# EDR open source : Wazuh, LimaCharlie et Velociraptor comparés

> Comparatif EDR open source 2026 : Wazuh, LimaCharlie et Velociraptor — architecture, règles de détection, threat hunting et limites vs EDR commerciaux.

La détection et réponse sur les endpoints (EDR) est devenue une capacité de sécurité non-négociable pour toute organisation sérieuse sur la cybersécurité. Les grandes entreprises investissent dans CrowdStrike Falcon, SentinelOne ou Microsoft Defender for Endpoint — des plateformes qui combinent agents légers, moteurs de détection basés sur le machine learning, threat intelligence propriétaire et équipes de support 24/7. Mais à 15-25 euros par endpoint et par mois, et avec des engagements contractuels rigides, ces solutions restent inaccessibles pour une grande partie du marché. PME, associations, collectivités, universités, startups en croissance : des milliers d'organisations ont un besoin réel de protection EDR sans le budget correspondant. Les solutions open source ont considérablement mûri ces dernières années. Wazuh a évolué d'un simple HIDS vers une plateforme XDR complète avec télémétrie endpoint. LimaCharlie propose une architecture cloud-native ultra-flexible avec 25 sensors gratuits. Velociraptor révolutionne le threat hunting avec son langage de requête VQL. Utilisés ensemble, ces trois outils constituent une stack de sécurité endpoint redoutablement efficace — à condition d'avoir les compétences techniques pour les configurer et les maintenir. Ce guide compare leurs architectures, documente leurs capacités réelles, et fournit les configurations concrètes pour commencer à les déployer.

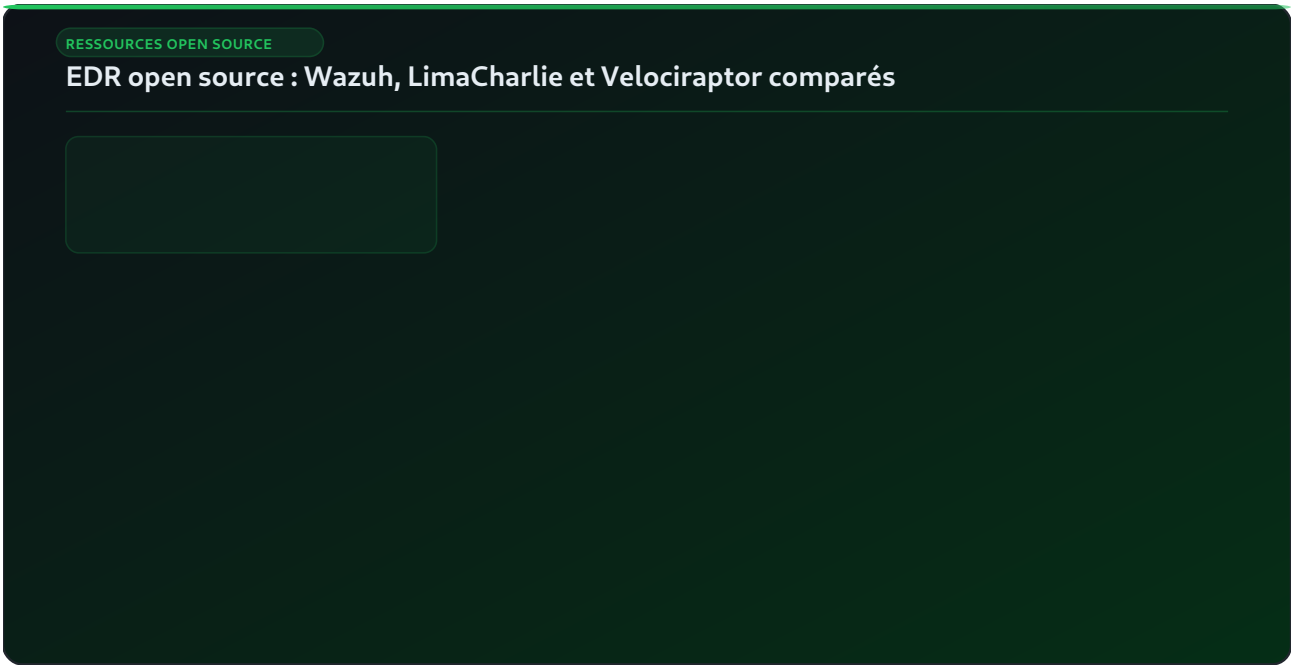
**À RETENIR**

**À retenir :**

Wazuh 4.x combine HIDS, FIM, EDR, SIEM et XDR dans une plateforme unifiée open source — la solution la plus complète du marché pour un coût zéro en licences.

LimaCharlie offre 25 sensors gratuits avec des capacités D&R rules en temps réel et une architecture cloud-native — idéal pour les équipes sécurité qui veulent de la flexibilité sans infrastructure à gérer.

> Velociraptor est le leader incontesté du threat hunting à grande échelle grâce à VQL — il peut interroger simultanement des milliers d'endpoints en quelques secondes.
>
> L'architecture recommandée combine les trois outils : Velociraptor pour le hunting forensique, Wazuh pour l'alerting SIEM continu, LimaCharlie pour la réponse automatisée.




La question du coût est la plus évidente mais pas la seule motivation. Un EDR commercial pour 500 endpoints représente un budget annuel de 90 000 à 150 000 euros en licences seules — sans compter l'intégration, la formation et le support. Pour une PME de 150 salariés, c'est souvent plus que le budget total de la direction informatique. L'open source élimine les coûts de licences et offre la liberté de déploiement (on-premise, cloud privé, hybride) sans contraintes contractuelles.

La **souveraineté des données** est une motivation croissante, notamment pour les organisations du secteur public et les entreprises sensibles. Un EDR commercial signifie que les télémétries de

vos endpoints — processus en cours d'exécution, connexions réseau, modifications de fichiers, lignes de commandes — transitent vers des serveurs contrôlés par un éditeur étranger. Pour les organisations soumises à des contraintes de confidentialité strictes (défense, santé, infrastructure critique), cette situation est problématique. L'open source permet d'héberger l'intégralité de la stack de sécurité sur des infrastructures sous contrôle.

La **personnalisation** représente l'avantage technique le plus souvent sous-estimé. Les EDR commerciaux sont des boîtes noires : impossible de modifier les règles de détection au-delà de ce que le fournisseur expose dans son interface. Avec Wazuh ou Velociraptor, chaque aspect du moteur de détection est personnalisable, extensible et adaptable aux spécificités de votre environnement. Les règles Sigma peuvent être importées directement. Les artefacts forensiques collectés sont configurables. Les automatisations de réponse sont scriptables en Python, Go ou Bash.

## Wazuh en mode EDR : bien au-delà du HIDS classique

Wazuh a commencé sa vie comme un fork d'OSSEC, un HIDS (Host-based Intrusion Detection System) historique. La version 4.x a opéré une transformation profonde qui le positionne désormais comme une plateforme XDR complète. L'agent Wazuh, disponible pour Linux, Windows, macOS, Solaris et AIX, collecte une télémétrie riche que le manager central corrèle et analyse.

⚡ **Retour terrain**

Lors de mes audits de stack technique, je vois régulièrement des outils open source de sécurité installés mais non maintenus — des versions de Nessus Community, TheHive ou MISP déployées il y a 3 ans sans processus de mise à jour. Un outil de sécurité non patché peut devenir lui-même un vecteur d'attaque. Pour un SOC régional, TheHive 3.x (EOL

depuis 2022) avait une CVE critique non patchée permettant une RCE non authentifiée sur l'interface d'administration.

Le module de **File Integrity Monitoring (FIM)** surveille en temps réel les modifications sur les fichiers et répertoires configurés : hash SHA1/MD5/SHA256, permissions, propriétaire, contenu (optionnel). Toute modification sur des chemins critiques (répertoires système, binaires, fichiers de configuration) génère une alerte. La corrélation avec un hash VirusTotal est configurée nativement dans Wazuh depuis la version 3.9.

Le module de **syscall monitoring** (via Linux Audit Framework ou Windows Event Forwarding) collecte les événements de création de processus, d'accès aux fichiers et de connexions réseau avec leur contexte complet. Sur Linux, l'intégration avec Auditd permet de collecter des événements équivalents aux Event Logs Windows avec une granularité similaire. Sur Windows, Sysmon est souvent utilisé en complément pour enrichir les Event Logs avant ingestion par l'agent Wazuh. Notre guide sur Wazuh SIEM/XDR déploiement détaille cette architecture complète.

Le mapping **MITRE ATT&CK** natif de Wazuh est l'une de ses fonctionnalités les plus utiles opérationnellement : chaque règle de détection est taguée avec les techniques ATT&CK correspondantes, permettant de visualiser la couverture de détection par tactique et de prioriser les règles manquantes. La détection d'attaques Active Directory est documentée dans notre article sur la détection AD avec Wazuh.

---

## LimaCharlie : architecture cloud-native et D&R rules en temps réel

LimaCharlie se distingue par une approche architecturale radicalement différente. Fondé en 2017, il propose un modèle cloud-native où l'infrastructure de collecte et d'analyse est entièrement gérée. Les sensors LimaCharlie sont des agents ultra-légers (moins de 5 Mo, empreinte RAM minimale) qui s'appuient sur des fonctionnalités noyau avancées (ETW sur Windows, eBPF sur Linux) pour collecter la télémétrie endpoint sans impacter les performances.

Le modèle commercial de LimaCharlie est attractif pour les petites structures : **25 sensors permanents gratuits**, puis tarification à la consommation (0,0025$/capteur/heure au-delà, soit environ 1,8$/endpoint/mois en usage continu — loin des prix des EDR commerciaux). Ce modèle freemium rend LimaCharlie accessible pour des labs de sécurité, des red teams, des MSSPs en phase de démarrage ou des organisations avec un parc endpoint limité.

Les **D&R rules (Detection & Response)** sont le cœur de la valeur ajoutée de LimaCharlie. Ce langage de règles YAML permet de définir en quelques lignes des détections complexes et des réponses automatisées. Une règle D&R peut détecter un processus suspect et automatiquement isoler l'endpoint du réseau, tuer le processus, collecter un dump mémoire et envoyer une alerte Slack — tout cela sans intervention humaine. Voici un exemple de règle D&R pour détecter une exécution de Mimikatz :

```
detect:
  event: NEW_PROCESS
  op: and
  rules:
    - op: is
      path: event/FILE_PATH
      case sensitive: false
      value: mimikatz.exe
    - op: or
      rules:
        - op: contains
          path: event/COMMAND_LINE
          value: sekurlsa
        - op: contains
          path: event/COMMAND_LINE
          value: lsadump

respond:
  - action: task
    command:
      - deny_tree
  - action: report
    name: mimikatz_detected
  - action: isolate_network
```

La collecte d'**artefacts forensiques** à distance est une fonctionnalité distinctive : depuis la console LimaCharlie, il est possible de demander à n'importe quel sensor de collecter une liste de

processus en cours, les connexions réseau actives, les clés de registre Run, les fichiers Prefetch, ou d'exécuter une commande shell arbitraire — le tout en temps réel, sans accès RDP ou SSH.

## Velociraptor : threat hunting à grande échelle avec VQL

Velociraptor est l'outil de threat hunting et de collecte forensique le plus puissant disponible en open source. Développé par Rapid7 avant d'être rendu open source, il est aujourd'hui maintenu par une communauté active. Son architecture client-serveur supporte des déploiements allant de quelques dizaines à plusieurs milliers d'endpoints.

Le **VQL (Velociraptor Query Language)** est la différence fondamentale qui positionne Velociraptor au-dessus de tout concurrent open source. Inspiré de SQL, VQL permet d'interroger les endpoints comme une base de données. En quelques secondes, une requête VQL peut lister tous les processus exécutés sur 1000 machines avec leur hash, identifier tous les services Windows dont le binaire n'est pas signé, ou chercher des IoCs spécifiques (hashes, noms de fichiers, clés de registre) sur l'ensemble du parc.

```
 -- Hunt: détection d'exécution PowerShell encodé (technique T1059.001)
SELECT Pid, Name, CommandLine, Username, CreateTime
FROM pslist()
WHERE Name =~ "powershell.exe"
  AND CommandLine =~ "-[Ee][Nn][Cc]"

-- Hunt: recherche de connexions réseau suspectes vers des ports non-standard
SELECT Pid, Name, RemoteAddr, RemotePort, State
FROM netstat()
WHERE RemotePort NOT IN (80, 443, 22, 25, 53, 3389)
  AND State = "ESTABLISHED"

-- Hunt: processus sans signature Microsoft dans System32
SELECT FullPath, Hash.SHA256, Authenticode.Trusted
FROM glob(globs="C:\\Windows\\System32\\*.exe")
WHERE NOT Authenticode.Trusted = "trusted"
```

La bibliothèque d'**artifacts Velociraptor** est une collection d'analyses forensiques préconfigurées couvrant Windows, Linux et macOS : collecte des fichiers Prefetch, analyse du registre,

extraction des Event Logs, investigation NTFS, analyse des navigateurs web, collecte d'artefacts mémoire. Cette bibliothèque est extensible et partageable dans la communauté. Pour l'écriture de règles de détection complémentaires, notre guide sur les règles Sigma est un complément indispensable.

## OpenEDR : l'alternative Windows-only

OpenEDR (anciennement Comodo Cybersecurity) est une solution EDR open source conçue spécifiquement pour Windows. Son architecture repose sur un driver noyau Ring 0 qui intercepte les appels système au niveau le plus bas, offrant une visibilité comparable aux EDR commerciaux sur les plateformes Windows. La télémétrie collectée couvre la création de processus avec arbres de dépendances, les injections de code, les modifications de mémoire, les accès aux fichiers et les connexions réseau.

Les limites d'OpenEDR sont significatives : **Windows uniquement** (aucun support Linux ou macOS), communauté moins active que Wazuh ou Velociraptor, documentation insuffisante pour les déploiements enterprise. Il reste un outil intéressant pour des labs Windows dédiés ou des environnements purement Windows où une visibilité kernel-level est prioritaire.

## Tableau comparatif 8 critères

Voici une comparaison objective des trois principales solutions sur les critères les plus importants pour un déploiement réel :

**1. Support OS** : Wazuh (Linux, Windows, macOS, Solaris, AIX, FreeBSD — le plus large), LimaCharlie (Linux, Windows, macOS, Chrome OS), Velociraptor (Linux, Windows, macOS). **2. Facilité de déploiement** : LimaCharlie (le plus simple — SaaS, pas d'infrastructure à gérer), Wazuh (modéré — Wazuh Central Components nécessite 4 vCPUs/8GB RAM minimum), Velociraptor (modéré — binaire unique, configuration YAML). **3. Règles SIGMA** : Wazuh

(import Sigma natif via sigma-converter), LimaCharlie (import Sigma via adaptateur D&R rules), Velociraptor (via artefacts, moins direct). **4. Playbooks IR automatisés** : LimaCharlie (D&R rules avec actions automatiques isolement/kill), Wazuh (active response scripts), Velociraptor (flows et hunts manuels ou schedulés). **5. Coût** : Wazuh (gratuit, coûts infra uniquement), LimaCharlie (gratuit jusqu'à 25 sensors, 1,8$/endpoint/mois ensuite), Velociraptor (gratuit, coûts infra uniquement). **6. Scalabilité** : Wazuh (clusters jusqu'à 100 000+ agents documentés), Velociraptor (millions d'endpoints théoriques), LimaCharlie (SaaS élastique). **7. Threat hunting** : Velociraptor (leader absolu — VQL), Wazuh (limité aux logs collectés), LimaCharlie (hunting via D&R rules et artefacts). **8. Support communauté** : Wazuh (le plus actif — Slack 10 000+ membres, documentation exhaustive), Velociraptor (Discord actif, Rapid7 backing), LimaCharlie (Discord modéré, documentation excellente).

## Architecture recommandée : les trois outils ensemble

La puissance réelle émerge de la complémentarité des trois outils. L'architecture recommandée pour une organisation de 100-500 endpoints combine :

**Velociraptor** comme plateforme de threat hunting réactif et d'investigation forensique : déployé en mode agentless ou avec client léger sur tous les endpoints, il permet de lancer des hunts ciblés en réponse à une alerte ou dans le cadre de campagnes proactives. Quand un IoC (hash, IP, nom de fichier) est reçu d'un feed de threat intelligence, une requête VQL peut vérifier en 30 secondes si cet IoC est présent sur l'ensemble du parc.

**Wazuh** comme SIEM/XDR central : collecte continue de la télémétrie endpoint (FIM, process creation, network connections, logon events), corrélation avec les logs infrastructure (firewall, proxy, AD), alerting temps réel, dashboards de conformité. Le comparatif SIEM open source complet est disponible dans notre article sur le comparatif SIEM open source.

**LimaCharlie** comme moteur de réponse automatisée : ses D&R rules permettent de déployer des playbooks de containment automatiques (isolation réseau, kill de processus, collecte de preuves) en secondes, sans intervention humaine pour les menaces clairement identifiées.

## Déploiement Wazuh agent en 5 commandes

```
 # Linux (Debian/Ubuntu) - Installation agent Wazuh 4.x
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --dearmor -o /usr/share/keyrings/wazuh
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable ma
apt-get update && apt-get install -y wazuh-agent
WAZUH_MANAGER="" WAZUH_AGENT_NAME="$(hostname)" dpkg-reconfigure wazuh-agent
systemctl enable --now wazuh-agent

# Windows (PowerShell - Admin)
Invoke-WebRequest -Uri "https://packages.wazuh.com/4.x/windows/wazuh-agent-4.9.0-1.msi" -OutFile
msiexec /i wazuh-agent.msi /q WAZUH_MANAGER="" WAZUH_REGISTRATION_SERVER=""
Start-Service -Name "Wazuh"
```

## Velociraptor : hunt pour PowerShell encodé

```
 -- Artifact: Windows.Detection.EncodedPowerShell
-- Lance ce hunt sur tous les endpoints pour détecter T1059.001

SELECT Pid, Name, CommandLine, Username,
       CreateTime, Exe, Hash.SHA256 as BinaryHash
FROM pslist()
WHERE Name =~ "(?i)powershell"
  AND CommandLine =~ "-[Ee][Nn][Cc][Oo][Dd][Ee][Dd]?[Cc]?[Oo]?[Mm]?[Mm]?[Aa]?[Nn]?[Dd]?"

-- Décodage automatique de la commande encodée
LET decoded = base64decode(
  string=parse_string_with_regex(
    string=CommandLine,
    regex="-[Ee]{1,2}[Nn][Cc][Oo]?[Dd]?[Ee]?[Dd]?[Cc]?[Oo]?[Mm]?[Mm]?[Aa]?[Nn]?[Dd]? ([A-Za-z0-9+
  ).g1
)
SELECT Pid, Name, decoded, Username FROM scope()
```

## Limites des EDR open source face aux EDR commerciaux

Une comparaison honnête doit nommer les domaines où les EDR commerciaux conservent un avantage significatif. Le **machine learning de détection comportementale** est le premier : CrowdStrike et SentinelOne investissent des centaines de millions en R&D pour entraîner des modèles sur des milliards d'événements endpoint provenant de leur base de clients mondiale. Leurs taux de détection sur les menaces nouvelles (zero-day, novel malware families) dépassent ce que les règles statiques de Wazuh peuvent atteindre sans investissement continu en threat intelligence.

La **threat intelligence propriétaire** intégrée dans les EDR commerciaux (CrowdStrike Intelligence, VirusTotal Enterprise, SentinelOne Singularity Intelligence) offre une contextualisation automatique des alertes que les solutions open source ne peuvent pas fournir sans abonnements tiers coûteux. Le **support 24/7** et les SLA de réponse aux incidents sont des capacités critiques pour les organisations sans SOC interne. Enfin, la **gestion centralisée à grande échelle** (déploiement, mises à jour, configuration de milliers d'agents depuis une console unifiée) reste plus mature dans les solutions commerciales — bien que Wazuh ait considérablement progressé sur ce point avec son Wazuh Dashboard.

## FAQ — Questions fréquentes

### Wazuh peut-il remplacer un SIEM commercial comme Splunk ou Microsoft Sentinel ?

Wazuh couvre les cas d'usage fondamentaux d'un SIEM : collecte de logs normalisée depuis des dizaines de sources (syslog, Windows Event Forwarding, AWS CloudTrail, Office 365, etc.), corrélation de règles, alerting, dashboards et reporting. Pour les organisations avec un volume de logs modéré (jusqu'à 50-100 GB/jour), Wazuh combiné à OpenSearch (son backend natif depuis la v4.4) offre des performances satisfaisantes. Là où Splunk ou Sentinel gardent un avantage : les capacités d'analytics complexes sur de très grands volumes (plusieurs TB/jour), l'intégration native avec les écosystèmes cloud Microsoft ou AWS, et les places de marché de contenu

(MITRE ATT&CK content packs, MSSP use cases). Pour une évaluation complète, notre article sur le comparatif SIEM open source détaille les performances et limites de chaque solution.

### LimaCharlie est-il vraiment gratuit pour 25 sensors, sans limitation cachée ?

Oui, le plan "Free" de LimaCharlie offre genuinement 25 sensors permanents avec l'accès complet aux fonctionnalités : D&R rules, collecte de télémétrie, artefacts forensiques, accès à la console. La seule limitation notable est la rétention des données (1 jour dans le plan gratuit vs 365 jours dans les plans payants). Cette contrainte de rétention est significative pour les investigations qui nécessitent de remonter dans l'historique. LimaCharlie Cloud est hébergé aux États-Unis, ce qui peut poser des questions de conformité RGPD pour les organisations européennes. Une alternative pour les cas d'usage souverains est d'utiliser LimaCharlie on-premise (self-hosted), disponible pour les organisations avec des contraintes réglementaires spécifiques.

### Comment intégrer des règles Sigma dans Wazuh ?

L'intégration Sigma dans Wazuh se fait via un convertisseur qui transforme les règles Sigma au format de règles XML Wazuh. Le projet sigma-converter (disponible sur GitHub) prend en charge la conversion automatisée. La commande de base est `sigma convert -t wazuh -o wazuh_rules.xml rules/windows/`. Les règles converties doivent être placées dans `/var/ossec/etc/rules/` et un `systemctl restart wazuh-manager` est nécessaire pour les charger. Points d'attention : toutes les règles Sigma ne sont pas convertibles parfaitement (certaines utilisent des fonctionnalités non supportées par Wazuh), et les règles à fort volume de faux positifs doivent être ajustées avant déploiement en production. Notre guide complet sur les règles Sigma couvre la méthodologie de tri et d'adaptation.

## Pour aller plus loin

Les concepts présentés dans cet article constituent une base solide pour approfondir le sujet. Ces ressources complémentaires permettent d'aller plus loin dans la compréhension et la mise en pratique.

### Ressources officielles de référence

**ANSSI — Guides et recommandations techniques** — La bibliothèque technique de l'ANSSI publie régulièrement des guides à jour sur tous les aspects de la sécurité des systèmes d'information. Disponibles gratuitement sur ssi.gouv.fr.

**NIST Cybersecurity Framework** — Référentiel international structurant la gestion des risques cyber en 6 fonctions. Version 2.0 publiée en 2024, disponible sur nist.gov.

**MITRE ATT&CK** — Base de connaissances des techniques adversariales, régulièrement mise à jour avec les nouvelles menaces observées dans le monde réel.

### Formation continue

Certifications professionnelles reconnues : CISSP, CISM (management), OSCP, CEH (technique)

Plateformes de formation pratique : HackTheBox, TryHackMe, Hack The Box Academy

Veille quotidienne : bulletins CERT-FR, alertes CISA, flux RSS NVD

### Mise en réseau professionnel

La communauté cybersécurité française est active et ouverte : les clubs RSSI, l'OSSIR, le CLUSIF, et les conférences comme le FIC (Forum International de la Cybersécurité) et les SSTIC sont des points de rencontre essentiels pour les professionnels du secteur. Ces échanges permettent de rester à jour sur les menaces émergentes et les bonnes pratiques réelles.

## Synthèse et perspectives 2026

Les techniques et recommandations présentées dans ce guide s'inscrivent dans un contexte de menaces en constante évolution. La cybersécurité offensive et défensive sont deux faces d'une même médaille : comprendre les mécanismes d'attaque est indispensable pour construire des défenses robustes et résilientes face aux acteurs malveillants les plus sophistiqués.

Pour les équipes sécurité, l'enjeu de 2026 est double : maintenir une veille continue sur les nouvelles techniques publiées par la communauté de recherche (CVE, exploit-db, GitHub, Secrech, SSTIC) tout en assurant le durcissement progressif de l'infrastructure existante. Le référentiel MITRE ATT&CK reste le fil conducteur le plus efficace pour structurer un programme de détection et de réponse face aux tactiques, techniques et procédures des groupes APT ciblant les secteurs critiques.

La formation continue des équipes, la simulation régulière d'incidents (exercices tabletop, exercices Red/Blue/Purple Team), et l'automatisation des tâches répétitives via des outils SOAR constituent les piliers d'une organisation cyber mature. Les organisations qui investissent dans ces trois axes démontrent systématiquement de meilleures métriques de détection et de réponse (MTTD et MTTR réduits de 40% en moyenne selon les benchmarks sectoriels) face aux incidents de sécurité.