flowlysis.

LE STOCK DE VULNÉRABILITÉS

On trie les vulnérabilités ouvertes selon qu'elles sont déjà exploitées, et on suit le délai de chaque classe, pas leur nombre. Le volume dit la charge, le délai des exploitées dit le risque.

AUSSI APPELÉ gestion des vulnérabilités, vulnerability management **PRINCIPE QU'IL APPLIQUE** mesurer sans fixer de cible, fiche P-12

SE PRÉPARE EN une demi-journée, stock croisé avec KEV et EPSS **SE FAIT EN** dix minutes par comité mensuel **LEVIER PRINCIPAL** Coût du retard

CE QUE ÇA RAPPORTE		CE QUE ÇA COÛTE	
Impact sur le TTM	Faible	Coût d'implémentation	Faible
Impact sur la qualité (FTR)	Moyen	Difficulté d'implémentation	Moyen
Impact sur l'Opex / Capex	Moyen	Difficulté de maintien	Moyen

Faible · Moyen · Élevé · N/A (sans objet)

1 Le problème auquel ça s'applique

Et ce qu'il vous coûte chaque année

CE QUE VOUS VOYEZ DÉJÀ

- « Il y a des milliers de vulnérabilités ouvertes. » Le comité passe au point suivant.
- La courbe du volume est plate depuis un an. Bon signe ou pas, personne ne sait.
- Le correctif du serveur de production est prêt. La prochaine fenêtre de maintenance est dans deux mois.

OÙ PART L'ARGENT

Une vulnérabilité exploitée ailleurs et ouverte chez vous est une porte que d'autres savent ouvrir. L'équipe ferme d'abord ce qui se ferme vite : le compteur baisse, le risque reste.

L'ORDRE DE GRANDEUR, À LA LOUCHE

Comptez-le avec le CISO. Le chiffrage en euros se fait scénario par scénario.

COMBIEN DE FOIS / AN		CE QUE ÇA COÛTE À CHAQUE FOIS		PART QU'ON ÉVITE		GAIN / AN
vulnérabilités du KEV apparues chez vous dans l'année	×	jours où chacune reste ouverte	×	baisse du délai obtenue par le tri	=	**jours d'exposition évités**

QUAND ÇA NE SERT À RIEN

Quand le stock tient sur une page et que chaque vulnérabilité se ferme dans la semaine. Le tri n'a rien à départager.

2 Comment ça marche

La mécanique, en clair

L'IDÉE EN UNE PHRASE

On corrige d'abord l'exploité, puis le probable, et on suit le délai de chaque classe.

LES GESTES, DANS L'ORDRE

1. Sortir le stock ouvert, daté, avec le système touché et son exposition.
2. Marquer celles du catalogue KEV de la CISA : leur exploitation est avérée.
3. Classer le reste avec EPSS, probabilité qu'une CVE soit exploitée dans les 30 jours. Le CISO fixe le seuil et classe ce qui n'a pas de CVE.
4. Fixer en comité un délai cible par classe : un engagement, jamais une prime.
5. Chaque mois, par classe, stock ÷ corrections ≈ délai moyen, tant que le stock est stable (fiche O-27). Le délai de chaque KEV corrigée va sur une carte de contrôle (fiche O-18).
6. Le COO ouvre fenêtres de maintenance et capacité. Le CISO garde le classement.

CE QU'IL FAUT AVOIR SOUS LA MAIN

Les scans datés et l'inventaire des systèmes. NIS2 charge les États de veiller à ce que les entités qu'elle vise prennent des mesures, dont « le traitement et la divulgation des vulnérabilités » (art. 21, § 2, point e).

LE SIGNE QUE ÇA A MARCHÉ

En comité, le CISO donne sans chercher l'âge de la plus ancienne KEV ouverte.

3 Les pièges de l'implémentation

Ce qui fait rater, et ce qu'on fait à la place

AU LANCEMENT **Piloter au volume**
Le nombre total reste plat, ou baisse. Il ne dit rien des exploitées.
→ Suivre le délai par classe, celui du KEV en premier.

AU LANCEMENT **Trier sur le seul score CVSS**
Une vulnérabilité du KEV attend derrière d'autres mieux notées.
→ Le KEV d'abord, puis EPSS. Dans chaque classe, exposition et gravité départagent.

PENDANT **Donner une cible de volume**
« Moins de 3 000 en juin. » On ferme les postes en série. Le serveur exposé attend.
→ Mesurer le délai sans cible primée. Un écart interroge le flux (fiche P-12).

PENDANT **Attendre la fenêtre**
Correctif prêt en deux jours, fenêtre dans deux mois. Le délai, c'est l'attente.
→ Le COO cale les fenêtres sur le délai cible du KEV, et arbitre la gêne.

DANS LA DURÉE **Garder sans date ce qu'on ne corrige pas**
L'application hors support reste au stock et fausse le délai de sa classe.
→ Une acceptation signée par le métier, avec échéance (fiche P-14).

4 Exemple

Cas type du tertiaire, du constat au résultat

LA SITUATION DE DÉPART

L'OBJET
Les vulnérabilités ouvertes d'un fournisseur d'énergie, comptées une fois par système touché, suivies chaque mois au comité des risques.

CE QUI CLOCHE
Les serveurs de facturation ne se corrigent que pendant une fenêtre de maintenance par trimestre.

CE QU'ILS REGARDAIENT AVANT
Un graphique du nombre de vulnérabilités ouvertes, plat autour de 4 200 depuis un an.

LES CHIFFRES DE DÉPART, HYPOTHÈSES DU CAS, CHAQUE CLASSE STABLE

4 200	vulnérabilités ouvertes
1400	entrées et autant de corrections par mois
90	au catalogue KEV, 18 entrées par mois
240	au-dessus du seuil EPSS, 60 entrées par mois

CE QU'ILS ONT FAIT

Le CISO a présenté le même stock trié par exploitation. Le COO a ouvert une fenêtre de maintenance toutes les deux semaines.

LE DÉCLENCHEUR Un administrateur demande si 4 200, c'est beaucoup. Personne ne sait répondre. ▶ **LE GESTE** Le stock croisé avec le KEV puis EPSS, chaque classe divisée par ses corrections. ▶ **CE QU'ILS ONT VU** Délai moyen de 3 mois pour l'ensemble, de 5 mois pour les 90 du KEV. ▶ **LA DÉCISION** 30 jours au plus au KEV, 60 jours au-dessus du seuil EPSS. Une fenêtre par quinzaine.

CE QUE ÇA A DONNÉ

5 → 0,5 mois	Le délai moyen au KEV : 90 ouvertes ÷ 18 corrections par mois = 5 mois. Après, 9 ouvertes ÷ 18 = 0,5 mois, environ 15 jours.
4 → 1 mois	Le délai moyen au-dessus du seuil EPSS : 240 ÷ 60 = 4 mois. Après, 60 ouvertes ÷ 60 = 1 mois.
4 200 → 4 200	Le volume total ne bouge pas : 1400 entrées, 1400 corrections. Le reste attend un peu plus : 3 870 ÷ 1322 = 2,9 mois, puis 4 131 ÷ 1322 = 3,1 mois.
18 480 € par an	Ce que ça a coûté : 26 fenêtres par an au lieu de 4, soit 22 de plus × 4 personnes × 3 h = 264 h, à 70 € l'heure (hypothèse).

Refaites-le avec votre stock : par classe, divisez les ouvertes par les corrections du mois. Posez le délai de chaque KEV corrigée sur une carte de contrôle, en tête du comité.



À gauche le tri en trois classes, le calcul du délai et le partage des rôles. À droite le graphique que recevait le comité, puis le même stock trié : délai moyen par classe, avant et après.

L'exemple est un cas type, reconstruit à partir de situations courantes du tertiaire. Aucune situation client n'y est identifiable.