RESSOURCE DIRIGEANT PME/ETI

Checklist maturité cyber PME/ETI

Conformité, résilience, rançongiciel et priorités 30/60/90 jours

Version dirigeant PME/ETI - Adrien Murillo

Lecture rapide	Atelier	Sortie attendue
5 minutes pour reperer les zones rouges	45-60 minutes avec direction + IT/RSSI	Score, preuves, risques et plan 30/60/90

Cette checklist aide une direction, une DSI ou un RSSI à situer rapidement la maturité cyber d'une organisation avant un audit découverte. Elle ne remplace pas un audit complet, une analyse de risques formelle, une qualification juridique ou une attestation de conformité.

Le principe est simple : obtenir une lecture décisionnelle en moins d'une heure, puis identifier les preuves à réunir, les responsabilités à clarifier et les actions à engager en priorité.

> **Positionnement : double lecture dirigeant + terrain. Les questions traduisent la conformité en décisions, preuves, routines et responsabilités exploitables.**

0–25	26–50	51–75	76–100
Exposition elevee	**Socle partiel**	**Maturite correcte**	**Pilotage avance**

Planifier un audit decouverte

1 Pourquoi évaluer la maturité cyber maintenant

Une évaluation courte évite de traiter la cybersécurité comme une liste de projets techniques déconnectés des risques métier. Pour une PME ou une ETI, le sujet combine quatre pressions : exposition opérationnelle, dépendance numérique, obligations de conformité et capacité réelle à reprendre l'activité après incident.

Les textes comme NIS2, DORA, CRA ou ISO 27001 ne demandent pas seulement des outils. Ils demandent une gouvernance, des preuves, des responsabilités et une capacité d'amélioration continue. La question utile n'est donc pas "sommes-nous conformes ?", mais "savons-nous démontrer ce que nous maîtrisons et décider ce qui doit être traité en premier ?".

Cette checklist sert à produire une première photographie. Elle doit faire émerger les zones rouges, les angles morts, les dépendances critiques et les sujets qui méritent un audit découverte.

PREUVE Ce que la direction doit obtenir

- Une lecture des risques prioritaires, exprimée en impact métier.
- Une vision des responsabilités : qui décide, qui exploite, qui prouve.
- Une première liste de preuves existantes et de preuves manquantes.
- Une trajectoire réaliste sur 30, 60 et 90 jours.
- Un périmètre clair pour la suite, sans promesse de conformité automatique.

PREUVE Ce que cette checklist ne fait pas

- Elle ne certifie pas une conformité NIS2, DORA, CRA ou ISO 27001.
- Elle ne remplace pas un audit technique ou juridique.
- Elle ne donne pas de garantie de protection contre un rançongiciel.
- Elle ne doit pas conduire à collecter des secrets, mots de passe ou informations sensibles dans ce document.

2 Mode d'emploi et règle de scoring

Prévoir 45 à 60 minutes pour une première passe complète. Si le temps est limité, commencer par le score rapide dirigeant en 15 minutes, puis revenir sur les domaines détaillés.

Pour chaque item, attribuer une note de 0 à 3. La note doit refléter la réalité observable, pas l'intention. Une procédure écrite mais jamais testée ne vaut pas une maturité complète. Une solution technique présente mais non supervisée doit rester partielle.

Score	Lecture	Exemple de preuve attendue
0	Absent ou non maîtrisé	Aucun propriétaire, aucune procédure, aucun contrôle identifiable
1	Partiel ou informel	Pratique connue de quelques personnes, non documentée, non suivie
2	En place mais non prouvé	Procédure ou outil présent, preuves incomplètes, test irrégulier
3	Maîtrisé, documenté, testé	Responsable nommé, preuve datée, routine suivie, test ou revue disponible

PREUVE Conseils de remplissage

- Noter 0 quand la réponse dépend d'une seule personne ou d'une supposition.
- Noter 1 quand la pratique existe mais ne survivrait pas à une absence, une crise ou un changement d'équipe.
- Noter 2 quand le dispositif existe mais que les preuves sont faibles ou dispersées.
- Noter 3 seulement si la preuve est exploitable par une direction, un auditeur ou une équipe d'exploitation.

ALERTE Règle de prudence

Quand plusieurs personnes hésitent entre deux notes, retenir la note la plus basse et inscrire la preuve à produire. Le but n'est pas de gonfler le score, mais d'obtenir une trajectoire défendable.

3 Grille de restitution globale

Additionner les points des sections détaillées, puis convertir le résultat sur 100. La valeur exacte compte moins que la tendance : exposition élevée, socle partiel, maturité correcte ou pilotage avancé.

Score final	Lecture décisionnelle	Priorité recommandée
0-25	Exposition élevée, cadrage prioritaire	Stabiliser les fondamentaux, identifier les actifs critiques, lancer un audit découverte
26-50	Socle partiel, priorités à arbitrer	Choisir 3 à 5 chantiers, formaliser les responsabilités, produire les preuves minimales
51-75	Maturité correcte, preuves à renforcer	Tester, industrialiser, compléter les preuves et piloter le risque résiduel
76-100	Maturité avancée, amélioration continue	Maintenir les routines, améliorer les indicateurs, préparer audits et exercices réguliers

PREUVE Restitution par domaine

Reporter un score sur 10 pour chaque domaine. Un domaine faible peut annuler un score global correct. Une organisation peut avoir une bonne conformité documentaire et une faible capacité de restauration, ou l'inverse.

Domaine	Score /10	Observation courte
Gouvernance et responsabilités		
Actifs critiques et dépendances		
Conformité et preuves		
Analyse de risques		
Sauvegardes et restauration		
PRA/PCA et crise		
Vulnérabilités et durcissement		
Identité et accès		
Supervision et journalisation		
Automatisation et DevSecOps		

4 Score rapide dirigeant en 15 minutes

Ce score permet de détecter les zones rouges sans entrer immédiatement dans le détail technique. Il doit être réalisé avec au moins une personne de direction et une personne qui connaît l'exploitation IT ou cyber.

Question	0	1	2	3
Les actifs critiques de l'entreprise sont identifiés et priorisés				
Une personne est responsable du risque cyber au niveau direction				
Les sauvegardes critiques sont restaurées en test au moins une fois par an				
Les accès à privilèges sont limités, tracés et protégés par MFA				
Les vulnérabilités critiques sont priorisées selon le risque métier				
Un scénario rançongiciel a déjà été discuté avec les décideurs				
Les obligations NIS2, DORA, CRA ou ISO applicables sont cadrées				
Les preuves de sécurité sont centralisées ou faciles à retrouver				
Un plan 30/60/90 jours existe pour réduire les risques prioritaires				
Les prestataires critiques ont des exigences cyber connues et suivies				

PREUVE Lecture rapide

- 0 à 10 : cadrage urgent, risque de dépendance aux personnes et aux suppositions.
- 11 à 20 : socle incomplet, choisir les fondamentaux avant les projets lourds.
- 21 à 25 : maturité émergente, formaliser les preuves et tester la reprise.
- 26 à 30 : bonne base, renforcer le pilotage et préparer les audits.

ACTION Décision à prendre

Si trois questions ou plus obtiennent 0, planifier un audit découverte avant de lancer des achats d'outils. Le besoin prioritaire est alors le cadrage, pas l'empilement technique.

5 Gouvernance, responsabilités et arbitrages

La gouvernance cyber doit répondre à une question simple : qui accepte le risque, qui finance le traitement, qui exécute, qui vérifie et qui conserve les preuves ? Sans cette clarification, les actions restent dépendantes de l'urgence et des personnes disponibles.

Contrôle	Score 0-3	Preuve attendue
Un responsable cyber ou sécurité SI est identifié, même à temps partiel		Lettre de mission, fiche de rôle, organigramme
La direction reçoit une synthèse cyber régulière et compréhensible		Comité, compte rendu, tableau de bord
Les décisions de risque sont arbitrées avec une notion d'impact métier		Registre risques, décisions, acceptations formalisées
Les responsabilités DSI, RSSI, métiers, achats et juridique sont séparées		RACI, processus, comité
Les incidents significatifs remontent à la direction avec critères connus		Procédure d'escalade, seuils, contacts
Les tiers critiques sont intégrés dans la gouvernance cyber		Clauses, revues fournisseurs, exigences sécurité

ALERTE Signaux d'alerte

- Le sujet cyber est porté uniquement par l'équipe IT sans relais direction.
- Les arbitrages sont faits après incident, jamais avant.
- Le budget sécurité est confondu avec le renouvellement d'outillage.
- Les preuves existent mais restent dans les boîtes mail ou les disques personnels.

ACTION Décision utile

Nommer un propriétaire de la feuille de route et un sponsor direction. Le sponsor arbitre les priorités. Le propriétaire coordonne les preuves, les actions et les points de blocage.

6 Budget, trajectoire et indicateurs

Un budget cyber défendable relie un risque, une obligation, une preuve et un résultat. Il ne s'agit pas de tout traiter immédiatement, mais de rendre les priorités lisibles et mesurables.

Contrôle	Score 0-3	Preuve attendue
Les dépenses cyber sont reliées à des risques ou obligations explicites		Budget annoté, feuille de route, arbitrages
Les actions sont classées en obligatoire, prioritaire, différable		Backlog, plan 30/60/90, matrice effort/impact
Les coûts d'indisponibilité sont estimés pour les processus critiques		BIA simplifiée, estimation métier
Les indicateurs distinguent activité, risque et preuve		KPI/KRI, compte rendu, tableau de bord
Les investissements sont revus après test ou incident		Retours d'exercice, REX, ajustements

PREUVE Exemples d'indicateurs utiles

- Pourcentage de sauvegardes critiques restaurées en test.
- Délai moyen de correction des vulnérabilités critiques exposées.
- Nombre de comptes privilégiés sans justification active.
- Couverture MFA sur les accès sensibles.
- Nombre de preuves de conformité à jour par référentiel.

ALERTE Erreur fréquente

Mesurer seulement le nombre de tickets fermés donne une impression d'activité. Une direction a besoin de savoir si le risque baisse, si les preuves sont prêtes et si la reprise d'activité est crédible.

7 Actifs critiques et dépendances

La maturité cyber commence par la connaissance de ce qui doit absolument fonctionner. Une cartographie exhaustive peut prendre du temps. Une première cartographie utile peut être obtenue rapidement en partant des processus métier critiques.

Contrôle	Score 0-3	Preuve attendue
Les processus métier critiques sont listés et priorisés		Liste validée direction, BIA simplifiée
Les applications, serveurs, données et fournisseurs liés sont identifiés		Cartographie, CMDB, schéma, contrat
Les dépendances réseau, identité, sauvegarde et supervision sont visibles		Diagrammes, inventaires, matrices
Les données sensibles ou réglementées sont localisées		Registre, classification, cartographie
Les actifs exposés à Internet sont inventoriés et suivis		Inventaire externe, revue DNS, scan exposition
Les propriétaires métier et techniques sont nommés		RACI, fiches actifs, annuaire de crise

PREUVE Questions de terrain

- Quelle application arrêterait l'activité en moins de 24 heures ?
- Qui peut décider de la couper temporairement en cas d'incident ?
- Où sont les sauvegardes et qui sait les restaurer ?
- Quel fournisseur peut bloquer la reprise ?
- Quelle donnée ne doit jamais être exposée publiquement ?

ACTION Livrable minimal

Produire une page par processus critique : objectif métier, applications, données, dépendances, propriétaires, temps d'arrêt tolérable, preuves disponibles.

8 Conformité NIS2, DORA, CRA et ISO 27001

La conformité doit être traduite en décisions opérationnelles. Les référentiels demandent souvent des notions proches : gouvernance, gestion des risques, contrôle des accès, continuité, sécurité des fournisseurs, journalisation, traitement des incidents et amélioration continue.

Contrôle	Score 0-3	Preuve attendue
Le périmètre réglementaire applicable est cadré		Note de périmètre, avis juridique si nécessaire
Les exigences sont traduites en contrôles concrets		Matrice exigences/contrôles/preuves
Les preuves sont datées, nommées et récupérables		Dossier preuves, index, référentiel documentaire
Les écarts sont priorisés selon risque, obligation et effort		Plan de traitement, arbitrages
Les fournisseurs critiques sont intégrés aux exigences		Clauses, questionnaires, revues
La direction sait distinguer conformité cible et conformité prouvée		Synthèse exécutive, score, limites

PREUVE Traduction pratique

- Une politique sans routine n'est pas une preuve suffisante.
- Un outil sans propriétaire ne démontre pas une maîtrise.
- Un plan non testé ne suffit pas pour prouver une capacité de reprise.
- Une conformité annoncée doit pouvoir être expliquée, montrée et maintenue.

ALERTE Point de vigilance

Cette checklist ne dit pas si l'organisation est légalement soumise à NIS2, DORA ou CRA. Elle aide à préparer les questions et les preuves à partager avec les personnes compétentes.

9 Lecture NIS2 pour dirigeants PME/ETI

NIS2 renforce la logique de gouvernance, de gestion des risques et de responsabilité. Pour un dirigeant, l'enjeu n'est pas de mémoriser le texte, mais de savoir si l'organisation peut montrer une maîtrise proportionnée des risques.

Sujet NIS2 à cadrer	Question de direction	Preuve terrain
Gouvernance	Qui suit le risque et qui arbitre ?	Comité, RACI, synthèse risques
Gestion des incidents	Qui décide, qui communique, qui conserve les preuves ?	Procédure, annuaire, registre incidents
Continuité	Quelle activité reprend en premier ?	PRA/PCA, tests, priorités métier
Sécurité fournisseurs	Quels tiers peuvent créer une rupture majeure ?	Liste tiers critiques, clauses, revues
Mesures techniques	Quels contrôles sont réellement déployés et suivis ?	MFA, durcissement, logs, supervision
Formation	Qui doit savoir réagir et à quel niveau ?	Sensibilisation, exercices, preuves

PREUVE Checklist ciblée

- ☐ Le périmètre NIS2 potentiel est documenté.
- ☐ Les obligations sont traduites en chantiers compréhensibles.
- ☐ Les responsabilités de direction sont expliquées sans jargon.
- ☐ Les actions prioritaires sont reliées à des preuves.
- ☐ Le calendrier de mise en conformité est réaliste.

ACTION Décision utile

Créer une matrice simple : exigence, contrôle existant, preuve disponible, écart, responsable, échéance. Cette matrice évite de transformer NIS2 en projet documentaire hors sol.

10 DORA, CRA et ISO 27001 : ne pas mélanger les preuves

DORA concerne principalement la résilience opérationnelle numérique du secteur financier et de son écosystème. Le CRA concerne la cybersécurité des produits comportant des éléments numériques. ISO 27001 structure un SMSI et une amélioration continue. Ces cadres peuvent se croiser, mais les preuves ne se substituent pas automatiquement.

Cadre	Question à clarifier	Exemple de preuve
DORA	Sommes-nous dans un périmètre financier ou fournisseur critique ?	Cartographie services ICT, registre incidents, tests résilience
CRA	Produisons-nous ou distribuons-nous un produit numérique concerné ?	Analyse produit, exigences sécurité, gestion vulnérabilités
ISO 27001	Avons-nous un système de management sécurité structuré ?	Politique, analyse risques, SoA, audits internes
ISO 22301	Avons-nous une continuité d'activité pilotée ?	BIA, PRA/PCA, exercices, REX

PREUVE Bon réflexe

Ne pas annoncer une conformité générale à partir d'une preuve isolée. Une sauvegarde testée est une excellente preuve de résilience, mais elle ne prouve pas à elle seule une gouvernance, une gestion des tiers ou un SMSI complet.

PREUVE Questions à poser avant un audit découverte

- Quel référentiel est prioritaire pour l'entreprise ?
- Quelle échéance déclenche la pression ?
- Quelles preuves existent déjà ?
- Quels écarts sont acceptables temporairement ?
- Quels contrôles doivent être prouvés devant un client, un auditeur ou une autorité ?

11 Analyse de risques et scénarios EBIOS RM simplifiés

Une analyse de risques utile rend les décisions possibles. Même sans conduire immédiatement une démarche EBIOS RM complète, il est possible de structurer quelques scénarios crédibles autour des actifs critiques.

Contrôle	Score 0-3	Preuve attendue
Les événements redoutés sont formulés en impacts métier		Liste validée, exemples de pertes
Les sources de risque sont discutées de manière réaliste		Ateliers, hypothèses, contexte menace
Les chemins d'attaque probables sont identifiés à haut niveau		Scénarios, schémas simples
Les mesures existantes sont reliées aux scénarios		Matrice risques/contrôles
Les risques résiduels sont acceptés ou traités explicitement		Décisions, plan de traitement

PREUVE Trame de scénario

Élément	À remplir
Actif ou processus critique	
Événement redouté	
Source de risque plausible	
Chemin d'attaque ou défaillance	
Impact métier	
Contrôles existants	
Preuves disponibles	
Risque résiduel	
Décision	

PREUVE Exemple de formulation

"Indisponibilité de l'ERP pendant cinq jours après compromission d'un compte administrateur et chiffrement des serveurs applicatifs, entraînant arrêt facturation, retard livraison et mobilisation de crise."

12 Sauvegardes et restauration

Les sauvegardes sont souvent citées comme protection majeure contre le rançongiciel. La preuve réelle n'est pas l'existence d'un outil de sauvegarde, mais la capacité à restaurer les bonnes données, dans le bon ordre, avec les bonnes personnes, dans un délai acceptable.

Contrôle	Score 0-3	Preuve attendue
Les données et systèmes critiques sont couverts par sauvegarde		Politique, périmètre, journaux
Les sauvegardes sont isolées ou protégées contre l'altération		Immutabilité, séparation, comptes dédiés
Des restaurations sont testées et documentées		Procès-verbal, captures, horodatage
Les objectifs RPO/RTO sont définis par processus critique		BIA, exigences métier
Les échecs de sauvegarde déclenchent une alerte traitée		Supervision, tickets, procédure
Les secrets et dépendances nécessaires à la restauration sont maîtrisés		Coffre, procédures, accès d'urgence

PREUVE Questions de validation

- Quel est le dernier test de restauration complet ?
- Le test a-t-il inclus l'application, la base, les dépendances et les accès ?
- Les sauvegardes peuvent-elles être supprimées par le même compte compromis ?
- L'ordre de restauration est-il documenté ?
- Qui valide que la donnée restaurée est utilisable métier ?

ACTION Action prioritaire

Choisir un actif critique et organiser un test de restauration limité mais complet. Documenter durée, obstacles, accès nécessaires, pertes de données et décisions à prendre.

13 PRA/PCA et continuité d'activité

Un PRA ou un PCA ne doit pas être un document dormant. Il doit permettre de prendre des décisions sous contrainte : quels services reprendre, dans quel ordre, avec quelles ressources, sur quelle infrastructure, avec quelle communication.

Contrôle	Score 0-3	Preuve attendue
Les processus critiques ont un temps d'arrêt tolérable défini		BIA, validation direction
Les dépendances techniques et fournisseurs sont connues		Cartographie, contrats, contacts
Les procédures de reprise sont testées		Exercices, chronos, REX
Les rôles de crise sont identifiés		Cellule de crise, annuaire, astreinte
Les modes dégradés métier sont préparés		Procédures, formulaires, seuils
Les communications internes et externes sont cadrées		Modèles, circuits validation

PREUVE Tests utiles

- Test papier : dérouler un scénario en comité sans toucher à la production.
- Test technique limité : restaurer un composant isolé.
- Test métier : vérifier que le service restauré permet réellement de travailler.
- Test de communication : valider annuaire, messages et chaîne de décision.

ALERTE Point dur fréquent

Le PRA échoue rarement sur une seule technologie. Il échoue plus souvent sur les dépendances oubliées : identité, DNS, certificats, réseau, comptes de service, fournisseur, procédure d'accès ou validation métier.

14 Rançongiciel et gestion de crise

Le rançongiciel combine crise technique, crise métier, crise juridique, communication et pression psychologique. La maturité se mesure à la capacité à ralentir la propagation, préserver les preuves, décider vite et restaurer sans improvisation excessive.

Contrôle	Score 0-3	Preuve attendue
Un scénario rançongiciel est documenté		Runbook, atelier, hypothèses
Les premières actions de confinement sont connues		Procédure, droits, contacts
Les preuves numériques à préserver sont identifiées		Guide collecte, journalisation
Les décisions direction sont préparées		Critères, cellule de crise, modèles
Les communications clients, salariés et partenaires sont pré-cadrées		Modèles, validation, porte-parole
Le retour d'expérience est prévu après incident ou exercice		Trame REX, plan d'amélioration

PREUVE Checklist de préparation

- ☐ Annuaire de crise accessible hors SI principal.
- ☐ Procédure de coupure réseau ou segmentation d'urgence.
- ☐ Liste des systèmes à préserver pour analyse.
- ☐ Contacts assurance, juridique, prestataires, autorités si applicables.
- ☐ Critères de restauration prioritaire validés par la direction.
- ☐ Message interne court pour limiter les actions dangereuses.

ACTION Décision utile

Organiser un exercice de crise de deux heures avec scénario réaliste. Le livrable attendu n'est pas une performance parfaite, mais la liste des points de rupture.

15 Vulnérabilités, durcissement et MCO/MCS

La correction des vulnérabilités doit être priorisée selon l'exposition, la criticité métier, l'exploitabilité et les contraintes d'exploitation. Corriger tout au même niveau est rarement réaliste. Ne rien prioriser crée une dette invisible.

Contrôle	Score 0-3	Preuve attendue
Les actifs exposés sont scannés ou revus régulièrement		Rapports, inventaire, tickets
Les vulnérabilités critiques ont des délais de traitement définis		Politique, SLA, tableaux de suivi
Les exceptions sont documentées avec risque résiduel		Dérogations, compensations
Les configurations de durcissement sont standardisées		Baselines, scripts, images, GPO
Les correctifs sont testés avant déploiement quand nécessaire		Procédure, environnement de test
Les systèmes hors support sont identifiés et arbitrés		Registre obsolescence, plan migration

PREUVE Lecture terrain

Un bon processus MCO/MCS distingue les actifs exposés, les actifs critiques, les actifs obsolètes et les actifs difficiles à redémarrer. Cette segmentation permet de prioriser sans bloquer l'exploitation.

PREUVE Preuves fortes

- Tableau des vulnérabilités critiques avec propriétaire et date cible.
- Liste des exceptions validées.
- Baseline de durcissement appliquée à un périmètre clair.
- Historique de correction sur les actifs exposés.

16 Accès, identité, MFA et comptes privilégiés

L'identité est souvent le point de bascule d'un incident. Un compte privilégié non maîtrisé peut contourner des investissements importants. La maturité se joue sur le cycle de vie, la MFA, la séparation des usages, la traçabilité et les revues régulières.

Contrôle	Score 0-3	Preuve attendue
La MFA couvre les accès sensibles et distants		Configuration, rapport couverture
Les comptes privilégiés sont séparés des comptes bureautiques		Annuaire, politique, contrôles
Les arrivées, départs et changements de poste sont suivis		Process RH/IT, tickets, revues
Les droits sont revus périodiquement		Campagnes de revue, validations
Les comptes de service sont inventoriés et justifiés		Registre, propriétaire, rotation
Les accès prestataires sont limités, tracés et révocables		Contrats, comptes nominatifs, logs

PREUVE Questions critiques

- Combien de personnes peuvent administrer l'environnement principal ?
- Combien de comptes privilégiés n'ont pas de propriétaire clair ?
- Un départ collaborateur désactive-t-il tous les accès utiles ?
- Les prestataires utilisent-ils des comptes partagés ?
- Les accès d'urgence sont-ils testés sans affaiblir la sécurité ?

ACTION Action prioritaire

Faire une revue ciblée des comptes administrateurs et des accès distants. Supprimer, justifier ou limiter ce qui ne peut pas être expliqué.

17 Supervision, journalisation et preuves

Les logs ne servent pas seulement à détecter. Ils servent aussi à comprendre, prouver, décider et reconstruire une chronologie après incident. Sans journalisation exploitable, la réponse à incident devient partiellement aveugle.

Contrôle	Score 0-3	Preuve attendue
Les systèmes critiques produisent des journaux exploitables		Configuration, périmètre, exemples
Les événements d'administration sont tracés		Logs IAM, bastion, EDR, SIEM
Les alertes importantes sont qualifiées et traitées		Règles, tickets, procédures
La rétention des logs est alignée avec les besoins incident et conformité		Politique, stockage, durée
Les preuves sont centralisées ou indexées		Dossier preuves, référentiel, liens
Les accès aux journaux sont protégés		Droits, séparation, immutabilité

PREUVE Preuves à conserver

- Liste des sources de logs critiques.
- Exemples d'événements utiles : connexion admin, échec MFA, création compte, désactivation antivirus.
- Procédure de recherche rapide.
- Règles de rétention.
- Liste des personnes habilitées à consulter les preuves.

ALERTE Erreur fréquente

Collecter beaucoup de logs sans scénario de détection ni responsable crée du bruit. La première question reste : quel événement critique voulons-nous voir à temps ?

18 Automatisation et DevSecOps

L'automatisation réduit le risque quand elle rend les contrôles répétables, visibles et maintenables. Elle augmente le risque quand elle propage une mauvaise configuration plus vite. La maturité consiste à automatiser les routines qui protègent vraiment l'exploitation.

Contrôle	Score 0-3	Preuve attendue
Les configurations critiques sont versionnées		Git, historique, revue
Les pipelines intègrent des contrôles sécurité proportionnés		SAST, scan dépendances, scan images
Les secrets ne sont pas stockés dans le code ou les artefacts		Coffre, scans, règles
Les images, scripts ou playbooks de durcissement sont maintenus		Dépôts, tests, changelog
Les changements sont revus avant production		Merge requests, validations
Les contrôles automatisés produisent des preuves lisibles		Rapports, artefacts, tableaux

PREUVE Exemples de routines utiles

- Scan de secrets sur dépôt et pipeline.
- Contrôle de dépendances vulnérables.
- Validation de configuration infrastructure as code.
- Durcissement standard des images.
- Vérification automatique des sauvegardes ou certificats.

ACTION Décision utile

Choisir une automatisation qui réduit une charge récurrente et produit une preuve. Éviter de commencer par le contrôle le plus complexe si les secrets, les droits et les baselines ne sont pas maîtrisés.

19 Synthèse : top 5 risques

Après remplissage, choisir les cinq risques les plus importants. Un risque prioritaire combine impact métier, probabilité crédible, faiblesse de contrôle et absence de preuve.

Rang	Risque	Impact métier	Cause probable	Contrôle existant	Décision
1					
2					
3					
4					
5					

PREUVE Aide au choix

- Risque d'arrêt d'activité prolongé.
- Risque d'exposition de données sensibles.
- Risque fournisseur ou dépendance non maîtrisée.
- Risque d'accès privilégié compromis.
- Risque de non-preuve face à une obligation, un client ou un audit.

PREUVE Formulation attendue

Un risque doit être formulé de manière actionnable. "Manque de sécurité" n'aide pas. "Compromission d'un compte administrateur sans MFA permettant chiffrement des serveurs critiques" permet de décider.

20 Synthèse : top 5 preuves manquantes

Les preuves manquantes sont souvent plus importantes que les outils manquants. Une organisation peut déjà avoir une pratique correcte, mais être incapable de la démontrer rapidement.

Rang	Preuve manquante	Domaine	Responsable	Échéance	Statut
1					
2					
3					
4					
5					

PREUVE Exemples de preuves à forte valeur

- Dernier test de restauration avec résultat et décision.
- Liste des actifs exposés à Internet.
- Revue des comptes privilégiés.
- Matrice exigences/contrôles/preuves.
- Procédure de crise et annuaire hors SI.
- Plan de traitement des vulnérabilités critiques.

PREUVE Règle de qualité

Une preuve utile doit être datée, compréhensible, rattachée à un périmètre et récupérable par une autre personne que son auteur.

21 Premières actions 30 jours

Les 30 premiers jours doivent produire de la clarté et réduire les risques immédiats. Éviter de lancer trop de chantiers en parallèle. Choisir peu d'actions, mais les mener jusqu'à une preuve exploitable.

Action	Objectif	Responsable	Preuve de fin
Valider les actifs et processus critiques	Savoir ce qui doit reprendre en premier	Direction + DSI	Liste priorisée signée
Tester une restauration critique	Vérifier la capacité réelle de reprise	IT/Ops	Compte rendu de test
Revoir les comptes privilégiés	Réduire le risque de compromission	DSI/RSSI	Liste nettoyée ou justifiée
Cadrer les obligations applicables	Éviter la conformité floue	Direction + juridique si besoin	Note de périmètre
Prioriser les vulnérabilités exposées	Réduire l'exposition immédiate	IT/Ops	Backlog priorisé

ACTION Critères de succès

- Les actions ont un propriétaire.
- Les preuves sont réunies dans un emplacement connu.
- Les blocages sont remontés à la direction.
- Les décisions de risque sont documentées.

ALERTE À éviter

Transformer les 30 premiers jours en inventaire exhaustif. L'objectif est de créer une base décisionnelle et de traiter les expositions les plus visibles.

22 Trame de plan 30/60/90 jours

Le plan doit rester lisible par la direction et exploitable par le terrain. Chaque ligne doit indiquer pourquoi l'action existe, qui la porte et quelle preuve montrera qu'elle est terminée.

Horizon	Priorité	Action	Responsable	Preuve	Risque réduit
30 jours					
30 jours					
60 jours					
60 jours					
90 jours					
90 jours					

PREUVE Exemple de logique

- 30 jours : sécuriser les accès critiques, tester une restauration, cadrer les obligations.
- 60 jours : formaliser PRA/PCA, durcir les actifs exposés, structurer les preuves.
- 90 jours : organiser un exercice de crise, industrialiser les indicateurs, préparer l'audit approfondi.

PREUVE Règle d'arbitrage

Si une action ne réduit pas un risque, ne produit pas une preuve ou ne répond pas à une obligation claire, elle doit être reformulée ou différée.

23 Préparer l'audit découverte

L'audit découverte doit transformer la photographie initiale en trajectoire. Il ne doit pas commencer par une collecte massive et floue. Les éléments ci-dessous permettent de gagner du temps et de concentrer l'échange sur les décisions utiles.

PREUVE Documents utiles

- Cartographie ou liste des processus critiques.
- Liste des applications et fournisseurs critiques.
- Derniers tests de sauvegarde ou restauration.
- Politique de gestion des accès ou revue des comptes privilégiés.
- Derniers rapports de vulnérabilités ou plans de correction.
- Procédures incident, crise, PRA/PCA si elles existent.
- Tableau des obligations, clients exigeants ou référentiels visés.

PREUVE Questions à clarifier avant l'échange

- Quelle échéance déclenche le besoin ?
- Quel incident, audit, client ou changement a créé l'urgence ?
- Quelle décision la direction doit-elle prendre après le diagnostic ?
- Quelles contraintes d'exploitation ne doivent pas être ignorées ?
- Quels sujets sont sensibles et doivent rester hors support partagé ?

ACTION Résultat attendu

Une synthèse priorisée : risques visibles, obligations concernées, preuves disponibles, écarts principaux, premières actions 30/60/90 jours et format d'accompagnement recommandé.

24 Page de restitution

Utiliser cette page comme support de synthèse pour un comité court. Les cases vides sont plus utiles qu'un score artificiellement élevé : elles montrent où la décision est nécessaire.

Élément	Synthèse
Score final /100	
Domaine le plus faible	
Domaine le plus solide	
Risque prioritaire numéro 1	
Preuve manquante la plus importante	
Décision direction à prendre	
Action à lancer sous 7 jours	
Audit découverte recommandé	Oui / Non

PREUVE

Message de synthèse

En une phrase : "Notre maturité cyber est principalement limitée par _____, ce qui expose _____. La priorité est de _____ sous _____ jours, avec _____ comme preuve attendue."

ACTION

Critère de passage à l'étape suivante

Planifier un audit découverte si le score est inférieur à 50, si plusieurs domaines critiques sont à 0 ou 1, si aucune restauration récente n'est prouvée, ou si une obligation client/réglementaire impose une trajectoire défendable.

25 Vous avez coché plusieurs zones rouges ?

Une zone rouge n'est pas un échec. C'est un signal utile : le sujet doit être cadré avant d'être transformé en chantier coûteux ou dispersé.

Un audit découverte permet de clarifier :

- le périmètre réellement prioritaire ;
- les obligations à traduire en contrôles et preuves ;
- les risques qui menacent l'activité ;
- les actions 30/60/90 jours ;
- les arbitrages à porter devant la direction ;
- les livrables attendus pour piloter la suite.

ACTION

Prochaine étape

Planifier un audit découverte

Préparer si possible le score rapide, les top 5 risques et les top 5 preuves manquantes. Aucun secret, mot de passe ou détail exposant n'est nécessaire pour ce premier cadrage.