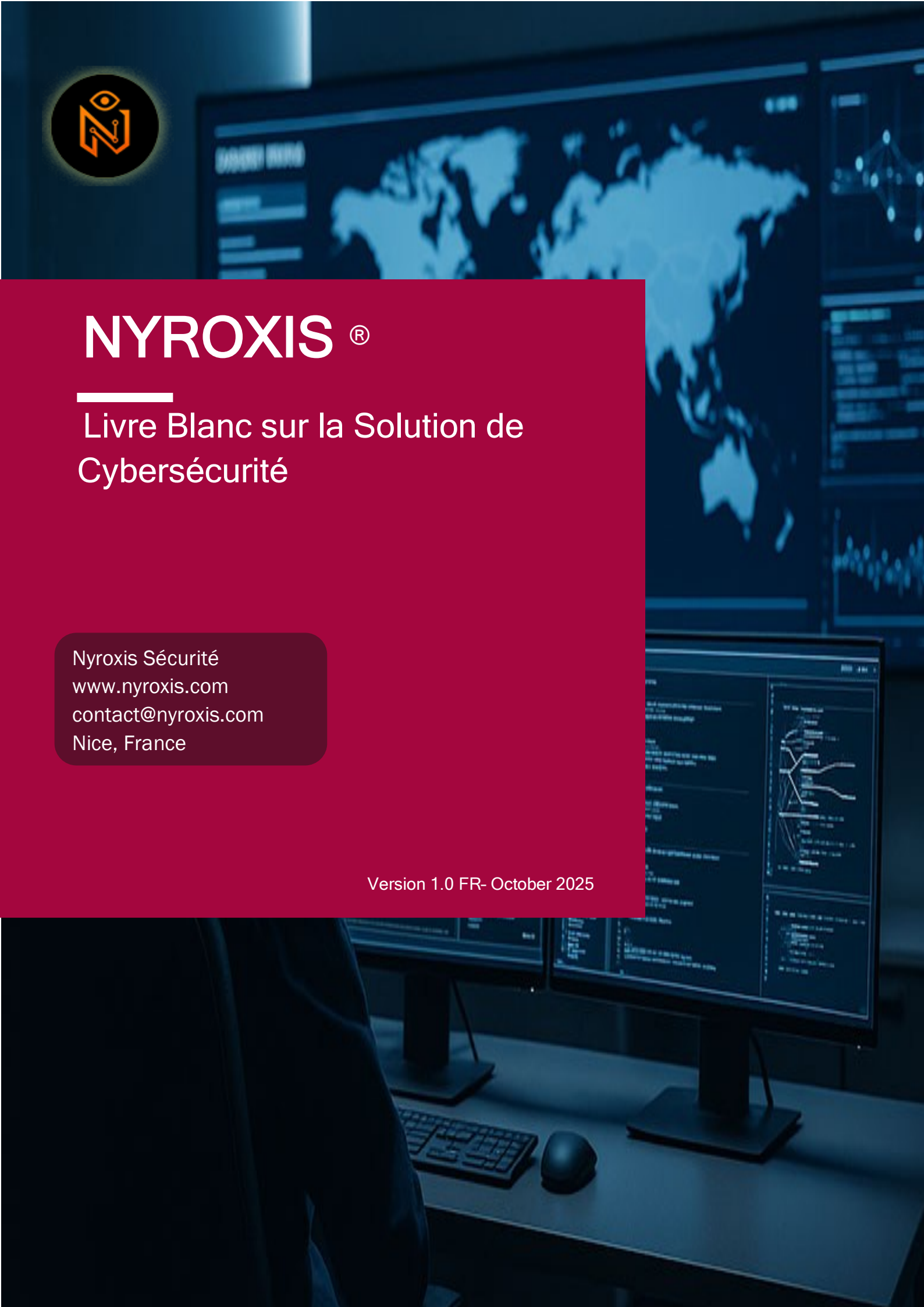


NYROXIS ®

Livre Blanc sur la Solution de Cybersécurité

Nyroxis Sécurité
www.nyroxis.com
contact@nyroxis.com
Nice, France

Version 1.0 FR- October 2025

Table des matières

La nouvelle réalité de la cybersécurité

Les menaces actuelles

Les cybermenaces dépassent aujourd'hui largement le périmètre des pare-feu d'entreprise. Les attaquants ciblent de plus en plus les appareils personnels des dirigeants, administrateurs, magistrats, médecins et autres professionnels dont les décisions sont stratégiques. Un simple ordinateur portable compromis à domicile, une tablette partagée ou un appareil familial non sécurisé peut devenir une porte d'entrée silencieuse vers des infrastructures critiques.

Le point aveugle

Les organisations investissent massivement dans la cybersécurité d'entreprise — pare-feu, SOC, plateformes de supervision avancées — mais ces protections s'arrêtent souvent aux frontières du bureau. La vie numérique personnelle des individus clés reste exposée, créant un point aveugle que les attaquants exploitent. Ce déséquilibre entraîne des pertes financières, une exposition réglementaire et des atteintes à la réputation.

La solution Nyroxis

Nyroxis comble cette faille grâce à un agent de sécurité léger, discret et capable de fonctionner hors ligne, associé à un tableau de bord intelligent. Il surveille silencieusement les terminaux, préserve des preuves à valeur légale et corrèle les activités suspectes sans dépendre d'une connectivité permanente. La solution est conçue pour compléter — et non remplacer — les défenses d'entreprise existantes, en étendant la protection là où elle est la plus nécessaire.

Avantages clés

- **Protection des décideurs et de leur entourage** : sécurise les personnes stratégiques ainsi que leur environnement personnel contre les intrusions ciblées.
- **Conformité & Assurance** : alignement sur les standards et directives internationales, dont le RGPD, la directive NIS2 et l'ISO/IEC 27001.
- **Préparation à la réponse judiciaire** : journaux inviolables et preuves fiables pour accélérer les enquêtes.
- **Simplicité opérationnelle** : intégration fluide dans les opérations de sécurité existantes, sans surcharge.
- **Impact métier** : réduction des coûts liés aux incidents, accélération de la réponse et extension des principes Zero Trust jusqu'au périmètre humain.

Conclusion

Nyroxis transforme le maillon le plus faible en une surface maîtrisée. En protégeant les terminaux personnels et en comblant le fossé entre domicile et entreprise, il apporte à la fois une confiance réglementaire et une valeur métier mesurable. Nyroxis n'est pas seulement un produit, mais une couche stratégique de défense pour les organisations qui ne peuvent se permettre de laisser des angles morts.

Introduction & Contexte

La cybersécurité à la croisée des chemins

Chaque semaine apporte son lot de gros titres : violations massives de données, campagnes de rançongiciels, ou attaques sophistiquées menées par des États. Malgré des milliards investis dans des pare-feu avancés, des plateformes SIEM et des centres opérationnels de sécurité (SOC), les attaquants continuent de réussir. La question n'est plus de savoir *si* une violation se produira, mais *quand* et *où*.

Le point d'entrée caché

Même si les infrastructures d'entreprise sont fortement protégées, les attaques commencent souvent là où les politiques de sécurité s'arrêtent : à domicile. L'ordinateur personnel d'un dirigeant, la tablette familiale connectée au même Wi-Fi qu'un administrateur, ou la navigation nocturne d'un juge ou d'un avocat peuvent tous devenir des vecteurs d'attaque. Ces appareils sont rarement surveillés avec le même niveau de rigueur que les actifs de l'entreprise, créant ainsi une fenêtre de vulnérabilité.

L'impact humain

Derrière chaque statistique se cache une histoire personnelle : des familles découvrant leurs comptes bancaires vidés, des professionnels exposés au chantage, ou des agents publics dont la crédibilité est sapée par un simple appareil compromis. La cybersécurité ne consiste pas seulement à protéger des données ; il s'agit de préserver la confiance, la dignité et la continuité des décisions critiques.

Pourquoi une nouvelle approche est nécessaire

Les antivirus traditionnels et les systèmes SIEM d'entreprise n'ont pas été conçus pour cette réalité. Optimisés pour les environnements corporatifs, ils échouent à couvrir la sphère personnelle dans laquelle vivent et travaillent des individus sensibles. Combler cette faille exige une solution légère, discrète et capable de fonctionner de manière fiable même hors ligne — une solution qui apporte une défense de niveau entreprise dans l'espace numérique personnel.

Notre engagement

Nyroxis a été créé pour relever directement ce défi. En étendant la protection au-delà du bureau et jusque dans la vie personnelle des individus sensibles, il offre aux organisations la couche manquante dont elles ont besoin pour prévenir les violations, réduire les risques et maintenir la confiance dans un monde numérique de plus en plus hostile.

Constat du problème

L'élargissement de la surface d'attaque

Les investissements en cybersécurité ont renforcé les infrastructures des entreprises, mais les attaquants ne sont pas découragés. Au contraire, ils s'adaptent en recherchant le point d'entrée le plus faible : la vie numérique personnelle des dirigeants, administrateurs et professionnels. Les réseaux domestiques, les appareils familiaux et les terminaux personnels non gérés sont devenus la nouvelle surface d'attaque.

Pourquoi les outils existants sont insuffisants

Les solutions de sécurité traditionnelles — antivirus, EDR et SIEM d'entreprise — sont conçues pour des environnements de bureau contrôlés. Elles manquent de visibilité sur les appareils personnels et ne peuvent surveiller de manière fiable les activités en dehors du périmètre corporatif. Ce point aveugle laisse les organisations vulnérables à des intrusions qui commencent loin du bureau mais se terminent au cœur du réseau.

Conséquences de l'inaction

- **Pertes financières** : un seul appareil compromis peut entraîner des violations coûtant plusieurs millions.
- **Atteinte à la réputation** : des incidents impliquant des dirigeants ou des agents publics érodent rapidement la confiance et la crédibilité.
- **Exposition réglementaire** : les lois sur la protection des données et les directives de cybersécurité exigent des organisations qu'elles démontrent leur diligence raisonnable sur l'ensemble de leur écosystème — y compris les terminaux ciblés par les attaquants.
- **Coût humain** : au-delà des chiffres, les violations affectent des familles, des carrières et la sécurité des personnes occupant des rôles critiques.

Le problème central

Il existe un écart critique entre les défenses de niveau entreprise et la vie numérique quotidienne de ceux qui dirigent, décident et protègent. Les attaquants savent que cet écart existe — et ils l'exploitent. Les organisations ne disposent actuellement d'aucune solution efficace, légère et respectueuse de la vie privée pour le combler.

Notre solution – Nyroxis

Combler la faille

Nyroxis a été conçu pour répondre à la vulnérabilité la plus négligée de la cybersécurité moderne : les appareils personnels et les réseaux domestiques des individus occupant des fonctions sensibles. En combinant un agent léger avec un tableau de bord intelligent, Nyroxis étend la défense de niveau entreprise à la sphère personnelle — là où les attaquants commencent le plus souvent.

Principes fondamentaux

- **Léger & Discret** : fonctionne silencieusement en arrière-plan avec une utilisation minimale des ressources, le rendant invisible aux attaquants et non intrusif pour les utilisateurs.
- **Capable hors ligne** : opère de manière fiable sans connectivité permanente, garantissant que les preuves sont préservées même lorsque les appareils sont isolés.
- **Surveillance à valeur judiciaire** : capture et chiffre les événements de sécurité afin de fournir des journaux inviolables et recevables devant les tribunaux.
- **Conception complémentaire** : fonctionne aux côtés des défenses existantes (AV, EDR, SIEM), en ajoutant une couche essentielle plutôt qu'en remplaçant les outils actuels.

Comment cela fonctionne

1. **Nyroxis Agent** – Déployé sur les appareils personnels, il observe en continu les processus, connexions et changements système.
2. **Nyroxis Dashboard** – Fournit une visibilité en temps réel, corrèle les événements suspects et génère des rapports simplifiés pour les décideurs et les équipes de sécurité.
3. **Cadre de licence & sécurité** – Garantit l'authenticité, l'intégrité et la confiance via un ancrage matériel (HWID) et une validation cryptographique.

Valeur unique

- Protège les dirigeants, administrateurs et professionnels contre les attaques ciblées à domicile.
- Réduit le risque de violation et la responsabilité réglementaire en comblant la faille de sécurité la plus critique.
- Améliore la réponse aux incidents grâce à des données fiables et prêtes pour l'analyse judiciaire.
- Offre une conception respectueuse de la vie privée, alignée sur les principes mondiaux de protection des données.

En une phrase

Nyroxis n'est pas un outil d'entreprise de plus — c'est la couche stratégique manquante qui protège les personnes là où la cybersécurité traditionnelle s'arrête.

Architecture & Technologie

Aperçu

Nyroxis est conçu comme une plateforme de sécurité modulaire et légère qui combine la surveillance des terminaux avec un tableau de bord central. Son architecture est pensée pour être simple à déployer, discrète dans son fonctionnement et robuste en matière d'intégrité judiciaire.

Composants clés

1. Nyroxis Agent
   - Installé sur les terminaux personnels (Windows, Linux ; macOS à venir).
   - Collecte de la télémétrie : processus, connexions, événements système.
   - Stocke les journaux sous format chiffré, résistant aux manipulations.
   - Fonctionne avec une consommation minimale de ressources, invisible pour les attaquants.
2. Nyroxis Dashboard
   - Interface moderne basée sur Windows (WPF) pour les équipes de sécurité et les utilisateurs sensibles.
   - Affiche des informations en temps réel, des résultats de corrélation et des données à valeur judiciaire.
   - Supporte la recherche dans les journaux, le filtrage par gravité, la visualisation et l'export (PDF/CSV).
   - Système d'alertes intégré pour les événements critiques.
3. Moteur de corrélation
   - Identifie les schémas suspects dans les événements collectés.
   - Prend en charge la détection basée sur des règles et des scénarios.
   - Conçu pour une future intégration d'IA et de Machine Learning.
4. Cadre de licence & sécurité
   - Licences liées au matériel (HWID).
   - Cryptographie avancée (signatures Ed25519, journaux chiffrés en AES).
   - Validation hors ligne pour garantir la résistance aux falsifications.

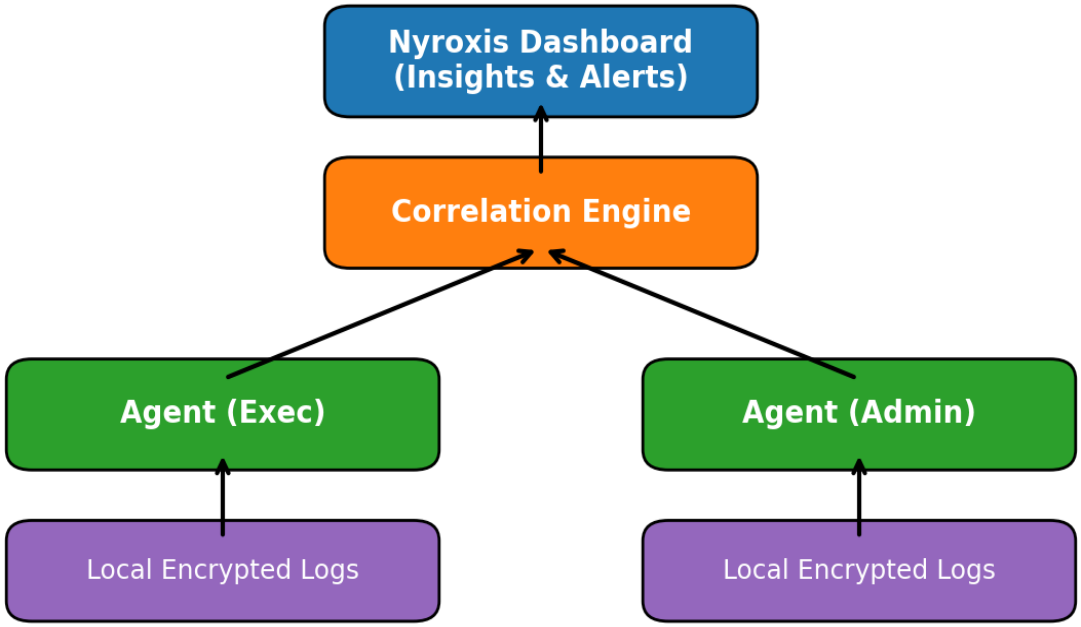
Pile technologique

- **Agent** : C# (.NET 8), Python (pour l'édition open source).
- **Tableau de bord** : WPF, LiveCharts/SkiaSharp pour la visualisation, SQLite pour le stockage local.
- **Cryptographie** : hachage SHA-256, signatures Ed25519, chiffrement AES-256.
- **Vision multiplateforme** : Windows (actuel), macOS/Linux (feuille de route).

Principes de conception

- **Simplicité** : déploiement facile, maintenance minimale.
- **Discrétion** : invisible pour les attaquants, non intrusif pour les utilisateurs.
- **Intégrité judiciaire** : les journaux restent fiables et recevables devant les tribunaux.
- **Complémentarité** : fonctionne avec, et non contre, les investissements existants en AV/EDR/SIEM.

Schéma d'architecture



- **Stockage à valeur judiciaire** (résistant aux falsifications)
- **Fonctionnement hors ligne** (Offline-Capable)

Résumé

L'architecture de Nyroxis garantit une visibilité continue, une préparation judiciaire et une conception respectueuse de la vie privée.
Sa structure modulaire permet aux entreprises d'évoluer d'un petit nombre de terminaux protégés jusqu'à des réseaux entiers de holdings — sans sacrifier ni la simplicité ni les performances.

Domaines d'application – Là où Nyroxis apporte une réelle valeur

Les menaces cyber évoluent en exploitant les angles morts. Nyroxis a été conçu pour combler les failles les plus critiques, là où les outils de cybersécurité traditionnels n'ont pas de portée. Les scénarios suivants illustrent les cas dans lesquels la solution crée un impact immédiat :

1. Protection des dirigeants et de leur famille

Les dirigeants, administrateurs et personnalités publiques sont des cibles de grande valeur. Leurs proches, souvent moins sensibilisés à la sécurité, deviennent des points d'entrée indirects pour les attaquants. Nyroxis garantit que les ordinateurs personnels, tablettes et appareils domestiques partagés sont surveillés de manière silencieuse, réduisant ainsi le risque qu'un seul compromis personnel ne se transforme en brèche au sein de l'entreprise.

2. Professions sensibles

Juges, policiers, avocats et administrateurs SOC détiennent des informations sensibles et exercent une influence sur des opérations critiques. Un compromis dans leur vie numérique personnelle peut conduire à du chantage, à des atteintes à la réputation ou même à une manipulation de la justice. Nyroxis protège ces individus grâce à une surveillance discrète et à valeur judiciaire, qui préserve à la fois leur vie privée et leur crédibilité professionnelle.

3. Groupes multinationaux

Les grandes entreprises avec une direction distribuée à l'international font face à un risque supplémentaire : une sécurité des appareils personnels incohérente d'un pays à l'autre. Les attaquants savent que cibler l'ordinateur portable personnel d'un cadre régional peut ouvrir un accès à l'infrastructure mondiale. Nyroxis fournit une couche de protection unifiée qui s'étend sans difficulté à travers les pays et filiales, fermant ainsi les maillons les plus faibles.

4. Déploiements organisationnels

Nyroxis ne se limite pas aux profils à haute responsabilité. Les entreprises peuvent l'utiliser pour des **simulations d'attaque interne (red-team)**, des programmes de sensibilisation ou la surveillance des risques liés aux initiés. Sa conception légère permet aux responsables de la sécurité d'étendre la visibilité aux environnements que les SIEM ou EDR traditionnels ne couvrent pas, créant ainsi une vision globale des risques de l'entreprise.

Résumé
Des salles de conseil aux tribunaux, des holdings multinationaux aux foyers familiaux, Nyroxis étend la protection au-delà du périmètre de l'entreprise. En suivant les individus partout où ils vivent et travaillent, il transforme les espaces les plus vulnérables en environnements surveillés et contrôlés — sans perturber la vie quotidienne.

Bénéfices & Proposition de valeur

Transformer la sécurité en valeur stratégique

La cybersécurité n'est pas seulement une préoccupation technique — c'est une question de continuité des activités, de réputation et de confiance. Nyroxis apporte de la valeur à tous les niveaux de l'organisation, du centre opérationnel de sécurité à la salle du conseil d'administration, jusqu'à l'utilisateur individuel.

1. Pour les responsables de la sécurité (CISO & équipes SOC)

- **Réduction de la surface d'attaque** : étend la visibilité aux appareils personnels des dirigeants et du personnel sensible, éliminant un angle mort fréquent.
- **Preuves à valeur judiciaire** : journaux sécurisés et inviolables qui accélèrent la réponse aux incidents et soutiennent les procédures légales.
- **Adaptation opérationnelle** : conçu pour s'intégrer aux flux de travail existants du SOC sans complexité supplémentaire.

2. Pour la direction générale (CEO & Conseil d'administration)

- **Protection des actifs immatériels** : préserve la réputation de la marque, la confiance des investisseurs et la qualité des décisions stratégiques.
- **Réduction de l'exposition au risque** : limite le potentiel de brèches coûteuses provenant des terminaux personnels.
- **Diligence démontrée** : prouve aux régulateurs, actionnaires et partenaires que la direction bénéficie d'une sécurité proactive.

3. Pour les utilisateurs sensibles (dirigeants, magistrats, agents publics)

- **Protection transparente** : sécurité légère, invisible et non intrusive, ne nécessitant aucune expertise technique.
- **Respect de la vie privée** : basé sur le chiffrement et une collecte minimale des données pour garantir la confidentialité personnelle.
- **Tranquillité d'esprit** : certitude que les appareils personnels et les environnements familiaux sont protégés contre les menaces sophistiquées.

L'avantage stratégique

Nyroxis transforme la sécurité personnelle en résilience organisationnelle. En protégeant les personnes les plus critiques, il prévient les brèches, accélère les enquêtes et réduit les coûts — tout en renforçant la confiance à tous les niveaux de l'entreprise.

Conformité & Normes

Une sécurité alignée sur les réglementations mondiales

Dans l'environnement réglementaire actuel, la cybersécurité ne se limite pas à la protection — elle concerne également la conformité et la responsabilité. Les organisations doivent démontrer qu'elles gèrent activement les risques à tous les niveaux de leur écosystème numérique, y compris sur les terminaux personnels exploités par les attaquants. Nyroxis a été développé avec ces exigences à l'esprit, garantissant que les entreprises puissent à la fois renforcer leurs défenses et prouver leur conformité.

Cadres européens

- **RGPD (Règlement général sur la protection des données)** : Nyroxis respecte les principes de minimisation des données, chiffre toutes les télémétries collectées et veille à ce que les informations personnelles ne soient jamais exposées inutilement.
- **Directive NIS2** : fournit une visibilité continue et une préparation aux incidents sur les terminaux personnels, aidant ainsi les organisations à répondre aux nouvelles obligations européennes en matière de cybersécurité.
- **Lignes directrices de l'ENISA** : alignement avec les meilleures pratiques européennes en matière de résilience, de surveillance et de signalement des incidents.

Normes internationales

- **ISO/IEC 27001** : Nyroxis soutient l'alignement avec la référence mondiale pour les systèmes de gestion de la sécurité de l'information.
- **Préparation judiciaire** : le stockage inviolable des journaux garantit que les preuves sont fiables, auditées et recevables dans un cadre légal ou réglementaire.

Bonnes pratiques américaines & mondiales

- **Cadre NIST Cybersecurity** : complète les fonctions Identifier–Protéger–Détecter–Répondre–Récupérer en couvrant les terminaux personnels souvent exclus du périmètre de l'entreprise.
- **Principes du Zero Trust** : étend le modèle « ne jamais faire confiance, toujours vérifier » à la sphère personnelle des dirigeants et des utilisateurs sensibles.

Résumé

En intégrant la conformité et la préparation aux audits dans sa conception, Nyroxis aide les organisations non seulement à **réduire les risques**, mais aussi à démontrer leur **diligence raisonnable** auprès des régulateurs, auditeurs et parties prenantes dans le monde entier. C'est une solution conçue pour la résilience, tant sur le plan technique que réglementaire.

Feuille de route

De la vision au déploiement à grande échelle

Nyroxis a été créé pour combler une faille de sécurité claire, mais son ambition va bien au-delà de la première version. Le projet est structuré autour d'une feuille de route progressive qui garantit une valeur immédiate aujourd'hui tout en posant les bases de l'innovation continue de demain.

Phase 1 – Community Edition (Open Source)

- Agent léger initial et tableau de bord publiés sur GitHub.
- Accent mis sur la transparence, la sensibilisation et l'éducation.
- Permet aux premiers adopteurs, chercheurs et passionnés de sécurité de tester la vision centrale.
- Sert de « première brique » de l'écosystème Nyroxis plus large.

Phase 2 – Pro Edition (Commerciale)

- Agent avancé avec licence liée au matériel (HWID) et résistance aux falsifications.
- Tableau de bord complet avec moteur de corrélation, export judiciaire et rapports conformes aux exigences réglementaires.
- Conçu pour les professionnels et les organisations qui ne peuvent tolérer aucun angle mort.
- Propose des modèles de licence à la fois par abonnement et perpétuels.

Phase 3 – Intégration Entreprise

- Support pour des déploiements à grande échelle dans les holdings multinationaux.
- Configurations personnalisées pour la conformité (RGPD, NIS2, ISO/IEC 27001).
- Intégration fluide avec les flux de travail SOC/CSIRT existants.
- Support entreprise et accords de niveau de service premium.

Développements futurs

- **Agent macOS** : extension de la protection aux environnements Apple utilisés par les dirigeants.
- **Corrélation IA/ML** : détection automatisée des anomalies pour des analyses plus rapides et plus intelligentes.
- **Intégration Cloud** : option d'analytique centralisée dans le cloud pour les grandes organisations nécessitant une supervision globale.

Résumé

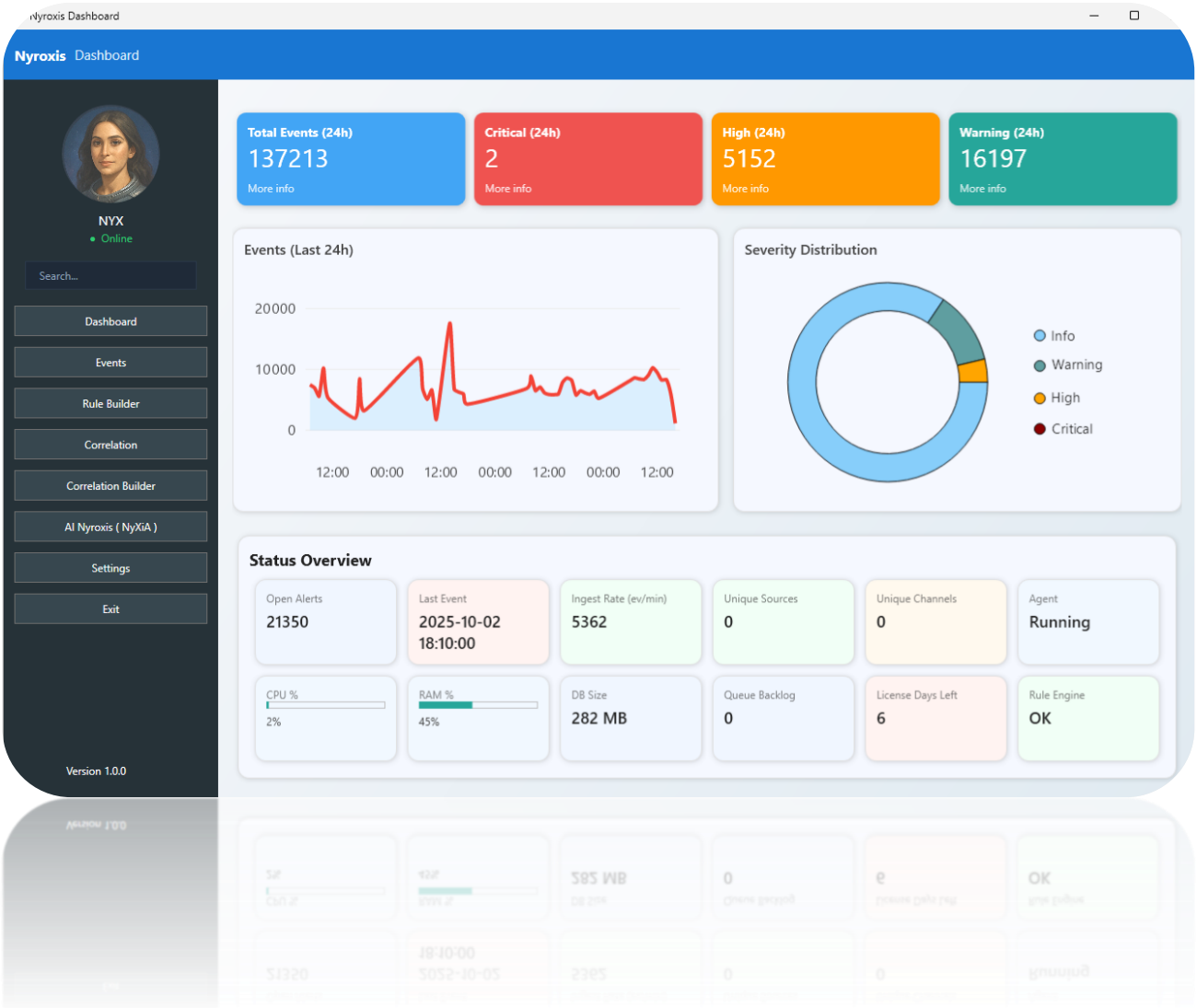
La feuille de route de Nyroxis reflète un équilibre entre la **praticité immédiate** et l'**innovation à long terme**. De la transparence open source aux déploiements de niveau entreprise, chaque phase est conçue pour combler la faille de sécurité personnelle et renforcer la résilience des individus comme des organisations.

Démonstration du tableau de bord

Nyroxis est livré avec un tableau de bord moderne et intuitif, conçu pour offrir une visibilité en temps réel, des corrélations et des analyses à valeur judiciaire.
Vous trouverez ci-dessous une sélection de captures d'écran illustrant les principales fonctionnalités :

1. Tableau de bord principal

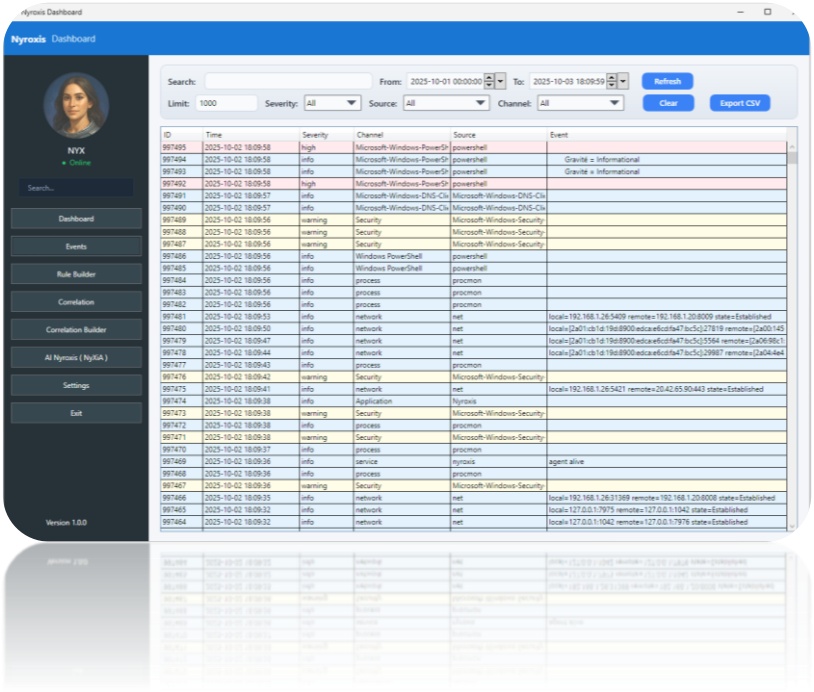
Fournit une vue d'ensemble du nombre total d'événements, de la répartition par niveau de gravité et de l'état global du système.



2. Vue des événements

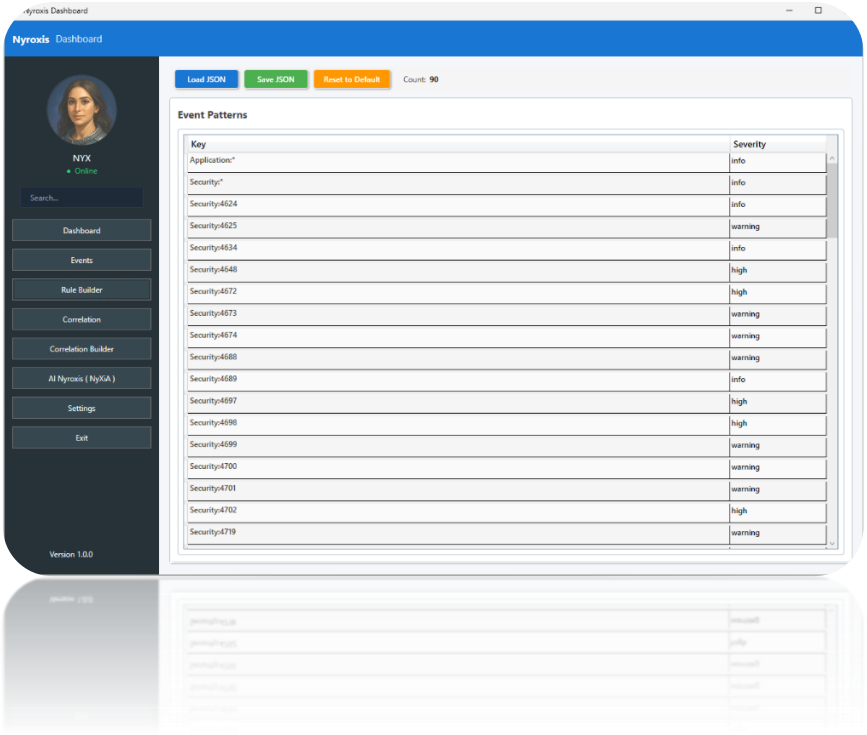
Affiche les journaux d’événements détaillés avec un filtrage par niveau de gravité, source et canal.

.



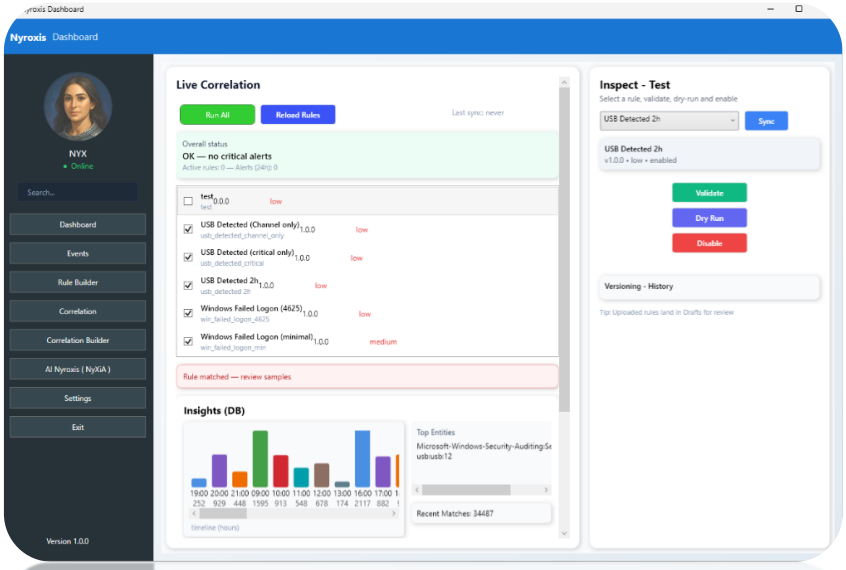
3. Générateur de règles

Permet aux équipes de sécurité de définir et personnaliser des règles de détection à l’aide de modèles JSON.



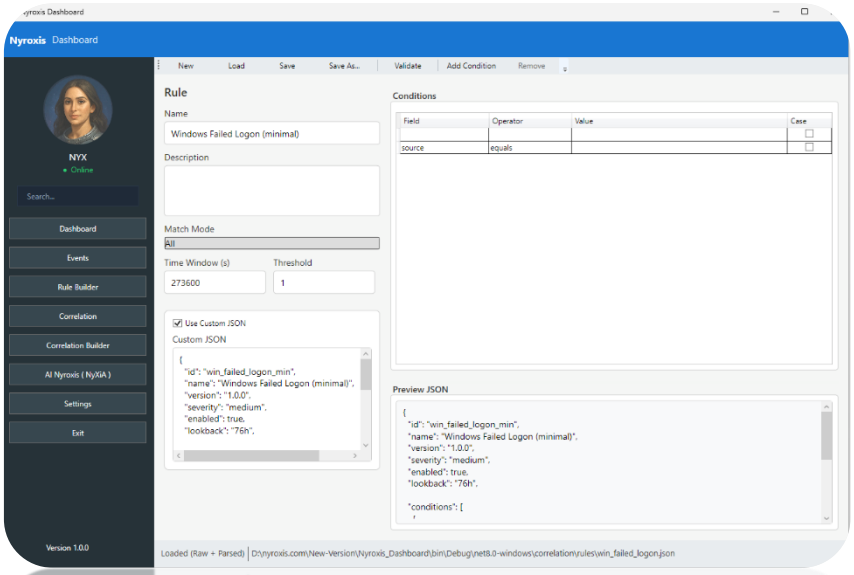
4. Corrélation en temps réel

Affiche les règles de corrélation actives, les correspondances détectées ainsi que les insights, avec indication des niveaux de gravité.



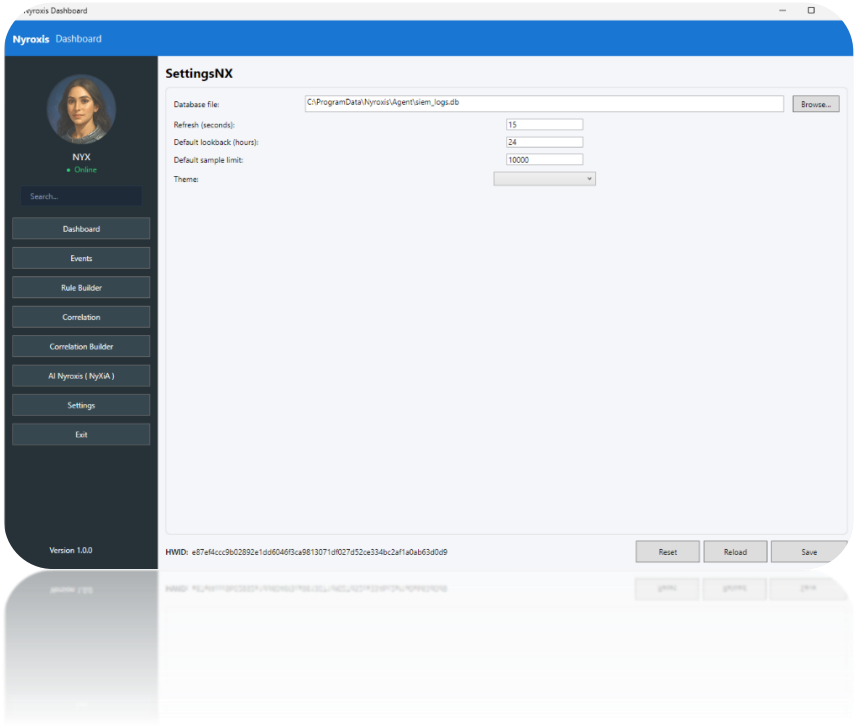
5. Édition des règles

Éditeur de règles avancé prenant en charge les conditions, les seuils et la gestion des versions.



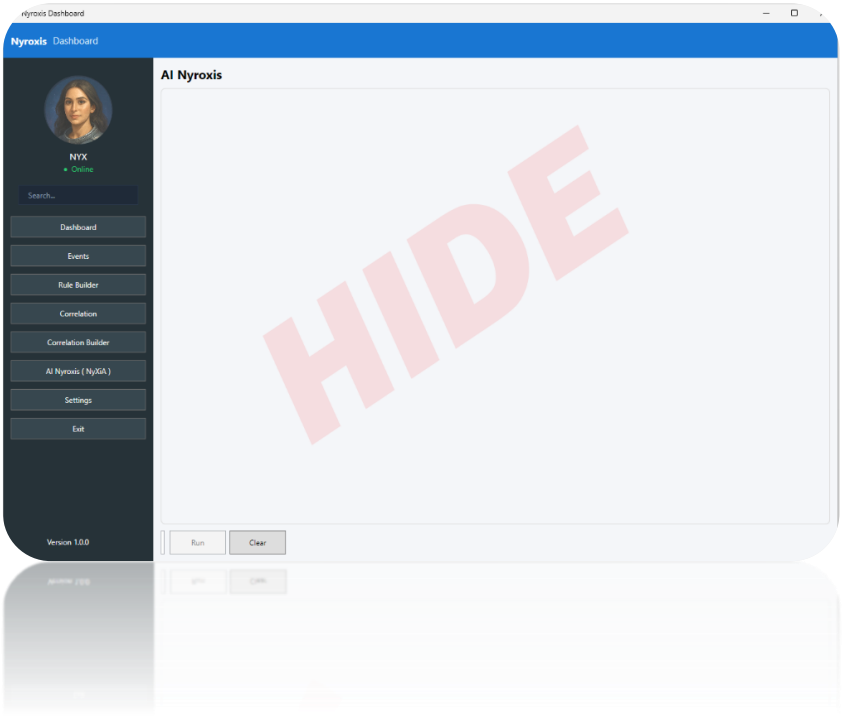
6. Paramètres

Configuration des chemins de base de données, des intervalles de rafraîchissement et des options de rétention/consultation historique.



7. Module IA Nyroxis (NyxIA)

Réservé aux analyses pilotées par l'intelligence artificielle et à la détection d'anomalies, permettant une intégration future.



Résumé

Le tableau de bord démontre que Nyroxis n'est pas qu'un concept, mais un produit pleinement opérationnel. Son interface a été conçue pour offrir de la clarté aux dirigeants et de la précision aux analystes SOC, ce qui la rend adaptée à la fois aux experts techniques et aux utilisateurs non techniques.

- **Pour les professionnels de la sécurité :** recherche avancée d'événements, corrélation en temps réel et personnalisation des règles, permettant des investigations détaillées et une réponse rapide aux incidents.
- **Pour les utilisateurs non techniques** : jeux de règles JSON **préconfigurés et prêts à l'emploi**. En un seul clic, ces règles se chargent et s'appliquent, sans configuration complexe — garantissant une protection de niveau entreprise même pour les profils peu techniques.
- **Pour les organisations :** comble l'écart entre la supervision technique et la gouvernance exécutive, en transformant la télémétrie brute en informations claires et actionnables, tout en restant léger et évolutif.

En substance, le tableau de bord Nyroxis convertit la télémétrie brute en **renseignements opérationnels** clairs et exploitables. Il prouve que Nyroxis n'est pas seulement une vision, mais une solution **prête au déploiement**, conçue pour combler les angles morts les plus négligés — des opérations SOC complexes jusqu'à l'expérience la plus simple de l'utilisateur final.

Nyroxis Agent – Service de sécurité central

Le cœur de Nyroxis

Si le tableau de bord apporte visibilité et contrôle, la véritable fondation de Nyroxis est son **Agent** — un service léger en arrière-plan qui surveille, enregistre et protège en continu l'activité des terminaux là où les solutions traditionnelles échouent.

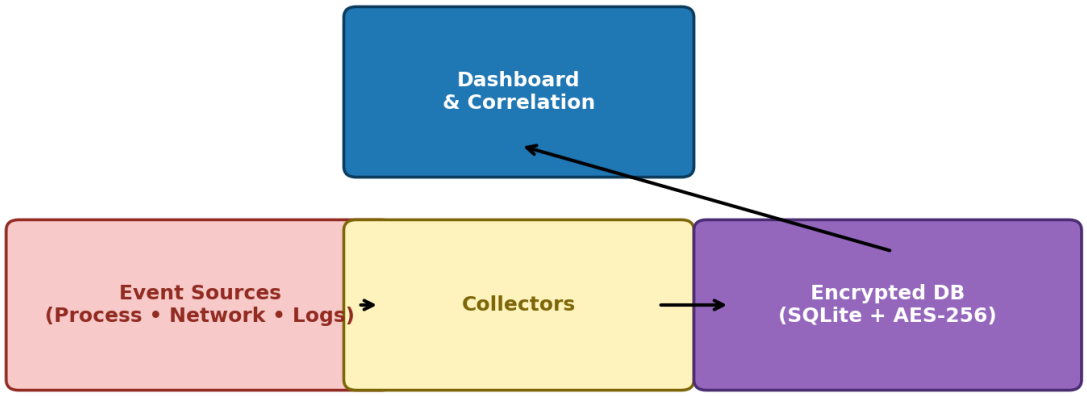
Capacités clés

- **Collecte d'événements** : observe en temps réel les processus, services, activités réseau, scripts et événements système.
- **Stockage chiffré** : toutes les télémétries sont enregistrées dans une base de données locale inviolable (SQLite, chiffrement AES-256).
- **Fonctionnement hors ligne** : fonctionne de manière fiable même sans connectivité réseau, garantissant qu'aucune preuve n'est perdue.
- **Couche de licence & sécurité** : chaque déploiement est lié au matériel (HWID) et validé par des signatures cryptographiques (Ed25519, SHA-256).
- **Discrétion & efficacité** : s'exécute silencieusement comme service Windows avec une consommation minimale de CPU et mémoire, invisible pour les attaquants et transparent pour les utilisateurs.

Rôle architectural

1. **Couche de collecte** → rassemble les données brutes du système d'exploitation.
2. **Couche de normalisation** → enrichit et standardise les événements pour la corrélation.
3. **Couche de protection** → chiffre et sécurise les journaux contre toute falsification.
4. **Couche d'intégration** → alimente le tableau de bord Nyroxis et le moteur de corrélation.

Flux de l’Agent Nyroxis



Nyroxis Agent Flow: Sources → Collectors → Encrypted DB → Dashboard & Correlation

Pourquoi c’est important

L’Agent garantit que :

- **Aucune activité** sur les terminaux critiques ne passe inaperçue.
- Les **preuves** sont conservées dans un format adapté à l’usage judiciaire et légal.
- La **couverture de sécurité** s’étend au-delà du périmètre de l’entreprise, jusque dans les environnements personnels et non gérés exploités par les attaquants.

Résumé

L'Agent Nyroxis constitue le **noyau de confiance et de résilience** de toute la plateforme. Contrairement aux collecteurs traditionnels ou aux antivirus, il est conçu pour offrir une sécurité **continue, vérifiable et résistante aux falsifications** sur des appareils auparavant hors du périmètre défensif de l'entreprise.

- **Pour les équipes de sécurité** : l'Agent garantit un flux de données fiable alimentant les moteurs de corrélation et les tableaux de bord avec des événements **normalisés de haute qualité**. Résultat : des enquêtes plus rapides, une réponse aux incidents renforcée et des éléments de preuve recevables en justice.
- **Pour les organisations** : il étend le périmètre de défense **au-delà du bureau**, transformant des terminaux personnels non gérés en **nœuds de sécurité contrôlés**, sans nécessiter de déploiements ou de maintenances complexes.
- **Pour les utilisateurs finaux** : une protection transparente ; l'Agent s'exécute silencieusement en arrière-plan, n'entrave pas les tâches quotidiennes et garantit une **surveillance constante et invisible** des appareils.

En combinant **fonctionnement hors ligne**, **validation cryptographique** et **faible empreinte** ressources, l'Agent Nyroxis comble l'une des failles les plus critiques de la cybersécurité moderne : **aucun événement n'est perdu, aucune preuve n'est altérée, aucun compromis ne passe inaperçu**.

En substance, l'Agent Nyroxis n'est pas un simple service endpoint — c'est **l'ancre stratégique de l'écosystème Nyroxis**, transformant des environnements personnels vulnérables en **extensions sécurisées** du dispositif défensif de l'organisation.