des procédures

9.2.1 Mise à jour des procédures

Révision après incident :

- ***Procédure*** *: Mise à jour si nécessaire*
- ***Formation*** *: Équipe informée*

- ***Test*** *: Validation sur cas similaire*
- ***Documentation*** *: Mise à jour helpdesk*
- ***Diffusion*** *: Toute l'équipe*

Révision périodique :

- ***Fréquence*** *: Trimestrielle*
- ***Responsable*** *: Responsable sécurité*
- ***Critères*** *: Efficacité, conformité*
- ***Validation*** *: Direction + équipe*
- ***Mise en œuvre*** *: Formation + tests*

9.2.2 Métriques et KPI

Indicateurs de performance :

- ***Nombre*** *d'incidents par mois*
- ***Temps*** *de détection moyen*
- ***Temps*** *de résolution par criticité*
- ***Satisfaction*** *client*
- ***Taux*** *de résolution au premier niveau*

Objectifs :

- ***P1*** *: Résolution < 4h (100%)*
- ***P2*** *: Résolution < 24h (95%)*
- ***P3*** *: Résolution < 72h (90%)*
- ***Satisfaction*** *client > 90%*
- ***Détection*** *automatique > 70%*

---

10. CONTACTS ET ESCALADE

10.1 Contacts internes

10.1.1 Équipe de réponse

Responsables incidents : *SJH / ADN / AWI*
Disponibilité : *24h/24 pour P1*
Responsable technique : *AWI*
Disponibilité : *7h-20h / Astreinte P1 – faisant partie de son contrat de travail*
Responsable communication : *SJH*
Disponibilité : *9h-18h / Astreinte P1*

10.1.2 Direction

Directeur Général : *SJH*
Notification : *P1 immédiat, P2 < 2h*

10.2.2 Autorités

CNIL :
Téléphone : *01 53 73 22 22*
Email : *[Via téléprocédure]*
Adresse : *3 Place de Fontenoy, 75007 Paris*

ANSSI :
Téléphone : *01 71 75 84 68*
Email : *cert-fr.cossi@ssi.gouv.fr*
Disponibilité : *24h/24 (incidents majeurs)*

10.2.3 Prestataires

Audit sécurité : *Adler Technologies*
Disponibilité : *Heures ouvrées*

ANNEXE 4 - LISTE DES SOUS-TRAITANTS AUTORISÉS

Conformément à l'article 28.2 du RGPD

CADRE LÉGAL ET OBLIGATIONS

Obligations générales

Conformément à l'article 28.2 du RGPD, le sous-traitant ne peut faire appel à un autre sous-traitant que :

- ***Avec l'autorisation** écrite du responsable de traitement*
- ***En respectant** les mêmes obligations de protection des données*
- ***Sous sa responsabilité** pleine et entière*

Garanties requises

Chaque sous-traitant ultérieur doit :

- ***Présenter** des garanties suffisantes de conformité RGPD*
- ***Mettre en œuvre** des mesures techniques et organisationnelles appropriées*
- ***Signer** un contrat de sous-traitance conforme au RGPD*
- ***Accepter** les audits et inspections*

SOUS-TRAITANT N°1 - AMAZON WEB SERVICES (AWS)

1.1 Identification du sous-traitant

***Raison sociale :** Amazon Web Services EMEA SARL*

***Adresse :** 38 Avenue John F. Kennedy, L-1855 Luxembourg*

***Pays :** Luxembourg (Union Européenne)*

***Numéro d'identification :** B-101818*

***Site web :** https://aws.amazon.com*

Entité contractante France :

Amazon Web Services France SAS

67 Boulevard du Général Leclerc, 92110 Clichy, France

1.2 Services fournis

Infrastructure cloud :

- ***Amazon EC2** : Serveurs virtuels pour hébergement applications*
- ***Amazon Aurora** : Base de données relationnelle managée*
- ***Amazon S3** : Stockage d'objets pour sauvegardes et fichiers*
- ***Amazon VPC** : Réseau privé virtuel et sécurité réseau*
- ***AWS Lambda** : Traitement serverless pour automatisations*

Services de sécurité :

- ***AWS IAM*** *: Gestion des identités et des accès*
- ***AWS KMS*** *: Gestion des clés de chiffrement*
- ***AWS CloudTrail*** *: Audit et traçabilité des actions*
- ***AWS GuardDuty*** *: Détection des menaces de sécurité*
- ***AWS Config*** *: Surveillance de la conformité*

Services de monitoring :

- ***AWS CloudWatch*** *: Monitoring et alertes*
- ***AWS X-Ray*** *: Traçage des requêtes applicatives*
- ***AWS Systems Manager*** *: Gestion et maintenance des instances*

Services de sauvegarde :

- ***AWS Backup*** *: Sauvegarde automatisée centralisée*
- ***Amazon EBS Snapshots*** *: Sauvegarde des volumes disques*
- ***Aurora Automated Backups*** *: Sauvegarde automatique des bases*

1.3 Localisation et transferts

Régions utilisées :

- ***Région principale :*** *EU-West-1 (Dublin, Irlande) - EU-West-3 (Paris, France)*
- ***Région de sauvegarde :*** *EU-West-1 (Dublin, Irlande) - EU-West-3 (Paris, France)*
- ***Aucune donnée*** *ne transite hors de l'Union Européenne*

Centres de données :

- ***Certifiés*** *ISO 27001, SOC 2 Type II*
- ***Redondance*** *géographique dans l'UE*
- ***Contrôle d'accès*** *physique renforcé*
- ***Surveillance*** *24h/24, 7j/7*

1.4 Catégories de données traitées

Données applicatives :

- ***Données d'identification*** *: Nom, prénom, email des utilisateurs*
- ***Données de pointage*** *: Horaires, présences, absences*
- ***Données de géolocalisation*** *: Coordonnées GPS des pointages*
- ***Données d'intervention*** *: Plannings, rapports, facturation*
- ***Données techniques*** *: Logs, métriques, configurations*

Métadonnées techniques :

- ***Logs système*** *: Connexions, erreurs, performances*
- ***Métriques*** *: Utilisation CPU, mémoire, réseau*
- ***Configuration*** *: Paramètres serveurs et applications*
- ***Sauvegardes*** *: Copies de sécurité des données*

1.5 Mesures de sécurité

Chiffrement :

- ***Au repos*** *: AES-256 avec AWS KMS*
- ***En transit*** *: TLS 1.2+ pour toutes les communications*
- ***Clés*** *: Gestion automatisée et rotation régulière*

Contrôle d'accès :

- ***IAM*** *: Authentification et autorisation granulaire*
- ***MFA*** *: Authentification multi-facteurs obligatoire*
- ***Audit*** *: Traçabilité complète via CloudTrail*

Sécurité réseau :

- ***VPC*** *: Isolation réseau dédiée*
- ***Security Groups*** *: Firewall applicatif*
- ***Network ACLs*** *: Filtrage au niveau sous-réseau*

Monitoring de sécurité :

- ***GuardDuty*** *: Détection automatique des menaces*
- ***Config*** *: Surveillance de la conformité*
- ***CloudWatch*** *: Alertes temps réel*

1.6 Certifications et conformité

Certifications obtenues :

- ***ISO 27001*** *: Management de la sécurité de l'information*
- ***ISO 27017*** *: Sécurité cloud computing*
- ***ISO 27018*** *: Protection des données personnelles dans le cloud*
- ***SOC 2 Type II*** *: Audit des contrôles de sécurité*
- ***CISPE*** *: Code de conduite pour la protection des données*

Conformité réglementaire :

- ***RGPD*** *: AWS Data Processing Agreement signé*
- ***Directive NIS*** *: Sécurité des réseaux et systèmes d'information*
- ***France*** *: Qualification SecNumCloud (en cours)*

1.7 Contrat et garanties

Contrat principal :

- ***AWS Customer Agreement*** *: Conditions générales*
- ***AWS Service Terms*** *: Conditions spécifiques par service*
- ***AWS Data Processing Agreement*** *: Clauses RGPD*

Garanties de service :

- ***Disponibilité*** *: 99.99% pour Aurora, 99.95% pour EC2*
- ***Durabilité*** *: 99.999999999% pour S3*
- ***Support*** *: 24h/24, 7j/7 selon plan choisi*
- ***Réversibilité*** *: Outils d'export des données*

Responsabilité :

- ***AWS*** *: Sécurité de l'infrastructure cloud*
- ***Client*** *: Sécurité dans le cloud (configuration, données)*
- ***Assurance*** *: Couverture des risques cyber*

1.8 Durée et évolution

Durée de la relation :

- ***Début*** *: 2009*
- ***Durée*** *: Indéterminée, résiliable à tout moment*
- ***Renouvellement*** *: Automatique par tacite reconduction*

Évolution des services :

- ***Nouveaux services*** *: Intégration selon besoins*
- ***Mises à jour*** *: Automatiques avec notification*
- ***Obsolescence*** *: Préavis de 12 mois minimum*

SOUS-TRAITANT N°2 - ACCESS SECURITY FIRST ASF

2.1 Identification du sous-traitant

Raison sociale : *ACCESS SECURITY FIRST ASF*
Adresse : *60 rue François 1er,*
Code postal : *75008*
Ville : *Paris*
Pays : *France*
SIRET : *93843466900017*
NAF : *8020Z*
Contact principal :
Nom : *Sandrine GARNIER*
Fonction : *resosnable ADV*
Téléphone : *0 189 708 221*
Email : *adv@asfirst.fr*

2.2 Services fournis

Installation et maintenance :

- ***Lecteurs de badges*** *: Installation, configuration, maintenance*
- ***Systèmes d'accès*** *: Contrôle d'accès physique aux locaux*
- ***Terminaux de pointage*** *: Équipements de gestion des temps*
- ***Matériels biométriques*** *: Lecteurs d'empreintes si applicable*
- ***Systèmes de surveillance*** *: Caméras et équipements de sécurité*

2.3 Localisation et interventions

Siège social : *Paris - France*
Zones d'intervention : *France*
Aucune donnée *ne sort du territoire français*
Lieux d'intervention :

- ***Locaux clients*** *: Installation et maintenance sur site*
- ***Ateliers ASF*** *: Réparation et configuration*
- ***Stockage*** *: Entrepôt sécurisé pour matériels*
- ***Pas de traitement*** *hors de France*

2.4 Catégories de données traitées

Données techniques :

- ***Configuration*** *: Paramètres des lecteurs*
- ***Maintenance*** *: Historique des interventions*
- ***Inventaire*** *: Matériels installés*

2.5 Finalités du traitement

Installation et configuration :

- ***Paramétrage*** *des lecteurs de badges*
- ***Test*** *des systèmes d'accès*
- ***Intégration*** *avec système de pointage*
- ***Validation*** *du fonctionnement*

Maintenance préventive :

- ***Vérification*** *périodique des équipements*
- ***Nettoyage*** *et calibrage*
- ***Mise à jour*** *des firmwares*
- ***Rapport*** *d'état des systèmes*

Maintenance corrective :

- ***Diagnostic*** *des pannes*
- ***Réparation*** *ou remplacement*
- ***Test*** *après intervention*
- ***Documentation*** *des actions*

2.6 Mesures de sécurité

Sécurité physique :

- ***Accès*** *limité aux techniciens habilités*
- ***Badge*** *d'identification pour interventions*
- ***Véhicules*** *sécurisés pour transport matériel*
- ***Outils*** *de chiffrement pour données sensibles*

Sécurité logique :

- ***Accès** aux systèmes par authentification*
- ***Logs** d'accès et d'actions*

Sécurité organisationnelle :

- ***Formation** du personnel à la confidentialité*
- ***Habilitation** des techniciens*
- ***Procédures** d'intervention documentées*

Gestion des données :

- ***Minimisation** : Seules données nécessaires*
- ***Effacement** : Suppression après intervention*
- ***Traçabilité** : Registre des actions*

GESTION DES CHANGEMENTS

3.1 Nouveau sous-traitant

Procédure d'ajout :

1. ***Évaluation** des besoins*
2. ***Recherche** et sélection*
3. ***Audit** de conformité*
4. ***Notification** au client*
5. ***Autorisation** écrite*
6. ***Contractualisation***
7. ***Mise à jour** de la liste*

Délais :

- ***Notification** : 30 jours avant*
- ***Réponse** client : 15 jours*
- ***Intégration** : Après accord*

3.2 Modification des services

Évolution des prestations :

- ***Analyse** de l'impact RGPD*
- ***Évaluation** des risques*
- ***Mise à jour** du contrat*
- ***Notification** au client*
- ***Validation** des mesures*

Nouveaux traitements :

- ***Finalités** définies*
- ***Catégories** de données*

- ***Mesures** de sécurité adaptées*
- ***Durée** de conservation*
- ***Autorisation** spécifique*

3.3 Cessation de la relation

Fin de contrat :

- ***Préavis** contractuel respecté*
- ***Restitution** des données*
- ***Destruction** des copies*
- ***Certificat** d'effacement*
- ***Transfert** si nouveau sous-traitant*

Procédure de sortie :

1. ***Notification** de fin de contrat*
2. ***Plan** de transfert/destruction*
3. ***Exécution** des opérations*
4. ***Vérification** de la conformité*
5. ***Attestation** finale*

SYNTHÈSE DES SOUS-TRAITANTS

Sous-traitant	***Services***	***Données traitées***	***Localisation***	***Certifications***
AWS	*Infrastructure cloud*	*Toutes données applicatives*	*EU (Paris/Dublin)*	*ISO 27001, SOC 2, CISPE*
ASF	*Matériels de pointage et d'accès*	*Données d'identification*	*France*	

Risques et mesures

Risque	***Probabilité***	***Impact***	***Mesures de mitigation***
Panne AWS	*Faible*	*Élevé*	*Redondance, backup, SLA*
Violation ASF	*Faible*	*Moyen*	*Audit, formation, contrat*
Transfert hors EU	*Très faible*	*Critique*	*Contrat, monitoring*

Cette liste est tenue à jour et communiquée au client à chaque modification. Tout nouveau sous-traitant fait l'objet d'une notification préalable et d'une autorisation écrite conformément au RGPD.

ANNEXE 5 : Guide d'exploitation des services de sécurité AWS

Dans un environnement AWS comprenant des instances EC2 et RDS, la surveillance active combine plusieurs services gérés (GuardDuty, Inspector, CloudWatch, CloudTrail, VPC Flow Logs) pour détecter et traiter les incidents de sécurité. Ce document décrit de manière exhaustive comment exploiter ces cinq briques, avec des procédures détaillées par scénario (incident réseau, vulnérabilité, alerte comportementale) et par périodicité (quotidien, hebdomadaire, mensuel), tout en respectant les exigences RGPD (chiffrement des logs, accès restreint, rétention limitée, etc.). Ce mode d'emploi s'adresse à un profil sécurité/compliance semi-fonctionnel et vise à rendre un nouvel employé totalement autonome.

Fonctionnement général

1.	Les données sont stockées dans Amazon S3 (fichiers texte, JSON, CSV, etc.)
2.	Vous définissez un **catalogue (via AWS Glue ou en ligne SQL)** : cela permet à Athena de "comprendre" la structure de vos données
3.	Vous exécutez des **requêtes SQL standard** pour filtrer, agréger, trier, croiser ces données

*Athena utilise en backend **Apache Presto / Trino**, un moteur de requêtes distribué très rapide et optimisé pour les analyses à grande échelle.*

Périodicité d'utilisation conseillée

Fréquence	Objectif
🕵️ Quotidien	Requêtes ponctuelles en cas d'alerte (ex. : une IP suspecte, une action critique)
🗓️ Hebdomadaire	Vérification ciblée des accès sensibles ou usage anormal des ressources
🗓️ Mensuel	Rapport d'audit RGPD, rapport de sécurité global, analyse des tendances

Bénéfices pour la conformité RGPD

Exigence RGPD	Fonctionnalité Athena associée
🔍 Traçabilité	Interroger l'historique des accès ou modifications
📁 Journalisation	Lire les logs sans les modifier
🔒 Confidentialité	Athena ne stocke pas les données, il les lit depuis S3
🗑️ Minimisation / Rétention	Requêtes filtrées sur une plage de date ; logs nettoyés à la source via lifecycle

Cas d'usage typiques

Cas	Exemple
🔎 **Analyse CloudTrail**	**Qui a démarré une instance EC2 le mois dernier ?**
🔒 **Sécurité RGPD**	**Quels utilisateurs ont modifié des permissions IAM ?**
🌐 **Réseau**	**Quelle IP a communiqué le plus avec nos serveurs ? (à partir des VPC Flow Logs)**
📜 **Reporting**	**Compter les appels API IAM par utilisateur et par jour**
📊 **Performance**	**Analyser les requêtes lentes sur RDS (si logs exportés dans S3)**

1. Présentation des outils AWS

- **Amazon GuardDuty –** Service de détection d'intrusion (threat detection). Il analyse en continu des sources de données AWS (journaux CloudTrail, flux VPC, logs DNS) pour repérer des comportements suspects (brute force, communication avec des C2, tentative d'escalade, etc.)aws.github.io. GuardDuty génère des *findings* détaillés (ressource affectée, type de menace, niveau de sévérité). Par exemple, la doc AWS indique que GuardDuty « surveille les logs AWS CloudTrail et les logs VPC Flow Logs pour détecter une activité malveillante » et crée des alertes détailléesaws.github.io. Les findings sont consultables dans la console GuardDuty, envoyés à Security Hub ou via EventBridge vers une file SNS/Lambda.

- **Amazon Inspector –** Service de gestion des vulnérabilités. Il découvre automatiquement les ressources (instances EC2, images conteneurs ECR, fonctions Lambda) et les analyse en continu pour détecter les failles logicielles et les expositions réseaudocs.aws.amazon.com. Contrairement aux scanners classiques, il n'exige pas de planification manuelle : « Amazon Inspector ne nécessite pas d'ordonnancement manuel des scans. Il découvre automatiquement vos ressources éligibles et continue de scanner votre environnement au fil des modifications (installation de nouveaux paquets, patchs, publication de nouveaux CVE)docs.aws.amazon.com ». Lorsqu'une vulnérabilité est détectée, Inspector crée un finding détaillé (gravité, ressource vulnérable, recommandation de remédiation). Ces findings sont accessibles dans la console ou via API, et peuvent être routés vers EventBridge/Security Hub.

- **Amazon CloudWatch (Métriques et Journaux)** – Service de surveillance des métriques, alarmes et logs. *Métriques* : CloudWatch collecte des métriques système des EC2 (CPU, disque, réseau), RDS (CPU, connexions, latence), ainsi que des métriques applicatives. On crée des alarmes CloudWatch pour déclencher des actions lorsque des seuils sont dépassés. Par exemple, la doc AWS note : « vous pouvez créer des alarmes qui surveillent des métriques et envoient des notifications ou effectuent automatiquement des modifications lorsque les seuils sont dépassés »docs.aws.amazon.com. Concrètement, on peut configurer une alarme CPU>80% (5 min) sur une instance EC2 ou RDS, qui notifie une équipe (SNS) ou déclenche une fonction Lambda pour isoler l'hôte.

Logs et CloudWatch Logs Insights : CloudWatch Logs centralise les journaux d'OS, d'applications ou AWS (par ex. logs RDS, logs de flux VPC). CloudWatch Logs Insights permet d'interroger ces logs avec un langage de requête puissant. Il est notamment utile pour diagnostiquer un incident : comme l'indique AWS, « CloudWatch Logs Insights permet de rechercher et analyser vos données de journaux pour répondre efficacement aux problèmes opérationnels »docs.aws.amazon.com. Par exemple, on peut publier les logs de requêtes lentes RDS vers CloudWatch Logs, puis exécuter une requête Insights pour détecter les requêtes les plus longuesdocs.aws.amazon.com.

- **AWS CloudTrail** – Service d'audit/API. CloudTrail enregistre l'historique complet des appels API effectués sur vos comptes AWS (console, CLI, SDK). Il fournit pour chaque événement l'utilisateur, l'adresse IP source, la date, l'action effectuée, etc. Comme le souligne AWS : « CloudTrail capture en continu les activités de votre compte AWS. Vous obtenez un historique des appels API, incluant quel utilisateur a fait quelle action, depuis quelle IP, et quand »docs.aws.amazon.com. Les logs CloudTrail (fichiers JSON) sont déposés dans un bucket S3. Pour la conformité RGPD, on recommande de configurer ce bucket avec des règles de cycle de vie (ex. purge après X mois) et de le chiffrer au repos (SSE-S3 ou SSE-KMS)docs.aws.amazon.comdocs.aws.amazon.com. Les logs CloudTrail permettent d'identifier toute opération administrative ou suspecte (ex. création d'un utilisateur IAM, modification de groupe de sécurité, etc.). De plus, CloudTrail peut émettre des événements CloudWatch Events : par exemple, on peut créer une règle CloudWatch qui déclenche une alerte email dès qu'une API EC2 spécifique est appelée, comme illustré dans l'architecture AWSdocs.aws.amazon.com.

- **VPC Flow Logs** – Journalisation du trafic réseau. VPC Flow Logs capture les flux IP (in/out) sur les interfaces réseau de votre VPC. Les logs de flux peuvent être envoyés vers CloudWatch Logs, S3 ou Kinesis Firehosedocs.aws.amazon.com. Selon AWS, VPC Flow Logs est utile « pour diagnostiquer des règles de sécurité trop restrictives, surveiller le trafic vers vos instances et déterminer la direction du trafic »docs.aws.amazon.com. Concrètement, on active Flow Logs sur les sous-réseaux ou sur l'interface d'une instance EC2. Ces logs permettent de vérifier, par exemple, qu'un serveur reçoit bien le trafic attendu, ou de détecter un pic inhabituel (scan, exfiltration). Des requêtes CloudWatch Logs Insights peuvent résumer ces flux (par source/destination, par protocole).

- **AWS Athena** est un service **d'interrogation de données (query) serverless** proposé par AWS. Il permet d'exécuter des **requêtes SQL directement sur des fichiers stockés dans Amazon S3**, sans avoir à déployer de base de données ni de serveur.

- **AWS Glue** est un **service d'intégration de données sans serveur (serverless)** conçu pour :
  - **Découvrir, cataloguer et préparer** automatiquement des données stockées sur AWS (notamment dans **Amazon S3**, mais aussi RDS, Redshift, etc.)
- Alimenter des analyses avec **Amazon Athena**, **Redshift**, ou des pipelines ETL (Extract-Transform-Load)
- *Objectif principal* : Centraliser les métadonnées de vos fichiers (CSV, JSON, logs, etc.) dans un **catalogue structuré**, qui permet ensuite d'effectuer des **requêtes SQL** ou des traitements automatiques sans configuration complexe.

2. Principes d'utilisation et procédures

2.1 Opération quotidienne et périodicité

- **Surveillance quotidienne :** Chaque jour, l'équipe sécurité doit vérifier les nouvelles alertes critiques. Cela inclut les findings *High* ou *Medium* de GuardDuty, les nouvelles vulnérabilités *High* d'Inspector, et les alarmes CloudWatch activées (par ex. CPU ou réseau). On consultera la console GuardDuty et le dashboard CloudWatch pour s'assurer qu'aucune alerte urgente n'est ignorée.

- **Surveillance hebdomadaire :** Une fois par semaine, examiner les rapports d'Inspector et purger les faux positifs de GuardDuty. Vérifier que toutes les alarmes CloudWatch sont pertinentes (ajuster les seuils si nécessaire) et valider la bonne collecte des logs.

- **Analyse mensuelle approfondie :** Chaque mois, réaliser un bilan complet :
  - Examiner les tendances (par ex. évolution mensuelle de l'utilisation CPU/RAM ou du trafic réseau) via les graphiques CloudWatch.
  - Exécuter des requêtes analytiques sur les logs historiques : par exemple, utiliser Amazon Athena pour interroger les logs CloudTrail archivés en S3 afin d'y repérer des anomalies de comportement sur le mois écoulé

docs.aws.amazon.com. Par exemple, on peut compter le nombre de créations d'utilisateurs IAM ou de modifications de sécurité par compte/IP.

- Relancer ou vérifier les scans de vulnérabilité d'Inspector et s'assurer que les corrections (patches, mises à jour) ont été appliquées.
- Générer un rapport de conformité (qui peut inclure des résultats de Security Hub, des scans CIS, etc.).
- Valider les cycles de vie S3 pour les logs (par ex. supprimer les logs plus anciens que la durée requise pour la conformité RGPD).

2.2 Procédure de gestion des alertes

2.2.1 Incident réseau (trafic anormal)

- **Détection :** Un incident réseau peut être détecté par une alarme CloudWatch (exemple : pics soudains sur la métrique « NetworkIn » d'une instance EC2 ou RDS), ou par un finding GuardDuty du type port scanning ou DDoS. On peut aussi le repérer en analysant les VPC Flow Logs (par ex. gros volume de trafic vers une IP non-routée).
- **Étapes de réponse :**
  1. **Collecte des informations :** Identifier l'instance concernée (via CloudWatch ou GuardDuty). Consulter les VPC Flow Logs associés, par exemple via une requête CloudWatch Logs Insights pour voir les connexions les plus volumineuses. Exemple de requête Insights pour lister les flux par volume :

SQL

```
stats sum(bytes) as bytesTransferred by srcAddr, dstAddr
sort bytesTransferred desc
limit 10
```

Cette requête (inspirée des exemples AWS docs.aws.amazon.com) permet de voir quels hôtes communiquent le plus.

  2. **Isolation :** Si l'instance est compromise, appliquer rapidement des mesures de confinement. Par exemple, désactiver les règles de sécurité entrantes (security group, NACL) ou déplacer l'instance dans un sous-réseau isolé. On peut également arrêter l'instance via AWS CLI ou console.
  3. **Analyse complémentaire :** Vérifier les logs CloudTrail pour tout événement lié (ex. modification récente de la configuration réseau,

arrêt/démarrage d'instance). Interroger CloudTrail pour les API suspectes, ex. :

SQL

```
SELECT useridentity.userName, eventName, sourceIPAddress, eventTime
FROM cloudtrail_logs
WHERE sourceIPAddress = 'X.X.X.X'
```

On peut créer une table Athena sur les logs CloudTrail et exécuter une telle requête pour identifier l'origine de la menacedocs.aws.amazon.com.

4. **Remédiation** : Bloquer définitivement l'attaque (par ex. bannir l'IP source au niveau du firewall ou WAF, appliquer un patch éventuel sur le service exposé, redémarrer avec une configuration sécurisée). Documenter l'incident (horodatage, impact, mesures prises).
5. **Revue post-incident** : Après résolution, faire un point avec l'équipe et ajuster la surveillance (ex. renforcer les alarmes, ajouter des règles GuardDuty ou AWS WAF si applicable).

2.2.2 Vulnérabilité logicielle

- **Détection** : Les vulnérabilités sont principalement détectées par Amazon Inspector. Par défaut, Inspector scanne régulièrement les instances EC2 et conteneurs via l'agent SSM. Lorsqu'une faille critique est trouvée, Inspector crée un finding précis (logiciel vulnérable, CVE, etc.).
- Étapes de réponse :
  1. **Examen du finding** : Dans la console Inspector, consulter la liste des findings classés par gravité. Pour chaque finding *High* ou *Medium*, lire la description (ressources affectées, CVE, solution suggérée).
  2. **Validation et application du correctif** : Vérifier que la vulnérabilité est toujours présente (ex. la version du paquet est toujours vulnérable). Appliquer le patch ou mettre à jour le paquet sur l'instance (via SSH/SSM Run Command). Par exemple, si un paquet système est obsolète, exécuter les commandes apt-get update && apt-get upgrade ou leur équivalent.
  3. **Vérification** : Relancer manuellement une analyse Inspector sur l'instance corrigée pour s'assurer que le finding a disparu. Si la vulnérabilité ne peut être corrigée immédiatement, envisager une mesure compensatoire (réduire les privilèges, filtre réseau, planification de migration, etc.).

4. **Automatisation/Rapports** : Noter la clôture des findings dans un rapport de sécurité. On peut aussi configurer EventBridge pour déclencher une alerte (SNS) à chaque finding critique d'Inspector, et ainsi notifier l'équipe de sécurité en temps réel.

- **Périodicité** : Inspector fonctionne en continu, mais il est recommandé de programmer une revue globale mensuelle des findings (en cohérence avec les cycles de patch mensuels) pour s'assurer qu'aucune faille n'a été ignorée.

2.2.3 Alerte comportementale (activation suspecte)

- **Détection** : Les alertes comportementales viennent souvent de GuardDuty (ex. activité anormale d'un utilisateur IAM, accès RDS inhabituel) ou d'une règle CloudTrail personnalisée. Par exemple, un finding GuardDuty de type *UnauthorizedAccess* ou *Recon: EC2/PortProbe* signale un comportement atypique. GuardDuty peut aussi détecter des connexions anormales à Amazon Auroraaws.github.io (utile pour RDS).
- Étapes de réponse :
    1. **Identification** : Analyser le finding GuardDuty pour extraire les détails (ressource, utilisateur, adresse IP, date). Par exemple, si GuardDuty signale un accès suspect à l'API IAM, on peut prendre la userIdentity du finding.
    2. **Requête de logs** : Utiliser CloudTrail pour tracer l'action. Par exemple, lancer une requête Athena ou Logs Insights sur les events CloudTrail pour cette période. Exemples de requêtes :
        - Dans Athena (sur les tables CloudTrail) :

SQL

```
SELECT eventtime, useridentity.username, eventname, sourceipaddress
FROM cloudtrail_logs
WHERE sourceipaddress = '1.2.3.4'
ORDER BY eventtime DESC;
```

Dans CloudWatch Logs Insights (si CloudTrail envoie ses logs à CloudWatch) **:**

SQL

```
fields @timestamp, userIdentity.userName, eventName, sourceIPAddress
| filter sourceIPAddress = "1.2.3.4"
| sort @timestamp desc
```

3. Ces requêtes (inspirées des exemples AWSdocs.aws.amazon.com) permettent de comprendre quelle action a été réalisée.
4. **Confinement** : Si un compte utilisateur a été compromis ou agi de manière malveillante, immédiatement révoquer ou désactiver les clés ou sessions concernées. Ex. : changer le mot de passe de l'utilisateur IAM, désactiver l'utilisateur, révoquer les tokens, ou mettre en quarantaine la machine source.
5. **Notification et remontée** : Informer l'équipe de sécurité et la hiérarchie si nécessaire (selon la politique). Si la tentative provient d'un acteur interne, l'équipe conformité peut être impliquée.
6. **False positive** : Si l'alerte est bénigne (ex. scanner de vulnérabilité légitime déclenché par GuardDuty), marquer le finding comme *suppressed* ou l'ignorer avec justification pour réduire le bruit.

- **Périodicité** : Les alertes comportementales sont traitées en temps réel/daily. On revoit mensuellement la liste des findings passés pour identifier les patterns (ex. un utilisateur tentant fréquemment des actions non autorisées).

3. Exemples de requêtes d'investigation
Pour appuyer les enquêtes, voici quelques requêtes types :

- CloudWatch Logs Insights (flux VPC) – Lister les flux par volume d'octets :

SQL

```
stats sum(bytes) as bytesTransferred by srcAddr, dstAddr
sort bytesTransferred desc  limit 10
```

Cette requête (issue des exemples AWSdocs.aws.amazon.com) affiche les dix communications ayant transféré le plus d'octets, par adresse source et destination. Elle aide à repérer rapidement des exfiltrations ou scans intensifs.

- CloudWatch Logs Insights (logs RDS/MySQL) – Exemple pour identifier les requêtes lentes dans les logs MySQL (à condition que slow_query_log soit activé et exporté) :

SQL

```
fields @message, @timestamp
filter @message like /Query_time/
parse @message "* Query_time: *" as exec_time
```

```
filter exec_time > 1
sort exec_time desc
limit 10
```

Cette requête extrait les requêtes dont le temps d'exécution dépasse 1 seconde, utile pour optimiser la base de données.

- Amazon Athena (CloudTrail) – Exemple pour lister les appels API par utilisateur :

SQL

```
SELECT useridentity.userName, eventName, sourceIPAddress, eventTime
FROM cloudtrail_logs
WHERE eventName LIKE 'StartInstances'
 AND eventTime BETWEEN date '2025-07-01' AND date '2025-07-31'
ORDER BY eventTime;
```

Cette requête (structure exemplaire du guide AWSdocs.aws.amazon.com) renvoie les utilisateurs ayant démarré des instances EC2 durant juillet 2025. On peut modifier le filtre pour tout autre évènement ou plage horaire.

- Amazon Athena (CloudTrail) – Exemple de requête pour détecter des connexions TLS obsolètes aux services AWS :

SQL

```
SELECT eventSource, eventName, sourceIPAddress, tlsDetails.tlsVersion, COUNT(*) as
count
FROM cloudtrail_logs
WHERE tlsDetails.tlsVersion IN ('TLSv1','TLSv1.1')
GROUP BY eventSource, eventName, sourceIPAddress, tlsDetails.tlsVersion;
```

Cette requête (inspirée des exemples AWS docs.aws.amazon.com) identifie les appels utilisant TLS 1.0 ou 1.1, ce qui peut être requis pour la conformité ou la sécurité. Chaque requête doit être adaptée à vos log groups et tables Athena configurées. Les résultats serviront à orienter la réponse (ex. identifier l'IP externe malveillante, l'utilisateur fautif, etc.).

4. Bonne pratique de conformité (RGPD)

- **Chiffrement et rétention des logs** : Les journaux peuvent contenir des données personnelles (ex. adresses IP, identifiants d'utilisateur). Il est essentiel de les protéger. Par défaut, AWS CloudTrail chiffre ses logs avec SSE-S3 docs.aws.amazon.com. Pour renforcer, on peut choisir SSE-KMS et attacher une politique KMS restreignant le déchiffrement aux rôles sécurité. De même, chiffrer les buckets CloudWatch Logs destinés à des données sensibles. AWS recommande explicitement de stocker les logs (notamment CloudTrail) dans des buckets S3 chiffrés et en accès restreintdocs.aws.amazon.com.
- **Accès et journalisation** : Limiter l'accès aux consoles CloudWatch/CloudTrail aux seuls administrateurs sécurité. Utiliser IAM et MFA pour tout accès à ces outilsdocs.aws.amazon.com. Activer la validation d'intégrité des fichiers CloudTrail pour détecter toute altérationdocs.aws.amazon.comdocs.aws.amazon.com.
- **Cycle de vie des données** : Mettre en place des règles de cycle de vie S3 pour purger les logs au-delà de la durée nécessaire. Par exemple, conserver seulement 90 jours de logs opérationnels si cela suffit pour la conformité, puis archiver ou supprimer le reste. AWS permet de définir ces lifecycles pour S3docs.aws.amazon.com.
- **Minimisation** : Ne pas envoyer de données utilisateurs (containing des PII) dans les métadonnées ou les logs personnalisés si possibledocs.aws.amazon.com. Par exemple, éviter de logguer l'adresse email complète d'un client dans CloudWatch.
- **Audits réguliers** : En complément de la surveillance technique, réaliser des audits mensuels de configuration (vérifier que CloudTrail est actif sur tous les comptes/régions, que les règles Flow Logs couvrent tous les VPC importants, etc.). Mettre à jour la documentation et les procédures suite à tout changement réglementaire ou infrastructurel.

5. Conclusion

Ce guide fournit un mode opératoire complet pour exploiter GuardDuty, Inspector, CloudWatch (métriques et logs), CloudTrail et VPC Flow Logs dans un contexte EC2/RDS. Pour chaque type d'alerte (réseau, vulnérabilité, comportement) et chaque période (quotidienne, mensuelle), il détaille les actions à entreprendre étape par étape, et présente des exemples de requêtes analytiques (Athena, CloudWatch Logs Insights) pour investiguer les incidents. Les bonnes pratiques RGPD – chiffrement, gestion des accès et cycles de vie – sont intégrées pour garantir la conformité. En suivant ces instructions et en adaptant les exemples proposés, un nouvel employé pourra assurer

en toute autonomie la sécurité et la conformité de la plateforme AWS, tout en répondant efficacement à tout incident.

ANNEXE 6 : POLITIQUE DE SÉCURITÉ SSH

1. Objectif

Cette politique a pour objectif de définir les règles de sécurité liées à l'accès SSH aux serveurs EC2 et Linux dans le cadre des opérations techniques internes ou externalisées. Elle vise à garantir la traçabilité, la confidentialité et l'intégrité des systèmes accessibles par SSH.

2. Authentification

- L'utilisation des clés SSH personnelles est **obligatoire**. Aucune authentification par mot de passe ne doit être activée.
- Chaque utilisateur doit disposer de **sa propre paire de clés SSH**, non partagée.
- Les clés doivent être **protégées par une passphrase**.
- La **rotation des clés** est effectuée tous les **6 mois**, ou immédiatement en cas de départ d'un collaborateur ou d'incident de sécurité.

3. Accès au travers d'un canal sécurisé

- L'accès SSH aux ressources sensibles (prod, base de données, réseaux internes) doit être **protégé par un VPN** ou via un **bastion host (jump server)**.
- L'accès direct depuis Internet est **strictement interdit**, sauf cas documenté et validé par le RSSI.

4. Journalisation & traçabilité

- Toute activité SSH doit être journalisée :
  - Soit via CloudTrail (pour EC2 AWS),
  - Soit via un agent local tel que auditd, Wazuh, OSSEC ou autre EDR.
- Les logs doivent être conservés **au minimum 1 an**, de manière **chiffrée et centralisée**.

5. Processus de gestion des accès

- Les accès doivent être **revus tous les trimestres**.
- Les clés des utilisateurs quittant l'entreprise doivent être **révoquées immédiatement**.
- Toute demande d'accès doit être formalisée, justifiée et validée par le manager et le RSSI.

6. Surveillance

- Une alerte CloudWatch ou GuardDuty doit être configurée pour :
  - Détection d'accès SSH depuis IP non autorisée,
  - Taux d'échec d'authentification élevé,
  - Connexion en dehors des horaires usuels.

7. Conformité et audit

- Cette politique est auditée annuellement.
- Toute non-conformité est consignée dans un registre de suivi et fait l'objet d'un plan de correction.

Manuel opérationnel : mode d'emploi pas à pas

J - Manuel de surveillance au quotidien (15 Mn)

Mode d'emploi - Surveillance quotidienne de la sécurité AWS (pour nouvel arrivant)

Temps estimé de la routine : 15 minutes
Responsable : Analyste sécurité ou référent conformité
Remonter tout comportement anormal à : SJH/AWI/ADN

***Objectif** : Ce guide pas-à-pas a pour but de permettre à un salarié nouvellement intégré de vérifier chaque jour, de manière systématique, les alertes de sécurité critiques dans l'infrastructure AWS. Il couvre GuardDuty, Inspector et CloudWatch.*

1. Vérification des alertes AWS GuardDuty

Objectif : Identifier les comportements suspects ou malveillants détectés par GuardDuty

➔ **Étapes à suivre :**
1. Se connecter à la console AWS : https://console.aws.amazon.com/
2. Dans la barre de recherche du haut, taper "GuardDuty" et cliquer sur le résultat correspondant.
3. Vous arrivez dans le Tableau de bord GuardDuty**.**

⚠ **Indicateurs à surveiller :**
- À gauche, cliquer sur "Findings / Resultats".
- Trier les findings par "Severity / Gravité" (cliquez sur l'entête de colonne).
- Lire uniquement les alertes "High" ou "Medium" datant de moins de 24h (colonne "Last Seen").

✉ **Que faire si une alerte est trouvée ?**
- Cliquer sur la ligne pour voir les détails (source IP, compte, type d'attaque).
- Prendre une capture d'écran et noter : type d'alerte, ressource impactée, action recommandée.
- Notifier l'équipe sécurité interne.

2. Vérification des vulnérabilités avec AWS Inspector

Objectif : Détecter les failles de sécurité sur les instances EC2 (ou conteneurs)

➔ **Étapes à suivre :**

1. Depuis la console AWS, rechercher "Inspector" dans la barre du haut.
2. Cliquer sur le service Amazon Inspector.
3. Accéder à la section "Findings / Resultats " (menu gauche).

⚠ **Indicateurs à surveiller :**

- Utiliser le filtre " Findings Status: Active" et "Severity: High / Critical".
- Lire les colonnes : "CVE ID – colonne titre", "Affected Resource / Ressource affectée", "Last Updated / Age".

✉ **Que faire si une faille est détectée ?**

- Cliquer sur le finding / Resultats pour voir les détails.
- Copier le CVE ID (ex : CVE-2018-8013) et chercher sur https://cve.mitre.org/
- Noter le paquet concerné, la version, et la recommandation.
- Informer l'équipe technique pour patch ou correctif.

Exemple d'analyse sur le site https://cve.mitre.org :
CVE-2018-8013
CNA : Fondation Apache Software
Dans Apache Batik 1.x avant 1.10, lors de la désérialisation d'une sous-classe de « AbstractDocument », la classe prenait une chaîne de l'inputStream comme nom de classe, puis l'utilisait pour appeler le constructeur sans argument de la classe. La correction consistait à vérifier le type de classe avant d'appeler newInstance lors de la désérialisation.

3. Vérification des alarmes CloudWatch

Objectif : Détecter un comportement anormal (CPU, RAM, latence, etc.)

➔ Étapes à suivre :

1. Depuis la console AWS, rechercher "CloudWatch".
2. Aller dans "Alarms" > "All alarms".
3. Option à choisir

Champ	Option à sélectionner	Pourquoi
État de l'alarme	***En alarme*** uniquement	Ne montrer que les alertes actives et urgentes
Type d'alarme	***Toutes*** ou ***Standard*** (par défaut)	Garde toutes les sources (CPU, disque, réseau…)
Statut des actions	***Toutes*** (laisser comme tel)	Permet de voir même les alarmes sans action automatique

⚠ **Indicateurs à surveiller :**

- Regarder la colonne "Alarm Name / Nom", "Metric / nom de la métrique" et "Threshold / Dimensions".
- Noter si une alarme concerne une instance EC2 ou base RDS critique.

✉ **Que faire si une alarme est active ?**

- Cliquer sur l'alarme pour afficher le graphe détaillé.
- Noter l'heure du pic, la ressource concernée, et l'action déclenchée.
- Avertir l'équipe exploitation si besoin de redémarrage, optimisation ou scaling.

Checklist journalière à cocher :

- [ ] Aucune alerte GuardDuty High/Medium active
- [ ] Aucune vulnérabilité High active dans Inspector
- [ ] Aucune alarme critique active dans CloudWatch
- [ ] Rapport journalier envoyé (capture + synthèse)

H - Manuel de surveillance hebdomadaire (45 Mn)

Temps estimé de la routine : 45 minutes
Responsable : Analyste sécurité ou référent conformité
Remonter tout comportement anormal à : SJH/AWI/ADN

Étape	Temps estimé
🧪 Examiner les rapports d'AWS Inspector (vulnérabilités critiques actives)	10 à 15 min
🧹 Purger les faux positifs dans GuardDuty	10 min
🔔 Vérifier la pertinence des alarmes CloudWatch (état, seuils, actions)	10 à 15 min
📦 Valider la bonne collecte des logs (CloudTrail, VPC, envois vers S3/CloudWatch)	10 min
🧮 Total estimé (hors correctifs)	~45 min

Examiner les rapports Amazon Inspector

1. **Connexion et navigation :** Connectez-vous à la console AWS et ouvrez le service **Amazon Inspector**docs.aws.amazon.com. Dans le panneau de gauche, sélectionnez **Dashboard** (optionnel pour un aperçu des vulnérabilités critiques) ou **Findings**docs.aws.amazon.com.

2. **Consulter les findings :** La page *Findings* affiche toutes les vulnérabilités actives dans un tableaudocs.aws.amazon.com. Repérez les nouvelles vulnérabilités, en filtrant éventuellement par sévérité (critique/haute). Pour chaque entrée intéressante, cliquez sur son nom pour voir les détails (ressource impactée, description, recommandation)docs.aws.amazon.com.

3. **Action sur les résultats :** Notez ou exportez les résultats si nécessaire (par exemple, télécharger en CSV via un filtre ou un rapport). Conservez les informations pour traitement ou pour remonter les vulnérabilités critiques aux

équipes concernées. (Aucun processus d'archivage automatique ne ferme les findings, ils restent jusqu'à remédiation.)

Purger les faux positifs de GuardDuty

1. **Ouverture de GuardDuty :** Dans la console AWS, ouvrez **Amazon GuardDuty**docs.aws.amazon.com. Dans le menu de gauche, cliquez sur **Findings / Résultats** docs.aws.amazon.com pour afficher toutes les alertes détectées. Par défaut, la liste est triée par date (Last seen) avec les événements récents en haut.

2. **Identifier les faux positifs :** Parcourez la liste pour repérer les faux positifs éventuels. GuardDuty marque les faux positifs en mettant le champ **Confidence** à 0 docs.aws.amazon.com. Vous pouvez filtrer le tableau par attributs (par exemple Confidence = 0) pour les repérer rapidement.

3. **Archiver ou supprimer :** Pour chaque faux positif identifié, ouvrez l'alerte (cliquer sur le titre) et choisissez **Archive finding** dans le menu *Actions* (cela peut nécessiter la console Amazon Detective, selon votre configuration)docs.aws.amazon.com. Cela retire l'alerte de la vue active (son statut devient *Archived*).

4. **Règles de suppression (facultatif) :** Si certains faux positifs reviennent régulièrement, créez une *suppression rule* dans GuardDuty pour les archiver automatiquement à l'avenir docs.aws.amazon.com. Ces règles filtrent les alerts "inutile" en les archivant dès leur création.

Vérifier et ajuster les alarmes CloudWatch

1. **Lister les alarmes :** Dans la console AWS, ouvrez **Amazon CloudWatch** puis dans le menu de gauche sélectionnez **Alarms > All alarms**. Vous verrez la liste de toutes les alarmes configurées. Trier ou filtrer selon l'**état** (OK, ALARM, INSUFFICIENT_DATA) pour cibler celles à vérifier en priorité.

2. **Examiner chaque alarme :** Pour chaque alarme, vérifiez le **métrique surveillé**, la **période** et le **seuil** définis. Comparez le seuil à des valeurs normales du métrique. Les bonnes pratiques recommandent de fixer les seuils en s'appuyant sur l'analyse des données historiques (« baselines »)awsforengineers.com. Par

exemple, si la charge CPU moyenne est 50%, ne mettez pas le seuil d'alarme à 51% sans raison : fixez-le légèrement au-dessus d'un pic normal pour éviter les fausses alertes.

3. **Ajuster si nécessaire :** Si une alarme déclenche trop fréquemment (bruit), éditez-la pour augmenter le seuil ou le nombre de périodes requises. À l'inverse, si une alarme importante ne déclenche pas même en cas de problème, baissez son seuil. Pour modifier une alarme, dans la console **CloudWatch Alarms** sélectionnez-la puis cliquez sur **Edit**, puis ajustez les paramètres (statistique, période, nombre de points, seuil, etc.).

4. **Supprimer ou désactiver :** Si une alarme n'est plus pertinente (ressource obsolète, métrique non critique, etc.), supprimez-la ou désactivez-la pour réduire le bruit. L'objectif est que chaque alarme restante soit justifiée. En résumé, gardez l'équilibre entre sensibilité et alertes inutilesawsforengineers.com. Les alarms efficaces sont celles qui détectent les réels problèmes sans « fatigue d'alerte »awsforengineers.comawsforengineers.com.

Valider la collecte des logs

1. **CloudTrail (événements de gestion) :** Ouvrez le service **AWS CloudTrail** dans la console. Allez dans **Event history** pour voir les derniers événements d'API (jusqu'à 90 jours)docs.aws.amazon.com. Vérifiez que des événements récents (par exemple des connexions, création de ressources) apparaissent. Si l'historique est vide ou incomplet, assurez-vous qu'un *trail* est bien actif (logging vers un bucket S3 ou vers CloudWatch Logs).

2. **Logs d'application et système :** Dans **CloudWatch Logs**, parcourez les *Log groups* existants (ex. pour EC2, Lambda, ECS, RDS, etc.). Ouvrez quelques log streams récents pour confirmer que des entrées de logs y sont bien écrites (timestamp récent). Si un *Log group* critique est vide ou absent, le module d'envoi de logs (par ex. CloudWatch Agent, EKS control plane logging) peut être mal configuré.

3. **VPC Flow Logs :** Dans la console **VPC**, consultez **VPC > Flow Logs** pour chaque VPC ou sous-réseau. Vérifiez que les flux de logs sont activés et que la

destination (CloudWatch Logs ou S3) reçoit des données. En effet, les enregistrements de VPC Flow Logs sont alors accessibles dans le groupe de logs CloudWatch ou dans le bucket S3 configurédocs.aws.amazon.com. Confirmez la présence de fichiers ou d'événements récents dans la destination.

4. **Autres sources de logs :** Si vous collectez d'autres logs (ex. AWS Config, WAF, Application Load Balancer, etc.), vérifiez également leurs destinations respectives (groupes CloudWatch ou buckets). En pratique, on s'assure chaque semaine que chaque pipeline de logs critique continue de livrer des données récentes.

Bonnes pratiques d'analyse métier

- **Aligner sur les indicateurs clés (KPIs) :** Identifiez les objectifs métier prioritaires (par exemple volume de ventes, temps de réponse client, taux d'erreur) et reliez-les aux métriques surveilléesaws-observability.github.io. Par exemple, un site e-commerce suivra ses transactions et taux de conversion, pas seulement l'utilisation CPU.

- **Corréler métriques techniques et business :** Assurez-vous que les métriques opérationnelles (latence, CPU, erreurs applicatives, etc.) sont pertinentes pour le business. Par exemple, une forte charge CPU qui dégrade la réponse utilisateur peut affecter la satisfaction clientaws-observability.github.io. Stockez et superposez vos métriques métiers et techniques pour comprendre leur impact conjoint sur les objectifs.

- **Connaître la « norme » :** Déterminez ce qui est *normal* pour votre système. Établissez des baselines (historique, tests de charge) afin de reconnaître rapidement les déviations. Comme le recommandent les bonnes pratiques, définissez vos seuils d'alerte juste au-dessus de vos valeurs normalesawsforengineers.com. Si le comportement attendu change (nouveau trafic, saisonnalité), ajustez les seuils en conséquence.

- **Éviter la surcharge d'alertes** : Un bon système de surveillance trouve l'équilibre entre sensibilité et bruitawsforengineers.comawsforengineers.com. Révisez régulièrement vos alarmes et supprimez celles qui sont redondantes ou peu

pertinentes. Pour les incidents réels, veillez à définir une procédure claire (reporting, plan d'action).

- **Amélioration continue :** Analysez les tendances sur plusieurs semaines. Utilisez, si possible, des outils de détection d'anomalies ou d'analyse prédictive pour affiner les alertesaws-observability.github.io. Documentez vos analyses et partagez les enseignements avec les équipes métier (par exemple en mettant à jour les KPIs surveillés ou les réponses opérationnelles).

Sources : Procédures et recommandations AWS pour Amazon Inspectordocs.aws.amazon.comdocs.aws.amazon.com, Amazon GuardDutydocs.aws.amazon.comdocs.aws.amazon.com, suppression de faux positifsdocs.aws.amazon.com, archivage des findingsdocs.aws.amazon.com, meilleurs usages des alarmes CloudWatchawsforengineers.comawsforengineers.com, validation de la collecte CloudTraildocs.aws.amazon.com, VPC Flow Logsdocs.aws.amazon.com, et bonnes pratiques d'observabilité AWSaws-observability.github.ioaws-observability.github.ioaws-observability.github.io.

M - Manuel de l'analyse mensuelle approfondie (1h30)

Temps estimé de la routine : 1h30 minutes
Responsable : Analyste sécurité ou référent conformité
Remonter tout comportement anormal à : SJH/AWI/ADN

Étape	Temps estimé
📊 Examiner les tendances CPU/RAM/trafic via CloudWatch	15 à 20 min
🔎 Exécuter les requêtes Athena sur logs CloudTrail	20 à 30 min
🛡️ Vérifier les scans Inspector et état des correctifs	15 à 25 min
📋 Générer et consolider un rapport de conformité (Security Hub)	20 à 30 min
🗂️ Vérifier les cycles de vie S3 (RGPD)	10 à 15 min
🧮 **Total estimé (hors remédiation technique)**	**~1h30 max**

Chaque mois, un suivi systématique permet de vérifier l'état de sécurité et de conformité de votre environnement AWS. Le manuel suivant détaille, étape par étape via la console AWS, les principales vérifications à effectuer :
1) analyser les tendances métriques avec CloudWatch,
2) interroger les logs historiques avec Amazon Athena (CloudTrail),
3) vérifier les scans de vulnérabilité avec Amazon Inspector,
4) générer un rapport de conformité (Security Hub, CIS, etc.), et
5) valider les règles de cycle de vie S3 pour les logs.

Examiner les tendances mensuelles (CloudWatch)
Pour repérer toute anomalie d'utilisation (CPU, mémoire, trafic réseau), exploitez les graphiques de CloudWatch en ajustant la période sur 30 jours. CloudWatch conserve les données métriques jusqu'à 15 mois docs.aws.amazon.com, ce qui permet de visualiser facilement l'évolution mensuelle.

- **Accéder à CloudWatch.** Ouvrez la console AWS et choisissez **CloudWatch** (rubrique Surveillance). Dans le volet de navigation, sélectionnez **Métriques**.
- **Sélectionner les métriques pertinentes.** Par exemple, sous *EC2* > *Par instance*, cochez la métrique CPUUtilization pour votre instance. De même, sélectionnez NetworkIn et NetworkOut pour le trafic réseau. Pour la mémoire ou le disque, si vous avez installé l'agent CloudWatch, cherchez les métriques MemoryUtilization ou DiskReadOps.

- **Configurer l'intervalle de temps.** En haut à droite du graphique, choisissez un intervalle de 30 jours (ou la période précise du dernier mois). Vous pouvez aussi cliquer sur l'icône de calendrier pour définir manuellement la plage (par exemple du 1er au 30 du mois écoulé). Les graphiques afficheront alors la tendance mensuelle.
- **Analyser les graphiques.** Observez si des pics ou des creux inhabituels apparaissent (par ex. forte augmentation de CPU le soir). Vous pouvez ajouter d'autres métriques ou comparer plusieurs courbes sur le même graphique. L'outil **CloudWatch Metrics Insights** permet également d'identifier des tendances par requêtes SQL sur les métriquesdocs.aws.amazon.com si besoin d'analyses plus avancées.
- **Créer un tableau de bord (facultatif).** Pour gagner du temps, créez un **Dashboard** dans CloudWatch (rubrique *Tableaux de bord*) comportant des widgets pour CPU, RAM et trafic. Vous pourrez y consulter rapidement chaque mois les mêmes graphiques.

En suivant ces étapes, vous disposerez d'un aperçu clair de l'utilisation CPU/RAM et du trafic réseau au cours du mois écoulé. Cela facilite la détection de dérives ou de comportements anormaux (p.ex. une hausse inattendue du trafic).

Analyser les logs historiques avec Amazon Athena (CloudTrail)

Amazon Athena permet d'exécuter des requêtes SQL sur les logs CloudTrail archivés dans S3. Grâce à Athena, on peut compter, par exemple, les créations d'utilisateurs IAM ou les modifications de sécurité par compte ou par IP sur le mois écoulé. La documentation AWS montre comment lancer de telles requêtes sur les logs CloudTraildocs.aws.amazon.com. Voici comment procéder :

1. **Vérifier les logs CloudTrail en S3.** Assurez-vous que vos journaux CloudTrail du mois écoulé sont bien archivés dans un bucket S3. Notez le préfixe ou le chemin d'accès (p.ex. s3://votre-bucket-logs/AWSLogs/...).
2. **Ouvrir Amazon Athena.** Dans la console AWS, sous **Analytics**, cliquez sur **Athena**. Sélectionnez la région appropriée (la même que vos logs).
3. **Créer/valider la table CloudTrail.** Dans Athena, vérifiez que vous avez une table pointant sur vos logs CloudTrail. Si ce n'est pas le cas, utilisez l'assistant de création de table ou exécutez la commande recommandée dans la documentation CloudTrail pour créer une table externe (en précisant le chemin S3 des logs et le schéma JSON). Par exemple, depuis la console CloudTrail vous pouvez générer automatiquement une table Athena partitionnée.

4. **Lancer des requêtes SQL.** Dans Le Sous-traitant-éditeur de requêtes Athena, écrivez et exécutez des requêtes SQL sur la table de logs. Voici deux exemples de requêtes que vous pouvez adapter au besoin :
    - *Compter les créations d'utilisateurs IAM par compte :*

SQL

```
SELECT
 userIdentity.accountId AS Compte,
 COUNT(*) AS NbCreations
FROM cloudtrail_logs
WHERE eventName = 'CreateUser'
 AND eventTime >= date '2025-06-01'
 AND eventTime <  date '2025-07-01'
GROUP BY userIdentity.accountId;
```

Cette requête compte le nombre d'événements CreateUser (création d'utilisateur IAM) par compte AWS pour le mois de juin 2025. Adaptez les dates au mois analysé.

- *Compter les modifications de sécurité par adresse IP :*

SQL

```
SELECT
 sourceIPAddress AS IP,
 COUNT(*) AS NbModifs
FROM cloudtrail_logs
WHERE eventName IN ('AuthorizeSecurityGroupIngress',
'AuthorizeSecurityGroupEgress')
 AND eventTime >= date '2025-06-01'
 AND eventTime <  date '2025-07-01'
GROUP BY sourceIPAddress;
```

Cet exemple compte les événements de modification des règles de sécurité (ajout de règles sur des groupes de sécurité) par adresse IP source. Vous pouvez ajuster la liste des eventName selon les actions de sécurité qui vous intéressent (p.ex. AttachRolePolicy, PutUserPolicy, etc.).

5. Après exécution, Athena affiche les résultats en colonne. Repérez les comptes ou IP avec des comptes élevés : cela peut indiquer un changement ou une

anomalie. Les résultats peuvent être téléchargés au format CSV pour documentation ou analyse ultérieure.

En résumé, Athena rend possible l'interrogation directe de vos logs CloudTrail pour repérer des anomalies mensuelles. Les exemples ci-dessus illustrent comment formuler des requêtes simples (AWS fournit aussi des exemples de basedocs.aws.amazon.com). Adaptez-les selon vos besoins pour surveiller d'autres actions (suppression d'utilisateurs, modifications IAM, etc.).

Vérifier les scans de vulnérabilité Amazon Inspector

Amazon Inspector analyse en continu vos ressources (instances EC2, images conteneurs, fonctions Lambda) pour détecter des vulnérabilités. Voici comment relancer ou vérifier ces scans chaque mois :

- **Accéder à Amazon Inspector.** Dans la console AWS, sous **Sécurité, identités et conformité**, ouvrez **Amazon Inspector**. Sélectionnez la région concernée. Si vous n'avez pas encore activé Inspector, cliquez sur **Activate** (il créera un rôle nécessaire en tâche de fond). Une fois actif, Inspector commence automatiquement à scanner vos ressources.
- **Consulter le Tableau de bord Inspector.** Dans la console, sélectionnez **Dashboard** (Tableau de bord). Vous y verrez un aperçu de la couverture de scan et des résultats critiquesdocs.aws.amazon.comdocs.aws.amazon.com. Par exemple, la section *Constatations critiques* présente le nombre de vulnérabilités critiques trouvées dans votre environnementdocs.aws.amazon.com. Cliquez sur ces chiffres pour accéder aux détails.
- **Lister les vulnérabilités et appliquer les correctifs.** Dans le tableau de bord ou dans **Findings** (Résultats), affichez les vulnérabilités trouvées ce mois-ci. Triez par gravité (Critical, High) et notez les ressources (instances, images) affectées. Pour chaque vulnérabilité critique, identifiez le correctif à appliquer (mise à jour du paquet logiciel, patch OS, etc.) sur l'instance concernée.
- **Relancer un scan (si nécessaire).** Après application des correctifs, vous pouvez lancer un scan de vérification. Dans Inspector, sous **Scan** > **On-demand scans** > **CIS scans**, créez ou sélectionnez une configuration de scan CIS (benchmark CIS AWS Foundations) et exécutez-la. Vous pouvez aussi lancer manuellement un scan sur une ressource spécifique si besoin. Par défaut, Inspector relance automatiquement le scan lorsqu'un patch est installé ou lorsqu'un nouveau CVE est publiéaws.amazon.com. Ainsi, après la mise à jour d'une instance, Inspector devrait la rescanner automatiquement pour confirmer la correction.
- **Vérifier les résultats CIS (CIS AWS Foundations).** Sous **On-demand scans** > **CIS scans**, cliquez sur l'onglet *Scan results*. Sélectionnez le scan récent pour voir quels contrôles CIS ont échoué ou passé. Cela montre votre conformité aux

meilleures pratiques CIS. Les résultats peuvent être exportés en CSV via la console si nécessaire.

En suivant ces étapes, vous actualisez le statut de sécurité de vos ressources. Le tableau de bord Inspector (couverture et vulnérabilités critiques) aide à cibler rapidement les prioritésdocs.aws.amazon.com. Amazon Inspector indique également les paquets les plus vulnérables et les comptes les plus exposés. Après remédiation, assurez-vous que plus aucun résultat critique ne subsiste (les scans automatiques d'Inspector vérifient ce pointaws.amazon.com).

Générer le rapport de conformité (Security Hub, CIS, etc.)
Pour valider la conformité globale, utilisez **AWS Security Hub** qui centralise les contrôles de sécurité et de conformité. Security Hub intègre des standards tels que les CIS AWS Foundations Benchmarks et les « AWS Foundational Security Best Practices ».

- **Accéder à Security Hub.** Dans la console AWS, sous **Sécurité, identités et conformité**, ouvrez **AWS Security Hub**. Vérifiez que les standards pertinents sont activés : par exemple *CIS AWS Foundations Benchmark* et *AWS Foundational Security Best Practices*. Ces standards analysent automatiquement vos ressources et génèrent des résultats (findings) pour chaque contrôle. Security Hub fournit une vue consolidée de votre état de conformitédocs.aws.amazon.com.
- **Consulter le Dashboard et les Standards.** Sur le tableau de bord de Security Hub, observez les indicateurs globaux (nombre de contrôles réussis/échoués). Sous **Standards** (ou **Security standards**), sélectionnez le standard *CIS AWS Foundations*. Vous verrez la liste des contrôles CIS avec leur état (PASS/FAIL). Prenez note des contrôles échoués (FAILED) et des ressources concernées. Faites de même pour tout autre standard (par ex. PCI-DSS, GDPR si activé, etc.).
- **Examiner les résultats de contrôle (findings).** Dans la section **Findings**, filtrez par normes (par ex. *Compliance:CIS_AWS_FOUNDATIONS_BENCHMARK*). Vous pouvez exporter les findings en CSV ou JSON via l'interface (bouton *Export findings*) ou utiliser l'AWS CLI/Athena pour extraire les données. Documentez les résultats pour le rapport mensuel : indiquez le pourcentage de contrôles CIS réussis et les principaux échecs à corriger.
- **Inclure d'autres sources de conformité.** Vous pouvez également inclure dans votre rapport les résultats d'autres outils, par exemple :
    - *Scans CIS AWS Foundations (via Inspector)* si vous en avez lancé (voir section précédente).

- *AWS Config*: si vous utilisez Config Rules (par ex. règles de sécurité) ou des packs de conformité, rappelez leur état global.
- *Résumé du Tableau de bord Security Hub*: mentionnez par ex. le nombre de comptes analysés, le nombre de normes activées, etc.

En résumé, Security Hub vous fournit les résultats des audits de configuration de sécurité. Comme l'explique AWS, ce service « fournit une vue complète de votre état de sécurité, vous permettant de vérifier votre conformité aux normes et meilleures pratiques du secteur »docs.aws.amazon.com. Ainsi, en générant chaque mois un rapport des findings CIS et des autres standards, vous obtenez une trace écrite de votre conformité.

Vérifier les règles de cycle de vie S3 pour les logs

Pour éviter de conserver indéfiniment des logs et respecter les obligations (ex. RGPD), assurez-vous que les buckets S3 de logs possèdent des règles de cycle de vie. Ces règles suppriment automatiquement les journaux au-delà d'un certain âge.

- **Identifier les buckets de logs.** Repérez les buckets S3 où sont stockés vos logs (CloudTrail, VPC Flow Logs, logs d'accès S3, etc.).
- **Ouvrir les règles de cycle de vie.** Dans la console S3, sélectionnez un bucket concerné puis l'onglet **Propriétés** (ou **Gestion** en français), puis **Règles de cycle de vie**.
- **Vérifier ou créer la règle de suppression.** Recherchez une règle existante qui concerne les objets de log (souvent identifiés par un préfixe, p.ex. AWSLogs/). Si une règle existe, vérifiez qu'elle comporte une action *Expiration* : par exemple, *Supprimer les versions actuelles des objets plus anciens de X jours*. Ce X doit correspondre à votre durée de conservation légale (souvent 365 jours pour les logs RGPD). S'il n'existe pas de règle, créez-en une nouvelle : donnez-lui un nom, spécifiez le préfixe des logs (ex. logs/ ou le chemin exact), puis cochez **Expiration** et renseignez le nombre de jours après lesquels supprimer les objets.
- **Enregistrer et appliquer.** Sauvegardez la règle. S3 traitera automatiquement tous les logs existants plus vieux que le seuil défini et les mettra en file de suppression. Comme l'indique la documentation AWS : on peut définir une règle de cycle de vie pour « supprimer automatiquement » les objets journaux lorsqu'ils ont dépassé leur période de conservationdocs.aws.amazon.com.

Enfin, répétez cette vérification pour chaque bucket de logs (CloudTrail, ELB, accès serveur, etc.). Ainsi, vous garantissez que les logs ne sont pas conservés au-delà des limites légales. La mise en place de règles de cycle de vie S3 est la méthode recommandée par AWS pour gérer la suppression automatique des logs après la période utiledocs.aws.amazon.com.

Sources : Documentation AWS sur CloudWatch, Athena, Inspector, Security Hub et S3 Lifecycledocs.aws.amazon.comdocs.aws.amazon.comdocs.aws.amazon.comdocs.aws.amazon.comaws.amazon.comdocs.aws.amazon.comdocs.aws.amazon.com. Ces références confirment l'usage des services décrits et les bonnes pratiques à suivre pour effectuer cette analyse mensuelle.

Annexe A : Feuille de Route Progressive vers la Conformité Intégrale RGPD

Indispensable : avant de libérer le document :

- Accès console AWS en MFA pour tous les comptes
    1. MJH
    2. ADN
    3. AWI
    4. SJH OK
- *AWS Inspector :A activer sur les instances Linux, associer IAM SSMManager (voir doc plus bas) A faire le Weekend*
- *Chiffrer la base de données RDS en* chiffrement AES-256 *(voir doc plus bas) A faire le Weekend*
- Vérifier que la sauvegarde est bien sur 30 jours,
- Vérifier que les Load-Balanceur (ALB)sont bien en HTTPS et que le HSTS est activé
- Vérifier que ***dans Amazon CloudWatch, ces métriques sont surveillées***
    - ***CPU*** *des instances EC2 > 80%*
    - ***Mémoire*** *des instances > 80%*
    - ***Connexions*** *Aurora > 80% du maximum*
    - ***Latence*** *des requêtes > 2 secondes*
    - ***Erreurs*** *HTTP 5xx > 1%*
- ***Comment peut-on*** *: Isolation une instance qui pose un souci de sécurité du réseau*

- **Données de pointage* (xt-time)** : 5 ans (obligation légale, Article L.3171-1 du Code du travail)
- **Données d'intervention* (xt-erp)** : 10 ans (prescription commerciale, Article L.110-4 du Code de commerce)
-

Urgent :

- Corrige les pb critique signalés (voir manuel quotidien)
- Mettre en place des règles d'escalade pour les alertes (AWS ou XT-erp):
    1. Mail + SMS (définir les règles)
    2. Envoi de mail au client et à l'équipe (voir spec OuestAM)

A faire après :

XT-erp / HD :

- Classification des incidents :
    1. P1 : critique
    2. P2 : élevé
    3. P3 : moyen
    4. P4 : Faible
- Créer les modèles de mails :
    1. 6.2.2 Modèles de communication
        1. Notification initiale :
        2. Notification de résolution
        3. VIOLATIONS DE DONNÉES PERSONNELLES
- **9.2.2 Métriques et KPI**

  Indicateurs de performance :
    - **Nombre** d'incidents par mois
    - **Temps** de détection moyen
    - **Temps** de résolution par criticité
    - **Satisfaction** client
    - **Taux** de résolution au premier niveau

  Objectifs :
    - **P1** : Résolution < 4h (100%)
    - **P2** : Résolution < 24h (95%)
    - **P3** : Résolution < 72h (90%)
    - **Satisfaction** client > 90%
    - **Détection** automatique > 70%

- **Il faut le connecter à n8n -> XT-erp HD : projet 2026**

    - *Exemple de ticket créé dans XT-helpdesk*
    -
    - *Titre : Alerte GuardDuty : UnauthorizedAccess:EC2/SSHBruteForce*
    - *Priorité : Haute*
    - *Description :*

- *Type : UnauthorizedAccess:EC2/SSHBruteForce*
- *Gravité : 8.1*
- *Ressource : i-07eabc123456def89*
- *Origine : Sécurité AWS*

	Thème	A faire	Par
		12.3 Purge automatique Le Sous-traitant-éditeur met en place des mécanismes de purge automatique selon les durées définies ci-dessus, sauf instruction contraire du Client.	
		~~**Données de sauvegarde** : 30 jours (mode SaaS, indicative pour optimisation)~~	
	Registre des traitements		
	Mesures de sécurité détaillées	~~***Configuration Aurora :***~~ ~~***Chiffrement*** ~~*au repos activé (AES-256)*~~ ~~*Condition réalisable si activée dès la création !!*~~ ~~*Vérifier la condition*~~	
		~~***Accès AWS console***~~ ~~***MFA*** ~~*obligatoire pour tous les accès*~~	

		~~*AWS Inspector :A activer sur les instances Linux*~~	
		~~***Vérifier que***~~ ~~***3.2.1 Application Load Balancer (ALB)***~~ ~~***Configuration HTTPS :***~~ • ~~***HSTS** activé*~~	
		• **c**	
		~~***Comment peut-on** : Isolation une instance qui pose un souci de sécurité du réseau*~~	
	Procédure de gestion des incidents		
		~~***3. DÉTECTION ET SURVEILLANCE***~~ ~~***3.1 Outils de surveillance AWS***~~ ~~***3.1.1 Amazon CloudWatch***~~ ~~***Métriques surveillées :***~~ • ~~***CPU** des instances EC2 > 80%*~~ • ~~***Mémoire** des instances > 80%*~~ • ~~***Connexions** Aurora > 80% du maximum*~~ • ~~***Latence** des requêtes > 2 secondes*~~ • ~~***Erreurs** HTTP 5xx > 1%*~~	
		~~Classification des incidents :~~ ~~P1 : critique~~ ~~P2 : élevé~~ ~~P3 : moyen~~ ~~P4 : Faible~~	
		~~***6.2.2 Modèles de communication***~~ ~~***Notification initiale :***~~ ~~*Objet : [INCIDENT] Problème technique sur [Service]*~~	

		~~*Cher client,*~~ ~~*Nous rencontrons actuellement un problème technique sur [Service] qui peut impacter [Fonctionnalités].*~~ ~~*Incident détecté : [Date/Heure]*~~ ~~*Services impactés : [Liste]*~~ ~~*Cause identifiée : [Cause ou "En cours d'investigation"]*~~ ~~*Estimation résolution : [Délai]*~~ ~~*Nos équipes travaillent activement à la résolution.*~~ ~~*Prochaine mise à jour : [Heure]*~~ ~~*Équipe technique [Entreprise]*~~ ~~***Notification de résolution :***~~ ~~*Objet : [RÉSOLU] Problème technique sur [Service]*~~ ~~*Cher client,*~~ ~~*Le problème technique sur [Service] est désormais résolu.*~~ ~~*Incident résolu : [Date/Heure]*~~ ~~*Durée d'impact : [Durée]*~~ ~~*Cause : [Cause identifiée]*~~ ~~*Solution appliquée : [Solution]*~~ ~~*Tous les services fonctionnent normalement.*~~ ~~*Un rapport d'incident détaillé suivra sous 48h.*~~ ~~*Équipe technique [Entreprise]*~~	

		~~**6. VIOLATIONS DE DONNÉES PERSONNELLES**~~ ~~*Objet : [URGENT] Violation de données personnelles*~~ ~~*Cher client,*~~ ~~*Nous vous informons qu'un incident de sécurité a affecté*~~ ~~*Certaines données personnelles traitées par nos services.*~~ ~~*Incident détecté : [Date/Heure]*~~ ~~*Nature : [Description]*~~ ~~*Données concernées : [Type et nombre]*~~ ~~*Personnes impactées : [Nombre et catégories]*~~ ~~*Mesures prises : [Actions correctives]*~~ ~~*Nous avons immédiatement :*~~ ~~*- Sécurisé les systèmes*~~ ~~*- Notifié la CNIL*~~ ~~*- Renforcé la surveillance*~~ ~~*Un rapport détaillé suivra sous 48h.*~~ ~~*Contact : [Email/Téléphone]*~~ ~~*Direction [Entreprise]*~~	
		~~**9.2.2 Métriques et KPI**~~ ~~**Indicateurs de performance :**~~ • ~~**Nombre** d'incidents par mois~~ • ~~**Temps** de détection moyen~~ • ~~**Temps** de résolution par criticité~~ • ~~**Satisfaction** client~~ • ~~**Taux** de résolution au premier niveau~~ ~~**Objectifs :**~~ • ~~**P1** : Résolution < 4h (100%)~~ • ~~**P2** : Résolution < 24h (95%)~~ • ~~**P3** : Résolution < 72h (90%)~~	

		• ~~***Satisfaction** client > 90%*~~ • ~~***Détection** automatique > 70%*~~	
	Liste des sous-traitants autorisés		
	Modèles de notification aux personnes concernées		
	Annexe 6 : POLITIQUE DE SÉCURITÉ SSH		

Voici le mode d'emploi pas à pas pour installer l'agent AWS Systems Manager (SSM)

sur une instance EC2 (Linux ou Windows), **prérequis indispensable** pour qu'**Amazon Inspector** puisse fonctionner pleinement (scan de vulnérabilités via SSM Agent).

🔧 Objectif

Installer et vérifier le bon fonctionnement de **SSM Agent** sur une instance **EC2** dans AWS afin de permettre à **AWS Inspector** d'exécuter ses analyses de sécurité.

🧩 Prérequis

Élément	Détail
✅ Instance EC2 lancée	Amazon Linux 2, Ubuntu, Debian, RHEL ou Windows

Élément	Détail
✅ IAM Role attaché	Le rôle EC2 doit contenir la policy AmazonSSMManagedInstanceCore
✅ Internet ou VPC Endpoint	L'instance doit avoir accès aux services AWS Systems Manager (soit via NAT, soit VPC Endpoint)

📘 Étapes pour EC2 Amazon Linux / Ubuntu / Debian / RHEL

1. ✅ Vérifiez si SSM Agent est déjà installé :

Connectez-vous à votre instance EC2 en SSH puis tapez :

sudo systemctl status amazon-ssm-agent

Si le service est actif, c'est que l'agent est déjà installé. Sinon :

---

2. 📥 Téléchargez et installez SSM Agent

➤ **Pour Amazon Linux 2 ou RHEL/CentOS 7 :**

sudo yum install -y amazon-ssm-agent

➤ **Pour Ubuntu/Debian :**

sudo snap install amazon-ssm-agent --classic

➤ **Alternative si snap non disponible :**

wget https://s3.amazonaws.com/amazon-ssm-<région>/latest/debian_amd64/amazon-ssm-agent.deb

sudo dpkg -i amazon-ssm-agent.deb

(remplacez <région> par eu-west-3 pour Paris par exemple)

---

3. ▶️ Démarrez le service SSM Agent

sudo systemctl enable amazon-ssm-agent

sudo systemctl start amazon-ssm-agent

---

4. 📋 Vérifiez l'état du service

sudo systemctl status amazon-ssm-agent

Le service doit être en état **active (running)**.

---

5. 🔎 Vérifiez l'enregistrement de l'instance

Allez dans la **console AWS > Systems Manager > Managed Instances**

- L'instance EC2 doit apparaître dans la liste.
- Statut attendu : **"Managed"**

- Colonne "Ping Status" = **"Online"**

⚠️ **Cas particulier : Windows Server EC2**

L'agent SSM est **préinstallé sur Windows Server 2016/2019/2022**.

Si besoin de redémarrer :

Restart-Service AmazonSSMAgent

🔐 **Vérification finale pour AWS Inspector**

1. Allez dans **AWS Inspector > Environnement**
2. L'instance doit apparaître dans les ressources surveillées
3. Vérifiez que les statuts **SSM agent** et **Inspector scan** sont **actifs et à jour**

Souhaitez-vous que je vous fournisse ce guide au format **Word**, prêt à intégrer dans vos procédures internes ?

Chiffrement RDS

Recommandations

- Effectuer cette opération **en heures creuses** (soirée, nuit, week-end).
- Préparer un **plan de rollback** : conservez l'ancienne base jusqu'à validation complète de la nouvelle.
- Vérifier que vos scripts de sauvegarde/restauration, monitoring et accès sont mis à jour.
- Interdire la connexion des utilisateurs à la base de données

Étapes pour migrer vers une base Aurora chiffrée

Étape	Description	Temps estimé
1. **Créer un snapshot**	Snapshot de votre base existante non chiffrée.	Instantané à quelques minutes
2. **Copier le snapshot**	En choisissant l'option **chiffrer avec une clé KMS**.	Dépend de la taille de la base (quelques minutes à plusieurs heures)
3. **Restaurer une instance ou un cluster Aurora à partir du snapshot chiffré**	Crée une **nouvelle base chiffrée**.	5 à 30 minutes généralement
4. **Basculer les connexions applicatives vers la nouvelle base**	Redirection DNS / mise à jour des paramètres de connexion	Très rapide, mais requiert un **arrêt de service** ou bascule contrôlée
5. **Vérifications post-migration**	Sanity check : intégrité, connexions, performances, backups	30 à 60 minutes selon vos procédures