



Diag *Flash* Cyber

Évaluer votre exposition
et préparer vos équipes



3 à 5 jours

TPE/PME industrielles sous-traitantes, exposées
via leur système d'information de production

Le jour où vos lignes s'arrêtent, la question ne sera pas technique.

Les attaques visent de plus en plus les PME industrielles, parce qu'elles constituent le point d'entrée le plus accessible d'une chaîne d'approvisionnement. La technique compte, mais l'essentiel se joue ailleurs : dans les comportements quotidiens, la gestion des accès et ce que fait votre équipe dans les premières heures. En trois à cinq jours, nous évaluons votre exposition réelle et nous construisons votre plan de résilience.

Vous êtes concerné si :

- Un ERP, une GPAO ou une supervision sont accessibles à distance
- Aucun plan de reprise d'activité n'est formalisé, ou jamais testé
- Des accès sont partagés entre plusieurs personnes, ou non révoqués après un départ
- Un donneur d'ordre commence à exiger des garanties de sécurité à ses fournisseurs
- Aucun référent n'est identifié en interne sur le sujet

Un cas rencontré dans l'industrie

Métallurgie, 35 salariés, Centre-Val de Loire

Un donneur d'ordre aéronautique conditionne le renouvellement du contrat à des garanties de sécurité du système d'information. L'entreprise n'a ni référent, ni politique d'accès, ni plan de reprise. Le Diag Flash évalue les risques, met en évidence une gestion des accès qui n'a pas suivi les mouvements de personnel des trois dernières années, et évalue la capacité de l'entreprise à gérer une crise. La recommandation structurante est organisationnelle : la désignation et la montée en compétences d'un référent interne, condition sans laquelle aucune mesure technique ne tiendra dans la durée.



3 à 5 jours

TPE/PME industrielles sous-traitantes, exposées
via leur système d'information de production

Ce que le diagnostic vous apporte



Entretiens avec la direction, l'informatique
ou le prestataire, et l'encadrement



Évaluation des risques du système
d'information, menaces internes et externes



Analyse des politiques de sécurité et de
la gestion des accès et des identités



Évaluation des plans de réponse aux incidents
et de la capacité à gérer une crise



Identification du référent à faire émerger
et des compétences à construire

Le volet compétences

Le CCTP est explicite : un diagnostic cybersécurité ne peut se limiter à un audit technique. Le produit identifie le rôle de référent à faire émerger en interne, les compétences à construire pour le tenir, et le niveau de sensibilisation à atteindre par population. Il traite les comportements et la gouvernance comme le premier facteur de résilience, parce qu'ils le sont.

Vos bénéfices

- Vous connaissez **votre exposition réelle**, au-delà de l'intuition
- Vous **répondez aux exigences de sécurité** de vos donneurs d'ordre
- Vous **savez qui fait quoi** dans les premières heures d'un incident
- Vous **faites de vos équipes le premier niveau de protection** plutôt que la faille

Et après : l'accompagnement jusqu'à 5 jours supplémentaires

Construction du plan de résilience, structuration de la gouvernance des accès, plan de sensibilisation des équipes et montée en compétences du référent interne.

Évaluons votre
exposition avant
qu'un tiers ne le fasse
à votre place.

Parlez-en à votre
conseiller OPCO 2i

réponse sous 5 jours ouvrés