Vytalx

Checklist de sécurité : sources de détection

Identifier les angles morts, fiabiliser l'alerte, prioriser les sources à intégrer (30 minutes)

Vytalx

Comment utiliser cette checklist ?

Cochez chaque point selon votre situation.
L'objectif étant d'identifier rapidement les zones à risque
et de prioriser les actions qui améliorent réellement la capacité de détection & réponse.

Mode d'emploi

1. **Choisissez un périmètre :**
   Identités, postes/serveurs, réseau, cloud/SaaS, sauvegarde, applications critiques (et OT si concerné).

2. **Cochez chaque point :**
   - ✅ Oui = mis en place et fonctionnel
   - ⚠️ Partiel = mis en place mais incomplet / pas fiable / pas systématique
   - ❌ Non = absent

3. **Notez une preuve (si possible) :**
   Où se trouvent les journaux, qui les consulte, combien de temps ils sont conservés, et quel type d'alerte est déclenché.

Exemple

"Tests de restauration mensuels"

- ✅ : test daté et documenté
- ⚠️ : test fait "de temps en temps"
- ❌ : aucun test effectué

Scoring simple

- ✅ = 2 points
- ⚠️ = 1 point
- ❌ = 0 point

Les 5 preuves attendues

1. Inventaire des sources (et responsable par source)
2. Rétention : durée + emplacement (où sont conservés les journaux ?)
3. Routage des alertes : qui reçoit, quand, et via quel canal
4. Exemples de traitement : tickets, comptes rendus, actions prises
5. Capacité d'investigation : "qui a fait quoi, quand" (recherche/export)

Objectif : Passer d'une détection "fragmentée"
à une couverture cohérente et exploitable:
sources prioritaires, qualité des logs, règles d'alerte, preuves.

Vytalx

Périmètre & criticité

Avant de vérifier vos sources, clarifiez les scénarios prioritaires.
Une bonne détection ne couvre pas “tout”, elle couvre ce qui compte :
identités, postes/serveurs, périmètre réseau, cloud/SaaS et systèmes critiques.

Menaces prioritaires

☐ Vol d’identifiants / connexions suspectes
☐ Phishing / BEC (prise de contrôle de boîte, fraude au virement)
☐ Ransomware (chiffrement, suppression de sauvegardes, propagation)
☐ Exfiltration (vol de données, partages anormaux, upload massif)
☐ Mouvement latéral (rebond entre machines/segments)
☐ Élévation de privilèges (passage admin, ajout de rôles, modifications critiques)
☐ Compromission SaaS/Cloud (apps OAuth, accès externes, partages)
☐ Altération de configurations (pare-feu, VPN, sauvegarde, politiques)

Autres: _____
_____
_____

Périmètres à couvrir

Domaine (Identités, M365, Postes, Serveurs, Réseau, VPN, Firewall, DNS-Proxy, Sauvegarde, Apps critiques, Cloud / OT)	**localisation des journaux** (outil / emplacement)	**Rétention** (Nombres de jours)	**Responsable** (équipe / personne)

Les 6 angles morts les plus fréquents

1. Identités : authentifications et changements de rôles/admin non suivis
2. M365 : règles de boîte / consentements apps / partage externe peu surveillés
3. Endpoints : absence de télémétrie sur postes “sensibles” (VIP/finance/admin)
4. Réseau : pas de visibilité sur DNS/proxy/VPN (sortant anormal, C2)
5. Sauvegarde/PRA : événements critiques non surveillés (suppression, échecs, changements)
6. Rétention trop courte : preuves insuffisantes pour investiguer (> 30 jours conseillé pour événements critique)

Vytalx

Checklist : Identités & Cloud/SaaS

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Journaux d'authentification exploitables (succès/échecs, IP, localisation, appareil)	☐	☐	☐	☐	
Alertes sur connexions à risque (pays atypiques, impossible travel, brute force)	☐	☐	☐	☐	
Alertes sur fatigue MFA / contournements (si applicable)	☐	☐	☐	☐	
Journalisation des actions administrateur (création comptes, changements politiques, rôles)	☐	☐	☐	☐	
Surveillance des élévations de privilèges (ajout rôles, changements de groupes sensibles)	☐	☐	☐	☐	
Journalisation et suivi des réinitialisations de mots de passe (et actions sensibles)	☐	☐	☐	☐	
Surveillance des applications tierces / OAuth (nouveaux consentements, permissions élevées)	☐	☐	☐	☐	
Processus d'approbation / revue des apps (qui valide, critères, périodicité)	☐	☐	☐	☐	
Journaux Microsoft 365 exploitables (audit unifié, Exchange, SharePoint/OneDrive, Teams)	☐	☐	☐	☐	
Détection sur messagerie : règles suspectes, transferts externes, connexions anormales.	☐	☐	☐	☐	
Détection sur partage & accès externes (guests, liens, partages anormaux, volume)	☐	☐	☐	☐	
Routage des alertes "identités & SaaS" vers un canal opéré (personnes, astreinte si besoin)	☐	☐	☐	☐	
Rétention suffisante sur ces sources (objectif : ≥ 30 jours sur critique, plus si besoin)	☐	☐	☐	☐	
Capacité d'investigation rapide (reconstituer une chronologie utilisateur)	☐	☐	☐	☐	

Priorité immédiate : Sans sources identités et journaux SaaS exploitables, la plupart des incidents restent invisibles ou incomplets.

Vytalx

Checklist :
Postes, serveurs & workloads

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Inventaire des postes et serveurs à couvrir (périmètre “critique” identifié)	☐	☐	☐	☐	
Couverture agent/télémétrie sur le périmètre critique (serveurs, postes VIP/finance/admin)	☐	☐	☐	☐	
Événements de sécurité exploitables (authent, élévations, échecs, changements sensibles)	☐	☐	☐	☐	
Télémétrie comportementale / EDR (si disponible) : processus, commandes, persistance	☐	☐	☐	☐	
Alertes sur exécutions suspectes (PowerShell/Script, outils d’admin détournés, LOLBins)	☐	☐	☐	☐	
Alertes sur persistance (tâches planifiées, services, clés registre, démarrage)	☐	☐	☐	☐	
Alertes sur mouvement latéral (RDP/SMB anormal, comptes admin utilisés hors périmètre)	☐	☐	☐	☐	
Détection ransomware (activité de chiffrement, suppressions massives, renommages)	☐	☐	☐	☐	
Protection contre altération/désactivation des agents (anti-tampering si applicable)	☐	☐	☐	☐	
Journalisation des actions administrateur sur serveurs (installations, désactivations, changements)	☐	☐	☐	☐	
Collecte d’événements sur contrôleurs de domaine / serveurs clés (si concernés)	☐	☐	☐	☐	
Centralisation des événements (corrélation possible, recherche unique)	☐	☐	☐	☐	
Rétention suffisante (objectif : ≥ 30 jours sur critique, plus selon besoin)	☐	☐	☐	☐	
Procédure de triage (quoi faire quand une alerte endpoint tombe)	☐	☐	☐	☐	

Signal d’alerte : Une couverture “partielle” sur les serveurs ou sur les postes à privilèges suffit à laisser un chemin de compromission.

Vytalx

Checklist : Réseau, périmètre & applications

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Firewall/UTM : journaux exploitables (accept/deny, menaces, admin changes)	☐	☐	☐	☐	
Alertes sur changements d'administration réseau (règles, NAT, VPN, comptes admin)	☐	☐	☐	☐	
VPN/ZTNA : journaux exploitables (connexions, échecs, géoloc, appareils)	☐	☐	☐	☐	
DNS : visibilité sur requêtes (domaines suspects, DGA, volumes anormaux)	☐	☐	☐	☐	
Proxy / web filtering : visibilité sortante (catégories, domaines rares, volumes)	☐	☐	☐	☐	
Détection exfiltration (volumes anormaux, uploads massifs, destinations atypiques)	☐	☐	☐	☐	
Messagerie / passerelle email (si distincte) : journaux & alertes exploitables	☐	☐	☐	☐	
Accès privilégiés (bastion/PAM si présent) : traces exploitables (sessions, commandes)	☐	☐	☐	☐	
Applications critiques : journaux applicatifs disponibles (auth, actions sensibles, erreurs)	☐	☐	☐	☐	
Surveillance des changements applicatifs sensibles (droits, exports, comptes admin appli)	☐	☐	☐	☐	
Sauvegarde/PRA : événements de sécurité suivis (échecs, suppressions, changements de politique)	☐	☐	☐	☐	
Centralisation des logs réseau et applicatifs (recherche unique, corrélation possible)	☐	☐	☐	☐	
Rétention et horodatage cohérents (NTP, time sync) pour corréler les événements	☐	☐	☐	☐	
Runbook d'investigation "réseau" (quoi vérifier en cas d'alerte)	☐	☐	☐	☐	

Angle mort courant : DNS, VPN et logs de sauvegarde sont souvent sous-exploités, alors qu'ils donnent des signaux très tôt (C2, accès à distance, sabotage).

Vytalx

Synthèse & plan d'action

Votre résultat

Score total : ____ / ____

Niveau : ☐ Risque élevé (0%-49%) ☐ À consolider (50%-74%) ☐ Structuré (75%-100%)

Barème :	Calcul :
✅ Oui = 2 pts ⚠️ Partiel = 1 pt ❌ Non = 0 pt	**Score obtenu** = somme des points **Score Max** = 2 × (nb de lignes évaluées)

Zones rouges

Vos 5 écarts prioritaires :

_____

_____

_____

_____

_____

Points bloquants

☐ Aucune source identités exploitable (authentifications + actions admin)
☐ Pas de télémétrie endpoint/serveur sur le périmètre critique
☐ Logs non centralisés ou rétention insuffisante (< 30 jours sur critique)
☐ Alertes sans destinataire / sans procédure de traitement
☐ Investigation impossible ("qui a fait quoi, quand ?")

Plan d'action

Phase 1 : Cartographier & attribuer

- Finaliser l'inventaire des sources (identités, M365, endpoints, réseau, sauvegarde)
- Désigner un responsable par domaine et clarifier le canal d'alerte
- Fixer une rétention cible sur le critique (≥ 30 jours)

Phase 2 : Couvrir l'essentiel (priorité identités + M365)

- Rendre exploitables les logs authentification et actions admin
- Mettre sous contrôle les signaux M365 : règles mailbox, consentements apps, partage externe
- Vérifier l'exportabilité des preuves (recherche, export, chronologie)

Phase 3 : Endpoints + réseau

- Étendre la télémétrie aux serveurs et aux postes à privilèges
- Centraliser les sources réseau : VPN, firewall, DNS/proxy
- Définir 5 alertes prioritaires (ransomware, admin change, exfiltration, login à risque, consentement app)

Phase 4 : Industrialisation

- Écrire 2 - 3 runbooks (compte compromis, ransomware, exfiltration)
- Mettre en place un rituel de revue (hebdo/mensuel) + tableau de bord simple
- Tester un scénario d'investigation : chronologie d'un utilisateur (preuve)