numberly

iooomercis group

Sécurité de la Numberly Martech Platform

Table des matières

Numberly conçoit depuis 20 ans des solutions techniques en prenant en compte les problématiques de sécurité à chaque étape de conception et à tous les niveaux : en ce sens, nous sommes bien conformes à l'ensemble des exigences rédigées dans le projet de PAS.

Conformité RGPD

La solution logicielle proposée dans le cadre du présent appel d'offres a été développée selon les principes du **Privacy by Design** :

- Les équipes conformité du groupe Numberly ont été associées à toutes les étapes de développement, de la phase de cadrage jusqu'au déploiement. Elles continuent d'être sollicitées à l'occasion de la mise en production de nouvelles versions et fonctionnalités.
- Une analyse juridique et sa traduction au niveau de la plateforme ont été menées dès la conception.
- Une attention spécifique a été portée aux processus de pseudonymisation, anonymisation, au respect des durées de détention adaptées aux finalités poursuivies par le Responsable de Traitement ainsi qu'à l' exercice des droits des personnes

Le paramétrage de la plateforme permet de se conformer strictement aux instructions particulières du responsable de Traitement.

La solution proposée dans le cadre du présent appel d'offres a été développée selon les principes de **l'accountability.** Les mécanismes et procédures permettant de démontrer le respect des règles relatives à la protection des données sont documentées et auditées.
Le groupe Numberly a organisé la protection des données personnelles avec une gouvernance solide qui s'articule autour :

- D'un Délégué à la Protection des Données (DPO) nommé en 2018, Correspondant Informatique et Liberté depuis 2008. Le DPO dispose de tous les moyens nécessaires à l'exécution de sa mission en toute indépendance.
- D'une équipe conformité RGPD, composée de cinq professionnels, juristes spécialisés et expérimentés
- D'un comité des risques dans lequel la direction du groupe est partie prenante

Le groupe dispose du label Privacy Protection Pact depuis 2019.

Organisation de la sécurité de l'information

Certification ISO 27001

Notre politique de sécurité de l'information suit ainsi les guidelines de la certification ISO 27001 et la philosophie du label SecNumCloud élaboré en 2016.

La Numberly Martech Platform est certifiée ISO-27001 depuis septembre 2024. Ceci atteste de notre engagement envers des normes internationales rigoureuses en matière de sécurité de l'information, garantissant ainsi une approche systématique et cohérente pour protéger les données sensibles.

Certificat FR24/00000194

Le système de management de

NUMBERLY

28 Rue de Châteaudun, 75009 Paris, France

a été audité et certifié selon les exigences de

NF ISO/IEC 27001 : 2023 - Gestion de la sécurité de l'information dans le domaine de la sécurité de l'information, de la cybersécurité et de la protection de la vie privée

Pour les activités suivantes
Développement, maintenance et hébergement en mode SaaS de la solution Numberly Martech Platform (NMP).
Dda : Déclaration d'applicabilité version 1.3 du 20/05/2023

Ce certificat est valable du 12 septembre 2024 au 11 septembre 2027 et reste valide jusqu'à décision satisfaisante à l'issue des audits de surveillance.
Version 1. Certifié depuis le 12 septembre 2024

Autorisé par
Siham VIDARD

SGS INTERNATIONAL CERTIFICATION SERVICES
29, avenue Aristide Briand 94110 Arcueil France
t +33 (0)1 41 24 88 88 - https://www.sgsgroup.fr/

Accréditation n°4-0008
Portée disponible sur
www.cofrac.fr

Ce document est un certificat électronique authentique destiné à l'usage professionnel du Client uniquement. Les versions imprimées du certificat électronique sont autorisées et seront considérées comme copies. Ce document est délivré par la société sous réserve des Conditions Générales SGS pour les Services de Certification disponibles sur Conditions Générales | SGS. Nous attirons votre attention aux clauses contenues sur la limitation de responsabilité, d'indemnisation et de juridiction. Ce document est protégé par le droit d'auteur et toute altération non autorisée, contrefaçon ou falsification du contenu ou de l'apparence de ce document est illégale.

Page 1 / 1

Organisation SMSI

Nous disposons d'un SMSI opérationnel qui se matérialise par un Comité de la Qualité et des Risques qui se réunit toutes les 5 semaines en regroupant a minima la Direction Générale, la Sécurité, le DPO, les équipes métiers et la direction technique pour assurer une parfaite maîtrise des risques : depuis l'identification des risques jusqu'à la mise en œuvre de solutions adéquates pour garantir la confidentialité, l'intégrité et la traçabilité des données.
Le groupe suit 4 principes clés en termes de politique de sécurité de l'information :

- **Confidentialité** : toutes nos données sont chiffrées en transit et au repos, incluant les sauvegardes.
- **Intégrité** : notre plateforme utilise des technologies permettant de garantir l'intégrité des données sur le plan technique. Le cycle de vie de ces données est suivi de près par nos équipes techniques et clientes grâce à nos différents outils de supervision.
- **Disponibilité** : l'ensemble de nos plateformes sont déployées sur deux datacenters via une architecture active-active. Cela facilite nos maintenances liées à des problématiques de sécurité ou d'évolutions tout en garantissant une continuité de service.
- **Traçabilité** : toutes les modifications opérées dans notre système d'information sont suivies, validées et tracées. L'ensemble des accès, qu'ils soient internes ou externes, sont centralisés dans un système centralisé. Cela permet de surveiller de manière proactive les erreurs logicielles sur nos plateformes applicatives, mais aussi de s'assurer qu'aucun accès frauduleux n'est réalisé.

Les exigences de sécurité mises en place sont les suivantes :

- Développer, mettre en place, et maintenir continuellement un système de management de sécurité de l'information
- Etablir un processus d'évaluation des risques propres à la sécurité de l'information et déterminer des mesures pour contrer l'apparition des risques
- S'assurer que les ressources dédiées au maintien d'un tel système sont suffisantes et adéquates, et que les responsabilités soient déléguées.
- Impliquer les directions opérationnelles
- Conserver la documentation propre au management de la sécurité de l'information
- Mettre à jour trimestriellement la cartographie des risques pour identifier et réduire les risques en protégeant l'organisation contre les menaces et les vulnérabilités pouvant impacter Numberly ou ses clients.
- Promouvoir l'amélioration continue selon le cadre PDCA

- **Plan** : Définir la politique et les objectifs du système de sécurité de l'information, identifier et évaluer les risques, définir un traitement du risque
- **Do** : Mettre en place un plan de traitement des risques, mettre en place les mesures de sécurité
- **Check** : Évaluer les mesures de sécurité adoptées, réaliser des audits interne et externe
- **Act** : Ajuster les processus et procédures pour pallier les défaillances constatées lors de la phase de Check

Documentation de la politique de l'information

Nous disposons d'une politique de sécurité de l'information (PSSI) basée sur l'ISO 27002 (version 2022), qui est diffusée au personnel et appliquée sur les périmètres de notre solution technique.
Cette PSSI est très régulièrement mise à jour et au moins une fois par an afin de tenir compte des évolutions techniques, de la réglementation ainsi que des évolutions de la certification ISO.

La documentation de notre politique de la sécurité contient plusieurs documents, en plus de notre PSSI, telles que :

- **Un Plan d'assurance Sécurité (PAS)** : Notre PAS permet d'informer nos clients sur les technologies et processus de sécurité informatique mis en œuvre dans le cadre des prestations fournies. Ce plan reprend notamment notre politique de la sécurité de l'information, l'organisation de la sécurité de l'information, la sécurité des ressources humaines, la gestion de nos actifs.
- **Plan de continuité d'activité (PCA)** : Ce plan vise à expliquer les moyens mis en place par numberly afin de sécuriser les enjeux business en cas de défaillance suite à un sinistre ou un évènement perturbant gravement le fonctionnement de notre solution technique. Ce PCA précise et identifie la méthodologie de notre gestion de crise, son activation,les contacts et son mode opératoire. Nous documentons également les conditions de déclenchement en fonction de grandes familles de risques techniques avec un RACI associé.
- Un **Plan d'Assurance Qualité (PAQ)** : Ce document a pour objet de décrire les modes de fonctionnement, les exigences qualité des prestations et services énoncés dans le cadre du contrat d'exécution du projet ainsi que toutes les dispositions spécifiques prises pour les satisfaire.
- Une **Procédure de gestion des incidents de Sécurité** : Ce document a pour objet de décrire les actions à effectuer en cas d'incident de Sécurité en définissant ce qu'est un incident, les catégories d'incidents, l'évaluation de leur criticité, le plan de communication à appliquer, les points de contacts et acteurs, ainsi que les actions générales à mener pour contenir l'incident, et

enfin le rapport d'incident à formaliser incluant l'identification de pistes d'amélioration afin qu'il ne se reproduise plus.

- **Une gestion des actifs** : En effet, l'ensemble des actifs matériels et immatériels sont documentés.
    - Périphériques et accessoires : Nous disposons de différents référentiels d'actifs tels que les périphériques et accessoires utilisés par l'ensemble de nos collaborateurs. Ce référentiel permet à de nombreux outils de sécuriser une partie de notre système d'information en vérifiant l'utilisation de périphériques autorisés et associés au bon utilisateur afin d'éviter les risques de vols en empêchant l'utilisation de périphériques non autorisés.
    - Les serveurs et équipements réseaux : L'ensemble de notre infrastructure est documentée dans une CMDB afin de connaître l'emplacement physique des équipements au sein de nos différents datacenters, des informations d'identifications, la fonction de l'équipement, son modèle, son propriétaire et des besoins de sécurité. Ce référentiel est mis à jour à chaque entrée et sortie de matériel et un inventaire annuel est réalisé afin de vérifier tout écart.
    - Nos code sources : L'ensemble de nos solutions sont développées en interne et le code source est stocké sur une solution sécurisée et redondée au sein de notre infrastructure. L'accès à ce code source est sécurisé de manière à ne pouvoir être accédé que par les personnes en ayant besoin. Notre système nous permet également de suivre et valider le cycle de vie de nos applications.

Formation des collaborateurs et sous-traitance

Au travers de notre politique de sécurité, Numberly s'efforce à sensibiliser l'ensemble de ses collaborateurs via des sensibilisations régulières aux sujets de la sécurité informatique.
Ainsi chaque collaborateur suit une formation obligatoire tous les ans, doit faire face à des campagnes de simulation de phishing.

Certaines populations bénéficient de formations plus spécifiques, comme nos développeurs à qui nous présentons les derniers risques en matière de vulnérabilité via la veille réalisée par nos équipes de sécurité. Tout au long de l'année, nous permettons à nos développeurs de participer à des évènements, organisés en interne ou en externe, de challenges de sécurité informatique leur permettant de mettre en application leurs connaissances et de les améliorer.

Numberly ne fait pas appel à la sous-traitance pour la mise en place ou la maintenance de ces flux et infrastructures, offrant ainsi une indépendance totale en tant que tiers de confiance.

En conclusion, la politique de sécurité de l'information est un point clé depuis la création de Numberly en 2000, et s'est inspirée au fil des années des différentes normes élaborées, notamment ISO 27001 et SecNumCloud.

Un socle d'infrastructure solide et éprouvé

Numberly propose à ses clients une infrastructure système dédiée pour héberger la Solution. Cette infrastructure est en design actif-actif permettant d'opérer de manière fiable et sereine. Nous assurons en effet une redondance complète, ce qui vous garantit une intégrité des données et une continuité de production et du service.

Nous sommes propriétaire de nos serveurs hébergés en cages privatives et sécurisées dans deux datacenters certifiés ISO 22301 et HDS notamment et localisés en région parisienne.

Nous avons une indépendance totale sans sous-traitant et nous avons la pleine propriété de nos infrastructures (IP, données, serveurs, réseau).

L'ensemble de l'infrastructure est opéré par des experts techniques internes à Numberly, ce qui assure les plus hauts standards de sécurité logiques et physiques, et nous donne une totale autonomie de maintenance et d'innovation de nos technologies.
Cela facilite les cycles de vie des serveurs et de nos solutions logicielles (correctifs, maintenances, upgrades).

Accès au service du titulaire via Internet

Numberly est un opérateur internet identifié par l'AS197205 qui dispose de plusieurs interconnexions avec des opérateurs Tier1 afin d'avoir les meilleures latences auprès de nos clients.
Nous sommes aussi connectés sur des points d'échanges tels que FranceIX et EquinixIX.
Ces interconnexions sont présentes sur chaque datacenter ce qui permet une redondance et un accès internet hautement sécurisé.

La Numberly Martech Platform et ses APIs sont accessibles uniquement en HTTPS sur le port 443 via Internet.
Les communications sont chiffrées à l'aide de certificats SSL d'une durée de vie de 3 mois, provenant d'une autorité de certification publique et les connexions SSL sont configurées en respectant les recommandations NT_TLS de l'ANSSI.

De ce fait, seules les connexions TLS v1.2 minimums sont autorisées via les ciphers recommandés par le guide l'ANSSI.

Il est également possible de mettre en place des certificats issus d'une autorité de certification privée et de procéder à une authentification par certificat client.

Une sécurité applicative robuste

Authentification

Notre système d'authentification est accessible uniquement par HTTPS. Il implémente les notions de CSRF, les authentifications sont tracées et permettent de savoir le succès ou non, la date et heure, l'IP ainsi que le port source utilisé et le nom d'utilisateur utilisé. Ce système dispose de procédures anti brute-force qui sont paramétrables, afin d'empêcher un attaquant d'effectuer trop de tentatives de connexion pour un même login ou depuis une IP. Cela peut amener au blocage temporaire ou définitif du compte en fonction de la demande du client.

Le service permettant de gérer l'authentification à la Numberly Martech Platform permet de se baser sur les informations fournies par des systèmes d'identité externe, notamment OpenID et les mécanismes basés sur du SAML 2.0 ou OAuth (SSO). Nous avons une expérience positive d'intégration à ce type de systèmes auprès de groupes ayant des milliers d'utilisateurs.

La session de l'utilisateur est paramétrable, ce qui permet de les déconnecter au bout d'un temps d'inactivité.
Nous disposons de mécanismes de double authentification : par email, ou application TOTP, à votre convenance, pour l'ensemble de vos utilisateurs.
Notre système d'authentification est régulièrement audité par des experts en sécurité informatique, dans des audits blancs (white-box). Le résultat de ces audits est communicable sur demande au client.

L'authentification de nos API implémente une authentification basée sur des tokens JWT.

Gestion des habilitations

Le service d'authentification unique (SSO) de la Solution peut se baser sur les informations fournies par des systèmes d'identité externe, notamment via le protocole SAML par exemple, permettant ainsi d'attribuer les droits et groupes décrits plus haut.

Pour l'initialisation de l'ensemble des comptes, notre suggestion serait de recevoir un fichier contenant l'ensemble des utilisateurs et de leurs droits à assigner afin de créer les bons profils, groupes et permissions utilisateurs.

Hébergement et reprise d'activité

Isolation logique

Numberly met à disposition une infrastructure d'hébergement de la donnée redondante dédiée et séparée logiquement du reste des clients. Elle sera donc dédiée à chaque client.
Les clefs de chiffrement sont elles aussi uniques et propres à chaque client afin d'assurer une parfaite isolation pour le chiffrement des données au repos ainsi que pour le stockage des sauvegardes.

Sécurité physique

Numberly dispose de cages privatives au sein de datacenters neutres localisés en région parisienne. Ces datacenters sont opérés par des entreprises mondialement reconnues sur le marché : Equinix et Interxion.
Nous avons choisi des datacenters situés en région parisienne et séparés de 10 km afin de réduire les risques environnementaux tout en conservant des latences optimales pour les enjeux métiers de nos applications. Ces zones disposent également de très fortes capacités électriques nous assurant une parfaite évolution au fur et à mesure de notre croissance : une stratégie éprouvée depuis 15 ans en multipliant le nombre de nos baies par 3.
Le choix de ces acteurs et de ces localisations nous permettent de répondre à de nombreux risques :

- **Risques physiques** : ces datacenters disposent des certifications suivantes : HDA, ISO 14001:2015, ISO 22301, ISO 27001, ISO 50001, ISO 9001:2015, OHSAS 18001, PCI DSS, SOC 1 Type II et SOC 2 Type II. Nos datacenters sont dotés d'équipements de sécurité de pointe assortis de techniques et de procédures de sécurité avancées. Ils disposent de divers contrôles de sécurité constitués de postes tenus 24/7 par des agents de sécurité, de sas de sécurité ainsi que de lecteurs biométriques. Bien entendu, de nombreux systèmes de vidéo surveillance sont installés dans l'ensemble du datacenters avec des enregistrements accessibles sur demande. Ils sont également conçus pour être discrets afin d'en optimiser le niveau de sécurité. Seuls quelques collaborateurs de Numberly disposent d'accès physiques. Nous accompagnons systématiquement les techniciens constructeurs qui pourraient intervenir sur site. Leurs identités et leurs casiers judiciaires sont vérifiés en amont de leur

intervention, suivant les dispositions contractuelles de nos contrats de maintenance constructeurs. Ces accès physiques sont revus systématiquement à chaque arrivée et départ d'un collaborateur de l'équipe Infrastructure.

- **Risques météorologiques** : nos datacenters ont été sélectionnés de manière à ne pas être impactés par des risques météorologiques tels que des inondations. Chacun de nos datacenters est protégé des risques de foudre. De plus, nos datacenters ne sont pas soumis aux risques sismiques.

- **Risques intrinsèques et électriques** : nos datacenters sont de type N+1 et certifiés Tier 3 par l'Uptime Institute. L'ensemble des installations (IT et Infra) sont adossées à des onduleurs et des groupes électrogènes. En cas de coupure électrique, les onduleurs prennent le relais le temps que les groupes électrogènes démarrent. Nos datacenters peuvent fonctionner 72 heures sur groupes et sont prioritaires sur le ravitaillement de fioul. Enfin chacune de nos baies disposent de deux arrivées électriques afin d'alimenter de manière distincte chaque équipement disposant également de doubles alimentations. Différents tests sont organisés afin de tester :
    - Les capacités électriques de nos baies et la bascule en cas de perte d'une des arrivées électriques, de manière trimestrielle.
    - La reprise par les groupes électrogènes en cas de coupure électrique, de manière trimestrielle.

Nos datacenters sont urbanisés avec des couloirs chauds et froids (cold-corridor) afin d'optimiser le refroidissement des équipements. Les équipements de refroidissement sont monitorés 24/7 et disposent de SLA sur la température et l'humidité en accord avec les recommandations de l'ASHRAE (American Society of Heating, Refrigerating and Air Conditioning). Enfin, l'ensemble de nos datacenters disposent de systèmes anti-incendies. Les locaux électriques, batteries, onduleurs, sont séparés des salles d'hébergement de nos baies de serveurs. Ces locaux sont naturellement protégés par détection et extinction automatiques. L'ensemble de nos fibres noires utilisent des chemins indépendants qui ne recoupent pas afin de se prémunir des risques d'incidents physiques (travaux, sabotage).

Dans ses locaux, Numberly met en place des zones sécurisées par des contrôles adéquats à l'entrée, afin de s'assurer que seul le personnel autorisé est admis. Tous les visiteurs sont encadrés pendant la totalité de leur temps de présence dans les locaux de Numberly. L'accès leur est par ailleurs accordé uniquement à des fins précises ayant fait l'objet d'une autorisation. Numberly accorde au personnel d'une organisation tiers chargé de l'assistance technique un accès limité aux zones sécurisées ou aux moyens de traitement de l'information confidentielle et uniquement en fonction des nécessités. Cet accès fait l'objet d'une autorisation et d'une surveillance permanente. Numberly revoit et met à jour régulièrement les

droits d'accès aux zones sécurisées et les révoque au besoin (arrivée, départ, changement de fonction dans l'organisation, etc.).
Les locaux sont protégés contre les menaces extérieures et environnementales, notamment contre le feu, grâce à des détecteurs multiples à chaque étage et dans la salle technique du sous-sol et présence d'extincteurs (AB) selon les dispositions législatives et réglementaires en vigueur régulièrement testés par une société spécialisée.
Les locaux sont protégés contre les intrusions :

- Dispositif de contrôle d'accès basé sur un code à 6 chiffres individuel ;
- Journal sécurisé de traçabilité électronique de tous les accès ;
- Télésurveillance via la société Securitas opérationnel 24/24h et 7/7j ;
- Système de vidéosurveillance du périmètre extérieur.

Continuité d'activité

L'ensemble des systèmes composants l'infrastructure sont configurés de manière à fonctionner de manière active-active. C'est-à-dire qu'à tout moment, les deux datacenters acceptent le trafic et le traitent.

Chacun de nos sites physiques est conçu de manière à pouvoir faire fonctionner seul notre solution de manière nominale, ce qui nous permet de disposer de capacités supplémentaires lorsque nos deux sites physiques sont disponibles. Cela nous permet également d'assurer de nombreux tests tel que prévu par notre PRA et ce, sans aucun impact pour le client. Numberly se tient à sa disposition afin de participer à ses exercices de test PRA.

Les maintenances de cycle de vie et évolutives de nos systèmes d'infrastructures sont réalisées avec beaucoup plus de simplicité et de fiabilité puisque nous pouvons couper chaque brique du système sur un datacenter donnée ce qui permet dans un même temps de tester en continue la continuité du service et de bénéficier d'un retour en arrière.

Numberly surveille de manière continue l'accessibilité aux solutions par l'intermédiaire d'un système de surveillance redondant sur nos deux datacenters. Nous disposons également de diverses sondes situées à l'extérieur de notre réseau afin de nous assurer de la bonne accessibilité externe. Au-delà de la supervision de nos applicatifs, ce système nous permet également de surveiller nos équipements que ce soit au niveau matériel (médias de stockage, alimentation, etc) ou au niveau logiciel.
Ce système se base également sur des règles métiers afin de nous alerter en cas d'utilisation inhabituelle : différence du nombre de requêtes trop importante par rapport à T-1 semaine, nombre d'envois d'emails ou SMS incohérent, tentative de connections échouées trop important sur un ou plusieurs utilisateurs.

Ces alertes nous permettent d'être très réactifs et de nous assurer qu'ils ne sont pas à l'origine d'un dysfonctionnement plus important.

De par cette conception, Numberly sait répondre aux exigences de DMIA et PDMA demandées par nos clients.

Sécurité logique et maintien en condition de sécurité

a. Serveurs

Les accès des équipes Numberly se basent sur l'existence de l'utilisateur au sein d'un annuaire Active Directory. Nous disposons d'automatisation à notre SIRH afin de nous assurer de la désactivation des accès de manière automatique lorsque nécessaire (fin de contrat, suspension). En parallèle de ce dispositif, nous organisons régulièrement des revues d'accès par l'intermédiaire de rapport de revues automatisés. Ce système lève des alarmes lorsque des accès administrateurs sont attribués à des utilisateurs lorsque cela n'est pas prévu. Les PV de revues sont stockés dans nos systèmes d'archivage et sont communicables au client sur demande.

Sur l'ensemble des accès aux infrastructures et applications, la politique du moindre privilège est systématiquement appliquée. Un système de rôle permet de s'assurer que seules les actions nécessaires sont réalisables aux seules personnes le nécessitant.

L'ensemble de ces accès internes sont régies par :

- L'utilisation d'un VPN disposant d'une authentification basée sur un certificat et une clé SSL nominative ainsi qu'une double authentification via l'OTP de la clef physique du collaborateur (Yubikey).
- Nous vérifions que la clef de sécurité correspond à celle attribuée dans notre annuaire.
- Un filtrage d'IPs pour les accès serveurs et applicatifs
- Une authentification forte via clé SSH. Celle-ci est stockée dans la clef physique du collaborateur (Yubikey). Nos systèmes vérifient l'appartenance de la clé publique à l'utilisateur donné. Enfin, les accès à forts privilèges ainsi que les actions réalisées par ceux-ci remontées des alertes au niveau de notre SIEM.

L'ensemble des serveurs disposent :

- de protections antivirales adossées à un système d'alerting pour prévenir en cas de défaut de mise à jour de la base de données de signature. Ces protections ne sont pas désactivables, hormis pour des super-administrateurs

identifiés. La désactivation remonte une alerte critique à nos équipes de sécurité. La mise à jour des signatures est effectuée quotidiennement.
- d'un pare-feu local appliqué automatiquement et dont la configuration est déployée via des outils d'infrastructure as code. Toute modification est obligatoirement revue par des membres de l'équipe infrastructure.
    - Un firewall en bordure de réseau permet également de filtrer toutes les connexions sortantes de notre réseau pour n'autoriser que des flux bien identifiés.
    - Cette configuration est également gérée par nos outils d'infrastructure as code.
- de mécanismes de remontées de vulnérabilités basées sur les applicatifs installés sur les serveurs afin de remonter des alertes et déclencher les procédures de mises à jour dans les délais prévus par notre Politique de gestion des vulnérabilités.

b. Poste de travail

L'authentification des postes de travail se fait via un compte Azure Active Directory qui bénéficie des règles de sécurité de nos infrastructures Active Directory comme précisé dans notre PAS, à savoir:
- une longueur de 12 caractères minimum. 20 pour les comptes à privilèges.
- trois types de caractères différents obligatoires
- une durée de vie maximale de 90 jours
- l'impossibilité de réutiliser les 5 derniers mots de passe
- un maximum de 5 tentatives possibles avant verrouillage du compte

Chaque nouveau mot de passe est vérifié via l'outil Have I Been Pwned qui permet de savoir si le mot de passe fait partie d'une base de données associée à une fuite de données publique.

De plus l'ensemble des postes de travails disposent :
- de protection anti-virale adossée à un système d'alerting pour prévenir en cas de défaut de mise à jour de la base de données de signature. Ces protections ne sont pas désactivables, hormis pour des super-administrateurs identifiés. La désactivation remonte une alerte critique à nos équipes de sécurité. La mise à jour est effectuée toutes les 4 heures.
- d'un pare-feu local non désactivable.
- des mécanismes de remontées de vulnérabilités basées sur les applicatifs installés sur les postes de travail afin de remonter des alertes et déclencher les procédures de mises à jour dans les délais prévus par notre Politique de gestion des vulnérabilités.

Sécurité des développements

Nos développements sont réalisés en interne et ne dépendent pas de solutions propriétaires (SDK propriétaires, appliances), nous avons la pleine maîtrise de la sécurité de la conception de la solution jusqu'à son déploiement et l'accès par les utilisateurs.
L'ensemble des développeurs qui sont amenés à contribuer au code source suivent une formation sécurité orientée techniquement sur leur périmètre technique (backend, frontend, data, etc).
Cette formation contient les bonnes pratiques de développement, les failles les plus courantes et les manières de s'en prémunir. Nous réalisons également régulièrement des concours de sécurité organisés en interne ou par des intervenants extérieurs. Ces concours prennent la forme de Capture The Flag, un jeu consistant à exploiter des vulnérabilités affectant des logiciels de manière à s'introduire sur des ordinateurs pour récupérer les drapeaux, preuves de l'intrusion.
Nous disposons également de ressources permettant à l'ensemble de nos développeurs de suivre des recommandations de développement qui sont communes pour l'ensemble du groupe Numberly.

Ces ressources établissent :

- **La gestion des données sensibles** : elles sont stockées, chiffrées et accédées de manière sécurisée. En effet, l'ensemble de nos mots de passe sont stockés, chiffrés par une fonction de dérivation de clé PBKDF2 adossée à l'utilisation d'un sel. L'ensemble des informations qui peuvent être échangées par des systèmes (API, bases de données) sont communiquées aux travers de connexions chiffrées, suivant les recommandations NT_TLS du référentiel SecNumCloud.
- **L'environnement de développement** : il est dédié et séparé physiquement et logiquement du reste de la production. Ils ne peuvent pas communiquer nativement. Les données de cet environnement sont réduites au strict minimum et sont bien sûr anonymisées. La sécurité de cet environnement est au même niveau que les autres environnements (production, préproduction). Les accès sont limités au strict nécessaire et aux seules personnes ayant besoin d'y accéder. Cet environnement est sauvegardé.
- **La modification de code source** : elle est réalisée sur des équipements dédiés qui sont la propriété de Numberly. L'ensemble des modifications sont signées par des clefs GPG stockées dans la clef de sécurité physique (Yubikey) de chaque développeur. Nos systèmes vérifient que la signature de chaque modification est associée à la clef GPG de l'utilisateur en question. Cela nous permet de nous assurer qu'aucune modification de code ne peut être effectuée par un tiers. Ces modifications de codes sont toutes reliées à des demandes précises statuant leur type : correctif, ajout de fonctionnalité afin d'en assurer la traçabilité. Ces modifications sont ensuite proposées par le

biais de Merge Request (MR). Elles sont obligatoirement revues par un ou plusieurs pairs et déclenchent automatiquement des tests de continuité d'intégration. Ces tests incluent :

  - des tests unitaires qui ont pour objectif de vérifier la compatibilité des modifications avec l'environnement précédent et de tester l'ensemble des régressions éventuelles.
  - des tests statiques de sécurité des applications (SAST). La méthodologie SAST englobe les outils et les technologies conçus pour vérifier la présence de failles et de vulnérabilités dans le code. Elle constitue une forme de test en boîte blanche – les outils correspondants sont parfois appelés contrôleurs de vulnérabilité – qui recherche les problèmes dans le code. Cela teste notamment les principales failles OWASP.

- **Le suivi et la mise à jour des dépendances** : nos développements peuvent se baser sur des dépendances publiques externes. Ces dépendances sont auditées en amont de leur utilisation afin d'en vérifier l'utilité et leur maintenabilité. Nous disposons d'un système nous permettant d'assurer automatiquement la vérification de montée de versions disponibles, associée à des CVE (recensement des failles et menaces) éventuelles. Cette vérification est effectuée tous les jours.
  Cela nous permet de prioriser des tests étendus afin de vérifier que ces montées de versions n'engendrent pas de régression, en parallèle de l'exécution des tests automatiques précisés dans le point précédent.

Afin de faciliter la gestion des évolutions, chaque brique logicielle composant la Numberly Martech Platform génère son propre “changelog” de manière automatique. Celui-ci étant souvent assez technique, chaque nouvelle version (*release*) de la solution s’accompagne d’une note permettant de comprendre les améliorations, les changements ou impacts auprès de nos utilisateurs. Cette release est réalisée en collaboration avec les équipes techniques et métiers, les *changelogs* aidant à faire le lien.

Une communication sera effectuée en respectant un délai de prévenance et une validation de la part des équipes du client. Celle-ci sera accompagnée du nom de la release et de son contenu. Nous invitons nos utilisateurs à confirmer la compréhension des changements, une démonstration ou formation est possible auprès de nos équipes pour fluidifier le processus.
Chaque changement s’accompagne par une qualification sur chacun des différents environnements (développement, recette/staging, production).
Dans un contexte de méthode agile, nous essayons d’utiliser au maximum des “features flag” pour aider nos partenaires à valider une nouvelle version. Cela désigne une technique de développement dont la principale mission est l’activation d’une ou plusieurs fonctionnalités sans nécessiter un déploiement de l’application.

Gestion des incidents de sécurité

Dans le cadre de l'organisation de la sécurité de l'information établit par les normes ISO-27001, Numberly dispose d'une procédure de gestion des incidents dédiés à la cybersécurité.
Ce document a pour objet de décrire les actions à effectuer en cas d'incident de Sécurité en définissant ce qu'est un incident, les catégories d'incidents, l'évaluation de leur criticité, le plan de communication à appliquer, les points de contacts et acteurs, ainsi que les actions générales à mener pour contenir l'incident, et enfin le rapport d'incident à formaliser incluant l'identification de pistes d'amélioration afin qu'il ne se reproduise plus.

Numberly s'engage à communiquer dans les plus brefs délais à ses clients, dans un délai maximum de 48h, tout incident relatif à la sécurité de la plateforme et des données.

Contrôle interne

Numberly fait auditer au minimum deux fois par an ses applicatifs en boîte noire et boîte blanche par des sociétés spécialisées et indépendantes afin de garantir un haut niveau de sécurité de la solution.
Il en va de même avec pour toute notre infrastructure, sur la surface externe comme la surface interne afin d'attester d'un haut niveau de sécurité sur les services hébergés et dans notre gestion des flux.
Pour cela Numberly travaille avec des sociétés renommées et fiables dans le monde de l'audit de sécurité (pentest et analyse de code) telles que Synacktiv ou Lexfo.
Nos contrats prévoient de manière standard la possibilité d'audits extérieurs mandatés par nos clients afin de leur démontrer le bon respect des obligations légales concernant le traitement et l'hébergement des données. Nous répondons régulièrement aux audits mandatés par nos clients et mettons en place les actions correctives le plus rapidement possible en conformité avec leurs exigences. Numberly s'engage à collaborer activement avec les auditeurs mandatés par ses clients et à remédier aux actions correctives dans les délais impartis.
Chaque remédiation sera expliquée techniquement à la DSI de nos clients et une preuve donnée de sa mise en œuvre effective.

Sur la partie organisation de la sécurité, Numberly a été régulièrement audité par des prestataires de nos clients.

En parallèle de ces audits externes, plusieurs contrôles internes sont définis, réalisés et revus par le comité SMSI de Numberly, tels que prévus par notre plan de contrôle.

Une sécurité des données irréprochable

Confidentialité des données

Protocoles web (IHM, API, ...)
L'ensemble des données en transit sont chiffrés à l'aide de protocoles TLS 1.2 minimum via les ciphers recommandés par le guide l'ANSSI.
Concernant les certificats TLS pour le HTTPS, nous utilisons des certificats basés sur les courbes elliptiques (ECC), recommandés par l'ANSII puisque plus sécurisés contre les attaques et plus performants que les clefs RSA.

Ces certificats ont une durée de vie de 3 mois, sont renouvelés automatiquement et sont monitorés.

Données stockées (bases de données, ...)
L'ensemble des données sont stockées et chiffrées:

- au repos : les données sont chiffrées à l'aide d'une clé symétrique AES-256 propre à chaque client, utilisée pour le stockage des données ainsi que les sauvegardes
- en transit : les données sont chiffrées en transit à l'aide de certificats TLS provenant d'une PKI interne (gestion d'autorité de certification) et ayant une durée de vie de 1 an. Le protocole utilisé est TLS 1.2.

L'ensemble de ces certificats sont sauvegardés dans un coffre fort HashiCorp Vault dont les accès sont sécurisés et limités aux seules personnes autorisées (équipe infrastructure devant opérer en astreinte).

Echanges de données par fichiers

Les échanges de données sont opérés par des systèmes d'échanges sécurisés et authentifiés.
Nous utilisons massivement le protocole SFTP via une authentification forte à base de clé SSH. Nous mettons en place également un filtrage par IP publique.

Cette plateforme SFTP est redondée et est disponible en actif-actif sur nos deux datacenters.

Conditions des données de test

Les données de l'environnement de développement sont réduites au strict minimum et sont bien sûr anonymisées. La sécurité de cet environnement est au même niveau que les autres environnements (production, préproduction).
Nous disposons de plusieurs procédures:

- génération de données de tests lorsqu'il n'est pas nécessaire d'utiliser des données venant de données de production
- anonymisation de données de production dans les rares cas nécessitant une reproduction de problèmes par exemple.

Ces procédures sont régulièrement utilisées et éprouvées.

Sauvegarde des données

Numberly héberge, en interne, une solution de stockage objet pour ses sauvegardes. Cette solution est redondée sur nos deux datacenters et utilise le principe d'Erasure Coding.

Des vérifications périodiques (1x par jour) sont réalisées sur les sauvegardes afin de vérifier leur intégrité. Des mécanismes de vérification d'intégrité de la donnée sont réalisés périodiquement par la solution et remontent des alertes en cas de perte d'intégrité sur les fichiers impactés. Toutes les sauvegardes sont compartimentées de manière logique, tout comme leurs accès. Aucune mutualisation n'est mise en place.

Le transfert des sauvegardes est chiffré de bout en bout, le stockage est également chiffré au repos. Les données sont chiffrées en AES 256 ou à l'aide de clés GPG publiques. En fonction du contexte client, nous pouvons chiffrer les sauvegardes à l'aide d'autres clés de chiffrement mais celles-ci devront être partagées avec Numberly afin de pouvoir tester les procédures de restauration et minimiser l'impact en cas d'incident nécessitant une restauration partielle ou totale.

La politique de sauvegarde est la suivante : complète tous les 3 jours, et transactionnelle toutes les 2 heures ou dès que le journal dépasse 1 Go.

La restauration de ces sauvegardes est testée tous les 2 mois. Selon la volumétrie nous mettons également en place des tests de restauration automatiques.

Traçabilité

Toutes les modifications opérées dans notre système d'information sont suivies, validées et tracées.

L'ensemble des accès, qu'ils soient internes ou externes, sont centralisés dans un système de journalisation centralisé et redondant.

Cela permet de surveiller de manière proactive les erreurs logicielles sur nos plateformes applicatives, mais aussi de s'assurer qu'aucun accès frauduleux n'est réalisé.

Par défaut, leur durée de rétention est fixée à 1 an.
S'agissant des conservation des traces d'accès aux données à caractère personnel, nous pouvons la paramétrer à 6 mois.

Toutes ces données sont exportables sur demande et seront envoyées dans un délai maximum de 3 jours.

L'ensemble des serveurs générant et centralisant ces traces utilisent les mêmes serveurs de temps de type Stratum 1.
La synchronisation avec ces serveurs de temps est monitorée et remonte des alertes critiques à notre astreinte en cas de non-conformité.

Réversibilité

La Numberly Martech Platform dispose d'un mécanisme de purge de données.

Numberly s'engage à traiter les demandes de purge formalisées par ses clients dans le périmètre de la prestation, et ce dans les meilleurs délais, ainsi qu'à fournir un rapport précisant le résultat et la méthode des purges demandées.

Numberly s'engage à maintenir le niveau de sécurité décrit dans le PAS jusqu'au terme de la prestation et à restituer de manière sécurisée toutes les données du client.

Numberly, dans la phase de réversibilité du contrat, met en place une procédure de destruction des données en fin de prestation et s'engage à détruire sous 30 jours ouvrés, ou toute autre durée convenue avec le Client, de façon définitive, l'ensemble des données du Client par le biais d'outils spécialisés. Un PV de destruction sera communiqué au Client au terme de cette procédure.

En cas de transfert de données, Numberly s'engage à garantir, lors du transfert vers le pouvoir adjudicateur, la sécurité et l'exhaustivité des données qui lui ont été confiées.

Nous mettrons à disposition via des mécanismes sécurisés (SFTP) l'ensemble des données de manière chiffrée (via AES, GPG, ..).

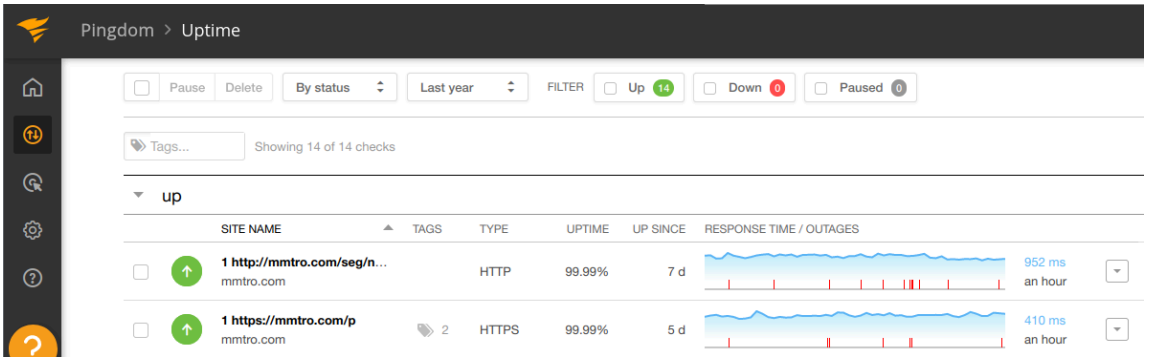
Disponibilité et supervision

La plateforme de Numberly permet de garantir une disponibilité de service élevée, à savoir :

- Une plage d'ouverture de service 24H/24h et 7j/7j,
- Une disponibilité d'au moins 99,5%, donc au-delà des exigences formulées dans le cahier des charges.

Pour garantir une transparence sur nos SLOs et plus précisement notre taux de disponibilité, nous passons par des acteurs tiers. A titre d'exemple, sur l'année dernière, notre taux de disponibilité était de >99.99%. Cette mesure est effectuée par un outil comme Pingdom.

Ci-dessous un exemple de sonde nous permettant de mesure notre SLI de taux de disponibilité



Grâce à notre totale maîtrise de la chaîne et notre indépendance, nous pouvons avoir une approche transverse au sein de notre SI pour adresser les problématiques de performance :

- Les temps de réponse sont monitorés
- Les seuils d'alerte sont définis et ajustés régulièrement selon les contraintes de nos clients
- Les indicateurs sont mis en forme via des outils de visualisation de données comme Grafana
- Les chiffres sont mis à disposition en temps réel via des systèmes de stockage de métriques (Prometheus) ou bien des via des calculs travaillant sur une plus grande plage de temps

De manière standard, nous supervisons les indicateurs suivants :

- Délivrabilité des campagnes (taux d'aboutis)
- Disponibilité des APIs et temps de réponse (cf. exemple ci-dessous)
- Temps moyen de transit d'une campagne
- Tableau de synthèse des incidents et indisponibilités éventuelles

L'ensemble des flux et actions sont enregistrés à des fins d'historisation et d'analyse. La solution enregistre en base de données des informations liées à :

- L'authentification : les authentifications sont tracées et permettent de savoir le succès ou non, la date et heure, l'IP ainsi que le port source utilisé et le nom d'utilisateur utilisé.
- La modification d'éléments métier : création/modification/suppression avec nom d'utilisateur et dates
- Diverses actions d'administration

L'ensemble de ces messages est centralisé et ils peuvent être consultés par les équipes Numberly sur une plateforme (GrayLog). Un contrôle strict est imposé sur les droits d'accès à ces logs de traitement informatique.

Nous sommes fiers d'avoir reçu le Technical Achievement Award for Outstanding Innovative Project de ScyllaDB. Ce projet vient récompenser la conception innovante de notre plateforme centrale de routage des messages qui met en œuvre des fonctions complètes de planification, de comptabilité, de traçage et, bien sûr, de routage des messages à l'aide des connecteurs de la plateforme ou de l'opérateur adéquats avec des garanties de robustesse et de fiabilité maximales, grâce à son idempotence, sa scalabilité et son observabilité.

Audits et contrôles de sécurité

Numberly fait auditer au minimum deux fois par an ses applicatifs en boîte noire et boîte blanche par des sociétés spécialisées et indépendantes afin de garantir un haut niveau de sécurité de la solution. Il en va de même avec pour toute notre infrastructure, sur la surface externe comme la surface interne afin d'attester d'un haut niveau de sécurité sur les services hébergés et dans notre gestion des flux. Pour cela Numberly travaille avec des sociétés renommées et fiables dans le monde de l'audit de sécurité (pentest et analyse de code) telles que Synacktiv.

Nos contrats prévoient de manière standard la possibilité d'audits extérieurs mandatés par nos clients afin de leur démontrer le bon respect des obligations légales concernant le traitement et l'hébergement des données. Nous répondons régulièrement aux audits mandatés par nos clients et mettons en place les actions correctives le plus rapidement possible en conformité avec leurs exigences. Numberly s'engage à collaborer activement avec les auditeurs mandatés par nos clients et à remédier aux actions correctives dans les délais impartis. Chaque remédiation sera expliquée techniquement à la DSI et une preuve donnée de sa mise en œuvre effective.