

Livre blanc

By xmco

COMMENT ORGANISER SA VEILLE EN VULNÉRABILITÉS

par le CERT-XMCO

Un guide en 4 étapes pour structurer, organiser et piloter votre dispositif de gestion des vulnérabilités.



We deliver cybersecurity

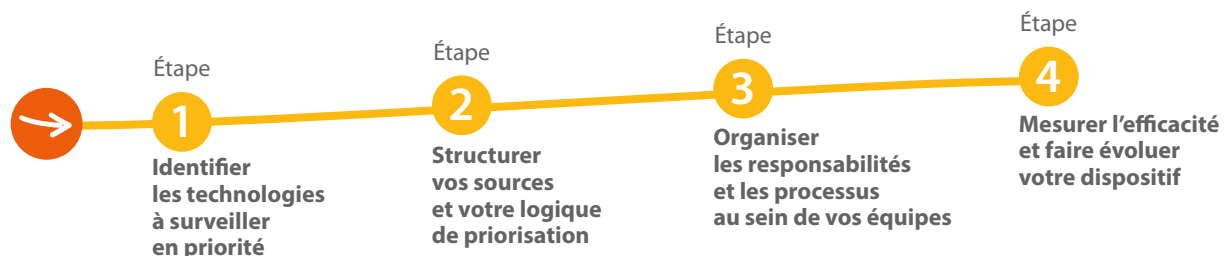
Avant-propos

La gestion des vulnérabilités est l'un des chantiers les plus structurants pour tout responsable de la sécurité des systèmes d'information. Non pas parce qu'elle serait négligée, bien au contraire, mais parce qu'elle se heurte à des contraintes réelles : un flux d'alertes exponentiel, des ressources opérationnelles limitées, des arbitrages permanents entre sécurité et continuité de service.

Plus de 130 nouvelles CVE publiées chaque jour. Des équipes sollicitées sur plusieurs fronts. Des décisions à prendre vite, avec des informations parfois incomplètes. Dans ce contexte, la question n'est pas « faut-il surveiller ? », tout le monde surveille, mais « comment surveiller avec méthode, sans s'y noyer ? ».

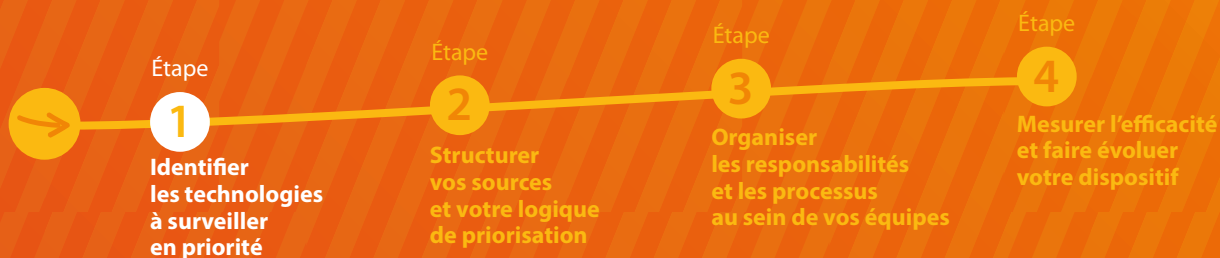
Ce livre blanc a pour vocation de vous faire gagner en efficacité et en lisibilité sur un sujet où la surcharge informationnelle est structurelle.

Il se déroule en quatre étapes complémentaires :



Chaque étape s'appuie sur la précédente. Vous pouvez les parcourir dans l'ordre ou naviguer directement vers celle qui correspond à votre étape de maturité actuelle.

1. IDENTIFIER LES TECHNOLOGIES À SURVEILLER EN PRIORITÉ



PLUS DE 130 NOUVELLES VULNÉRABILITÉS CHAQUE JOUR : LE DÉFI DE LA SÉLECTION

Lundi matin, 8h30. La boîte mail déborde : 47 nouveaux bulletins de sécurité publiés ce week-end, 12 alertes marquées « critique », des dizaines de failles fraîchement découvertes. Parmi ce déluge d'informations, laquelle concerne réellement votre infrastructure ? Laquelle nécessite un patch immédiat ? Laquelle peut attendre ?

En 2025, plus de 49 000 identifiants CVE (Common Vulnerabilities and Exposure) ont été publiés, soit une moyenne de plus de 130 nouvelles failles détectées chaque jour. Face à ce flux, surveiller l'intégralité des vulnérabilités publiées est tout simplement impossible.

La bonne question n'est pas « tout surveiller », mais « comment identifier ce qui compte vraiment pour mon organisation ». Cette première étape est déterminante : elle pose les fondations de toute approche structurée de gestion des vulnérabilités.

CARTOGRAPHIER VOS ÉDITEURS ET PRODUITS

Avant de pouvoir surveiller efficacement les vulnérabilités, vous devez savoir précisément quels éditeurs et produits vous utilisez. Cette cartographie devient votre boussole.

➔ RECENSER L'EXISTANT DE MANIÈRE PRAGMATIQUE

Commencez par lister les éditeurs et produits les plus à risque pour votre infrastructure. L'objectif n'est pas d'être exhaustif, mais d'avoir une vision suffisamment précise pour démarrer.

Ordre de priorité recommandé :

- **Équipements réseau** : Cisco, Fortinet, Juniper
- **Serveurs** : Microsoft Windows Server, Ubuntu, Red Hat Enterprise Linux
- **Applications métier critiques** : SAP ERP, Salesforce, Oracle E-Business Suite

- **Bases de données** : Oracle Database, PostgreSQL, MySQL, Microsoft SQL Server
- **Postes de travail** : Windows, macOS

Une organisation de 200 personnes gère entre 80 et 150 produits différents de 30 à 40 éditeurs. Ne vous découragez pas si votre liste semble longue : vous allez la prioriser à l'étape suivante.

Sources d'information à exploiter : votre CMDB (Configuration Management Database) si vous en disposez, les outils de gestion de parc, les documentations d'architecture, et les connaissances de vos équipes IT.

➔ ÉVALUER LA CRITICITÉ DE CHAQUE PRODUIT

Tous les produits ne présentent pas le même niveau de risque. Trois critères complémentaires permettent de les évaluer.

Criticité métier : quel impact si ce produit est compromis ou indisponible ? Votre ERP et votre CRM sont critiques car ils traitent les données clients et génèrent vos revenus. Un serveur de test interne l'est beaucoup moins. La question « si cette application est inaccessible pendant 24h, quel est l'impact sur mon activité ? » guide naturellement vers les priorités.

Exposition au risque : un produit exposé sur Internet présente un risque supérieur à un produit isolé en réseau interne. Un serveur web public, un VPN d'accès distant, ou un pare-feu en frontal Internet doivent être surveillés en priorité.

Sensibilité des données : les systèmes traitant des données personnelles, de la propriété intellectuelle ou des informations financières nécessitent une attention particulière. La réglementation (RGPD, NIS2) renforce cette exigence.



À RETENIR

Cette cartographie déclarative vous permet de définir consciemment votre périmètre : non pas « tout ce qui existe », mais « tout ce qui compte stratégiquement ». C'est cette vision qui transformera votre veille en véritable outil de pilotage.

PRIORISER POUR DÉMARRER RAPIDEMENT

Une fois vos éditeurs et produits cartographiés, il est temps de prioriser. Le principe de Pareto s'applique directement : concentrez-vous sur les 20 % de produits qui représentent 80 % de votre risque. Cette approche pragmatique permet de démarrer rapidement avec des résultats tangibles.

Concrètement, si vous avez identifié 120 produits, commencez par surveiller les 20 à 25 les plus critiques. Vous étendrez progressivement le périmètre une fois le processus rodé.

Une vulnérabilité critique sur votre pare-feu Fortinet exposé sur Internet passe avant une vulnérabilité modérée sur un serveur de test PostgreSQL interne isolé. L'exposition et l'impact métier doivent guider les choix.



ACTIONS CONCRÈTES POUR CETTE ÉTAPE

- 1 Listez vos 20 applications métier critiques : celles dont l'indisponibilité bloquerait votre activité en moins de 24h. Identifiez l'éditeur et la version précise.
- 2 Cartographiez vos actifs exposés sur Internet : serveurs web, VPN, pare-feu, applications SaaS que vous gérez.
- 3 Identifiez un interlocuteur technique par périmètre : qui connaît précisément les versions de chaque produit et peut valider l'inventaire.

QUESTIONS FRÉQUENTES



COMMENT MAINTENIR CET INVENTAIRE À JOUR DANS UN ENVIRONNEMENT QUI ÉVOLUE CONSTAMMENT ?

Prévoyez une revue trimestrielle de votre inventaire. Lors de chaque nouveau déploiement, ajoutez systématiquement l'éditeur et le produit à votre liste. Les plateformes de veille spécialisées facilitent cette maintenance : une fois vos éditeurs et produits

déclarés, vous êtes automatiquement alerté dès qu'une vulnérabilité les affecte.



QUE FAIRE SI JE N'AI PAS DE CMDB NI D'OUTIL DE GESTION DE PARC ?

Commencez avec un tableur simple. Cinq colonnes suffisent : Éditeur, Produit, Version, Criticité (Critique / Haute / Modérée), Exposition (Internet / DMZ / Interne). Ce niveau de granularité suffit largement pour démarrer.



VOUS SAVEZ DÉSORMAIS QUOI SURVEILLER. L'ÉTAPE SUIVANTE CONSISTE À DÉFINIR COMMENT RESTER INFORMÉ EFFICACEMENT SUR LES VULNÉRABILITÉS QUI AFFECTENT CE PÉRIMÈTRE.

2. STRUCTURER VOS SOURCES ET VOTRE LOGIQUE DE PRIORISATION



DE LA CARTOGRAPHIE À LA SURVEILLANCE ACTIVE

Vous avez identifié vos éditeurs et produits critiques et cartographié votre parc. Une nouvelle problématique émerge naturellement : comment rester informé des vulnérabilités qui affectent ces produits ? Quelles sources consulter parmi les centaines disponibles ? Comment distinguer le signal du bruit dans le flux quotidien d'alertes ?

Sans méthodologie de centralisation et de qualification, le risque est de passer plusieurs heures par jour à trier manuellement des bulletins, sans garantie d'identifier les vulnérabilités qui vous concernent réellement.

Cette deuxième étape transforme votre cartographie en dispositif de surveillance opérationnel.

SÉLECTIONNER DES SOURCES FIABLES ET PERTINENTES

→ LES SOURCES OFFICIELLES INCONTOURNABLES

Les bulletins de sécurité des éditeurs constituent la source la plus directe et fiable. Qu'il s'agisse de Microsoft, Fortinet, Cisco ou tout autre fournisseur de votre stack, ces bulletins publient en première main les correctifs disponibles. C'est l'information la plus proche de la source, celle sur laquelle s'appuient ensuite les bases de données publiques et la plupart des autres relais d'information.

En complément, les bases de données officielles jouent un rôle important de centralisation et de normalisation :

- **Le Programme CVE** (Common Vulnerabilities and Exposures) du MITRE, qui attribue les identifiants uniques
- **Le NVD** (National Vulnerability Database) maintenu par le NIST américain
- **L'EU-VD** (European Union Vulnerability Database) géré par l'ENISA

Il est toutefois essentiel d'en connaître les limites : ces bases ne recensent pas toutes les failles. Certaines vulnérabilités n'obtiennent jamais d'identifiant CVE et ne sont donc pas cataloguées. La bonne pratique consiste à partir des sources primaires que sont les bulletins éditeurs, directement alignés sur vos éditeurs et produits suivis, puis à les compléter par les bases officielles.

→ LE DÉFI DE LA CENTRALISATION

Face à cette diversité de sources, la centralisation devient rapidement critique. Sans filtrage, plus de 130 nouvelles CVE par jour peuvent remonter, dont seulement 5 à 8 concernent réellement vos éditeurs et produits suivis.

Les outils gratuits permettent un premier niveau d'agrégation : agrégateurs de flux RSS, alertes emails dans une boîte dédiée, scripts maison pour automatiser la collecte. Ces solutions conviennent pour démarrer, mais présentent des limites : nécessité de filtrer manuellement les bulletins, pas de qualification contextuelle, pas de priorisation intelligente, et un investissement temps conséquent (2 à 6 heures par jour) pour traiter le flux.

Les services spécialisés de veille permettent de franchir un cap en externalisant ces tâches chronophages. Ils combinent agrégation multi-sources, qualification par des analystes experts et priorisation contextuelle. Pour une organisation qui doit suivre plusieurs dizaines d'éditeurs et de produits critiques, cette approche transforme un flux brut en informations directement actionnables, avec un temps de revue réduit à quelques dizaines de minutes par jour.

PRIORISER LES ACTIONS DE REMÉDIATION

La réception des bulletins ne constitue que la première étape. L'enjeu réel réside dans la transformation de ces informations en actions concrètes et hiérarchisées.

→ AU-DELÀ DU SCORE CVSS

Le CVSS (Common Vulnerability Scoring System) reste l'indicateur le plus utilisé pour évaluer la sévérité

technique d'une faille, avec un score de 0 à 10. Il présente néanmoins certaines limitations relatives aux éléments de contexte métier et environnemental.

3 critères contextuels permettent de le compléter :

- **L'exposition de l'actif** : Internet, DMZ ou réseau interne ?
- **L'exploitabilité réelle** : existe-t-il un code d'exploitation public (PoC) ? La vulnérabilité est-elle activement exploitée (catalogue KEV du CISA) ?
- **L'impact métier** : quelles données ou services sont concernés ?

ILLUSTRATION

Exemple concret : une vulnérabilité CVSS 7.5 activement exploitée (présence KEV) sur un serveur web Apache public mérite une attention immédiate. À l'inverse, un CVSS 9.8 sur un serveur de test PostgreSQL isolé sans données sensibles peut être traité de manière planifiée.

➔ STRUCTURER VOS PRIORITÉS : LA MATRICE DE GESTION DES CORRECTIFS

Organisez vos actions selon une matrice de gestion des correctifs adaptée à votre capacité de traitement :

- **Traitement immédiat (J+0 à J+2)** : vulnérabilités critiques, activement exploitées, affectant des actifs exposés et critiques, ou vulnérabilités majeures avec PoC disponible impactant des actifs sensibles.
- **Traitement rapide (J+7)** : vulnérabilités majeures affectant des actifs sensibles, sans PoC ni exploitation active à ce stade.
- **Traitement planifié (J+30)** : vulnérabilités modérées, sans exploitation connue, en environnement contrôlé.
- **Veille et documentation** : vulnérabilités mineures ou ne concernant pas votre parc actuel.

Cette approche structurée permet de planifier les remédiations, d'anticiper l'impact opérationnel des patches, et de maintenir un équilibre entre sécurité et continuité de service.



ACTIONS CONCRÈTES POUR CETTE ÉTAPE

- 1 **Identifiez les bulletins de sécurité à suivre pour chacun de vos éditeurs prioritaires** : localisez les pages ou flux de bulletins correspondants.
- 2 **Évaluez votre temps disponible** : chronométrez pendant 2 à 3 jours le temps passé à rechercher des informations sur les vulnérabilités. Cette base de référence vous permettra de mesurer le gain apporté par une solution structurée.
- 3 **Définissez vos critères de priorisation** : formalisez par écrit vos 3 critères principaux pour décider quelles vulnérabilités traiter en priorité (exposition Internet, criticité métier, exploitabilité active).



VOTRE VEILLE EST DÉSORMAIS STRUCTURÉE. L'ÉTAPE SUIVANTE CONSISTE À DÉFINIR QUI, DANS VOS ÉQUIPES, FAIT QUOI ET DANS QUELS DÉLAIS - POUR TRANSFORMER CE DISPOSITIF TECHNIQUE EN ORGANISATION HUMAINE EFFICACE.

3. ORGANISER LES RESPONSABILITÉS ET LES PROCESSUS AU SEIN DE VOS ÉQUIPES



DE LA VEILLE STRUCTURÉE À L'ORGANISATION OPÉRATIONNELLE

Vous avez posé les bases de votre dispositif : vous savez quoi surveiller et comment structurer vos sources via une logique de priorisation. Votre veille en vulnérabilités est désormais capable de faire remonter les bonnes informations sur les bons produits, au bon moment.

Une veille bien conçue ne se déploie cependant pas seule : sans organisation claire des responsabilités et des processus, les alertes s'accumulent, les responsabilités se diluent, le risque augmente. Cette troisième étape consiste à transformer ce dispositif technique en organisation humaine efficace : définir qui fait quoi, dans quels délais, avec quelles règles de décision.

TROIS PILIERS POUR UNE ORGANISATION EFFICACE

➔ DÉSIGNER DES RESPONSABLES PAR PÉRIMÈTRE

Désigner des responsables pour la remédiation par périmètre technologique ou métier évite les doublons, élimine les angles morts, et garantit un suivi efficace.

Un exemple de structure possible :

- **Responsable infrastructure** : gère les équipements réseau (routeurs, pare-feu) et serveurs (Windows, Linux)
- **Responsable applicatif** : supervise les applications métier (ERP, CRM) et bases de données
- **Responsable sécurité périmétrique** : pilote les équipements de protection (pare-feu, VPN, antivirus)

Cette répartition doit être formalisée et communiquée à toute l'organisation. L'objectif : chaque alerte doit trouver son interlocuteur en quelques minutes. Lorsqu'une vulnérabilité critique Apache est détectée, les entités concernées sont identifiées

instantanément, au lieu de lancer une investigation de plusieurs jours. Cette réactivité peut faire la différence entre un patch préventif et une exploitation active.

Une veille bien structurée crée également un langage commun entre IT, Sécurité et Direction : tous parlent en délais de correction et criticité métier, améliorant significativement la coordination.

➔ TRACER SYSTÉMATIQUEMENT POUR JUSTIFIER ET CAPITALISER

Tracer systématiquement les actions réalisées permet de répondre à plusieurs enjeux : quelle vulnérabilité (avec son identifiant CVE) ? Quel actif concerné ? Quelle action entreprise (installation du patch, solution de contournement, acceptation temporaire du risque) ? Par qui ? Quand ?

Cette traçabilité permet de justifier les décisions en cas d'audit ou d'incident, de capitaliser sur l'expérience pour anticiper les prochains patches complexes, et de mesurer la performance avec des indicateurs fiables. Avec la directive NIS2, documenter les décisions protège également juridiquement l'organisation et ses dirigeants. En cas d'incident, prouver qu'une vulnérabilité a été identifiée, évaluée et traitée selon un processus documenté constitue un élément de conformité important.

Les plateformes collaboratives facilitent cette organisation en permettant l'attribution automatique des tickets par périmètre, le partage de méthodologie de traitement, et la consolidation des informations via des tableaux de bord.

➔ LA MATRICE DE GESTION DES CORRECTIFS COMME LANGAGE COMMUN

La matrice de priorisation posée à l'étape précédente (traitement immédiat, J+7, J+30, veille) prend ici toute sa valeur opérationnelle : chacun sait, pour une vulnérabilité donnée, qui agit et dans quel délai. Les délais doivent être suffisamment ambitieux pour réduire réellement le risque, mais assez réalistes pour être tenables par les équipes au quotidien.

Exemple de mise en œuvre :

- **48 heures (traitement immédiat)** : vulnérabilités critiques, activement exploitées, affectant des actifs exposés et critiques. Tickets transmis en priorité aux équipes pour traitement en urgence, éventuellement hors des fenêtres de changement habituelles.
- **7 jours (traitement rapide)** : vulnérabilités majeures affectant des actifs sensibles, sans PoC public ni exploitation active connue. Intégrées dans le backlog des équipes avec objectif de correction sous une semaine, via le processus de changement standard.
- **30 jours (traitement planifié)** : vulnérabilités modérées, sans exploitation connue, en environnement contrôlé avec des mesures compensatoires en place. Traitées dans le cadre des campagnes de patching planifiées (maintenances mensuelles).
- **Veille et documentation / Acceptation du risque** : vulnérabilités mineures, ou cas où le coût de correction dépasse clairement le risque résiduel (actif en fin de vie, système isolé, vulnérabilité nécessitant un accès physique). Consigner ces situations dans un registre d'acceptation des risques.



Valeur opérationnelle

Pour les équipes techniques, cette matrice fournit un cadre clair de traitement et facilite l'arbitrage entre urgences et backlog. Pour la direction, elle sert de langage partagé : au lieu de parler de « CVE critiques » de manière abstraite, on parle de vulnérabilités « 48h » ou « 7 jours » selon une grille validée.



ACTIONS CONCRÈTES POUR CETTE ÉTAPE

- 1 **Formalisez les responsabilités** : créez un document simple définissant qui est responsable de chaque périmètre technologique. Partagez-le avec toutes les équipes concernées.
- 2 **Établissez votre registre de traçabilité** : préparez la structure de votre système de suivi (colonnes : CVE, Actif, Action, Responsable, Date). Même un tableur simple suffit pour commencer.

3 **Validez votre matrice d'échéances** : organisez un atelier d'une heure avec les parties prenantes concernées pour définir les délais de correction par niveau de criticité.

QUESTIONS FRÉQUENTES



COMMENT ORGANISER MON ÉQUIPE SI JE SUIS SEUL RESPONSABLE IT/SÉCURITÉ ?

Si vous êtes seul, adaptez l'organisation en définissant des plages horaires dédiées par périmètre (lundi matin = infrastructure, mardi = applicatif). L'essentiel est d'avoir une méthode claire et de la documenter. Les services de veille spécialisés deviennent particulièrement pertinents pour les équipes réduites : ils prennent en charge toute la complexité de surveillance et de qualification, vous permettant de vous concentrer sur les décisions de remédiation.



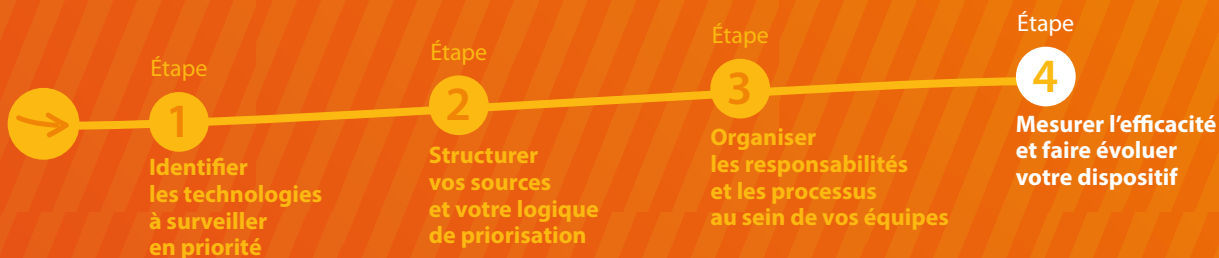
DOIS-JE VRAIMENT DOCUMENTER TOUTES LES VULNÉRABILITÉS, MÊME CELLES QUE JE DÉCIDE DE NE PAS TRAITER ?

Documenter les acceptations de risque (pourquoi vous ne patchez pas une vulnérabilité) est aussi important que documenter les corrections. En cas d'audit ou d'incident, cette traçabilité prouve une approche raisonnée de la sécurité, et constitue un élément de conformité important vis-à-vis des obligations de la directive NIS2.



VOTRE ORGANISATION EST EN PLACE. L'ÉTAPE SUIVANTE CONSISTE À MESURER L'EFFICACITÉ DE CE DISPOSITIF ET À LE FAIRE ÉVOLUER DANS LA DURÉE.

4. MESURER L'EFFICACITÉ ET FAIRE ÉVOLUER VOTRE DISPOSITIF



DE L'ORGANISATION À LA MESURE D'EFFICACITÉ

Vous avez posé les fondations de votre dispositif : identification des technologies et éditeurs à surveiller, structuration des sources et des priorités, organisation des équipes autour de responsabilités claires et d'une matrice de gestion des correctifs. Votre veille en vulnérabilités ne se limite plus à un flux d'alertes : elle s'appuie sur un périmètre défini, des règles de priorisation et des rôles bien attribués.

Comment savoir si ce dispositif fonctionne vraiment ? Comment identifier les axes d'amélioration ? C'est là qu'interviennent les indicateurs de performance. Bien choisis, ils transforment votre veille en levier stratégique mesurable.

MESURER L'EFFICACITÉ AVEC DES INDICATEURS PERTINENTS

La traçabilité mise en place à l'étape précédente alimente directement des indicateurs pour mesurer votre efficacité.

→ LES INDICATEURS STRATÉGIQUES

Les indicateurs stratégiques des parties prenantes :

- **Conformité réglementaire** : respectez-vous vos obligations sectorielles ?
- **Réduction mesurable du risque** : combien de vulnérabilités exploitées activement avez-vous patché avant une potentielle compromission ?
- **Efficience opérationnelle** : quel temps gagné par rapport à une approche manuelle ?

Une veille bien structurée offre une couverture efficace (impossible à obtenir manuellement avec 130 nouvelles vulnérabilités publiées chaque jour), un format enrichi avec explication et niveau de criticité déjà intégrés, et une régularité garantie.

→ LES KPIs OPÉRATIONNELS

Les indicateurs opérationnels mesurent la capacité à détecter et corriger les vulnérabilités, et aident à mieux piloter les équipes et les priorités :

- **Délai de correction par niveau de sévérité** : les objectifs fixés (critiques sous 48h, hautes sous 7 jours) sont-ils respectés ?
- **Taux de couverture** : quel pourcentage du parc critique est effectivement surveillé ?
- **Répartition et traitement** : combien de vulnérabilités critiques détectées ? Quelle proportion traitée dans les délais ?

Ces métriques révèlent rapidement les axes d'amélioration : manque de ressources, processus de validation trop long, dépendances externes bloquantes. Elles identifient également les périmètres nécessitant un accompagnement renforcé.

→ LE GAIN DE TEMPS MESURABLE

Pour les équipes traitant manuellement les flux, comptez entre 2 et 6 heures par jour selon la taille du parc. Une solution automatisée et qualifiée par des experts réduit ce temps à 15 à 30 minutes de revue quotidienne, soit un gain potentiel de 85 %, réinvestissable dans des projets à plus forte valeur ajoutée : projets de durcissement, recherche proactive de menaces, amélioration continue.

La combinaison d'une vision consolidée et de la traçabilité permet de démontrer des résultats concrets et de transformer des données techniques en arguments compréhensibles : « 70 % de nos vulnérabilités critiques sont traitées en moins de 48h ».

L'ÉVOLUTION PROGRESSIVE DE VOTRE DISPOSITIF

Votre veille évolue par phases successives, chacune apportant son lot d'améliorations. Comprendre cette progression permet d'avoir des attentes réalistes et de valoriser chaque étape franchie.



PHASE 1 À 3 MOIS : LE CALIBRAGE

Les premiers mois constituent une phase de calibrage où le dispositif prend forme. Vous validez quels éditeurs et produits sont réellement critiques, affinez vos processus internes et vos filtres de veille. Il est normal à ce stade de découvrir quelques décalages : un périmètre trop large, des délais optimistes, des

points de friction dans la coordination. Ces ajustements progressifs permettent d'obtenir une vision fiable du système d'information et un processus de gestion des vulnérabilités opérationnel.

C'est également pendant cette phase que les équipes s'approprient progressivement leurs nouveaux rôles et responsabilités, en testant concrètement la matrice de gestion des correctifs au quotidien.



PHASE 4 À 6 MOIS : L'OPTIMISATION

L'historique accumulé permet d'optimiser les délais de correction. Vous identifiez les produits problématiques (certains nécessitent des tests longs, d'autres ont des fenêtres de maintenance limitées) et anticipez mieux les dépendances.

Les KPIs s'améliorent naturellement : le délai moyen de correction diminue, le taux de respect de la matrice augmente. Des résultats tangibles peuvent être présentés aux parties prenantes.



PHASE 7 À 12 MOIS : L'ANTICIPATION

L'anticipation devient possible. Vous identifiez les patterns récurrents (Patch Tuesday de Microsoft le deuxième mardi du mois, pics de vulnérabilités critiques en fin de trimestre) et lissez la charge de travail.

Les équipes ne sont plus en mode urgence permanente, mais en amélioration continue. Du temps peut être alloué aux projets de sécurisation proactive plutôt que de subir le flux.



ACTIONS CONCRÈTES POUR CETTE ÉTAPE

1 Sélectionnez vos KPIs essentiels : un opérationnel (délai moyen de correction des critiques) et un stratégique (% de conformité avec vos SLA). Documentez comment vous allez les mesurer.

2 Planifiez leur suivi : une revue mensuelle technique (30 min) et une revue trimestrielle avec les parties prenantes (1h) pour suivre l'évolution des indicateurs.

3 Évaluez votre phase de maturité : êtes-vous dans la phase de calibrage, d'optimisation ou d'anticipation ? Définissez 2 objectifs concrets pour progresser vers la phase suivante.

CONCLUSION

La gestion des vulnérabilités ne se résume pas à un problème technique : c'est un enjeu d'organisation, de priorisation et de pilotage. Ce livre blanc décrit une approche méthodique qui répond à la réalité des équipes : des ressources constantes, un flux d'informations croissant, et la nécessité de faire des choix éclairés.

Les quatre étapes décrites forment un continuum :

- **Cartographier son périmètre pour surveiller ce qui compte vraiment**
- **Structurer ses sources pour capter le signal dans le bruit**
- **Organiser ses équipes pour que chaque alerte trouve un responsable et un délai**
- **Mesurer pour ajuster, progresser et démontrer la valeur du dispositif**

Aucune de ces étapes ne nécessite de repartir de zéro. Chacune s'appuie sur ce qui existe et l'enrichit. La maturité ne se mesure pas à la sophistication des outils, mais à la cohérence entre le dispositif technique, l'organisation humaine et les indicateurs de suivi.



EN RÉSUMÉ, L'OBJECTIF N'EST PAS LA PERFECTION. C'EST LA PROGRESSION MESURABLE, AVEC UN DISPOSITIF QUI GAGNE EN FIABILITÉ, EN RÉACTIVITÉ ET EN LISIBILITÉ À CHAQUE ITÉRATION.

Déployer votre veille en une heure avec yuno

By xMCO



- ✓ **TYPE DE VEILLE**
Couverture complète : bulletins de sécurité, menaces et incidents, actualités, ransomware, IOC, catalogue KEV et veille sectorielle
- ✓ **GESTION DU BRUIT**
Synthèse quotidienne permettant une prise de connaissance complète en moins de 5 minutes
- ✓ **PERSONNALISATION DE LA VEILLE**
Personnalisation granulaire selon vos technologies, vos niveaux de criticité et vos destinataires
- ✓ **RÉACTIVITÉ ET ACTIONNABILITÉ**
Informations disponibles dès J+1, priorisées et immédiatement exploitables
- ✓ **INDÉPENDANCE DES SOURCES**
Production Yuno alimentée directement par les bulletins éditeurs, collectés via des scrapers propriétaires. Enrichissement complémentaire à partir de sources institutionnelles.
- ✓ **PILOTAGE & SUIVI**
Tableaux de bord intégrés pour le pilotage et le suivi de la remédiation
- ✓ **QUALITÉ DE L'ANALYSE**
Chaque vulnérabilité est consolidée, replacée dans son contexte et synthétisée pour une lecture immédiate
- ✓ **INTÉGRATION / CONNECTEURS**
API disponible pour une intégration flexible dans votre système d'information existant
- ✓ **DÉPLOIEMENT**
Opérationnel en 1 heure, pas d'installation requise, simple paramétrage de la plateforme SaaS

➤ Testez gratuitement
yuno
By xmco



<https://content.xmco.fr/demande-de-demo-yuno>



We deliver cybersecurity expertise

Nos consultants pensent comme les attaquants pour mieux les contrer, puis vérifient manuellement chaque vulnérabilité potentielle afin de livrer une vision claire et exploitable des risques Cyber. Audits, pentests, réponse à incident, conformité PCI DSS, veille CERT et CTI : nous couvrons tout le cycle de vie de la cybersécurité.

Cette exigence transforme la sécurité en levier de performance mesurable. Certifiés PASSI et PCI QSA, nous demeurons indépendants et engagés pour la réussite numérique de nos clients.

Date de création : 2002
Effectif salariés : plus de 100

Qualifications : PASSI, QSA et CERT officiel

Clients actifs : plus de 450
dont clients CERT : plus de 100

Secteurs : Banque, Assurance,
Industrie, Institutions,
Transports, Médias,
Luxe, etc.



Renseignement :
info@xmco.fr

01 79 35 29 30



www.xmco.fr