CLOUD TEMPLE
Innovative by design

OSSIR

Qualification SecNumCloud

Retour d'expérience

cloud-temple.com

Intervenant

GIULIANO IPPOLITI

DIRECTEUR DE LA CYBERSÉCURITÉ

CLOUD TEMPLE
Innovative by design

- *Services*
  - *Cloud de confiance*
  - *Services managés*
  - *Cybersécurité*

- *Informations*
  - *Groupe Neurones*
  - *Chiffre d'affaires*
    - *2024 : 52,5 M€*
    - *2023 : 45,9 M€*
    - *2022 : 40,4 M€*
    - *2021 : 37,8 M€*
  - *Implantation géographique*
    - *La Défense*
    - *Tours*
    - *Lyon*
    - *Caen*
    - *Nantes*
    - *Tunis*

Sommaire

/ Contexte et importance de SecNumCloud

/ Aspects organisationnels

/ Aspects techniques

/ Relever les défis

/ [Bonus] RETEX complémentaire

Référentiel SecNumCloud

- **Historique**
  - *2014 : Première version expérimentale du label Secure Cloud*
  - *2016 : Première version officielle du référentiel SecNumCloud (version 3.0)*
  - *2018 : Révision majeure (version 3.1) pour aligner le référentiel avec le RGPD*
  - *2022 : Dernière mise à jour majeure (version 3.2) avec de nouvelles exigences, notamment concernant la protection contre les lois extra-européennes*

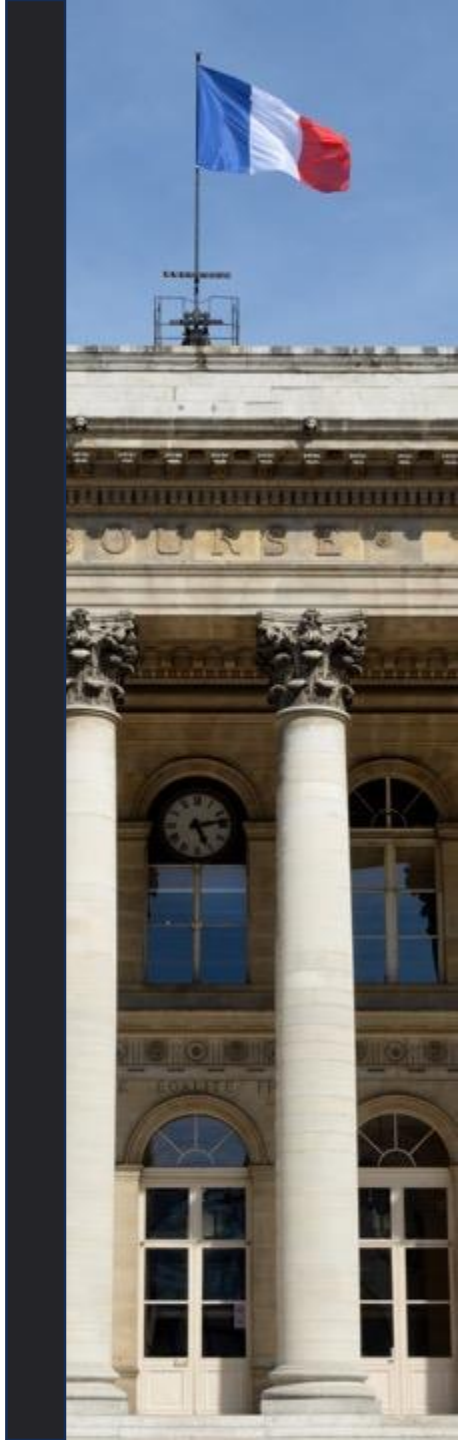
- **Structure**
  - *Adhérence avec ISO 27001/27002*
  - *Exigences supplémentaires adaptées aux services cloud : convention de service, localisation des données, régionalisation, fin de contrat, garanties de sécurité juridique*
  - *Documents annexés : Guide d'Hygiène Informatique, recommandations et notes techniques de l'ANSSI*
  - *Plus de 700 exigences unitaires*
  - *Esprit : réduire le risque de compromission causée par une défaillance du fournisseur cloud*

- **Qualification** *(pas certification)*
  - *Délivrée par l'ANSSI*
  - *Approche différente par rapport à C5 (Allemagne)*

SecNumCloud… pourquoi se lancer ?

- **Business**
  - *Renforcement de la confiance des clients*
    - *Sécurité : principal frein à l'adoption du cloud*
  - *Différentiation concurrentielle… voire facteur de survie*
  - *Renforcement de la marque et de la notoriété*
  - *Accès à de nouveaux marchés*
    - *[FR] : Doctrine "Cloud au Centre" établie en 2021*
    - *[EU] : Validation du référentiel EUCS en standby…*
    - *Éditeurs de solutions SaaS*

- **Sécurité**
  - *Montée en maturité dans tous les domaines*
  - *Réduction du risque vital pour un fournisseur cloud : compromission multi-clients*
  - *Réduction des risques juridiques et réglementaires*
  - *Facilitation des démarches de conformité*
    - *« Qui peut le plus, peut le moins » : NIS 2, DORA, HDS, C5, …*



Le parcours de Cloud Temple

- **2017** : *Naissance, avec l'ambition de démocratiser le cloud au sein des secteurs sensibles*
  - *Choix de placer la sécurité au cœur de l'offre de services*
- **2018** : *Certification ISO 27001*
- **2019** : *Premiers échanges avec l'ANSSI pour initier la démarche de qualification SecNumCloud*
- **2022**
  - **Mars** : *Qualification de l'offre IaaS « Secure Temple » (IaaS VMware)*
  - **Mai** : *Validation d'une roadmap ambitieuse, pour qualifier de nouveaux services, avec le PaaS OpenShift en priorité*
- **2024**
  - **Juin** : *Qualification de l'offre « PaaS OpenShift », et du complément S3 de l'offre IaaS*
- **2025**
  - **Février** : *Présentation de nouveaux services à l'audit de renouvellement :*
    - *Open IaaS*
    - *Bare Metal*
    - *Chiffrement HSM dans l'offre IaaS VMware*

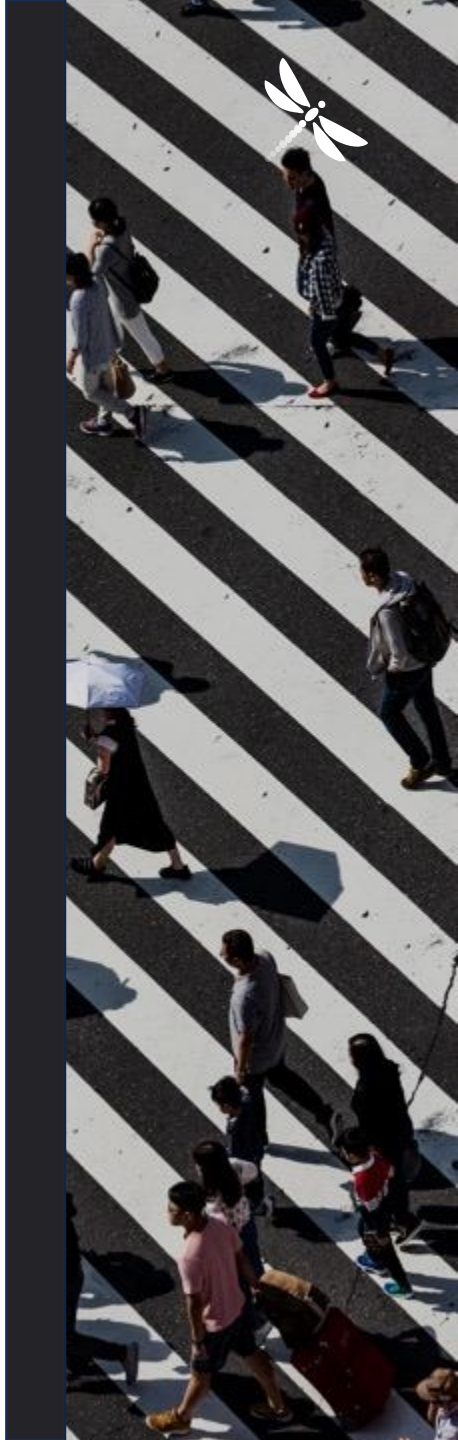
Dispositif organisationnel

- **Gouvernance**
  - *Nomination d'un Chef de Projet pour les travaux avant l'audit initial*
    - *Pour la suite (surveillance, renouvellement) : pilotage par l'équipe Sécurité*
  - *Implication forte de la Direction générale*
  - *Capitalisation sur le SMSI mis en place pour ISO 27001*
  - *2 gros chantiers, avec « porosité » :*
    - *Travaux techniques*
    - *Travaux « GRC »*

- **Parties intéressées à coordonner**
  - *Internes*
    - *Équipes « CSP » (Système, Réseau, Développement)*
    - *Sécurité*
    - *Direction générale*
    - *Fonction support (RH, Achats, Juridique, Account Management)*
  - *Externes*
    - *ANSSI*
    - *Fournisseurs (impliqués dans la délivrance des services / audit et conseil)*

Gestion de la documentation et des preuves

- **Principe de surcharge de la documentation du SMSI « ISO 27001 »**
- **Corpus des documents de sécurité**
  - *Politiques (stockées en format markdown dans un dépôt git)*
  - *Processus*
  - *Procédures*
- **Documentation technique**
  - *Intranet interne (wiki)*
  - *Pas de CMDB unique*
- **Appréciation des risques**
  - *Coexistence entre ISO 27005 et EBIOS RM*
  - *Analyse "maintstream" + analyses spécifiques aux nouveaux services, intégrées dans la mainstream pour l'itération suivante*
  - *Risques majeurs selon l'ANSSI :*
    - *Latéralisation*
    - *Accès aux données par un tier « hors UE » (ex : Data Centers)*
- **Preuves**
  - *Maintient d'un tableau de correspondance entre exigences de SNC et preuves*
  - *Migration en cours vers un outil spécifique*



Points techniques notables

- **Cloisonnement**
  - *Hyperviseurs dédiés*
    - *Technologie « historique » : VMware*
    - *Nouvelle offre Open IaaS en cours de qualification, basée sur xcp-ng (solution 100% open source développée par Vates, fork de Citrix XenServer)*
  - *Mutualisation au niveau des baies de stockage*
  - *Zones réseau avec niveaux de sensibilité différents*
  - *Recommandé (pas obligatoire) d'utiliser des produits certifiés ou qualifiés*

- **Chiffrement**
  - *Exigences du référentiel :*
    - *Respect des annexes « indigestes » B1 et B2 du RGS*
      - *Ça revient à utiliser des algorithmes modernes avec des tailles de clés suffisantes*
    - *Chiffrement des données au repos et en transit*
      - *Au repos : baies de stockage, postes de travail, bandes de sauvegarde, …*
      - *En transit : IPsec, TLS, MACsec*
  - *Chiffrement hardware des VMs déployé en 2025*

- **Automatisation poussée de la sécurité**
  - *Exemple : gestion des règles des pares-feux dans git + appels API pour déployer*
  - *Durcissement « as code »*
    - *Référentiels : CIS, ANSSI, Éditeurs*

Points techniques notables

- **Interface de gestion web (console) « maison » développée en interne**
  - *Pratiques DevSecOps :*
    - *Outils d'analyse statique et dynamique intégrées à la pipeline de CI/CD*
    - *Collaboration entre devs et sécurité, agrémentée de démonstrations de piratage*
    - *Security Champions parmi les devs*
  - *Possibilité d'utiliser les annuaires propres aux clients (fédération d'identité)*
  - *API exposée + provider Terraform, pour l'automatisation*
  - *Disséquée par l'ANSSI*

- **Réseau d'administration**
  - *Annuaire dédié*
  - *Postes d'administration dédiés et durcis*
  - *Bastion « maison » sur la base de briques open source*

- **Solutions open source privilégiées**
  - *Exemples :*
    - *Linux pour tous les OS des serveurs et des postes d'administration*
    - *Keycloak pour l'IAM*
    - *Wiki.js pour la documentation*

Relever les défis

- **Concilier « time to market » rapide et sécurité**
  - *Collaboration entre équipes techniques et de sécurité*
    - *Shift Security to the Left / Security by Design*
  - *Équipe Sécurité « au service du business »*

- **Concilier richesse de fonctionnalités et sécurité**
  - *Point d'équilibre à trouver pour maîtriser la surface d'attaque*
  - *Possibilité de proposer des services non qualifiés en parallèle (ex : PaaS)*

- **Accompagner le changement**
  - *Implication nécessaire de la direction générale*
  - *Reconnaissance des efforts par les managers*
  - *Communication, pédagogie, …*

- **S'adapter au processus de qualification**
  - *Peu adapté aux ambitions de qualifier 5 à 10 services par an*
  - *Échanges avec l'ANSSI pour améliorer la souplesse*

[Bonus] RETEX complémentaire

- **Relations avec l'ANSSI : très bonnes**
  - *Chargé de qualification très aidant*
  - *Points trimestriels fructueux*
  - *Possibilité de solliciter les experts de la Division Assistance Technique (DAT), qui comprennent bien les contraintes métier*
  - *À prendre en compte, circuit de signature long :*
    - *Chargé de qualification > Assistant bureau BQA > Chef BQA > Chef Division PSS > Sous-Directeur Expertise > Cabinet > DG*

- **Audit**
  - *Audit initial : participation sur site de l'ANSSI*
  - *2 audits en parallèle : organisationnel et technique*
  - *Durée : 6-7 jours en début de cycle, 3-4 jours pour la surveillance*
  - *Relation fluide entre auditeurs et audités (« gagnant – gagnant »)*
  - *Note importante : l'ANSSI a la possibilité de requalifier les constats des auditeurs*
    - *Cela réduit fortement la « tolérance/indulgence » de l'équipe d'audit (mais n'élimine pas complètement la dimension client-fournisseur)*

[Bonus] RETEX complémentaire

- **Appel à l'expertise externe**
  - *Cabinet spécialisé dans l'accompagnement à la qualification*
    - *Aide dans l'interprétation du référentiel, en complément de la DAT de l'ANSSI*
    - *Conception sécurisée de nouveaux services*
    - *Durcissement*
    - *Préparation des audits*
    - *Accompagnement lors des audits*
  - *Partenaires technologiques*
    - *Conception et construction de nouveaux services*
  - *Important de ne pas créer une dépendance, notamment pour l'exploitation des services*
    - *Transfert de compétences nécessaire, focus sur les livrables documentaires et sur la formation*


Questions ?

Merci !

CLOUD TEMPLE
Innovative by design

Giuliano IPPOLITI
Directeur de la cybersécurité
giuliano.ippoliti@cloud-temple.com
+33 6 19 59 01 41

www.cloud-temple.com