Quel contrôle opérationnel pour ses contrats de sous-traitance ?

Nicolas LEVAIN (Emagine)

Introduction

- RETEX d'une méthode de contrôle des engagements
  - Construction & conduite opérationnelle

- Contexte de développement de cette méthode :
  - Société en prestation intellectuelle en IT
  - Nombreux contrats avec des petites sociétés et des freelances
  - Peu de maturité en sécurité

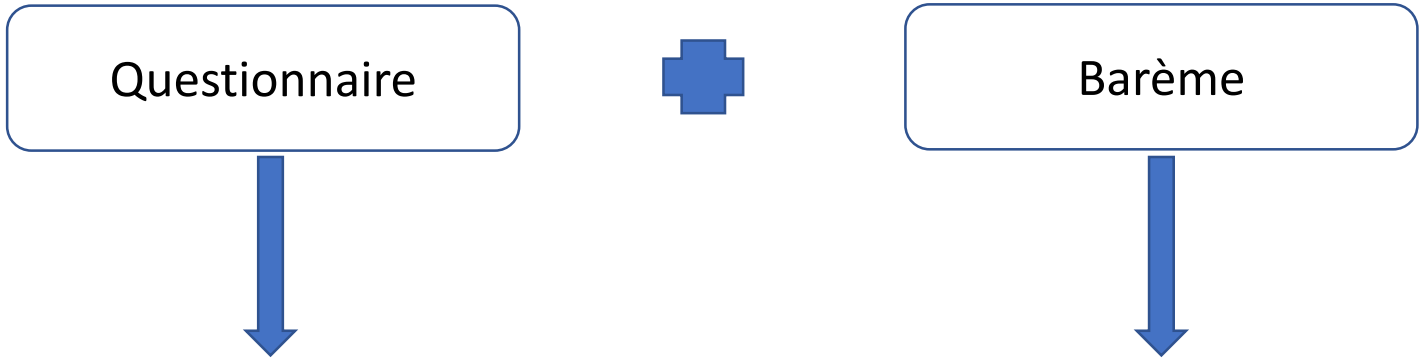
- Nécessité d'une méthode industrialisée et rapide

Introduction

- Objectif principal :
  - Contrôler **a priori** la conformité aux engagements contractuels en sécurité.
- Nous ajoutons :
  - Informer et sensibiliser les partenaires
  - Accompagner et faire progresser
- La présentation qui suit se concentre sur …
  - Le cadrage, l'industrialisation de la méthode, le suivi
- Mais passera rapidement sur…
  - L'évaluation en elle-même

Construction de la méthode

- Quel outil ?



- Traduction des exigences contractuelles
- Pondération des différentes exigences

Construction de la méthode

Exemple

Engagements contractuels

- « Tous les employés du prestataire doivent être sensibilisés aux problématiques de sécurité »

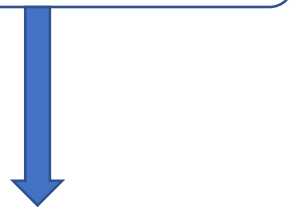
Questionnaire

1. Quelles **initiatives de sensibilisation** ont eu lieu ?
2. Ces initiatives sont-elles **périodiques ?**
3. Ces initiatives incluent-elles des formations à la **sécurisation des applications web ?**

Construction de la méthode

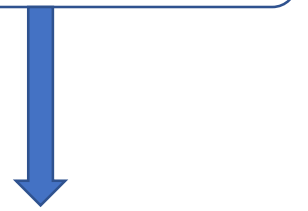
Exemple

Questionnaire



1. Quelles **initiatives de sensibilisation** ont eu lieu ?
2. Ces initiatives sont-elles **périodiques ?**
3. Ces initiatives incluent-elles des formations à la **sécurisation des applications web ?**

Barème



- Chaque question est notée 0, 5 ou 10 points
- La pondération est la suivante :
  1. 30 %
  2. 30 %
  3. 40 %
- La question 1 est éliminatoire pour la catégorie « sensibilisation »

Construction de la méthode

RETEX

- Le découpage en questions et le barème orientent fortement les résultats

- Ils doivent refléter :
  - Les enjeux de sécurité du client
  - Son analyse de risques

- Les objectifs de l'évaluation :
  - Évaluation de maturité en sécurité
  - Conformité « stricte » à un référentiel

- Prioriser : tout n'est pas critique ou éliminatoire

Évaluation

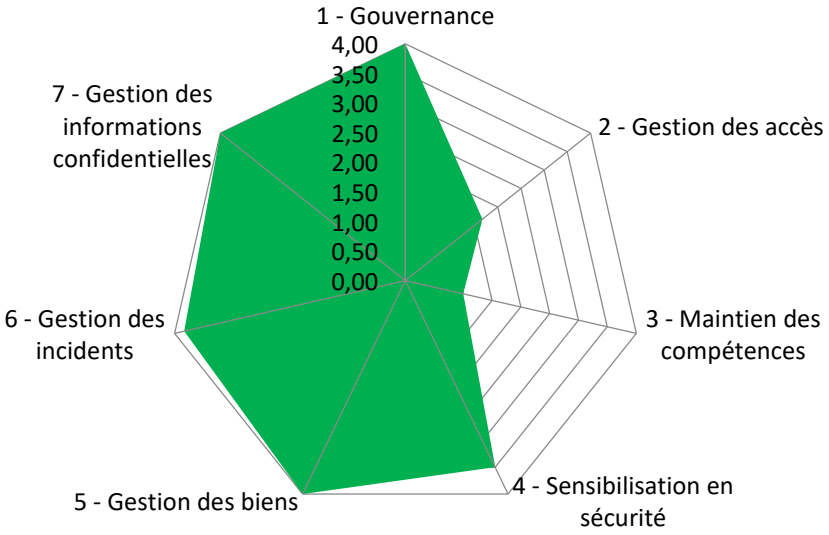
Exemple

Questionnaire	Réponses	Évaluation
1. Quelles **initiatives de sensibilisation** ont eu lieu ?	1. « Simulation de phishing pour tous les employés »	1. Partiellement conforme : 5/10
2. Ces initiatives sont-elles **périodiques ?**	2. « Une campagne de simulation tous les six mois »	2. Conforme : 10/10
3. Ces initiatives incluent-elles des formations à la **sécurisation des applications web ?**	3. « Rien en place, une formation est en cours de préparation »	3. Non conforme : 0/10

Total sensibilisation : 4,5/10

Après l'évaluation

- Quelle communication avec les parties prenantes ?
  - Fournisseur
  - Achats
  - Prescripteur métier
  - …



Questionnaire
Réponses non conformes

→

Plan d'action précis

Après l'évaluation

Exemple

Réponses

1. « Simulation de phishing pour tous les employés »
2. « Une campagne de simulation toutes les six mois »
3. « Rien en place, une formation est en cours de préparation »

Plan d'action

1. Compléter la sensibilisation par des actions concernant l'hygiène informatique au sens large
3. Mettre en place une formation s'appuyant sur les bonnes pratiques et référentiels du secteur (OWASP TOP 10 par exemple)

Après l'évaluation

RETEX

- Un plan d'action clair est critique pour :
  - L'**acceptation** de la méthode
  - La **communication** avec les fournisseurs, achats, prescripteurs métier…
- Sert également de support pour renouveler l'évaluation

Conclusions

Bénéfices et limites

- Résultats **reproductibles et comparables**
- Finesse de **personnalisation** avec le questionnaire et le barème
- Support de **communication** et d'**amélioration continue**
- **Implication forte** dans la démarche sécurité des fournisseurs
- Moins pertinent pour un référentiel qui exige une conformité absolue