45’ pour découvrir notre SOC souverain : votre bouclier par Linkt !

Votre webinar va bientôt commencer

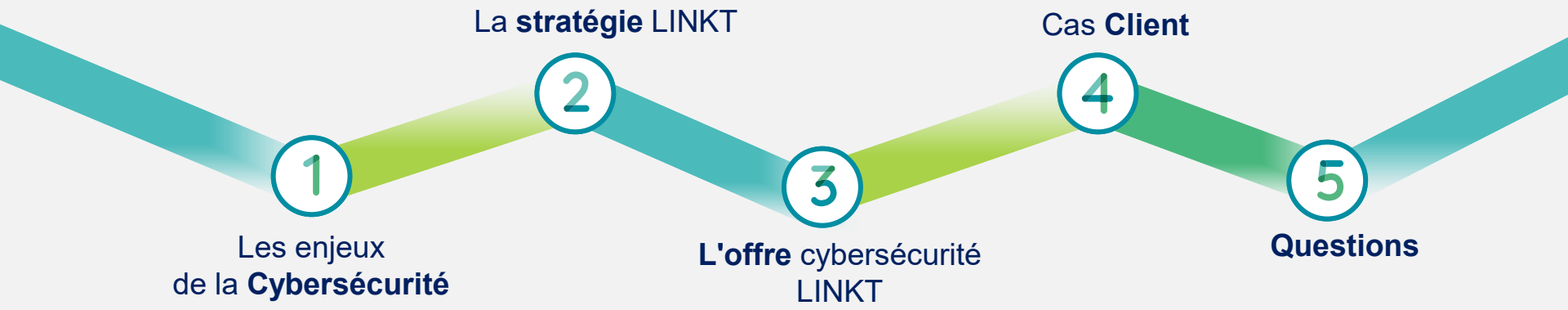
VOS INTERVENANTS

Bruno BOUTET
Directeur BU Cybersécurité

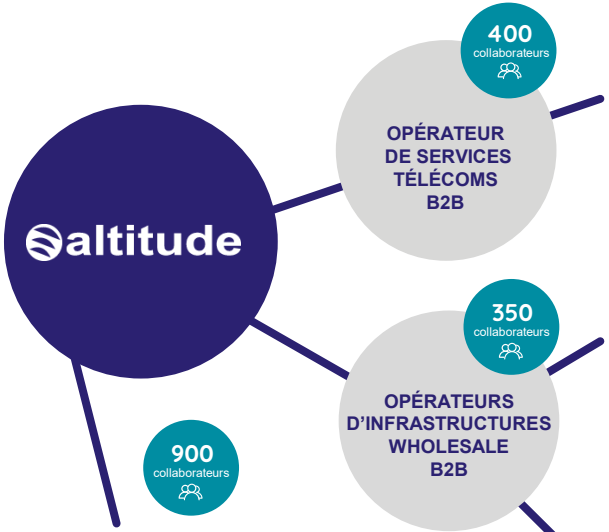
Lidao BILESAH
Architecte cybersécurité

Pierre MEGANCK
Chef de projet cybersécurité

SOMMAIRE


1
Les enjeux de la **Cybersécurité**
2
La **stratégie** LINKT
3
L'offre cybersécurité LINKT
4
Cas **Client**
5
Questions

UN GROUPE ENGAGÉ DANS LES TÉLÉCOMS B2B



Linkt

Opérateur de services Télécom 100% B2B
Linkt adresse les besoins critiques des entreprises et collectivités en services télécoms, intégration, cybersécurité et Cloud.

COVAGE

Opérateurs d'Infrastructures Fibre Optique Entreprise
L'acteur **wholesale B2B fixe** 3e réseau fibre optique par sa capillarité.

altitude Infra.

Leader de l'aménagement numérique du territoire et premier partenaire des collectivités locales
4,5 millions prises FTTH

Airmob.net

Opérateur Full MVNO 5G
L'acteur **wholesale B2B mobile** alternatif des opérateurs.

817 millions d'€ de CA en 2024

+ 2 000 collaborateurs sur l'ensemble du territoire

5 milliards d'€ d'investissements sur 2017-2022

+ 150 000 entreprises raccordées en 2024

Un groupe indépendant, conscient de son impact social, sociétal et environnemental.

1. Les enjeux de la cybersécurité

LES DÉFIS DE LA CYBERSÉCURITÉ DES ÉQUIPES IT

Recrudescence de la **menace Cyber** tous secteurs – **49%** des organisations impactées en France **2024 (Allianz)**
Industrialisation de l'écosystème cybercriminel
Perfectionnement des attaques (IA, Deepfake,...)

Augmentation de la **surface d'attaque**
(OnPrem, Cloud, Hybride, Nomadisme, Transformation Numérique , IA …)

Renforcement des obligations **légales et réglementaires,**
Incertitudes sur le plan géopolitique

Linkt

ÉTAT DES LIEUX DE LA CYBERSÉCURITÉ

Dans le monde

Les vols d'identifiants, Phishing, Vulnérabilités sont les **3 principaux vecteurs** exploités dans les **cyberattaques**

Source : DBIR 2024

15 % des incidents impliquaient des partenaires

Source : DBIR 2024

+280 000

D'échantillons de programmes malveillants et d'applications indésirables par jour

Source : Av-Atlas 2025

France

75 %
des cyberattaques sont opportunistes
InterCERT France (2024)

27
jours en moyenne entre l'intrusion et la détection
InterCERT France (2024)

50
jours est la durée moyenne d'une crise cyber
InterCERT France (2024)

RÉGLEMENTATIONS ET SOUVERAINETÉ

Les lois extraterritoriales

un risque pour la souveraineté des données

Cloud Act, FISA, Patriot Act : Accès des autorités américaines aux données des entreprises, même hébergées à l'étranger

National Intelligence Law (Chine) : Obligation pour les entreprises chinoises de coopérer avec les services de renseignement, y compris via la transmission de données.

Les lois européennes

pour renforcer la cybersécurité et la souveraineté

RGPD : Protection des données personnelles et limitation des transferts vers des pays tiers.

NIS2 : Renforcement des exigences de cybersécurité pour les infrastructures critiques en Europe.

DORA : Sécurisation du secteur financier face aux cybermenaces et garantie de la résilience numérique.

RÉGLEMENTATIONS ET SOUVERAINETÉ

Accélération de la réduction de la dépendance aux technologies non-européennes

Pays-Bas
Mars 2025

Le Parlement néerlandais adopte des motions pour réduire l'usage de logiciels américains, au nom de l'autonomie stratégique et de la cybersécurité.

➤ Contexte géopolitique marqué par la présidence de Donald Trump.

Danemark
Juin 2025

Le ministère de la Digitalisation, Copenhague et Aarhus abandonnent progressivement Microsoft 365 et Azure.

➤ Adoption d'alternatives open source : LibreOffice & Linux.

Ville de Lyon
Juin 2025

Transition annoncée vers des outils souverains : Territoire Numérique Ouvert (suite collaborative, data centers régionaux), OnlyOffice, Linux, PostgreSQL.

➤ Souveraineté numérique, soutien à l'écosystème local, réduction de l'empreinte environnementale.

2. LA STRATÉGIE LINKT

SOUVERAINETÉ DES DONNÉES VS SOUVERAINETÉ TECHNOLOGIE

Souveraineté des données	Souveraineté technologique
Souveraineté légale où les fournisseurs utilisent des technologies étrangères/américaines dans un contexte sécurisé (hébergement local, chiffrement …)	Vise à développer une propriété industrielle et à soutenir des éditeurs européens pour viser l'indépendance technologique.

Le SOC 6e Sens est basé sur le modèle de souveraineté technologique

UN SERVICE 100% SOUVERAIN

- **Une infrastructure SOC hébergée en France** chez un fournisseur Cloud Français.
- **Service labellisé France Cybersecurity**, membre Hexatrust.
- **Un choix unique** de regrouper les Éditeurs Français par vecteur d'attaque pour mieux défendre nos clients et protéger la confidentialité de leurs données.
- **Un service 24/7 100%** effectué sur le territoire national .
- **Solutions de sécurité françaises**, hébergées en France, avec des labels de confiance :

VISA DE SÉCURITÉ ANSSI

FRANCE CYBER SECURITY

LOGICIELS FRANÇAIS UTILISÉ PAR LES ARMÉES FRANÇAISES

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Linkt

3. L'OFFRE CYBERSÉCURITÉ LINKT

LINKT PROTÈGE VOTRE SI ET PÉRENNISE VOTRE ACTIVITÉ

Cyber SOC souverain
(Security Operation Center)

- SOC : Anticipation, Détection et Réponse aux incidents de cybersécurité
- CSIRT / Gestion de crise

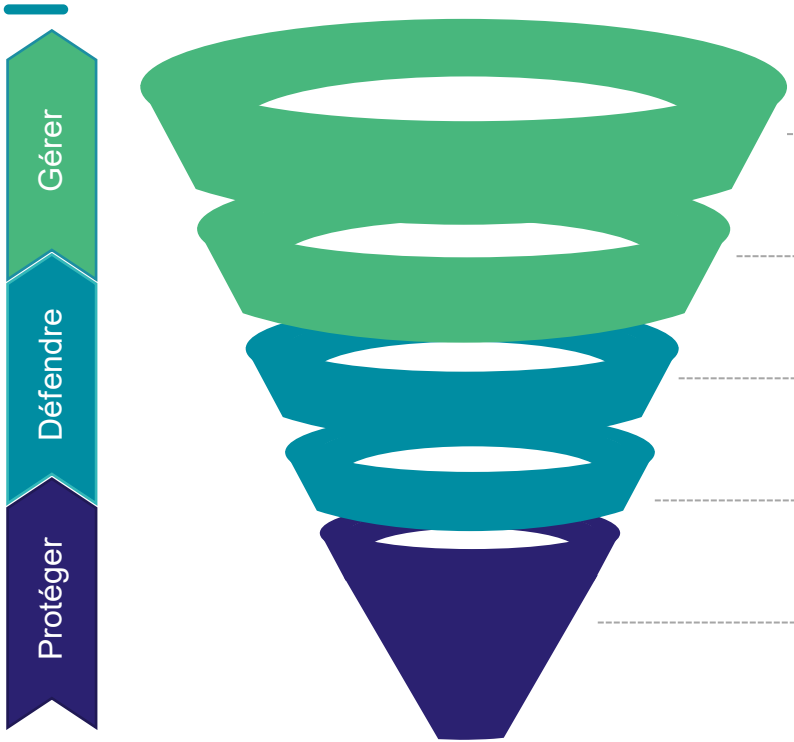
Diagnostic de maturité

- Analyse de maturité Cybersécurité
- Feuille de route de cybersécurité

Sensibilisation au risque Cyber

- Campagnes de phishing et de sensibilisation utilisateurs

AMÉLIORATION DE LA POSTURE CYBERSÉCURITÉ



Stratégique
Tableau de bord SSI

Conforme
Audit , Conformité ANSSI, NIS2, DORA, ISO27K, …

Proactive
CTI,CSIRT, Exercices CyberCrise

Réactive
EDR, SIEM, NDR, SOAR, UBEA

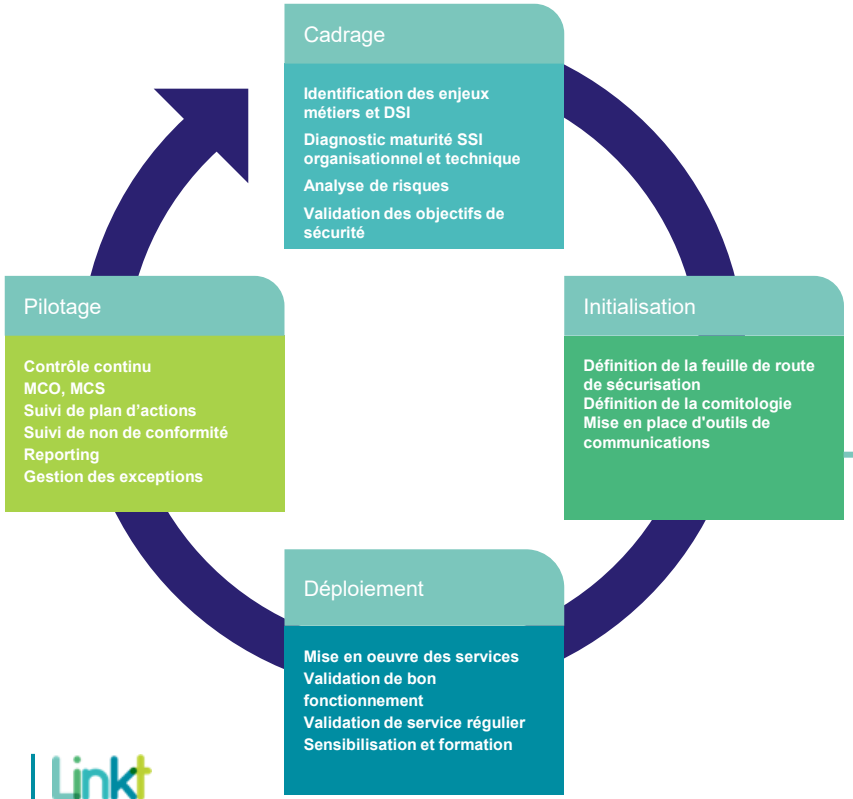
Préventive
AVV, EPP, FW, PROXY, WAF , VPN, MFA, PAM, MTD, ZTNA Anti-Spam, Anti-phishing, Sensibilisation

Notre clientèle

Aéroport
Industriel
Assurance
Collectivité territoriale
Cabinet de propriété Intellectuelle
Société de service Cyber
Armateur
Retail
Energie

4. CAS CLIENT

UNE DÉMARCHE STRUCTURÉE ET FLEXIBLE



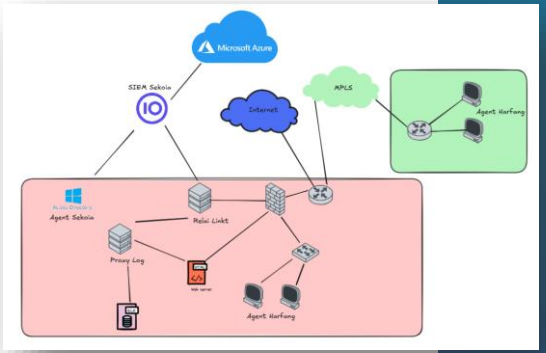
Montée en maturité du SOC

Attaques opportunistes
Hygiène cyber

Attaques ciblées
Menaces internes
Chaîne d'approvisionnement
Exigences de conformité

CAS CLIENT - CONTEXTE

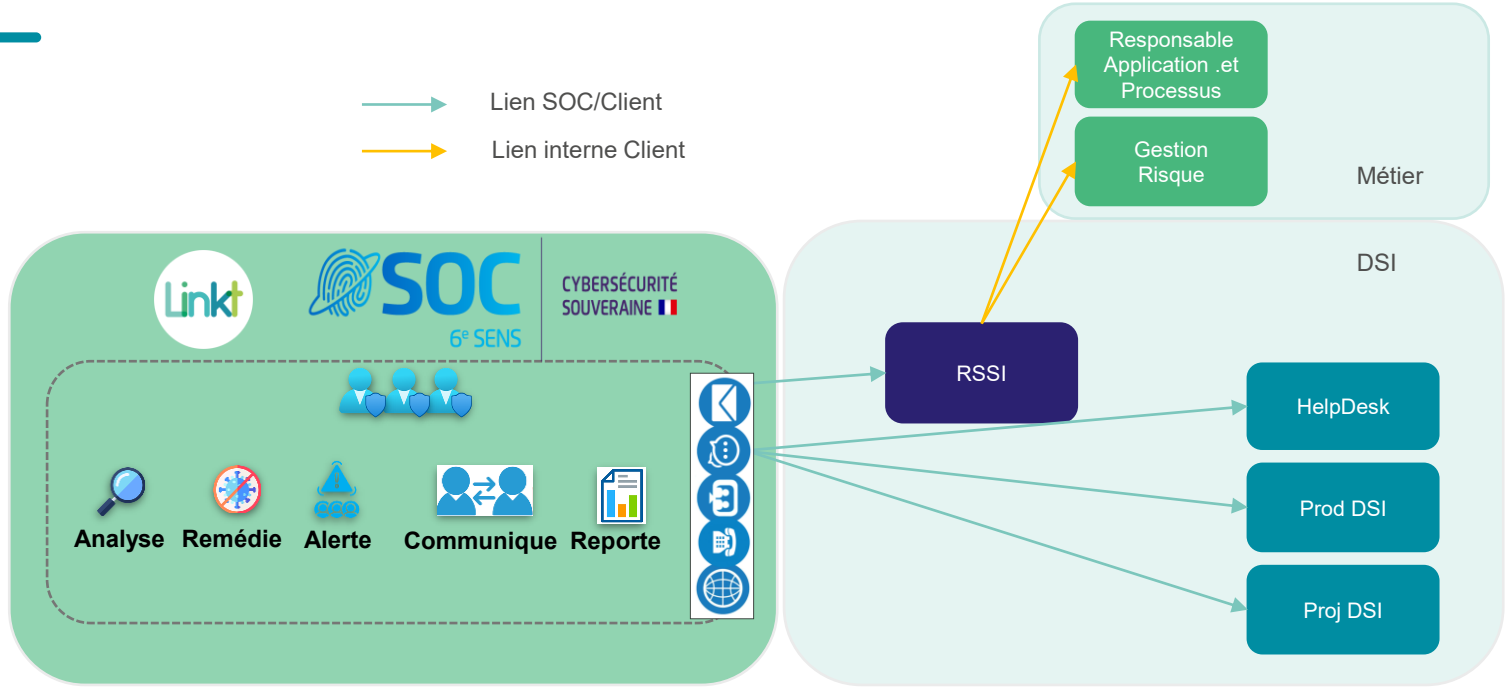
- **Périmètre**
  - Energie
  - Multi sites
  - 1800 utilisateurs
  - 400 serveurs (Windows + Linux)
  - 1800 Pdt
  - 120 actifs périmétriques (FW, WAF, Proxy , Bastion)
- **Enjeux cybersécurité**
  - Absence d'équipe dédiée à la cybersécurité
  - Absence de visibilité centrale du SI
  - Pas de supervision 24/7
  - Pas de cartographie du SI
  - Besoin de conformité NIS 2



Bénéfices obtenus:

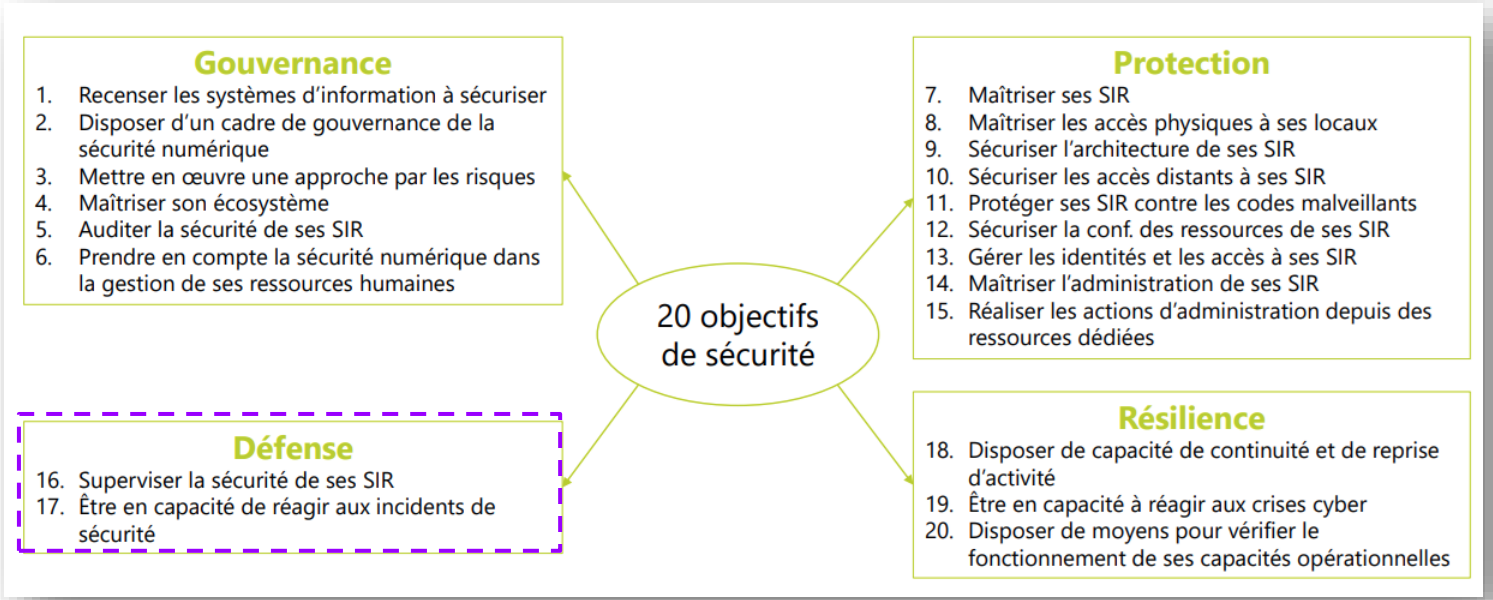
- Réduire l'impact d'une cyberattaque
- Conformité NIS2
- Inventaire des assets critiques
- Accès continu aux métriques opérationnels
- Supervision 24/7 des évènements de sécurité
- Accompagnement en phase de réponse incident
- Recommandations d'amélioration continue de la posture cybersécurité

LA GOUVERNANCE DU SERVICE SOC



Pour garantir une communication efficace et une priorisation adéquate des demandes du SOC, le projet a bénéficié de l'appui de la direction

NIS2 : L'INTÉRÊT D'UN SERVICE SOC



Les 4 piliers et 20 objectifs de sécurité pour une approche holistique et structurer de la mise en place des mesures NIS2

LES FACTEURS DE SUCCÈS D'UN SOC

Protection 360

- Assurer une protection et une visibilité sur chaque vecteur d'attaque

Souveraineté

- Garantir la localisation des données en France ou au sein de l'UE
- Assurer l'immunité contre les lois extraterritoriales

Proximité

- Apporter un service transparent et une communication fluide avec les clients à partir d'outils collaboratifs sécurisés

Flexibilité

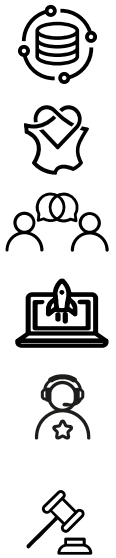
- Adapter le service par rapport au contexte client
- Faciliter la réversibilité

Conseil

- Fournir des recommandations et un plan d'action d'amélioration continue de la posture cybersécurité

Conformité

- Apporter la réponse aux exigences de journalisation et signalement des incidents de sécurité



MERCI DE VOTRE ATTENTION