NYROXIS®

Cybersecurity Solution Whitepaper

Nyroxis Security

www.nyroxis.com | contact@nyroxis.com

Nice, France

Version 1.0 EN — January 2026

Table of Contents

1. Executive Summary

The New Cybersecurity Reality

Despite billions invested in enterprise firewalls, SOC operations, and advanced SIEM platforms, cyberattacks continue to succeed. The reason is simple: attackers no longer target the fortified front door — they enter through the back, via the personal devices of executives, administrators, judges, and professionals whose decisions carry real-world weight.

The Nyroxis Philosophy

Cybersecurity must begin at the home of decision-makers, not inside corporate headquarters.

The most sophisticated enterprise infrastructure means little if the personal laptop of a CEO or the home network of a senior administrator remains unmonitored and exposed.

The Solution

Nyroxis delivers a lightweight, offline-capable security platform that brings SOC-grade monitoring to personal endpoints. It combines four core components — Nyroxis Agent, Nyroxis Intelligence, Nyroxis System Guardian, and the Dashboard — with a fully local AI/ML engine, ensuring that no data ever leaves the user's device.

Key Highlights

- Real-time detection across 27 detection rules, 12 correlation rules, and 2 chain rules
- Fully local Machine Learning — no cloud, no data transfer
- Forensic-grade encrypted storage (AES-256)
- HWID-based licensing with cryptographic validation
- Compliant with GDPR, NIS2, and ISO/IEC 27001
- Available in English, French, and German
- Windows (v1.0) — macOS & Linux coming soon
- One month free trial

2. Introduction & Context

Cybersecurity at a Crossroads

Every week brings new headlines — ransomware campaigns, data breaches, nation-state attacks. Yet the pattern is always the same: organizations invest heavily in enterprise defenses, and attackers simply go around them. The question is no longer if a breach will occur, but where it will begin.

The Hidden Entry Point

The answer, increasingly, is: at home.

A personal laptop of a CEO. A family tablet sharing the same Wi-Fi as a senior administrator. The late-night browsing session of a judge or a lawyer. These devices exist outside corporate security perimeters — unmonitored, unprotected, and invisible to enterprise SIEM platforms. Attackers know this. They exploit it deliberately.

Why Existing Tools Fall Short

Traditional antivirus software and enterprise EDR solutions were designed for controlled office environments. They have no visibility into personal devices, no ability to monitor activity outside the corporate network, and no mechanism to preserve forensic evidence on unmanaged endpoints. This creates a structural blind spot that no amount of enterprise investment can close — because the problem lives outside the enterprise.

The Human Dimension

Behind every breach statistic is a real person: an executive whose strategic communications are compromised, a public servant whose credibility is undermined, a family whose privacy is violated. Cybersecurity is not only about protecting data — it is about protecting the people who make critical decisions, and the trust that surrounds them.

Our Response

Nyroxis was built specifically for this reality. By extending SOC-grade monitoring to personal endpoints — running silently, working offline, storing everything locally — it closes the gap that enterprise tools cannot reach.

3. Problem Statement

The Gap No One Is Closing

Enterprise cybersecurity has never been stronger. Firewalls, intrusion detection systems, SIEM platforms, and dedicated SOC teams represent enormous investments in protection. And yet, breaches continue — not because enterprise defenses have failed, but because attackers have moved elsewhere.

They have moved to the personal digital lives of the people inside those enterprises.

The Structural Blind Spot

Home networks are not monitored. Personal laptops are not enrolled in corporate EDR systems. Family devices share Wi-Fi with sensitive professional communications. These environments sit entirely outside the scope of enterprise security policies — and entirely within the reach of sophisticated attackers.

A single compromised personal device can become the silent entry point into critical infrastructure, executive communications, or sensitive legal proceedings. The attacker does not need to breach the firewall. They only need to reach the person behind it.

Who Is at Risk

- **Executives & Senior Management** — whose strategic decisions and communications carry financial and reputational weight
- **Public Servants & Legal Professionals** — judges, lawyers, police officers, whose personal compromise can affect the integrity of institutions
- **SOC Administrators & IT Leaders** — whose personal credentials, if stolen, can unlock enterprise infrastructure directly
- **Their Families** — who share networks and devices, often with no security awareness at all

The Cost of Inaction

- Financial losses from breaches originating outside the corporate perimeter
- Reputational damage when executives or public figures are compromised
- Regulatory exposure under GDPR, NIS2, and related frameworks
- Personal harm — blackmail, privacy violations, manipulation — targeting individuals in critical roles

The Core Problem

There is no lightweight, privacy-respecting, offline-capable solution designed specifically to protect personal endpoints of high-value individuals. Enterprise tools are too heavy, too intrusive, and too dependent on corporate infrastructure. Consumer antivirus is too shallow. The gap is real, it is exploited daily, and until now, it has remained unaddressed.

Nyroxis exists to close it.

4. Our Solution – Nyroxis

A Different Kind of Security

Nyroxis is not another enterprise tool scaled down for personal use. It was designed from the ground up with a single purpose: to bring SOC-grade protection to the personal endpoints of high-value individuals — silently, locally, and without compromise.

The Core Philosophy

Where traditional cybersecurity stops at the office door, Nyroxis begins. It operates on the conviction that the most critical security gap is not technical — it is geographical. The personal device of a decision-maker is as strategically valuable as any corporate server, and it deserves the same level of protection.

How Nyroxis Works

The platform is built around four core components working in concert:

Nyroxis Agent

Continuously collects logs from multiple system channels — processes, network activity, services, scripts, and system events. It normalizes this data in real time, encrypts the payload, and stores everything in a local encrypted database. Nothing leaves the device.

Nyroxis Intelligence

Applies an intelligent rule engine across three detection layers: Detection (27 rules identifying known threat patterns), Correlation (12 rules connecting related events across time and sources), and Chain (2 rules detecting multi-stage attack sequences). When a match is found, the system raises an alert immediately. The rule engine is open to extension by security professionals.

Nyroxis System Guardian

Runs quietly in the Windows system tray, acting as the platform's guardian. It monitors the operational status of all services every 3 seconds, manages database backups, validates the license in real time, checks for updates, and automatically stops services if the license expires — ensuring the entire platform remains active, intact, and trustworthy at all times.

Nyroxis Dashboard

A clear, intuitive interface designed for both security professionals and non-technical users. It provides real-time visibility across events, detections, correlations, and chains, with built-in reporting, forensic search, and an integrated AI/ML analysis engine — all running locally on the user's own machine.

What Makes Nyroxis Different

- Fully offline-capable — no dependency on cloud infrastructure, no data transfer, ever
- Forensic-grade storage — AES-256 encrypted, tamper-resistant, court-admissible
- Lightweight & silent — minimal resource usage, invisible to attackers
- Extensible — security teams can build and deploy custom detection rules
- Multilingual — English, French, and German interface
- Privacy by design — personal data never leaves the user's device

Nyroxis is the missing layer — the protection that starts where enterprise security ends.

5. Architecture & Technology

Overview

Nyroxis is built as a modular, lightweight security platform combining endpoint monitoring, real-time detection, and local AI analysis. Its architecture is designed around three principles: simplicity of deployment, integrity of evidence, and absolute data locality.

Core Components

Component	Role	Key Technology
Nyroxis Agent	Log collection, normalization, encrypted storage	Rust, SQLite, AES-256
Nyroxis Intelligence	Detection, correlation, chain rule engine	Rust, JSON rule engine
Nyroxis System Guardian	Service monitoring, backup, license, updates	Rust, system tray
Nyroxis Dashboard	UI, forensics, AI/ML, reporting	Tauri + WebView

Detection Layers

Layer	Rules	Purpose
nyroxis_detection	27	Identify known threat patterns in individual events
nyroxis_correlations	12	Connect related suspicious events across time and sources
nyroxis_chains	2	Detect multi-stage attack sequences

Technology Stack

Component	Technology
Core Services	Rust
Dashboard	Tauri + WebView
Local Database	SQLite
Encryption	AES-256 (logs), Ed25519 (signatures), SHA-256 (hashing)

Component	Technology
ML Engine	Isolation Forest — pure Rust, no external ML library
Statistical Analysis	Z-Score, IQR, Moving Average — local computation
Platform	Windows (v1.0) — macOS & Linux: Coming Soon

Design Principles

- **Data Locality** — all processing, storage, and analysis happens on the user's device. No cloud, no telemetry, no external transmission of any kind
- **Forensic Integrity** — encrypted, tamper-resistant logs suitable for legal and regulatory proceedings
- **Stealth** — invisible to attackers, non-intrusive for users
- **Extensibility** — rule engine designed for expert customization without system modification
- **Complementarity** — works alongside existing AV, EDR, and enterprise SIEM investments

6. Core Components

Nyroxis Agent — The Collection Engine

Nyroxis Agent is the foundation of the entire platform. Running as a silent Windows service, it operates continuously in the background, ingesting security-relevant data from multiple system channels simultaneously:

- Windows Event Logs (Security, System, Application)
- Network connections and traffic metadata
- Running processes and service activity
- PowerShell and script execution
- File system and registry changes

Each collected event passes through a normalization pipeline that standardizes format, enriches context, and prepares the data for the detection engine. The normalized payload is then encrypted using AES-256 and written to a local SQLite database — on the user's device, under the user's control, with no external transmission at any stage.

Resource usage: approximately 57 MB RAM, 0.1% CPU — suitable for continuous operation on personal laptops without impacting daily productivity.

Nyroxis Intelligence — The Detection Engine

Nyroxis Intelligence is the analytical core of the platform. It operates at high speed across three sequential detection layers, each designed to catch threats at a different level of complexity:

Layer 1 — Detection (27 rules)

Identifies known threat patterns within individual events. Each rule targets a specific indicator of compromise: suspicious process execution, unauthorized service installation, abnormal network behavior, credential access attempts, and more.

Layer 2 — Correlation (12 rules)

Connects related events across time and sources to identify threat patterns that no single event would reveal alone. A failed login followed by a successful one from a different location. A new process spawning immediately after a USB device is connected.

Layer 3 — Chain (2 rules)

Detects multi-stage attack sequences — the kind of coordinated, progressive intrusion that characterizes advanced persistent threats. Chain rules track the evolution of an attack across multiple events and time windows.

Extensible by Design

Security professionals can author new detection, correlation, or chain rules and deploy them directly into the system without modifying core components. Rules follow a structured JSON-based format, making Nyroxis adaptable to emerging threats and specific organizational contexts.

Resource usage: approximately 87 MB RAM, 1.8% CPU.

Nyroxis System Guardian — The Platform Guardian

Nyroxis System Guardian runs quietly as a system tray application (6.5 MB RAM, 0.1% CPU), providing continuous oversight of the entire platform. Its responsibilities are:

Service Monitoring

Every 3 seconds, System Guardian verifies that Nyroxis Agent and Nyroxis Intelligence are running. If either service stops unexpectedly — due to a system event, crash, or deliberate interference — Guardian detects the disruption immediately and can take corrective action.

License Validation

Guardian oversees the HWID-based license framework continuously. If a license expires or is invalidated, Guardian automatically stops both services to enforce compliance. Validation operates entirely offline using AES-GCM encryption and HMAC verification.

Backup Management

All Nyroxis databases are critical forensic assets. Guardian manages scheduled and on-demand backups, monitoring file size, timestamp, and integrity — ensuring that event history is preserved even in the event of hardware failure.

Update Checking

Guardian automatically checks for new versions at configurable intervals, notifying users when updates are available. Critical updates are flagged immediately.

Together, these four components form a self-contained, resilient security fabric — one that monitors, detects, and protects itself, so that the user never has to.

7. AI & Machine Learning Engine

A Different Approach to AI

Most AI-powered security solutions rely on cloud infrastructure — sending telemetry to remote servers for analysis. Nyroxis takes the opposite approach. Every aspect of the Nyroxis AI engine runs locally, on the user's own device. No data is transmitted. No external service is consulted. No behavioral profile ever leaves the machine.

Isolation Forest — Anomaly Detection

At the core of the Nyroxis ML engine is a custom implementation of the Isolation Forest algorithm, built entirely in Rust without dependency on any external machine learning library.

Isolation Forest works by constructing a forest of random decision trees. Anomalous events — those that are statistically rare or structurally unusual — require fewer splits to isolate, and therefore receive a higher anomaly score.

The Nyroxis implementation operates with 100 isolation trees per cycle, 256 samples maximum per tree, and 8 behavioral features per analysis window:

Feature	Description
Event count	Total events in the analysis window
Unique sources	Number of distinct event sources
Unique destinations	Number of distinct network destinations
Hour of day	Time context for behavioral baseline
Day of week	Weekly pattern recognition
Events per hour	Activity rate normalization
New sources ratio	Proportion of previously unseen sources
New destinations ratio	Proportion of previously unseen destinations

Statistical Analysis Engine

Alongside the Isolation Forest, Nyroxis runs a parallel statistical analysis layer providing continuous, interpretable anomaly scoring across all monitored metrics.

Z-Score Classification

Z-Score	Severity	Confidence
> 3.0	Critical	99.7%
> 2.0	High	95%
> 1.5	Medium	86%
> 1.0	Low	68%

Additional Statistical Methods

- **IQR Outlier Detection** — identifies values outside the interquartile range
- **Moving Average** — tracks behavioral trends over configurable time windows
- **Exponential Moving Average** — applies greater weight to recent activity for faster response
- **Spike Detection** — flags sudden deviations from historical norms
- **Correlation Analysis** — measures statistical relationships between independent behavioral signals

Why Local ML Matters

For the individuals Nyroxis protects — executives, legal professionals, public servants — the sensitivity of their behavioral data is itself a security concern. A local ML engine eliminates this risk entirely. The Nyroxis AI engine delivers the analytical depth of cloud-based behavioral intelligence, without the privacy trade-off that cloud dependency requires.

8. Use Cases / Scenarios

Where Nyroxis Delivers Real Impact

Nyroxis was designed for environments where traditional security tools cannot or do not reach. The following scenarios illustrate the real-world contexts in which the platform creates immediate and measurable value.

Scenario 1 — The Executive at Home

A CFO works from home three days a week. His personal laptop has never been enrolled in the corporate EDR system. One evening, a phishing email installs a silent backdoor. The corporate firewall never sees it.

With Nyroxis installed, Nyroxis Agent captures the anomalous process execution the moment it occurs. Nyroxis Intelligence correlates it with a suspicious outbound connection attempt minutes later. An alert is raised before any data leaves the machine. The incident is contained, logged, and forensically preserved — before it becomes a breach.

Scenario 2 — The Legal Professional

A senior judge uses a personal laptop to review case documents outside the courthouse. An attacker injects malicious scripts into browser sessions via a compromised router.

Nyroxis detects the abnormal script execution pattern through its detection rule engine and flags the unusual network behavior through correlation. The judge is alerted. The attempt is documented with forensic-grade evidence. The integrity of the proceedings is preserved.

Scenario 3 — The SOC Administrator

A SOC team leader accesses internal systems remotely at night from a personal device. Attackers target this device specifically, knowing that its compromise could yield direct access to the enterprise environment.

Nyroxis monitors the device continuously, detects credential access attempts and lateral movement indicators through its chain detection layer, and raises a critical alert. The enterprise perimeter is never reached.

Scenario 4 — The Multinational Organization

A holding company with operations across multiple countries faces an inconsistent personal device security landscape. Regional executives travel frequently and use personal devices that vary in security posture from country to country.

Nyroxis provides a unified protection layer deployable across all endpoints regardless of geography. Each installation operates independently, stores data locally, and requires no centralized infrastructure.

Scenario 5 — The Security-Aware Organization

A forward-thinking enterprise deploys Nyroxis as part of a broader internal security awareness and monitoring program. The extensible rule engine allows the security team to write custom detection rules tailored to their specific threat model, enriching existing SOC workflows with personal endpoint data that was previously unavailable.

9. Benefits & Value Proposition

Security That Creates Strategic Value

Cybersecurity is not only a technical discipline — it is a matter of business continuity, institutional trust, and personal safety. Nyroxis delivers value across every level: from the individual user whose device is protected, to the organization whose reputation and operations depend on the people within it.

For Security Leaders — CISO & SOC Teams

- **Visibility Where It Did Not Exist** — extends monitoring reach into personal endpoints that enterprise tools cannot cover
- **Forensic-Grade Evidence** — encrypted, timestamped, tamper-resistant logs accelerate response and support legal proceedings
- **Seamless Integration** — complements existing AV, EDR, and SIEM deployments without adding complexity
- **Extensible Detection** — security teams can write and deploy custom rules tailored to their specific environment

For Senior Management — CEO & Board

- **Protection of Intangible Assets** — safeguards brand reputation, investor confidence, and strategic decision-making capacity
- **Demonstrated Due Diligence** — provides documented, verifiable evidence of active risk management for regulators and auditors
- **Reduced Breach Cost** — detects threats at the personal endpoint before they reach corporate infrastructure

For the Protected Individual — Executive, Professional, Public Servant

- **Silent, Seamless Protection** — runs invisibly in the background, requires no technical expertise, no ongoing interaction
- **Absolute Privacy** — no behavioral data, event log, or personal activity is ever transmitted outside the device
- **Peace of Mind** — genuine confidence that personal devices and family environments are monitored and protected

The Strategic Advantage

Dimension	Without Nyroxis	With Nyroxis
Personal endpoint visibility	None	Full, real-time
Threat detection at home	None	27+12+2 rule layers
Forensic evidence	Unavailable	Encrypted, court-admissible
AI anomaly detection	None	Local Isolation Forest
Data privacy	At risk	Guaranteed — fully local
Compliance posture	Incomplete	GDPR, NIS2, ISO 27001 aligned
User disruption	N/A	Zero

10. Compliance & Standards

Security That Satisfies Regulators

In today's regulatory environment, cybersecurity is evaluated by demonstrable accountability. Organizations must prove that they have actively managed risk across their entire digital ecosystem, including the personal endpoints of key personnel. Nyroxis was designed with this requirement at its core.

European Frameworks

GDPR — General Data Protection Regulation

Nyroxis is built around data minimization and privacy by design. All collected telemetry is encrypted at rest using AES-256. No personal data is transmitted externally. The user retains complete sovereignty over their own data at all times.

NIS2 Directive

NIS2 requires organizations to demonstrate continuous monitoring capability, incident readiness, and active risk management. Nyroxis extends this capability to personal endpoints — precisely the environments most likely to be attacked through.

ENISA Guidelines

Nyroxis aligns with European Union Agency for Cybersecurity best practices for endpoint resilience, behavioral monitoring, and incident documentation.

International Standards

ISO/IEC 27001

Nyroxis supports alignment with the global benchmark for information security management systems. Its forensic-grade logging, structured detection framework, and documented rule engine extend ISMS coverage to personal endpoints.

Forensic Readiness

Every event captured by Nyroxis is encrypted, timestamped, and stored in a tamper-resistant local database — meeting forensic readiness requirements across jurisdictions.

NIST Cybersecurity Framework

NIST Function	Nyroxis Contribution
Identify	Continuous visibility into personal endpoint activity and asset behavior
Protect	Encrypted storage, HWID-based licensing, tamper-resistant architecture
Detect	27 detection rules, 12 correlation rules, 2 chain rules, local ML anomaly detection
Respond	Real-time alerts, forensic evidence, extensible rule engine for rapid adaptation

Compliance Summary

Framework	Nyroxis Alignment
GDPR	Privacy by design, data minimization, local-only storage
NIS2	Continuous monitoring, incident readiness, personal endpoint coverage
ENISA Guidelines	Endpoint resilience, behavioral monitoring, incident documentation
ISO/IEC 27001	Forensic logging, structured detection, ISMS extension
NIST CSF	Identify, Protect, Detect, Respond functions covered
Zero Trust	Continuous verification at personal endpoint level

11. Roadmap

From Foundation to Full Ecosystem

Nyroxis 1.0 represents a fully functional, production-ready platform. The roadmap ahead extends what already works into new environments, new capabilities, and new communities.

Current — Version 1.0 (Available Now)

- Nyroxis Agent — multi-channel log collection, normalization, AES-256 encrypted local storage
- Nyroxis Intelligence — three-layer detection engine (27 detection, 12 correlation, 2 chain rules)
- Nyroxis System Guardian — service monitoring, backup management, license validation, update checking
- Nyroxis Dashboard — real-time visibility, forensic search, detection visualization, reporting
- Local AI/ML Engine — Isolation Forest anomaly detection, statistical analysis, fully offline
- Multilingual interface — English, French, German
- One month free trial

Phase 2 — Platform Expansion

macOS & Linux Support

The Nyroxis agent and dashboard are being extended to macOS and Linux environments — bringing the same level of protection to the full range of personal devices used by executives and professionals. These platforms are actively in development.

Extended Detection Library

New detection, correlation, and chain rules will be released to address emerging threat patterns, with community contributions from security professionals welcomed through the extensible rule engine.

Enhanced ML Capabilities

The local AI engine will be deepened with additional behavioral models, longer baseline windows, and more granular contributing feature analysis — without ever introducing cloud dependency.

Phase 3 — Education & Community

Nyroxis Security Education Program

Nyroxis will launch a structured security education initiative beginning with schools — introducing the next generation to practical cybersecurity thinking through short, focused, and accessible training content. This program reflects the core Nyroxis philosophy: that sustainable security begins with people, not just platforms.

Security Professional Community

The extensible rule engine creates a natural foundation for a practitioner community — a structured channel through which security professionals can contribute, share, and grow the collective detection capability of the platform.

Phase 4 — Enterprise Integration

For enterprises seeking to extend Nyroxis protection across their entire leadership and operational staff, a structured organizational deployment model will provide centralized oversight while preserving the data locality guarantees that define the platform. Nyroxis event data and detection findings will be made available for integration with existing SOC and CSIRT workflows.

Roadmap Summary

Phase	Focus	Status
v1.0	Full Windows platform	✓ Available now
Phase 2	macOS & Linux, extended ML	In development
Phase 3	Education program, community	Launching 2026
Phase 4	Enterprise integration, SOC/CSIRT	Planned

12. Licensing Model

Simple, Transparent, Privacy-Respecting

The Nyroxis licensing model reflects the same principles as the platform itself: simplicity, integrity, and respect for the user. There are no subscription traps, no hidden data collection tied to license validation, and no dependency on external servers to keep the software running.

How Licensing Works

Every Nyroxis license is bound to the user's hardware through a unique identifier derived from the physical characteristics of the device. A cryptographic key is generated from this same hardware profile, creating a license that is:

- **Non-transferable** — tied to the specific device it was issued for
- **Tamper-resistant** — any modification to the license is detected immediately by Nyroxis System Guardian
- **Fully offline** — validation requires no internet connection, no external server, and no ongoing connectivity

Trial

Every new Nyroxis installation includes a one month free trial — providing full access to all platform features without restriction. No credit card is required. The trial period is designed to give individuals and organizations sufficient time to evaluate the complete platform in their real environment.

Licensing Tiers

Tier	Target	Features
Trial	All users	Full platform access — 1 month, no restrictions
Personal	Executives, professionals, individuals	Full platform, single device, HWID-bound
Professional	Security practitioners, consultants	Full platform, custom rule deployment, priority support
Enterprise	Organizations, holdings, institutions	Multi-device deployment, organizational oversight, dedicated support

What Is Always Included

- Nyroxis Agent, Nyroxis Intelligence, Nyroxis System Guardian — complete platform

- Local AI/ML engine — fully offline, no cloud dependency
- Full detection, correlation, and chain rule library
- Multilingual dashboard — English, French, German
- Forensic-grade encrypted local storage
- Database backup management
- Offline license validation

What Is Never Included

- No telemetry sent to Nyroxis or any third party
- No behavioral data collected for licensing purposes
- No dependency on internet connectivity for platform operation
- No hidden costs tied to data volume or event counts

Contact

Nyroxis Security

www.nyroxis.com | contact@nyroxis.com

Nice, France

13. Dashboard Demonstration

Visibility by Design

The Nyroxis Dashboard is the operational interface of the entire platform. It was designed with two users in mind simultaneously: the security professional who needs precision, depth, and forensic capability — and the non-technical executive who needs clarity, simplicity, and immediate situational awareness.

1. Main Overview

The entry point of the dashboard provides an at-a-glance picture of the current security posture: total events collected in the last 24 hours, active alerts by severity (Critical, High, Warning, Info), real-time event timeline, severity distribution, and system status including agent state, database size, rule engine health, license validity, and backup status.

2. Events

The Events view is the forensic core of the dashboard. It provides complete access to the raw event database with full search, filter, and export capability — including forensic inspection of individual events with full payload detail and export to CSV for legal documentation.

3. Detection

The Detection view presents all findings generated by the Nyroxis Intelligence detection rule layer. Each finding includes the rule that triggered, the specific events that matched, severity classification, timestamp and source information, and a direct link to underlying raw events for forensic drill-down.

4. Correlation

The Correlation view surfaces findings from the 12-rule correlation engine — the patterns that emerge not from individual events, but from the relationships between them. This is where isolated signals become actionable intelligence.

5. Chain

The Chain view presents findings from the most sophisticated detection layer — multi-stage attack sequence detection. Chain findings represent the highest-priority alerts in the system. Each finding includes a full reconstruction of the detected sequence.

6. Reports

The Reports section provides structured, exportable documentation of platform activity and findings. Reports can be generated across configurable time windows and exported in PDF or CSV format — suitable for internal review, regulatory submission, or legal proceedings.

7. AI / ML Analysis

The AI module provides access to the local machine learning engine. Analysts can review anomaly detection findings with contributing feature breakdown, inspect Z-score classifications, track behavioral baseline evolution, and identify statistical outliers. All analysis is performed locally — no data leaves the device at any stage.

8. Settings

The Settings view provides complete platform configuration: database file path, dashboard refresh interval, default lookback window, default sample limit, interface language selection (English, French, German), theme configuration, and hardware ID display for license reference.

9. Backup

The Backup section provides direct management of database backup operations — scheduling, on-demand execution, and backup history. All backup files are encrypted and stored locally, ensuring that forensic evidence is preserved even in the event of primary database corruption.

Designed for Everyone

The Nyroxis Dashboard does not ask its users to choose between power and simplicity. Security professionals have the depth they need — forensic search, rule inspection, correlation analysis, AI-driven anomaly review. Non-technical users have the clarity they need — severity indicators, one-click rule loading, clean visual summaries.

This is the Nyroxis design principle made visible: enterprise-grade protection, accessible to everyone it protects.