NYROXIS®

Livre Blanc — Solution de Cybersécurité

Nyroxis Security

www.nyroxis.com | contact@nyroxis.com

Nice, France

Version 1.0 FR — Janvier 2026

Table des matières

1. Résumé Exécutif
2. Introduction & Contexte
3. Énoncé du Problème
4. Notre Solution – Nyroxis
5. Architecture & Technologies
6. Composants Principaux
7. Intelligence Artificielle & Machine Learning
8. Cas d'Usage & Scénarios
9. Bénéfices & Proposition de Valeur
10. Conformité & Standards
11. Feuille de Route
12. Modèle de Licence
13. Démonstration du Tableau de Bord

1. Résumé Exécutif

La Nouvelle Réalité de la Cybersécurité

Malgré des milliards investis dans les pare-feux d'entreprise, les opérations SOC et les plateformes SIEM avancées, les cyberattaques continuent de réussir. La raison est simple : les attaquants ne ciblent plus la porte d'entrée fortifiée — ils s'infiltrent par la porte de derriere, via les appareils personnels des dirigeants, administrateurs, juges et professionnels dont les décisions ont un impact réel.

La Philosophie Nyroxis

La cybersécurité doit commencer au domicile des décideurs, et non au sein des sièges d'entreprise.

L'infrastructure d'entreprise la plus sophistiquée ne sert à rien si l'ordinateur portable personnel d'un PDG ou le réseau domestique d'un administrateur senior reste non surveillé et exposé.

La Solution

Nyroxis fournit une plateforme de sécurité légère, fonctionnant hors ligne, qui apporte une surveillance de niveau SOC aux terminaux personnels. Elle combine quatre composants principaux — Nyroxis Agent, Nyroxis Intelligence, Nyroxis System Guardian et le Tableau de Bord — avec un moteur d'IA/ML entièrement local, garantissant qu'aucune donnée ne quitte jamais l'appareil de l'utilisateur.

Points Clés

- Détection en temps réel avec 27 règles de détection, 12 règles de corrélation et 2 règles de chaîne
- Machine Learning entièrement local — aucun cloud, aucun transfert de données
- Stockage chiffré de qualité légale (AES-256)
- Licences basées sur l'identifiant matériel (HWID) avec validation cryptographique
- Conforme au RGPD, NIS2 et ISO/IEC 27001
- Disponible en anglais, français et allemand
- Windows (v1.0) — macOS & Linux bientôt disponibles
- Un mois d'essai gratuit

2. Introduction & Contexte

La Cybersécurité à un Tournant

Chaque semaine apporte son lot de nouvelles têtes — campagnes de rançongiciels, violations de données, attaques d'états nations. Pourtant, le schéma est toujours le même : les organisations investissent massivement dans les défenses d'entreprise, et les attaquants les contournent simplement. La question n'est plus de savoir si une violation se produira, mais où elle commencera.

Le Point d'Entrée Caché

La réponse, de plus en plus souvent, est : à domicile.

L'ordinateur portable personnel d'un PDG. Une tablette familiale partageant le même Wi-Fi qu'un administrateur senior. La session de navigation nocturne d'un juge ou d'un avocat. Ces appareils existent en dehors des périmètres de sécurité des entreprises — non surveillés, non protégés et invisibles pour les plateformes SIEM d'entreprise. Les attaquants le savent. Ils l'exploitent délibérément.

Pourquoi les Outils Existants Sont Insuffisants

Les logiciels antivirus traditionnels et les solutions EDR d'entreprise ont été conçus pour des environnements de bureau contrôlés. Ils n'ont aucune visibilité sur les appareils personnels, aucune capacité à surveiller l'activité en dehors du réseau d'entreprise, et aucun mécanisme pour préserver les preuves légales sur les terminaux non gérés. Cela crée un angle mort structurel qu'aucun investissement en entreprise ne peut combler.

La Dimension Humaine

Derrière chaque statistique de violation se trouve une personne réelle : un dirigeant dont les communications stratégiques sont compromises, un fonctionnaire dont la crédibilité est minée, une famille dont la vie privée est violée. La cybersécurité ne concerne pas seulement la protection des données — il s'agit de protéger les personnes qui prennent des décisions critiques.

Notre Réponse

Nyroxis a été conçu spécifiquement pour cette réalité. En étendant la surveillance de niveau SOC aux terminaux personnels — fonctionnant silencieusement, travaillant hors ligne, stockant tout localement — il comble le vide que les outils d'entreprise ne peuvent pas atteindre.

3. Énoncé du Problème

Le Vide que Personne ne Comble

La cybersécurité des entreprises n'a jamais été aussi solide. Les pare-feux, les systèmes de détection d'intrusion, les plateformes SIEM et les équipes SOC dédiées représentent d'énormes investissements en matière de protection. Pourtant, les violations continuent — non pas parce que les défenses des entreprises ont échoué, mais parce que les attaquants se sont déplacés ailleurs.

Ils se sont déplacés vers la vie numérique personnelle des personnes au sein de ces entreprises.

L'Angle Mort Structurel

Les réseaux domestiques ne sont pas surveillés. Les ordinateurs portables personnels ne sont pas enrôlés dans les systèmes EDR d'entreprise. Les appareils familiaux partagent le Wi-Fi avec des communications professionnelles sensibles. Ces environnements se situent entièrement en dehors du champ des politiques de sécurité des entreprises — et entièrement à la portée des attaquants sophistiqués.

Un seul appareil personnel compromis peut devenir le point d'entrée silencieux vers une infrastructure critique, des communications de direction ou des procédures judiciaires sensibles.

Qui Est à Risque

- **Dirigeants & Direction Générale** — dont les décisions et communications stratégiques ont un poids financier et réputationnelfinanciaire et réputationnel
- **Fonctionnaires & Professionnels du Droit** — juges, avocats, policiers, dont la compromission personnelle peut affecter l'intégrité des institutions
- **Administrateurs SOC & Responsables IT** — dont les identifiants personnels, s'ils sont volés, peuvent déverrouiller directement l'infrastructure d'entreprise
- **Leurs Familles** — qui partagent réseaux et appareils, souvent sans aucune sensibilisation à la sécurité

Le Coût de l'Inaction

- Pertes financières liées aux violations provenant en dehors du périmètre de l'entreprise
- Atteinte à la réputation lorsque des dirigeants ou des personnalites publiques sont compromis
- Exposition réglementaire sous le RGPD, NIS2 et les cadres connexes
- Préjudice personnel — chantage, violations de la vie privée, manipulation — ciblant des individus dans des rôles critiques

Le Problème Fondamental

Il n’existe pas de solution légère, respectueuse de la vie privée et fonctionnant hors ligne, conçue spécifiquement pour protéger les terminaux personnels des individus à haute valeur. Les outils d’entreprise sont trop lourds, trop intrusifs et trop dépendants de l’infrastructure d’entreprise. L’antivirus grand public est trop superficiel.

Nyroxis existe pour combler ce vide.

4. Notre Solution – Nyroxis

Un Type de Sécurité Différent

Nyroxis n'est pas un autre outil d'entreprise réduit à un usage personnel. Il a été conçu de zéro avec un seul objectif : apporter une protection de niveau SOC aux terminaux personnels des individus à haute valeur — silencieusement, localement et sans compromis.

La Philosophie Fondamentale

Là où la cybersécurité traditionnelle s'arrête à la porte du bureau, Nyroxis commence. Il opère sur la conviction que le vide de sécurité le plus critique n'est pas technique — il est géographique. L'appareil personnel d'un décideur est aussi stratégiquement précieux que n'importe quel serveur d'entreprise.

Comment Nyroxis Fonctionne

La plateforme est construite autour de quatre composants principaux travaillant de concert :

Nyroxis Agent

Collecte en continu les journaux de plusieurs canaux système — processus, activité réseau, services, scripts et événements système. Il normalise ces données en temps réel, chiffre le contenu et stocke tout dans une base de données chiffrée locale. Rien ne quitte l'appareil.

Nyroxis Intelligence

Applique un moteur de règles intelligent sur trois couches de détection : Détection (27 règles identifiant les menaces connues), Corrélation (12 règles reliant les événements liés dans le temps) et Chaîne (2 règles détectant les séquences d'attaques en plusieurs étapes). Le moteur de règles est ouvert à l'extension par les professionnels de la sécurité.

Nyroxis System Guardian

Fonctionne discrètement dans la barre d'outils système Windows, agissant comme gardien de la plateforme. Il surveille l'état opérationnel de tous les services toutes les 3 secondes, gère les sauvegardes de base de données, valide la licence en temps réel, vérifie les mises à jour et arrête automatiquement les services si la licence expire.

Tableau de Bord Nyroxis

Une interface claire et intuitive conçue pour les professionnels de la sécurité comme pour les utilisateurs non techniques. Elle offre une visibilité en temps réel sur les événements, les détections, les corrélations et les chaînes, avec des rapports intégrés, une recherche légale et un moteur d'analyse IA/ML — tout s'exécutant localement.

Ce qui Distingue Nyroxis

- Entièrement hors ligne — aucune dépendance à l'infrastructure cloud, aucun transfert de données
- Stockage de qualité légale — chiffré AES-256, infalsifiable, admissible en justice
- Léger & silencieux — utilisation minimale des ressources, invisible pour les attaquants
- Extensible — les équipes de sécurité peuvent créer et déployer des règles de détection personnalisées
- Multilingue — interface en anglais, français et allemand
- Protection de la vie privée par conception — les données personnelles ne quittent jamais l'appareil

Nyroxis est la couche manquante — la protection qui commence là où la sécurité d'entreprise se termine.

5. Architecture & Technologies

Vue d'ensemble

Nyroxis est conçu comme une plateforme de sécurité modulaire et légère combinant la surveillance des terminaux, la détection en temps réel et l'analyse IA locale. Son architecture repose sur trois principes : simplicité de déploiement, intégrité des preuves et localité absolue des données.

Composants Principaux

Composant	Rôle	Technologie Clé
Nyroxis Agent	Collecte, normalisation, stockage chiffré	Rust, SQLite, AES-256
Nyroxis Intelligence	Détection, corrélation, moteur de règles	Rust, moteur JSON
Nyroxis System Guardian	Surveillance, sauvegarde, licence, mises à jour	Rust, barre système
Tableau de Bord Nyroxis	Interface, analyse légale, IA/ML, rapports	Tauri + WebView

Couches de Détection

Couche	Règles	Objectif
nyroxis_detection	27	Identifier les menaces connues dans les événements individuels
nyroxis_correlations	12	Relier les événements suspects dans le temps et entre les sources
nyroxis_chains	2	Détecter les séquences d'attaques en plusieurs étapes

Pile Technologique

Composant	Technologie
Services principaux	Rust
Tableau de bord	Tauri + WebView
Base de données locale	SQLite

Composant	Technologie
Chiffrement	AES-256 (journaux), Ed25519 (signatures), SHA-256 (hachage)
Moteur ML	Forêt d'isolement — Rust pur, sans bibliothèque ML externe
Analyse statistique	Z-Score, IQR, Moyenne mobile — calcul local
Plateforme	Windows (v1.0) — macOS & Linux : bientôt disponibles

Principes de Conception

- **Localité des Données** — tout le traitement, le stockage et l'analyse ont lieu sur l'appareil de l'utilisateur. Aucun cloud, aucune télémétrie, aucune transmission externe
- **Intégrité Légale** — journaux chiffrés et infalsifiables adaptés aux procédures judiciaires et réglementaires
- **Discrétion** — invisible pour les attaquants, non intrusif pour les utilisateurs
- **Extensibilité** — moteur de règles conçu pour la personnalisation par des experts
- **Complémentarité** — fonctionne aux côtés des investissements AV, EDR et SIEM existants

6. Composants Principaux

Nyroxis Agent — Le Moteur de Collecte

Nyroxis Agent est le fondement de toute la plateforme. Fonctionnant comme un service Windows silencieux, il opère en continu en arrière-plan, ingérant des données pertinentes pour la sécurité depuis plusieurs canaux système simultanément :

- Journaux d'événements Windows (Sécurité, Système, Application)
- Connexions réseau et métadonnées de trafic
- Processus en cours d'exécution et activité des services
- Exécution de scripts PowerShell
- Modifications du système de fichiers et du registre

Chaque événement collecté passe par un pipeline de normalisation qui standardise le format et enrichit le contexte. Le contenu normalisé est ensuite chiffré avec AES-256 et écrit dans une base de données SQLite locale — sur l'appareil de l'utilisateur, sous son contrôle.

Utilisation des ressources : environ 57 Mo de RAM, 0,1% CPU — adapté au fonctionnement continu sur les ordinateurs portables personnels sans affecter la productivité.

Nyroxis Intelligence — Le Moteur de Détection

Nyroxis Intelligence est le cœur analytique de la plateforme. Il opère à haute vitesse sur trois couches de détection séquentielles :

Couche 1 — Détection (27 règles)

Identifie les menaces connues dans les événements individuels : exécution de processus suspects, installation de services non autorisés, comportement réseau anormal, tentatives d'accès aux identifiants, et plus encore.

Couche 2 — Corrélation (12 règles)

Relie les événements liés dans le temps et entre les sources pour identifier des schémas de menaces qu'aucun événement individuel ne révèlerait seul. Une connexion échouée suivie d'une réussie depuis un autre emplacement. Un nouveau processus démarrant immédiatement après la connexion d'un périphérique USB.

Couche 3 — Chaîne (2 règles)

Détecte les séquences d'attaques en plusieurs étapes — le type d'intrusion progressif et coordonné qui caractérise les menaces persistantes avancées.

Extensible par Conception

Les professionnels de la sécurité peuvent créer de nouvelles règles et les déployer directement dans le système sans modifier les composants principaux. Les règles suivent un format structuré basé sur JSON.

Utilisation des ressources : environ 87 Mo de RAM, 1,8% CPU.

Nyroxis System Guardian — Le Gardien de la Plateforme

Nyroxis System Guardian fonctionne discrètement comme une application de barre système (6,5 Mo de RAM, 0,1% CPU), assurant une surveillance continue de l'ensemble de la plateforme :

Surveillance des Services

Toutes les 3 secondes, System Guardian vérifie que Nyroxis Agent et Nyroxis Intelligence fonctionnent. Si l'un des services s'arrête de manière inattendue, Guardian détecte immédiatement la perturbation.

Validation de la Licence

Guardian supervise le cadre de licence basé sur HWID en continu. Si une licence expire ou est invalidée, Guardian arrête automatiquement les deux services. La validation fonctionne entièrement hors ligne via le chiffrement AES-GCM et la vérification HMAC.

Gestion des Sauvegardes

Toutes les bases de données Nyroxis sont des actifs légaux critiques. Guardian gère les sauvegardes planifiées et à la demande, surveillant la taille, l'horodatage et l'intégrité des fichiers.

Vérification des Mises à Jour

Guardian vérifie automatiquement l'existence de nouvelles versions à des intervalles configurables, notifiant les utilisateurs lorsque des mises à jour sont disponibles. Les mises à jour critiques sont signalées immédiatement.

Ensemble, ces quatre composants forment un tissu de sécurité autonome et résilient — qui se surveille, se détecte et se protège lui-même, afin que l'utilisateur n'ait jamais à le faire.

7. Intelligence Artificielle & Machine Learning

Une Approche Différente de l'IA

La plupart des solutions de sécurité basées sur l'IA s'appuient sur une infrastructure cloud. Nyroxis adopte l'approche opposée. Chaque aspect du moteur IA de Nyroxis fonctionne localement, sur l'appareil de l'utilisateur. Aucune donnée n'est transmise. Aucun profil comportemental ne quitte jamais la machine.

Forêt d'Isolement — Détection des Anomalies

Au cœur du moteur ML de Nyroxis se trouve une implémentation personnalisée de l'algorithme de Forêt d'Isolement (Isolation Forest), construite entièrement en Rust sans dépendance à une bibliothèque de machine learning externe.

La Forêt d'Isolement fonctionne en construisant une forêt d'arbres de décision aléatoires. Les événements anormaux reçoivent un score d'anomalie plus élevé car ils nécessitent moins de séparations pour être isolés.

L'implémentation Nyroxis opère avec 100 arbres d'isolement par cycle, 256 échantillons maximum par arbre et 8 caractéristiques comportementales par fenêtre d'analyse :

Caractéristique	Description
Nombre d'événements	Événements totaux dans la fenêtre d'analyse
Sources uniques	Nombre de sources d'événements distinctes
Destinations uniques	Nombre de destinations réseau distinctes
Heure de la journée	Contexte temporel pour la référence comportementale
Jour de la semaine	Reconnaissance des schémas hebdomadaires
Événements par heure	Normalisation du taux d'activité
Ratio de nouvelles sources	Proportion de sources nouvellement observées
Ratio de nouvelles destinations	Proportion de destinations nouvellement observées

Moteur d'Analyse Statistique

Classification par Score Z

Score Z	Sévérité	Confiance
> 3,0	Critique	99,7%
> 2,0	Élevée	95%

Score Z	Sévérité	Confiance
> 1,5	Moyenne	86%
> 1,0	Faible	68%

Méthodes Statistiques Supplémentaires

- **Détection des valeurs aberrantes IQR** — identifie les valeurs en dehors de l'écart interquartile
- **Moyenne mobile** — suit les tendances comportementales sur des fenêtres temporelles configurables
- **Moyenne mobile exponentielle** — accorde plus de poids à l'activité récente pour une réponse plus rapide
- **Détection de pics** — signale les écarts soudains par rapport aux normes historiques
- **Analyse de corrélation** — mesure les relations statistiques entre les signaux comportementaux indépendants

Pourquoi le ML Local Est Important

Pour les individus que Nyroxis protège — dirigeants, professionnels du droit, fonctionnaires — la sensibilité de leurs données comportementales est elle-même une préoccupation de sécurité. Un moteur ML local élimine ce risque entièrement, offrant la profondeur analytique de l'intelligence comportementale cloud sans compromis sur la confidentialité.

8. Cas d'Usage & Scénarios

Où Nyroxis Crée un Impact Réel

Nyroxis a été conçu pour des environnements où les outils de sécurité traditionnels ne peuvent pas atteindre. Les scénarios suivants illustrent les contextes réels dans lesquels la plateforme crée une valeur immédiate et mesurable.

Scénario 1 — Le Dirigeant à Domicile

Un directeur financier travaille depuis chez lui trois jours par semaine. Son ordinateur portable personnel n'a jamais été enrôlé dans le système EDR de l'entreprise. Un soir, un e-mail de phishing installe une porte d'entrée discrète. Le pare-feu de l'entreprise ne le détecte jamais.

Avec Nyroxis installé, Nyroxis Agent capture l'exécution anormale du processus dès qu'elle se produit. Nyroxis Intelligence la corrèle avec une tentative de connexion sortante suspecte quelques minutes plus tard. Une alerte est émise avant qu'aucune donnée ne quitte la machine.

Scénario 2 — Le Professionnel du Droit

Un juge senior utilise un ordinateur portable personnel pour examiner des documents d'affaires en dehors du palais de justice. Un attaquant injecte des scripts malveillants dans les sessions du navigateur via un routeur compromis.

Nyroxis détecte le schéma d'exécution de scripts anormal et signale le comportement réseau inhabituel. Le juge est alerté. La tentative est documentée avec des preuves de qualité légale.

Scénario 3 — L'Administrateur SOC

Un responsable d'équipe SOC accède aux systèmes internes à distance la nuit depuis un appareil personnel. Les attaquants ciblent spécifiquement cet appareil, sachant que sa compromission pourrait donner accès direct à l'environnement d'entreprise.

Nyroxis surveille l'appareil en continu, détecte les tentatives d'accès aux identifiants via sa couche de détection de chaîne et émet une alerte critique. Le périmètre d'entreprise n'est jamais atteint.

Scénario 4 — L'Organisation Multinationale

Un holding avec des opérations dans plusieurs pays fait face à un paysage de sécurité incohérent pour les appareils personnels. Nyroxis fournit une couche de protection unifiée déployable sur tous les terminaux quelle que soit la géographie, chaque installation opérant indépendamment sans infrastructure centralisée.

Scénario 5 — L'Organisation Sensibilisée à la Sécurité

Une entreprise avant-gardiste déploie Nyroxis dans le cadre d'un programme plus large de sensibilisation et de surveillance interne. Le moteur de règles extensible permet à l'équipe de sécurité de rédiger des règles de détection personnalisées adaptées à son modèle de menace spécifique.

9. Bénéfices & Proposition de Valeur

Une Sécurité qui Crée de la Valeur Stratégique

La cybersécurité n'est pas seulement une discipline technique — c'est une question de continuité des activités, de confiance institutionnelle et de sécurité personnelle. Nyroxis apporte de la valeur à tous les niveaux de l'organisation.

Pour les Responsables Sécurité — RSSI & Équipes SOC

- **Visibilité Là Où Elle N'Existait Pas** — étend la surveillance aux terminaux personnels que les outils d'entreprise ne couvrent pas
- **Preuves de Qualité Légale** — journaux chiffrés, horodatés et infalsifiables accélèrent la réponse et soutiennent les procédures judiciaires
- **Intégration Transparente** — complète les déploiements AV, EDR et SIEM existants sans ajouter de complexité
- **Détection Extensible** — les équipes peuvent créer et déployer des règles personnalisées adaptées à leur environnement

Pour la Direction Générale — PDG & Conseil d'Administration

- **Protection des Actifs Immatériels** — préserve la réputation de la marque, la confiance des investisseurs et la capacité de décision stratégique
- **Diligence Raisonnable Démontrée** — fournit des preuves documentées et vérifiables de la gestion active des risques pour les régulateurs
- **Réduction du Coût des Violations** — détecte les menaces au niveau du terminal personnel avant qu'elles n'atteignent l'infrastructure d'entreprise

Pour l'Individu Protégé — Dirigeant, Professionnel, Fonctionnaire

- **Protection Silencieuse et Transparente** — fonctionne invisiblement en arrière-plan, sans expertise technique requise
- **Confidentialité Absolue** — aucune donnée comportementale n'est jamais transmise en dehors de l'appareil
- **Tranquillité d'Esprit** — confiance que les appareils personnels et l'environnement familial sont surveillés et protégés

L’Avantage Stratégique

Dimension	Sans Nyroxis	Avec Nyroxis
Visibilité terminal personnel	Aucune	Complète, en temps réel
Détection des menaces à domicile	Aucune	Couches 27+12+2 règles
Preuves légales	Indisponible	Chiffrées, admissibles en justice
Détection IA des anomalies	Aucune	Forêt d’isolement locale
Confidentialité des données	À risque	Garantie — entièrement locale
Posture de conformité	Incomplète	RGPD, NIS2, ISO 27001 alignée
Perturbation de l’utilisateur	N/A	Zéro

10. Conformité & Standards

Une Sécurité qui Satisfait les Régulateurs

Dans l'environnement réglementaire actuel, la cybersécurité est évaluée par la responsabilité démontrable. Les organisations doivent prouver qu'elles gèrent activement les risques sur l'ensemble de leur écosystème numérique, y compris les terminaux personnels du personnel clé. Nyroxis a été conçu avec cette exigence en son cœur.

Cadres Européens

RGPD — Règlement Général sur la Protection des Données

Nyroxis est conçu autour de la minimisation des données et de la protection de la vie privée par conception. Toute la télémétrie collectée est chiffrée au repos avec AES-256. Aucune donnée personnelle n'est transmise extérieurement. L'utilisateur conserve une souveraineté complète sur ses propres données.

Directive NIS2

NIS2 exige que les organisations démontrent une capacité de surveillance continue, une préparation aux incidents et une gestion active des risques. Nyroxis étend cette capacité aux terminaux personnels — précisément les environnements les plus susceptibles d'être attaqués.

Lignes Directrices ENISA

Nyroxis s'aligne sur les meilleures pratiques de l'Agence de l'Union européenne pour la cybersécurité en matière de résilience des terminaux, de surveillance comportementale et de documentation des incidents.

Standards Internationaux

ISO/IEC 27001

Nyroxis soutient l'alignement avec la référence mondiale pour les systèmes de management de la sécurité de l'information. Sa journalisation de qualité légale et son cadre de détection structuré étendent la couverture SMSI aux terminaux personnels.

Préparation Légale

Chaque événement capturé par Nyroxis est chiffré, horodaté et stocké dans une base de données locale infalsifiable — répondant aux exigences de préparation légale dans toutes les juridictions.

Cadre de Cybersécurité NIST

Fonction NIST	Contribution Nyroxis
Identifier	Visibilité continue sur l'activité des terminaux personnels et le comportement des actifs
Protéger	Stockage chiffré, licences basées sur HWID, architecture infalsifiable
Détecter	27 règles de détection, 12 règles de corrélation, 2 règles de chaîne, détection IA locale
Répondre	Alertes en temps réel, preuves légales, moteur de règles extensible

Résumé de Conformité

Cadre	Alignement Nyroxis
RGPD	Protection de la vie privée par conception, minimisation des données, stockage local uniquement
NIS2	Surveillance continue, préparation aux incidents, couverture des terminaux personnels
Lignes directrices ENISA	Résilience des terminaux, surveillance comportementale, documentation des incidents
ISO/IEC 27001	Journalisation légale, détection structurée, extension SMSI
NIST CSF	Fonctions Identifier, Protéger, Détecter, Répondre couvertes
Zéro Confiance	Vérification continue au niveau du terminal personnel

11. Feuille de Route

De la Fondation à l'Écosystème Complet

Nyroxis 1.0 représente une plateforme complètement fonctionnelle et prête pour la production. La feuille de route à venir étend ce qui fonctionne déjà vers de nouveaux environnements, de nouvelles capacités et de nouvelles communautés.

Actuel — Version 1.0 (Disponible Maintenant)

- Nyroxis Agent — collecte multi-canaux, normalisation, stockage local chiffré AES-256
- Nyroxis Intelligence — moteur de détection trois couches (27 détection, 12 corrélation, 2 chaîne)
- Nyroxis System Guardian — surveillance des services, gestion des sauvegardes, validation des licences, vérification des mises à jour
- Tableau de Bord Nyroxis — visibilité en temps réel, recherche légale, visualisation des détections, rapports
- Moteur IA/ML local — détection des anomalies par Forêt d'Isolement, analyse statistique, entièrement hors ligne
- Interface multilingue — anglais, français, allemand
- Un mois d'essai gratuit

Phase 2 — Expansion de la Plateforme

Support macOS & Linux

L'agent et le tableau de bord Nyroxis sont étendus aux environnements macOS et Linux — apportant le même niveau de protection à toute la gamme d'appareils personnels utilisés par les dirigeants et professionnels.

Bibliothèque de Détection Étendue

De nouvelles règles de détection, de corrélation et de chaîne seront publiées pour faire face aux nouvelles menaces, avec des contributions de la communauté des professionnels de la sécurité.

Capacités ML Améliorées

Le moteur IA local sera approfondi avec des modèles comportementaux supplémentaires, des fenêtres de référence plus longues et une analyse des caractéristiques contributives plus granulaire.

Phase 3 — Éducation & Communauté

Programme d'Éducation à la Sécurité Nyroxis

Nyroxis lancera une initiative d'éducation à la sécurité structurée commenpant par les écoles — introduisant la prochaine génération à la pensée pratique en matière de cybersécurité. Ce programme

reflète la philosophie fondamentale de Nyroxis : une sécurité durable commence par les personnes, pas seulement par les plateformes.

Communauté de Professionnels de la Sécurité

Le moteur de règles extensible crée une base naturelle pour une communauté de praticiens — un canal structuré via lequel les professionnels de la sécurité peuvent contribuer, partager et développer la capacité de détection collective de la plateforme.

Phase 4 — Intégration en Entreprise

Pour les entreprises cherchant à étendre la protection Nyroxis à l'ensemble de leur direction et du personnel opérationnel, un modèle de déploiement organisationnel structuré fournira une supervision centralisée tout en préservant les garanties de localité des données qui définissent la plateforme.

Résumé de la Feuille de Route

Phase	Objectif	Statut
v1.0	Plateforme Windows complète	✓ Disponible maintenant
Phase 2	macOS & Linux, ML amélioré	En développement
Phase 3	Programme éducatif, communauté	Lancement 2026
Phase 4	Intégration entreprise, SOC/CSIRT	Planifié

12. Modèle de Licence

Simple, Transparent, Respectueux de la Vie Privée

Le modèle de licence Nyroxis reflète les mêmes principes que la plateforme elle-même : simplicité, intégrité et respect de l'utilisateur. Il n'y a pas de pièges d'abonnement, pas de collecte de données cachée liée à la validation de la licence, et aucune dépendance à des serveurs externes.

Fonctionnement de la Licence

Chaque licence Nyroxis est liée au matériel de l'utilisateur via un identifiant unique dérivé des caractéristiques physiques de l'appareil (HWID). Une clé cryptographique est générée à partir du même profil matériel, créant une licence qui est :

- **Non transférable** — liée à l'appareil spécifique pour lequel elle a été émise
- **Infalsifiable** — toute modification de la licence est immédiatement détectée par Nyroxis System Guardian
- **Entièrement hors ligne** — la validation ne nécessite aucune connexion internet, aucun serveur externe

Période d'Essai

Chaque nouvelle installation Nyroxis inclut un mois d'essai gratuit — offrant un accès complet à toutes les fonctionnalités de la plateforme sans restriction. Aucune carte de crédit n'est requise.

Niveaux de Licence

Niveau	Cible	Fonctionnalités
Essai	Tous les utilisateurs	Accès complet à la plateforme — 1 mois, sans restrictions
Personnel	Dirigeants, professionnels, particuliers	Plateforme complète, appareil unique, lié au HWID
Professionnel	Praticiens, consultants en sécurité	Plateforme complète, déploiement de règles, support prioritaire
Entreprise	Organisations, holdings, institutions	Déploiement multi-appareils, supervision organisationnelle, support dédié

Toujours Inclus

- Nyroxis Agent, Nyroxis Intelligence, Nyroxis System Guardian — plateforme complète
- Moteur IA/ML local — entièrement hors ligne, sans dépendance cloud
- Bibliothèque complète de règles de détection, corrélation et chaîne
- Tableau de bord multilingue — anglais, français, allemand
- Stockage local chiffré de qualité légale
- Gestion des sauvegardes de base de données
- Validation de licence hors ligne

Jamais Inclus

- Aucune télémétrie envoyée à Nyroxis ou à des tiers
- Aucune donnée comportementale collectée à des fins de licence
- Aucune dépendance à la connectivité internet pour le fonctionnement de la plateforme
- Aucun coût caché lié au volume de données ou au nombre d'événements

Contact

Nyroxis Security

www.nyroxis.com | contact@nyroxis.com

Nice, France

13. Démonstration du Tableau de Bord

Visibilité par Conception

Le Tableau de Bord Nyroxis est l'interface opérationnelle de toute la plateforme. Il a été conçu pour deux types d'utilisateurs simultanément : le professionnel de la sécurité qui a besoin de précision, de profondeur et de capacité légale — et le dirigeant non technique qui a besoin de clarté, de simplicité et de conscience situationnelle immédiate.

1. Vue d'Ensemble Principale

Le point d'entrée du tableau de bord fournit une image instantanée de la posture de sécurité actuelle : événements totaux collectés dans les dernières 24 heures, alertes actives par sévérité (Critique, Élevé, Avertissement, Info), chronologie des événements en temps réel, distribution des sévérités et état du système.

2. Vue des Événements

La vue des événements est le cœur légal du tableau de bord. Elle offre un accès complet à la base de données d'événements bruts avec des capacités complètes de recherche, de filtrage et d'exportation — y compris l'inspection légale des événements individuels et l'exportation en CSV.

3. Vue des Détections

La vue de détection présente tous les résultats générés par la couche de règles de détection de Nyroxis Intelligence. Chaque résultat inclut la règle déclenchée, les événements correspondants, la classification de la sévérité et un lien direct vers les événements bruts sous-jacents.

4. Vue des Corrélations

La vue de corrélation fait remonter les résultats du moteur de corrélation à 12 règles — les schémas qui émergent non pas des événements individuels, mais des relations entre eux. C'est là que les signaux isolés deviennent une intelligence actionnable.

5. Vue des Chaînes

La vue des chaînes présente les résultats de la couche de détection la plus sophistiquée — la détection de séquences d'attaques en plusieurs étapes. Les résultats de chaîne représentent les alertes de la plus haute priorité dans le système.

6. Rapports

La section des rapports fournit une documentation structurée et exportable de l'activité de la plateforme. Les rapports peuvent être générés sur des fenêtres temporelles configurables et exportés en PDF ou CSV — adaptés à l'examen interne, la soumission réglementaire ou les procédures judiciaires.

7. Analyse IA / ML

Le module IA offre un accès au moteur de machine learning local. Les analystes peuvent examiner les résultats de détection des anomalies avec la décomposition des caractéristiques contributives, inspecter les classifications par score Z et identifier les valeurs aberrantes statistiques. Toute l'analyse est effectuée localement.

8. Paramètres

La vue des paramètres fournit la configuration complète de la plateforme : chemin du fichier de base de données, intervalle de rafraîchissement du tableau de bord, fenêtre de consultation par défaut, limite d'échantillon, sélection de la langue de l'interface (anglais, français, allemand) et configuration du thème.

9. Sauvegarde

La section de sauvegarde fournit une gestion directe des opérations de sauvegarde de la base de données — planification, exécution à la demande et historique des sauvegardes. Tous les fichiers de sauvegarde sont chiffrés et stockés localement.

Conçu pour Tous

Le Tableau de Bord Nyroxis ne demande pas à ses utilisateurs de choisir entre puissance et simplicité. Les professionnels de la sécurité ont la profondeur dont ils ont besoin. Les utilisateurs non techniques ont la clarté dont ils ont besoin.

C'est le principe de conception Nyroxis rendu visible : une protection de niveau entreprise, accessible à tous ceux qu'elle protège.