

HELIOS

Micro-SOC XDR

Rapport complet de conception, détection, réponse et pilotage

Laboratoire multi-client Endpoint · Identity · Cloud · Mobile · Network

Données entièrement synthétiques

Version 1.0 · 14 juillet 2026

Résumé exécutif

Un environnement synthétique complet a été construit afin de démontrer une chaîne SOC de bout en bout, reproductible et auditable.



Principaux indicateurs opérationnels sur la période simulée.

HELIOS simule un service Micro-SOC XDR pour trois organisations françaises fictives. Le périmètre comprend 1 790 actifs, 75 000 événements normalisés et cinq domaines de télémétrie. Vingt-quatre règles versionnées transforment les traces en 776 alertes brutes ; le tuning gouverné réduit ce volume à 255 alertes, ensuite regroupées en 43 cas et 39 incidents confirmés.

La performance médiane atteint 32 minutes de MTTD, 51 minutes de MTTA et 106 minutes de confinement. Trente-sept incidents sur trente-neuf respectent leur SLA, soit 94,87 %. La couverture télémétrique pondérée est de 92,88 % et la qualité de parsing atteint 99,21 %.

- Résultat principal : réduction de 67,14 % du bruit d'alerte avec une précision des cas de 90,70 %.
- Risque résiduel principal : onboarding incomplet de certains terminaux mobiles et capteurs réseau.
- Priorité detection engineering : faire progresser la couverture des techniques ATT&CK prioritaires de 70 % vers 80 %.
- Dispositif de preuve : règles, tests, exclusions, chronologies, playbooks, modèle Excel et contrôles QA livrés ensemble.

1. Identité et objectifs du projet

HELIOS est un laboratoire personnel de cybersécurité défensive. Il ne représente aucune infrastructure réelle et ne contient aucune donnée personnelle ou information d'entreprise. Les noms, utilisateurs, actifs, incidents et résultats opérationnels sont synthétiques.

Objectifs

- Concevoir une architecture Micro-SOC multi-client cloisonnée et traçable.
- Normaliser des événements Endpoint, Identity, Cloud, Mobile et Network dans un schéma commun.
- Développer et tester des détections Sigma, KQL, Wazuh, Suricata et de corrélation.
- Diagnostiquer des incidents, appliquer des playbooks et mesurer la réponse.
- Gouverner les exclusions et démontrer leur caractère limité, approuvé et réversible.
- Produire une synthèse technique et client à partir d'un modèle Excel avancé.

Critères de succès

Dimension	Critère	Résultat
Tuning	Réduction des alertes ≥ 65 %	67,14 %
Qualification	Précision des cas ≥ 85 %	90,70 %
Détection	MTTD médian ≤ 45 min	32 min
Réponse	Confinement médian ≤ 120 min	106 min
Service	SLA ≥ 90 %	94,87 %
Qualité	Parsing ≥ 99 %	99,21 %
Règles	Tests réussis ≥ 95 %	96,88 %

2. Périmètre multi-client

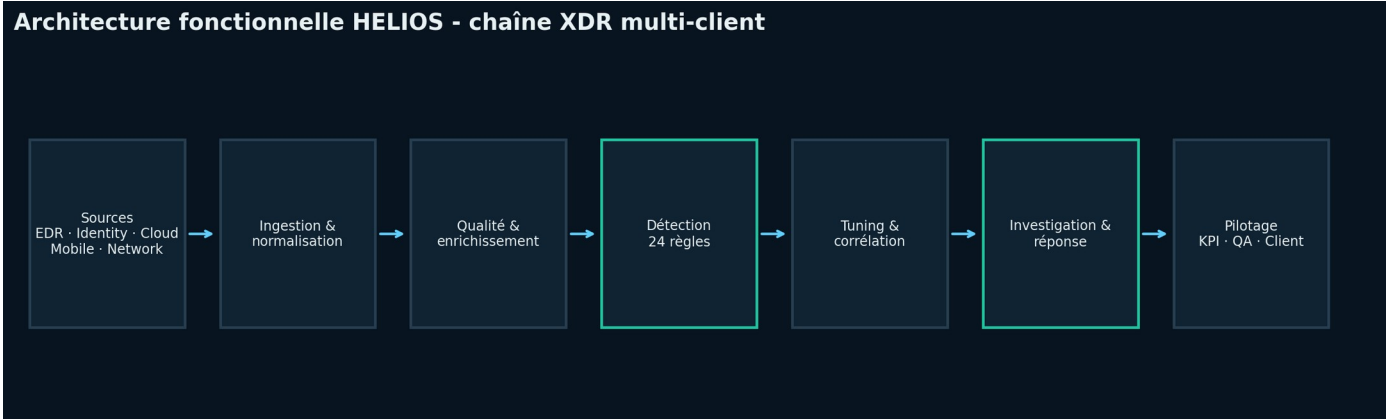
Le portefeuille synthétique couvre trois contextes français contrastés afin de tester la capacité du dispositif à adapter criticité, sources et réponses.

ID	Organisation fictive	Secteur	Ville	Actifs	Tier	Contexte
FR-RET	HexaRetail France	Commerce omnicanal	Paris	760	Advanced	Réseau de points de vente, e-commerce, Microsoft 365, Azure et AWS.
FR-SAN	SantéNova	Santé	Lyon	520	Advanced	Établissements de santé, données sensibles, Microsoft 365 et Azure.
FR-IND	Alcyon Industrie	Industrie	Nantes	510	Advanced	Sites industriels, serveurs, accès distants, Azure et AWS.

Principes de cloisonnement

- Chaque événement, alerte, exclusion, cas et incident possède un client_id valide.
- Les agrégations client sont calculées indépendamment avant consolidation.
- Les exclusions ne peuvent pas s'étendre implicitement à plusieurs clients.
- Les preuves et chronologies restent adressables par identifiants uniques.

3. Architecture fonctionnelle



Chaîne fonctionnelle de collecte, détection, réponse et pilotage.

La chaîne sépare ingestion, qualité, détection, tuning, corrélation, réponse et pilotage. Cette séparation permet de distinguer une absence de visibilité, une mauvaise qualité de parsing, une règle inadéquate et un problème de traitement opérationnel.

Couche	Responsabilité	Preuve
Sources	EDR, identité, cloud, mobile et réseau	data/raw, telemetry_coverage.csv
Normalisation	Schéma canonique et enrichissement actif	events_normalized.csv, data_dictionary.md
Détection	24 règles versionnées	rules/, detection_catalog.csv
Tuning	Seuils, déduplication, exclusions	exclusion_register.csv
Corrélation	Regroupement en campagnes/cas	alerts_tuned.csv
Réponse	Chronologie, playbook, confinement	incidents.csv, playbooks/
Pilotage	KPI, SLA, ATT&CK, QA	Excel, dashboards/, qa/

4. Sources de télémétrie et normalisation

Cinq familles de sources sont représentées : Endpoint via MDE/Wazuh/Sysmon, identité via Entra ID Sign-in & Audit, cloud via Azure Activity et CloudTrail, mobile via Intune/MTD, et réseau via Suricata/Zeek.

Schéma canonique

Champ	Rôle	Exemple
event_id	Identifiant immuable	EVT-0020324
timestamp	Horodatage UTC	2026-06-01T00:30:06Z
client_id	Cloisonnement logique	FR-SAN
asset_id	Lien vers inventaire	AST-01128
actor	Compte ou principal	svc_cloudops@...
domain	Endpoint/Identity/Cloud/Mobile/Network	Endpoint
event_type	Type normalisé	powershell_encoded
severity_hint	Signal de criticité	High
source_system	Traçabilité de génération	PYTHON_OUTPUT

La qualité est contrôlée par taux de parsing, latence P95, couverture attendue/connectée, présence du client_id, intégrité des identifiants et cohérence temporelle.

5. Méthodologie de risque et scénarios de menace

Les scénarios sont construits à partir d'actifs critiques, chemins d'attaque plausibles et conséquences opérationnelles. L'approche s'inspire d'EBIOS Risk Manager pour relier valeurs métier, sources de risque, événements redoutés et scénarios opérationnels.

ID	Scénario	Domaines	Techniques
SCN-01	Phishing et vol d'identité	Identity / Cloud	T1204.002, T1110, T1098.003
SCN-02	Intrusion endpoint et mouvement latéral	Endpoint / Network	T1003.001, T1021.001, T1021.002
SCN-03	Précurseurs de rançongiciel	Endpoint	T1562.001, T1560.001, T1486
SCN-04	Escalade et exfiltration cloud	Cloud	T1098, T1098.001, T1530
SCN-05	Compromission mobile et accès conditionnel	Mobile / Identity	T1625, T1476, T1437, T1621

Priorisation

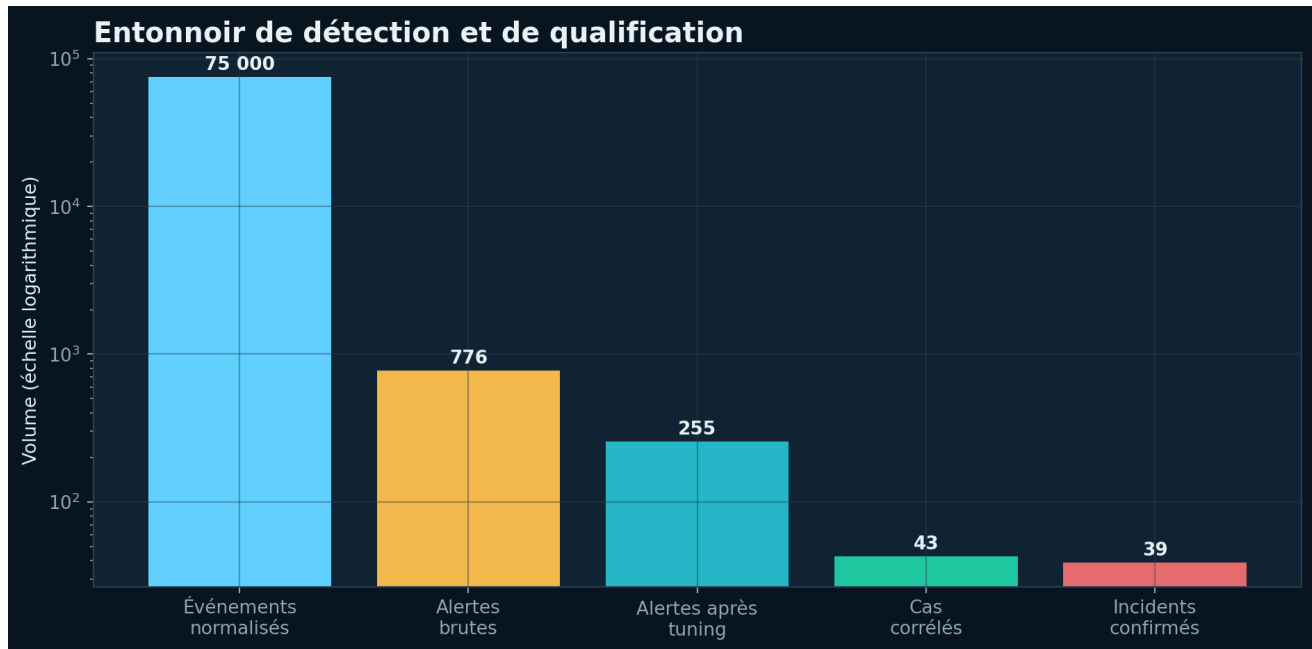
- P1 : impact élevé et prérequis techniques accessibles ; couverture et réponse impératives.
- P2 : scénario significatif nécessitant détection ou enrichissement supplémentaire.
- P3 : surveillance planifiée, après traitement des gaps P1/P2.

6. Detection engineering

Le catalogue comprend 24 règles : 6 Sigma, 6 KQL, 5 corrélations, 4 Suricata et 3 Wazuh. La distribution par domaine est Endpoint 8, Cloud 5, Identity 4, Network 4 et Mobile 3.

Cycle de vie d'une règle

- Hypothèse de détection rattachée à une technique ATT&CK.
- Implémentation portable ou spécifique à la plateforme.
- Test positif primaire et variante.
- Test négatif bénin et de frontière.
- Revue par pair, version, propriétaire et cadence de revue.
- Mesure du volume, des faux positifs et des conversions en incident.
- Tuning limité ou révision de la logique, puis non-régression.



Entonnoir de détection, qualification et corrélation.

7. Catalogue de règles - extrait

ID	Règle	Domaine	Sévérité	ATT&CK	Format
R001	PowerShell encodé ou obfusqué	Endpoint	High	T1059.001	Sigma
R002	Accès suspect à LSASS	Endpoint	Critical	T1003.001	Sigma
R003	Processus enfant inhabituel de Microsoft Office	Endpoint	High	T1204.002	Sigma
R004	Renommage massif de fichiers	Endpoint	Critical	T1486	Sigma
R005	Téléchargement via LOLBin	Endpoint	High	T1105	Sigma
R006	Échecs puis succès d'authentification	Identity	High	T1110	KQL
R007	Connexion géographique impossible	Identity	High	T1078	KQL
R008	Consentement OAuth à privilèges élevés	Cloud	High	T1098.003	KQL
R009	Attribution administrateur global	Cloud	Critical	T1098	KQL
R010	Stockage cloud rendu public	Cloud	High	T1530	KQL
R011	Téléchargement cloud volumineux	Cloud	High	T1530	KQL
R012	Terminal mobile rooté ou jailbreaké	Mobile	High	T1625	Correlation
R013	Application mobile sideloadée à risque	Mobile	Medium	T1476	Correlation
R014	Menace réseau sur terminal mobile	Mobile	High	T1437	Correlation
R015	Tunneling DNS	Network	High	T1071.004	Suricata
R016	Domaine C2 connu	Network	Critical	T1071.001	Suricata

L'intégralité des vingt-quatre règles est fournie dans le répertoire rules/ et le catalogue CSV. Chaque entrée contient propriétaire, version, fréquence de revue, technique ATT&CK, statut et système source.

8. Validation des règles

La campagne contient 96 tests, dont 93 réussis, soit 96.88 %. Les tests couvrent les déclenchements attendus, les variantes et les cas négatifs.

Type de test	Objectif	Décision
positive_primary	Valider le scénario nominal	La règle doit alerter
positive_variant	Tester une variation syntaxique/contextuelle	La règle doit alerter
negative_benign	Éviter un cas métier autorisé	La règle ne doit pas alerter
negative_boundary	Contrôler le seuil ou la frontière	Résultat conforme à la spécification

Le quality gate bloque une règle si son taux de réussite est inférieur à 95 %, si la revue est échue ou si la preuve n'est pas traçable. Les trois échecs résiduels alimentent le backlog de correction à 30 jours.

9. Tuning et gouvernance des exclusions

Le registre contient 8 exclusions approuvées et 2 demandes rejetées. La durée maximale autorisée est de 30 jours.

ID	Règle	Décision	Portée	Début	Fin	Alertes supprimées
EXC-001	R001	Approved	Scoped	2026-05-15	2026-08-15	9
EXC-002	R004	Approved	Scoped	2026-05-20	2026-08-20	2
EXC-003	R017	Approved	Scoped	2026-05-28	2026-07-28	4
EXC-004	R011	Approved	Scoped	2026-06-01	2026-07-31	5
EXC-005	R021	Approved	Scoped	2026-06-03	2026-09-03	5
EXC-006	R024	Approved	Scoped	2026-06-05	2026-08-05	2
EXC-007	R005	Approved	Scoped	2026-06-07	2026-07-20	5
EXC-008	R010	Approved	Scoped	2026-06-10	2026-07-25	7
EXC-009	R002	Rejected	Scoped	2026-06-12	2026-12-31	0
EXC-010	R016	Rejected	Scoped	2026-06-14	2026-12-31	0

Garde-fous

- Rationale, approbateur, champ de correspondance et date d'expiration obligatoires.
- Portée la plus étroite possible : actif, compte de service ou valeur précise.
- Interdiction d'une exclusion globale pour une détection critique.
- Mesure du nombre d'alertes supprimées et revue à l'expiration.
- Test de non-régression après toute modification de règle ou seuil.

10. Corrélation et qualification des cas

Après tuning, les alertes sont regroupées par client, acteur, actif, fenêtre temporelle, campagne synthétique et cohérence de techniques. La corrélation vise à transformer des signaux isolés en hypothèses d'incident actionnables.

Étape	Volume	Taux
Événements normalisés	75 000	100 %
Alertes brutes	776	1,03 % des événements
Alertes après tuning	255	32,86 % des alertes
Cas corrélés	43	16,86 % des alertes qualifiées
Incidents confirmés	39	90,70 % des cas

Quatre cas restent non confirmés. Ils sont conservés comme faux positifs qualifiés ou activité bénigne, afin d'alimenter le tuning sans affaiblir les détections critiques.

11. Processus de réponse à incident

Le processus suit un cycle préparation, détection, analyse, confinement, éradication, récupération et amélioration continue. Chaque incident contient une chronologie complète, un diagnostic, un playbook, une action de confinement et un statut.

Phase	Décision attendue	Preuve
Détection	Le signal est-il fiable et prioritaire ?	Alertes, règle, ATT&CK
Analyse	Quel actif, compte et chemin d'attaque ?	Timeline, enrichissements
Confinement	Quelle action réduit le risque sans aggraver l'impact ?	Action horodatée
Éradication	Quels artefacts, secrets ou persistances retirer ?	Checklist playbook
Récupération	Quand et comment rétablir le service ?	Validation technique/métier
Amélioration	Quelle règle, source ou procédure modifier ?	RCA, backlog, test

12. Playbooks opérationnels

ID	Playbook	Actions clés
PB01	Endpoint Malware	Isoler le poste, préserver les preuves, stopper le processus, réinitialiser les secrets et rechercher le mouvement latéral.
PB02	Identity Compromise	Révoquer sessions/tokens, imposer MFA, réinitialiser le compte, vérifier consentements OAuth et règles de messagerie.
PB03	Cloud Privilege Abuse	Révoquer secrets, retirer rôles, isoler ressources, préserver logs et effectuer une rotation contrôlée.
PB04	Mobile Risk	Mettre le terminal en quarantaine, bloquer l'accès conditionnel, révoquer sessions et déclencher remédiation MDM.
PB05	Ransomware	Isoler endpoints, bloquer IOC, arrêter propagation, préserver preuves, vérifier sauvegardes et restaurer par vagues.

Chaque playbook distingue actions réversibles, actions à fort impact, approbation requise, preuves à conserver et critères de sortie. Cette structure évite une remédiation improvisée et facilite la communication client.

13. Étude de cas incident - INC-2026-001

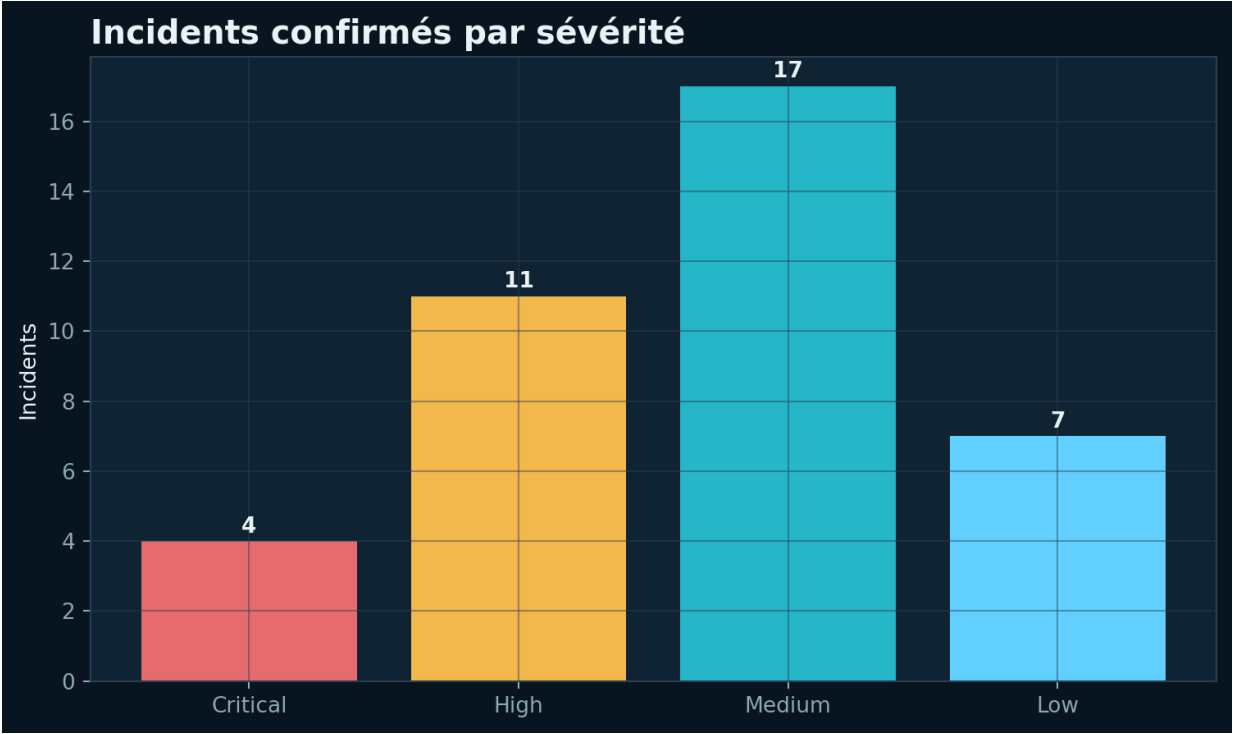
Champ	Valeur
Titre	Escalade et exfiltration cloud
Client	FR-IND
Sévérité	Medium
Actif	AST-01643
Acteur	user028@fr-ind.example
Techniques	T1098;T1098.001;T1530
Cause racine	Secret cloud compromis puis élévation de privilèges et extraction.
Playbook	PB03_Cloud_Privilege_Abuse.md
MTTD	26.0 min
MTTA	57.0 min
Confinement	145.0 min
Remédiation	4.84 h

Chronologie

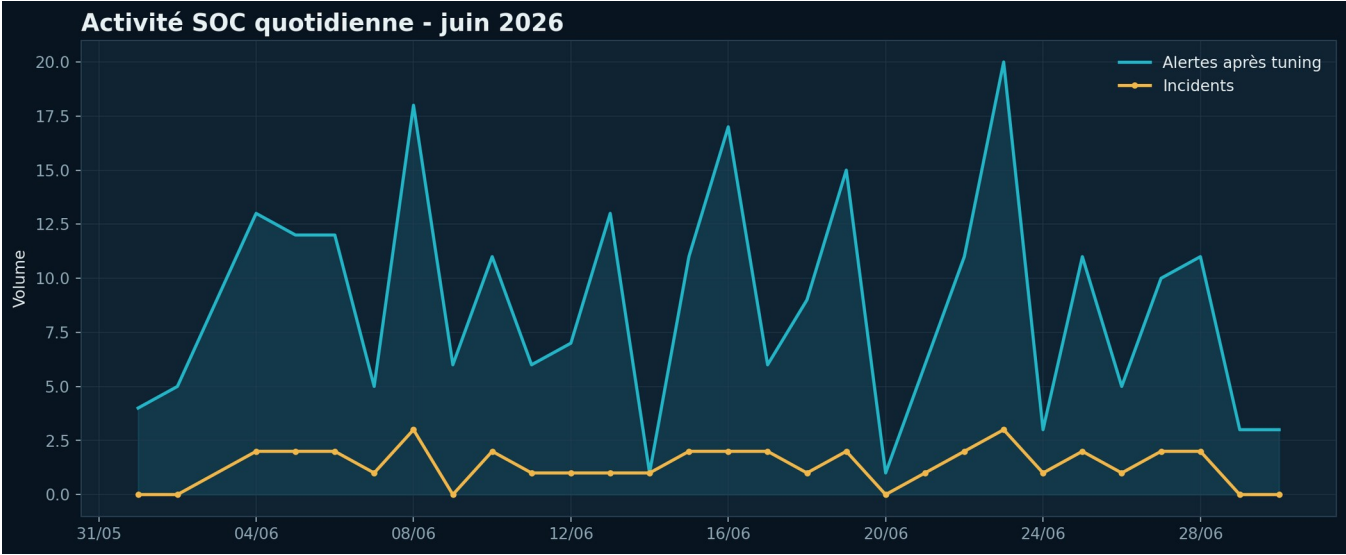
Jalon	Horodatage
Première activité	2026-06-11 02:52:34+00:00
Détection	2026-06-11 03:18:34+00:00
Acquittement	2026-06-11 04:15:34+00:00
Confinement	2026-06-11 06:40:34+00:00
Résolution	2026-06-11 11:30:58+00:00

Diagnostic : un secret cloud compromis a été utilisé pour accroître les privilèges et extraire des données. La réponse applique la révocation, le retrait du rôle, la rotation de secrets, la préservation des traces et la validation des ressources impactées.

14. Résultats opérationnels



Répartition des incidents confirmés par sévérité.



Activité quotidienne des alertes qualifiées et incidents.

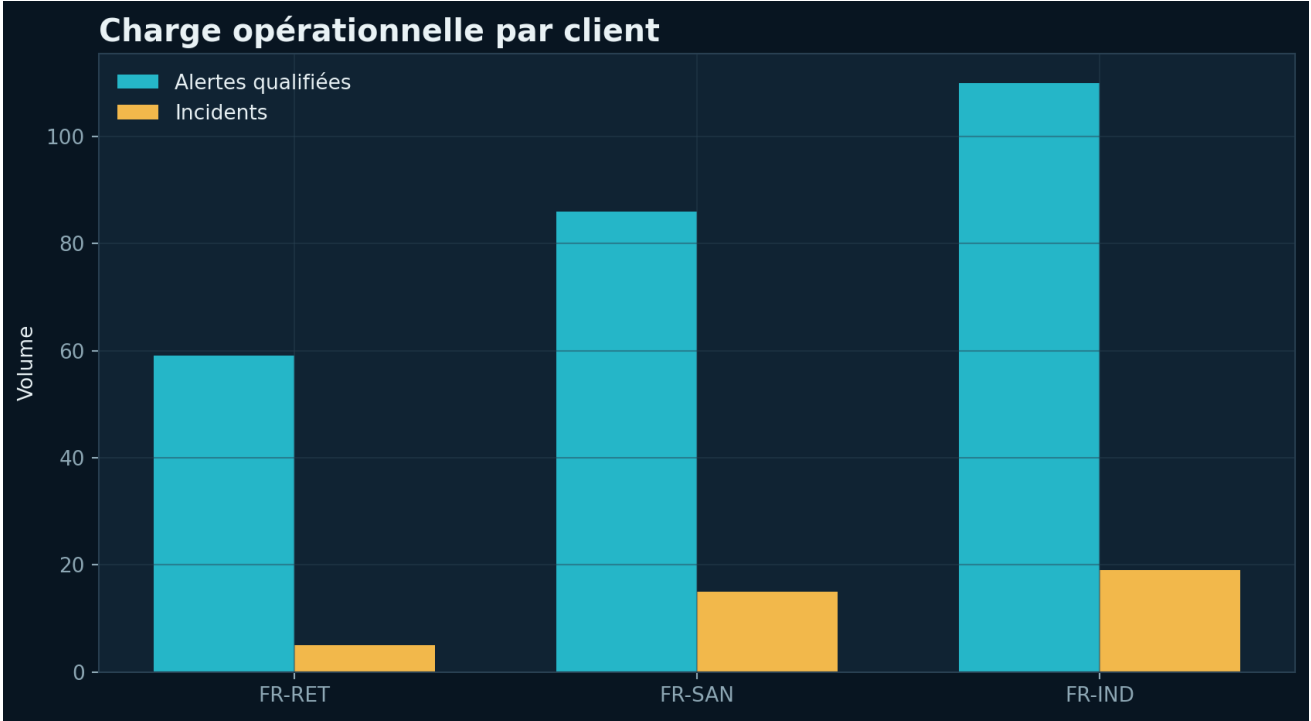
Indicateur	Valeur	Lecture
MTTD médian	32 min	Détection dans la cible de 45 min
MTTA médian	51 min	Acquittement dans la cible de 60 min
Confinement médian	106 min	Sous la cible de 120 min
Remédiation médiane	3,96 h	Sous la cible de 6 h
SLA	94,87 %	37 incidents conformes sur 39

15. Analyse des deux breaches SLA

Incident	Client	Scénario	Sévérité	Confinement	SLA	Écart
INC-2026-008	FR-IND	Compromission mobile et accès conditionnel	Medium	310.0 min	240 min	+70 min
INC-2026-027	FR-IND	Intrusion endpoint et mouvement latéral	Medium	310.0 min	240 min	+70 min

Les deux breaches sont des incidents Medium avec 310 minutes de confinement pour une cible de 240 minutes. La cause de performance retenue est un délai de coordination et de validation avant une action à impact. Les actions correctives sont : matrice d'autorisation pré-approuvée, étapes de confinement réversibles, exercice de table et escalade automatique à 75 % du SLA.

16. Charge opérationnelle par client

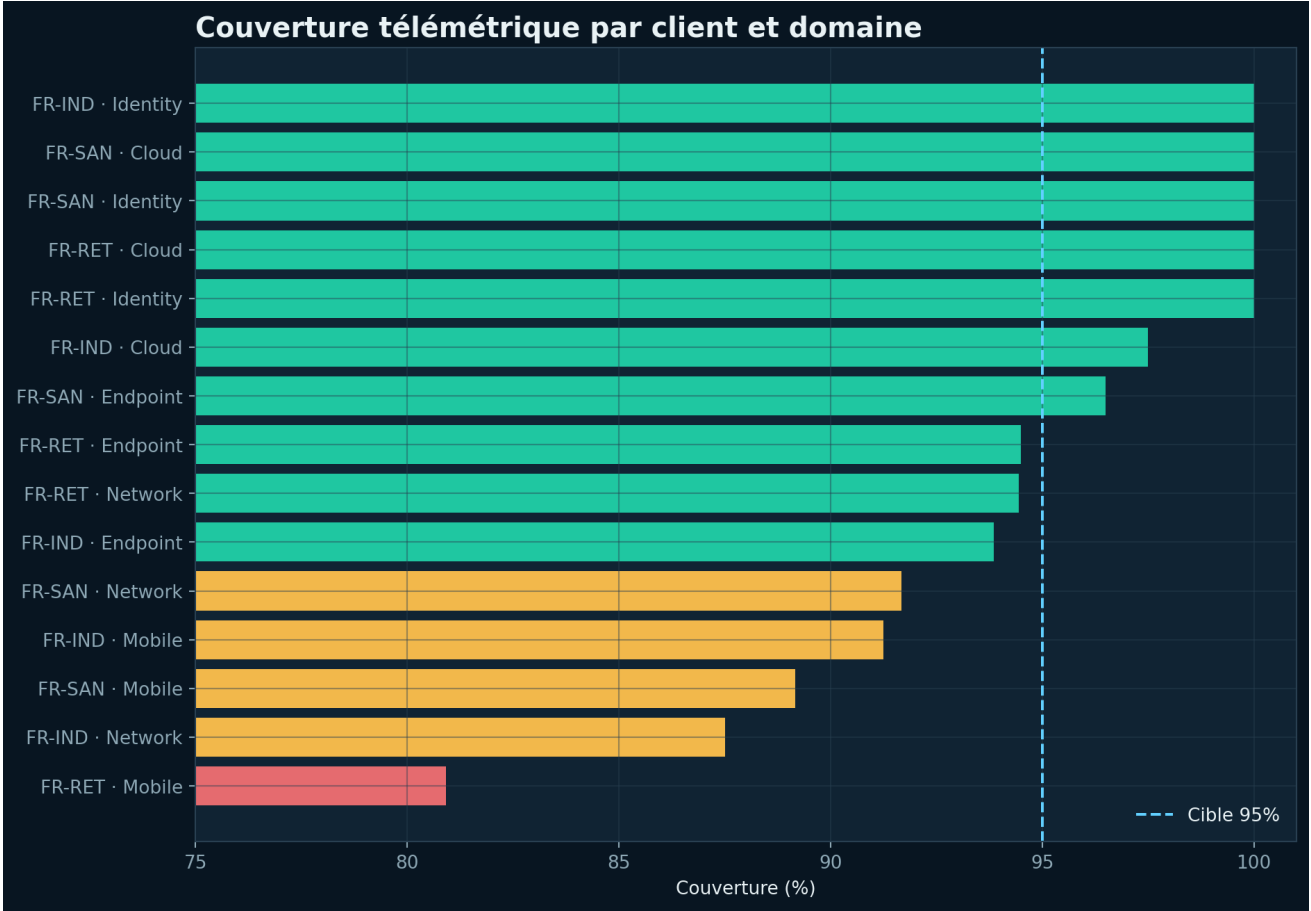


Alertes qualifiées et incidents par client.

Client	Actifs	Alertes qualifiées	Incidents	SLA	Télémétrie
FR-RET	760	59	5	100.0 %	91.0 %
FR-SAN	520	86	15	100.0 %	94.9 %
FR-IND	510	110	19	89.5 %	93.6 %

FR-IND concentre le volume d'incidents le plus élevé. FR-RET présente la couverture téléométrique la plus faible, principalement en raison du domaine Mobile. Les revues de service doivent donc distinguer charge de traitement et visibilité disponible.

17. Couverture télémétrique

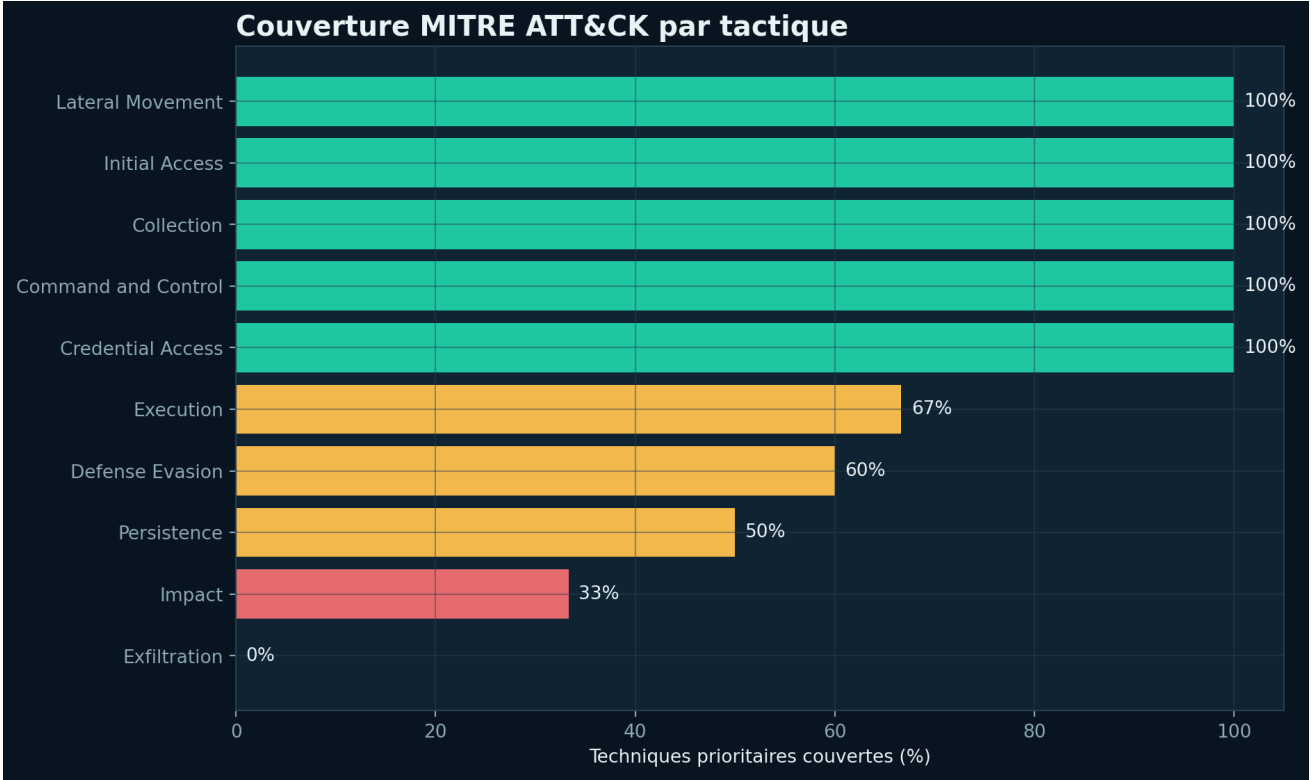


Couverture par client et domaine, avec cible de 95 %.

Client	Domaine	Connecteur	Couverture	Événements	Parsing	Statut
FR-RET	Mobile	Intune + MTD	80.91 %	3344	99.4 %	Watch
FR-SAN	Mobile	Intune + MTD	89.17 %	2375	99.28 %	Watch
FR-IND	Network	Suricata + Zeek	87.5 %	2884	98.89 %	Watch

Le taux de parsing dépasse 98,89 % pour chaque connecteur et atteint 99,21 % pondéré. Le risque principal est donc l'absence partielle de capteurs, et non la transformation des événements reçus.

18. Couverture MITRE ATT&CK



Couverture des techniques prioritaires par tactique.

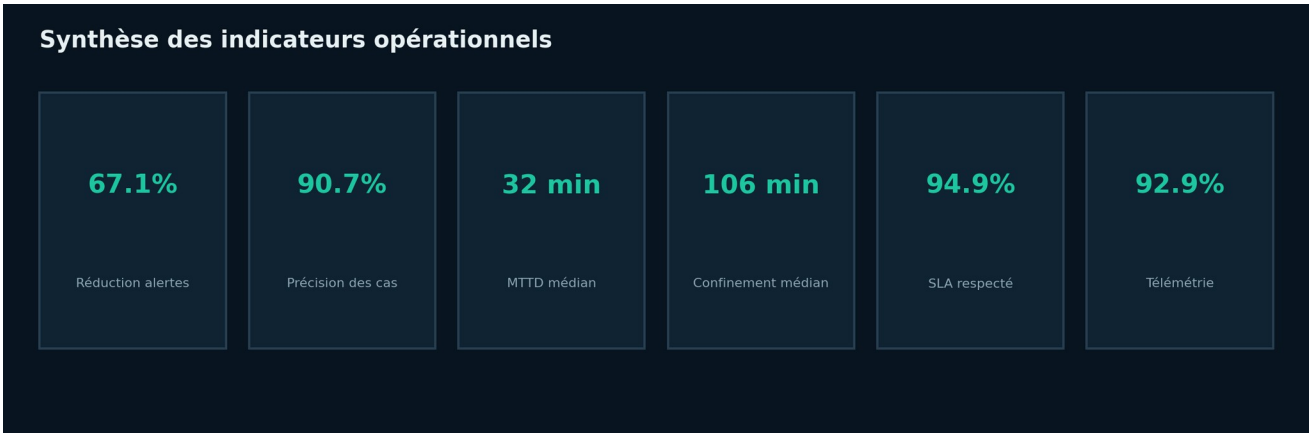
La liste de travail contient 30 techniques prioritaires et 21 techniques couvertes, soit 70 %. Le dénominateur est un backlog de techniques issues des scénarios de risque, pas le catalogue ATT&CK complet.

Technique	Nom	Tactique	Priorité	Statut
T1053.005	Scheduled Task	Persistence	P2	Gap
T1547.001	Run Keys	Persistence	P2	Gap
T1047	WMI	Execution	P2	Gap
T1041	Exfiltration over C2	Exfiltration	P2	Gap
T1550.003	Pass the Ticket	Defense Evasion	P2	Gap
T1218.011	Rundll32	Defense Evasion	P2	Gap
T1136.003	Cloud Account	Persistence	P2	Gap
T1496	Resource Hijacking	Impact	P2	Gap
T1485	Data Destruction	Impact	P2	Gap

19. Modèle Excel avancé

Le workbook comporte 18 feuilles et 17 457 formules. Il sépare hypothèses saisissables, sorties Python et calculs Excel, selon un code couleur bancaire : bleu sur jaune pour les inputs, vert sur vert clair pour les sorties Python et noir pour les formules.

Bloc	Contenu	Fonctions principales
Référentiels	Clients, actifs, télémétrie, règles	COUNTIF, INDEX/MATCH
Opérations	Alertes, incidents, exclusions	IF, RANK.EQ, calculs temps
Pilotage	SLA, KPI, dashboard, brief client	COUNTIFS, SUMIFS, SUMPRODUCT, MEDIAN
Qualité	Tests, réconciliations, seuils	IFERROR, contrôles croisés, conditional formatting



KPI repris dans le dashboard Excel.

Les feuilles volumétriques incluent 8 950 formules sur l'inventaire d'actifs, 5 432 sur les alertes brutes, 1 530 sur les alertes après tuning et 429 sur les incidents. Les résultats du moteur KPI sont réconciliés avec les valeurs attendues.

20. Contrôles QA et acceptation

ID	Contrôle	Résultat
QA-001	3 clients	Pass
QA-002	1 790 actifs	Pass
QA-003	776 alertes brutes	Pass
QA-004	255 alertes qualifiées	Pass
QA-005	39 incidents	Pass
QA-006	Réduction $\geq 65\%$	Pass
QA-007	Précision $\geq 85\%$	Pass
QA-008	MTTD ≤ 45 min	Pass
QA-009	Confinement ≤ 120 min	Pass
QA-010	SLA $\geq 90\%$	Pass
QA-011	Parsing $\geq 99\%$	Pass
QA-012	Tests règles $\geq 95\%$	Pass
QA-013	Aucun actif orphelin	Pass
QA-014	Aucune durée négative	Pass
QA-015	Aucune exclusion approuvée hors politique	Pass

Le pipeline se réexécute avec ``python run_pipeline.py``. Le test automatisé ``pytest -q`` retourne un test réussi. Le manifeste SHA-256 final permet de contrôler l'intégrité de chaque fichier livré.

21. Communication technique et client

Le dispositif fournit deux niveaux de documentation. Le niveau technique décrit architecture, données, détections, exclusions, incidents et preuves. Le niveau client limite la revue à quelques décisions : risque, tendance, service, gaps de visibilité et actions datées.

Audience	Message	Format
Analyste SOC	Chronologie, hypothèses, preuves, prochaines actions	Incident report
Detection Engineer	Performance par règle, tests, faux positifs, ATT&CK	Catalogue + evidence
Manager SOC	MTTD/MTTA/confinement/SLA, charge, backlog	Dashboard Excel
Client	Risque, incidents significatifs, couverture, décision	Brief mensuel 10 min
Audit/QA	Traçabilité, réconciliation, intégrité	QA report + hashes

La synthèse client est calculée par client dans le workbook : actifs, alertes qualifiées, incidents, sévérités, conformité SLA, couverture télémétrique, gap principal, action recommandée et statut exécutif.

22. Reproductibilité et arborescence

Répertoire	Rôle
data/	Sources synthétiques, référentiels et sorties traitées
src/helios_soc/	Pipeline Python
rules/	Sigma, KQL, Wazuh, Suricata, corrélations
playbooks/	Procédures de réponse
notebooks/	Analyses exécutables
model/	Workbook Excel
dashboards/	KPI et graphiques
docs/	Architecture, méthodologie, spécifications et rapport
evidence/	Tests de règles
qa/	Contrôles, previews et manifestes
website/	Données et prompt du one-pager

La graine de génération et les règles de calcul sont fixées dans le code. Les jeux de données sont volontairement suffisamment volumineux pour tester les agrégations, tout en restant exécutables localement.

23. Feuille de route 30/60/90 jours

Horizon	Priorités	Critère de sortie
30 jours	Onboarding Mobile/Network, correction des trois tests, alerte à 75 % du SLA	Télémétrie ≥ 95 %, tests ≥ 99 %
60 jours	Règles pour gaps ATT&CK P1, exercices PB03/PB04, revue exclusions	ATT&CK ≥ 80 %, zéro exclusion échue active
90 jours	Enrichissement automatisé, actions réversibles orchestrées, revue de service	MTTD < 30 min, SLA ≥ 97 %

La feuille de route évite d'augmenter artificiellement le nombre de règles avant de corriger la visibilité et la qualité. Les nouveaux cas d'usage doivent être justifiés par les scénarios prioritaires et accompagnés de tests positifs/négatifs.

24. Limites et précautions d'interprétation

- Les événements et comportements sont synthétiques ; ils ne reproduisent pas toute la variabilité d'un SI réel.
- Les produits éditeurs sont représentés par des formats et concepts, sans connexion à un tenant de production.
- Les métriques de temps sont simulées et servent à valider les calculs, SLA et décisions.
- La couverture ATT&CK porte sur une liste de techniques prioritaires, pas sur la totalité des matrices.
- Le taux de précision ne remplace pas une validation sur historique réel et feedback analyste.
- Toute automatisation de confinement en production exigerait approbation, rollback, tests et contrôle d'impact.

Ces limites sont explicites afin de préserver la crédibilité du projet : la méthodologie et les artefacts sont concrets, mais les résultats ne prétendent pas décrire un service réel.

25. Conclusion

HELIOS démontre une chaîne cohérente de détection et réponse : architecture multi-client, collecte, normalisation, règles multi-technologies, tuning gouverné, corrélation, investigation, remédiation, documentation et pilotage. Les résultats sont traçables des données sources jusqu'au dashboard et contrôlés par formules et tests.

Les principaux enseignements sont la valeur de la corrélation multi-source, la nécessité de gouverner les exclusions et l'importance de traiter la couverture télémétrique avant d'élargir le catalogue de règles. Le backlog 30/60/90 jours traduit ces enseignements en décisions mesurables.

Bibliographie méthodologique

Organisme	Référence	URL
ANSSI	Recommandations de sécurité pour l'architecture d'un système de journalisation	https://messervices.cyber.gouv.fr/guides/recommandations-de-securite-pour-larchitecture-dun-systeme-de-journalisation
ANSSI	EBIOS Risk Manager	https://messervices.cyber.gouv.fr/guides/la-methode-ebios-risk-manager-le-guide
CNIL	Sécurité : tracer les opérations	https://www.cnil.fr/fr/securite-tracer-les-operations
MITRE	ATT&CK Enterprise	https://attack.mitre.org/matrices/enterprise/
MITRE	ATT&CK Mobile	https://attack.mitre.org/matrices/mobile/
NIST	SP 800-61 Rev. 3	https://csrc.nist.gov/pubs/sp/800/61/r3/final
SigmaHQ	Sigma Rules Specification	https://sigmahq.io/sigma-specification/specification/sigma-rules-specification.html
Microsoft	Defender XDR Advanced Hunting	https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-overview
Wazuh	Architecture	https://documentation.wazuh.com/current/getting-started/architecture.html
Suricata	Rules format	https://docs.suricata.io/en/latest/rules/intro.html

Annexe A - Catalogue complet des règles

ID	Nom	Domaine	Sévérité	Technique	Tactique	Format
R001	PowerShell encodé ou obfusqué	Endpoint	High	T1059.001	Execution	Sigma
R002	Accès suspect à LSASS	Endpoint	Critical	T1003.001	Credential Access	Sigma
R003	Processus enfant inhabituel de Microsoft Office	Endpoint	High	T1204.002	Execution	Sigma
R004	Renommage massif de fichiers	Endpoint	Critical	T1486	Impact	Sigma
R005	Téléchargement via LOLBin	Endpoint	High	T1105	Command and Control	Sigma
R006	Échecs puis succès d'authentification	Identity	High	T1110	Credential Access	KQL
R007	Connexion géographiquement impossible	Identity	High	T1078	Defense Evasion	KQL
R008	Consentement OAuth à privilèges élevés	Cloud	High	T1098.003	Persistence	KQL
R009	Attribution administrateur global	Cloud	Critical	T1098	Persistence	KQL
R010	Stockage cloud rendu public	Cloud	High	T1530	Collection	KQL
R011	Téléchargement cloud volumineux	Cloud	High	T1530	Collection	KQL
R012	Terminal mobile rooté ou jailbreaké	Mobile	High	T1625	Defense Evasion	Correlation
R013	Application mobile sideloadée à risque	Mobile	Medium	T1476	Initial Access	Correlation
R014	Menace réseau sur terminal mobile	Mobile	High	T1437	Collection	Correlation
R015	Tunneling DNS	Network	High	T1071.004	Command and Control	Suricata
R016	Domaine C2 connu	Network	Critical	T1071.001	Command and Control	Suricata
R017	Rafale SMB latérale	Network	High	T1021.002	Lateral Movement	Suricata
R018	RDP depuis une source rare	Network	Medium	T1021.001	Lateral Movement	Suricata
R019	Désactivation de l'isolation EDR	Endpoint	High	T1562.001	Defense Evasion	Wazuh
R020	Altération d'un agent de sécurité	Endpoint	Critical	T1562.001	Defense Evasion	Wazuh
R021	Clé API depuis région inhabituelle	Cloud	High	T1098.001	Persistence	Wazuh
R022	Rafale de demandes MFA	Identity	High	T1621	Credential Access	Correlation
R023	Authentification legacy sensible	Identity	Medium	T1078	Defense Evasion	Correlation
R024	Archive avant exfiltration	Endpoint	Medium	T1560.001	Collection	Sigma

Annexe B - Connecteurs de télémétrie

Client	Domaine	Connecteur	Attendus	Connectés	Couverture	Événement s	Parsing	Latence P95
FR-RET	Endpoint	MDE/Wazuh + Sysmon	490	463	94.49 %	12673	99.21 %	83.2 s
FR-RET	Identity	Entra ID Sign-in & Audit	1	1	100.0 %	6354	99.23 %	83.6 s
FR-RET	Cloud	Azure Activity + CloudTrail	50	50	100.0 %	5032	99.26 %	82.4 s
FR-RET	Mobile	Intune + MTD	220	178	80.91 %	3344	99.4 %	82.8 s
FR-RET	Network	Suricata + Zeek	18	17	94.44 %	4230	99.31 %	82.3 s
FR-SAN	Endpoint	MDE/Wazuh + Sysmon	370	357	96.49 %	8708	99.04 %	83.1 s
FR-SAN	Identity	Entra ID Sign-in & Audit	1	1	100.0 %	4387	99.32 %	83.8 s
FR-SAN	Cloud	Azure Activity + CloudTrail	30	30	100.0 %	3574	98.94 %	83.9 s
FR-SAN	Mobile	Intune + MTD	120	107	89.17 %	2375	99.28 %	81.5 s
FR-SAN	Network	Suricata + Zeek	12	11	91.67 %	2901	99.03 %	82.8 s
FR-IND	Endpoint	MDE/Wazuh + Sysmon	390	366	93.85 %	8582	99.3 %	83.0 s
FR-IND	Identity	Entra ID Sign-in & Audit	1	1	100.0 %	4209	99.14 %	83.5 s
FR-IND	Cloud	Azure Activity + CloudTrail	40	39	97.5 %	3448	99.42 %	81.8 s
FR-IND	Mobile	Intune + MTD	80	73	91.25 %	2299	99.3 %	83.1 s
FR-IND	Network	Suricata + Zeek	16	14	87.5 %	2884	98.89 %	81.9 s