10 vérifications avant votre premier café.

La posture de sécurité ne se construit pas le jour de l'audit.
Elle se joue chaque matin — dans la routine.

DÉTECTER | PROTÉGER | GOUVERNER

Ignace YAO
EXPERT CYBERSÉCURITÉ · AUDITEUR SI

Glissez →

Un incident ne se gère pas quand il éclate.
Il se gagne — ou se perd — dans la routine qui le précède.

Ces 10 contrôles ne sont pas une checklist de conformité. C'est une **discipline quotidienne** : transformer la réactivité en proactivité, avant que la menace ne dicte le tempo.

Je les regroupe en **3 réflexes** — Détecter, Protéger, Gouverner.

Détecter

[01] ALERTES SIEM

Traiter les alertes critiques des 24 dernières heures

Prioriser ce qui indique une exfiltration ou une compromission active, pas le bruit de fond.

RISQUE Chaque minute de latence **élargit la fenêtre d'exposition**.

[02] PARE-FEU & IDS / IPS

Inspecter connexions bloquées, scans de ports, trafic anormal

Enquêter sur les anomalies répétées ou persistantes en périphérie.

RISQUE Les signaux faibles d'une **reconnaissance en cours**.

[03] JOURNAUX D'AUTHENTIFICATION

Repérer échecs répétés, horaires atypiques, géolocalisations improbables

Identifier les accès non autorisés et les tentatives de mouvement latéral.

RISQUE La signature d'un **compte compromis**.

[04] REMONTÉES UTILISATEURS

Exploiter les signalements de phishing et emails suspects

Le signalement n'est pas une nuisance : c'est du renseignement de terrain.

RISQUE L'humain reste votre **premier capteur**.

Protéger

[05] SAUVEGARDES

Vérifier l'exécution ET la restaurabilité

Contrôler les jobs de la nuit et tester réellement une restauration.

RISQUE Une sauvegarde jamais testée est un **pari face au ransomware.**

[06] ENDPOINTS · EDR

Agents à jour, actifs, aucune machine muette

Traiter immédiatement toute menace active et toute perte de télémétrie.

RISQUE Un poste non couvert est un **angle mort.**

[07] CORRECTIFS CRITIQUES

Couvrir les CVE activement exploitées et les zero-day

Prioriser par le risque réel : exploitabilité et exposition, pas le seul score CVSS.

RISQUE Une vulnérabilité connue non corrigée est une **porte laissée ouverte**.

[08] SANTÉ DES OUTILS

SIEM, FW, EDR, Mail Gateway, PAM, SASE, SD-WAN

Confirmer que chaque brique de sécurité est opérationnelle et collecte bien.

RISQUE Un capteur en panne = une **cécité silencieuse**.

Gouverner

[09] VEILLE & CTI

Croiser IOC et campagnes actives ciblant votre secteur

Adapter les défenses aux tendances du jour, pas à celles du trimestre dernier.

RISQUE Une défense figée face à une **menace mouvante**.

[10] DOCUMENTATION & ESCALADE

Consigner les anomalies, escalader au bon niveau, au bon moment

Tracer chaque déviation et alerter l'équipe responsable du périmètre.

RISQUE Sans traçabilité : **ni preuve, ni amélioration**.

La discipline avant la conformité.

01 Alertes SIEM
DETECT

02 Pare-feu & IDS/IPS
DETECT

03 Journaux d'authentification
DETECT

04 Remontées utilisateurs
DETECT

05 Sauvegardes & restauration
PROTECT

06 Endpoints · EDR
PROTECT

07 Correctifs critiques
PROTECT

08 Santé des outils de sécurité
PROTECT

09 Veille & CTI
GOVERN

10 Documentation & escalade
GOVERN

Cette liste n'est pas exhaustive — **et c'est volontaire.** L'objectif n'est pas de tout couvrir, mais d'**ancrer un réflexe** : rendre la proactivité systématique.

// À VOUS DE JOUER

Quel contrôle ajouteriez-vous à cette routine ?

La meilleure To-Do quotidienne est celle qu'une équipe s'approprie.
Complétez-la avec vos propres réflexes de terrain.

ENREGISTREZ gardez cette routine à portée de main

PARTAGEZ envoyez-la à votre équipe SOC / IT

COMMENTEZ quel 11e contrôle manque à cette liste ?

IY

Ignace YAO

EXPERT EN CYBERSÉCURITÉ · AUDITEUR SI

#Cybersécurité · #SOC · #RSSI · #BlueTeam · #SécuritéOpérationnelle