# SOC : Définition et rôle en cybersécurité défensive

Antoine Bénar

abenar@omnesintervenant.com

# Objectifs du cours

- C’est quoi un SOC ?
- Compréhension des outils de sécurité
- Bases en
  - Investigation
  - Catégorisation d’incidents de sécurité
  - Gestion de crises et compromissions

# Introduction

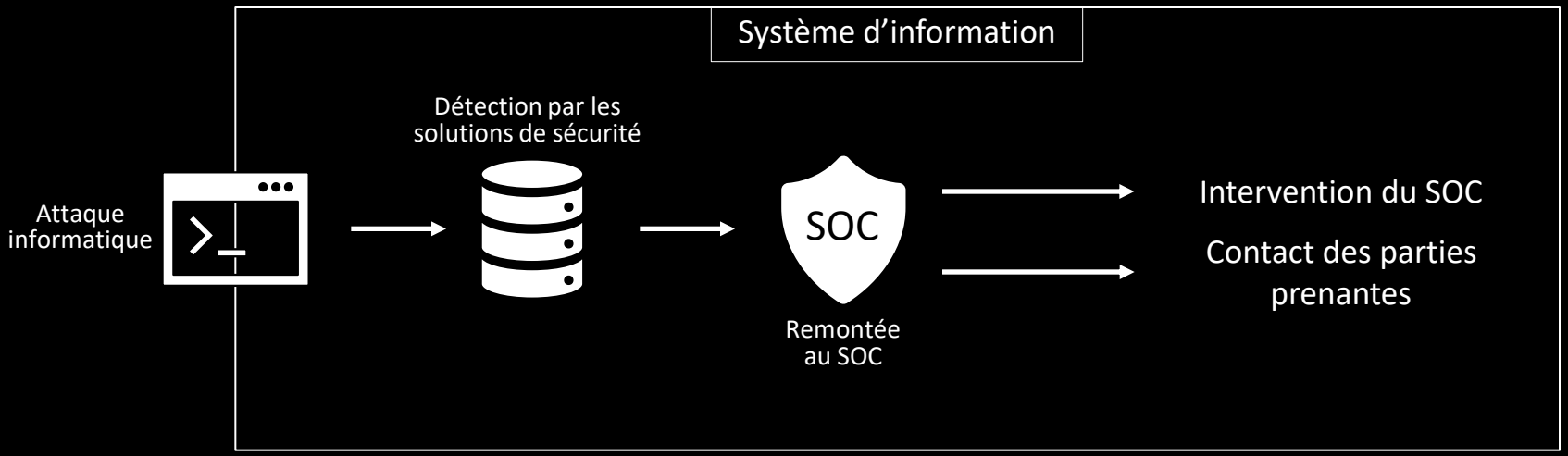
Proposition du **NIST** :
1. Identify
2. Protect
3. Respond
4. Recover

Un SOC (Security Operations Center) est au cœur de la cybersécurité défensive

Il supervise, détecte et répond aux incidents 24/7

# Définition d'un SOC

Un SOC est une équipe dédiée à la surveillance, la détection, l'analyse et la réponse aux incidents de sécurité.



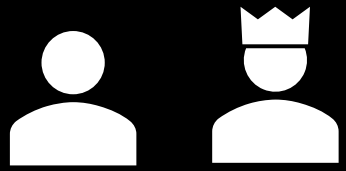
# Différents SOC

## Co-Managé

ESN — Client

≈ 20–25 %

## Managé

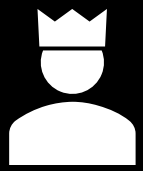


Client — ESN

≈ 45–50 %

## Interne

≈ 25–30 %



Client

Les consoles managées impliquent souvent un **MSSP (Managed Security Service Provider)**, c'est-à-dire un prestataire externe qui supervise la sécurité 24/7 à la place ou aux côtés de l'entreprise.

# Objectifs principaux

1. Détecter les attaques
2. Réagir rapidement
3. Minimiser l'impact
4. Améliorer la posture de sécurité en continu

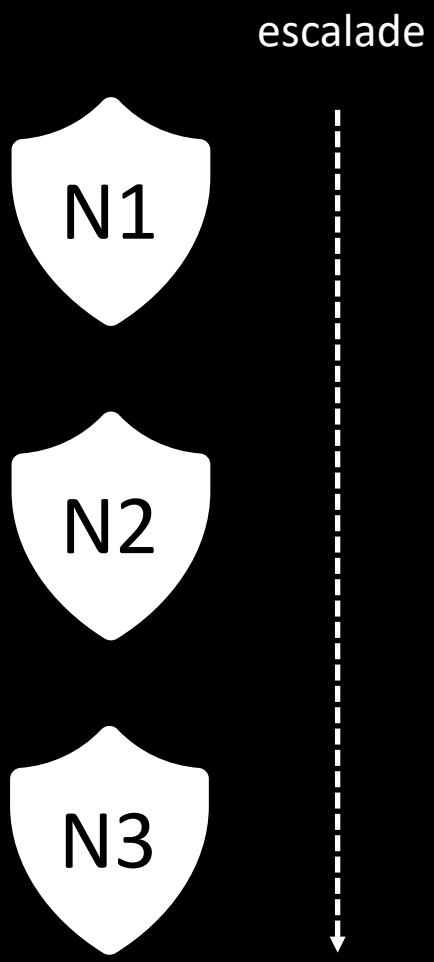
Le SOC **analyse** en temps réel les événements des systèmes informatiques pour identifier les **activités suspectes**.

# Structure classique d'un SOC

Niveau 1 (N1) : Surveillance basique et escalade

Niveau 2 (N2) : Analyse approfondie

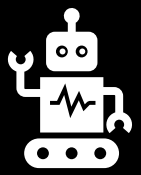
Niveau 3 (N3) : Réponse à incidents (IR)



# Outils principaux du SOC

EDR/XDR (Endpoint Detection & Response – Extended Detection & Response)

SIEM (Security Information and Event Management)



SOAR (Security Orchestration, Automation and Response)

# L'EDR : Protection des machines

Le terme EDR (**Endpoint Detection and Response**) apparaît autour de 2013, une époque où les antivirus classiques ne suffisent plus.

Pour faire simple, un EDR :

Est un « Antivirus amélioré », réalise des détections **comportementales**

S'installe sur **toutes les machines du SI** (ou presque)

Est la **brique principale** des SOC modernes

Prends des actions de **remédiation automatiques** (quarantaine des fichiers…)

Des exemples : SentinelOne, Cortex, Crowdstrike, HarfangLab

# Le SIEM - historique

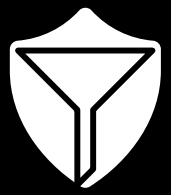
Les SIEM : Security Information and Event Management, sont apparu dans les années 2000 pour centraliser & analyser les journaux de sécurité du SI

Permet de **rassembler** en un seul endroit toute la **sécurité** du SI, de créer des **règles de détection**, et **d'historiser** en cas d'incidents

Il nécessite souvent un **concentrateur**, « forwarder » de journaux vers une brique centrale qui stockera ces données sous le même format (localement ou dans le cloud)

Des exemples : Splunk, Wazuh, IBM QRadar.

# XDR : Protection périmétrique



L'XDR, «Extended» Detection & Response est un terme assez large qui naît en 2019 et qui explose depuis.

Souvent,
**XDR ≃ SIEM + EDR + Playbooks**
(les XDR remplacent les SIEM)

Et ajoute la création de **playbooks** ('plans d'action' prêts à appliquer en cas d'incident)

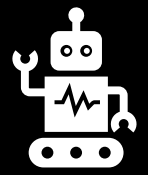
Permet l'utilisation de **règles de détections**…

Et contrairement à un EDR, permet la surveillance du **réseau**

Des exemples : Sekoia.io, Cortex XDR, Sophos

# SOAR : Automatisation & Orchestration

Le SOAR (Security Orchestration, Automation and Response) **automatise** les réponses aux alertes et **orchestre** plusieurs outils.



Il est né ces dernières années en raison de la quantité d'alertes générées par les multiples solutions

Véritable **chef d'orchestre** de l'ensemble des outils de sécurité du SI

Permet une **gestion d'incidents** inter-technos, des **playbooks**, des interconnexions…

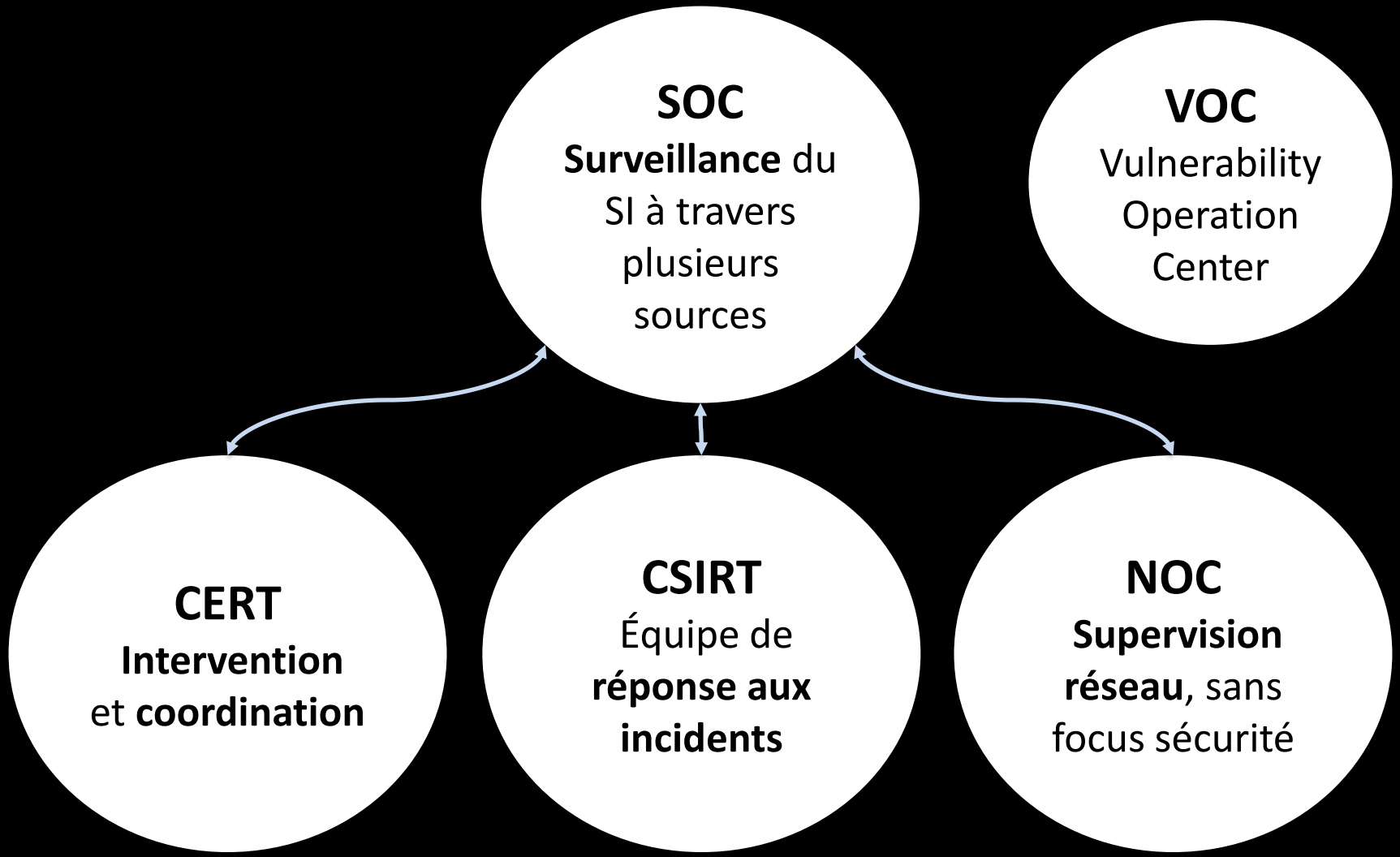
Des exemples : Palo Alto XSOAR, Microsoft Sentinel, FortiSOAR

# Challenges d'un SOC

- Volumétrie des incidents
  - Filtres & Exclusions
  - Risques acceptés
- Criticités des incidents
  - Trop de critiques tuent les critiques
- Classification des incidents
  - Définitions vrais positifs / faux positifs
  - Définition de process

La **connaissance** du SI est primordiale !

# SOC vs CERT, CSIRT, NOC



# Conclusion

Le SOC surveille le(s) SI, analyse les incidents de sécurité et communique efficacement

Il peut être sollicité en réponse à incident en cas de crises…

Et il vise une amélioration continue concernant les règles, playbooks, process…

# Questions