« Qui ne connaît pas plus l'autre qu'il ne se connaît sera toujours perdant. »

— Sun Tzu, L'Art de la guerre

JSSI 2026 - mardi 10 mars 2026

Sécurité de la Supply Chain : **Pourquoi l'inventaire ne suffit plus**

www.x43c.com

Pourquoi l’inventaire ne suffit plus

Les attaques par la supply chain explosent, pourtant nos tableaux Excel restent bien au chaud.

Les risques liés à la chaîne d'approvisionnement représentent 10,6 %* d’attaques, montrant que les attaquants exploitent activement les canaux indirects via les fournisseurs tiers et les dépendances.

*Sources ENISA octobre 2025
ENISA THREAT LANDSCAPE 2025

- De nombreuses organisations se reposent sur un inventaire des fournisseurs, souvent incomplet.
- Une menace dynamique face à une évaluation statique.

Notre vision

“On ne demande pas si le verrou est fermé, on s’en assure”

X43C est un acteur indépendant spécialisé dans l’accompagnement des organisations pour sécuriser et piloter leurs systèmes d’information

- **Pilotage des fournisseurs** : De nombreuses attaques trouvent leur origine chez les fournisseurs. Auditer vos fournisseurs selon les meilleures pratiques.
- **L’assistance à maîtrise d’ouvrage** (AMOA) : Faire les bons choix numériques n’est jamais simple, entre contraintes budgétaires et complexité technique.
- **L’audit des systèmes d’information** : Adapté à chaque maturité, nos audits couvrent chaque dimension du système d'information et de sa sécurité, en toute indépendance.

Notre objectif : rendre la cybersécurité accessible, pragmatique et réellement utile au quotidien.

Je transmets également mon expérience, sur l’**ISO 27001** et **l’audit des prestataires**.

Un constat simple

Le village Potemkine

L'inventaire des fournisseurs, c'est souvent le décor d’un bon **Western**.

On construit une belle façade, mais dès qu'on pousse la porte, on se rend compte qu'il n'y a personne dans le **saloon**.

Un inventaire Potemkine : une façade rassurante, qui **donne l’impression** de contrôle, mais qui ne reflète **pas la réalité** technique.

_ T’inquiète, le client ne verra jamais nos pistolets à eau !
_ Que dieu puisse t’entendre !

“Pourquoi votre inventaire est une illusion”

Le déclaratif, n’a jamais été une preuve de contrôle et encore moins de sécurité.

Sur le papier, tout est propre : une liste, des réponses, des cases cochées.

- Pour de nombreuses organisations, la sécurité des fournisseurs repose principalement sur un **inventaire** et un **questionnaire**.
- Un inventaire construit sur du **déclaratif**.
- Des questionnaires de **180 questions** : on imagine que cela rassure tout le monde, on a fait le job, on a coché une case.
- Un risque fournisseur établi sur :
  - La dépendance, la pénétration.
  - La maturité, la confiance … **là ça se gâte**

Pourquoi je devrais accorder ma confiance au pretexte que l’organisation a de la **notoriété**, ou qu’elle est certifiée **ISO 27001** ?

Un constat simple

Un tiers n’est pas statique

“La supply chain n’est pas statique, elle évolue en permanence.”

Vous ne pouvez pas **sécuriser** ce que vous ne voyez pas évoluer.

Un inventaire devient très rapidement **obsolète**.

- Vos fournisseurs migrent vers le cloud, ajoutent de nouveaux services, changent d’infrastructure, ou font appel à d’autres sous-traitants. **C’est la vie d’une organisation**.
- Dans la majorité des cas, vous n’êtes **pas informés** de ces changements, notamment techniques.
- Le **risque** lié à votre fournisseur n’est plus le même.
- Le périmètre **évolue** en permanence sans contrôle.

Votre niveau de confiance est-il **réellement** toujours le même ? Peut-on parler de confiance s’il ne vous tient pas **informé** des évolutions ?

Pourquoi l’évaluation échoue

“Une évaluation statique face à une menace dynamique”

L’évaluation donne **une impression** de contrôle, mais ne reflète pas le niveau de risque réel dans le temps

- Elle repose sur du déclaratif, sans validation technique, c’est même l’IA qui s’en charge maintenant.
- Elle est ponctuelle ou planifiée dans le meilleur des cas. Or, une infrastructure peut changer une semaine après l’évaluation.
- Elle ne donne aucune visibilité sur la réalité opérationnelle, notamment l’exposition ou les nouvelles surfaces d’attaque

Comment je m’adapte au **risque** dans ce contexte ?

Du déclaratif à la vérification

“La sécurité ne doit plus être déclarée. Elle doit être vérifiée.”

Plusieurs solutions présentées cet après-midi, je n’en dis pas plus …

- La solution n’est pas de supprimer l’inventaire. Il reste **nécessaire**, mais il n’est plus suffisant.
- Une **surveillance continue** est plus efficace qu’une évaluation ponctuelle.
- Rapprocher le déclaratif de **preuves techniques** est la seule solution pour être en confiance avec son fournisseur.

Une relation avec un fournisseur doit être de confiance, **travailler ensemble** est la meilleure façon de lutter contre les attaques.

Rendre le fournisseur redevable

“La sécurité fournisseur doit devenir contractuelle et mesurable.”

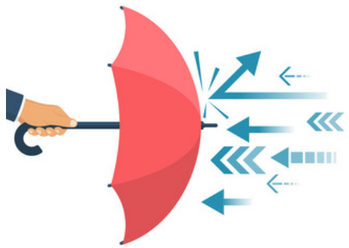
Définition de KPIs de sécurité mesurables (délais de correction, gestion des vulnérabilités, réactivité, etc.)

- La vérification technique est essentielle, mais elle doit être accompagnée d’un **cadre contractuel** solide.
- Trop souvent, les contrats évoquent la sécurité de manière générique, **sans exigences opérationnelles** mesurables.
- **Le droit d’audit doit évoluer**. Il ne s’agit plus seulement de vérifier des politiques, mais de comprendre les flux, les accès réels, et les mécanismes de protection des données.

Ce qui n’est pas **mesuré** et contractualisé n’est pas **maîtrisé**.

“Appliquer le Zero Trust aux fournisseurs.”

L’objectif est de structurer la confiance par des contrôles techniques permanents.



- Considérer **tout accès** tiers comme un point d’entrée potentiel.
- Appliquer avec rigueur le principe du **moindre privilège**.
- **Surveiller** en continu les connexions entrantes et les usages anormaux.

Le fournisseur n’est pas un périmètre de **confiance**. C’est un périmètre à **contrôler**.

“Que faire dès demain matin.”

Commencez petit, mais commencez !

- **Remplacer** le questionnaire générique par une demande de preuves techniques ciblées, ce que vous voulez voir.
- Mettez en place un **monitoring minimal** mais continu de la posture de sécurité du fournisseur.
- Définissez des **indicateurs** contractuels.

L’objectif est de passer d’un inventaire **statique** à une maîtrise **progressive et active**.

“Votre inventaire ne vous sauvera pas, mais votre vigilance, oui.”

Merci