Plan d'Assurance Sécurité My Silae

(Annexe au Plan d'Assurance Sécurité Global Silae)

V1.01

Dernière révision : 03 mars 2025

Sommaire

1. Objet et domaine d'application

Ce document a pour objectif de définir les spécificités du Plan d'Assurance Sécurité (PAS) relatives au service My Silae (le Service), l'offre de Paie digitalisé de Silae. Le présent document est une annexe du Plan d'Assurance Sécurité Global de Silae.

Le service My Silae est accessible aux moyens de différentes applications (client Desktop, mobile ou web) qui communiquent avec une architecture commune hébergée sur Azure via des APIs privées ou publiques.

Ce document est destiné aux partenaires de Silae et il est classifié à usage Restreint [(1)]. Il n'est pas possible de le partager à des tiers sans une requête formelle et un accord explicite de Silae.

Ce document a pour but de préciser les modalités mises en place par Silae pour contribuer à la disponibilité du service et répondre aux exigences de cybersécurité.

Ce document pourra être modifié par Silae à tout moment sans notification préalable. Les informations renseignées sont l'état de l'art au moment de sa rédaction. Silae est engagé dans une démarche d'amélioration continue et proactive. Les informations, les services exposés sont susceptibles d'évoluer à tout moment pour améliorer la posture de sécurité de Silae ou du service My Silae.

2. Acronymes et Definitions

« My Silae » La solution Paie & RH collaborative fournie par Silae qui englobe l'ensemble des applications (Web, Mobile, Application de bureau) nécessaires à son utilisation.

« My Silae Gestionnaire de Paie ou My Silae GP » Nom de l'application de bureau SaaS déployé sur les stations de travail et principalement utilisé par les gestionnaires de paie.

« My Silae Entreprise » correspond aux différents portails client (web ou mobile) utilisés par les salariés, les managers ou les dirigeants.

« Applications Hébergées » correspond à l'ensemble des applications liées au service My Silae et délivrées en mode SaaS.

« Infrastructure Technique » désigne l'ensemble des équipements, systèmes et technologies qui permettent le bon fonctionnement du service My Silae.

« CNIL » Commission Nationale de l'Informatique et des Libertés est une autorité administrative indépendante française en charge de veiller à la protection des données

personnelles contenues dans les traitements informatiques opérés par des organismes publics ou privés (cnil.fr).

« Cloud » (ou cloud computing) : en français « informatique en nuage », correspond à la fourniture de services informatiques (serveurs, stockage, bases de données, réseaux, etc.) à distance via Internet et un fournisseur spécialisé. Le principal service logiciel proposé en cloud computing est le SaaS.

« SaaS » (Software as a Service) Logiciel en tant que Service est un modèle de distribution de logiciel à travers le Cloud. L'hébergement des applications est sous la responsabilité du fournisseur du Service. La solution SaaS est accessible à la demande via une connexion Internet. La mise à disposition, la maintenance évolutive et corrective, les mises à jour sont de la responsabilité de l'éditeur du logiciel SaaS.

« Microsoft Azure » désigne la plate-forme Microsoft Azure et correspond aux offres d'informatique en nuage public de type SaaS, PaaS et IaaS de Microsoft. Microsoft est un fournisseur de service critique pour Silae.

« Période de Maintenance » désigne une période durant laquelle le Service peut être interrompu pour effectuer des maintenances applicatives et techniques conformément aux dispositions du présent document.

« Mises à Jour » désigne les améliorations apportées au Service My Silae (logiciel et infrastructures informatiques sous-jacentes). Les Mises à Jour comprennent également la correction d'éventuelles anomalies et les améliorations fonctionnelles ou légales liées au domaine de la Paie.

« API » (Application Programming Interface), en français « interface de programmation d'application », désigne l'ensemble des définitions et des protocoles qui facilitent l'intégration du Service avec d'autres applications.

« Géoredondance » est un concept de sécurité des données que de plus en plus d'entreprises intègrent dans leur infrastructure de sécurité numérique afin de protéger les données et les opérations contre les événements imprévus tels que les catastrophes naturelles, les défaillances matérielles ou les cyberattaques. La géoredondance implique que les données sont répliquées dans plusieurs emplacements géographiques.

« Incident Critique » désigne un incident entraînant une interruption totale et non programmée du Service.

« ISO » (International Organisation for Standardization) ou Organisation Internationale de Normalisation est une organisation ayant pour but de produire des normes internationales dans les domaines industriels et commerciaux.

« Cloud Security Alliance (CSA) » est la principale organisation mondiale qui se consacre à la définition et à la sensibilisation des meilleures pratiques afin de garantir un environnement informatique en nuage sécurisé.

« Cloud Controls Matrix (CCM) » est un cadre de contrôle de la cybersécurité pour l'informatique en nuage piloté par la Cloud Security Alliance.

« CSA STAR Certification » désigne un label de sécurité pour le Cloud. Les Certifications de la « Cloud Security Alliance » s'appuient sur les certifications ISO 27001 et la Cloud Control Matrix.

3. HEBERGEMENT AZURE

L'hébergement du service My Silae est assuré par Microsoft Azure.

3.1 Certifications et conformité

La plateforme Microsoft Azure dispose de nombreuses certifications ISO (International Organization for Standardization) et CSA (Cloud Security Alliance) et propose une couverture de conformité réglementaire très large.

Microsoft Azure est, entre autres, certifié ISO27001, SOC I, SOC II et PCI DSS.

Les différents certificats relatifs à Microsoft Azure sont disponibles ici :
https://servicetrust.microsoft.com/

L'ensemble de la documentation liée à la conformité Azure est disponible ici :
https://docs.microsoft.com/fr-FR/azure/compliance/

Les certifications CSA STAR sont disponibles ici :
https://cloudsecurityalliance.org/star/registry/microsoft/

Les rapports d'audit et les certifications associées sont disponibles ici :
https://servicetrust.microsoft.com/Documents/ComplianceReports

3.2 Niveaux de service

Les niveaux de service (SLA - Service Level Agreement) associés aux différents services Microsoft Azure sont répertoriés ici :
https://azure.microsoft.com/fr-fr/support/legal/sla/

Une représentation visuelle des SLA est disponible ici :
https://azurecharts.com/sla

3.3 Localisation de l'exploitation

Les infrastructures Azure (serveurs de calcul, serveurs de bases de données, stockages, services réseau, etc.), les données et les sauvegardes exploitées par le service My Silae sont exclusivement localisées sur le territoire métropolitain français.

La région Microsoft Azure « France Central » est la zone de référence pour l'intégralité de l'exploitation.

Les spécifications de cette région sont consultables ici :
https://azure.microsoft.com/fr-fr/regions/

Silae se réserve le droit d'exploiter tous les centres de données existants ou futurs liés à cette région Azure ou situé sur le territoire métropolitain français.

La région « France South » est la région de référence pour la géoredondance des données.

La plateforme Microsoft Azure fournit une description détaillée des mécanismes d'accès aux données dans le document suivant :
https://www.microsoft.com/fr-fr/trustcenter/privacy/who-can-access-your-data-and-on-what-terms

3.4 Sécurité de l'exploitation

Dans le cadre de son exploitation, Silae s'appuie sur l'expérience et sur l'expertise de Microsoft au travers des services proposés par la plateforme Microsoft Azure.

La plateforme Azure offre de nombreux mécanismes pour effectuer la sécurisation, la gestion et la surveillance des services et des équipements. La sécurité du service My Silae hérite implicitement d'un nombre important de fonctionnalités Azure liées à la sécurité.

L'ensemble de la Sécurité du service My Silae repose sur une responsabilité partagée. Microsoft est responsable de la gestion de ces centres de données et de l'ensemble du périmètre de sécurité associé (intégrité physique des bâtiments et des équipements, protocoles d'accès, protections incendie, etc.). Azure fournit aussi un ensemble de services logiciels liés à la sécurité qui répond aux exigences de Silae.

Une présentation de la stratégie de sécurité Microsoft Azure est disponible ici :
https://docs.microsoft.com/fr-fr/azure/security/fundamentals/overview

Microsoft met en œuvre les meilleures pratiques de sécurité existantes sur l'ensemble de ses services pour garantir la disponibilité, l'intégrité et la confidentialité des données. Silae se conforme à ces bonnes pratiques pour mettre en œuvre l'exploitation et la sécurité de son offre My Silae.

3.5 Sécurité physique de l'hébergement

Microsoft conçoit, crée et utilise des centres de données de manière à assurer un contrôle strict de l'accès physique aux zones où les données sont stockées. Microsoft comprend

l'importance de protéger les données de ses clients et s'engage à contribuer à la sécurisation des centres de données qui contiennent les données de Silae. Microsoft dispose d'une division entière dédiée à la conception, à la création et au fonctionnement des installations physiques qui gèrent Azure. Ces équipes sont investies dans la conservation d'une sécurité physique à la pointe.

Microsoft adopte une approche en couche de la sécurité physique, pour réduire les risques et éviter que des utilisateurs non autorisés puissent avoir un accès physique aux données et aux ressources des centres de données. Les centres de données gérés par Microsoft présentent des couches de protection complètes : approbation de l'accès au périmètre de l'installation, au périmètre du bâtiment, à l'intérieur du bâtiment et à l'étage du centre de données. Les couches de la sécurité physique sont :

- **Demande d'accès et approbation.** Vous devez demander l'accès avant d'arriver au centre de données. Vous êtes obligé de fournir une justification professionnelle valide de votre visite, par exemple pour des raisons de conformité ou d'audit. Toutes les demandes sont approuvées au cas par cas par les employés de Microsoft. La gestion des accès au cas par cas permet de garder le nombre de personnes qui ont besoin d'effectuer une tâche dans les centres de données au strict minimum. Une fois qu'une personne obtient une autorisation de Microsoft, elle n'a accès qu'à la zone du centre de données requise, pour laquelle sa justification a été approuvée. Les autorisations sont limitées dans le temps et expirent.

- **Accès des visiteurs.** Les badges d'accès temporaires sont stockés dans le centre des opérations de sécurité (SOC) à accès contrôlé et inventoriés au début et à la fin de chaque changement d'équipe. Tous les visiteurs dont l'accès au centre de données est approuvé se voient attribuer un badge *Escort Only* (escorte obligatoire) et doivent toujours rester en compagnie de leur escorte. Les visiteurs escortés n'ont pas de niveau d'accès spécifié, et peuvent uniquement se déplacer dans les lieux auxquels leur escorte a accès. L'escorte est chargée d'examiner les actions et les accès du visiteur durant sa visite au centre de données. Les visiteurs doivent rendre leurs badges quand ils quittent un bâtiment Microsoft. Les niveaux d'accès sont supprimés de tous les badges visiteurs avant leur réutilisation pour d'autres visites.

- **Périmètre des locaux.** Quand vous arrivez dans un centre de données, vous êtes obligé de passer par un point d'accès bien défini. En règle générale, des clôtures hautes en acier et en béton couvrent chaque centimètre du périmètre. Des caméras sont postées autour des centres de données et une équipe de sécurité visionne les vidéos en permanence. Des patrouilles d'agents de sécurité veillent à ce que l'entrée et la sortie soient limitées aux zones désignées. Des bornes et d'autres mesures protègent l'extérieur du centre de données contre les menaces potentielles, notamment les accès non autorisés.

- **Entrée du bâtiment.** L'entrée des centres de données est surveillée par des professionnels de la sécurité qui ont suivi une formation stricte et dont les antécédents ont été vérifiés. Ces professionnels de la sécurité patrouillent aussi régulièrement dans le centre de données tout en contrôlant les vidéos des caméras qui se trouvent à l'intérieur en permanence.

- **À l'intérieur du bâtiment.** Après être entré dans le bâtiment, vous devez passer une authentification à deux facteurs avec biométrie pour pouvoir vous déplacer dans le centre de données. Si votre identité est validée, vous pouvez entrer dans la partie du centre de données pour laquelle votre accès a été approuvé. Vous pouvez y rester uniquement pendant la durée approuvée.

- **Étage du centre de données.** Vous n'êtes autorisé à vous rendre qu'à l'étage pour lequel votre accès a été approuvé. Vous êtes obligé de passer sous un portique de détection de métaux. Pour réduire le risque que des données non autorisées entrent ou sortent du centre de données sans notre connaissance, seuls les appareils approuvés sont admis à l'étage du centre de données. Par ailleurs, des caméras vidéo surveillent les deux côtés de chaque rack de serveurs. Quand vous quittez l'étage du centre de données, vous devez repasser par le portique de détection de métaux. Pour quitter le centre de données, vous devez passer par un autre scan de sécurité.

3.6 Révisions de la sécurité physique

Les révisions de la sécurité physique des bâtiments sont effectuées régulièrement pour s'assurer que les centres de données répondent aux critères de sécurité d'Azure. Le personnel du fournisseur d'hébergement du centre de données ne fournit aucune gestion des services Azure. Il ne peut pas se connecter aux systèmes Azure, n'a pas d'accès physique à la salle et aux cages de collocation Azure.

4. MAINTENANCE

Le service My Silae peut être interrompu durant les périodes de maintenance, qu'il s'agisse de maintenances standards, exceptionnelles ou urgentes.

Les équipes de Silae mettent en œuvre tous les moyens à leur disposition pour minimiser le nombre d'opérations et la durée des maintenances. Lorsque cela est possible, les maintenances sont préparées et testées dans des environnements hors production afin de valider le comportement attendu. Les maintenances sont indispensables pour assurer la continuité d'activité ainsi que la sécurité des infrastructures et des services.

Les maintenances d'infrastructures sont généralement réalisées sans interruption de service car les services sont redondés. Des mises à jour de certains services Azure peuvent

cependant entraîner une période d'interruption. Dans ce cas, nos équipes s'efforcent dans la mesure du possible de programmer et d'assurer ces maintenant dans la Période de Maintenance indiquée ou en Astreinte pendant les week-ends et jour fériés.

Périodes de Maintenance :

- Maintenance Standard

  Toutes les nuits entre 2h00 et 4h00 (Central European Time CET).

  La période de Maintenance Standard permet d'assurer une tranche horaire de mise à jour du Service (logiciel et infrastructures) pour garantir la qualité de service. Cette période de maintenance n'est pas systématiquement exploitée toutes les nuits, le Service peut rester accessible pendant la Période de Maintenance car la probabilité de couper l'accès aux Services sur l'intégralité de la Période de Maintenance reste très faible.

- Maintenance Exceptionnelle et Planifiée

  Une Maintenance Exceptionnelle et Planifiée peut être opérée en dehors des périodes de Maintenance Standard. Silae a l'obligation de communiquer sur cette intervention au moins 48 heures avant l'heure prévue de ladite maintenance.

- Maintenance Urgente

  Une Maintenance Urgente est susceptible d'intervenir à tout moment. Cette maintenance peut intervenir en cas de force majeure et Silae s'engage à mettre en œuvre tous les moyens possibles pour tenir informé les Partenaires et les Clients sur l'évolution des opérations liées à cette maintenance.

5. DISPONIBILITE DU SERVICE

Les Applications Hébergées et l'Infrastructure Technique associée à My Silae sont accessibles en permanence, 24 heures sur 24 et 7 jours sur 7.

Les applications My Silae et/ou l'infrastructure technique correspondante peuvent être temporairement indisponibles lorsque Silae doit effectuer des opérations de maintenance, conformément aux conditions énoncées dans la section Maintenance de ce document.

Silae met en œuvre tous les moyens nécessaires pour superviser ses services. La **disponibilité** des applications hébergées et des infrastructures techniques est supervisée en continu, y compris les jours fériés. Cette supervision est assurée par les équipes

opérationnelles de 9h00 à 18h00, puis relayée par l'équipe d'astreinte en dehors de ces horaires.

La continuité du service est notre priorité. Dès la détection d'un incident, Silae mobilise immédiatement les ressources requises afin de le corriger ou de le contourner, dans le but de limiter au maximum la durée d'indisponibilité.

L'indisponibilité du service est constatée dès lors que l'accès à l'application est totalement interrompu. En revanche, les périodes de ralentissement ne peuvent en aucun cas être considérées comme une indisponibilité.

Silae s'engage, dans le cadre d'une obligation de moyens, à garantir un Taux de Disponibilité (TD) mensuel du service d'au moins 99,5 %.

Le taux de disponibilité (TD) est défini comme la possibilité de se connecter au Service dans la période de référence (PR).

La période de référence (PR) correspond aux temps en dehors des Périodes de Maintenance effectives (de tout type).

Le temps d'indisponibilité (TI) du service n'est calculé qu'en dehors des Périodes de Maintenance effectives (et de tout type) et lorsque le Service est totalement inaccessible (Incident Critique.)

Formule de calcul : TD = (PR-TI) / PR

TD : taux de disponibilité
PR : période de référence
TI : temps d'indisponibilité

Les incidents entraînant des problèmes d'accès au Service et ne relevant pas du contrôle de Silae ne peuvent, en aucune manière, être considérés comme du Temps d'Indisponibilité.

Incidents non éligibles :

- Difficultés d'accès au Service dues à une mauvaise configuration du poste de travail du Client.
- Problèmes de télécommunication (accès internet et réseau d'entreprise) chez le Client ou chez le fournisseur d'accès du Client.
- Défaut dans le système informatique du Client.
- Tout autre incident, hors de contrôle de Silae, interdisant le fonctionnement optimal du Service pour le Client.
- Un incident lié à un fournisseur critique et hors de contrôle de Silae.

6. SEPARATION DES ENVIRONNEMENTS

Silae exploite deux types d'environnement dans ses infrastructures : Production et Hors Production.

Il existe une séparation stricte entre les environnements pour prévenir et réduire les risques de propagation d'une faille de sécurité ou d'une mauvaise configuration. Cela participe également à la prévention des erreurs humaines qui pourraient conduire un développeur ou un administrateur à effectuer une opération non souhaitée dans un environnement en dehors de son périmètre.

Chacun de ses environnements et assujetties à des règles de sécurité distinctes concernant la Gestion des identités et des accès (IAM).

6.1 Environnement de Production

L'environnement de production contient des systèmes critiques, des données réelles et des applications en service pour les utilisateurs finaux. Il nécessite un contrôle strict des accès pour garantir sa stabilité et sa sécurité.

6.2 Environnement Hors production

L'environnement hors production contient des ressources liées aux développements, aux tests, à la préproduction, etc. Il ne contient pas de systèmes critiques, de données réelles ou d'applications accessibles aux utilisateurs finaux.

Il est utilisé pour le développement de nouvelles fonctionnalités et les tests avant déploiement en production. Cet environnement est souvent moins sécurisé, car il peut impliquer des versions expérimentales du logiciel et des configurations en cours de modification.

7. CERTIFICATIONS DE SILAE

Silae ne bénéficie pas de certification.

Un projet de certification ISO 27001 est en cours pour viser une certification dans le premier semestre 2025. Cette date est donnée à titre indicatif, sans engagement et susceptible d'évoluer.

8. RESPECT DES BONNES PRATIQUES

Les bonnes pratiques sur Azure permettent de sécuriser, optimiser et assurer une gestion efficace des ressources cloud tout en maintenant un niveau de performance et une conformité élevée.

Silae applique systématiquement ces pratiques pour couvrir divers aspects des infrastructures Azure : gestion des identités et de la surveillance, gestion de la sécurité et optimisation des coûts.

8.1 Gestion des identités et des accès (IAM)

Principe du moindre privilège

Silae applique le principe du moindre privilège en utilisant Azure RBAC (Role-Based Access Control).
Les utilisateurs et services reçoivent uniquement les autorisations dont ils ont besoin pour accomplir leurs tâches.

Multifactor Authentication (MFA)

Silae active systématiquement l'authentification multifactorielle (MFA) pour les comptes utilisateur (Microsoft Authenticator, Clé FIDO2).

Silae utilise des politiques d'accès conditionnel pour forcer des méthodes de MFA plus sécurisées lors des connexions à partir d'environnements non sécurisés ou d'emplacements géographiques inhabituels.

Exemples :

- Règle MFA : oblige l'utilisation du MFA pour tous les utilisateurs, token de 24h.
- Règle Sign-in risk-based multifactor authentication : Oblige le renouvellement du token MFA pour un utilisateur identifié à risque.
- Require multifactor authentication for risky sign-ins : Oblige la connexion MFA si une action d'authentification remonte en risque élevé, par exemple un compte légitime qui se connecterait depuis l'étranger. L'action remontera en risque élevé.

Utilisation de Privileged Identity Management (PIM)

Silae implémente Azure PIM (Privileged Identity Management) pour une gestion just-in-time des rôles à privilège, en limitant la durée pendant laquelle les utilisateurs peuvent exercer des actions administratives.

Limitation du nombre de compte d'administration

- Silae limite le nombre d'utilisateur avec des rôles Entra ID à hauts privilèges
    - **Global Administrator :** 1 compte bris de glace avec le rôle actif et 4 comptes éligibles par le PIM
    - **User Administrator :** 2 comptes éligibles par le PIM
    - **Security Administrator** : 1 compte éligible par le PIM

8.2 Sécurité et conformité

Azure Security Center et Microsoft Defender

Silae utilise Azure Security Center pour surveiller en continu l'état de sécurité des ressources, détecter les menaces et recevoir des recommandations d'amélioration et Microsoft Defender for Cloud pour une détection et une protection avancée contre les menaces, en appliquant des configurations de sécurité à travers les abonnements Azure.

Chiffrement des données

Silae chiffre les données au repos avec Azure Storage Service Encryption (SSE) ou en utilisant des clés gérées dans des Azure Key Vault.

Silae active le chiffrement des données en transit avec SSL/TLS pour sécuriser les communications entre les services et les utilisateurs.

Contrôle des accès réseau

Chaque projet dispose de ses propres sous-réseaux, garantissant un cloisonnement strict entre les différents environnements. Silae s'appuie sur des NSG (Network Security Groups) pour contrôler et filtrer le trafic entrant et sortant des sous-réseaux et des machines virtuelles, limitant ainsi les connexions aux seules sources de confiance.
Les VNets assurent une isolation renforcée des environnements, avec des accès publics (Internet) désactivés par défaut.
Dans les cas où des flux Internet entrants sont requis, ils transitent nécessairement par une couche de sécurisation, telle qu'Azure Application Gateway ou Azure Front Door, avec la fonctionnalité WAF activée.
Lorsqu'une communication entre différents services indépendants est nécessaire au sein de Silae, les flux remontent dans les couches d'isolation jusqu'au service Azure Firewall. Ce dernier effectue des contrôles au niveau applicatif avant que le trafic ne redescende vers le NSG de la plateforme de destination, pour finalement atteindre le service concerné.

8.3 Organisation et gestion des ressources

Tagging des ressources

Silae utilise les tags pour organiser et classer les ressources selon des critères comme l'environnement (production, développement), l'équipe responsable, ou les projets pour faciliter la gestion et l'analyse des coûts.

Groupes de ressources

Silae organise les ressources dans des groupes de ressources en fonction de leur cycle de vie, des équipes ou des plateformes. Cela permet de gérer les ressources de manière plus modulaire et de faciliter les politiques de gouvernance.

Abonnements multiples

Silae segmente les infrastructures dans des abonnements multiples, en séparant les projets et les environnements de production.

8.4 Optimisation de l'empreinte énergétique

Silae a mis en place des fonctionnalités d'autoscaling (mise à l'échelle) de ses infrastructures pour adapter automatiquement les ressources en fonction de la demande, ce qui permet de contrôler les coûts tout en maintenant les performances. L'autoscaling permet de réduire l'empreinte énergétique de nos opérations et d'adopter une meilleure posture RSE (responsabilité sociétale des entreprises).
Des règles de mise à l'échelle sont configurées pour éviter de sous-utiliser ou surdimensionner les ressources.

Des tâches planifiées permettent de purger les données obsolètes ou inutiles, contribuant ainsi à réduire l'empreinte des espaces de stockage.

8.5 Performance et disponibilité

Répartition de charge et redondance

Silae utilise des services Azure Load Balancers et Application Gateway pour distribuer uniformément le trafic réseau entre plusieurs instances, assurant la haute disponibilité et la résilience des applications.

La redondance géographique est activée pour les données critiques en configurant des services comme Azure Site Recovery pour la reprise après sinistre et Azure Backup pour les sauvegardes régulières.

Optimisation des bases de données

Silae utilise des services managés de bases de données comme Azure MySQL Flexible Server pour réduire la charge administrative et assurer des performances optimales grâce à des fonctions intégrées comme le scaling automatique et les sauvegardes automatiques.

8.6 Surveillance et gestion des incidents

Silae utilise Azure Monitor pour suivre les performances et l'intégrité des ressources Azure. Des alertes surveillent les métriques critiques comme l'utilisation de la CPU, la latence du réseau ou l'état des services.
Silae utilise Log Analytics pour centraliser et analyser les logs de certaines ressources, ce qui permet d'identifier rapidement les problèmes de performance ou de sécurité pour ces ressources.

8.7 Déploiement et DevOps

Infrastructure as Code (IaC)

Silae a automatisé la gestion des environnements Azure à l'aide de modèles ARM (Azure Resource Manager) ou d'outils comme **Bicep** ou **Terraform**. L'IaC garantit la reproductibilité, la cohérence et l'automatisation des déploiements.

Azure DevOps et CI/CD

Silae utilise Azure DevOps pour créer des pipelines d'intégration continue et de déploiement continu (CI/CD).
Cela permet des mises à jour rapides et fiables des applications tout en réduisant les risques d'erreurs manuelles.

Les environnements de déploiement sont gérés avec **Azure DevOps Environments** afin de garantir la traçabilité et la sécurité. Chaque déploiement est associé à un environnement Azure spécifique et soumis à un système de validation par un administrateur qualifié.

9. GESTION DES ACCES ET DES IDENTITES (INFRASTRUCTURES)

9.1 Organisation des comptes utilisateurs

L'organisation des comptes utilisateurs et comptes de service au sein du tenant Azure de Silae est un aspect essentiel pour assurer la sécurité, l'évolutivité et la gestion des accès. Cette approche structurée permet de contrôler efficacement qui a accès à quelles ressources, d'appliquer des principes de sécurité comme le moindre privilège, et de garantir la conformité aux réglementations internes ou externes.

Silae utilise **EntraID** comme solution de gestion des identités et des accès.
Les comptes sont structurés de manière à garantir la sécurité et l'efficacité dans la gestion des accès aux ressources.

- **Comptes utilisateurs**
  Utilisés par les membres de l'organisation pour accéder à Azure et aux applications intégrées à Azure AD (Azure Active Directory). Chaque compte est associé à un utilisateur spécifique (employé, consultant, etc.)
  Les utilisateurs ont des accès limités aux ressources Azure. Nous appliquons systématiquement les principes de moindre privilège pour tous les utilisateurs et sur tous les abonnements.

- **Comptes d'administration**
  Les administrateurs ont des privilèges plus élevés sur les abonnements et les ressources. Ces comptes possèdent des accès à l'administration du tenant et d'Entra ID. Ils sont détenus uniquement par l'équipe d'administration DevOps

- **Comptes utilisateurs invités**
  Les utilisateurs invités (externes) ne sont pas autorisés sur le tenant Azure

- **Comptes de service**
  Les comptes de service utilisent des identités managées d'Azure. Les droits se basent sur les principes de moindre privilège et un compte de service ne sert que pour une utilisation précise.

Les utilisateurs font partis de groupes de sécurité. Ces groupes sont identifiés en fonction des équipes ou des projets.

Les droits accès (RBAC- Role-Based Access Control) des abonnements et des ressources sont attribués aux groupes.

Il n'y a pas d'attribution de droit par utilisateur.

Cette gestion permet aussi l'intégration de nouveaux utilisateurs à des groupes existants et de simplifier la gestion d'attribution de droits d'accès.
La gestion des actifs et des droits sur l'environnement Azure est procédurée.

Ce process est piloté par le service RH et Silae utilise un outil qui recense les mutations de personnel (entrée/sortie/changement de poste) ainsi que les actifs attribués à chaque utilisateur.

Le service d'administration DevOps fournit des comptes et des droits selon une matrice établie.

9.2 Segmentation & cloisonnement des comptes

Le cloisonnement des comptes sur Azure chez Silae consiste à organiser, restreindre et gérer les comptes d'utilisateurs et comptes de service de manière à isoler les accès et les responsabilités. Cette pratique renforce la sécurité en limitant la portée des privilèges des utilisateurs et en assurant une meilleure gestion des accès aux ressources.

Le cloisonnement vise à :

- **Limiter les privilèges d'accès** : Chaque utilisateur ou service doit avoir uniquement les droits nécessaires pour effectuer ses tâches (principe du moindre privilège.)
- **Isoler les environnements** : Les environnements de production, de développement, de test, etc., doivent être séparés pour éviter les erreurs et les interférences.
- **Assurer la sécurité** : En limitant les droits et en cloisonnant les comptes, la surface d'attaque potentielle est considérablement réduite en cas de compromission.
- **Faciliter la gestion des identités** : Une segmentation claire simplifie l'administration des comptes et la traçabilité des actions effectuées par chaque entité (utilisateur ou service).

9.2.1 Cloisonnement basé sur les rôles (RBAC)

RBAC (Role-Based Access Control) est une des méthodes centrales pour organiser et segmenter les comptes sur Azure. Azure propose des rôles prédéfinis qui permettent de donner des droits d'accès aux ressources, en fonction du rôle de l'utilisateur ou du service dans l'organisation.

Attribution des rôles

- Les rôles sont attribués aux utilisateurs, groupes ou comptes de service selon leur besoin d'accès aux ressources.
- Ces rôles peuvent être appliqués à différents niveaux : abonnement, groupe de ressources, ou ressource spécifique.

9.2.2 Segmentation par environnement

Une segmentation stricte des comptes par environnement (production, hors production) assure la sécurité et évite les erreurs.

Les comptes de service utilisés pour les applications ou les processus automatisés sont segmentés par projet/environnement. Azure Managed Identities permet de gérer ces comptes de manière sécurisée sans exposer directement les identifiants.

- **Comptes distincts** : Chaque environnement (production, hors production) a ses propres comptes de service.
- **Règles d'accès différentes** : Les utilisateurs ayant accès à l'environnement de production sont limités en nombre et ont des droits fortement contrôlés, tandis que les environnements hors production (développement, test, QA) sont plus permissifs.
- **Politiques RBAC distinctes** : Les développeurs peuvent potentiellement avoir des droits d'administration complets dans un environnement de développement, mais être restreints à un rôle de lecteur dans un environnement de production.

9.2.3 Groupes de sécurité et groupes Azure AD

L'utilisation des groupes Azure AD (Active Directory) est un moyen efficace de cloisonner les comptes à grande échelle, en appliquant des règles d'accès uniformes aux utilisateurs d'un même groupe.
Les groupes basés sur les rôles et responsabilités et les utilisateurs sont regroupés selon leurs rôles dans l'organisation.

9.2.4 Cloisonnement avec les abonnements Azure

Les abonnements Azure offrent une autre manière de segmenter les comptes et les accès aux ressources.
Un abonnement représente un conteneur qui regroupe des ressources Azure et où des règles spécifiques de gouvernance et de facturation peuvent être appliquées.

Silae utilise des abonnements distincts pour séparer les projets/environnements.
Chaque abonnement a ses propres groupes de ressources, ses rôles RBAC, et ses politiques de sécurité.

9.2.5 Accès conditionnel

Les politiques d'accès conditionnel permettent d'appliquer des règles supplémentaires aux comptes, selon des facteurs comme la localisation, l'appareil utilisé, ou le niveau de risque.

Les comptes d'administration accédant à des ressources critiques en production sont soumis à des règles d'authentification multifactorielle (MFA) strictes et des restrictions d'accès depuis certaines zones géographiques.

Les comptes peuvent être restreints à l'utilisation de dispositifs gérés ou dispositifs conformes selon les politiques de Silae. Cela renforce le cloisonnement des accès en évitant l'utilisation de comptes à partir de dispositifs non sécurisés.

9.2.6 Gestion des comptes invités et externes

Aucun utilisateur externe n'est habilité à accéder aux Tenant Silae ni à ses ressources. L'utilisation de comptes invités n'est pas autorisée par Silae. Si, dans le cadre d'un projet, un accès doit être accordé à un utilisateur externe (partenaires, sous-traitants), un compte spécifique sera créé avec les droits nécessaires à la mission, puis révoqué à la fin de celle-ci.

9.2.7 Surveillance et gestion des accès avec Azure PIM

Pour les comptes à haut privilège, Silae utilise Azure Privileged Identity Management (PIM) afin d'appliquer des mesures supplémentaires de cloisonnement et de sécurité.

Avec PIM, les utilisateurs ont des accès temporaires aux rôles privilégiés uniquement lorsqu'ils en ont besoin (principe de *just-in-time access*). En dehors de ces périodes, leurs droits sont révoqués.

PIM est également utilisé pour auditer l'usage des comptes avec des privilèges élevés et pour revoir régulièrement les rôles attribués afin de garantir qu'ils sont toujours nécessaires.

9.3 Azure Privileged Identity Management (PIM)

Azure Privileged Identity Management (PIM) est un service de Microsoft Entra ID qui permet de gérer, contrôler et surveiller l'accès aux ressources et aux droits importants d'une organisation.

Voici quelques-unes de ses principales fonctionnalités :

- **Accès juste-à-temps** : Les utilisateurs peuvent obtenir un accès temporaire aux ressources et aux droits critiques, réduisant ainsi les risques d'accès excessif ou non justifié.
- **Activation de rôle basée sur l'approbation** : Les rôles à privilège peuvent nécessiter une approbation avant d'être activés, ajoutant une couche de sécurité supplémentaire.
- **Authentification multifacteur (MFA)** : Pour activer certains rôles, les utilisateurs doivent passer par une authentification multifacteur.
- **Révisions d'accès** : Les organisations peuvent effectuer des révisions périodiques pour s'assurer que les utilisateurs ont toujours besoin de leurs rôles privilégiés.
- **Notifications et audits** : Les administrateurs reçoivent des notifications lors de l'activation des rôles et peuvent consulter les historiques d'audit pour surveiller les activités.

Ces fonctionnalités aident à renforcer la sécurité en limitant l'accès permanent aux rôles à privilèges et en surveillant les actions des utilisateurs ayant des accès élevés.

PIM est utilisé chez Silae dans EntraID pour les rôles à privilège :
Aucun compte personnel d'administration n'a de rôle permanent à privilège.
Quand un administrateur a besoin d'un rôle a privilège pour effectuer des actions, celui-ci peut s'auto-élever les droits pour une durée déterminée (maximum 8h).
L'information est transmise à l'ensemble des administrateurs pour alerter de l'élévation de privilège.

Il n'existe qu'un compte d'utilisateur "bris de glace" avec des droits permanents exclus du PIM.
C'est un compte d'administration d'urgence, qui n'est utilisé que dans des situations critiques où l'accès immédiat à l'environnement Azure est nécessaire. Ce type de compte est utilisé pour résoudre des problèmes de sécurité ou des pannes majeures lorsque les administrateurs réguliers ne peuvent pas se connecter ou lorsque d'autres méthodes d'accès ont échoué. L'objectif principal d'un compte bris de glace est de fournir un accès minimal mais critique, tout en restant très sécurisé.
Les identifiants du compte bris de glace (nom d'utilisateur, mot de passe, méthode MFA) sont stockés dans un emplacement hautement sécurisé (coffre-fort et solution de gestion des mots de passe d'entreprise).
L'accès à ces identifiants est restreint à quelques personnes clés au sein de l'organisation.

PIM est également utilisé pour certains droits RBAC qui sont d'un niveau un peu plus élevé sans être des droits d'administration et qui ne nécessitent pas d'être permanent sur les abonnements Azure.

9.4 Principes de moindre privilège

Silae applique le principe de moindre privilège.

Le principe du moindre privilège est une pratique de sécurité qui consiste à accorder aux utilisateurs et aux systèmes uniquement les permissions nécessaires pour accomplir leurs tâches spécifiques. Cela signifie que chaque utilisateur ou application reçoit le niveau d'accès minimum requis pour effectuer son travail, réduisant ainsi les risques de sécurité.

Dans une infrastructure Azure, l'application de ce principe est essentielle pour minimiser les risques de failles de sécurité, d'accès non autorisés ou d'erreurs humaines.

Azure Role-Based Access Control (RBAC)

Le contrôle d'accès chez Silae est basé sur les rôles (RBAC), c'est un mécanisme fondamental dans Azure pour implémenter le principe du moindre privilège. Avec RBAC, l'équipe d'administration DevOps accorde aux utilisateurs les autorisations nécessaires uniquement pour accomplir leurs tâches spécifiques, en fonction des rôles.

Azure Active Directory (Azure AD)

Azure Active Directory (Azure AD) gère l'authentification et les permissions pour les utilisateurs et les applications dans Azure. Le principe du moindre privilège est appliqué via plusieurs fonctionnalités d'Azure AD.

- **Groupes basés sur les rôles**
  L'équipe d'administration DevOps crée des groupes d'utilisateurs et attribue des permissions spécifiques à ces groupes en fonction de leur rôle dans l'organisation. Cela évite d'attribuer directement des droits individuels et permet une gestion plus fine des privilèges.

- **Accès conditionnel**
  Azure AD Conditional Access permet de restreindre l'accès aux ressources en fonction de conditions spécifiques (comme la localisation, l'appareil utilisé ou le risque associé à la connexion.)

- **Privileged Identity Management (PIM)**
  Azure Privileged Identity Management (PIM) est utilisé pour appliquer le principe du moindre privilège aux comptes administrateurs et autres rôles à privilèges. PIM

permet d'accorder des rôles privilégiés de manière temporaire et juste-à-temps (Just-in-Time, JIT), au lieu de laisser les utilisateurs détenir ces privilèges en permanence.

Sécurité des réseaux et des ressources

L'infrastructure réseau Silae dans Azure suit le principe du moindre privilège en limitant l'accès aux ressources uniquement à ce qui est nécessaire.

Les Groupes de sécurité réseau (NSG) et pare-feu Azure permettent de contrôler le trafic réseau entrant et sortant au niveau des sous-réseaux ou des interfaces réseau des machines virtuelles. L'accès aux ressources du réseau est restreint uniquement à certaines IP ou à des services spécifiques.

9.5 Usages réseau virtuel privé (VPN)

Les politiques de sécurité permettent l'administration des ports de management et des machines virtuelles uniquement sur des interfaces réseau privées et interdisent ces accès sur des IP publiques.

Silae impose systématiquement l'usage de VPN pour accéder sur ces interfaces privées ou se connecter aux infrastructures Azure.

Il existe plusieurs typologies de VPN selon les projets et selon le type d'environnement (Production/Hors Production).

Les accès sont gérés dans l'EntraID par des App registration.

En fonction du rôle des utilisateurs, Silae définit des accès différenciés.

Les sécurités EntraID s'appliquent donc lors de l'authentification aux VPN et particulièrement les conditionnals access (MFA, politique de mot de passe, emplacement, etc.)

Chaque passerelle VPN est reliée à son propre ensemble de réseau virtuel (VNet) distinct correspondant aux environnements. Cela garantit que le trafic réseau et les accès sont isolés entre les différents environnements.

Grâce aux logs générés par les différentes passerelles VPN, il est possible de surveiller les accès, d'auditer les actions réalisées dans chaque environnement et de démontrer la conformité aux exigences réglementaires ou de sécurité.

9.6 Authentification multifacteur (MFA)

Silae impose systématiquement l'usage d'une authentification MFA pour tous ses comptes et environnements.

L'authentification multifacteur (MFA) est une méthode de sécurité qui exige que les utilisateurs fournissent deux ou plusieurs formes d'authentification pour accéder à une ressource, comme une application, un compte en ligne ou un réseau.

Les facteurs d'authentification peuvent inclure :

Quelque chose que vous connaissez : un mot de passe ou un code PIN.
Quelque chose que vous possédez : un smartphone ou un badge de sécurité.
Quelque chose qui vous caractérise : des données biométriques comme une empreinte digitale ou la reconnaissance faciale.

L'utilisation du MFA renforce la sécurité en rendant plus difficile l'accès non autorisé, même si un mot de passe est compromis.

Tous les utilisateurs du Tenant Azure sont soumis au MFA via les politiques de conditionnal access.

La politique de MFA de l'EntraID sur le tenant autorise seulement deux méthodes :

- Applications Microsoft Authenticator ou Google Authenticator
- Clé de sécurité FIDO2 (YubiKey)

9.7 Usage clés FIDO2

Silae a mis en place une politique stricte d'utilisation de clé FIDO2 Yubikey pour les comptes à hauts privilèges.

Ces comptes appartiennent uniquement à l'équipe dédiée d'administration DevOps en charge des infrastructures.

L'usage des clés FIDO2 YubiKey pour sécuriser les accès administrateurs à Azure repose sur le principe de l'authentification à plusieurs facteurs (MFA) pour renforcer la sécurité des comptes privilégiés.

Les clés FIDO2 YubiKey sont des dispositifs matériels qui permettent une authentification forte, reposant sur un standard ouvert et sécurisé. Elles combinent la possession d'un élément physique (la clé) et une interaction humaine (comme toucher la clé et entrer un PIN) pour valider un accès.

Bien que l'utilisation d'application de MFA (comme Microsoft Authenticator / Google Authenticator) soit déjà un outil de sécurisation important, les clés matérielles comme YubiKey offrent des protections supplémentaires sur six éléments, notamment dans les cas d'accès administrateur où la sécurité est cruciale :

- **Sécurité renforcée contre le phishing**

- **Protection contre les attaques Man-in-The-Middle (MiTM)**
  Protocoles cryptographiques avancés (comme le challenge-response basé sur des clés privées stockées sur le dispositif.)

- **Facteur matériel inviolable**
  Microsoft Authenticator repose sur un téléphone mobile. Si ce dernier est compromis (malware, vol du téléphone, etc.), l'application Authenticator peut être potentiellement vulnérable. Les téléphones peuvent être victimes d'attaques par carte SIM, redirections de SMS, ou d'autres formes de piratage ciblé.

- **Indépendance vis-à-vis du smartphone**
  La clé YubiKey ne dépend pas d'une connexion à Internet, d'une batterie ou d'un appareil mobile pour fonctionner. Elle est autonome et peut être utilisée sur n'importe quel appareil (PC, laptop, tablette.)

- **Absence de dépendance à une connexion Internet ou réseau mobile**
  Les clés YubiKey n'ont pas besoin d'être connectées à Internet ou à un réseau mobile. Elles fonctionnent de manière complètement hors ligne, éliminant les risques liés aux interruptions réseau, au roaming ou à d'autres problèmes de connectivité.

- **Conformité avec des normes de sécurité strictes**
  Les clés YubiKey sont conformes à des normes de sécurité très strictes (comme FIDO2, U2F, PIV). Elles sont particulièrement recommandées pour les organisations devant se conformer à des réglementations de sécurité de haut niveau, comme le RGPD, PCI-DSS, ou encore des exigences gouvernementales.

9.8 Traçabilité des accès

Silae met systématiquement en œuvre tous les mécanismes permettant d'assurer la traçabilité la plus totale.

La traçabilité des accès dans Azure est une fonction clé pour surveiller, auditer et analyser les actions et les accès aux ressources dans l'environnement cloud. Azure propose une

série d'outils et de services qui permettent aux administrateurs et aux équipes de sécurité de suivre de manière détaillée qui accède à quoi, quand, et ce qu'ils ont fait.

Cette traçabilité est cruciale pour la sécurité, la conformité réglementaire et la gestion des accès dans des environnements complexes.

Silae a mis en place les éléments suivants :

9.8.1 Azure Active Directory (Azure AD) Audit Logs

Azure Active Directory (Azure AD) est la solution d'identité centrale d'Azure. Azure AD conserve des journaux d'audit détaillés qui enregistrent chaque action administrative et d'accès utilisateur. Ces logs comprennent :

- **Connexion réussie ou échouée**
  Quand un utilisateur ou un administrateur essaie de se connecter à une ressource Azure, Azure AD enregistre si la connexion a réussi ou échoué.

- **Modifications des permissions**
  Toute modification des rôles d'utilisateurs (ajout/retrait de rôles) est consignée, ce qui permet de savoir qui a modifié les droits d'accès, quand et pour quelle ressource.

- **Modifications d'authentification**
  Tout changement dans les paramètres de sécurité, comme la mise en place d'une authentification multifacteur (MFA) ou l'enregistrement d'un nouveau facteur d'authentification, est enregistré.

- **Activités d'administration**
  Par exemple, l'ajout ou la suppression d'utilisateurs, de groupes ou de stratégies dans Azure AD.

9.8.2 Azure Activity Logs

Les journaux d'activités d'Azure (ou Activity Logs) sont un autre ensemble de logs générés par Azure qui suivent les actions sur les ressources de votre environnement cloud. Ils enregistrent :

- Toutes les actions effectuées sur les ressources : par exemple, la création ou la suppression de machines virtuelles, la modification des configurations de réseau, ou les changements dans les paramètres de stockage.

- Les tentatives d'accès aux ressources : chaque tentative d'accès à une ressource, réussie ou échouée, est enregistrée. Cela inclut les actions initiées par des utilisateurs et les services gérés par Azure.
- Changements de configuration : Tout changement dans la configuration des ressources (réseaux, bases de données, VM, etc.) est consigné.
- Actions par les rôles ou services managés : Les actions effectuées par des applications ou des services dotés d'accès basés sur des rôles (Role-Based Access Control - RBAC) sont également enregistrées, ce qui permet de tracer les actions automatiques ou orchestrées.

La durée de rétention de ces logs est de 90 jours sur l'environnement Azure.
Ils sont exportés vers des comptes de stockage pour augmenter la durée de rétention à un an.

9.8.3 Azure Monitor et Azure Log Analytics

Azure Monitor et Azure Log Analytics permettent de collecter, analyser, et alerter sur les journaux d'activités et les métriques. Azure Monitor est utilisé pour :

- Centraliser les logs : Tous les journaux d'accès (Azure AD, Activity Logs, etc.) sont envoyés dans un storage account pour une analyse plus approfondie.
- Configurer des alertes : Des alertes sont configurées pour informer les administrateurs ou les équipes de sécurité lorsqu'une activité suspecte ou inhabituelle est détectée (par exemple, de nombreuses tentatives d'accès échouées ou des connexions depuis un emplacement inhabituel.)
- Analyser les données : Log Analytics permet de créer des requêtes pour filtrer et analyser les événements d'accès afin d'identifier des tendances, des anomalies ou des violations de sécurité potentielles.

9.8.4 Role-Based Access Control (RBAC) Audit Logs

Azure utilise un modèle RBAC (contrôle d'accès basé sur les rôles) pour accorder des permissions granulaires aux utilisateurs et services. Les logs d'audit RBAC permettent de tracer :

- Qui a reçu quels droits : Les modifications apportées aux rôles RBAC (par exemple, attribuer un rôle d'administrateur à un utilisateur) sont enregistrées.
- Accès aux ressources par les rôles : Cela permet de comprendre si les utilisateurs agissent dans les limites de leurs droits ou non.

9.8.5 Azure Security Center & Defender for Cloud

Azure Security Center et Defender for Cloud fournissent une couche supplémentaire pour surveiller la sécurité et la conformité de nos environnements Azure. Ils permettent :

- D'Analyser les journaux d'accès et de sécurité : En surveillant les logs d'activités et d'accès, le Security Center détecte et signale les menaces potentielles.
- De Détecter les comportements anormaux : Ces outils utilisent des algorithmes d'intelligence artificielle pour détecter des modèles d'accès inhabituels ou des activités qui dévient des comportements normaux.
- De Recommander des mesures de sécurité : Le Security Center fournit des recommandations proactives basées sur les logs, par exemple, en suggérant de renforcer les stratégies d'accès.

9.8.6 Azure Privileged Identity Management (PIM)

Pour les comptes ayant des droits d'accès privilégiés (administrateurs), Azure propose Azure PIM (Privileged Identity Management), un service qui permet de gérer et surveiller l'accès aux rôles privilégiés. PIM fournit des fonctions de traçabilité spécifiques aux accès administrateurs :

- Audit des accès privilégiés : Pour suivre qui a eu accès à des rôles d'administrateurs, quand cet accès a été accordé, et pour combien de temps. PIM permet également d'enregistrer les raisons pour lesquelles un utilisateur a demandé un accès temporaire.
- Rapports d'audit : Les rapports PIM fournissent une vue consolidée des activités des administrateurs et des utilisateurs à privilèges, ce qui facilite les audits et la détection de comportements non conformes.
- Alertes et approbation d'accès : PIM permet de configurer des flux d'approbation pour les demandes d'accès, et d'envoyer des alertes pour surveiller les changements dans les rôles d'administrateurs.

Cette approche permet à Silae de renforcer la sécurité et de maintenir la conformité réglementaire et opérationnelle.

10. CHIFFREMENT

10.1 Périmètre de chiffrement

Toutes les données stockées sur Azure sont systématiquement chiffrées au repos.

Toutes les données en transit sur Azure sont systématiquement chiffrées.

Différentes technologies de chiffrements sont mises en œuvre pas Azure sur l'ensemble de ses solutions. Silae active systématiquement les options de chiffrement sur l'ensemble des services déployés.

Au-delà des chiffrements appliqués aux infrastructures et services, le service My Silae applique un chiffrement sur les données sensibles en base de données.

10.2 Chiffrement des données en transit

La plateforme Azure fournie des services des chiffrements de bout en bout. Le trafic réseau interne entre les différents services et équipements de l'infrastructure est systématiquement chiffré via un protocole sécurisé TLS 1.2

10.3 Chiffrement des bases de données

Les bases de données sont systématiquement chiffrées au repos. Les mécanismes de Chiffrement transparent des données (TDE, Transparent Data Encryption) assurent le chiffrement et le déchiffrement des données et des journaux en temps réel via une clé de chiffrement symétrique.

Les services exploités sont configurés pour utiliser les services de chiffrement au repos de la façon suivante :

- Les disques des serveurs Azure Database pour MySQL, les sauvegardes de bases de données et les fichiers temporaires sont encryptés via le protocole FIPS 140-2 et l'algorithme AES 256 bits.
- Les bases de données sont accessibles uniquement localement (réseau virtuel) et via un protocole sécurisé par TLS 1.2
- Chaque instance PaaS d'Azure Database pour MySQL dispose de sa propre clé de chiffrement.
- Les clés de chiffrement sont stockées dans un coffre-fort numérique à accès restrictif.
- Référence : Security - Azure Database for MySQL | Microsoft Docs https://docs.microsoft.com/en-us/azure/mysql/concepts-security

10.4 Chiffrement des stockages

Les services exploités sont configurés pour utiliser les services de chiffrement de la façon suivante :

- Les disques des machines virtuelles (VMs, groupes de VMs ou AppService) sont des Disques Gérés (Managed Disks) avec chiffrement au repos SSE de type PMK.

- Les services de stockage ne sont accessibles que sur le réseau virtuel interne de chaque groupe de ressources et via des protocoles sécurisés : TLS 1.2, ou SMB avec sécurisation Azure Managed Identities.
- Référence : chiffrement côté serveur de disques managés Azure - Azure Virtual Machines | Microsoft Docs
  https://docs.microsoft.com/fr-fr/azure/virtual-machines/disk-encryption

10.5 Chiffrement des échanges client/serveur

Les applications My Silae Entreprise (Web et Mobiles) ou l'application de bureau My Silae Gestionnaire de Paie déployée sur les stations de travail communiquent systématiquement avec les serveurs via un protocole sécurisé HTTPS.

Au-delà de ce chiffrement du transit, l'application My Silae Gestionnaire de Paie effectue aussi un chiffrement supplémentaire directement dans l'application pour toutes les données échangées entre le client et le serveur.

Ce chiffrement permet de sécuriser l'échange des données dans tous les cas : authentification SSL corrompue ou interceptée (Adversary-in-the-Middle/Man-in-the-Middle.)

Le principe de fonctionnement est basé sur chiffrement asymétrique pour échanger une clé symétrique, puis d'utiliser cette clé symétrique pour chiffrer les données elles-mêmes. Le client et le serveur génèrent localement chacun une paire de clés, et échangent au début la partie publique de la clé, et conservent la partie privée.
C'est une clé RSA de 2048 bits. Une fois que cet échange a été réalisé, au début de la session, ces deux paires de clés ne changent plus pendant toute la durée de la session.
Ensuite l'algorithme utilisé pour chiffrer les données est une variante d'AES, avec une clé de 256 bits en mode CBC (Cipher Block Chaining).

10.6 Responsable du chiffrement et de la gestion des clés

MySilae utilise Azure Key Vault pour gérer et protéger les clés cryptographiques nécessaires au chiffrement des données stockées ou transmises au sein de l'infrastructure.

La rotation des clés pour les comptes de stockage Azure en utilisant des clés gérées par le client (Customer-Managed Keys, CMK) est un processus permettant de renforcer la sécurité des données en renouvelant périodiquement les clés de chiffrement.

Silae implémente les bonnes pratiques associées dans un environnement Azure :

1. **Stockage des clés dans Azure Key Vault** : Les clés CMK pour les comptes de stockage sont stockées dans Azure Key Vault, qui fournit un environnement sécurisé et conforme pour leur gestion. Silae a mis en place une politique de rotation automatique à intervalles réguliers, tous les 6 mois, pour suivre les recommandations des normes ISO 27001, NIST SP 800-57, HIPAA et PCI-DSS.

2. **Rotation automatique** : Azure permet la rotation des clés CMK de manière automatisée.
   Des règles sont définies dans Azure Key Vault pour déclencher la création d'une nouvelle version de la clé à la fréquence de deux fois par an. Une fois une nouvelle clé générée, les comptes de stockage sont configurés pour utiliser automatiquement la nouvelle version.

3. **Surveillance et alertes** : La rotation des clés est suivie par des alertes et des journaux d'audit pour surveiller tout accès ou modification des clés. Ces informations sont utiles pour détecter toute activité anormale ou non autorisée et pour assurer la conformité des processus de gestion des clés.

4. **Validation de la continuité d'accès** : Après chaque rotation de clé, des tests d'accès aux ressources sont implémentés pour s'assurer que les services dépendants peuvent toujours décrypter les données et accéder aux comptes de stockage.

My Silae utilise également Azure Key Vault pour stocker et gérer les **secrets** nécessaires au fonctionnement de ses applications.

Les secrets incluent :

- Les identifiants pour des bases de données ou des API externes.
- Les certificats SSL/TLS pour sécuriser les communications.
- Les tokens d'authentification ou des clés API pour des services tiers.

Exemple : L'application My Silae contient ses "connection strings" stockées en tant que secret dans Azure Key Vault.

Les applications n'accèdent jamais directement aux secrets sensibles via le code. Elles obtiennent une identité managée (identité gérée par Azure Active Directory) qui est utilisée pour accéder au Key Vault sans nécessiter de secrets supplémentaires.
Cela élimine les dépendances aux identifiants codés en dur.

Classification des secrets

Les secrets sont classés selon leur sensibilité et leur criticité.
Les noms de secrets utilisent une convention de nommage stricte pour une identification rapide.

Rotation des secrets

Tous les secrets ont une date d'expiration définie.
Selon la criticité et le type de secret, la durée d'expiration est de 3 mois à 1 an.

Silae a mis en place des politiques de rotation automatique avec des outils intégrés aux pipelines CI/CD pour gérer le renouvellement.

11. TECHNOLOGIES ET MECANISMES DE SURVEILLANCE

11.1 Protection des identités

Les identités des utilisateurs et des applications (app registration) sont supervisées dans Entra ID (Azure AD) pour détecter les comportements suspects sur les comptes à privilèges, les tentatives d'escalade de privilèges, ou des connexions anormales. Cela permet de prévenir les attaques liées aux identités et aux accès.

Au-delà des pratiques mise en œuvre pour la sécurisation des accès et des identités avec Entra ID, **Silae a déployé CrowdStrike Falcon® Identity Threat Detection sur son environnement de production.**

Les alertes remontent dans la console de sécurité CrowdStrike et sont supervisées par les équipes CrowdStrike en charge du SOC Managé.

CrowdStrike Falcon® Identity Threat Detection donne une visibilité sur les attaques et les anomalies basées sur l'identité, en comparant le trafic en temps réel aux lignes de base et aux règles de comportement afin de détecter les attaques et les mouvements latéraux. Via des alertes en temps réel, Falcon Identity Threat Detection offre une visibilité sur les informations d'identification compromises dans les magasins d'identité. La plupart des brèches impliquent des informations d'identification compromises et des mouvements latéraux, la meilleure façon de sécuriser chaque domaine est d'automatiser la détection des menaces et de créer un profil de risque dynamique et des alertes sur le trafic d'identité.

11.2 Posture de sécurité Cloud

Silae utilise les solutions Azure Defender for Cloud et Crowdstrike Cloud Security comme solutions de gestion de la posture de sécurité (Cloud Security Posture Management (CSPM)) et de protection des charges de travail (Cloud Workload Protection Platform (CWPP)).

Ces outils analysent les configurations des ressources Azure et fournissent des recommandations pour améliorer la posture de sécurité. Cela inclut l'identification des vulnérabilités et des configurations non sécurisées. Cela permet aussi de repérer toute erreur de configuration potentiellement apportée par un administrateur.

Silae utilise Azure Defender pour surveiller les ressources critiques (base de données MySQL, compte de stockage) et les points d'entrée réseau (Application Gateway, Azure Front Door).

Grâce à l'intégration d'analyses avancées et du machine learning, nous pouvons détecter des comportements anormaux qui pourraient indiquer une attaque en cours, comme des tentatives d'accès en provenance d'une source ou à des horaires inhabituels, un volume inhabituel de données transférés, etc.

Un antivirus est systématiquement déployé sur tous les serveurs applicatifs.

L'antivirus Falcon® Prevent de l'éditeur CrowdStrike est l'antivirus de référence pour sécuriser le service My Silae.

Les alertes remontent dans la console de sécurité CrowdStrike et sont supervisées par les équipes CrowdStrike en charge du SOC Managé.

Falcon Prevent offre une prévention complète contre les logiciels malveillants et les attaques sans logiciels malveillants. Ses capacités antivirales étendues de nouvelle génération (NGAV) comprennent la capacité d'identifier les logiciels malveillants connus, l'apprentissage automatique pour les logiciels malveillants inconnus, le blocage des exploits et des techniques comportementales exclusives d'indicateurs d'attaque (IOA). Outre la prévention des exécutions malveillantes, Falcon Prevent est une solution complète qui inclut une visibilité en temps réel et fournit le contexte de toutes les activités liées aux menaces.

CrowdStrike Falcon® est le seul fournisseur de cybersécurité que Gartner, Forrester et IDC ont tous reconnu comme leader dans la sécurité moderne des terminaux. CrowdStrike Falcon® obtient régulièrement les meilleurs résultats lors de tests effectués par des tiers, notamment SE Labs, AV Comparatives et AV-Test. CrowdStrike est approuvé par AV Comparatives, avec un taux de blocage des logiciels malveillants de 99,2 % et zéro faux positif.

Falcon Prevent ne s'appuie pas sur des signatures. Il n'est pas nécessaire de déployer quotidiennement des fichiers de mise à jour des définitions de virus sur tous les terminaux.

Falcon Prevent s'appuie sur l'apprentissage automatique pour identifier et bloquer les logiciels malveillants. L'apprentissage automatique est particulièrement efficace pour bloquer les nouveaux logiciels malveillants, polymorphes ou obscurcis.

Falcon Prevent utilise des indicateurs d'attaque (Indicators of Attack- IOA) pour identifier les menaces en fonction de leur comportement, quels que soient les logiciels malveillants ou les outils utilisés. La compréhension des séquences de comportement malveillant permet à Falcon Prevent d'arrêter les attaques qui vont au-delà des logiciels malveillants.

Les exemples incluent la protection contre les mouvements latéraux, les attaques webshell et les attaques sans fichier.
Falcon Prevent élimine les angles morts grâce à des analyses de la mémoire très performantes, supprimant ainsi les contraintes de performance de l'analyse traditionnelle de la mémoire, ce qui permet aux menaces sans logiciels malveillants de se cacher nulle part.

Les événements peuvent être contextualisés à l'aide de renseignements intégrés sur les menaces, fournissant des détails sur l'adversaire attribué et toute autre information connue sur l'attaque.

Les alertes remontent dans la console de sécurité CrowdStrike et sont supervisées par les équipes CrowdStrike en charge du SOC Managé.

Références
https://www.crowdstrike.com/products/endpoint-security/falcon-prevent-antivirus/faq/
https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/

11.3 Stratégie Antimalware

Pour gérer la menace malware, Silae a implémenté une stratégie de cybersécurité multicouche en combinant des services Microsoft Defender et des EDR CrowdStrike

Cette approche combinée permet de prévenir, détecter, répondre et analyser efficacement les incidents de sécurité, garantissant ainsi une protection complète des données et des systèmes.

La stratégie Antimalware de Silae repose principalement :

- Sur l'ensemble des services utilisés pour la protection des services et notamment les EDR Crowdstike ou les différentes solutions Microsoft Defender déployées en production (Microsoft Defender for Storage, Microsoft Defender for App Service, Microsoft Defender for SQL, Microsoft Defender for Cloud.)
- Sur une stratégie de sauvegardes des données systématiquement géoredondée et immutable.

Prévention de la menace

- **Microsoft Defender**

- Protection en temps réel : Microsoft Defender propose une protection en temps réel contre les malwares, en bloquant les fichiers malveillants avant qu'ils ne puissent être exécutés.
- Analyse comportementale : Microsoft Defender utilise des techniques d'apprentissage automatique pour détecter des comportements suspects, contribuant ainsi à prévenir les infections par des malwares.

- **CrowdStrike EDR**

  - Blocage des menaces avancées : CrowdStrike utilise une combinaison de détection basée sur les signatures et l'analyse comportementale pour identifier et bloquer les malwares avant qu'ils ne causent des dommages.

Détection proactive

Les deux outils envoient des alertes en temps réel vers le SOC Managé en cas de détection de menaces et collectent des journaux d'activité qui peuvent être analysés pour détecter des anomalies.
CrowdStrike offre une visibilité en temps réel sur l'activité des endpoints, facilitant la détection rapide des malwares.

Réponse aux incidents

- Remédiation automatisée : Des plans d'actions automatisés sont implémentés pour éliminer les malwares détectés, minimisant l'impact sur les opérations.
- Isolation des appareils : En cas de détection d'une menace, les VM ou les équipements compromis sont mis en quarantaine pour éviter la propagation.

11.4 Stratégie Anti DdoS

Silae applique les stratégies de protection anti-DDoS intégrées dans les infrastructures Azure.

Chaque service qui expose une adresse IP publique est inclus automatiquement dans le système anti-DDoS.
En particulier Silae n'expose sur Internet que les services suivants : Azure Frontdoor, App Gateway, App Service et Azure Firewall.

Les fonctionnalités anti-DDoS appliquées sont :

- Surveillance continue : Le trafic entrant vers les adresses IP publiques est constamment surveillé pour détecter des anomalies indiquant une attaque DDoS.
- Atténuation automatique : En cas de détection d'une attaque DDoS, Azure commence immédiatement à atténuer le trafic suspect. Cela inclut des mécanismes

comme le filtrage basé sur le volume de trafic, les types de protocoles, et les signatures d'attaque connues.

- Protection du réseau : La protection DDoS s'applique sur le périmètre du réseau Azure, ce qui signifie que les attaques sont gérées au niveau des datacenters Azure avant même d'atteindre les ressources de Silae.
  Cela inclut :
  - La limitation du trafic volumétrique : les pics soudains de trafic massifs générés par des attaques DDoS volumétriques, qui visent à saturer la bande passante ou les ressources réseau, sont limités.
  - Le filtrage par taux de connexion : Les attaques qui impliquent un grand nombre de connexions simultanées (par exemple, SYN flood) sont filtrées pour éviter que les ressources ne soient submergées par un grand volume de requêtes non légitimes.
  - L'absorption des attaques au niveau global : Grâce à l'infrastructure globale d'Azure, les attaques volumétriques sont absorbées avant de perturber les ressources de Silae. Azure dispose d'une capacité de mitigation de DDoS à très grande échelle répartie sur ses datacenters.

11.5 Pare-feu et sécurisation des réseaux

Silae utilise ensemble les services NSG et Azure Firewall pour créer une couche de sécurité robuste permettant d'accéder aux ressources Azure.

Les NSG peuvent gérer le trafic au niveau du réseau, tandis qu'Azure Firewall fournit une protection plus approfondie et centralisée, permettant une approche de défense en profondeur.

Les Network Security Groups (NSG) permettent de définir des règles de sécurité qui contrôlent le trafic entrant et sortant vers les ressources Azure, comme les machines virtuelles et les sous-réseaux. Silae définit les règles basées sur des adresses IP, des ports et des protocoles propres à chaque plateforme de service.

En complément des NSG, Silae utilise le service Azure Firewall pour fournir une gestion plus avancée des règles réseau, avec des capacités d'inspection approfondie des paquets.

L'administration centralisée permet à Silae de définir des règles de filtrage qui s'appliquent à tout le trafic vers et depuis Azure. Cela inclut des règles basées sur des applications et des URL

En contrôle, Silae utilise Azure Network Watcher pour surveiller et diagnostiquer les règles de NSG, notamment en vérifiant régulièrement les journaux de flux réseau.

11.6 Web Application Firewall (WAF)

Silae utilise la fonctionnalité Web Application Firewall en combinaison avec les services d'Application Gateway pour sécuriser les flux entrants sur les plateformes de service.

Cela permet de filtrer le trafic HTTP/HTTPS entrant et de protéger les applications contre diverses menaces. Silae utilise un jeu de règles OWASP, basées sur le projet OWASP ModSecurity Core Rule Set (CRS). Ces règles aident à protéger contre des vulnérabilités courantes comme l'injection SQL, les scripts intersites (XSS), etc.

Des alertes basées sur les événements enregistrés par le WAF sont configurées pour remonter dans Azure Monitor.

11.7 Alertes Intrusion

Les alertes d'intrusion sur Azure sont des notifications automatiques qui informent les administrateurs et les équipes de sécurité de Silae ou du SOC Managé CrowdStrike lorsqu'une activité suspecte ou potentiellement malveillante est détectée dans l'infrastructure. Ces alertes sont principalement générées par des solutions de sécurité intégrées comme Microsoft Defender for Cloud et Crowdstrike.

Les alertes peuvent provenir de plusieurs sources de sécurité sur Azure, notamment :

- **Microsoft Defender for Cloud** : Ce service analyse les ressources Azure de Silae (machines virtuelles, bases de données, réseaux, etc.) et génère des alertes de sécurité en fonction des anomalies détectées. Il couvre une large gamme de menaces, y compris des intrusions potentielles, des accès non autorisés, des logiciels malveillants et des failles de configuration.

- **Azure Firewall et NSG (Network Security Group)** : Ces composants réseau peuvent générer des alertes en cas de détection de trafic suspect ou non autorisé, par exemple, des scans de ports ou des tentatives d'accès non autorisées.

- **Azure Active Directory (Entra ID)** : Azure AD (Entra ID) peut générer des alertes sur des comportements suspects liés aux identités et aux authentifications, comme des tentatives de connexion inhabituelles, des escalades de privilèges, ou des connexions depuis des emplacements géographiques inhabituels.

Types d'alertes d'intrusion courantes

Voici quelques exemples d'alertes supervisées par Silae : tentative d'escalade de privilèges, activité réseau suspecte, tentatives de connexion non autorisées, activité suspecte sur les ressources de stockage.

Réponse automatisée et actions correctives

Azure et CrowdStrike proposent des mécanismes pour non seulement détecter les intrusions, mais aussi y répondre automatiquement. Silae a configuré des playbooks pour déclencher des actions en réponse aux alertes, telles que : Bloquer des adresses IP, Révoquer des accès utilisateurs, Mettre en quarantaine des machines virtuelles.

Rôle de l'intelligence artificielle (IA) et du machine learning

L'IA et le machine learning sont intégrés dans les solutions comme Microsoft Defender et CrowsdStrike pour améliorer la détection des intrusions. L'IA analyse en permanence les modèles de comportement et identifie les anomalies qui pourraient passer inaperçues par des systèmes de détection traditionnels. Ces technologies permettent d'**Identifier des schémas de comportement** qui pourraient indiquer des activités malveillantes ou des tentatives d'intrusion et de **Réduire les faux positifs** en affinant les modèles de détection au fil du temps.

En synthèse, les **alertes d'intrusion** sont des notifications générées par plusieurs solutions de sécurité pour informer les administrateurs de tentatives d'accès non autorisé, de comportement réseau suspect, ou d'activités inhabituelles dans les environnements cloud de Silae. Elles sont centrales pour la surveillance proactive et la réponse aux incidents.

12. SUPERVISION DE LA SECURITE

12.1 Centre Opérationnel de Sécurité (SOC & MDR)

Les infrastructures Silae sont supervisées par un SOC Managé (Centre Opérationnel de Sécurité / Security Operations Centers) géré par les équipes CrowdStrike via l'offre de service CrowdStrike Falcon Complete. Au-delà du SOC, CrowdStrike Falcon Complete intègre aussi un service de détection et de réponse gérées (Managed Detection and Response (MDR)).

La supervision et la gestion de la réponse aux incidents sont opérées 24h sur 24 et 7 jours sur 7 par des experts sécurité de CrowdStrike.

Un mode opératoire (Operating Model) et une stratégie de réponse aux incidents ont été mis en place avec Crowdstrike pour définir la posture de remédiation à adopter en fonction de la criticité de l'incident identifié. Le mode opératoire intègre des contres mesures

pouvant aller jusqu'à l'extinction des ressources dans certains scénarios critiques afin de limiter une propagation par exemple.

Les équipes en charge sur SOC Managé de Crowdstike sont en relation permanente avec les équipes DevOps de Silae. Une stratégie d'escalade est en place avec différents intervenants Silae allant des DevOps (astreintes) aux Ingénieurs Sécurité et jusqu'à la Direction Technique.

Référence
https://www.crowdstrike.fr/services/managed-services/falcon-complete/

12.2 Astreinte technique

Les opérateurs DevOps Silae sont mobilisés en permanence via une politique d'astreinte contractualisée et planifiée.

Silae dispose en permanence et a minima d'un opérateur en astreinte, 24h sur 24 et 7 jours sur 7.

L'astreinte s'applique aussi pendant les jours fériés. Le calendrier d'astreinte est piloté automatiquement via l'application PagerDuty et les alertes de production sont remontées à l'opérateur via différents mécanismes (émail, SMS, appel téléphonique) en fonction de l'horaire et de la criticité de l'alerte.

L'astreinte est aussi directement intégrée dans la stratégie d'escalade du SOC Managé.

13. INFRASTRUCTURES CLOUD

Silae a adopté un ensemble de ressources Azure pour répondre aux besoins de ses infrastructures cloud.

Ces services, allant des machines virtuelles à la gestion des identités, permettent de garantir une haute disponibilité, une sécurité renforcée et une gestion optimisée des applications et données de Silae.

Grâce à ces services, Silae peut faire évoluer rapidement les infrastructures et les applications tout en maintenant des standards élevés de performance, de scalabilité et de fiabilité.

Voici une liste des services utilisés. Cette liste est donnée à titre indicatif et Silae se réserve le droit de mettre en œuvre de nouveaux services sans préavis pour garantir la meilleure qualité de service possible.

- **Virtual Machine (VM)**
  Une VM est une ressource informatique dédiée qui exécute des applications ou des systèmes d'exploitation sur Azure. Elle permet de créer un environnement flexible et évolutif pour diverses applications en définissant la taille, les ressources CPU/mémoire, et la gestion du stockage.

- **Virtual Machine Scale Set (VMSS)**
  Un VMSS permet de déployer et de gérer un ensemble de VMs identiques, facilitant l'auto-scaling et la haute disponibilité. VMSS est conçu pour gérer automatiquement l'ajout ou la suppression de VMs en fonction de la demande et est souvent utilisé dans des architectures d'applications distribuées.

- **MySQL Flexible Server**
  Un service de base de données relationnelle qui offre des options de déploiement flexible pour MySQL sur Azure. Il permet de configurer des instances dans des zones de disponibilité pour la redondance et la résilience, avec des options de scaling, de sauvegarde et restauration automatique.

- **Service Bus**
  Azure Service Bus est une solution de messagerie cloud fiable et sécurisée, conçue pour intégrer de manière fluide les applications et services distribués. Elle garantit une communication asynchrone performante avec une haute disponibilité et une gestion simplifiée des files d'attente, des sujets et des abonnements. Idéale pour des architectures complexes, elle assure une scalabilité et une résilience adaptées aux besoins critiques de Silae. Azure Service Bus contribue à la sécurité générale on cloisonnant les différents services d'un système distribué.

- **Application Gateway**
  Service d'équilibrage de charge de niveau applicatif (couche 7) qui distribue le trafic pour les applications web. Il offre des fonctionnalités telles que le routage basé sur des chemins d'URL, la répartition de charge, et des capacités de Web Application Firewall (WAF) pour protéger les applications contre les attaques.

- **Storage Account**
  Azure Storage Account fournit un stockage dans le cloud hautement disponible, durable et scalable. Il prend en charge plusieurs types de stockage : Blobs (fichiers non structurés), Tables (données NoSQL), Files (système de fichiers partagé) et Queues (systèmes de messagerie).

- **Key Vault**
  Key Vault est un service permettant de gérer les secrets (mots de passe, clés d'API), les certificats et les clés cryptographiques. Il permet un contrôle d'accès strict et des journaux d'audit pour sécuriser les informations sensibles dans une organisation.

- **App Configuration**
  Un service de gestion de configuration centralisée pour les applications Azure, qui permet de stocker et de distribuer les paramètres de configuration dynamiquement à travers plusieurs environnements d'application, facilitant la gestion des versions et des déploiements.

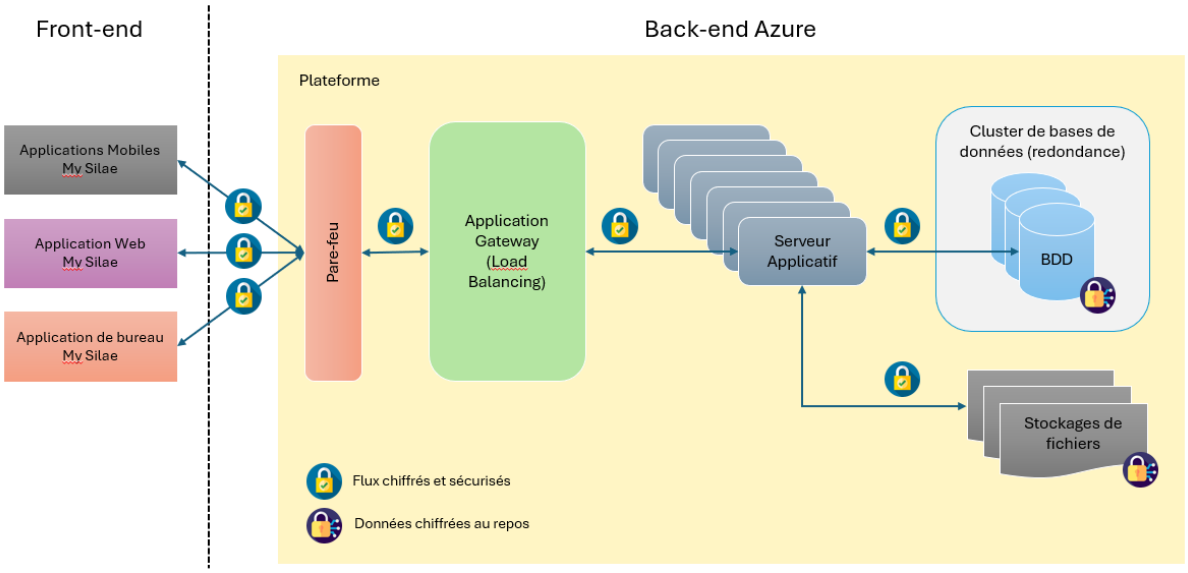
- **Application Insights**
  Service de télémétrie qui fait partie d'Azure Monitor. Il collecte des données sur les performances et les erreurs des applications afin d'offrir des insights détaillés pour améliorer les performances et détecter les anomalies.

- **Managed Identity**
  L'identité managée est une identité gérée par Azure distincte des identités utilisateur traditionnelles, utilisée par les services et applications pour accéder à d'autres ressources Azure sans avoir besoin de gérer des secrets ou des clés. Elle s'intègre facilement avec des services comme Key Vault, Storage et SQL Database pour sécuriser les connexions.

14. SCHEMA D'ARCHITECTURE HAUT NIVEAU

Le schéma haut niveau ci-dessous reprend les principaux éléments d'architectures et les flux entre les différents services.

Ce schéma est volontairement simplifié car Silae ne souhaite pas divulguer l'exhaustivité des services mis en œuvre pour garantir la confidentialité de ses choix d'architecture.



15. SOLUTIONS D'AUTHENTIFICATION (APPLICATIONS)

15.1 Authentification par mot de passe

L'application My Silae fournit un mécanisme d'authentification universel via identifiant et mot de passe.

15.1.1 Politique de mot de passe

Une politique de mot de passe par défaut est en vigueur dans l'application.
Cette politique est conforme aux exigences de la CNIL.

Attention, la politique de mot de passe définie ne s'applique pas si une connexion SSO est configurée et activée dans l'application. Dans ce cas, c'est le fournisseur identité (Microsoft/Google/Okta/etc.) du client qui pilote la politique de mot de passe ou les conditions de l'authentification multifactorielle (MFA) des utilisateurs.

La politique de mot de passe n'est pas modifiable. Elle est gérée par Silae et elle est susceptible d'évoluer pour suivre les recommandations de la CNIL. Une évolution entraînera une procédure de mise à jour du mot de passe à tous les utilisateurs lors de la connexion.

Voici les obligations liées à cette politique :

- Au moins une minuscule (a-z).
- Au moins une majuscule (A-Z).
- Au moins un chiffre (0-9).
- Au moins deux caractères spéciaux (&~#'{([-|`_\^@)]=+}^$%*!:/;.,?<>).
- Les caractères accentués sont autorisés.
- La longueur minimale du mot de passe est de 12 caractères.
- L'utilisateur sera bloqué au bout de 3 saisies d'un mot de passe incorrect.
- L'utilisateur sera débloqué automatiquement au bout de 30 minutes.
- L'utilisateur ne pourra réutiliser le même mot de passe (sauvegarde des 3 derniers).

15.1.2 Mot de passe oublié

Les utilisateurs de l'application peuvent réinitialiser ou changer librement et en autonomie leur mot de passe avec une fonctionnalité intégrée à la mire de connexion. Cette procédure respecte les normes en vigueur :

- L’énumération des identifiants n’est pas possible dans la mire de connexion (message générique d’erreur.)
- Si l'utilisateur fourni 3 identifiants invalides, l'application se ferme automatiquement, l'obligeant à relancer l'application.
- La procédure implique un partage de code expédié à l’adresse email de l’utilisateur
- Le code expédié n’est valide que 5 minutes
- La saisie du code est contrôlée, l’application se ferme au bout de 3 tentatives invalides
- Les mots de passes ne sont jamais partagés en clair ou affichées

15.1.3 Chiffrement des mots de passe

Les mots de passe de connexion de My Silae sont stockés en base de données dans le respect des préconisations de la CNIL :

« Lorsqu'il est conservé, tout mot de passe utile à la vérification de l'authentification doit être préalablement transformé au moyen d'une fonction cryptographique spécialisée, non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant un " sel " et des paramètres relatifs aux coûts en temps et/ou en mémoire nécessaire à son attaque.
Le sel devrait être généré aléatoirement et avoir une longueur minimale de 128 bits. Il est généré pour chaque utilisateur et stocké dans la même base de données que les mots de passe. »
(Référence : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046432885)

Le hachage des mots de passe My Silae est réalisé selon la norme PBKDF2 (Password-Based Key Derivation Function) avec un algorithme HMAC-SHA512 et un sel de 128-bit.
La fonction de dérivation de clé est exécutée 100 000 fois pour ralentir les attaques par force brute en augmentant le coût de calcul pour chaque tentative de mot de passe.

Cette configuration garantit un niveau de sécurité élevé en rendant le calcul des mots de passe coûteux pour les attaquants, tout en produisant des clés cryptographiques fortes.

15.1.4 Protection contre les attaques force brute

L'application My Silae dispose d'un mécanisme de protection contre les attaques Force Brute. L'utilisateur est bloqué 30 minutes après 3 tentatives de mot de passe en erreur. Les tentatives de connexions en erreurs sont systématiquement enregistrées dans les historiques de connexion.

15.1.5 Expiration de mot de passe

Il est possible de configurer une expiration du mot de passe en nombre de jours à partir de la date de création ou de modification du mot de passe. Par défaut, l'application n'impose pas d'expiration des mots de passe.

Cette approche n'est plus recommandée par la CNIL :
De plus en plus d'études démontrent que forcer l'utilisateur à changer son mot de passe à une fréquence régulière n'est pas une mesure réellement efficace. Les stratégies utilisées par les utilisateurs pour s'adapter aux politiques d'expiration de mots de passe sont généralement prévisibles et abaissent le niveau de sécurité effectif. En effet, la majorité des participants utilise une version légèrement modifiée de leur mot de passe précédent, par exemple en ajoutant un chiffre à la fin. Les bénéfices en termes de sécurité sont ainsi mineurs et largement contrebalancés par l'expérience utilisateur négative.
https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite

15.2 Single Sign On (Authentification Unique)

L'application My Silae Gestionnaire de Paie intègre un module d'Authentification Externe. Il est possible de configurer une Authentification Externe pour se connecter à un annuaire géré par provider Microsoft, Google ou Okta via des protocoles OIDC (OpenID Connect) ou SAML V2. La mise en place de ces fonctionnalités est décrite dans la documentation du produit.

15.3 Authentification Multifacteur (MFA)

L'application My Silae Gestionnaire de Paie ne fournit pas nativement de mécanisme MFA pour l'authentification par mot de passe.

La mise en place d'une authentification MFA nécessite de configurer une authentification externe (celle du partenaire ou du client final) et de configurer une politique MFA au travers du provider SSO.

15.4 Historisation des connexions utilisateurs

Les connexions des utilisateurs sont enregistrées dans un historique de connexion accessible dans l'administration de My Silae GP. La date, l'heure, l'identifiant et l'adresse IP source de la connexion sont systématiquement enregistrés.

Au-delà des informations de connexions, toutes les actions critiques effectuées dans l'application par les utilisateurs (modifications importantes, suppression, etc.) sont aussi enregistrées.

Les données historisées de connexion, de modification, d'usage, etc. sont conservées pendant 1 an. La consultation est uniquement accessible par les Collaborateurs du domaine de paie disposant d'un droit d'administration.

16. Sauvegarde et Restauration des Stockages et des Fichiers

16.1 En synthèse

- Les comptes de stockage sont conservés 365 jours (suppression réversible.)
- Les fichiers eux-mêmes sont sauvegardés quotidiennement et chaque sauvegarde est conservée 30 jours.
- La sauvegarde est assurée au niveau des partages de fichiers et sur les services de stockage eux-mêmes pour assurer la sauvegarde la plus complète afin de répondre à tous les scénarios de suppression volontaires ou involontaires de fichiers ou de services.
- Le RSV (Recovery Service Vault) est configuré pour être immutable, c'est-à-dire qu'aucune modification n'est possible sur aucune donnée sauvegardée, et ce paramètre est permanent, il n'est plus possible de retirer ce paramètre d'immutabilité.

16.2 Redondance des sauvegardes

Les sauvegardes sont géoredondées sur les régions Azure France Central et France South via le service GRS (Geo-Redundant Storage).

16.3 Sauvegarde des fichiers

Les fichiers sont sauvegardés sur des partages de fichiers créés dans des comptes de stockage « Azure Files ».

Un mécanisme de suppression réversible (Soft Delete en anglais) est configuré sur les partages de fichiers Azure Files et permet de restaurer les comptes de stockage supprimés pendant 365 jours.

La suppression réversible permet de récupérer les fichiers lorsqu'ils ont été supprimés par erreur par une application ou un utilisateur. Le mécanisme de suppression réversible ne supprime pas les données physiquement, elles sont mises dans un état de sommeil et invisible aux différents services. La suppression définitive est réalisée à la fin de la période de réversibilité.

Les spécifications techniques sont disponibles ici :
https://learn.microsoft.com/fr-fr/azure/storage/files/storage-files-prevent-file-share-deletion

16.4 Modification des fichiers

Une politique de sauvegarde est mise en œuvre au niveau des partages de fichiers dans les comptes de stockage qui hébergent les fichiers de l'application.

Cette politique consiste en une sauvegarde quotidienne avec une rétention à 30 jours.
https://learn.microsoft.com/fr-fr/azure/backup/azure-file-share-backup-overview

16.5 Sécurisation des services de stockage

Les services Azure Files exploités par Silae sont sécurisés et sauvegardés avec Azure Recovery Service. L'intégralité des stockages et des services de stockage sont sauvegardés.

Ce mécanisme offre une double protection au niveau des fichiers et au niveau des services opérant ces fichiers. Azure Recovery Service expose un mécanisme de suppression réversible exploité par Silae. Si un intervenant malveillant supprime complètement un compte de stockage (ou même si le compte de stockage est accidentellement supprimé), les données du service sont intégralement conservées pendant 365 jours, ce qui permet la récupération de cet élément.

Les spécifications techniques d'Azure Recovery Service sont disponibles ici :
https://docs.microsoft.com/fr-fr/azure/backup/backup-azure-recovery-services-vault-overview

Les sauvegardes de fichiers sont systématiquement chiffrées au repos avec des clés de chiffrement basées sur l'algorithme AES 256.

16.6 Restauration des fichiers

Silae s'engage à restaurer les fichiers sur la base de la sauvegarde la plus appropriée avec un RTO (Recovery Time Objective) maximum de 24 heures, et ce, dans les meilleurs délais.

Restauration d'un fichier supprimé

- Le RPO minimal pour la restauration d'un fichier correspond à sa date de suppression dans la limite de 365 jours.

Restauration d'une version antérieure d'un fichier

- Le RPO minimal pour la restauration d'une version antérieure d'un fichier correspond à l'heure de la dernière sauvegarde dans la limite de 24 heures.
- La perte de données maximale est donc de 24 heures.

17. SAUVEGARDE ET RESTAURATION DES BASES DE DONNEES

Les sauvegardes et les restaurations sont essentielles de la stratégie de continuité d'activité de Silae, car elles protègent les données contre toute corruption ou suppression accidentelle.

Silae est responsable de la conduite des sauvegardes et des restaurations afin de sécuriser les données du Client.

17.1 En synthèse

- Silae s'appuie sur les mécanismes exposés par le service « Azure Database for MySQL Flexible Server ».
- Des sauvegardes complètes des bases de données sont générées quotidiennement et conservé pendant 35 jours sur des stockages dédiés.
- Des sauvegardes des logs de transactions sont réalisées toutes les cinq minutes.
- Les bases de données peuvent être restaurées à partir de ces points de restauration sur un serveur MySQL provisionné sur demande.
- Les spécifications techniques sont disponibles ici : https://learn.microsoft.com/fr-fr/azure/mysql/flexible-server/concepts-backup-restore

17.2 Redondance des sauvegardes

Les sauvegardes sont redondées plusieurs fois et au sein de la zone géographique définie dans la section « Localisation de l'exploitation ». Elles sont géoredondées (via GRS, Geo-Redundant Storage) et protégées contre les événements planifiés et non planifiés, notamment les défaillances matérielles transitoires, les pannes de réseau, les pannes électriques et les catastrophes naturelles.

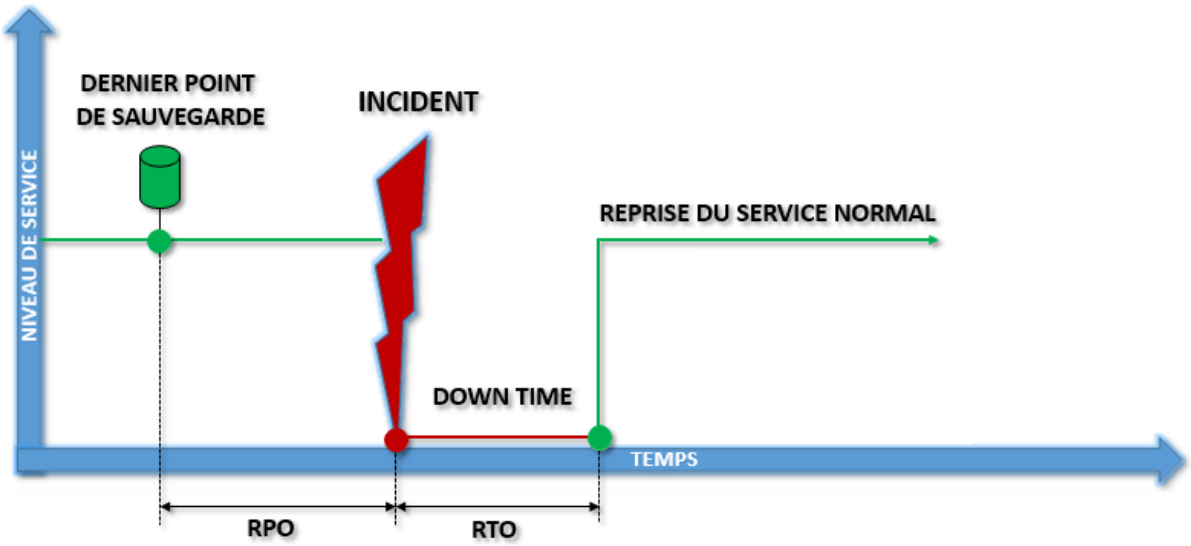
17.3 Fréquence des sauvegardes

Les sauvegardes des bases de données sont effectuées une fois par jour et avec une historisation de 35 jours.

Au-delà de cette période de 35 jours, Silae conserve une sauvegarde mensuelle pour les 12 derniers mois (la politique de rétention actuelle est mentionnée ici à titre indicatif et pourrait évoluer.) Cette sauvegarde mensuelle est déportée sur un compte de stockage de fichiers répondant aux exigences de sauvegarde (géoredondance et immutabilité) des fichiers décrites dans ce document.

17.4 Restauration des Bases de Données (RTO/RPO)

Silae s'engage à restaurer les sauvegardes les plus appropriées avec un RTO (Recovery Time Objective) maximum de 24 heures, et ce, dans les meilleurs délais.



Le RTO de 24h démarre à partir de la confirmation de la demande de restauration de la base de données. 24h00 est un temps maximum. Si une demande est réalisée le lundi à 9H00, la sauvegarde sera restaurée au plus tard mardi à 9h00. Cette fenêtre de temps est assez large car il est impossible de préjuger de la taille de la base de données du Client. Silae dispose de sauvegardes clients qu'il est possible de restaurer en 15 minutes et d'autres (avec 10 ans d'historique) qui peuvent nécessiter plusieurs heures.

Le service est totalement inaccessible pendant toute la période de la restauration.

Le RPO minimal pour la restauration d'une base de données est d'une heure. En effet, Silae dispose de 35 jours d'historisation et de logs transactionnels qui permettent de cibler une heure donnée.

La perte de données maximale est donc d'une heure.

Le RPO peut être n'importe quelle heure sur les 35 derniers jours. Au-delàs de ces 35 jours, Silae peut s'appuyer sur une des bases de données historisées chaque mois sur les 12 derniers mois.

18. PLAN DE REPRISE D'ACTIVITE

18.1 Mise en œuvre

Silae met en œuvre des moyens et des investissements importants pour sécuriser ses infrastructures et ses opérations. Le cloisonnement des abonnements et des services mis en œuvre dans nos infrastructures permet de limiter l'impact de la propagation d'un incident.

Le Plan de Reprise d'Activité (PRA) Silae est basé sur :

- **La géoredondance des sauvegardes** entre les régions France Central et France South. Le stockage géoredondant (GRS - Geo-Redundant Storage) garantie que des sauvegardes (bases de données et fichiers) sont systématiquement disponibles dans plusieurs Datacenters.
- **Des sauvegardes sur des stockages isolés et immutables**. L'immutabilité (protection de type WORM (Write Once Read Many)) des sauvegardes est activée pour garantir que les données ne puissent jamais être modifiées ou altéré directement dans les sauvegardes. L'immutabilité est un moyen de protection éprouvé contre les attaques de type Ransomware ou Cryptolocker.
- **Différents formats de sauvegardes**. Au-delà des sauvegardes natives des bases de données proposées par le service Azure Database for MySQL, Silae opère des sauvegardes de type DUMP en parallèle, ces sauvegardes sont déposées sur des Storage Account, sauvegardés en GRS et immutables.
- **Et un ensemble de procédure permettant le redéploiement** d'une architecture de production 100% opérationnelle.

Le PRA est basé les mêmes méthodes d'approvisionnement que celles appliquées à l'environnement de production et repose notamment sur l'ensemble des scripts (IAC) et des procédures permettant de redéployer une infrastructure identique à la production.

Un PRA secondaire et permanent est en cours d'étude pour opérer la production et les sauvegardes dans une région Azure située dans l'Union Européenne en dehors de la Région Azure de référence pour l'exploitation actuelle.

Des études sont en cours pour valider la possibilité de mettre en place un PCA (Plan de Continuité d'Activité) dans un autre Région Azure en Europe.

18.2 Durée maximale d'interruption admissible

La durée maximale d'interruption (Recovery Time Objective (RTO)) est fixée à 48 heures et est conditionnée par :

- Le temps d'approvisionnement des infrastructures Azure à restaurer,
- le temps nécessaire à la remontée des sauvegardes
- les procédures de validation opérationnelles avant la remise en service.

Le temps indiqué ici est dans le « pire de scénario » (« worst case scenario »). La durée de remise en production peut réduire significativement en fonction des capacités d'Azure dans le cycle d'approvisionnement.

Silae étudie des solutions alternatives pour pré-approvisionner des équipements et réduire ce délai.

19. AUDIT DE SECURITE (PENTEST)

Les conditions d'audit du service My Silae sont décrites dans le Plan d'Assurance Sécurité Global de Silae.

20. MANAGEMENT DES MISES A JOUR ET VULNERABILITES

20.1 IaaS Patch Management (Machines Virtuelles)

Silae utilise Azure Update Manager qui est l'outil intégré à Azure pour la gestion des mises à jour et l'application des correctifs aux machines virtuelles.

Des politiques différentes sont appliquées en fonction du type d'environnement (Production/Hors production) et par typologie fonctionnelle des VM.

Mise à jour des systèmes d'exploitation

Globalement, les mises à jour des systèmes d'exploitation (OS) sont installées sur les environnements Hors Production la semaine suivante leur date de sortie puis dans les environnements de Production la semaine suivante si aucune régression n'est constatée dans l'intervalle.

Dans tous les cas, les mises à jour OS sont systématiquement installées dans les 30 jours qui suivent la date de publication.

Gestion des mises à jour pour les vulnérabilités Zero-Day

Les vulnérabilités Zero-day sont des vulnérabilités critiques qui n'ont pas de correctif immédiatement disponible au moment de leur découverte. Leur gestion repose sur une stratégie proactive et réactive.

Dès qu'un correctif est disponible pour une faille Zero-day, il est appliqué immédiatement. Azure Update Manager permet de déployer rapidement ces correctifs, garantissant que toutes les VMs soient sécurisées dès que les correctifs sont publiés.

L'usage de stratégie de distribution de charge (Load Balancing) et de machines virtuelles à la demande (Scaleset) permet de déployer rapidement des correctifs sans altérer la qualité du service Silae.

20.2 PaaS Patch Management (Services Managés)

Les services **PaaS (Platform as a Service)** sur Azure (MySQL Flexible Server, Application Gateway, etc.), sont managés directement par Microsoft. Cela inclut, entre autres : les maintenances applicatives, les correctifs de sécurité, les règles de sécurité (WAF), les optimisations de performance, les mises à jour de firmware, les adaptations de conformité, etc.

Les équipes de Silae ne sont pas impliquées dans la gestion des mises à jour liées à ces services et bénéficient directement de toute l'expertise de Microsoft dans ce domaine.

Dans certains cas, les équipes de Silae peuvent indiquer la période ou l'heure de mise à jour le plus appropriée pour assurer la disponibilité du service concerné.

La seule exception aux mises à jour automatiques concerne les mises à jour majeures du moteur des bases de données (par exemple, MySQL 8.x vers 9.x). Ce type de mise à jour n'est pas automatique et nécessite une planification manuelle car elle peut introduire des changements incompatibles avec les applications existantes.

21. APPLICATIONS & APIS MY SILAE

21.1 Application Web My Silae Entreprise

L'application Web My Silae Entreprise est accessible via l'adresse :
https://my.silae.fr/

L'application repose sur l'usage du socle APIs Silae. Elle bénéficie des infrastructures Azure et de tous les mécanismes de sécurité exposés dans ce document (Pare-feu, chiffrement, etc.) Tous les flux sont systématiquement sécurisés et chiffrés selon les règles de l'art grâce au protocole TLS.

L'application est distribuée via Azure Static Web App, le code client est minifié pour optimiser le chargement et complexifier sa compréhension. Le déploiement est assuré par une CI/CD intégralement automatisée (sans aucune interaction humaine).

Les appels API sont sécurisés via des Tokens JWT signés, il n'y a aucun secret présent dans le code de l'application.

Un environnement hors production ISO à la production (génération IAC) est utilisé pour tester les nouvelles versions et assurer les tests de non-régression.

21.2 Applications Mobile My Silae Entreprise

La sécurisation des applications mobiles repose sur les mécanismes respectifs mis en place par les systèmes d'exploitation Android et iOS. Les communications sont systématiquement sécurisées et chiffrées selon les normes les plus strictes grâce au protocole TLS.
Les permissions et les mises à jour sont gérées par chaque système d'exploitation. Par ailleurs, les applications doivent obligatoirement être signées pour être admises dans les magasins d'applications (app stores).
Les applications utilisent les mécanismes de Keychain pour stocker toutes les informations sensibles liées à la sécurité (Tokens API, etc.).
Le code des applications Android est obfusqué (il n'existe pas d'équivalent pour iOS).

21.3 Application My Silae GP

21.3.1 Déploiement sécurisé via Microsoft ClickOnce

L'application My Silae GP est déployée au moyen de la technologie Microsoft ClickOnce. Les mécanismes de sécurité de ClickOnce reposent sur des certificats, des politiques de sécurité d'accès par le code et une invite d'approbation. Un certificat Authenticode garantit à l'utilisateur que le programme provient bien de la source vérifiée « Silae » et n'a pas été modifié.

Pour en savoir plus sur ClickOnce :
https://learn.microsoft.com/fr-fr/visualstudio/deployment/clickonce-security-and-deployment?view=vs-2022

21.3.2 Prérequis Framework .NET

L'application My Silae GP nécessite la version 4.8.1 du Framework .NET. À ce jour, Microsoft n'a annoncé aucune date de fin de support pour le Framework .NET 4.8 et ses sous-

versions. Silae se réserve la possibilité de faire évoluer la version du Framework .NET utilisée afin de respecter les exigences et évolutions en matière de sécurité. Si une telle évolution devait avoir lieu, elle serait anticipée, et une communication serait effectuée avec un préavis suffisant (minimum de 4 mois).

21.3.3 Communication et flux entrants

L'application My Silae GP ne communique qu'en HTTPS (via le port 443). Le poste client doit disposer d'un accès Internet classique et sécurisé. Le port 80 n'est pas utilisé, et aucun prérequis ne nécessite d'ouvrir des flux vers le poste client.

21.3.4 Flux Sortants

L'application My Silae GP permet de configurer des exports de données automatisés pour plusieurs fonctionnalités. Les flux sortants sont systématiquement sécurisés via différents protocoles disponibles : FTPS, SFTP ou FTP over TLS. Les paramètres de ces interfaces (utilisateurs, mot de passes, clés SSH, etc.) sont centralisés dans une page accessible depuis l'administration de l'application et géré directement (self-service) par les partenaires et les clients.

21.3.5 Obfuscation

Afin de réduire la surface d'attaque et de limiter la quantité d'informations accessibles aux potentiels attaquants, des mesures de durcissement et d'obfuscation ont été mises en place au sein de l'application My Silae GP pour la rendre plus résistante aux attaques. L'application est obfusquée depuis la version 1.1346.0.3, déployée le 5 avril 2022.

En informatique, l'obfuscation désigne l'ensemble des méthodes visant à altérer la lisibilité et la compréhension d'une partie du code source sans en modifier le fonctionnement. Elle peut être utilisée pour protéger une application en production et prévenir le « reverse engineering », c'est-à-dire la possibilité pour un utilisateur externe de comprendre le code source et, potentiellement, d'exploiter ses vulnérabilités.

Le niveau d'obfuscation de l'application Silae évolue vers une complexité accrue au fil du temps. Pour accompagner cette complexification, diverses campagnes de tests sont menées afin de garantir que l'obfuscation n'entraîne pas de dysfonctionnements ou de régressions dans l'application, qui repose sur de nombreux comportements dynamiques.

Version obfusquée de l'application :

21.4 APIs My Silae

Des APIs REST sont disponibles pour accéder à un ensemble de fonctionnalité. Les flux API transitent systématiquement en HTTPS et sont sécurisés par une authentification OAuth2 (Client Credentials) et un service Azure AD B2C.

Les flux APIs sont managés par un service Azure API Management, tous les appels API sont enregistrés et conservés dans des logs pendant un an.

Un mécanisme de Rate Limiting est en place pour sécuriser les infrastructures et contrôler les usages abusifs ou les tentatives de saturation.

Un portail web sécurisé permet de gérer les comptes APIs.
Pour en savoir plus sur les API, merci de vous référer à la documentation My Silae.

(1) Document à usage Restreint :
- Le document ne contient pas d'informations qui pourraient avoir un impact sur la sécurité de l'information comme des procédures internes, des informations détaillées sur les réseaux, des informations personnelles des employés de Silae, des informations Client, etc.
- Le document ne contient pas d'informations commerciales qui pourraient donner un avantage compétitif à la concurrence.
- Le document ne contient pas d'informations techniques qui pourraient donner des opportunités d'accès à des personnes extérieures.
- Le document ne contient pas d'informations financières à propos de Silae ou de ses Clients.
- Le document ne contient pas d'informations régulées par le RGPD ou les lois applicables.