Projet SR2I208

Sécurité Cloud

Membres du groupe :
ABDELJAWED Teyssir
BEN AMMAR Ghada
BEN BETTAIEB Wissem
BEN HAMOUDA Amine

Encadré par :
Mme CHEBARO Maha

2022-2023

Table des matières

Table des figures

1 Introduction

À l'ère de la transformation numérique, de plus en plus d'entreprises reconnaissent les avantages potentiels de migrer leurs infrastructures et leurs applications vers le cloud. Cependant, avec cette évolution technologique vient une série de défis en matière de sécurité. Les fournisseurs de services de cloud, tout comme les utilisateurs, doivent comprendre et aborder les risques associés à l'utilisation du cloud.
L'un des principaux défis de la migration vers le cloud est de garantir la sécurité des données et des systèmes dans cet environnement partagé. C'est là qu'interviennent les normes de sécurité du cloud. Ces normes, souvent basées sur des certifications ou des attestations, fournissent un cadre pour maintenir l'intégrité des données et des systèmes dans un environnement de cloud computing.

Dans le cadre de ce projet, nous examinerons deux normes spécifiques qui attestent du niveau de sécurité d'un hébergeur de cloud : l'attestation SOC2 et la certification SecNumCloud. Nous décrirons leur applicabilité et explorerons la différence entre l'attestation SOC2 Type 1 et l'attestation SOC2 Type 2. Nous analyserons également la relation entre la certification SecNumCloud et le schéma de certification européen relatif aux prestataires de cloud (EUCS).

Ce projet vise à apporter une compréhension détaillée de l'importance de la sécurité dans le cloud et de la façon dont ces normes aident à maintenir un niveau de sécurité adéquat.

2 La sécurité Cloud

2.1 Définition

La sécurité du cloud est un sous-domaine de la cybersécurité qui se concentre sur la sécurisation des systèmes, des données et des infrastructures dans le cloud. Elle englobe un ensemble de politiques, de technologies et de contrôles qui travaillent ensemble pour protéger les données, les applications et l'infrastructure associées au cloud computing.
La sécurité du cloud couvre plusieurs aspects de la sécurité de l'information, tels que la protection des données, la gestion de l'accès, la protection de la vie privée, la conformité aux réglementations, l'audit de la sécurité et l'assurance de la qualité.

2.2 Les services impactés par la sécurité Cloud (SaaS, PaaS, IaaS)

La sécurité du cloud a un impact direct sur trois modèles de service clés du cloud computing : Software as a Service (SaaS), Platform as a Service (PaaS) et Infrastructure as a Service (IaaS).
SaaS (Software as a Service) : Le modèle SaaS implique la fourniture par un prestataire d'applications hébergées sur une plateforme de cloud computing. Dans ce modèle, le client ne possède pas la maîtrise de l'infrastructure sous-jacente du cloud. Le prestataire assume la responsabilité de tous les aspects techniques nécessitant des compétences informatiques, de manière transparente pour le client. Toutefois, le client conserve la flexibilité d'effectuer des paramétrages spécifiques liés à son activité au sein de l'application.
La sécurité dans le SaaS implique la protection des données de l'utilisateur, la restriction de l'accès non autorisé et la prévention de la perte de données[1].
PaaS (Platform as a Service) : Le modèle PaaS consiste à mettre à disposition du client des plateformes d'hébergement d'applications par le biais d'un prestataire de services. Dans ce modèle, le client ne possède pas le contrôle direct sur l'infrastructure technique sous-jacente, qui est gérée et contrôlée par le prestataire. Cela englobe des éléments tels que le réseau, les serveurs, le système d'exploitation, le stockage, et autres. Néanmoins,

le client conserve le contrôle sur les applications déployées sur la plateforme. En fonction de la répartition des responsabilités définie dans le service, le client peut également avoir la possibilité de gérer certains services ou de configurer certains aspects spécifiques de la plateforme.
La sécurité PaaS peut inclure des politiques d'accès, la sécurisation des applications développées sur la plateforme et la protection de l'intégrité des ressources de la plateforme[1].
IaaS (Infrastructure as a Service) : Le modèle IaaS offre la possibilité au client d'accéder à des ressources informatiques abstraites, telles que la puissance de calcul, la mémoire et le stockage. Ce service permet au client de bénéficier de ressources externes, éventuellement virtualisées. Dans le cadre de ce modèle, le client conserve le contrôle total sur le système d'exploitation (OS), le stockage, les applications déployées, ainsi que sur certains éléments du réseau, tels que les pare-feu. En d'autres termes, le client peut gérer et personnaliser ces composants selon ses besoins et sa configuration spécifique.
La sécurité IaaS se concentre sur la protection de l'infrastructure virtuelle, y compris les systèmes d'exploitation, les réseaux, les firewalls et les données[1].
La figure 1 illustre les différences entre les services du cloud : SaaS, PaaS et IaaS[5].

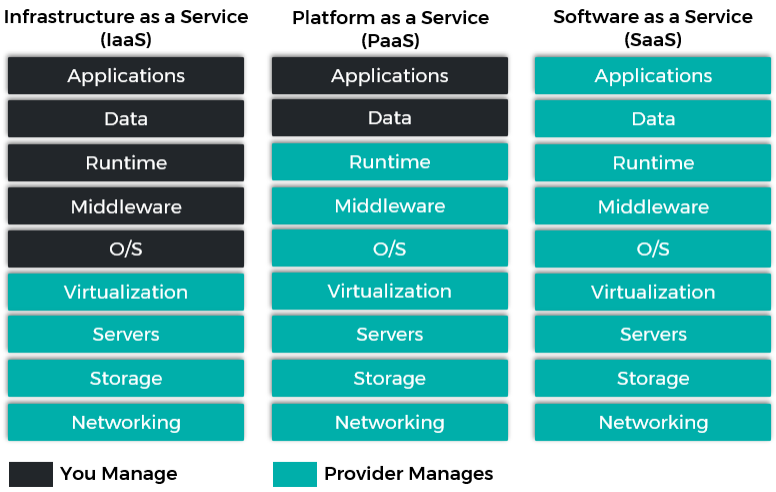

FIGURE 1 – Différence entre IaaS, PaaS et SaaS

3 Les normes de sécurité pour un hébergeur Cloud

3.1 Aperçu des normes clés de la sécurité Cloud

Pour assurer une sécurité robuste dans le cloud, différents organismes ont mis en place des normes de sécurité spécifiques. Ces normes, adoptées par les fournisseurs de services de cloud, établissent des exigences minimales pour la protection des données et des systèmes. Parmi les normes de sécurité du cloud les plus reconnues, citons l'attestation SOC2, la certification SecNumCloud et ISO/IEC 27001.

3.2 Importance des normes de sécurité dans le Cloud

Les normes de sécurité jouent un rôle crucial en établissant des pratiques de sécurité uniformes dans le secteur du cloud computing. Elles aident à atténuer les risques de sécurité, à protéger les données sensibles et à assurer la conformité avec les réglementations en matière de protection des données. Elles fournissent également un cadre de confiance pour les clients, en leur assurant que leur fournisseur de services de cloud suit les meilleures pratiques de l'industrie en matière de sécurité.

3.3 Les risques de non-qualification aux normes de sécurité du cloud

Les risques potentiels associés à l'utilisation d'un service informatique en nuage non qualifié peuvent inclure une exposition accrue du client à des incidents tels que la fuite d'informations confidentielles, la compromission de la sécurité, la perte de données ou l'indisponibilité du système d'information. Il est donc fortement recommandé que, dans le cas d'une prestation non qualifiée, le client exige du prestataire un document détaillant toutes les exigences du référentiel de sécurité qui ne sont pas couvertes par le service proposé. Cela permet au client de prendre connaissance des risques auxquels il s'expose et de mieux évaluer sa posture de sécurité.

En demandant une liste des exigences non couvertes, le client peut obtenir une vision claire des lacunes potentielles en matière de sécurité. Cela lui permet de comprendre les risques spécifiques auxquels il est confronté et d'adopter des mesures supplémentaires pour atténuer ces risques. Par

exemple, le client peut décider de mettre en place des contrôles de sécurité supplémentaires ou de rechercher un prestataire qualifié offrant une conformité plus complète aux normes de sécurité[1].

4 Attestation SOC2

4.1 Présentation de la norme SOC2

SOC2 (Service Organization Control Type 2) est une certification développée par l'AICPA (American Institute of Certified Public Accountants) qui est un réseau de plus de 400 000 professionnels à travers le monde. La norme SOC2 permet de tester la fiabilité des services fournis par une société à leurs clients en terme de sécurité.
Ayant réussi la conformité à la norme, une attestation SOC2 sera fournie à l'organisation prestataire de services. Il s'agit d'un type de rapport d'audit qui atteste la crédibilité de ces prestations. Le SOC 2 fait partie d'un trio de référentiels de contrôles définis par l'AICPA.
La figure 2 [3] présente les trois types de SOC existants.

	Objet du rapport	Usage
SOC 1	Contrôle interne relatif aux états financiers.	Usage restreint à l'entreprise faisant appel aux prestataires et à ses auditeurs.
SOC 2	Contrôles relatifs à la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité ou la protection des données à caractère personnel.	Usage est restreint à l'entreprise faisant appel à des prestataires, à ses auditeurs et à d'autres tiers spécifiques ayant une connaissance du Système.
SOC 3	Contrôles relatifs à la sécurité, la disponibilité, l'intégrité du traitement, la confidentialité ou la protection des données à caractère personnel.	Accessible à tous, le rapport ne contient pas les résultats détaillés de tests des auditeurs

FIGURE 2 – Les différents types de SOC et leurs usages

4.2 Les principes Trust Services Criteria (TSC)

Pour assurer leur conformité à la norme SOC2, les organisations doivent vérifier à quel point leurs activités répondent aux principes TSC (Trust Services Criteria) définis par l'AICPA qui sont : La sécurité, la disponibilité, l'intégrité, la confidentialité et le respect de la vie privée [4].

— **Sécurité :** Cette règle générale peut être appliquée pour évaluer la protection du système contre les accès non autorisés. L'utilisation abusive de logiciels, la diffusion d'informations, la suppression de données non autorisées et les abus potentiels du système sont autant d'exemples de failles de sécurité qui peuvent être évitées grâce aux contrôles d'accès.

— **Disponibilité :** Ce principe fait référence à la disponibilité d'un système, d'un produit ou d'un service tel que spécifié dans un contrat ou un accord de niveau de service. Il s'applique généralement aux entreprises qui fournissent des services à leurs clients. En d'autres termes, il exige aux fournisseurs de services qu'ils s'assurent que leur système est disponible pour être utilisé et exploité conformément au contrat.

— **Intégrité du traitement :** L'intégrité du traitement assure que les systèmes traitent les données comme autorisé et évalue l'exactitude, la validité et l'actualité des données.

— **Confidentialité :** Cette règle vise à garantir que les données restent protégées et sécurisées grâce à des techniques de cryptage des données en transit ainsi que les certificats clients et les certificats d'authentification personnelle.

— **Respect de la vie privée :** Cette régle régit la collecte et l'utilisation de données personnelles par des fournisseurs tiers. Elle envisage le partage et la destruction des données personnelles identifiables (PII) conformément à l'avis de confidentialité de l'organisation.

La figure 3 [3] illustre les cinq critères définies par l'AICPA et les techniques utilisées pour garantir leur applicabilité.

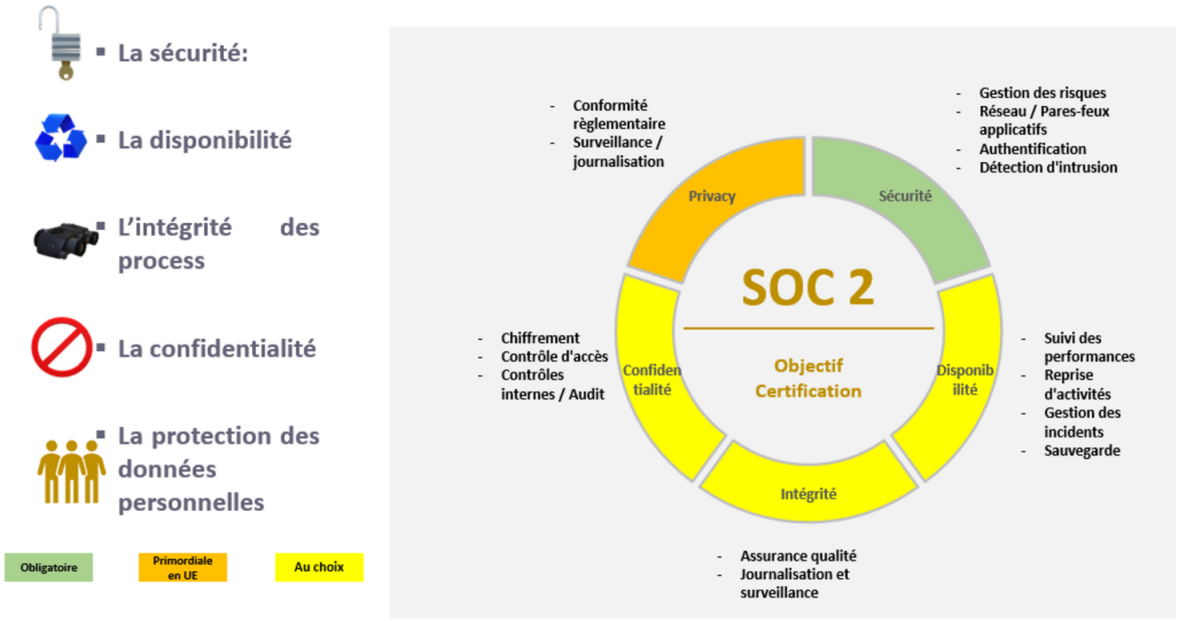

FIGURE 3 – Les cinq principes de TSC

En résumé, selon les objectifs et les tiers cibles de l'entreprise, l'évaluation SOC 2 portera sur une partie ou sur l'ensemble des TSP.

4.3 Les étapes clés du processus d'audit SOC2

Le processus d'audit SOC 2 comprend généralement les étapes suivantes :

1. Planification : cette phase consiste à définir les objectifs, la portée et les domaines de contrôle spécifiques à évaluer. L'auditeur et l'organisation cliente élaborent conjointement un plan d'audit détaillé.

2. Collecte de données : dans cette phase, l'auditeur recueille des informations sur les contrôles de sécurité mis en œuvre par l'organisation cliente. Cela peut inclure l'examen de documents, de politiques, de procédures, de journaux de suivi, etc.

3. Évaluation de l'audit : L'auditeur évalue les contrôles de sécurité de l'organisation cliente en fonction de critères définis. Cela peut inclure des entretiens avec des employés de l'organisation, des observations de processus en action, des tests techniques, etc.

4. Rapport d'audit : à la fin de l'évaluation, l'auditeur prépare un rapport d'audit détaillant les constatations, les conclusions et les recommandations. Ce rapport décrit également les contrôles mis en place par l'organisation et leur conformité aux critères établis.

5. Suivi et amélioration continue : Une fois le rapport d'audit fourni, l'organisation cliente peut mettre en œuvre les recommandations et travailler à l'amélioration continue de ses contrôles de sécurité. L'auditeur peut vérifier que des mesures correctives ont été prises.

Dans la partie suivante, nous allons définir les différents types du certificat SOC2 et leurs cas d'usage.

4.4 Les types des attestations SOC2

Il existe deux types d'attestations SOC2 : Type 1 et Type 2.

4.4.1 Attestation SOC2 Type 1

Cette attestation traite les contrôles mis en place à un moment précis dans le temps. En effet, elle se concentre seulement sur l'évaluation des politiques, des procédures pour déterminer si elles sont conçues de manière appropriée pour répondre aux critères de confiance de la SOC2 [7].

Le rapport SOC 2 Type 1 est particulièrement utile aux entreprises de services qui cherchent à prouver rapidement la conformité à la procédure d'audit AICPA.
En effet, la génération d'un rapport SOC 2 Type 1 est rapide après qu'une entité de service a terminé une évaluation de l'état de préparation. Les clients recherchent souvent ce rapport d'autant plus que l'autre type de rapport SOC 2, le type 2 qui peut prendre jusqu'à un an pour être complété. De plus, l'audit de ce rapport est généralement moins coûteux car les auditeurs ont besoin d'un minimum de données pour déterminer la position de conformité d'une organisation de services. Il n'exige pas l'implication du personnel et il ne nécessite pas beaucoup de documentations [4].

4.4.2 Attestation SOC2 Type 2

Cette attestation examine à la fois la conception des contrôles et leur efficacité opérationnelle sur une période donnée. Cela implique un processus d'audit plus rigoureux où l'auditeur doit confirmer que les contrôles ont fonctionné efficacement tout au long de la période d'examen [4]. On peut

dire que la conformité SOC 2 Type 2 donne un niveau d'assurance supérieur par rapport à SOC 2 Type 1.

4.4.3 Comparaison entre les 2 types

Le tableau 1 résume les principales différences qui existent entre l'attestation SOC2 type 1 et SOC2 type 2.

	SOC 2 Type 1	**SOC 2 Type 2**
Période d'évaluation	Ponctuelle, à un moment précis	Sur une période prolongée (généralement 6 mois ou plus)
Objectif principal	Évaluer la conception et l'existence des contrôles de sécurité à un moment précis	Évaluer l'efficacité continue des contrôles de sécurité sur une période prolongée
Utilisation courante	Pour les nouveaux prestataires de services ou pour répondre à une demande urgente de conformité	Pour les prestataires de services établis qui veulent démontrer leur conformité continue et leur engagement en matière de sécurité

TABLE 1 – Tableau comparatif : SOC 2 Type 1 vs SOC 2 Type 2

4.5 Domaines d'application de la norme SOC2

La norme SOC 2 s'applique à toute organisation souhaitant prouver de manière efficace à leurs parties prenantes les contrôles associés aux principes TSC de l'AICPA.
Elle est adaptée à plusieurs domaines notamment les organisations qui fournissent des services du Cloud Computing. Ces fournisseurs de services Cloud cherchent souvent à garantir à leurs clients la protection et la sécurité de leurs données.

De plus, certaines entreprises qui utilisent le Cloud pour stocker et traiter leurs données exigent aux fournisseurs Cloud une certification SOC2 pour s'assurer que les règles de contrôle de sécurité du fournisseur répondent à leurs exigences en termes de protection des données.
Outres les fournisseurs et les entreprises utilisant les services Cloud, SOC2 est appliquée dans le secteur des services financiers tels que le Payment Card Industry Data Security (PCI DSS) et la Gramm-Leach-Bliley Act (GLBA).

De même, les organisations de santé qui sont censées respecter les exigences de sécurité et de confidentialité des données de leurs patients doivent prouver la conformité aux réglementations de HIPAA (Health Insurance Portability and Accountability) et ceci peut être effectué grâce à la norme SOC2.

L'objectif est de fournir une assurance et une transparence reliée à la mise en place de mesures de sécurité adéquates dans le cadre de ces relations avec des tiers.

Voici quelques exemples d'entreprises connues qui utilisent le SOC 2 :
1. Amazon Web Services (AWS) : AWS est un fournisseur de services cloud très populaire et utilise le SOC 2 pour attester de la sécurité de ses services et des données stockées sur leur plateforme.
2. Microsoft : Microsoft propose divers services cloud, tels que Azure, et met en œuvre des contrôles de sécurité conformes aux normes SOC 2 pour garantir la confidentialité, l'intégrité et la disponibilité des données de leurs clients.
3. Google Cloud Platform (GCP) : GCP est une autre plateforme de services cloud majeure qui utilise le SOC 2 pour démontrer la conformité et la sécurité de ses services cloud.
4. Dropbox : Dropbox est une plateforme de stockage et de partage de fichiers en ligne. Ils ont mis en place des contrôles de sécurité conformes aux exigences du SOC 2 pour protéger les données stockées sur leur plateforme.

Dans la partie suivante, nous passerons à une autre norme importante de la sécurité du cloud, la certification SecNumCloud, et nous explorerons sa relation avec le schéma de certification européen relatif aux prestataires de cloud (EUCS).

5 Certification SecNumCloud

5.1 Applicabilité de la norme SecNumCloud

5.1.1 Présentation de la certification SecNumCloud

La certification SecNumCloud est une reconnaissance formelle décernée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France. Elle atteste que les prestataires de services d'informatique en nuage, tels que les fournisseurs d'Infrastructure en tant que Service (IaaS), de Conteneur en tant que Service (CaaS), de Plateforme en tant que Service (PaaS), et de Logiciel en tant que Service (SaaS), respectent les exigences de sécurité définies dans le référentiel SecNumCloud[1].

Cette certification vise à renforcer la sécurité des systèmes d'information et à assurer une meilleure protection des données hébergées dans le cloud. Elle donne aux clients la confiance nécessaire pour utiliser ces services, en sachant que les prestataires ont été évalués et ont démontré leur conformité à des normes de sécurité strictes.

La certification SecNumCloud s'appuie sur la norme internationale ISO 27001. Mais, il est important de noter que l'obtention de cette certification n'indique pas une équivalence directe avec ISO 27001. Elle comprend des exigences supplémentaires spécifiques à l'informatique en nuage et au contexte de sécurité français.

En novembre 2021, l'ANSSI a finalisé et publié la version 3.2.a de son référentiel SecNumCloud, à la suite d'une phase de commentaires publics. Cette mise à jour visait à renforcer les garanties juridiques du référentiel à ce moment-là et à préparer le terrain pour l'introduction du label "Cloud de confiance"[6].

5.1.2 Importance de la qualification SecNumCloud

Lorsqu'un prestataire de cloud est qualifié SecNumCloud, cela signifie qu'il a été évalué et certifié par l'ANSSI selon des critères rigoureux de sécurité. Ces critères portent notamment sur la gestion des accès, la protection des données, la résilience des infrastructures, la gestion des incidents

de sécurité et la conformité aux réglementations en vigueur. La qualification SecNumCloud offre plusieurs avantages pour les clients [1] :

- **Sécurité renforcée :** Les prestataires qualifiés SecNumCloud doivent mettre en place des mesures de sécurité avancées pour protéger les données de leurs clients contre les menaces internes et externes. Cela comprend des mécanismes de chiffrement, des politiques d'accès strictes et des mécanismes de détection d'intrusion.
- **Conformité réglementaire :** Les prestataires qualifiés SecNumCloud sont tenus de se conformer aux réglementations en matière de protection des données, telles que le Règlement général sur la protection des données (RGPD) en Europe. Cela assure aux clients que leurs données sont traitées et stockées en conformité avec les exigences légales.
- **Transparence :** Les prestataires qualifiés SecNumCloud sont soumis à des audits réguliers par l'ANSSI, ce qui garantit une transparence accrue sur leurs pratiques de sécurité. Les clients peuvent ainsi avoir confiance dans les processus et les politiques de sécurité mis en place par le prestataire.
- **Réduction des risques :** En choisissant un prestataire qualifié SecNumCloud, les clients minimisent les risques de violation de données, de perturbation des services et d'autres incidents de sécurité. La qualification offre une assurance supplémentaire quant à la fiabilité et à la résilience du prestataire.

5.1.3 Les exigences de la certification SecNumCloud

La certification SecNumCloud impose plusieurs exigences de sécurité pour les fournisseurs de services cloud qui souhaitent héberger des données sensibles. Parmi ces exigences, on distingue plusieurs régles conçernant les domaines suivants :

- **Politiques de sécurité de l'information et gestion des risques :**
  Les prestataires de services d'informatique en nuage doivent mettre en place des mesures adéquates. Cela comprend l'utilisation de logiciels sécurisés, conformes aux normes en vigueur, et l'application du guide d'hygiène informatique de l'ANSSI. Ils doivent également élaborer et mettre en œuvre une politique de sécurité de l'information, incluant les engagements de conformité légale et réglementaire. Une évaluation

des risques doit être réalisée en tenant compte de différents facteurs tels que la sécurité des données personnelles, les ressources partagées, l'exposition des interfaces d'administration et les risques liés aux tiers impliqués. Les risques résiduels doivent être identifiés, documentés et acceptés par la direction du prestataire. Ces politiques et évaluations des risques doivent être révisées régulièrement pour garantir une sécurité optimale[1].

- **Organisation de la sécurité de l'information :** Dans le cadre de l'organisation de la sécurité de l'information, les prestataires doivent établir une structure interne pour assurer le bon fonctionnement de la sécurité de l'information. Cela implique la désignation de responsables de la sécurité des systèmes d'information et de la sécurité physique, ainsi que la définition et l'attribution des responsabilités en matière de sécurité de l'information pour le personnel impliqué. Ils doivent également prendre en compte les risques liés aux cumuls de responsabilités ou de tâches, établir des relations avec les autorités compétentes et les groupes spécialisés, et réaliser une évaluation des risques avant chaque projet potentiellement impactant. Le commanditaire doit être informé des impacts, des mesures prises et des risques résiduels[1].
- **Contrôle d'accès et gestion d'identité :** La certification SecNumCloud exige une politique de contrôle d'accès documentée, en se basant sur l'analyse des risques et le partage des responsabilités. Cette politique doit être révisée régulièrement et lors de tout changement majeur. Les prestataires des sevices cloud doivent également établir une procédure pour gérer les droits d'accès aux ressources du système d'information, en fournissant des outils de différenciation des rôles des utilisateurs et en maintenant un inventaire à jour des utilisateurs ayant des droits d'administration. De plus, ils doivent éviter les conflits de droits en définissant une liste de droits d'accès incompatibles. Pour la gestion des authentifications, les prestataires doivent mettre en place des procédures pour gérer les moyens d'authentification, incluant l'authentification à multiples facteurs et le blocage des comptes après plusieurs tentatives infructueuses. Ils doivent également proposer des moyens d'authentification à multiples facteurs pour les utilisateurs finaux dans le cas d'un service SaaS. Enfin, lorsqu'ils utilisent des comptes techniques non nominatifs, les utilisateurs doivent s'authentifier avec leur

compte nominatif avant d'accéder à ces comptes techniques[1].

- **Cryptologie :** Les organismes proposant un service d'informatique en nuage doivent mettre en place un mécanisme de chiffrement pour empêcher la récupération des données des commanditaires en cas de réallocation de ressources ou de récupération du support physique. Le chiffrement peut être réalisé en chiffrant le disque ou le système de fichier dans le cas d'un service IaaS ou CaaS, ou en utilisant un chiffrement applicatif dans le cas d'un service PaaS ou SaaS. Le chiffrement des données doit respecter les règles et recommandations de sécurité spécifiées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). En ce qui concerne le chiffrement des flux réseau, le prestataire doit se conformer aux règles et recommandations spécifiées par l'ANSSI lors de la mise en œuvre de mécanismes de chiffrement. Enfin, pour le hachage des mots de passe, le prestataire doit stocker uniquement l'empreinte des mots de passe des utilisateurs et des comptes techniques, en utilisant une fonction de hachage avec un sel cryptographique conforme aux recommandations de l'ANSSI[1].
- **Sécurité des communications :** les prestataires de services d'informatique en nuage doivent établir et maintenir à jour une cartographie détaillée de leur système d'information. Cela comprend la liste des ressources matérielles ou virtualisées, les noms et fonctions des applications, le schéma d'architecture réseau. De plus, le prestataire doit mettre en œuvre des mesures de séparation logique, physique ou par chiffrement pour les flux réseau, en se basant sur la sensibilité des informations transmises, la nature des flux, le domaine d'appartenance des flux et le domaine technique. Il doit aussi disposer de sondes de détection d'incidents de sécurité sur son système d'information. Ces sondes doivent permettre la supervision des interconnexions avec des systèmes tiers et des réseaux publics, et servir de source de collecte pour l'infrastructure d'analyse et de corrélation des événements[1].
- **Sécurité physique :**
  Le réferentiel SecNumCloud exige la mise en place des périmètres de sécurité physique en définissant des zones publiques, privées et sensibles. Les zones publiques sont accessibles au public et ne doivent pas contenir de ressources liées au service. Les zones privées comprennent les plateformes de développement, les postes d'administration et les

locaux opérationnels du prestataire. Les zones sensibles sont réservées à l'hébergement du système d'information de production, à l'exclusion des postes d'administration et d'exploitation[1].

5.2 Relation entre SecNumCloud et le schéma de certification européen relatif aux prestataires de cloud (EUCS)

La relation entre SecNumCloud et le schéma de certification européen relatif aux prestataires de cloud (EUCS) est étroite et stratégique. La certification de sécurité SecNumCloud délivré par l'ANSSI en France est considéré comme une référence en matière de sécurité dans le cloud, ce qui a conduit à son utilisation comme base pour la conception de la future certification européenne de l'ENISA. Ainsi, les critères et les exigences du SecNumCloud sont susceptibles d'influencer l'EUCS, garantissant ainsi un niveau élevé de sécurité pour les prestataires de services cloud dans toute l'Europe.
De plus, la Commission européenne a exprimé le besoin d'ajouter des exigences de souveraineté au projet de l'EUCS, ce qui est en ligne avec les critères de la qualification SecNumCloud. Les deux initiatives mettent l'accent sur la garantie des engagements et des valeurs européennes, renforçant ainsi la confiance des utilisateurs envers les acteurs du numérique.
L'EUCS est destiné à devenir le référentiel de sécurité unique pour l'ensemble des pays européens. Par conséquent, il est crucial de positionner cette certification comme une certification d'excellence, en ligne avec les niveaux d'assurance les plus élevés en matière de cybersécurité et de protection des données, tels que ceux offerts par les visas de sécurité référents sur le marché, dont fait partie le SecNumCloud.
Enfin, la préservation des critères d'immunité aux lois extraterritoriales est un aspect essentiel de la relation entre SecNumCloud et l'EUCS. L'Union européenne cherche à être autosuffisante et à devenir une puissance technologique mondiale, ce qui nécessite de garantir à la fois d'un point de vue technique et juridique que les données et les activités des utilisateurs européens sont protégées contre les lois et les réglementations étrangères.
En résumé, la relation entre SecNumCloud et l'EUCS est basée sur une collaboration étroite et mutuellement bénéfique. Les critères de sécurité, les exigences de souveraineté et la volonté de préserver l'immunité aux lois extraterritoriales convergent pour créer une certification d'excellence

européenne cohérente, renforçant la confiance des utilisateurs et favorisant la transformation numérique en toute confiance au sein de l'Union européenne[2].

6 Conclusion

En conclusion, la sécurité du cloud est une nécessité absolue dans le monde numérique actuel. Alors que nous nous appuyons de plus en plus sur le cloud pour stocker et traiter des données sensibles, il est essentiel que les fournisseurs de services de cloud adhèrent à des normes de sécurité strictes et prouvent leur conformité par le biais de certifications reconnues, comme l'attestation SOC2 et la certification SecNumCloud. En adoptant ces normes, les fournisseurs de services de cloud peuvent garantir à leurs clients que leurs données sont en sécurité, quelles que soient les menaces auxquelles ils sont confrontés.

Références

[1] *ANSSI*. https://www.ssi.gouv.fr/uploads/2021/10/anssi-referentiel_exigences-secnumcloud-v3.2.a.pdf.

[2] *EUCS*. https://www.eurocloud.fr/vers-un-plus-haut-niveau-de-securite-en-europe/.

[3] *Introduction SOC 2*. https://www.linkedin.com/pulse/soc-2-processus-daudit-et-bonnes-pratiques-oppida-vous-billong/?originalSubdomain=fr.

[4] *Les principes TSC*. https://blog.rsisecurity.com/what-are-the-soc-2-compliance-requirements/#more-5333.

[5] *Les services du cloud*. https://www.inap.com/blog/iaas-paas-saas-differences/.

[6] *SecNumCLoud*. https://cloud-computing.developpez.com/actu/328248/SecNumCloud-l-ANSSI-adapte-son-referentiel-au-Cloud-de-confiance-qu-est-ce-qui-change-Le-nouveau-referentiel-s-arme-contre-les-lois-extracommunautaires/.

[7] *SOC2-type1*. https://sprinto.com/blog/soc-2-type-1/.