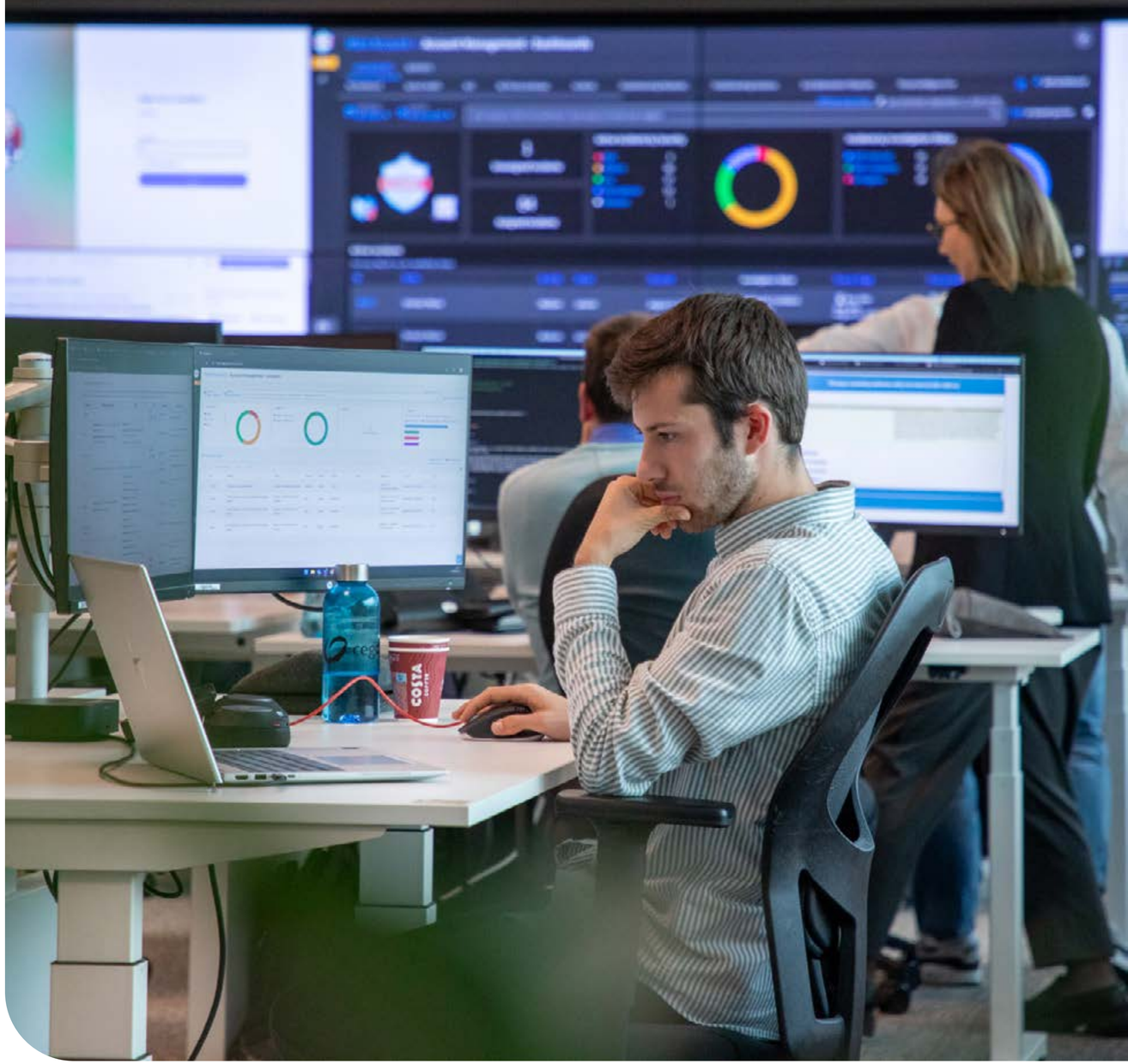
nsi

La cybersécurité, un impératif stratégique

Construisez votre chemin vers la cyber-résilience



Livre blanc

La menace cyber n’est plus un simple incident technique : elle représente aujourd’hui **un risque majeur pour la continuité, la confiance et la performance des organisations**.

Dans un environnement où les attaques gagnent en vitesse, en sophistication et en automatisation, seules les entreprises capables d’**anticiper et de réagir plus vite que les attaquants** peuvent protéger durablement leurs opérations.

Renforcer sa posture cyber, c’est donc **protéger son activité, ses clients**… et sa capacité à rester compétitif dans un marché où la résilience devient un **avantage stratégique**.

Table des matières

Introduction	4
Etape 1 - Evaluer	6
Etape 2 - Prioriser	8
Etape 3 - Prévenir	10
Etape 4 - Détecter & répondre	12
Etape 5 - Récupérer	14
Etape 6 - Gouverner	16
Les domaines d’expertise cyber de NSI	18
Pourquoi NSI ? Votre partenaire de confiance	18
Conslusion	19

01

Introduction
La cybersécurité, un impératif stratégique

Introduction

La cybersécurité, un impératif stratégique

La transformation numérique a profondément remodelé les modèles d'affaires. Chaque fonction de l'entreprise dépend désormais d'un système d'information toujours plus ouvert, distribué et interconnecté. Cette dynamique crée des opportunités… mais aussi une exposition accrue à des menaces rapides, sophistiquées et souvent invisibles.

Les chiffres sont sans appel :

51 %

51 % des entreprises victimes d'une perte de données sévère cessent leurs activités dans les deux ans.

Source: VikingCloud 2025 SMB Threat Landscape Report

4,45 M$

Le coût moyen d'une violation de données dépasse 4,45 millions de dollars.

Source: IBM, Ponemon Institute

19 secondes

Un ransomware a frappé une entreprise toutes les 19 secondes en 2024.

Source: DNI – Worldwide Ransomware 2024

Ajoutons à cela une pression réglementaire croissante (NIS2, DORA, ISO 27001, CyFUN) et nous obtenons un constat clair :

La cybersécurité n'est plus une question IT. C'est une question de gouvernance, de continuité et de compétitivité.

Pour répondre à ces enjeux, les organisations doivent adopter une approche structurée, progressive et mesurable : **la cyber-résilience**.

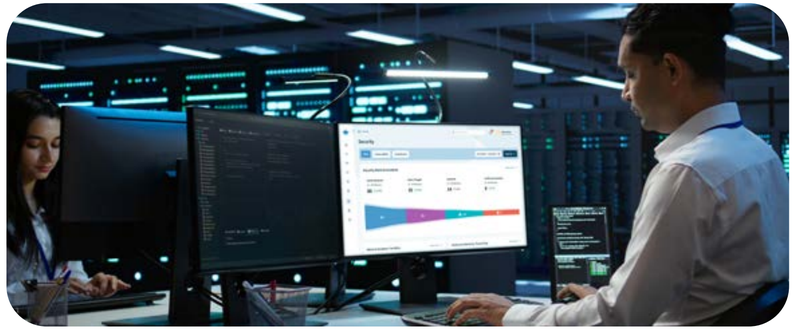
Ce livre blanc propose un **parcours en 6 étapes**, enrichi de retours d'expérience, d'indicateurs clés, et de solutions concrètes issues de l'écosystème NSI.

02

Etape 1 - Evaluer

Diagnostic cybersécurité 360°

Avant d’agir, encore faut-il comprendre.
Le diagnostic constitue votre **point de départ**.



Objectif : obtenir une vision claire et complète de votre posture de sécurité.

Sans diagnostic, impossible d’identifier les points faibles, les actifs critiques, ou les angles morts de votre organisation.

Ce que couvre un diagnostic 360° :

- Actifs sensibles (serveurs, données, applications critiques)
- État des protections et des contrôles en place
- Exposition aux menaces (ransomwares, phishing, DDoS, compromission d’identités)
- Préparation organisationnelle (politiques, processus, sensibilisation)
- Analyse M365 / Azure
- Conformité aux référentiels (ISO, CyFUN).

Exemple concret

Lors d’un diagnostic mené auprès d’un industriel, **35 % des comptes à privilèges restaient actifs après le départ de collaborateurs**, créant une surface d’attaque majeure. Leur suppression a immédiatement renforcé la posture globale.

03

Etape 2 - Prioriser

Analyse & plan de traitement des risques

Une fois les vulnérabilités identifiées, l’enjeu devient la priorisation

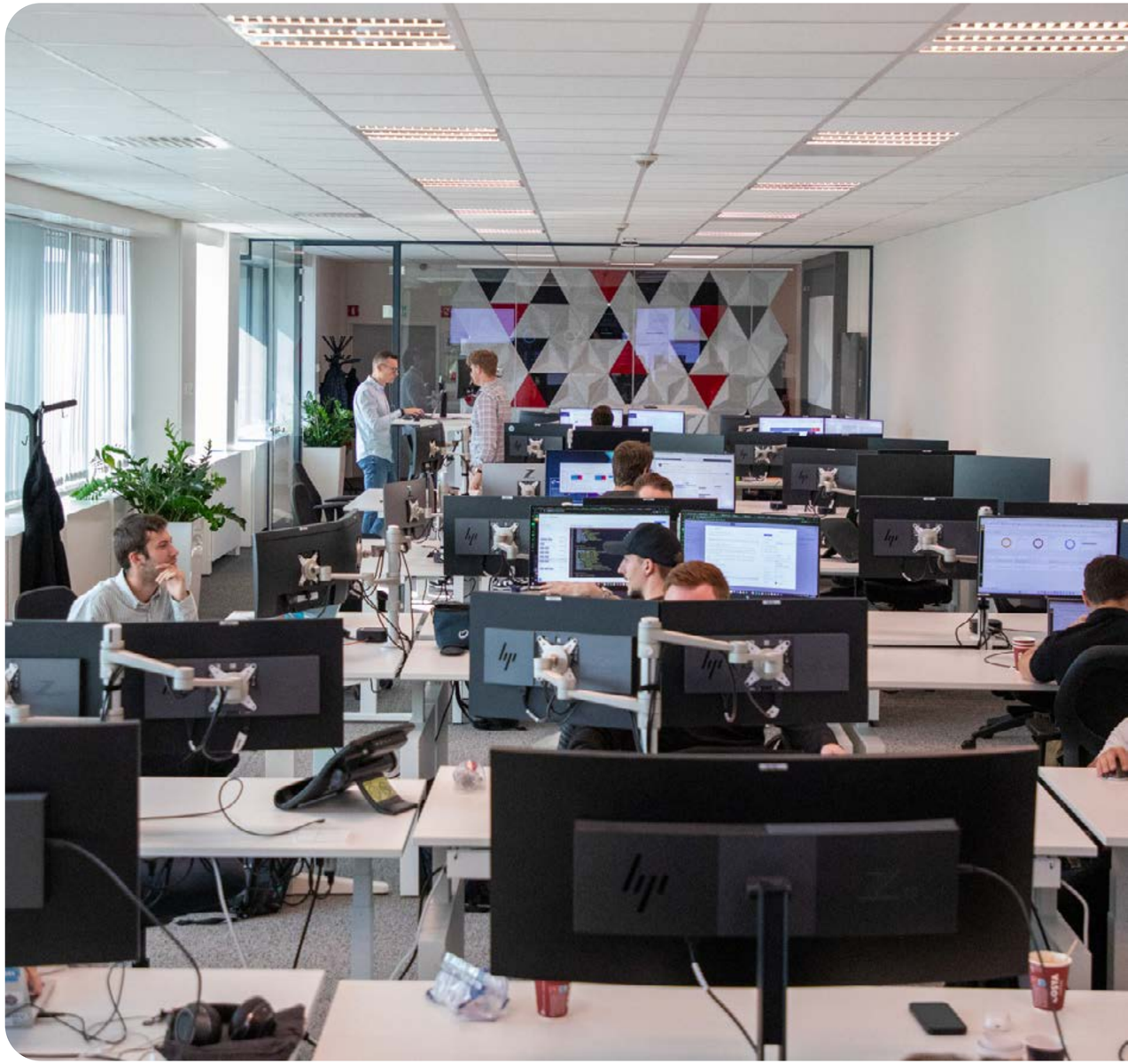
Objectif : transformer l’analyse en feuille de route exploitable.

Cette étape hiérarchise les risques selon leur **probabilité** et leur **impact opérationnel**, **financier ou réputationnel**.

Éléments clés de l’analyse :

- Cartographie réseau et segmentation
- Analyse sur les politiques de cyber sécurité existantes et procédures
- Circulation des données sensibles
- Vulnérabilités techniques (scans + tests manuels)

À retenir : agir en priorité sur les vulnérabilités exposées à Internet et les accès à privilèges permet de réduire **70 % de la surface d’attaque**.



04

Etape 3 - Prévenir

Sensibilisation, outils & alignement

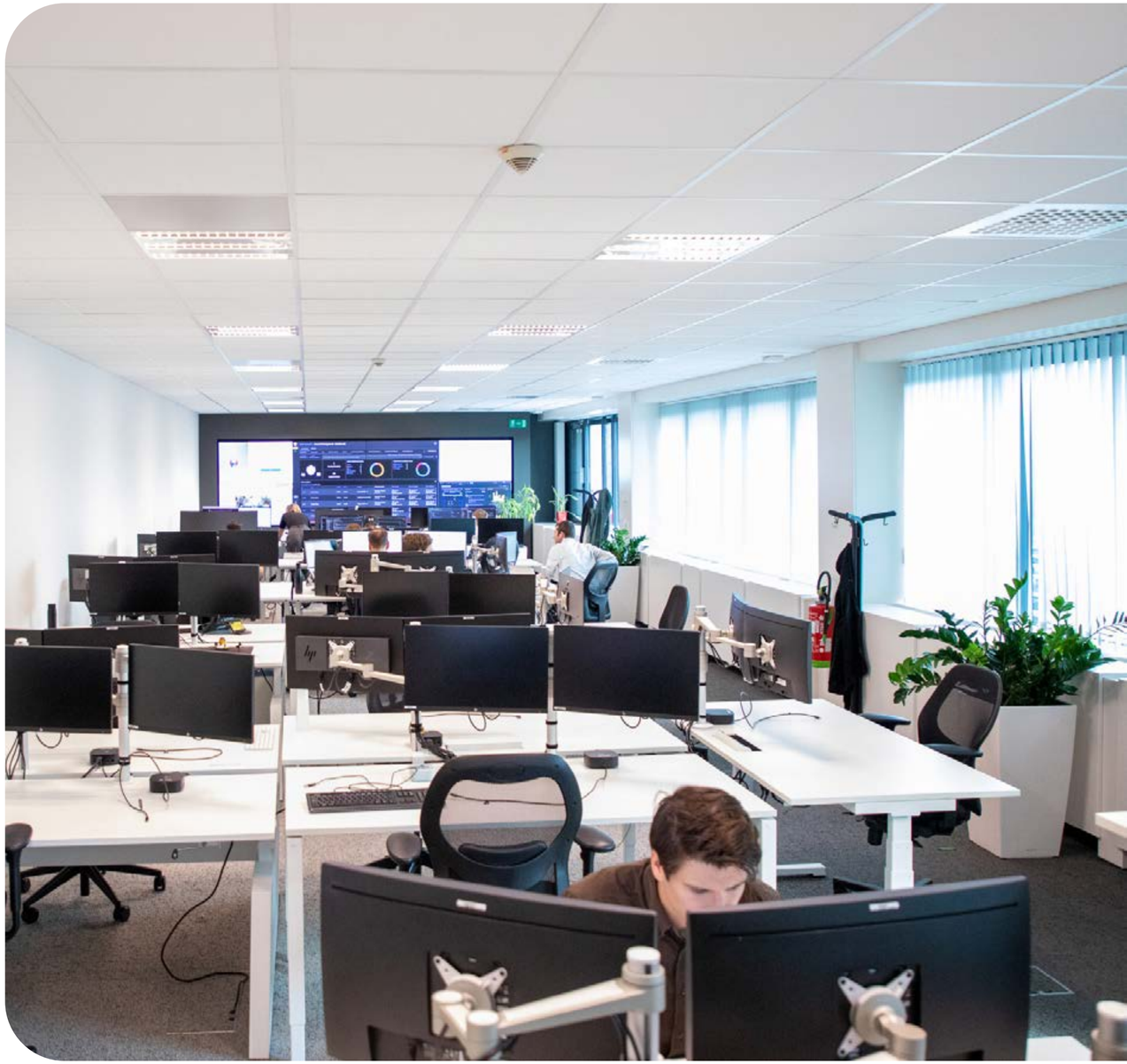
La meilleure technologie ne suffit pas si les collaborateurs ne sont pas alignés.

Objectif : réduire le risque humain et structurer le cadre organisationnel.

3 piliers incontournables :

- **Technique** :
  SIEM, EDR/MDR, patch management automatisé.
- **Humain** :
  Campagnes de sensibilisation, phishing simulé, formation.
- **Organisationnel** :
  Clarification des rôles, procédures documentées, chaîne d'escalade.

Cas client
Un acteur public a réduit **40 % des incidents liés au phishing** en 12 mois grâce à un programme de sensibilisation NSI.



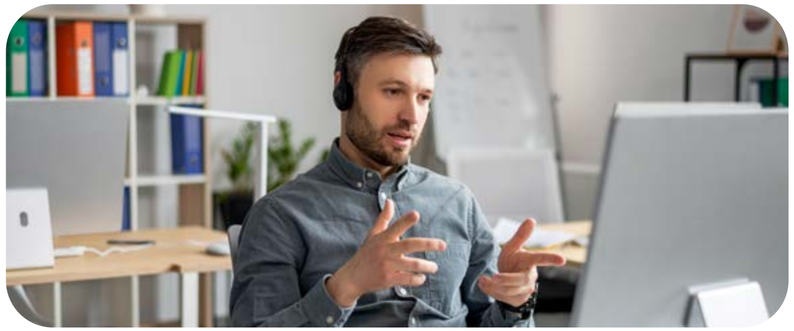
05

Etape 4 - Détecter & répondre

Le role central du soc

La rapidité de détection conditionne la gravité de l'incident.

Sans SOC, une attaque reste en moyenne 280 jours non détectée. Avec supervision active, la détection tombe à quelques heures.



Objectif : détecter précocement et répondre immédiatement.

Les défis actuels :

- Pénurie de compétences
- Attaques 24/7 (nuit, week-end, congés)
- Obligations réglementaires (NIS2, CyFUN)
- Ressources internes saturées .

Le SOC NSI - votre tour de contrôle en 24/7

Le SOC NSI fournit une supervision éprouvée, capable de :

- Détecter les comportements anormaux
- Qualifier & prioriser les incidents
- Intervenir immédiatement dans les premières actions
- Vous accompagner dans le containment et la reprise
- Fournir indicateurs, tendances et recommandations

Pourquoi choisir NSI ?

- Intervention rapide dès la détection d'un comportement suspect
- Équipe certifiée et multisectorielle
- Alignement CyFUN pour accélérer votre conformité NIS2
- Industrialisation & fiabilité d'un SOC managé
- Vision complète des infrastructures clients (réseau, identité, cloud...)
- Expertise en Incident Response Team (IRT), de la gestion de crise à la remédiation complète

06

Etape 5 - Récupérer

Continuité et reprise d’activité

Une attaque peut impacter votre activité… mais elle ne doit pas l’arrêter.

Objectif : maintenir l’activité et restaurer rapidement les opérations.

Composantes clés :

- Plans de réponse & reprise d’activité testés régulièrement
- Exercices de crise impliquant la direction
- Analyse postincident pour renforcer la posture future

Cas client
Grâce à un PRA testé trimestriellement, une société de services a restauré ses opérations en moins de **2 heures** après un ransomware.

07

Etape 6 - Gouverner

Conformité, pilotage & amélioration continue

La maturité cyber devient un facteur de confiance, de crédibilité et de performance.

Objectif : démontrer vos efforts, rassurer vos parties prenantes et structurer une amélioration durable.

Cadres clés :

- ISO 27001
- NIS2
- DORA
- CyFUN

Pourquoi viser la conformité ?

- Réduction du risque
- Renforcement de la confiance (clients, investisseurs, autorités)
- Baisse potentielle du coût des assurances
- Alignement des pratiques internes et partenaires

L'accompagnement NSI NIS2

NSI fournit un dispositif complet, du périmètre à la mise en œuvre : analyse de maturité, feuille de route, Security Advisor, suivi des actions, contrôle de l'efficacité.

(Les risques : Réduction du risque cyber et des arrêts opérationnels associés.**)**

Les domaines d'expertise cyber de NSI

NSI couvre l'ensemble du spectre cyber grâce à une expertise pluridisciplinaire :

- **Secure Endpoint**
  Protection, chiffrement, MDM, hardening, DLP
- **Secure Identity**
  MFA, IAM, XDR, gouvernance des identités
- **Secure Network**
  Firewall, SDWAN, NAC, détection réseau
- **Secure Server**
  Protection serveurs physiques/virtuels, hardening, EDR
- **Secure Platform (Cloud)**
  Cloud security, container security, XDR cloud
- **Secure Code**
  DevSecOps, WAF, tests d'intrusion, code analysis
- **Secure Facility**
  Sécurité physique : caméras, alarmes, contrôle d'accès
- **Secure IA**

Pourquoi NSI ? Votre partenaire de confiance

Avec plus de 30 ans d'expérience, NSI offre une approche :

- **Intégrée** :
  IT + Cyber, de la conception à la remédiation.
- **Industrialisée** :
  Services managés, SOC 24/7, processus éprouvés.
- **Certifiée** :
  ISO 27001 et ISO 9001.
- **Proche du terrain :**
  Présence en Belgique, Luxembourg et France.
- **Pluridisciplinaire** :
  Ingénieurs, analystes, pentesters, Security Advisors.
- **Orientée amélioration continue** :
  Gouvernance, conformité, modernisation

Conclusion

La cyber-résilience n'est pas un état final.

C'est une **démarche continue**, un avantage compétitif et un facteur de confiance.

En suivant ce parcours en 6 étapes, votre organisation renforce sa capacité à :

- Résister aux attaques
- Réduire les impacts
- Assurer sa continuité
- Gagner la confiance du marché
- Respecter les exigences réglementaires
- Transformer la cybersécurité en levier de performance

Avec NSI, vous bénéficiez d'un partenaire capable d'agir sur l'ensemble du cycle cyber, de l'analyse initiale à la remédiation complète.

Envie d'avancer ?
NSI vous accompagne à chaque étape vers la cyberrésilience.

Contactez nos experts et construisez, dès aujourd'hui,
votre chemin vers la cyberrésilience.

nsi

Rue de Bruxelles 174A
4340 Awans, Belgique