

Identifiez les failles qui peuvent arrêter l'activité.

Une revue de sécurité ciblée pour les dirigeants qui ont besoin de réponses claires sur l'interruption, la reprise, l'exposition des accès et la résilience opérationnelle avant qu'un incident impose la discussion.

Auto-évaluation gratuite en cinq minutes

audit.nulvex.com

LANCER L'AUTO-ÉVALUATION GRATUITE

Les incidents sont techniques. L'impact est business.

Nulvex Baseline transforme l'incertitude sécurité en clarté pour la direction. Il aide à comprendre ce qui tomberait en premier, ce qui serait rétabli en premier et ce qui mérite attention avant une vraie interruption.

01

Priorité d'interruption

Identifiez les systèmes qui maintiennent l'activité et qui décide l'ordre de reprise.

02

Confiance de reprise

Distinguez l'existence de sauvegardes d'une restauration réellement testée, mesurée et prouvée.

03

Exposition des accès

Vérifiez si un compte compromis pourrait atteindre trop de périmètre.

04

Visibilité opérationnelle

Sachez si votre équipe détecterait tôt le problème ou seulement après l'impact client.

Une première revue pratique pour des opérateurs sérieux.

Nulvex Baseline est le point de départ avant des travaux plus profonds de durcissement, de surveillance ou de réponse. Il cartographie les faiblesses qui créent une exposition business et donne à la direction une vue claire et priorisée des prochaines actions.

Vue du risque business

01

Une lecture claire de ce qui pourrait interrompre les opérations, les revenus ou la confiance client.

Questions fondées sur les preuves

02

Des vérifications concrètes que votre équipe IT ou votre prestataire doit pouvoir prouver.

Orientation suivante

CLARITY · PRIORITY · A PRACTICAL NEXT STEP

Répondez aux questions que l'entreprise ne peut pas deviner.

Ce contrôle n'est pas un test d'intrusion et ne remplace pas Nulvex Baseline. Il donne un signal immédiat : clair, incertain ou exposé.

01

Si les systèmes principaux tombaient demain, l'ordre de reprise est-il déjà validé ?

Oui, documenté et attribué · Partiellement, mais pas testé récemment · Pas de réponse claire

02

Le même incident pourrait-il toucher la production et les sauvegardes ?

Sauvegardes isolées et restauration testée · Sauvegardes présentes, mais isolation incertaine · Nous ne sommes pas sûrs

03

Un compte compromis exposerait-il trop l'entreprise ?

Accès limité, revu et journalisé · Certains contrôles existent, mais la couverture varie · Probablement, ou nous ne savons pas

04

Sauriez-vous qu'un problème sérieux existe avant vos clients ?

Oui, alertes actives et revues · Quelques alertes existent, mais la réponse est informelle · Seulement après signalement des utilisateurs

05

La direction connaît-elle le coût d'un jour d'arrêt ?

Oui, avec impact opérationnel et client · À peu près, mais pas formalisé · Pas d'estimation fiable

Un prestataire sérieux doit accepter des questions claires.

Si votre prestataire IT ou sécurité actuel répond aux questions Baseline avec des preuves, c'est bon signe. Si les réponses sont vagues, Nulvex Baseline donne une méthode structurée pour fermer les écarts.

01

Demandez des preuves

Tests de restauration, revues d'accès, responsables d'alertes, contacts incident et hypothèses d'impact business.

02

Priorisez l'essentiel

Commencez par les systèmes, comptes et chemins de reprise qui protègent revenus et confiance client.

03

Passez de la revue à l'action

Utilisez Baseline pour décider si Nulvex Core, Watch, Response ou une remédiation ciblée est nécessaire.

Commencez par les failles qui peuvent arrêter l'activité.

Apportez le PDF en réunion de direction, envoyez-le à votre prestataire ou demandez à Nulvex d'exécuter Baseline avec vous.

L'auto-évaluation gratuite et la note publique n'incluent ni analyse technique, ni accès à vos systèmes, ni opinion d'audit formelle. La revue payante ne commence qu'après validation écrite du périmètre et de l'autorisation. · audit.nulvex.com · contact@nulvex.com