THIRD PARTY CYBER RISK · NIS2 & DORA

Le risque entre par vos fournisseurs

Identifier les fournisseurs qui comptent, mesurer leur posture de sécurité et la garder sous contrôle dans la durée. Un service géré qui associe la plateforme Panorays à l'accompagnement continu de notre vCISO.

Fournisseurs critiques | Questionnaires & preuves | Surveillance continue

Votre posture vaut celle de votre fournisseur le plus faible

PÉRIMÈTRE · MESURE · PREUVES

NIS2 impose aux entités concernées de **maîtriser la sécurité de leur chaîne d'approvisionnement**, et DORA en fait autant pour les tiers TIC du secteur financier. Ce n'est pas un exercice documentaire : il s'agit de savoir quels fournisseurs comptent, à quel point ils sont exposés et ce qui se passe s'ils s'arrêtent. NSI Advisor en fait un processus continu — une plateforme qui mesure, un CISO qui décide.

Périmètre
Qui sont réellement vos fournisseurs critiques, sur des critères défendables

Mesure
Posture vérifiée de l'extérieur, pas seulement déclarée

Preuves
Documentation prête pour les auditeurs, les clients et les autorités

Continuité
Une surveillance qui dure, pas une photographie qui vieillit

Démarrage accompagné
inventaire et première évaluation

Revue périodique
la posture évolue, le registre suit

Appui aux audits
à vos côtés quand les questions arrivent

De l'inventaire à la surveillance continue

SEPT ÉTAPES

Un parcours qui part de la liste des fournisseurs et aboutit à un processus qui se maintient seul — le vCISO qui oriente les décisions, Panorays qui mesure.

1 Inventaire des fournisseurs

CARTOGRAPHIE · CRITÈRES APPLICABLES

Collecte et normalisation de la liste des fournisseurs, avec identification de ceux qui sont critiques selon les critères applicables : fourniture TIC et non-substituabilité du service.

2 Classification de la criticité

IMPACT · DÉPENDANCE · DONNÉES TRAITÉES

Chaque fournisseur reçoit un niveau de criticité selon ce qu'il touche, les données qu'il traite et ce qui se passerait s'il défaillait. C'est la base pour décider où concentrer l'effort.

3 Évaluation avec Panorays

SURFACE EXTERNE + QUESTIONNAIRE

La plateforme analyse la posture externe du fournisseur et recueille les réponses au questionnaire de sécurité, produisant une note comparable entre tous les fournisseurs.

4 Analyse des écarts

ATTENDU FACE AU MESURÉ

Comparaison entre le niveau de sécurité attendu pour cette criticité et celui réellement mesuré, avec les écarts classés par importance.

5 Plan de remédiation et dialogue

REMÉDIATION · ÉCHANGE AVEC LE FOURNISSEUR

Définition des actions correctives et conduite de l'échange avec le fournisseur — la partie la plus délicate : obtenir le changement sans abîmer la relation commerciale.

6 Surveillance continue

ALERTES SUR LES ÉVOLUTIONS

L'évaluation ne reste pas figée : toute évolution significative de la surface exposée ou de la posture déclenche une alerte, et la revue repart.

7 Preuves et reporting

AUDIT · CLIENTS · DIRECTION

Registre des fournisseurs, scorecards, historique des évaluations et synthèse pour la direction : le matériel nécessaire lorsqu'un client, un auditeur ou une autorité demande des comptes.

UN SERVICE, PAS UN RAPPORT

Ce qui reste dans l'entreprise

Des documents utilisables devant un auditeur, un client qui envoie un questionnaire ou un conseil d'administration qui demande où vous en êtes.

- Registre des fournisseurs
- Matrice de criticité
- Scorecard par fournisseur
- Analyse des écarts
- Plan de remédiation
- Rapport de direction
- Preuves d'audit

Étendez la maîtrise avec les services opérationnels

Le risque de la chaîne d'approvisionnement n'est qu'une partie du tableau. Ces services, activables séparément ou ensemble, couvrent le reste.

1 vCISO — Virtual CISO

GOUVERNANCE · STRATÉGIE · CONFORMITÉ

L'accompagnement continu qui traduit les objectifs métier en décisions de sécurité.

2 SOC — Security Operations Center

OPEN XDR NATIF IA

Détection, investigation et réponse assurées par nos analystes, jusqu'au 24/7.

3 CTI — Cyber Threat Intelligence

DARK/DEEP WEB · OSINT

Identifiants compromis et données exfiltrées repérés avant d'être exploités.

4 Vulnerability Assessment

POWERED BY QUALYS

Analyses récurrentes avec priorisation du risque et reporting clair.

Savez-vous lesquels de vos fournisseurs sont critiques ?

C'est par là que nous commençons. Une première évaluation du périmètre, sans engagement.

Demander une évaluation →