LinuXMaine.org

CYBERSÉCURITÉ DÉFENSIVE

SIEM · XDR · EDR
IDS / IPS & Sondes

Comprendre, choisir et déployer les technologies
de détection et de réponse aux menaces

Snort · Suricata · Zeek · Wazuh · OSSEC · Elastic · Splunk · Sentinel

Auteur : LinuXMaine.org

Guide technique — technologies, licences, rôles, sites officiels, installation, lexique, bibliographie

Édition du 4 juin 2026

À propos de ce document

Ce guide présente de façon technique et synthétique l'écosystème de la **cybersécurité défensive** : la collecte et la corrélation des journaux (**SIEM**), la détection et la réponse sur les postes (**EDR**), sur le réseau (**NDR**) et de façon unifiée (**XDR**), ainsi que les systèmes de **détection/prévention d'intrusion** (IDS/IPS) tels que Snort, Suricata ou Zeek. Pour chaque famille : rôle, fonctionnement, principales solutions (open source et commerciales), **licences**, **sites officiels**, **modes d'installation**, et — pour les SIEM — le **déploiement des sondes**. Le document se termine par un **lexique**, une **bibliographie en français** et une liste de **liens utiles**.

Cadre légal et éthique

Les techniques et outils décrits relèvent de la **sécurité défensive** et de l'administration de systèmes que vous êtes autorisé à surveiller. La capture de trafic, l'installation de sondes et la collecte de journaux doivent respecter le **RGPD**, le droit du travail et les politiques internes (information des utilisateurs, proportionnalité, durée de conservation). N'auditez ou ne surveillez que des systèmes vous appartenant ou pour lesquels vous disposez d'une autorisation écrite.

Table des matières

1 Introduction : la défense en profondeur et le SOC **4**
- 1.1 Le SOC : centre des opérations de sécurité . . . 4
- 1.2 Comprendre l'attaquant : Kill Chain et MITRE ATT&CK . . . 5

2 Les SIEM : corrélation et supervision des journaux **7**
- 2.1 Rôle et fonctionnement . . . 7
  - 2.1.1 Les huit étapes de la chaîne SIEM . . . 7
- 2.2 Panorama des solutions SIEM . . . 7
- 2.3 Étude de cas : architecture et installation de Wazuh . . . 8
  - 2.3.1 Les trois composants centraux . . . 9
  - 2.3.2 Installation « tout-en-un » du serveur (assistant officiel) . . . 9
  - 2.3.3 Déploiement des sondes : les agents Wazuh . . . 9
- 2.4 Les sondes d'un SIEM : comment collecter . . . 9
  - 2.4.1 Exemple : centraliser des journaux via syslog (rsyslog) . . . 10
- 2.5 La stack Elastic (ELK) comme socle SIEM . . . 10

3 Les EDR : détection et réponse sur les postes **11**
- 3.1 Antivirus (EPP) vs EDR . . . 11
- 3.2 Ce que permet un EDR . . . 11
- 3.3 Panorama des solutions EDR . . . 11
- 3.4 Installer un EDR open source : OSQuery + Velociraptor . . . 12

4 Les XDR : détection et réponse étendues **13**
- 4.1 SIEM, EDR, NDR, XDR, MDR : comment se situer . . . 13
- 4.2 Panorama des solutions XDR . . . 14

5 IDS / IPS : détection et prévention d'intrusion **15**
- 5.1 NIDS vs HIDS, et placement dans le réseau . . . 15
- 5.2 Méthodes de détection . . . 16
- 5.3 Anatomie d'une règle Snort . . . 16
- 5.4 Panorama des IDS/IPS . . . 16
- 5.5 Installer et exécuter Suricata (NIDS) . . . 17
- 5.6 Installer Snort 3 . . . 17

6 NDR et sondes réseau **18**
- 6.1 Capturer le trafic : TAP, SPAN et NetFlow . . . 18
- 6.2 Outils NDR / NSM open source . . . 19
- 6.3 Déployer une sonde Zeek . . . 19

7 Synthèse comparative **20**
- 7.1 Quelle solution pour quel besoin ? . . . 20

8 Lexique **21**

9 Bibliographie en français **22**

10 Liens utiles **23**
- 10.1 Sites officiels des solutions . . . 23
- 10.2 Référentiels, organismes et ressources . . . 23

Table des figures

1.1 Le modèle de défense en profondeur : chaque anneau ajoute un type de protection et de visibilité. . . . 4
1.2 Architecture type d'un SOC : les sources alimentent les sondes/collecteurs, qui alimentent le SIEM ; les analystes exploitent les alertes et déclenchent la réponse (manuelle ou via SOAR). . . . 5
1.4 Les sept étapes de la Cyber Kill Chain. . . . 5
1.5 La pyramide de la douleur : plus on détecte haut, plus on gêne durablement l'attaquant. 6

2.1 Chaîne de traitement d'un SIEM, de la collecte brute jusqu'à la réponse. . . . 7
2.2 Architecture de Wazuh : agents et sources syslog → serveur (analyse) → indexer (stockage) → dashboard. . . . 8
2.3 Stack Elastic : Beats/Logstash → Elasticsearch → Kibana (application SIEM). . . . 10

3.1 Architecture d'un EDR : télémétrie des endpoints → moteur de détection → console → réponse/remédiation. . . . 11

4.1 Le XDR fédère plusieurs sources de signaux et corrèle entre domaines avant de présenter un incident unifié. . . . 13

5.1 Placement type : IPS en coupure derrière le pare-feu, NIDS en écoute passive sur un TAP/SPAN, HIDS sur les hôtes. . . . 15
5.2 Chaîne de traitement d'un moteur de type Snort/Suricata, de la capture des paquets à la sortie (alerte ou *drop*). . . . 16

6.1 Trois méthodes d'alimentation d'une sonde : TAP physique, port SPAN/mirror, et export NetFlow/IPFIX. . . . 18

Chapitre 1

Introduction : la défense en profondeur et le SOC

La cybersécurité défensive ne repose pas sur un produit unique mais sur un empilement de couches complémentaires — c'est le principe de *défense en profondeur*. Aucune barrière n'étant infaillible, on multiplie les points de détection et de contrôle pour qu'un attaquant ayant franchi une couche soit arrêté ou repéré à la suivante.

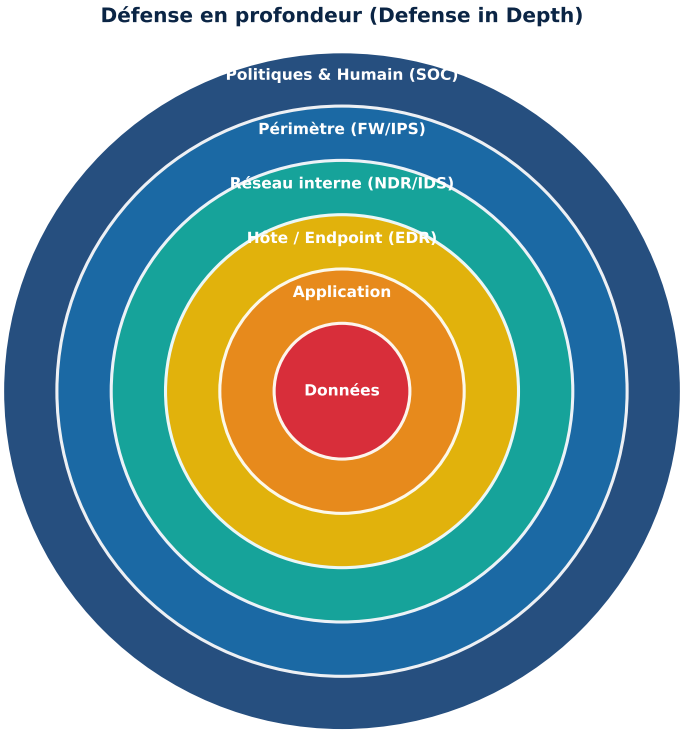

Figure 1.1: *Le modèle de défense en profondeur : chaque anneau ajoute un type de protection et de visibilité.*

1.1 Le SOC : centre des opérations de sécurité

Le **SOC** (*Security Operations Center*) est l'équipe — et la plateforme — chargée de surveiller, détecter, analyser et répondre aux incidents de sécurité, idéalement 24h/24. Il s'appuie sur des outils (SIEM, EDR, XDR, IDS…) et sur des analystes organisés par niveaux (N1 tri des alertes, N2 investigation, N3 *threat hunting* et forensic).

Les grandes missions d'un SOC :

- **Prévention** : durcissement, gestion des vulnérabilités.
- **Détection** : corrélation d'événements, signatures, anomalies.
- **Investigation** : qualification, analyse de la portée.

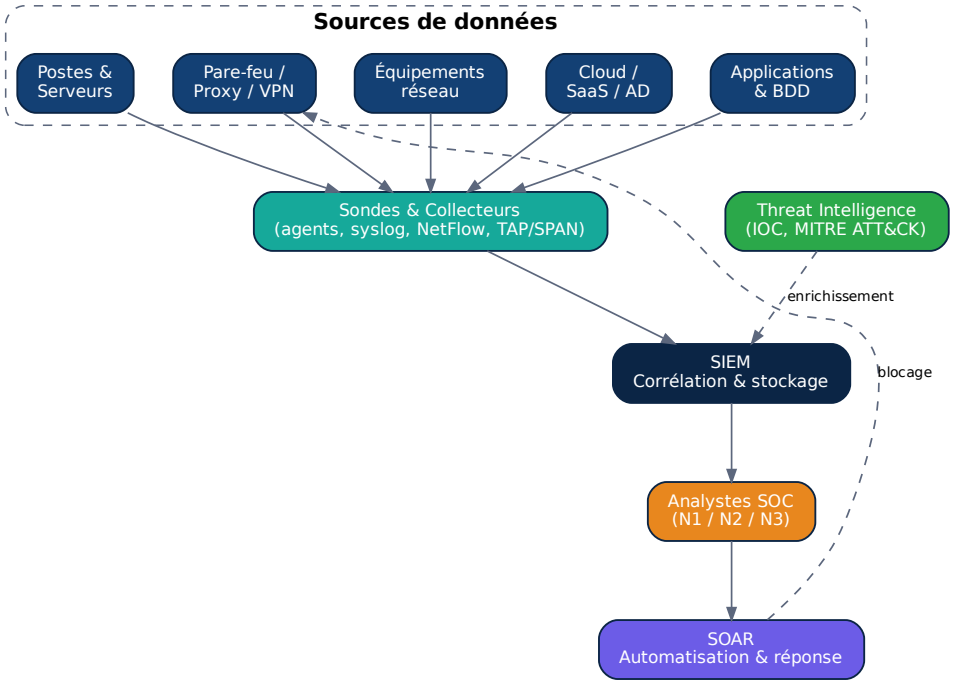

Figure 1.2: *Architecture type d'un SOC : les sources alimentent les sondes/collecteurs, qui alimentent le SIEM ; les analystes exploitent les alertes et déclenchent la réponse (manuelle ou via SOAR).*

- **Réponse** : confinement, éradication, remédiation.
- **Conformité** : journalisation, audits, reporting (PCI-DSS, ISO 27001, RGPD, NIS2).

1.2 Comprendre l'attaquant : Kill Chain et MITRE ATT&CK

Pour détecter efficacement, on modélise le déroulement d'une attaque. La **Cyber Kill Chain** de Lockheed Martin décompose une intrusion en étapes ; plus on détecte tôt, plus la remédiation est simple et peu coûteuse.

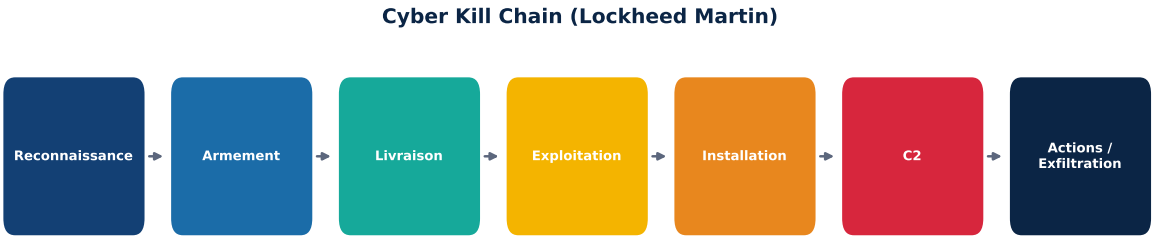

Figure 1.4: *Les sept étapes de la Cyber Kill Chain.*

Le référentiel **MITRE ATT&CK** complète ce modèle en cataloguant les *tactiques* (objectifs) et *techniques* (moyens) réellement observés. La **pyramide de la douleur** (*Pyramid of Pain*) illustre quant à elle qu'il est bien plus pénalisant pour un attaquant de devoir changer ses *TTP* (tactiques, techniques et procédures) que de changer une simple adresse IP : c'est pourquoi les outils modernes (EDR/XDR) cherchent à détecter les *comportements* plutôt que de simples indicateurs.

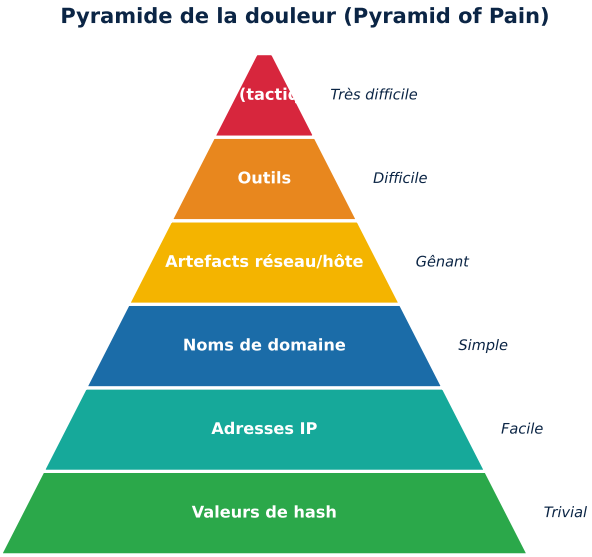

Figure 1.5: *La pyramide de la douleur : plus on détecte haut, plus on gêne durablement l'attaquant.*

IOC vs comportement

Un **IOC** (*Indicator of Compromise*) est un artefact ponctuel : hash, IP, domaine, URL. Facile à contourner. Une **TTP** décrit une manière d'agir (ex. « persistance via tâche planifiée »), bien plus stable et donc plus précieuse à détecter.

Chapitre 2

Les SIEM : corrélation et supervision des journaux

SIEM

Un **SIEM** (*Security Information and Event Management*) centralise les **journaux** et événements de tout le système d'information, les **normalise**, les **corrèle** pour détecter des scénarios d'attaque, et fournit **alertes**, tableaux de bord et rapports de conformité. C'est la « tour de contrôle » du SOC. Il combine historiquement le *SIM* (gestion de l'information de sécurité, archivage/analyse) et le *SEM* (gestion des événements, temps réel).

2.1 Rôle et fonctionnement

Le SIEM répond à trois besoins : **visibilité** (tout voir au même endroit), **détection** (corréler ce qui, pris isolément, paraît anodin) et **conformité** (conserver et prouver). Une règle de corrélation typique : « 10 échecs d'authentification suivis d'un succès depuis la même IP, puis une connexion VPN depuis un pays inhabituel » déclenche une alerte alors que chaque événement isolé serait ignoré.

Figure 2.1: *Chaîne de traitement d'un SIEM, de la collecte brute jusqu'à la réponse.*

2.1.1 Les huit étapes de la chaîne SIEM

1. **Collecte** : agents, syslog, API, Beats, NetFlow, WMI/WEF.
2. **Normalisation / parsing** : mise au format commun (ex. ECS, CEF, LEEF).
3. **Enrichissement** : GeoIP, *threat intelligence*, inventaire (CMDB).
4. **Indexation / stockage** : moteur de recherche, rétention « chaude/froide ».
5. **Corrélation** : règles, séquences, seuils, listes de référence.
6. **Détection** : alertes, scoring de risque, UEBA (analyse comportementale).
7. **Restitution** : tableaux de bord, recherche, rapports de conformité.
8. **Réponse** : intégration SOAR, tickets, actions automatiques.

2.2 Panorama des solutions SIEM

Solution	Licence	Type	Site officiel
Wazuh	GPLv2 (open source)	SIEM + XDR + HIDS	https://wazuh.com
Elastic SIEM	Elastic License / parties open	SIEM sur stack ELK	https://www.elastic.co/security

Solution	Licence	Type	Site officiel
Security Onion	GPL / Elastic (open)	Distribution SIEM+NSM	https://securityonionsolutions.com
Graylog	SSPL / GPL (Open) + Enterprise	Gestion de logs / SIEM	https://graylog.org
OSSIM (AlienVault)	GPL (open source)	SIEM unifié (USM)	https://cybersecurity.att.com/products/ossim
Splunk Enterprise Security	Propriétaire (volume/jour)	SIEM leader du marché	https://www.splunk.com
Microsoft Sentinel	Propriétaire (cloud, à l'usage)	SIEM/SOAR cloud-natif	https://azure.microsoft.com/products/microsoft-sentinel
IBM QRadar	Propriétaire	SIEM entreprise	https://www.ibm.com/qradar
Google SecOps (Chronicle)	Propriétaire (cloud)	SIEM cloud à très grande échelle	https://chronicle.security
LogRhythm / Exabeam	Propriétaire	SIEM + UEBA	https://www.exabeam.com
Sumo Logic	Propriétaire (SaaS)	SIEM/observabilité cloud	https://www.sumologic.com
Securonix	Propriétaire (SaaS)	SIEM + UEBA	https://www.securonix.com

Tableau 2.1: *Principales solutions SIEM (open source en haut, commerciales ensuite).*

Open source ou commercial ?

Les solutions **open source** (Wazuh, Elastic, Graylog, Security Onion, OSSIM) suppriment les coûts de licence mais demandent davantage d'ingénierie et d'exploitation. Les solutions **commerciales** (Splunk, Sentinel, QRadar) offrent intégrations, support et modules prêts à l'emploi, mais leur coût croît avec le **volume de données ingérées** (Go/jour) ou le nombre d'événements par seconde (EPS) — le poste budgétaire à surveiller de près.

2.3 Étude de cas : architecture et installation de Wazuh

Wazuh est le SIEM/XDR open source le plus déployé. Il combine HIDS (détection sur l'hôte), surveillance d'intégrité des fichiers (FIM), évaluation de configuration (SCA/CIS), détection de vulnérabilités, et corrélation, le tout stocké dans un moteur de recherche dérivé d'OpenSearch.

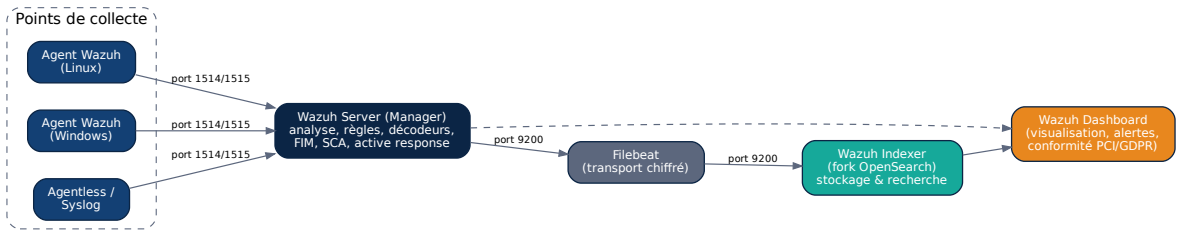

Figure 2.2: *Architecture de Wazuh : agents et sources syslog → serveur (analyse) → indexer (stockage) → dashboard.*

2.3.1 Les trois composants centraux

- **Wazuh Server (Manager)** : reçoit les données des agents, applique décodeurs et règles, déclenche la *réponse active*.
- **Wazuh Indexer** : moteur de recherche/stockage (fork d'OpenSearch).
- **Wazuh Dashboard** : interface web de visualisation et de conformité.

2.3.2 Installation « tout-en-un » du serveur (assistant officiel)

```
# Installation automatisée de la central components (Indexer + Server +
    Dashboard)
curl -sO https://packages.wazuh.com/4.x/wazuh-install.sh
sudo bash ./wazuh-install.sh -a

# A la fin, le script affiche l'utilisateur/mot de passe admin.
# Acces a l'interface : https://<IP_du_serveur>  (port 443)
sudo systemctl status wazuh-manager wazuh-indexer wazuh-dashboard
```

2.3.3 Déploiement des sondes : les agents Wazuh

Les **agents** sont les sondes hôtes. On les déclare puis on les installe sur chaque machine à surveiller.

```
# --- Sur Linux (Debian/Ubuntu) : installer et enregistrer un agent ---
curl -sO
    https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent.deb
sudo WAZUH_MANAGER="10.0.0.10" dpkg -i ./wazuh-agent.deb
sudo systemctl enable --now wazuh-agent

# --- Sur Windows (PowerShell administrateur) ---
# msiexec /i wazuh-agent.msi /q WAZUH_MANAGER="10.0.0.10"
    WAZUH_REGISTRATION_SERVER="10.0.0.10"
# NET START WazuhSvc
```

Bonne pratique

Vérifiez la remontée de l'agent dans l'onglet *Agents* du dashboard (statut *Active*). Activez ensuite les modules **FIM** (surveillance de `/etc`, `C:\Windows\System32`), **SCA** (référentiels CIS) et la **détection de vulnérabilités**.

2.4 Les sondes d'un SIEM : comment collecter

Au-delà des agents, un SIEM collecte de multiples façons. Choisir la bonne méthode par source est déterminant pour la couverture *et* le volume.

Méthode	Usage	Exemples
Agent	Collecte locale riche + réponse active	Wazuh agent, Beats, Splunk UF
Syslog (UDP/TCP 514)	Équipements réseau, pare-feu, Unix	rsyslog, syslog-ng
Windows Event Forwarding	Journaux Windows centralisés	WEF/WEC, Winlogbeat
API / Cloud	SaaS, Office 365, AWS, Azure	connecteurs natifs
NetFlow / IPFIX	Métadonnées de flux réseau	nfdump, Elastiflow

Méthode	Usage	Exemples
Capture paquets (TAP/SPAN)	Analyse profonde du trafic	Packetbeat, Zeek

Tableau 2.2: *Méthodes de collecte (sondes logiques) d'un SIEM.*

2.4.1 Exemple : centraliser des journaux via syslog (rsyslog)

```
# Sur le collecteur : activer la reception syslog (rsyslog)
sudo nano /etc/rsyslog.conf
#   module(load="imudp")  input(type="imudp" port="514")
#   module(load="imtcp")  input(type="imtcp" port="514")
sudo systemctl restart rsyslog

# Sur un equipement source : envoyer les logs vers le collecteur
echo '*.* @@10.0.0.10:514' | sudo tee -a /etc/rsyslog.d/90-forward.conf
sudo systemctl restart rsyslog
```

2.5 La stack Elastic (ELK) comme socle SIEM

Très répandue, la stack Elastic sert de base à de nombreux SIEM (y compris l'application *Elastic Security*). La chaîne typique :

Figure 2.3: *Stack Elastic : Beats/Logstash → Elasticsearch → Kibana (application SIEM).*

- **Beats** : agents légers (Filebeat pour les logs, Winlogbeat pour Windows, Packetbeat pour le réseau, Metricbeat pour les métriques).
- **Logstash** : pipeline de transformation (filtres *grok*, mutations).
- **Elasticsearch** : indexation et recherche temps réel.
- **Kibana** : visualisation, détections (règles), *timelines*.

Chapitre 3

Les EDR : détection et réponse sur les postes

EDR

Un **EDR** (*Endpoint Detection and Response*) est un agent installé sur les postes et serveurs qui **enregistre en continu** l'activité (processus, connexions, fichiers, registre), **détecte** les comportements malveillants (heuristiques, ML, règles ATT&CK) et permet une **réponse** à distance : isolement réseau de la machine, arrêt de processus, suppression de fichier, voire *rollback* d'un chiffrement par rançongiciel.

3.1 Antivirus (EPP) vs EDR

L'**EPP** (*Endpoint Protection Platform*, l'antivirus moderne) *prévient* en bloquant les menaces connues (signatures, réputation). L'EDR ajoute la *détection comportementale*, l'*enregistrement* pour investigation et la *réponse*. Les deux sont complémentaires et souvent réunis dans une même suite.

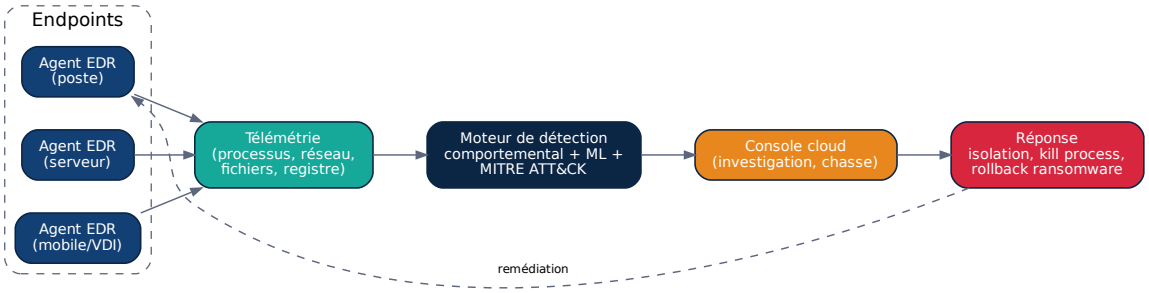

Figure 3.1: *Architecture d'un EDR : télémétrie des endpoints → moteur de détection → console → réponse/remédiation.*

3.2 Ce que permet un EDR

- **Visibilité** : arbre des processus, lignée d'exécution, télémétrie horodatée.
- **Détection comportementale** : techniques ATT&CK, *living-off-the-land*.
- **Chasse aux menaces** (*threat hunting*) sur les données historisées.
- **Réponse** : isolement, *kill*, quarantaine, collecte forensic à distance.
- **Remédiation** : restauration de fichiers, rollback (anti-ransomware).

3.3 Panorama des solutions EDR

Solution	Licence	Type	Site officiel
Wazuh	GPLv2 (open source)	EDR/XDR open	https://wazuh.com
OSQuery	Apache 2.0 / GPL (open)	Télémétrie SQL	https://osquery.io
Velociraptor	AGPLv3 (open source)	DFIR / chasse	https://docs.velociraptor.app
Microsoft Defender for Endpoint	Propriétaire (M365)	EDR/EPP intégré	https://www.microsoft.com/security
CrowdStrike Falcon	Propriétaire (SaaS)	EDR/XDR leader	https://www.crowdstrike.com
SentinelOne Singularity	Propriétaire (SaaS)	EDR/XDR autonome	https://www.sentinelone.com
Palo Alto Cortex XDR	Propriétaire	EDR/XDR	https://www.paloaltonetworks.com/cortex
Sophos Intercept X	Propriétaire	EDR/EPP	https://www.sophos.com
ESET Inspect	Propriétaire	EDR	https://www.eset.com
Trend Micro Apex One	Propriétaire	EDR/EPP	https://www.trendmicro.com

Tableau 3.1: *Solutions EDR (open source puis commerciales).*

3.4 Installer un EDR open source : OSQuery + Velociraptor

```
# OSQuery : interroger un endpoint comme une base SQL (Debian/Ubuntu)
export OSQUERY_KEY=1484120AC4E9F8A1A577AEEE97A80C63C9D8B80B
sudo apt install -y osquery
osqueryi "SELECT name, path, pid FROM processes WHERE on_disk = 0;"  #
   processus sans binaire (suspect)

# Velociraptor : binaire unique (serveur + agents), DFIR et chasse a
   grande echelle
wget
   https://github.com/Velocidex/velociraptor/releases/latest/download/velociraptor-l
chmod +x velociraptor-linux-amd64
./velociraptor-linux-amd64 gui   # demarre une console locale de
   demonstration
```

Chapitre 4

Les XDR : détection et réponse étendues

XDR

Un **XDR** (*Extended Detection and Response*) unifie en une seule plateforme la télémétrie de **plusieurs domaines** — endpoint (EDR), réseau (NDR), e-mail, identité (IAM/AD), cloud — pour **corréler** les signaux *entre domaines* et offrir une détection et une réponse cohérentes là où le SIEM se contentait d'agréger des journaux. On distingue le XDR *natif* (un seul éditeur) et le XDR *ouvert* (intègre des sources tierces).

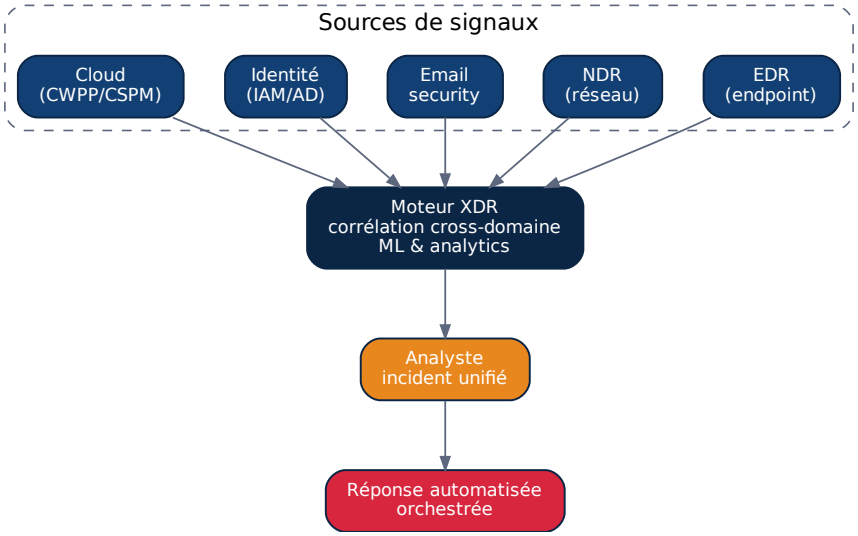

Figure 4.1: *Le XDR fédère plusieurs sources de signaux et corrèle entre domaines avant de présenter un incident unifié.*

4.1 SIEM, EDR, NDR, XDR, MDR : comment se situer

Ces solutions ne s'opposent pas, elles se complètent. Le schéma ci-dessous résume leur articulation, et la matrice de couverture montre les domaines couverts.

Et le MDR ?

Le **MDR** (*Managed Detection and Response*) n'est pas une technologie mais un **service** : un prestataire opère pour vous l'EDR/XDR/SIEM avec une équipe d'analystes 24/7. Idéal quand on manque de ressources internes pour tenir un SOC.

4.2 Panorama des solutions XDR

Solution	Licence	Nature	Site officiel
Wazuh (Open XDR)	GPLv2 (open)	Ouvert	https://wazuh.com
Microsoft Defender XDR	Propriétaire	Natif	https://www.microsoft.com/security
Palo Alto Cortex XDR	Propriétaire	Natif/ouvert	https://www.paloaltonetworks.com/cortex
CrowdStrike Falcon Insight XDR	Propriétaire	Ouvert	https://www.crowdstrike.com
Trend Micro Vision One	Propriétaire	Natif	https://www.trendmicro.com
SentinelOne Singularity XDR	Propriétaire	Natif/ouvert	https://www.sentinelone.com
Cisco XDR	Propriétaire	Ouvert	https://www.cisco.com

Tableau 4.1: *Principales plateformes XDR.*

Chapitre 5

IDS / IPS : détection et prévention d'intrusion

IDS et IPS

Un **IDS** (*Intrusion Detection System*) analyse le trafic ou l'activité d'un hôte et **alerte** en cas d'activité suspecte (mode passif). Un **IPS** (*Intrusion Prevention System*) va plus loin : placé **en coupure** (*inline*), il peut **bloquer** le trafic malveillant en temps réel. On distingue le **NIDS/NIPS** (réseau) et le **HIDS/HIPS** (hôte).

5.1 NIDS vs HIDS, et placement dans le réseau

Le **NIDS** surveille le trafic réseau (souvent via un TAP ou un port SPAN) ; le **HIDS** surveille un hôte (intégrité de fichiers, journaux, processus). L'IPS, lui, est traversé par le trafic pour pouvoir le couper.

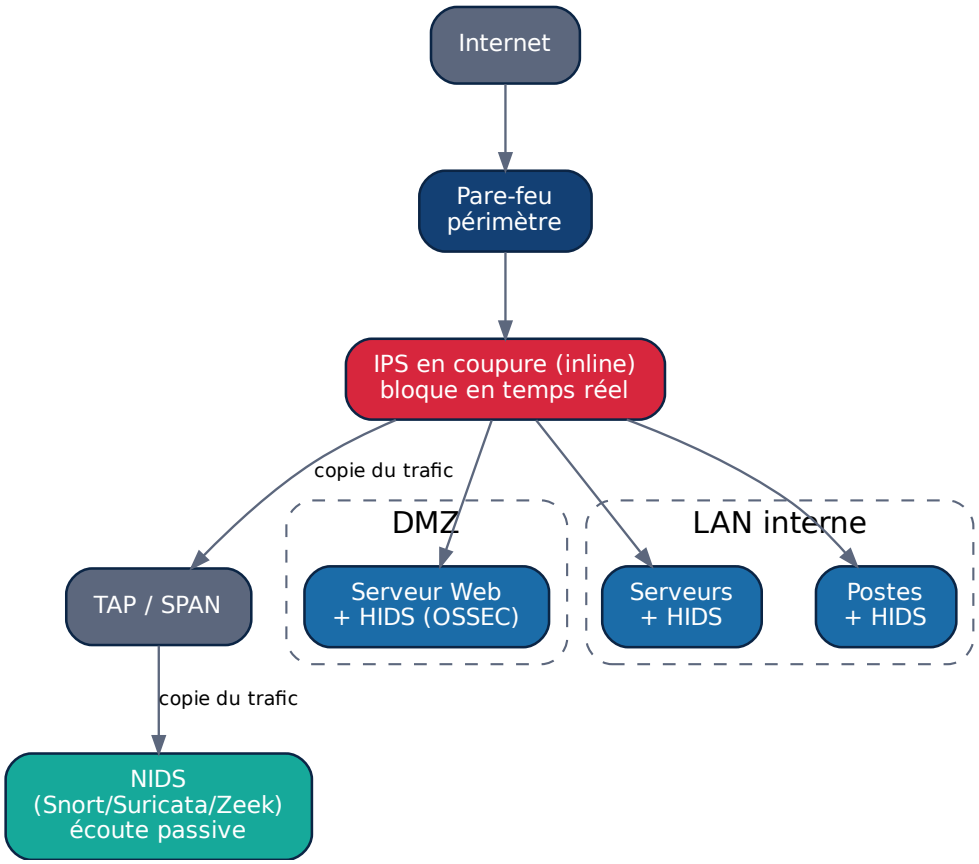

Figure 5.1: *Placement type : IPS en coupure derrière le pare-feu, NIDS en écoute passive sur un TAP/SPAN, HIDS sur les hôtes.*

5.2 Méthodes de détection

- **Par signatures** : on compare le trafic à une base de règles (efficace sur le connu, aveugle au *zero-day*). Ex. Snort, Suricata.
- **Par anomalie / comportement** : on modélise le « normal » et on alerte sur l'écart (détecte l'inconnu, mais génère des faux positifs).
- **Par analyse protocolaire** : Zeek interprète les protocoles et produit des journaux riches plutôt que de simples alertes.

Figure 5.2: *Chaîne de traitement d'un moteur de type Snort/Suricata, de la capture des paquets à la sortie (alerte ou* drop*).*

5.3 Anatomie d'une règle Snort

```
# alert <proto> <ip_src> <port_src> -> <ip_dst> <port_dst> ( options )
alert tcp any any -> $HOME_NET 22 ( \
   msg:"SSH - tentative de connexion"; \
   flags:S; sid:1000001; rev:1; )

# Detection d'une chaine suspecte dans une requete HTTP
alert tcp any any -> $HOME_NET 80 ( \
   msg:"Possible injection SQL"; content:"UNION SELECT"; nocase; \
   sid:1000002; rev:1; )
```

5.4 Panorama des IDS/IPS

Outil	Licence	Type	Site officiel
Snort	GPLv2 (open source)	NIDS/NIPS signatures	https://www.snort.org
Suricata	GPLv2 (open source)	NIDS/NIPS multi-thread	https://suricata.io
Zeek (ex-Bro)	BSD (open source)	NSM / analyse protocolaire	https://zeek.org
OSSEC	GPLv2 (open source)	HIDS	https://www.ossec.net
Wazuh	GPLv2 (open source)	HIDS + SIEM	https://wazuh.com
Security Onion	GPL/Elastic (open)	Distribution IDS+NSM+SIEM	https://securityonionsolutions.com
Fail2ban	GPLv2 (open source)	IPS hôte (bannissement IP)	https://github.com/fail2ban/fail2ban
Cisco Firepower / Snort 3	Propriétaire	NGIPS	https://www.cisco.com

Outil	Licence	Type	Site officiel

Tableau 5.1: *Systèmes de détection/prévention d'intrusion.*

5.5 Installer et exécuter Suricata (NIDS)

```
# Installation (Debian/Ubuntu)
sudo apt update && sudo apt install -y suricata

# Mettre a jour les regles (ET Open via suricata-update)
sudo suricata-update
sudo suricata-update list-sources
sudo suricata-update enable-source et/open

# Definir l'interface a ecouter dans /etc/suricata/suricata.yaml
   (af-packet)
# puis lancer en mode IDS sur eth0 :
sudo suricata -i eth0
# Les alertes apparaissent dans /var/log/suricata/eve.json et fast.log
tail -f /var/log/suricata/fast.log
```

5.6 Installer Snort 3

```
# Sur de nombreuses distributions, Snort 3 est dispo en paquet
sudo apt install -y snort

# Verifier la configuration et lancer en mode console sur eth0
sudo snort -c /etc/snort/snort.lua --daq pcap -i eth0 -A alert_fast -s
   65535
```

Bonne pratique

Snort vs Suricata : Snort est la référence historique (mono-thread, Snort 3 améliore les perfs) ; Suricata est multi-thread, gère nativement le multi-cœur, le NetFlow, l'extraction de fichiers et la sortie JSON (EVE) — très adapté à une intégration SIEM. Les deux partagent une syntaxe de règles proche.

Chapitre 6

NDR et sondes réseau

NDR

Le **NDR** (*Network Detection and Response*) applique au **réseau** ce que l'EDR fait à l'endpoint : analyse continue du trafic (souvent par ML et analyse comportementale), détection des mouvements latéraux et de l'exfiltration, et réponse (alerte, *quarantaine* réseau). Zeek, Suricata et Arkime en sont des briques open source de référence.

6.1 Capturer le trafic : TAP, SPAN et NetFlow

Une sonde réseau ne voit que ce qu'on lui donne. Trois grandes méthodes d'alimentation existent, avec des compromis différents.

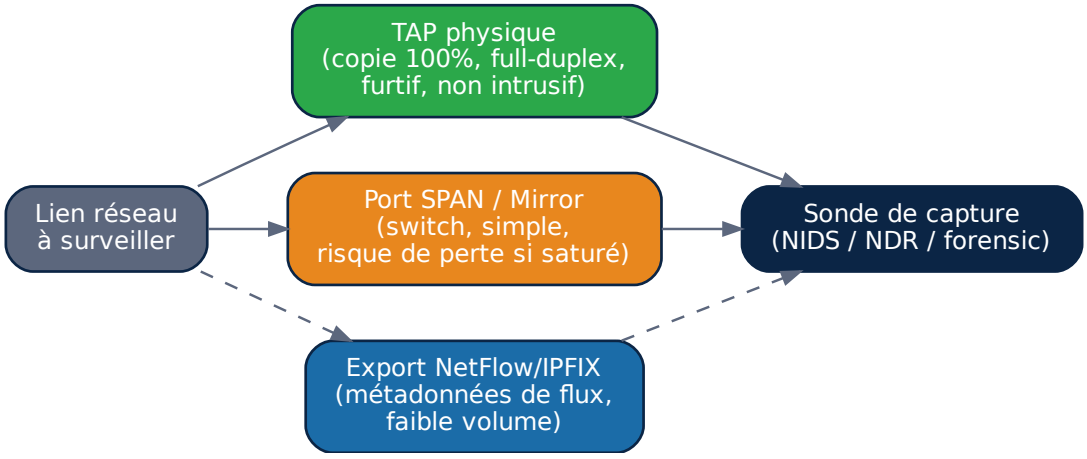

Figure 6.1: *Trois méthodes d'alimentation d'une sonde : TAP physique, port SPAN/mirror, et export NetFlow/IPFIX.*

Méthode	Avantages	Limites
TAP physique	Copie 100% du trafic, full-duplex, furtif, sans charge	Matériel dédié, point d'insertion physique
Port SPAN / Mirror	Simple, sans matériel, configurable sur switch	Peut perdre des paquets si saturé, charge le switch
NetFlow / IPFIX	Faible volume, vue d'ensemble des flux	Métadonnées seulement (pas le contenu)

Tableau 6.1: *Comparaison des méthodes de capture pour alimenter une sonde.*

6.2 Outils NDR / NSM open source

- **Zeek** (https://zeek.org, BSD) — produit des journaux protocolaires détaillés (conn, dns, http, ssl, files...).
- **Suricata** (https://suricata.io, GPLv2) — IDS/IPS + extraction de fichiers + sortie EVE JSON.
- **Arkime** (ex-Moloch, https://arkime.com, Apache 2.0) — capture et indexation *full packet* avec recherche.
- **Security Onion** (https://securityonionsolutions.com) — distribution clé en main réunissant Zeek, Suricata, Elastic et la chasse.

6.3 Déployer une sonde Zeek

```
# Installation de Zeek (depuis les depots officiels OpenSUSE Build
   Service)
echo 'deb
   http://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04/
   /' \
  | sudo tee /etc/apt/sources.list.d/security:zeek.list
sudo apt update && sudo apt install -y zeek

# Configurer l'interface d'ecoute puis deployer via ZeekControl
sudo /opt/zeek/bin/zeekctl deploy
# Journaux produits dans /opt/zeek/logs/current/ (conn.log, dns.log,
   http.log...)
```

Chapitre 7

Synthèse comparative

7.1 Quelle solution pour quel besoin ?

Famille	Périmètre	Force	À combiner avec
SIEM	Tous les journaux du SI	Corrélation, conformité, vue globale	EDR, NDR, SOAR
EDR	Postes & serveurs	Détection comportementale + réponse hôte	SIEM, XDR
NDR	Réseau	Mouvements latéraux, exfiltration	SIEM, IDS
XDR	Multi-domaines	Corrélation cross-domaine unifiée	SOAR, TI
IDS/IPS	Réseau / hôte	Détection (et blocage) par signatures	SIEM, NDR
MDR	Service	Analystes 24/7 externalisés	EDR/XDR/SIEM

Tableau 7.1: *Positionnement synthétique des familles d'outils.*

Trajectoire de déploiement conseillée

1) Centraliser les journaux (SIEM, ex. Wazuh) ; 2) déployer un EDR sur les postes sensibles ; 3) installer une sonde réseau (Suricata/Zeek) sur un TAP/SPAN ; 4) corréler le tout (XDR ouvert) ; 5) automatiser la réponse (SOAR) ; 6) mesurer (MTTD/MTTR) et affiner les règles pour réduire les faux positifs.

Chapitre 8

Lexique

Terme	Définition
APT	*Advanced Persistent Threat* — attaquant sophistiqué et persistant, souvent étatique.
C2 / C&C	*Command and Control* — infrastructure pilotant les machines compromises.
CEF / LEEF	Formats normalisés de journaux (ArcSight / QRadar).
DAQ	*Data Acquisition* — couche de capture de paquets de Snort.
DFIR	*Digital Forensics & Incident Response* — investigation numérique et réponse.
ECS	*Elastic Common Schema* — schéma commun de champs pour les logs Elastic.
EDR	*Endpoint Detection and Response* — détection/réponse sur l'hôte.
EPP	*Endpoint Protection Platform* — antivirus moderne (prévention).
EPS	*Events Per Second* — débit d'événements, métrique de dimensionnement SIEM.
EVE JSON	Format de sortie JSON de Suricata (*Extensible Event Format*).
FIM	*File Integrity Monitoring* — surveillance d'intégrité des fichiers.
Grok	Langage de motifs de Logstash pour parser du texte non structuré.
HIDS / HIPS	IDS/IPS basé sur l'hôte.
IDS / IPS	Système de détection / prévention d'intrusion.
IOC	*Indicator of Compromise* — artefact témoignant d'une compromission.
IPFIX	Standard d'export de métadonnées de flux (successeur de NetFlow).
Kill Chain	Modèle des étapes d'une cyberattaque (Lockheed Martin).
MDR	*Managed Detection and Response* — service de détection/réponse managé.
MITRE ATT&CK	Référentiel des tactiques et techniques d'attaque observées.
MTTD / MTTR	Temps moyen de détection / de réponse (ou remédiation).
NDR	*Network Detection and Response* — détection/réponse réseau.
NIDS / NIPS	IDS/IPS réseau.
NetFlow	Protocole Cisco d'export de métadonnées de flux réseau.
NSM	*Network Security Monitoring* — supervision de sécurité réseau.
OSSEC	HIDS open source historique, base de Wazuh.
SCA	*Security Configuration Assessment* — audit de configuration (CIS).
SIEM	*Security Information and Event Management.*
SOAR	*Security Orchestration, Automation and Response* — orchestration et automatisation.
SOC	*Security Operations Center* — centre des opérations de sécurité.
SPAN	*Switched Port Analyzer* — port miroir d'un switch.
TAP	*Test Access Point* — dispositif passif de copie du trafic.
Threat hunting	Recherche proactive de menaces non détectées par les alertes.
TI	*Threat Intelligence* — renseignement sur la menace (IOC, TTP).
TTP	Tactiques, Techniques et Procédures d'un attaquant.
UEBA	*User and Entity Behavior Analytics* — analyse comportementale.
XDR	*Extended Detection and Response* — détection/réponse étendue multi-domaines.
Zero-day	Vulnérabilité inconnue de l'éditeur, sans correctif disponible.

Tableau 8.1: *Lexique des principaux acronymes et termes.*

Chapitre 9

Bibliographie en français

Ouvrages recommandés (langue française)

Sélection d'ouvrages, en français, pour approfondir la sécurité défensive, les SOC et la détection d'intrusion. Les éditeurs **ENI** et **Eyrolles** publient de nombreux titres techniques régulièrement réédités.

- **Sécurité informatique — Principes et méthodes** — L. Bloch, C. Wolfhugel (Eyrolles). Ouvrage de référence pour les RSSI et administrateurs.
- **Sécurité opérationnelle — Conseils pratiques pour sécuriser le SI** — A. Fernandez-Toro (Eyrolles).
- **Management de la sécurité de l'information — ISO 27001 / 27002** — A. Fernandez-Toro (Eyrolles).
- **La collection « Sécurité informatique » des Éditions ENI** : titres sur *Ethical Hacking*, *tests d'intrusion*, *analyse forensique*, *sécurité réseau* et *Linux* — bonnes bases pratiques.
- **Linux — Sécuriser un réseau** (collection ENI) — pare-feu, IDS/IPS (Snort), durcissement, supervision.
- **Cybersécurité — Analyser les risques, mettre en œuvre les solutions** — S. Ghernaouti (Dunod).
- **Tableaux de bord de la sécurité réseau** — C. Llorens, L. Levier, D. Valois (Eyrolles) — supervision, métriques et sondes.
- **Guides et publications de l'ANSSI** (gratuits, en français) : guides d'hygiène informatique, journalisation, recommandations d'architecture — voir le chapitre Liens utiles.
- **Wireshark — Analyse de trafic réseau** (collection ENI) — complément indispensable à l'analyse de sondes.

Bonne pratique

Pour rester à jour, privilégiez les **dernières éditions** : ce domaine évolue vite (versions d'outils, menaces, réglementation NIS2). Les documentations officielles en ligne (Wazuh, Suricata, Elastic, MITRE) restent la source la plus actuelle.

Chapitre 10

Liens utiles

10.1 Sites officiels des solutions

SIEM

- Wazuh — https://wazuh.com
- Elastic Security — https://www.elastic.co/security
- Graylog — https://graylog.org
- Security Onion — https://securityonionsolutions.com
- OSSIM — https://cybersecurity.att.com/products/ossim
- Splunk — https://www.splunk.com
- Microsoft Sentinel — https://azure.microsoft.com/products/microsoft-sentinel
- IBM QRadar — https://www.ibm.com/qradar

EDR / XDR

- CrowdStrike — https://www.crowdstrike.com
- SentinelOne — https://www.sentinelone.com
- Microsoft Defender — https://www.microsoft.com/security
- Palo Alto Cortex — https://www.paloaltonetworks.com/cortex
- OSQuery — https://osquery.io
- Velociraptor — https://docs.velociraptor.app

IDS / IPS / NDR

- Snort — https://www.snort.org
- Suricata — https://suricata.io
- Zeek — https://zeek.org
- OSSEC — https://www.ossec.net
- Arkime — https://arkime.com
- Fail2ban — https://github.com/fail2ban/fail2ban

Règles & threat intel

- Emerging Threats (règles) — https://rules.emergingthreats.net
- Snort Rules — https://www.snort.org/downloads
- Sigma (règles SIEM) — https://github.com/SigmaHQ/sigma

10.2 Référentiels, organismes et ressources

- **ANSSI** (France) — https://www.ssi.gouv.fr et https://cyber.gouv.fr
- **CERT-FR** (alertes et avis) — https://www.cert.ssi.gouv.fr
- **cybermalveillance.gouv.fr** — https://www.cybermalveillance.gouv.fr
- **MITRE ATT&CK** — https://attack.mitre.org
- **MITRE D3FEND** (contre-mesures) — https://d3fend.mitre.org
- **NIST Cybersecurity Framework** — https://www.nist.gov/cyberframework
- **OWASP** — https://owasp.org
- **ENISA** (UE) — https://www.enisa.europa.eu
- **CIS Benchmarks** — https://www.cisecurity.org/cis-benchmarks
- **The DFIR Report** (cas réels) — https://thedfirreport.com

---

Document rédigé par **LinuXMaine.org** — 4 juin 2026.
Diagrammes générés avec Graphviz et Matplotlib ; mise en page LaTeX.