

3 catégories, 5 fonctions, 15 façons de vous défendre.

ISO 27002:2022 · NIST CSF 2.0 · ITGC

Aucun contrôle n'est infaillible. La sécurité naît de leur combinaison en couches — la défense en profondeur.

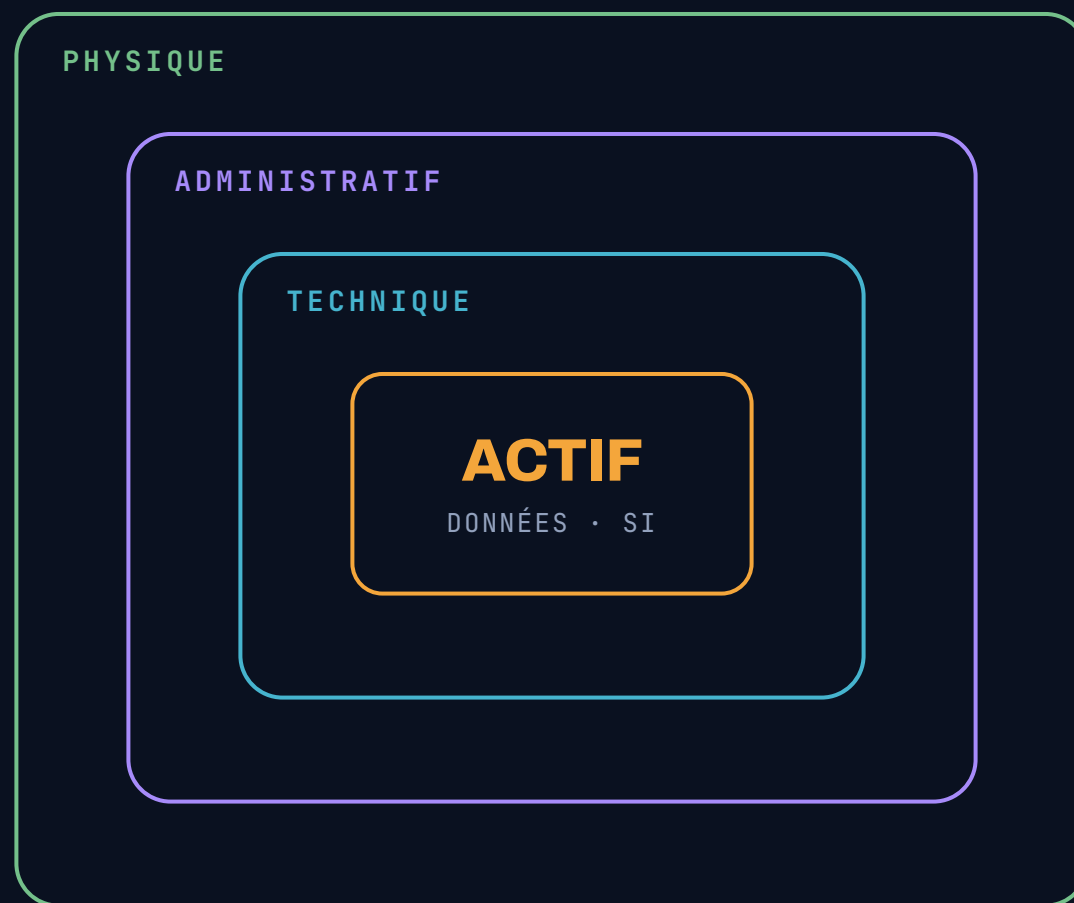
| TECHNIQUE

| ADMINISTRATIF

| PHYSIQUE

On ne protège pas un actif avec un mur.

On l'entoure de couches.



Chaque couche rattrape les défaillances de la précédente. **Franchir une barrière ne suffit jamais** à atteindre l'actif : c'est toute la logique de la **défense en profondeur.**

5 fonctions

Préventif

> PROTECT

Empêcher l'incident avant qu'il survienne. La barrière en amont.

Détectif

> DETECT

Repérer l'incident quand il se produit. La visibilité.

Correctif

> RESPOND · RECOVER

Réduire l'impact et rétablir après l'incident. La résilience.

Dissuasif

> DETER

Décourager l'attaquant avant même la tentative. Le signal.

Compensatoire

> RISK TREATMENT

Suppléer un contrôle principal impossible ou défaillant. Le plan B.

ISO 27002:2022 formalise 3 types via l'attribut `#Control_types` (Préventif / Détectif / Correctif). Dissuasif & Compensatoire complètent la taxonomie (CISSE · NIST SP 800-53).

Technique

Préventif > PROTECT	MFA · Chiffrement · Pare-feu · Filtrage web · EDR
Détectif > DETECT	IDS · SIEM · Surveillance des logs
Correctif > RESPOND	Sauvegardes automatiques · Reprise après sinistre (DRP) · Patch automatique
Dissuasif > DETER	Bannières d'avertissement · Messages de connexion · Notifications d'audit
Compensatoire > COMPENSATING	Backup cloud quand la sauvegarde locale est impossible

Administratif

Préventif > PROTECT	Politiques de sécurité · Formation · Procédures (SOP)
Détectif > DETECT	Audits · Revues de logs · Évaluations des risques
Correctif > RESPOND	Plan de réponse aux incidents · Gestion de crise · Sanctions
Dissuasif > DETER	Charte de confidentialité · Règlement intérieur
Compensatoire > COMPENSATING	Supervision renforcée · Contrôles croisés · Alternative réalisable

Physique

Préventif

> PROTECT

Portes sécurisées · Badges d'accès · Clôtures & barrières

Détectif

> DETECT

Caméras · Détecteurs de mouvement · Alarmes

Correctif

> RECOVER

Groupes électrogènes · Systèmes anti-incendie · Premiers secours

Dissuasif

> DETER

Signalisation · Éclairage de sécurité · Agents visibles

Compensatoire

> COMPENSATING

Sites de repli · Accès alternatifs · Surveillance redondante

15 combinaisons, 1 stratégie

FONCTION \ COUCHE	TECHNIQUE	ADMINISTRATIF	PHYSIQUE
Préventif PROTECT	MFA · Chiffrement · Pare-feu · EDR	Politiques · Formation · SOP	Portes · Badges · Clôtures
Détectif DETECT	IDS · SIEM · Logs	Audits · Revues de logs · Éval. risques	Caméras · Détecteurs · Alarmes
Correctif RESPOND · RECOVER	Sauvegardes · DRP · Patch auto	Réponse incident · Crise · Sanctions	Générateurs · Anti-incendie · Secours
Dissuasif DETER	Bannières · Notifications d'audit	Charte · Règlement intérieur	Signalisation · Éclairage · Agents
Compensatoire COMPENSATING	Backup cloud (si local KO)	Supervision · Contrôles croisés	Sites de repli · Redondance

À retenir : une posture solide couvre les 3 couches ET les 5 fonctions – pas une ligne, pas une colonne : toute la grille.

Ce que disent les référentiels

CATÉGORIES > THÈMES ISO 27002:2022

Technique = Technologique (cl. 8) · **Administratif** = Organisationnel (cl. 5) + Personnes (cl. 6) · **Physique** = Physique (cl. 7)

FONCTIONS > ATTRIBUTS & NIST CSF 2.0

ISO **#Control_types** : Préventif / Détectif / Correctif — mappés **PROTECT** · **DETECT** · **RESPOND/RECOVER**. Dissuasif & Compensatoire : extension CISSP / NIST SP 800-53.

LE PRINCIPE > DEFENSE IN DEPTH & ITGC

Aucune couche ni aucun type ne suffit seul : la **résilience naît de la combinaison**. La logique préventif/détectif est aussi le socle des **ITGC** en audit SI.

// À VOUS DE JOUER

Quelle case de votre matrice est **encore vide** ?

La défense en profondeur ne se mesure pas au nombre d'outils, mais à la couverture des 15 cases. Repérez vos angles morts.

ENREGISTREZ

gardez la matrice comme grille d'auto-évaluation

PARTAGEZ

diffusez-la à votre équipe sécurité / audit

COMMENTEZ

quel contrôle placeriez-vous en priorité ?



Ignace YAO

EXPERT EN CYBERSÉCURITÉ · AUDITEUR SI

#IS027002 · #NIST · #ITGC · #DefenseInDepth · #Cybersécurité · #RSSI