

Gestion des vulnérabilités dans un SOC

De l'identification à la remédiation continue : Le manuel d'ingénierie

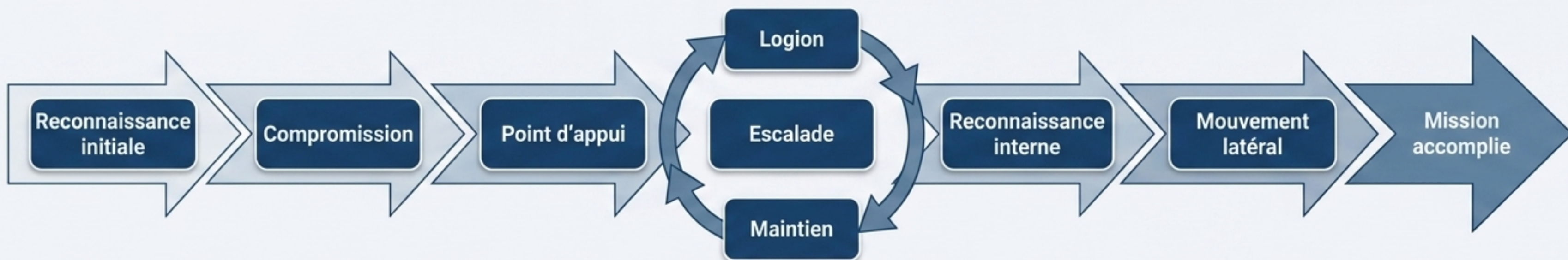
« Le maillon le plus faible d'une chaîne est le plus fort, car c'est lui qui peut la briser. »

— Stanislaw Jerzy Lec

Une seule faille suffit pour qu'un attaquant établisse de multiples points d'ancrage, rendant la remédiation complète extrêmement complexe.

L'anatomie d'une compromission

Le parcours de l'attaque



La réalité du terrain

35 jours

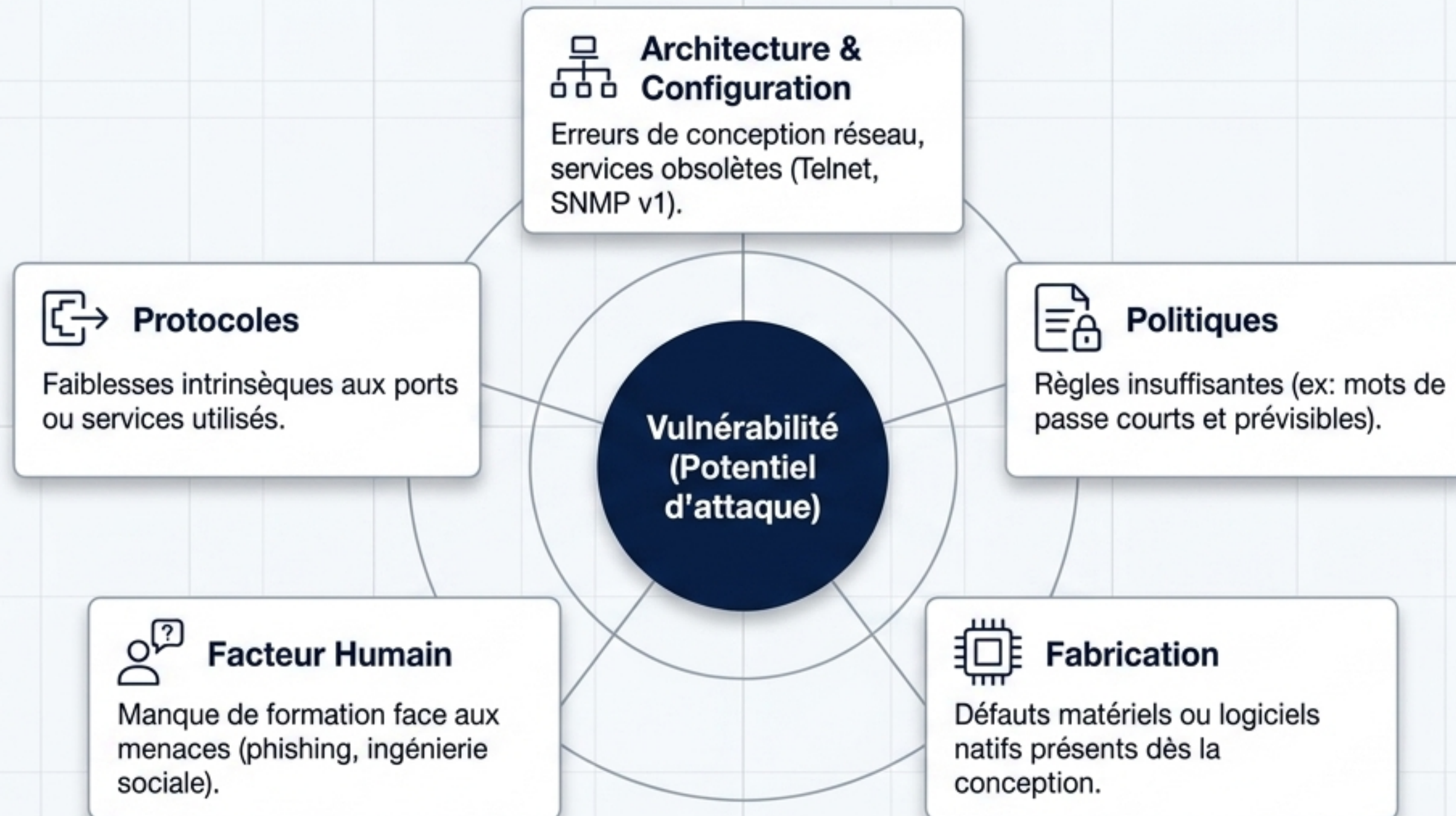
Délai (ou moins) requis par 50 % des organisations pour découvrir un logiciel malveillant interne.

99,9 %

Des vulnérabilités exploitées avec succès l'ont été plus d'un an après la publication de leur correctif (CVE).

La majorité des compromissions auraient pu être évitées par un audit continu.
L'objectif n'est pas la correction absolue, mais la gestion rigoureuse.

Typologie des vulnérabilités



Note Opérationnelle : Être vulnérable signifie avoir un potentiel d'attaque, mais le risque réel dépend de l'exposition. Un service web vulnérable non connecté à Internet présente un risque gérable.

Matrice diagnostique des services de sécurité

	Objectif principal	Limites	Cas d'utilisation optimal
Audits de conformité	Prouver la conformité légale (ex: PCI DSS) ou vérifier des politiques internes.	Peut donner un faux sentiment de sécurité ; en retard sur les tactiques réelles.	Validation réglementaire obligatoire.
Évaluation des vulnérabilités	Découvrir et lister les failles connues et inconnues via des outils automatisés.	Failles non validées ; génère des faux positifs potentiels.	Surveillance continue de l'état des risques.
Évaluation de la configuration	Analyser l'architecture par rapport aux meilleures pratiques de l'industrie.	Identifie le problème de configuration, mais ne valide pas toujours l'exploitabilité.	Renforcement proactif (Hardening) des systèmes.
Tests d'intrusion (Pen Test)	Tenter d'exploiter activement une faille pour en valider la criticité.	Coûteux et ciblé ; risque de gaspillage si la portée est mal définie.	Boîte noire, blanche ou grise ; idéal pour valider une évaluation préalable.

L'arsenal de détection : Cartographie des outils

Rack 1 : Découverte & Inventaire

```
root@kali:~# nmap 10.0.2.62
Starting Nmap 6.47 ( http://nmap.org ) at 2013-09-19 21:59 EDT
Nmap scan report for 10.0.2.62
Host is up (0.0091s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
445/tcp    open  wsddapi
5357/tcp   open  wsddapi
```

- **Nmap** : Cartographie réseau, détection d'hôtes, de services, OS et pare-feu. Outil de base de l'inventaire.

Rack 2 : Analyse automatisée

- **OpenVAS** : Framework libre, mises à jour quotidiennes, plus de 35 000 tests de vulnérabilité.
- **Nessus (Tenable)** : Scanner commercial populaire, permet d'appliquer des exploits basiques pour valider les failles.

Rack 3 : Validation & Tests d'intrusion

- **Metasploit (Rapid7)** : Framework open source pour concevoir et exécuter du code d'exploitation ciblé.
- **Core Impact** : Plateforme commerciale pour tests multi-vectoriels (réseaux, web, mobiles).
- **Kali Linux** : L'écosystème complet avec plus de 600 outils de test d'intrusion intégrés.

Les 4 postures face au risque

Atténuer (Mitigate)

Mettre en œuvre une contre-mesure technique ou procédurale pour réduire activement le risque ou l'exposition de l'actif.

Transférer (Transfer)

Souscrire une cyberassurance ou externaliser le service pour transférer tout ou partie du coût d'une perte potentielle.

Accepter (Accept)

Reconnaître l'existence du risque et choisir d'absorber la perte potentielle (souvent parce le coût de correction dépasse l'impact).

Éviter (Avoid)

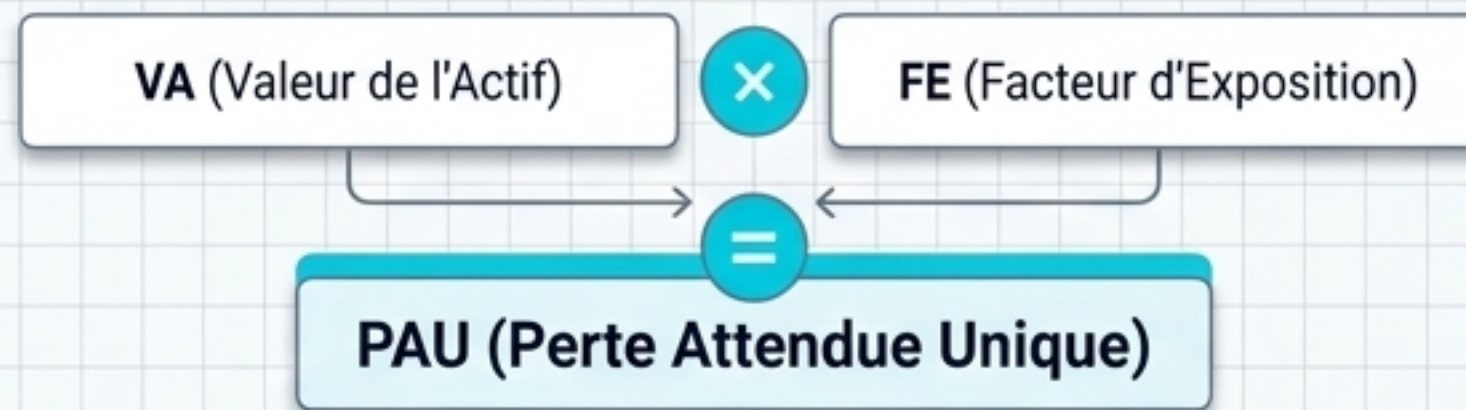
Ignorer le risque délibérément ou cesser l'activité commerciale qui génère cette exposition.

Le paramètre géographique

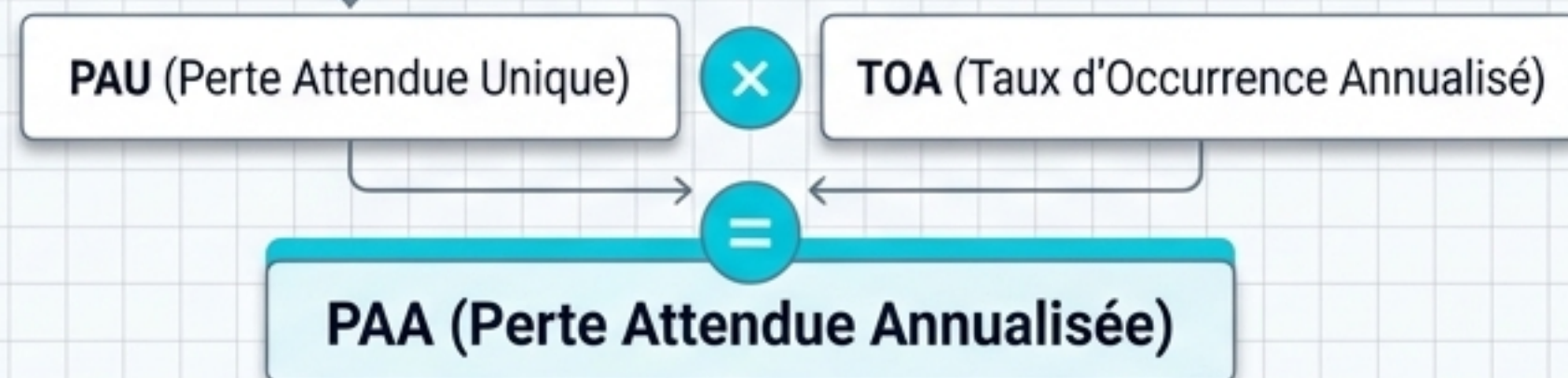
La posture est contextuelle. Face à un risque sismique, un bureau en Floride pourrait l'Accepter (faible probabilité), tandis qu'un bureau en Californie choisira de l'Atténuer ou de le Transférer.

Analyse quantitative du risque (Le ROI de la sécurité)

Étape 1 : Le risque unitaire



Étape 2 : L'échelle annuelle



Étape 3 : La décision d'investissement



Règle de décision : Si la VM est négative (ou si le CAM dépasse la VA), l'investissement n'est pas financièrement justifié, sauf obligation réglementaire.

Méthodologie OWASP : L'équation du risque

$$\text{Risque} = \text{Probabilité} \times \text{Impact}$$

Hémisphère Gauche : Probabilité (Scores 0-9)

Agents de menace :

- Niveau de compétence
- Motivation
- Opportunité
- Taille du groupe

Facteurs de vulnérabilité :

- Facilité de découverte
- Facilité d'exploitation
- Notoriété
- Détection d'intrusion

Hémisphère Droit : Impact (Scores 0-9)

Impact Technique :

- Perte de confidentialité
- Perte d'intégrité
- Perte de disponibilité
- Perte de traçabilité

Impact Commercial :

- Dommages financiers
- Atteinte à la réputation (ex: violation RSA de 66 M\$)
- Non-conformité
- Violation de la vie privée

Matrice de sévérité (Heatmap OWASP)

		Impact			
		Négligeable	Marginal	Critique	Catastrophique
Probabilité	Certain	MOYEN	ÉLEVÉ	ÉLEVÉ	EXTRÊME
	Probable	FAIBLE	MOYEN	ÉLEVÉ	EXTRÊME
	Possible	FAIBLE	MOYEN	ÉLEVÉ	ÉLEVÉ
	Improbable	FAIBLE	FAIBLE	MOYEN	ÉLEVÉ
	Rare	FAIBLE	FAIBLE	MOYEN	ÉLEVÉ

Le Gradient d'Action SOC :

- Faible ($0 < 3$)
- Moyen ($3 < 5$)
- Élevé ($5 < 7$)
- Extrême ($7 < 9$)

Application : Le SOC cible instantanément les vulnérabilités du quadrant supérieur droit pour une remédiation immédiate.

Le cycle de vie SANS (Vue d'ensemble)

1. Inventaire des actifs

2. Gestion de l'information

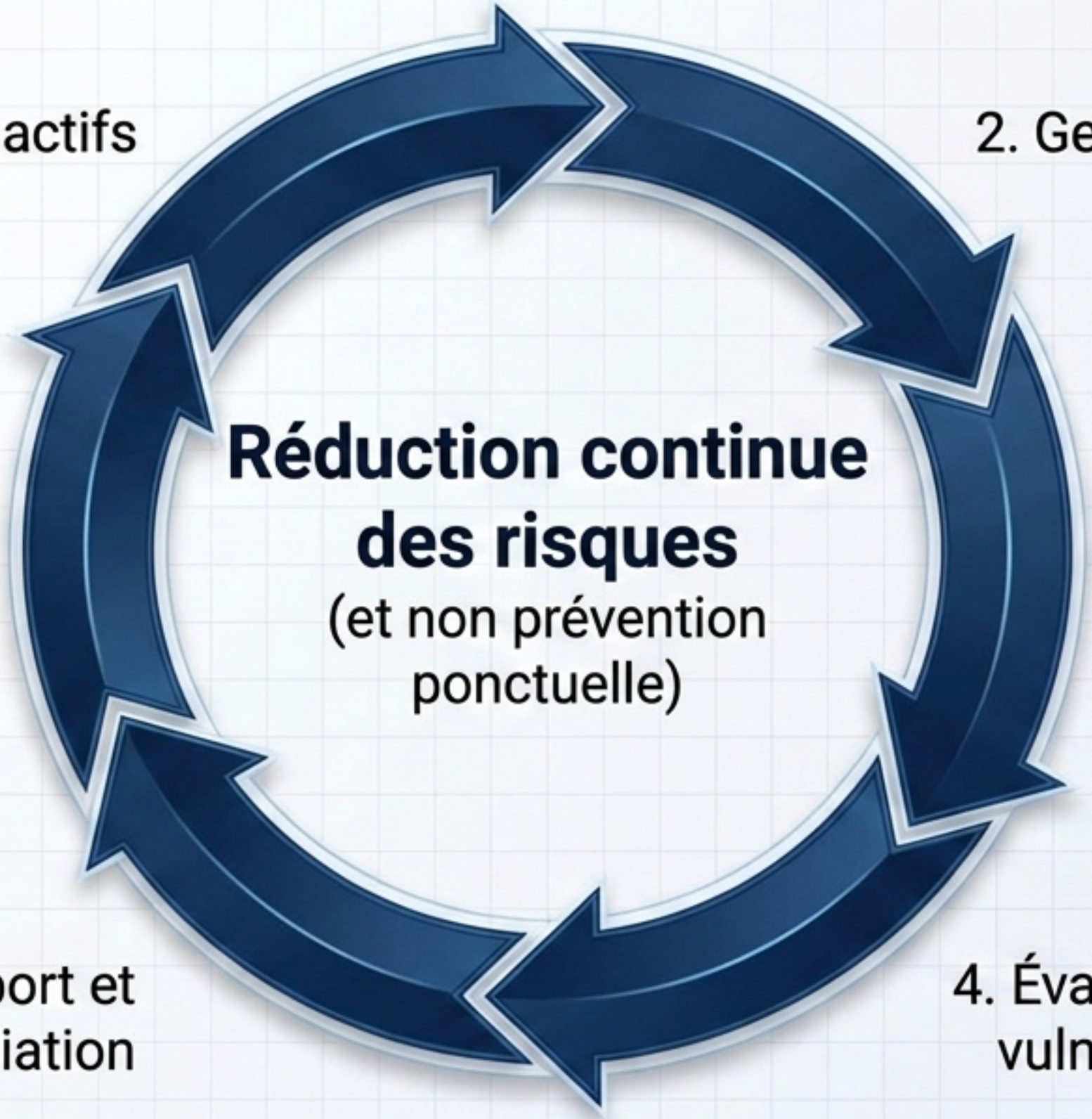
3. Évaluation des risques

4. Évaluation des
vulnérabilités

5. Rapport et
remédiation

6. Réponse

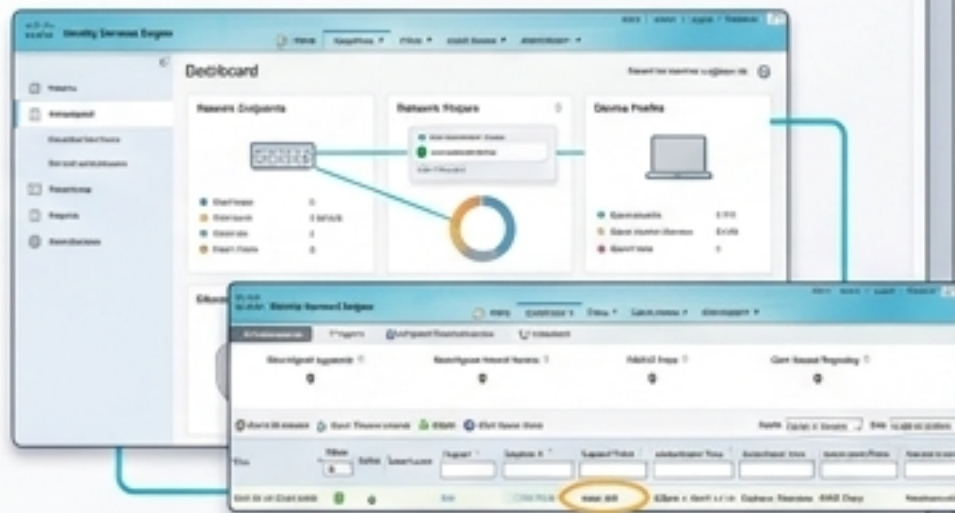
**Réduction continue
des risques**
(et non prévention
ponctuelle)



Les Fondations : Étapes 1 à 3 du cycle SANS

1

Inventaire des actifs



Le défi de la visibilité réseau totale.
Utilisation du contrôle d'accès (NAC).

Outil clé : Cisco ISE pour profiler dynamiquement les appareils (DHCP, DNS, ARP) et déjouer l'usurpation d'adresse MAC.

2

Gestion de l'information

Maîtrise des données sensibles relatives aux risques et communication d'urgence coordonnée.



Acteur : Une équipe CSIRT dédiée.

Outils : Cisco WebEx, TelePresence, listes de diffusion sécurisées pour la mobilisation rapide.

3

Évaluation des risques

Coter le risque avant d'effectuer les scans pour prioriser l'effort sur les actifs critiques.



Outils : Plateformes GRC (comme RSA Archer), OpenFISMA, ou feuilles de calcul automatisées pour appliquer les calculs ISC.

L'Action : Étapes 4 à 6 du cycle SANS

4

Évaluation des vulnérabilités

Déploiement tactique d'audits et de tests ciblés selon le niveau de tolérance au risque établi à l'étape 3.

Outils clés : Scanners automatisés comme Nessus et OpenVAS.

5

Rapport et Correction

Justification budgétaire, centralisation des événements et suivi granulaire des correctifs appliqués.

Outils : Plateformes SIEM (Splunk couplé à Cisco ISE pour la quarantaine), outils de gestion de tickets (TeamSupport, Mhelpdesk).

6

Réponse

Exécution du plan global basé sur l'impact commercial (qui prime sur l'impact système).

Action : Collaboration avec les fournisseurs et déploiement de mesures de contournement (Workarounds) temporaires si aucun correctif n'est disponible.

Intégration du Renseignement sur les menaces (Threat Intel)

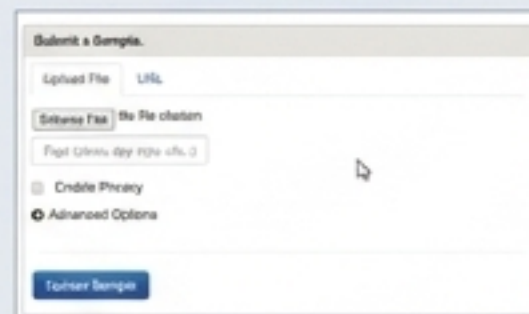
Sources Externes

- Signatures d'attaque (Atomiques et Dynamiques).
- Flux STIX/TAXII via MITRE.
- Bases de données partagées.



Le Moteur d'Intel

Cisco ThreatGrid : Analyse unifiée (Sandbox)

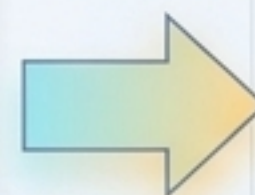


recevant plus de 200 000 échantillons par jour.

Lancope StealthWatch : Télémétrie NetFlow

Dest Adress	Alarm	Source	Détails	Target Threat	Target
192.168.1.100	High	192.168.1.100	Source IP: 192.168.1.100 Destination IP: 192.168.1.100 Destination Port: 80 Destination Country: US Destination City: New York Destination State: New York	Destination Country: US Destination City: New York Destination State: New York	192.168.1.100

pour détecter les communications vers les serveurs C&C.

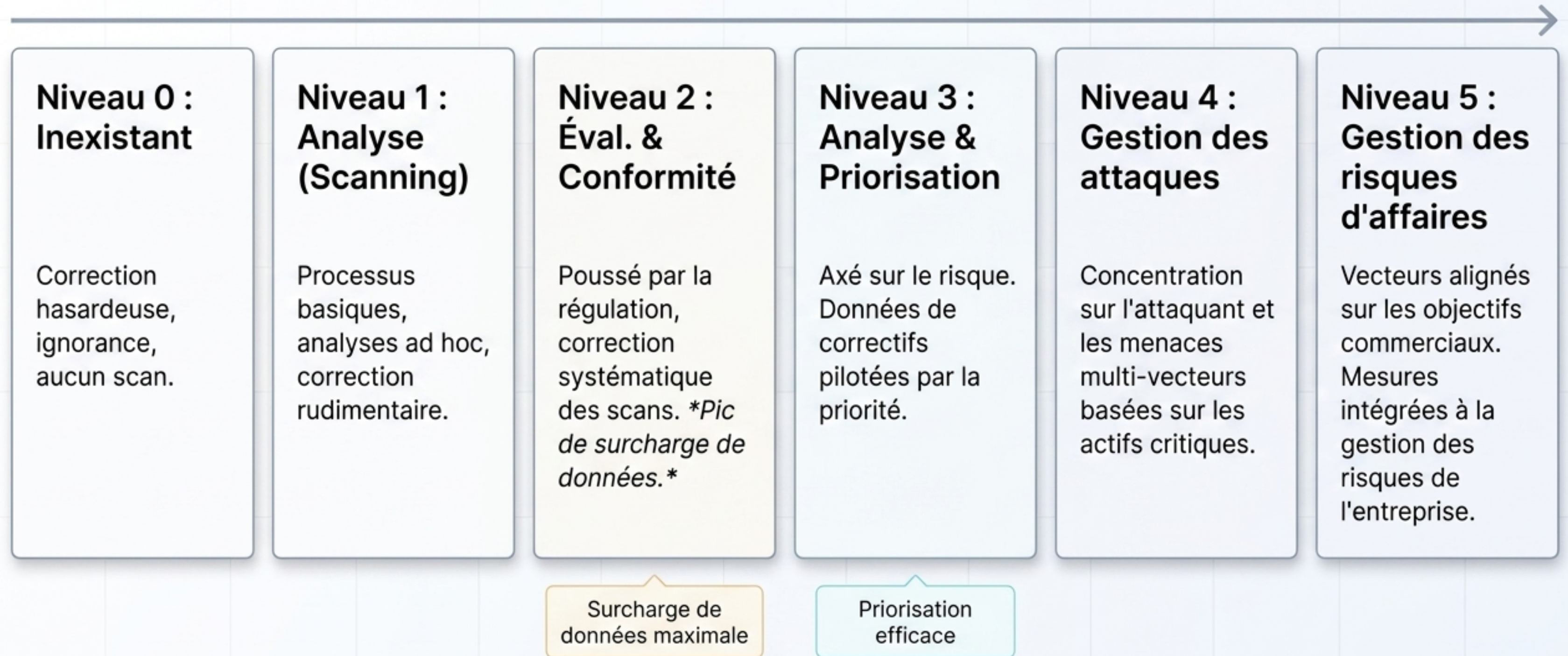


Action / Déchargement

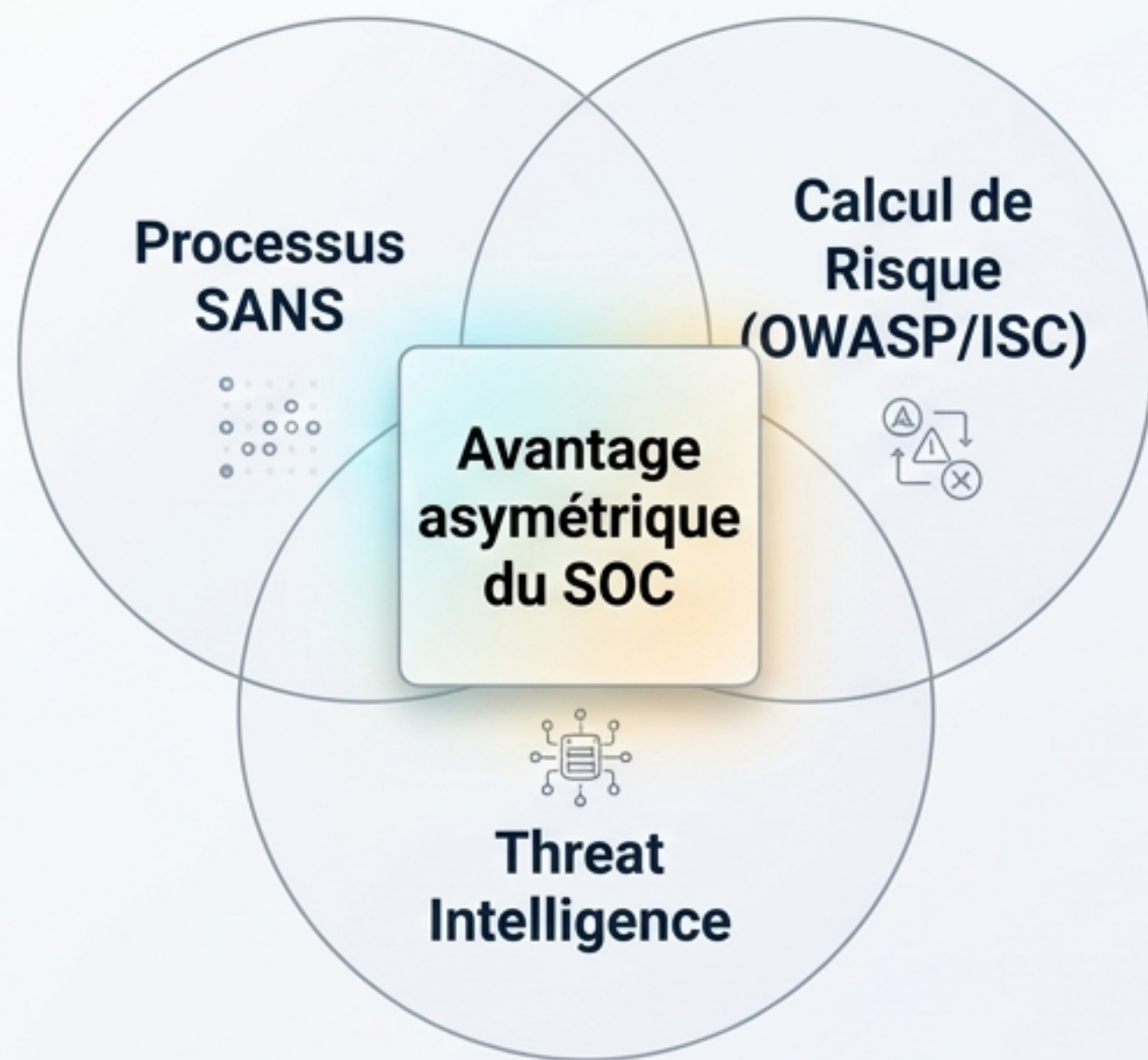


- Externalisation du premier filtre : Utilisation des scores de réputation (Cisco WSA) pour bloquer en amont.
- Avantage : Libère la puissance de calcul locale du SOC pour les menaces complexes.

Modèle de maturité de la gestion des vulnérabilités



Synthèse : L'ingénierie continue du SOC



1. L'automatisation est vitale

Face au fait que 99,9 % des exploitations réussies touchent des failles anciennes, les processus manuels échouent systématiquement face au volume.

2. L'architecture de la réponse

Réunir rapidement les bonnes personnes (CSIRT) est souvent plus critique pour la résilience de l'entreprise que la technologie elle-même.

3. L'externalisation du premier filtre

Bloquer automatiquement par réputation IP/URL permet de concentrer la puissance d'analyse locale du SOC sur les menaces les plus sophistiquées.

La sécurité n'est pas un état de fait, c'est une ingénierie continue.