ÉTAT DE L'ART DE L'ACTIVITÉ DE SOC EN 2022

BASÉ SUR LE RÉFÉRENTIEL PDIS

WELAN

PRÉSENTATION

- David Weber
  - Consultant cybersécurité depuis 10 ans
  - Fondateur de la société WELAN
- Audit intrusif (Tests d'intrusion), Audit GRC, Réponse sur Incident
- Accompagnement équipe Blue Team
- Intégration de SIEM
- Auditeur PDIS / Audit de SOC

RÉFÉRENTIELS ANSSI

- L'ANSSI a publié plusieurs référentiels afin de faire qualifier des prestataires / services

- PASSI - Prestataires d'audit de la sécurité des systèmes d'information
- PRIS - Prestataires de réponse aux incidents de sécurité
- PDIS - Prestataires de détection des incidents de sécurité
- SecNumCloud - Prestataires de service d'informatique en nuage
- PAMS - Prestataires d'administration et de maintenance sécurisées
- …

OBJECTIFS DE LA PRÉSENTATION

Comment se construit / se met en place un SOC (Interne ou Externe)

- basé sur le référentiel PDIS.

Cette présentation s'adresse :

- Aux entités qui souhaitent mettre en place SOC (interne ou externe)
- Aux services SOC qui souhaitent se faire qualifier PDIS
- Aux clients qui souhaitent contractualiser auprès d'un service de SOC

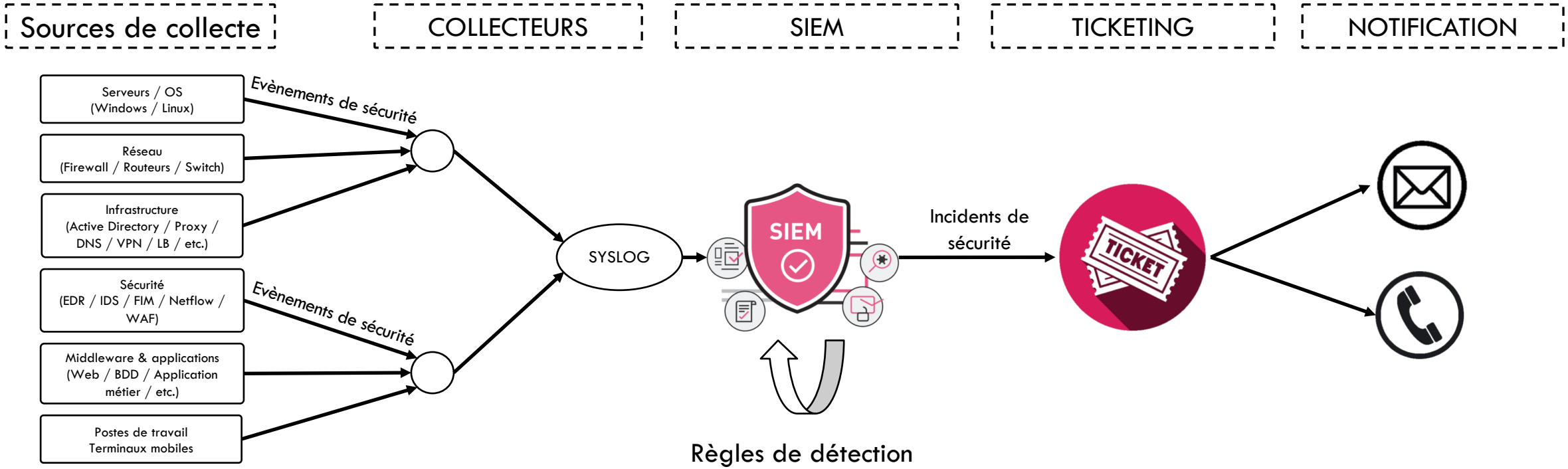
QU'EST-CE QU'UN SECURITY OPERATIONS CENTER ?

- Source: Wikipédia FR
  - Ensemble de Personnes, de Processus et de Technologies
  - Assurer la connaissance de la situation grâce à la détection, au confinement et à l'assainissement des menaces informatiques
  - Le SOC va collecter des informations du SI […] les analyser […] détecter d'éventuelles anomalies […] va permettre d'alerter
  - Les compétences dans ce domaine restent rares […] L'établissement et l'exploitation d'un SOC est coûteux et difficile.
  - Les organisations doivent avoir besoin de bonnes raisons pour le mettre en place.
  - Un SOC va pouvoir permettre à une entreprise d'administrer son réseau informatique à distance et ainsi de réduire les risques

QU'EST-CE QU'UN SECURITY OPERATIONS CENTER ?

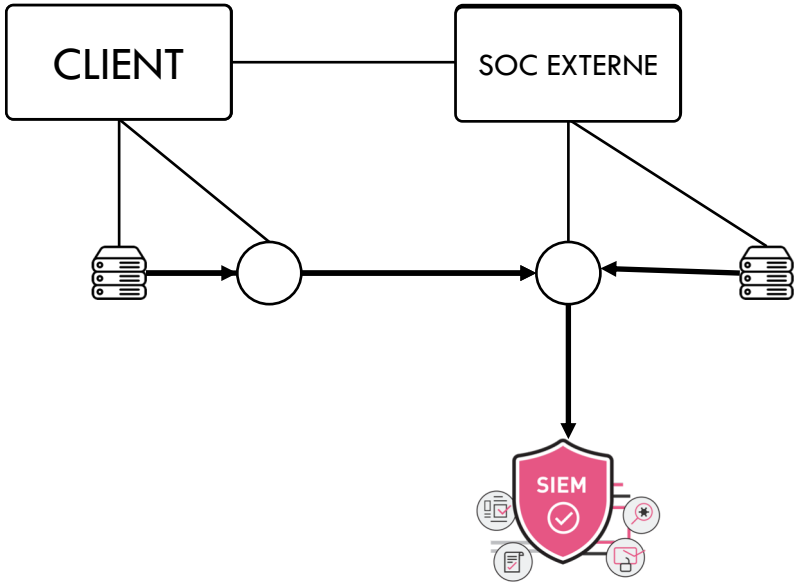
- Ensemble de Ressources Humaines, de Procédures et de Technologies
- Collecte d'évènements de sécurité
- La corrélation et l'analyse des évènements de sécurité
  - Transformation « évènements de sécurité » en « incidents de sécurité potentiels »
- La qualification des incidents de sécurité
- Remontée d'alertes

TERMINOLOGIE & ARCHITECTURE DE COLLECTE



CONSTRUCTION DU SERVICE

- Positionnement des collecteurs
  - Acheminer les évènements jusqu'au service de supervision
  - Relais du SIEM (ex: Splunk Forwarder ou WinLogBeat) ou serveur SYSLOG



CONSTRUCTION DU SERVICE

- Positionnement des collecteurs
  - Acheminer les évènements jusqu'au service de supervision
  - Relais du SIEM (ex: Splunk Forwarder ou WinLogBeat) ou serveur SYSLOG
- Coupure réseau / Congestion
  - Privilégier les protocoles connectés (i.e. TCP et non UDP)
  - Configurer les collecteurs avec un stockage local en cas de coupure réseau
- Différences entre les environnements (ex: gap sécurité, ownership, gouvernance, etc.)
- Mettre en place du chiffrement si non maitrise des équipements traversés par les journaux
- Durcissement des collecteurs / serveur(s) SYSLOG
  - Restriction de droits / Incompatibilité de droits
  - Sortir ces équipements de l'Active Directory

CONSTRUCTION DU SERVICE

- Définir les sources de collecte
  - /!\ Inventaire du périmètre à superviser
- Définir les évènements à collecter par source

Stratégie de Collecte

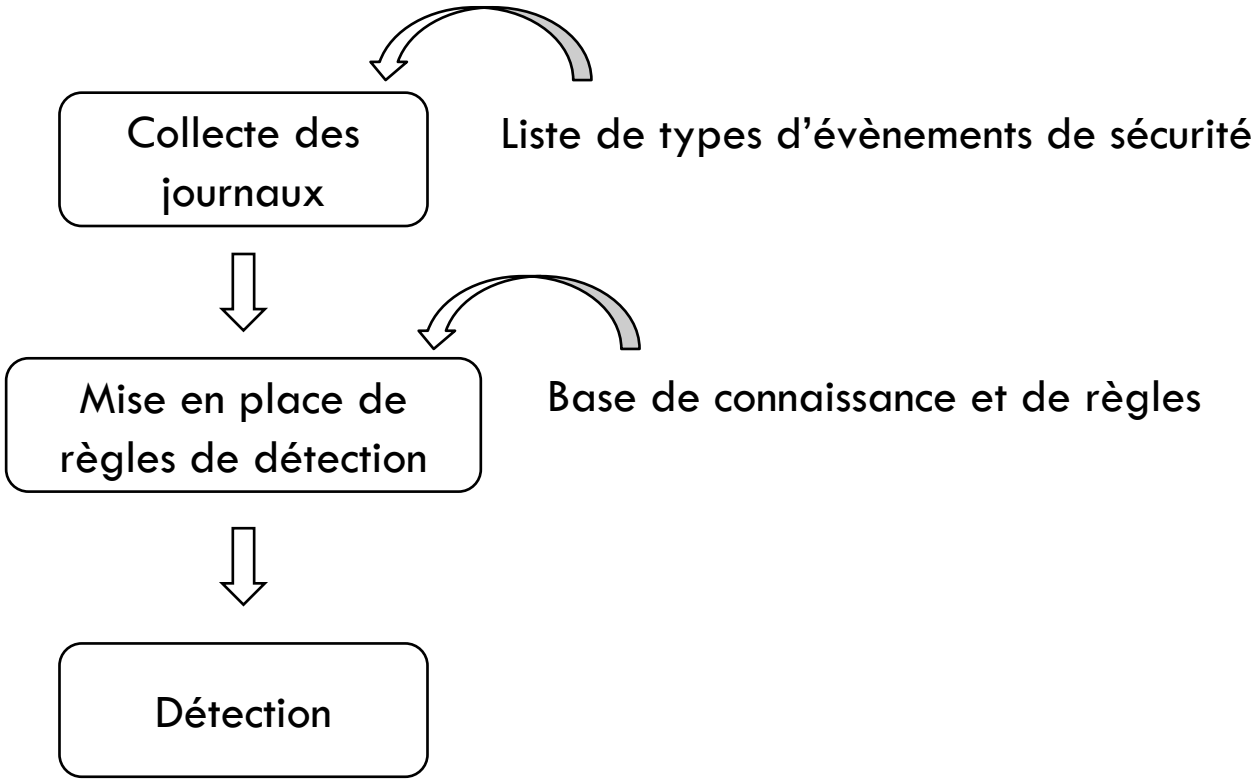
- Définir les incidents de sécurité à détecter et les règles associées
- Définir la méthode de qualification des incidents de sécurité

Stratégie d'Analyse

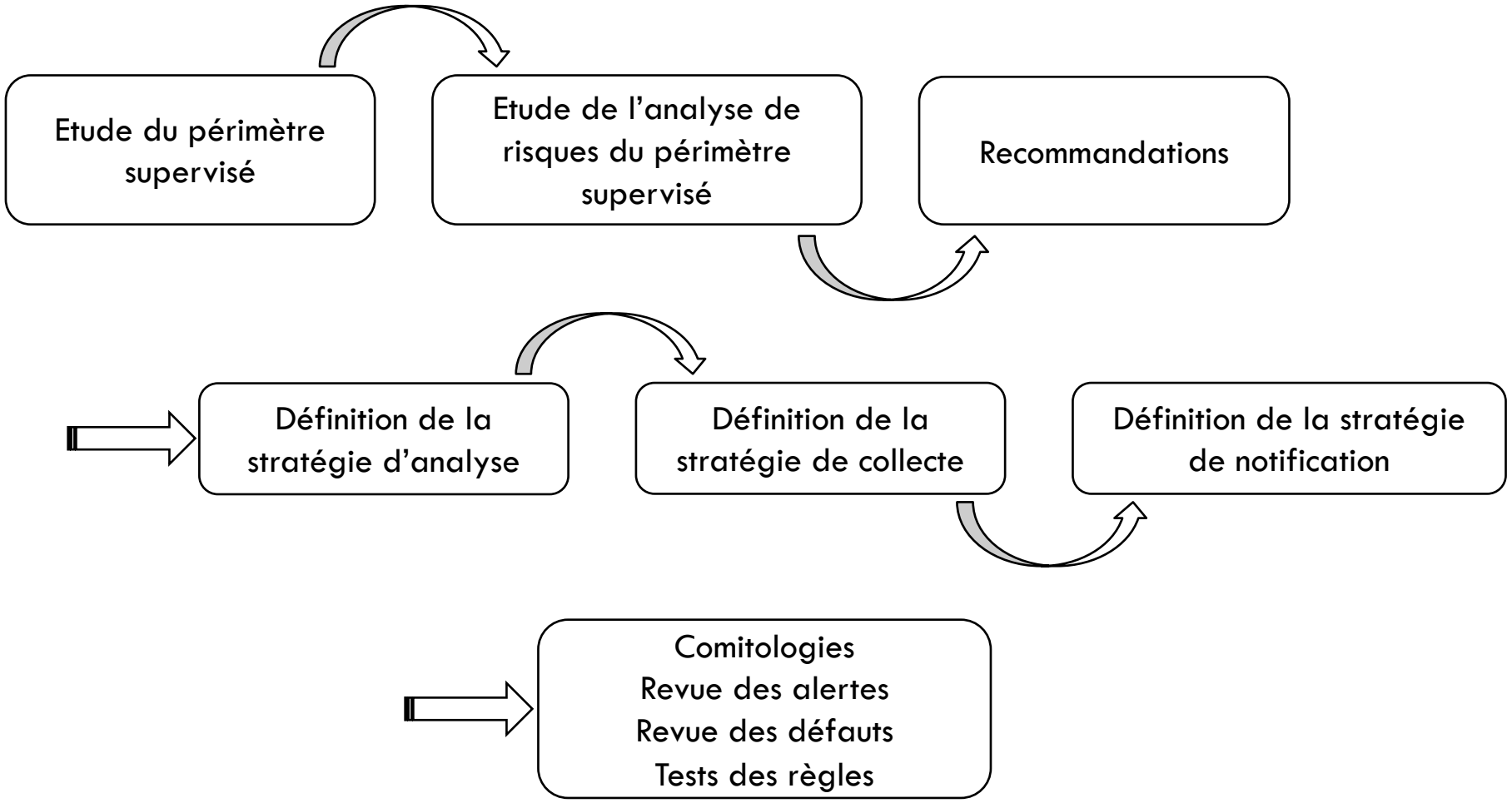
- Définir les procédures de remontée d'alertes
  - Tickets / mails / téléphones / SMS / etc.

Stratégie de Notification

LE BON SOC ET LE MAUVAIS SOC



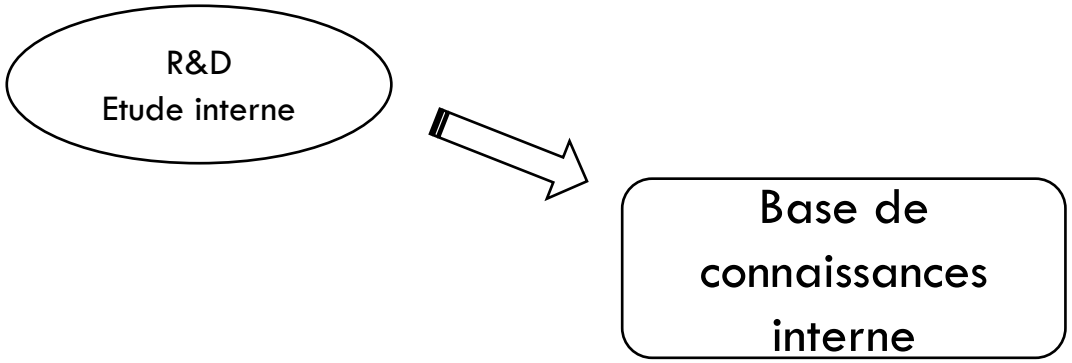
LE BON SOC ET LE MAUVAIS SOC



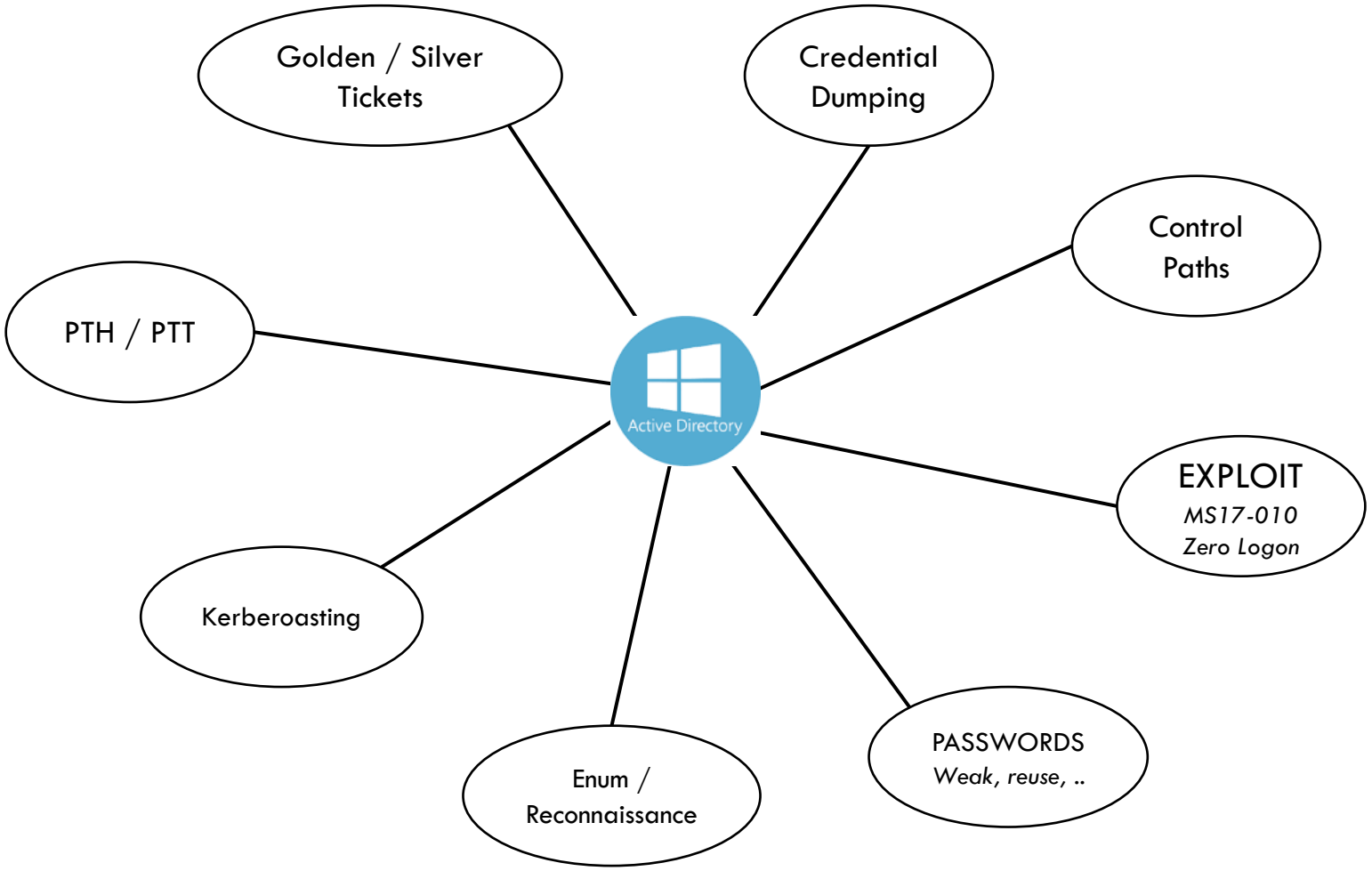
LE SOC EST LE GARANT DE LA **CAPACITÉ** ET DE LA **QUALITÉ** DE DÉTECTION

LA CAPACITÉ ET LA QUALITÉ DE LA DÉTECTION DÉPENDENT DE LA CAPACITÉ DU CLIENT À **IMPLÉMENTER LES RECOMMANDATIONS** ET **CORRIGER LES DÉFAUTS**

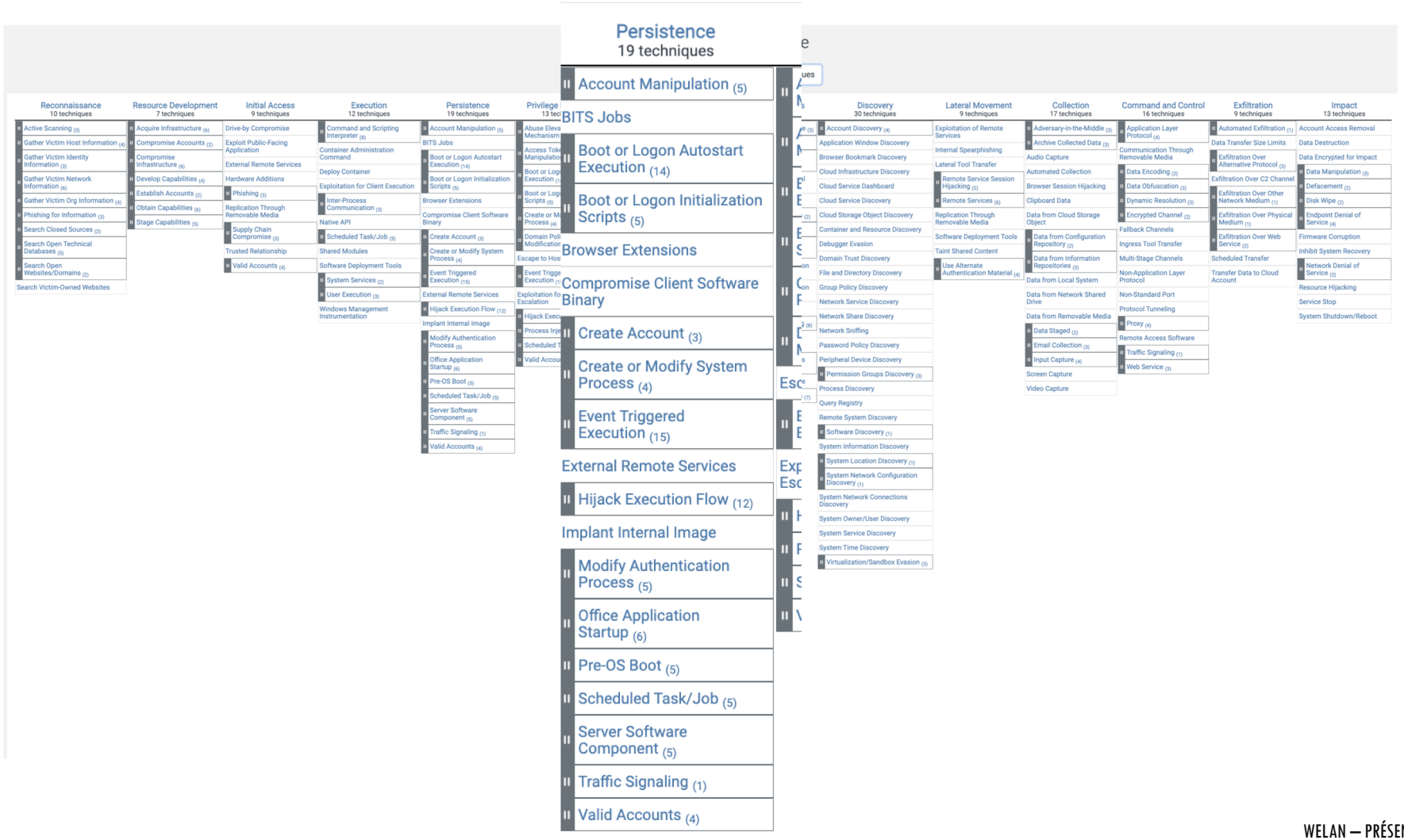
LA STRATÉGIE D'ANALYSE



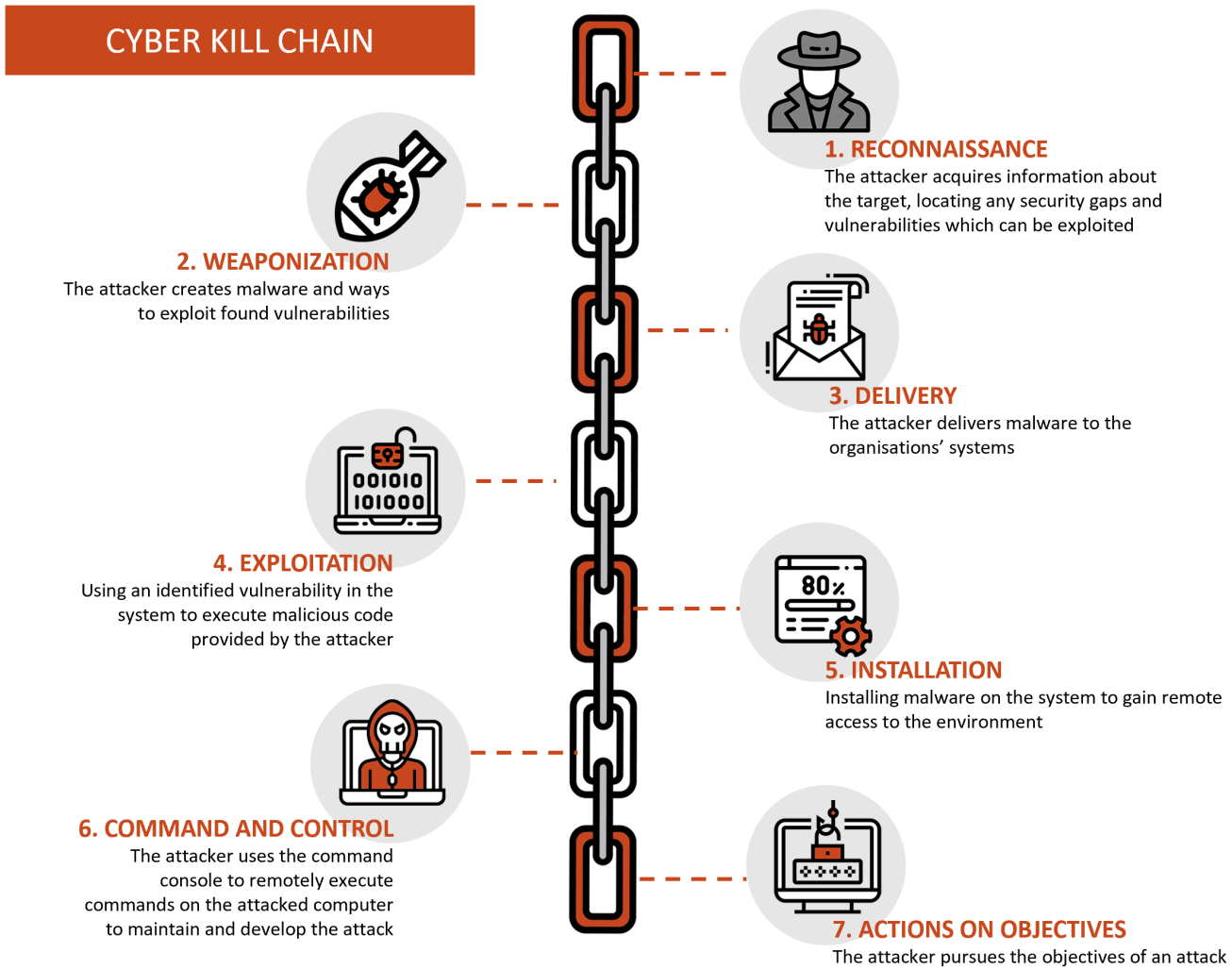
COUVRIR LES ATTAQUES DES SOURCES SUPERVISÉES



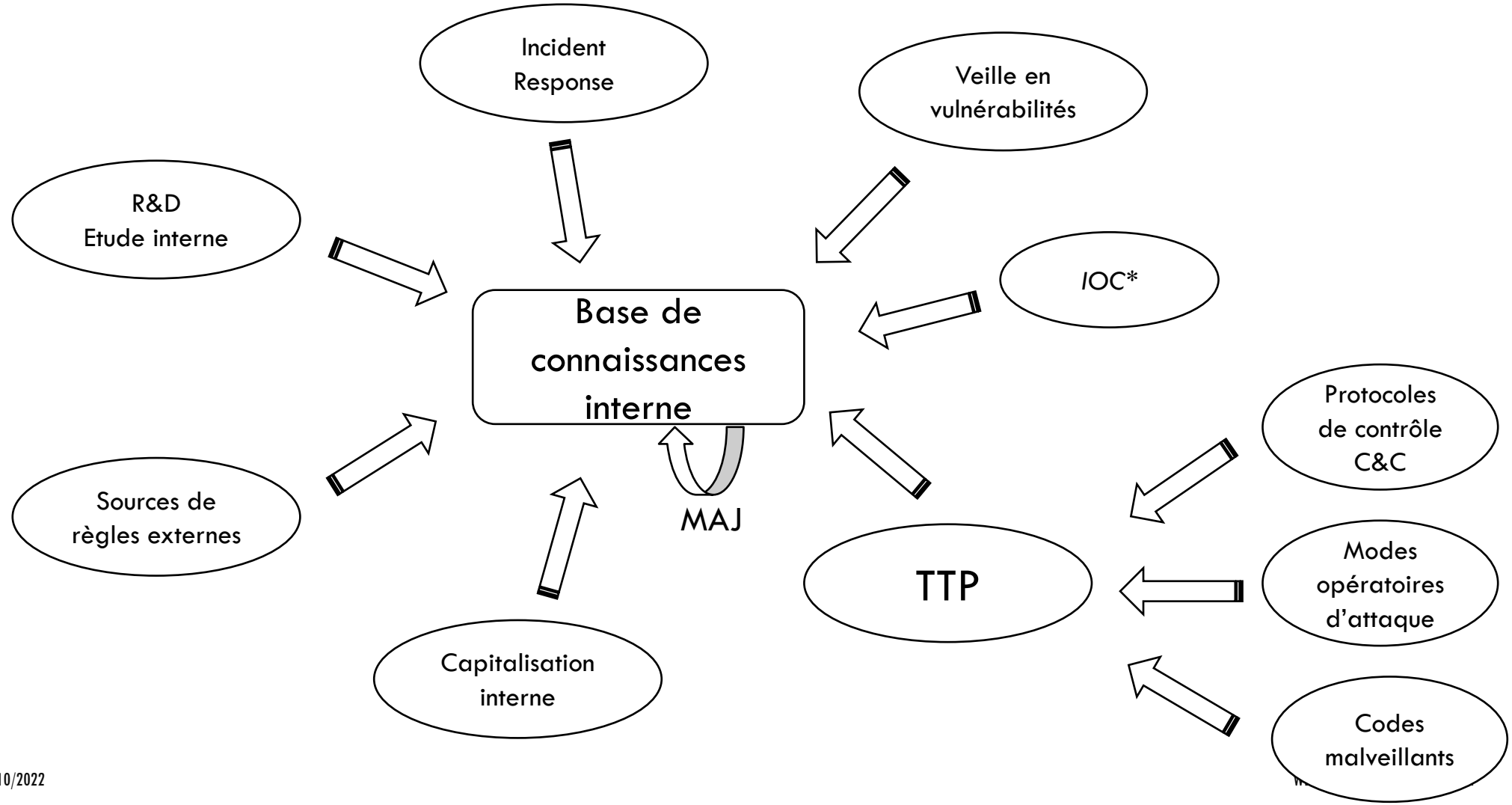
MITRE ATT&CK


Persistence
19 techniques
Account Manipulation (5)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (15)
External Remote Services
Hijack Execution Flow (12)
Implant Internal Image
Modify Authentication Process (5)
Office Application Startup (6)
Pre-OS Boot (5)
Scheduled Task/Job (5)
Server Software Component (5)
Traffic Signaling (1)
Valid Accounts (4)
Reconnaissance
10 techniques
Resource Development
7 techniques
Initial Access
9 techniques
Execution
12 techniques
Persistence
19 techniques
Discovery
30 techniques
Lateral Movement
9 techniques
Collection
17 techniques
Command and Control
16 techniques
Exfiltration
9 techniques
Impact
13 techniques

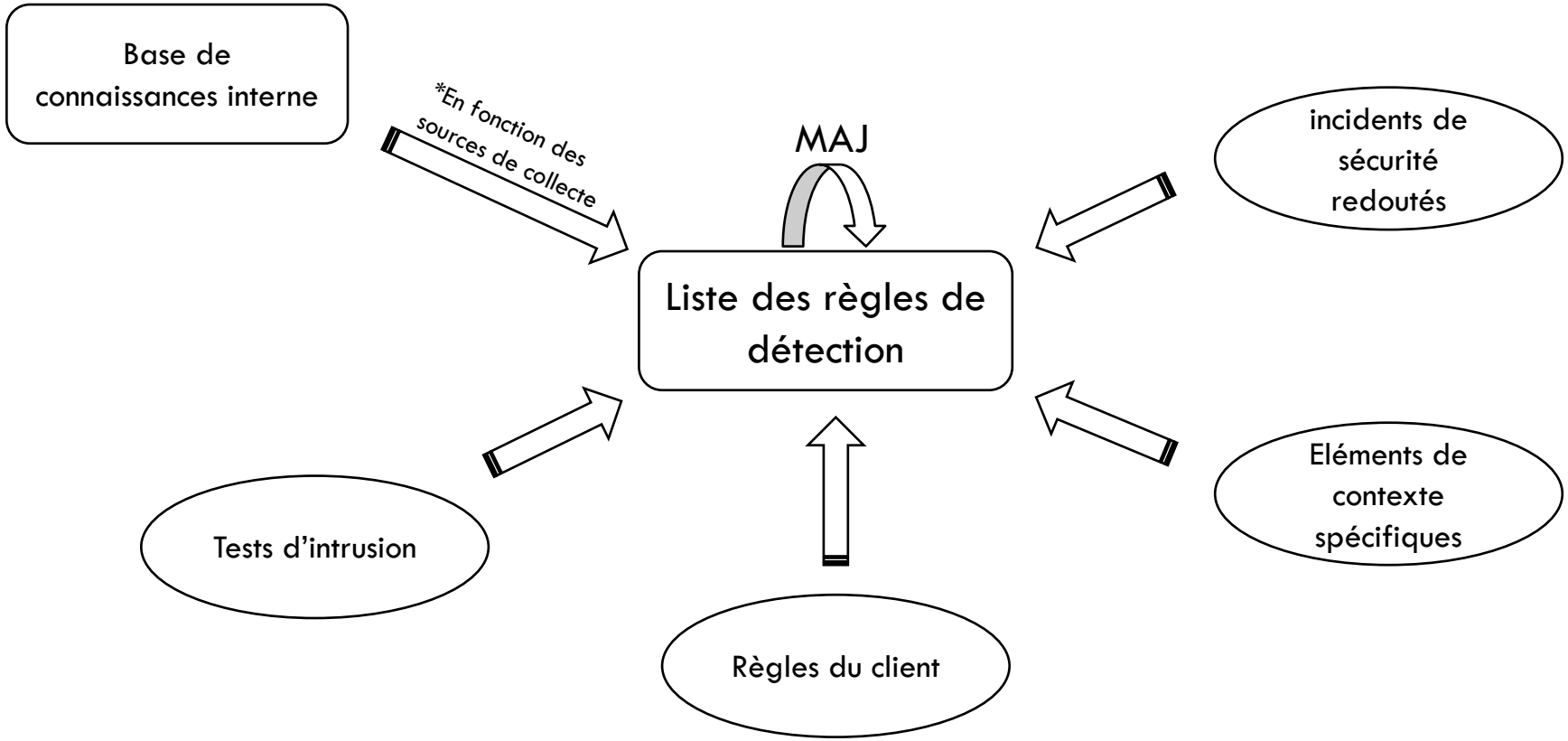
CYBER KILL CHAIN



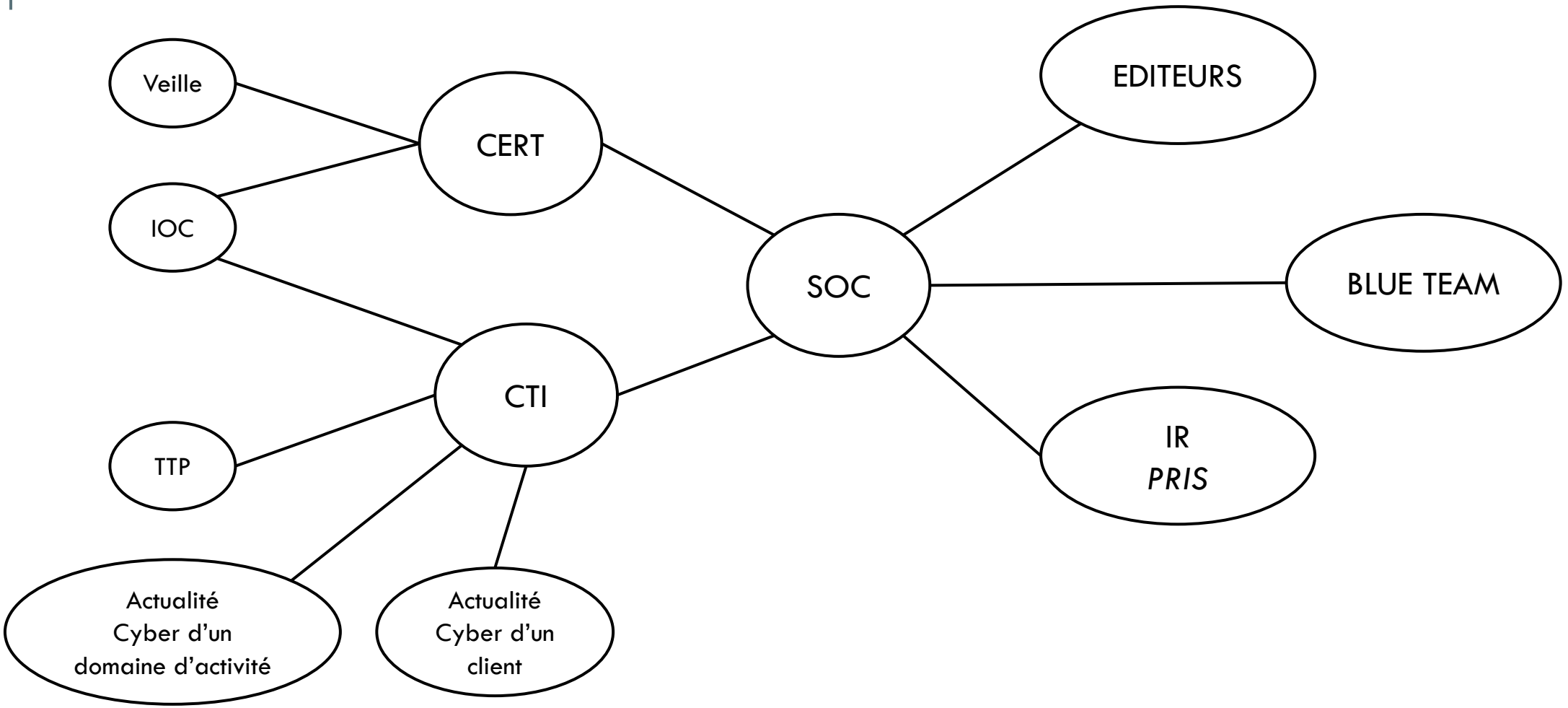
LA STRATÉGIE D'ANALYSE



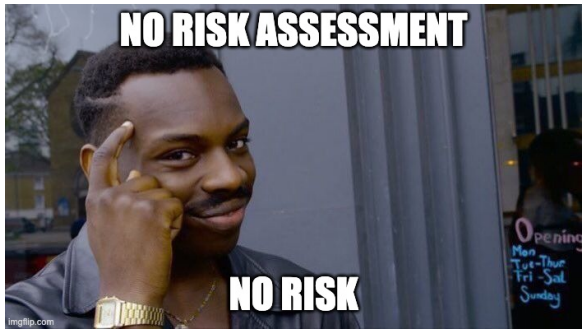
LA STRATÉGIE D'ANALYSE



RELATION AVEC LES TIERS



ANALYSE DE RISQUES ET INCIDENTS REDOUTÉS

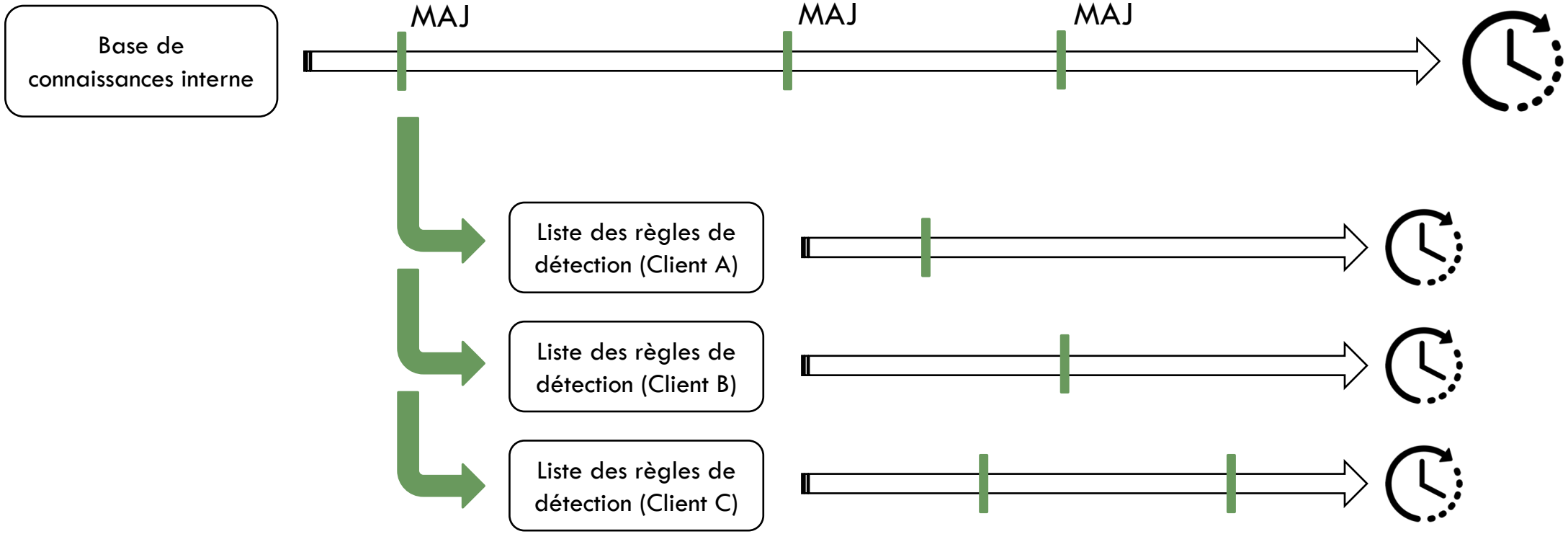


- Analyse de risques existante ?
- Analyse de risques à jour ?
- Analyse propre au contexte du périmètre supervisé ?
- Risques pertinents ?

- Risque résiduel = Risque brut x Mesures d'atténuation

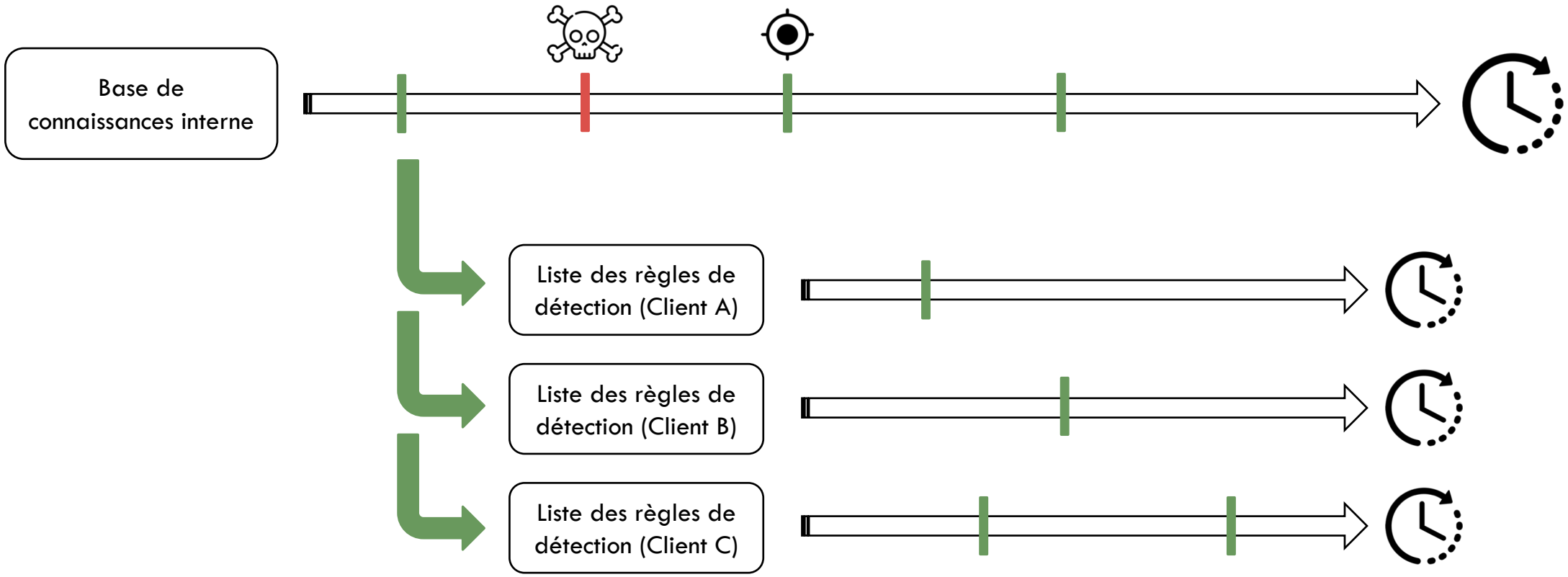
Préventive
Détective
Corrective
Dissuasive
Reprise
Compensatoire

HISTORISATION DE L'IMPLÉMENTATION DES RÈGLES DE DÉTECTION



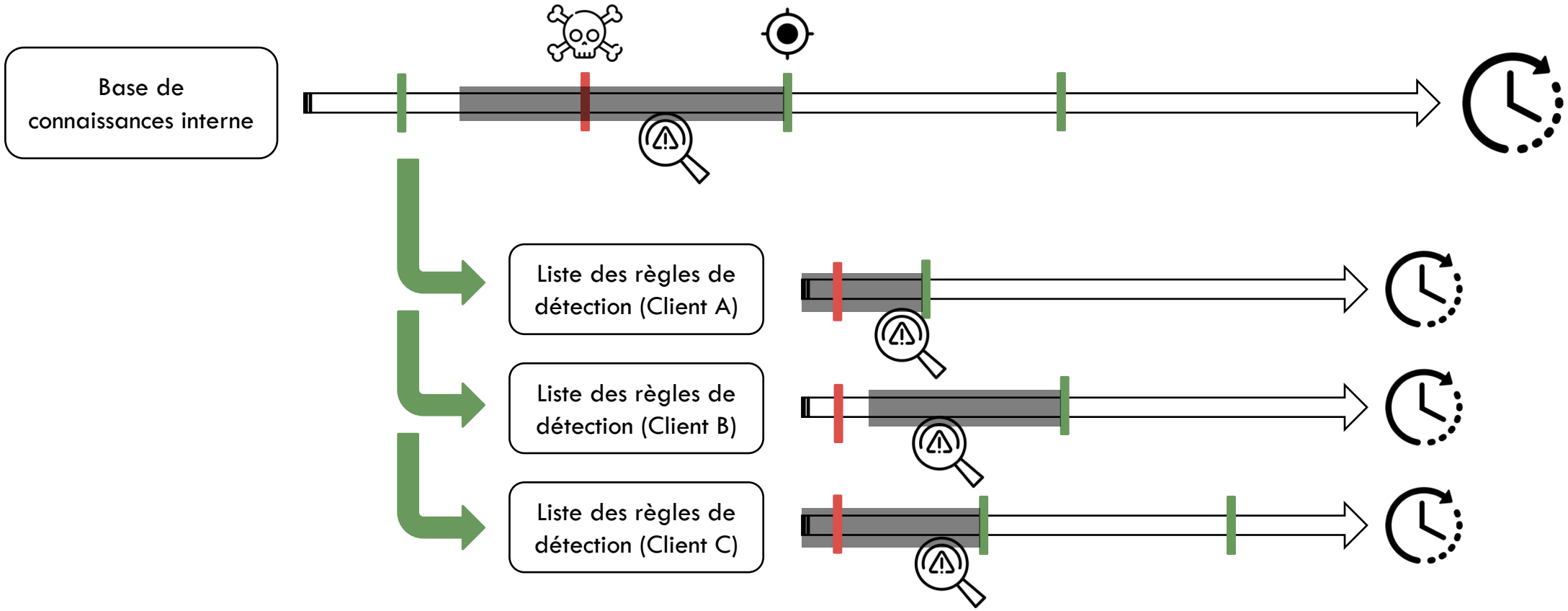
LE SOC DOIT POUVOIR DÉTERMINER CE QU'IL ÉTAIT EN MESURE DE DÉTECTER À UN **INSTANT T**

HISTORISATION DE L'IMPLÉMENTATION DES RÈGLES DE DÉTECTION



LE SOC DOIT ÊTRE EN MESURE D'EFFECTUER DES RECHERCHES **A POSTERIORI**

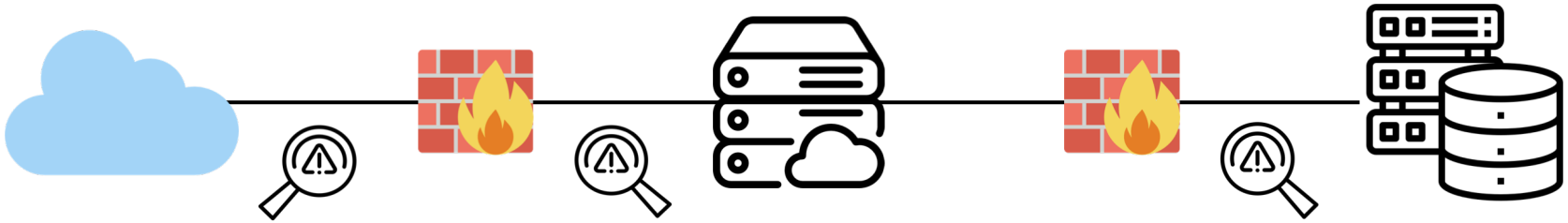
HISTORISATION DE L'IMPLÉMENTATION DES RÈGLES DE DÉTECTION



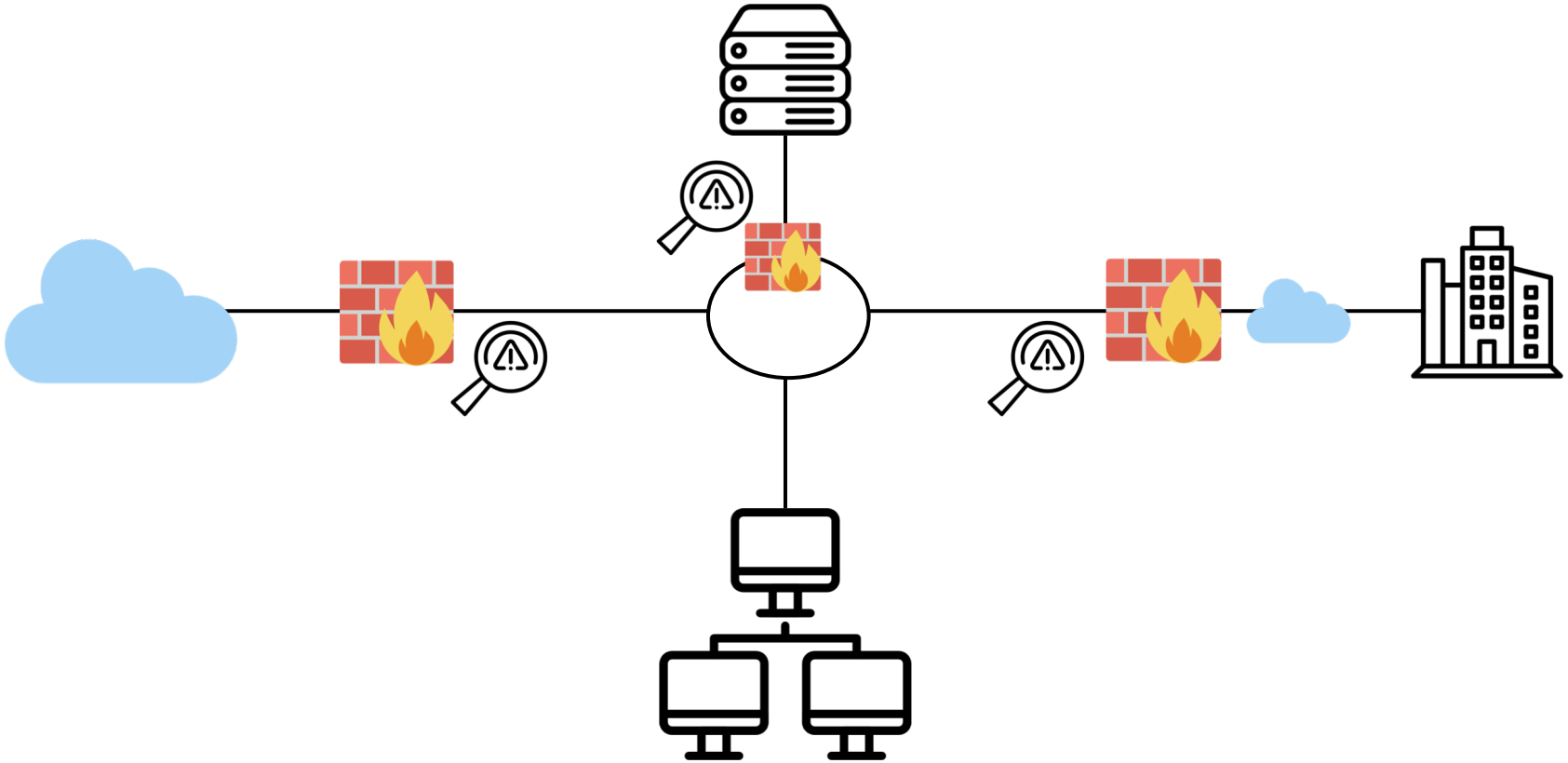
RECOMMANDATIONS

- Configuration des sources de collecte
- Sonde réseau
  - IDS / IPS
  - Point de collecte pour analyse (Zeek)
- Installation d'outils complémentaires
  - SYSMON
  - MDI* pour AD
  - Sentinel pour Azure / GuardDuty pour AWS
- Honeypot
  - Système
  - Données (BDD / Comptes)

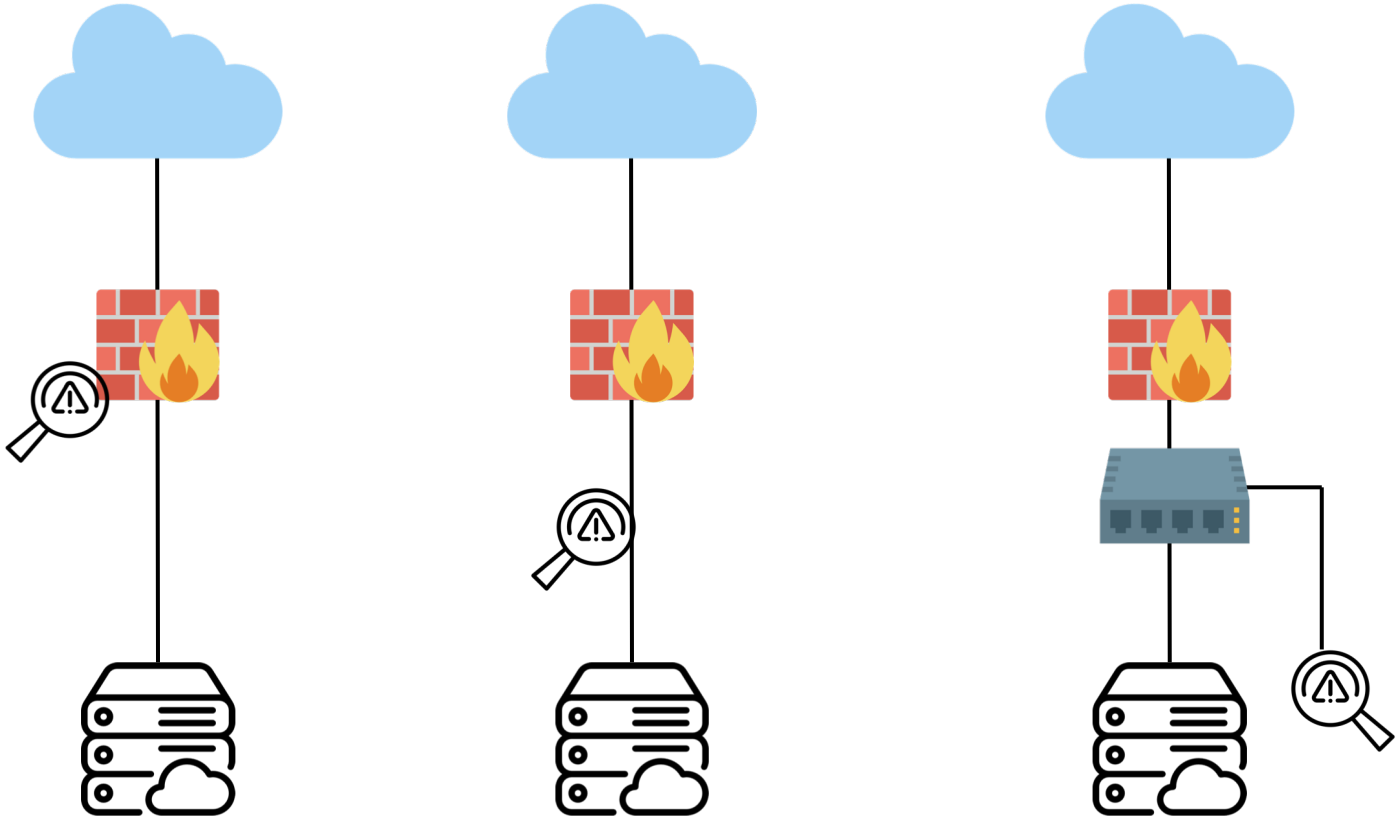
SONDES DE DÉTECTION RÉSEAU (IDS / IPS)

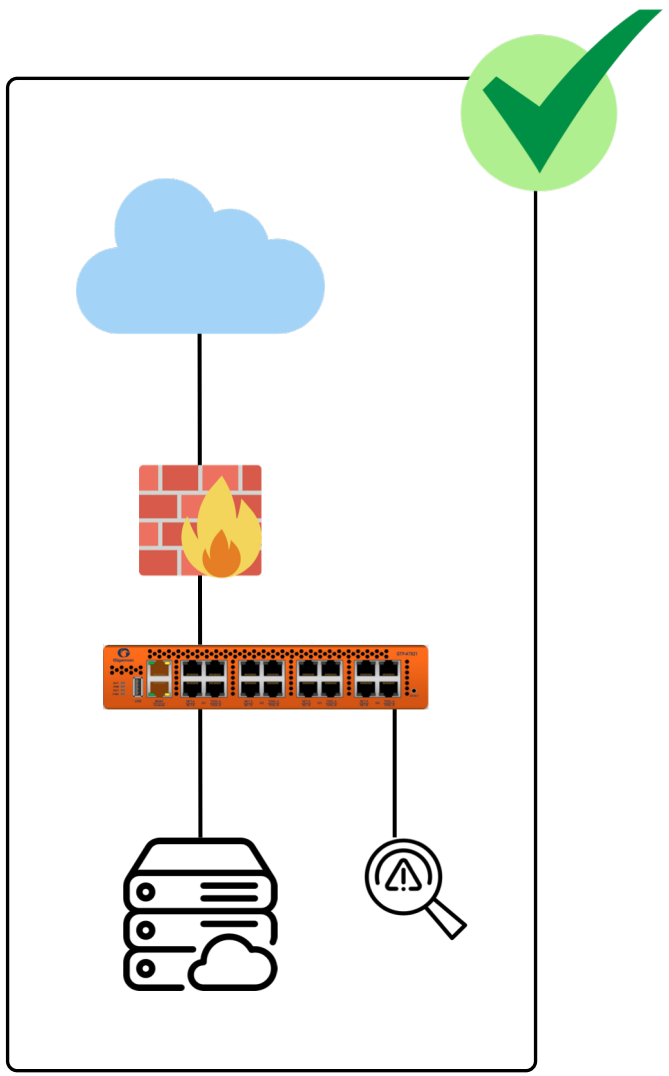


SONDES DE DÉTECTION RÉSEAU (IDS / IPS)



SONDES DE DÉTECTION RÉSEAU (IDS / IPS)





LES INDICATEURS DE COMPROMISSION (IOC)

- Fichiers
  - Empreinte (MD5, SHA1, SHA256), Nom, Empreinte du nom, Chemin d'accès, Extension, …
- Adresses IP publiques
- Nom de domaines
- URL
- User-agent
- Champs d'emails
  - domaine source, domaine destination, empreinte du sujet
- Champs de certificats *X509*

LES INDICATEURS DE COMPROMISSION (IOC)

- Où chercher ?
  - Log Proxy
  - Log Serveur Web
  - Log Firewall / Données Netflow
  - Log DNS

- Et les champs des certificats *X509* ?
- Et les empreintes de fichiers ?

- Hors déploiement d'un outil de Hunting

LES INDICATEURS DE COMPROMISSION (IOC)

- Agent Système
  - SYSMON

- Sonde de collecte réseau (ex: Zeek)
  - Extraction d'artefacts des protocoles réseau
    - Nom de domaine
    - User-Agent
    - Domaines
    - Fichiers transférés
    - Champs X509

QUID DE L'ENVIRONNEMENT SUPERVISÉ

LA CAPACITÉ ET LA QUALITÉ DE LA DÉTECTION DÉPENDENT

DU NIVEAU DE MATURITÉ DU CLIENT

BONNES PRATIQUES QUI FACILITENT LA DÉTECTION

- Filtrage de flux
  - Flux d'administration depuis des serveurs / réseau d'administration
  - Flux BDD depuis serveurs identifiés
- Nomenclature de nommage des objets
  - Compte, groupe, computer, OU, GPO, fichiers/répertoires, Shares, etc.
- Architecture de délégation de droits / administration
- Gestion du changement
  - Ex: Pas de changement (structurant) sans ticket

BONNES PRATIQUES QUI FACILITENT LA DÉTECTION

- Usage d'un serveur mandataire
  - Surveillance des tentatives de contournement
  - Identification de flux suspects
- Deny-All par défaut des flux en sortie
  - Identification de flux non légitimes
- Serveur DNS interne
  - Exfiltration de données via un tunnel DNS
  - Egalement applicable à l'ICMP
- Désactivation des protocoles et services obsolètes

BONNES PRATIQUES QUI FACILITENT LA DÉTECTION

- Durcissement des systèmes
  - Restriction des droits d'administration
  - Whitelist des applications qui peuvent s'exécuter sur un système (AppArmor, AppLocker / SRP)
- Désactivation des modules / services inutiles sur les systèmes
- Uniformisation des mesures de sécurité
  - Solution EDR homogène et actif partout
  - Mécanisme de journalisation et de centralisation des journaux
  - Service de sauvegarde

RECHERCHES EN SOURCES OUVERTES

- Les services en source ouverte peuvent donner des informations sur les données recherchées
  - Hash sur VirusTotal => VT révèle la date de dernière recherche
- Peuvent donner des informations aux attaquants
- Privilégier les sources internes
  - Bases *RIPE*, plateformes antivirales hors ligne, bases de résolution DNS
  - Plateforme d'analyse dynamique de malware

GESTION DU TEMPS

- Synchronisation NTP
  - QUID de la synchronisation des collecteurs des SOC externes
- UTC vs GMT
  - Ok pour les journaux des principaux systèmes (UTC)
  - /!\ Journaux applicatifs
- Règles de détection basées sur le temps
  - Prendre en compte le décalage horaire

MERCI

david.weber@welan.fr