



Présentation ALEKSO

Marché UGAP - SCC

01 Stratégie et moyens ALEKSO



1.1 Qui sommes-nous



- ALEKSO, créée en Septembre 2018
 - Editeur de solutions de Cybersécurité
 - Opérateur de Télécommunications Sécurisées



- Une équipe d'experts : cybersécurité, infrastructures SI, réseaux
- Plus de 20 collaborateurs fin 2022
- Plus de 150 ans d'expérience cumulée en cybersécurité et SI
- Des solutions développées en ressources propres



- Une plateforme de services unique
- 2 Datacenters souverains (IDF et Grand-Est)
- 2 Centres de Services (Le Plessis-Robinson, Colmar)



- La volonté de proposer des offres simples et efficaces
- Des services sécurisés « by design »

1.2 Ils nous ont audité ... et référencé ...

En tant qu'Entreprise Innovante, investie dans la R&D en informatique de cybersécurité, ALEKSO bénéficie des aides et reconnaissances suivantes :

■ Innovation et R&D :

- JEI : « Jeune Entreprise Innovante » : nouvelle entreprise qui investit dans la R&D. Pour obtenir le statut, l'entreprise doit notamment être PME, création de moins de 11 ans, indépendante, réaliser des dépenses de R&D à hauteur de 15 % minimum des charges fiscalement déductibles au titre de cet exercice.
- CIR : « crédit d'impôt recherche » : mesure de soutien aux activités de R&D des entreprises. Les entreprises qui engagent des dépenses de recherche fondamentale et de développement expérimental peuvent bénéficier de déduction d'impôts.
- Accompagnement de la BPI : Banque Publique d'Investissement : organisme français de financement et de développement des entreprises, chargée de soutenir les PME, ETI et les entreprises innovantes en appui des politiques publiques de l'Etat et des Régions.

■ Cybersécurité

- Partenariat de recherche en cybersécurité avec le CNAM
- ANSSI : référencé « Prestataire Terrain »
- Cybermalveillance.gouv.fr : « Professionnel Référencé »
- Région Grand Est : ALEKSO est référencé comme partenaire des dispositifs suivants :
 - DIAG CYBER
 - CSIRT Grand-Est
 - GET Numérique

1.3 Notre positionnement

■ Objectifs : le «Projet » ALEKSO

- Répondre aux enjeux techniques et réglementaires des **Collectivités locales et territoriales, PME et ETI**
- Proposer une **solution « clé en main » de Cybersécurité**
- Apporter de la **simplicité** dans un marché complexe
- Miser sur la **modularité** pour développer la relation Client



Simple as a service

■ La démarche et les moyens mis en œuvre : le SOC Alekso

- Mise en œuvre d'une **plateforme propriétaire de cybersécurité**
- Développement et exploitation de solutions performantes et complémentaires
- Multiplication des solutions pour **augmenter la couverture sécuritaire**
- Développement du **Machine Learning et IA** pour améliorer l'analyse comportementale
- Expertise et analyse « humaine » par des analystes cyber.

■ Nos Solutions :

- Une **offre complète de Cybersécurité en SaaS**
- Des modules complémentaires adaptés aux usages



1.4 Les infrastructures et moyens ALEKSO

■ Une équipe pluridisciplinaire

- Experts Cybersécurité
- Développeurs
- Compétences réseaux et telecoms
- Exploitation et supervision
- Conduite de projet et Fonctions support



■ 2 DataCenters : Courbevoie et Strasbourg

- Souverains
- Infrastructures propriétaires Alekso
- Opérés par nos équipes

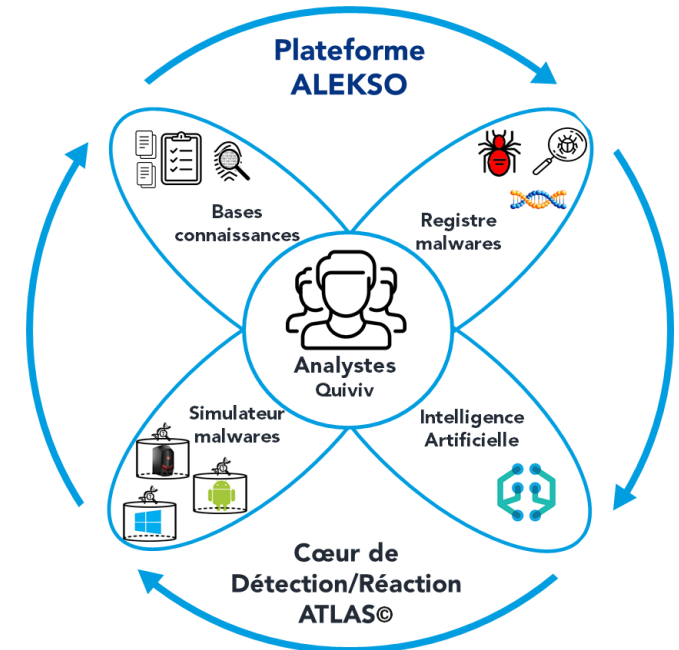


■ Centre de Support ALEKSO : hot-line et MCO/MCS

■ Portail QUIVIV : Gestion, ticketing et tableaux de bord

■ Le Cœur de Détection ATLAS

- Consolidation de 4 dispositifs automatisés conçus et animés par l'expérience des analystes QUIVIV
 - Fourniture des informations aux modules QUIVIV-Protect pour pouvoir choisir l'action à réaliser
 - En réponse à une sollicitation,
 - Sous forme de règles de protection
- Recueil des évènements pour analyse et conservation des traces
- Mise à jour et amélioration continue



02 Les solutions Quiviv by ALEKSO



Passez à la cybertranquillité.

2.1 Notre approche pour les Collectivités et PME/ETI

Approche unifiée et modulable :

- Des solutions par **modules** de sécurité, par équipement/instance à protéger
- Des modules complémentaires qui augmentent progressivement le niveau de sécurité
- Tous les modules bénéficient de notre plateforme de sécurité et de nos engagements (support, disponibilité, ...)
- Une sécurité augmentée pour répondre aux nouveaux enjeux de la cybercriminalité
- La conformité aux obligations légales

Offre de sécurité en mode SaaS : pour un budget maîtrisé

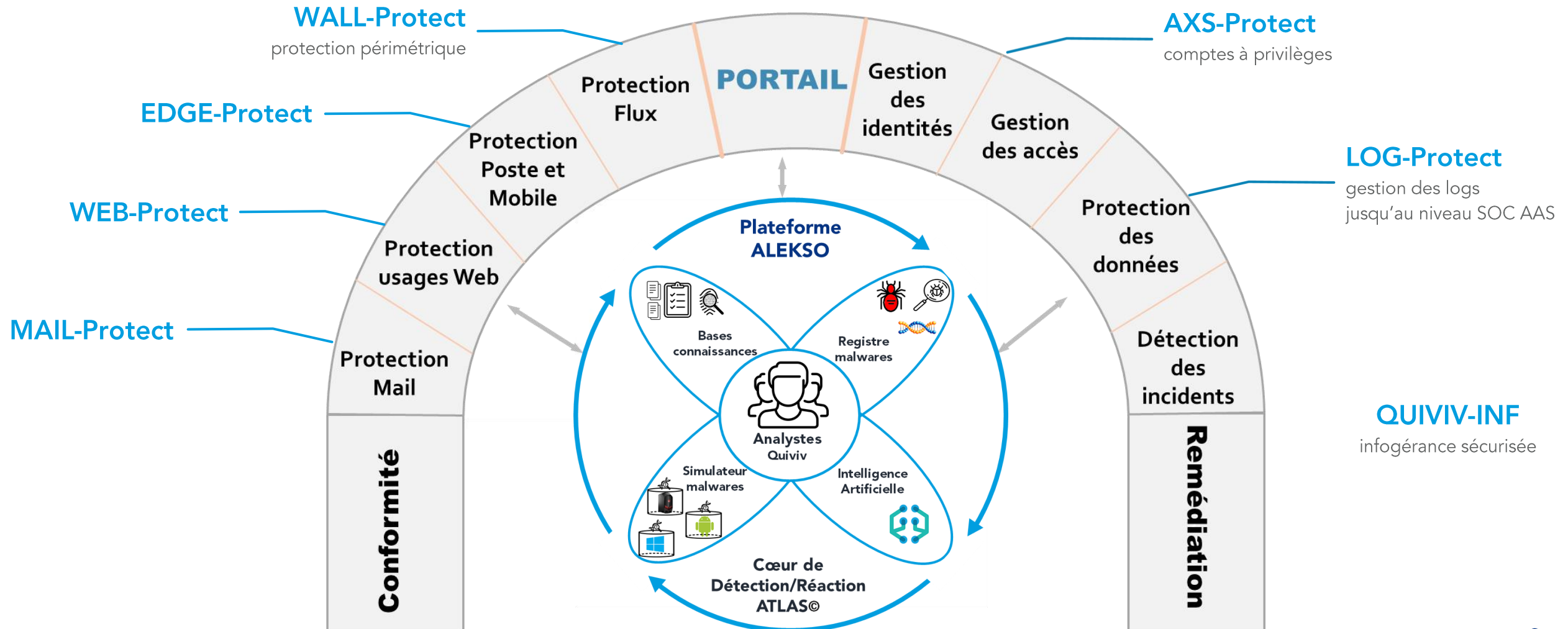
- Solution « clés en main »
- Licences à l'utilisateur ou au système à protéger
- Evolutive et opérée par une seule et même équipe au service de nos Clients
- MCO/MCS inclus dans la souscription

Notre Centre de Services : point de contact unique

- Support Client de 8h30 à 18h30 : mail, téléphone, tchat (français, anglais)
- Astreinte 24/7 sur incident critique

2.2 L'Offre de Service : QUIVIV

ALEKSO éditeur de Software Security-as-a-Service (SaaS)



2.3 Les services QUIVIV by ALEKSO

Les 4 Piliers de la sécurité

MAIL-Protect : messagerie

- ✓ Protection contre tous les types d'attaque
- ✓ Antivirus, anti-malware
- ✓ Antispam, antiphishing
- ✓ Arnaque au président, ...

WEB-Protect : navigation web

- ✓ Filtrage par catégorie de sites web
- ✓ Gestion de l'utilisation non conforme
- ✓ Anti-malware
- ✓ Protection contre l'exploitation des failles navigateurs
- ✓ Respect de la loi et de la PSSI
- ✓ Sécurité positive, ...

EDGE-Protect : PCs et serveurs

- ✓ Veiller au quotidien sur les signaux de sécurité : EPP/EDR
- ✓ Scan de vulnérabilités
- ✓ Protection contre les failles de sécurité système et applicatives
- ✓ Maintien de l'intégrité
- ✓ Correction des failles, ...

WALL-Protect : protection périmétrique

- ✓ Protection contre les tentatives d'intrusion, destruction,
- ✓ Protection contre les malware, vol de données, ...

Les services avancés

LOG-Protect : gestion des logs >jusqu'au niveau SOC AAS

- ✓ Collecte des événements de sécurité
- ✓ Issus de tous les composants d'infrastructures (Cloud, on-premise)
- ✓ Normalisation, Enrichissement (« parsing »)
- ✓ Stockage, archivage sur 12 mois glissants
- ✓ Analyse par corrélation d'événements
- ✓ Détection des alertes de sécurité
- ✓ Remédiation sur incidents de sécurité, ...

AXS-Protect : authentification des accès

- ✓ Protection des accès sur vos infrastructures (cloud, on-premise)
- ✓ Simplification de la gestion des mots de passe et identités
- ✓ Accès unique indépendant du positionnement des machines cibles,
- ✓ Traçabilité totale des actions et des accès
- ✓ Service d'analyse des fichiers échangés, ...

QUIVIV-INF : infogérance sécurisée

- ✓ PCs, serveurs, network, NAS, ...
- ✓ Prise en charge et maintien en conditions opérationnelles
- ✓ Supervision et management
- ✓ Détection, gestion et suivi des incidents
- ✓ Relation avec tiers mainteneurs
- ✓ Visibilité sur le suivi opérationnel
- ✓ Gestion des bases documentaires.

2.4 L'accompagnement QUIVIV : services inclus

- Le Cœur de Détection ATLAS

- L'accès au Portail de Gestion HYPERION

- L'accès au Centre de Service ALEKSO (hot-line)

- L'accès aux fonctions de sécurité au travers d'une appliance logicielle dédiée au Client.
- La mise à disposition d'une interface de gestion du Service Fonctionnel dédiée au Client, qui permet :
 - d'accéder aux paramètres de sécurité,
 - d'accéder aux indicateurs générés,
 - d'accéder aux éventuels tickets d'incidents.
- Disponibilité du support en H8/5 et astreinte 24/7 sur incident critique
- Plateforme opérationnelle et supervision 24/7

- Les demandes de changement

- Le traitement des alertes de sécurité

- Prise en compte d'une Alerte de Sécurité : en moins de 2 heure,
- Traitement d'une Alerte de Sécurité : en moins de 8 heures,
- Traitement d'un Incident de Sécurité : en moins de 24 heures.

*Services inclus dans chacun
des modules Quiviv*

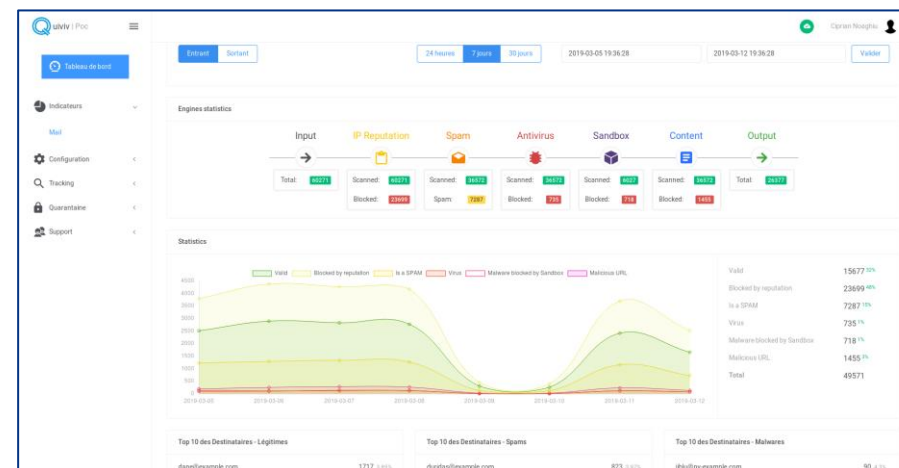
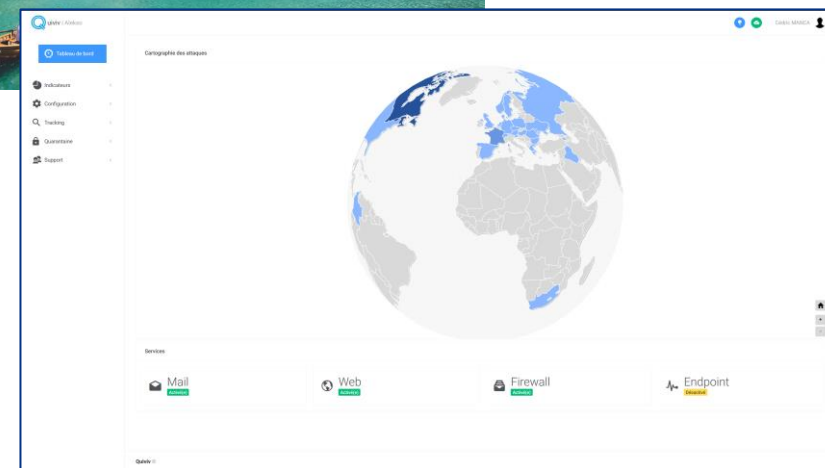
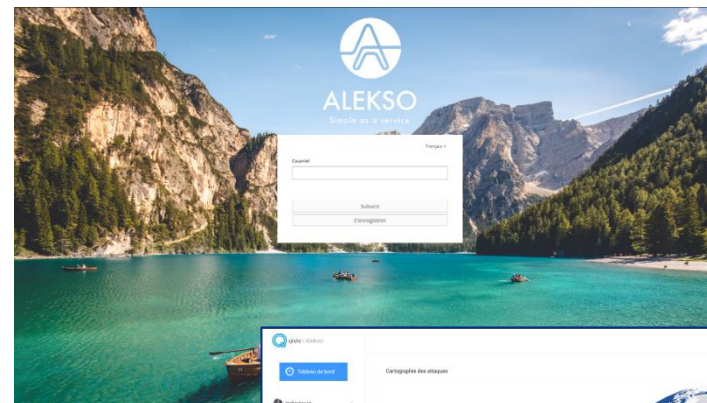
Type de Changement	Nombre inclus par période de 12 mois	Délai maximal de prise en compte	Exemples
Mineur	Illimité	1 jour ouvré	- mises à jour des bases de détection
Majeur	6	2 jours ouvrés	- ajout d'un nouveau composant d'analyse dans la chaîne de détection
Demande	36	3 jours ouvrés	- fourniture de journaux d'événements de sécurité bruts, - investigations sur les journaux d'événements de sécurité disponibles.

2.5 Extranet QUIVIV

Associé à notre service, le Client a accès à notre portail de gestion et suivi des services :

Un portail web unique pour tout piloter

- Authentification par SSO, en simple ou multi-facteurs
- Gestion des accès par profil :
 - ✓ Profil « Utilisateur »
 - ✓ Profil « Administrateur »
 - ✓ Profil « Super-Administrateur »
- Possibilité de construire des profils personnalisés
- Possibilité d'affecter chaque profil à une entité ou un service
- Suppression de la complexité technique des produits utilisés



Nos engagements

- SLA contractualisés
- Garantie de disponibilité de la plateforme **Quiviv** à 99,98%, 365 jours par an et 24x7

Nos services

- Equipe dédiée au service BUILD et RUN
- Support niveau 1, 2 et 3
- Contact direct avec les collaborateurs du Client ou avec une équipe dédiée au sein de l'Entreprise
- Contact direct et immédiat en cas d'incident de sécurité
- Services rendus de 8h30 à 18h30, en jours ouvrés
- Astreinte H24/7 pour le traitement des incidents critiques
- Accès en temps réel permanent au portail de suivi de l'activité du service
- Traitement des changements en 36 heures ouvrées (moyenne)
- Traçabilité totale
- Archivage légal des traces
- Réversibilité

99,98%

Disponibilité de nos plateformes

