OSINT Tools

- Visual Osint (FotoForensics / ExifTool / Risk Score)
- Social Media Search
- Brand Reputation

Visual Osint (FotoForensics / ExifTool / Risk Score)

Overview of the Service

The **Visual OSINT** module — available as part of the NiamonX investigation suite — is an advanced **photo forensics and metadata analysis tool** that helps identify image manipulation, origin, and authenticity indicators.
It integrates multiple forensic technologies — including **FotoForensics-style artifact analysis**, **ExifTool-based metadata extraction**, and **CASIA AI prediction** — to deliver a complete visual intelligence assessment for investigators, journalists, and security analysts.

? What the Tool Does

Visual OSINT performs a deep, server-side forensic analysis of uploaded images, combining pixel-level inspection, metadata parsing, and AI-driven anomaly detection.

Supported file types: **JPEG, PNG, WebP** (up to 25 MB).
Each file is securely uploaded to NiamonX's processing server, analyzed through a FotoForensics-like API, and returned with visual and statistical breakdowns.

The system enforces a **cooldown of 30 seconds per request** and allows up to **90 seconds for processing**.

? Core Analysis Features

1. **Image Forensics (Visual Analysis)**
   The tool generates multiple forensic artifacts and comparisons:
   - **Original / Compressed Copy**
   - **Diff & Amplified Diff** (highlights pixel-level differences)
   - **Overlay & Artifact Grid** (visualizes edited regions)
   - **ELA (Error Level Analysis)** — identifies compression and tampering zones
   - **Noise Map** — isolates sensor and noise inconsistencies
   - **CASIA Prediction** — AI model inference from CASIA dataset to detect manipulation patterns
2. **EXIF & Metadata Extraction**
   Metadata is extracted using **PHP EXIF and ExifTool** modules, including:
   - Camera and software data
   - Creation timestamps
   - GPS coordinates (if embedded)
   - Editing traces and unusual tags
   - Hidden text or string data (binary text extraction)
3. **String Analysis**
   The tool detects **embedded ASCII or Unicode strings**, sometimes hidden within images.
   Long strings can indicate **metadata injection** or **hidden payloads**.
4. **GPS & Geolocation**
   If available, GPS coordinates are extracted and highlighted for quick mapping or cross-verification.

?? Risk Score System

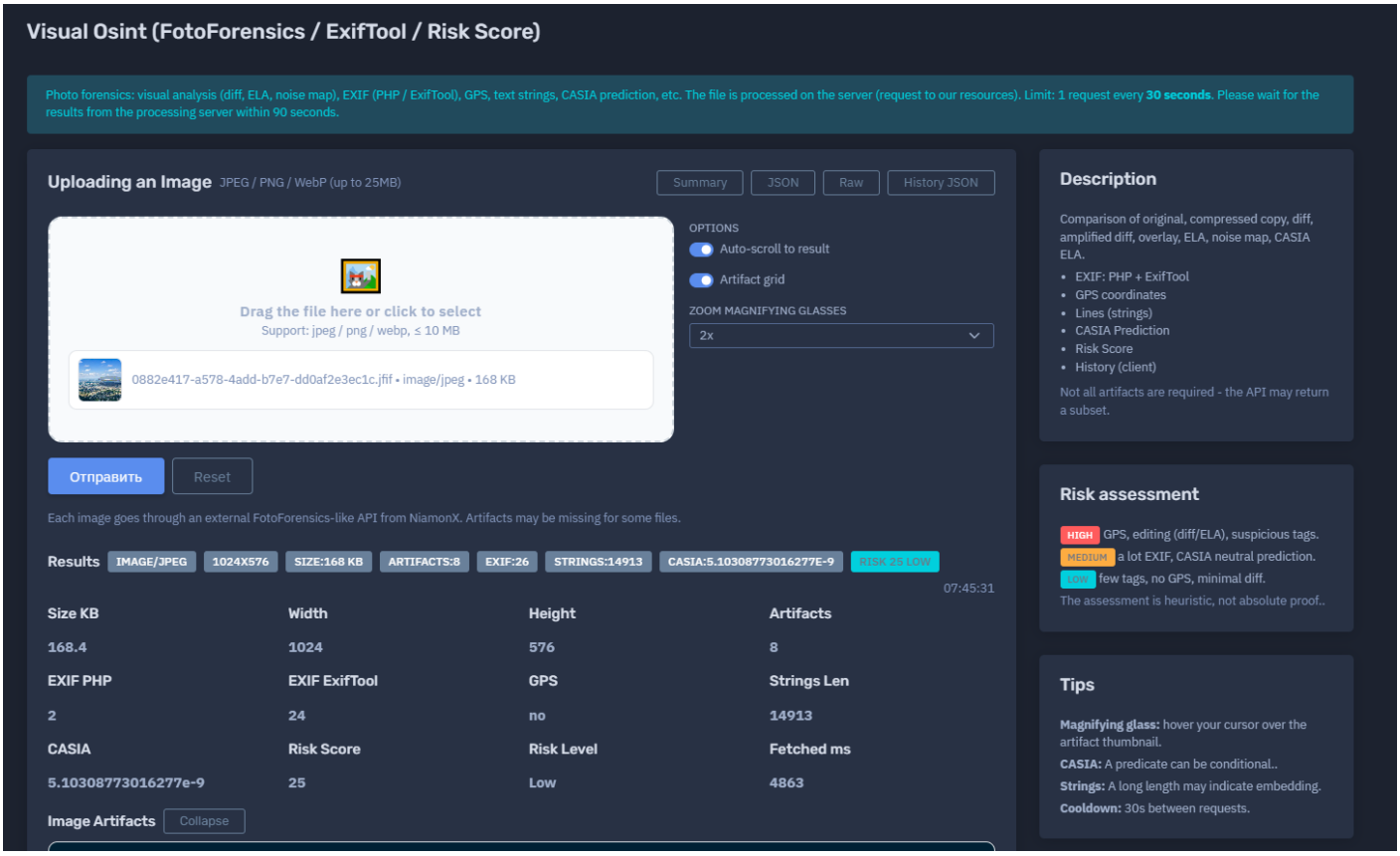
Each image receives a **heuristic Risk Score**, assessing the likelihood of manipulation or sensitive content presence:

- **High Risk:**
  GPS data present, strong ELA/diff indicators, suspicious or inconsistent tags.
- **Medium Risk:**
  Rich EXIF metadata, CASIA neutral or borderline prediction, potential editing hints.
- **Low Risk:**
  Minimal tags, no GPS, stable compression, and no visible tampering evidence.

> ⚠ The score is **heuristic** — not absolute proof — and should be interpreted as an analytical indicator rather than forensic certification.

? Tips for Use

- Hover the mouse over **artifact thumbnails** to use the built-in **magnifying glass (4x zoom)**.
- Enable **auto-scroll** to jump to results automatically after processing.
- Some files may return **partial artifacts** depending on compression level or EXIF structure.
- Long embedded strings or missing ELA layers can be signals of **steganography** or **format re-encoding**.



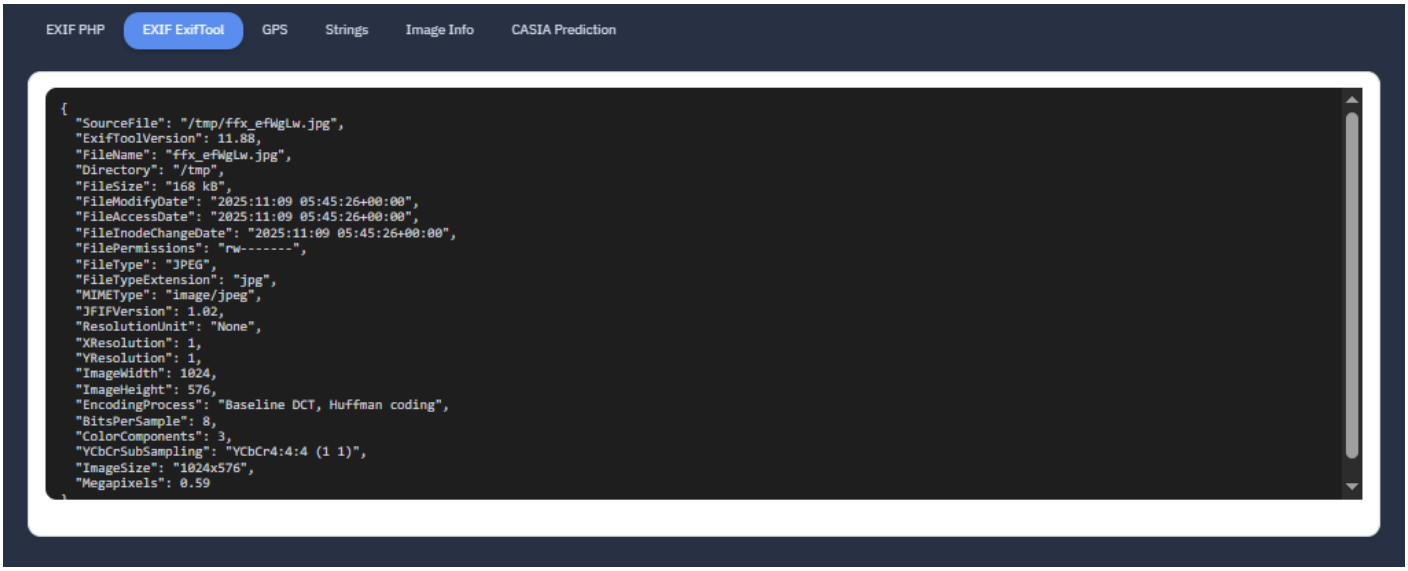
? Request History

- Stored **locally only** (up to 50 entries).
- Records include: filename, file size, GPS presence, calculated risk score, and main detected features.
- No data or images are stored on NiamonX servers after processing completion.

?? Security & Privacy

All image uploads and forensic analyses are processed via **secure, encrypted channels**.
The service never retains or shares the uploaded files or results.
Each request is isolated and deleted after processing to maintain strict **data confidentiality** and **user privacy**.

Users are encouraged to perform analyses only on **legally obtained images** and to respect privacy and consent regulations when handling visual materials.



? Contact Information

For inquiries, assistance, or data-related requests, contact the NiamonX team:

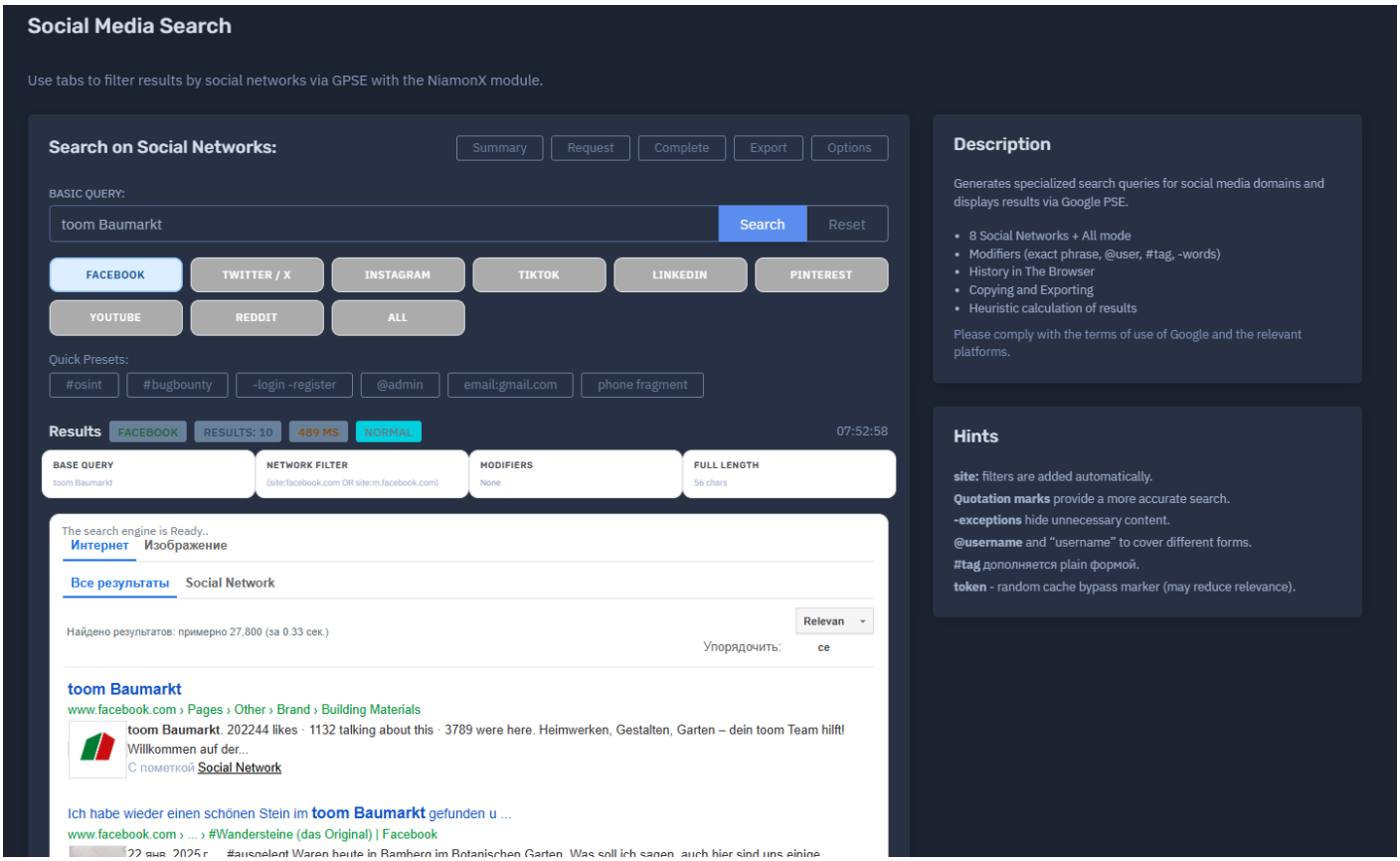
- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Questions
- **takedown @ niamonx.io** — Requests for Data Removal / Privacy Takedowns
- **legal @ niamonx.io** — Legal or Compliance Matters

Alternative contact channel:

□□ **Helpdesk:** https://support.niamonx.io/

In summary, **NiamonX Visual OSINT** is a **comprehensive image forensics platform** combining traditional EXIF metadata inspection, advanced artifact visualization, and AI-driven manipulation detection.
It provides investigators with reliable insights into image authenticity and integrity — while maintaining the highest standards of **security, privacy, and digital ethics**.

Social Media Search



Social Media Search — NiamonX

Link: https://dash.niamonx.io/social_msearch

What it is
The Social Media Search tool is a focused OSINT utility that generates and runs specialized search queries across social media domains using **Google Programmable Search Engine (GPSE)** combined with NiamonX query logic. It helps investigators, analysts, and researchers locate public social footprints quickly by applying network-specific filters, modifiers and heuristics — without scraping protected APIs.

Key functionality

- **Tab-based network filtering:** Switch between tabs for individual social networks (8 supported networks) or run in **All** mode to cover multiple platforms at once.
- **Query types supported:** username, email, keywords, hashtags, mentions, and free-text phrases.
- **Smart query generation:** The interface auto-builds site: and domain-specific queries for each social network using GPSE and NiamonX heuristics.
- **Modifiers & presets:** Use exact-phrase (`"..."`), `@user`, `#tag`, `-excludedword` and other modifiers to refine results. Quick presets speed up common searches.
- **Heuristic scoring:** Results are scored/filtered by a heuristic engine that highlights higher-probability matches (based on signal strength, domain match, recency and pattern matching).
- **History & local storage:** Recent queries are stored locally in the browser (history, filters) for convenience — nothing is pushed to public indexes by the tool itself.
- **Copying & export:** Ability to copy results and export structured lists for reporting or follow-up analysis.
- **Token parameter:** An optional random token parameter can be appended to bypass aggressive caching (note: may reduce relevance).

How the search works (high level)

1. You enter a basic query (username, email, keywords).
2. NiamonX constructs network-aware GPSE queries (site:facebook.com “username”, site:twitter.com @user, etc.) and applies modifiers you selected.
3. GPSE executes the search and returns results; NiamonX post-processes them with heuristic filters and presents ranked results in the UI.
4. You can switch tabs to view results restricted to a given social domain or view aggregated results in All mode.

Because the tool relies on Google’s index, results depend on what Google has crawled and indexed for each social network.

What you can search for

- Public profiles by **username** or handle.
- Mentions or posts containing **emails** or **keywords**.
- **Hashtags** and topical content (`#tag`).
- **Exact phrases** (use quotes) and exclusion filters (`-word`).
- Quick multi-network scans (All mode) for footprint discovery.

Limitations & important notes

- **Depends on Google index:** not a replacement for direct API access to private or rate-limited platform data. If something isn't on Google, the tool won't find it.
- **No protected-data access:** does not access private profiles or bypass platform protections.
- **Token cache-bypass:** using the random token can force fresher Google results but may lower result relevance.
- **Respect platform TOS:** you must comply with Google's and target platforms' terms of service. Abuse may result in blocked access.
- **Local history only:** history is kept in the browser (not shared publicly); sensitive searches should be handled carefully.

Best-practice tips

- Use quotation marks for exact phrase matches.
- Combine `@username` and `"username"` to cover different forms and variations.
- Use `-word` to remove noisy sources from results.
- Try All mode first for broad reconnaissance, then switch to a specific network tab to drill down.
- If results look stale, re-run the query or tweak modifiers (Google index freshness varies).

Privacy & security

- The tool generates queries and shows results via GPSE; it does **not** harvest private data or bypass access controls.
- Query history resides in the user's browser. NiamonX post-processing applies heuristics but does not expose private platform data.
- Use the tool only for lawful, authorized investigations and with respect for privacy.

Contact / support

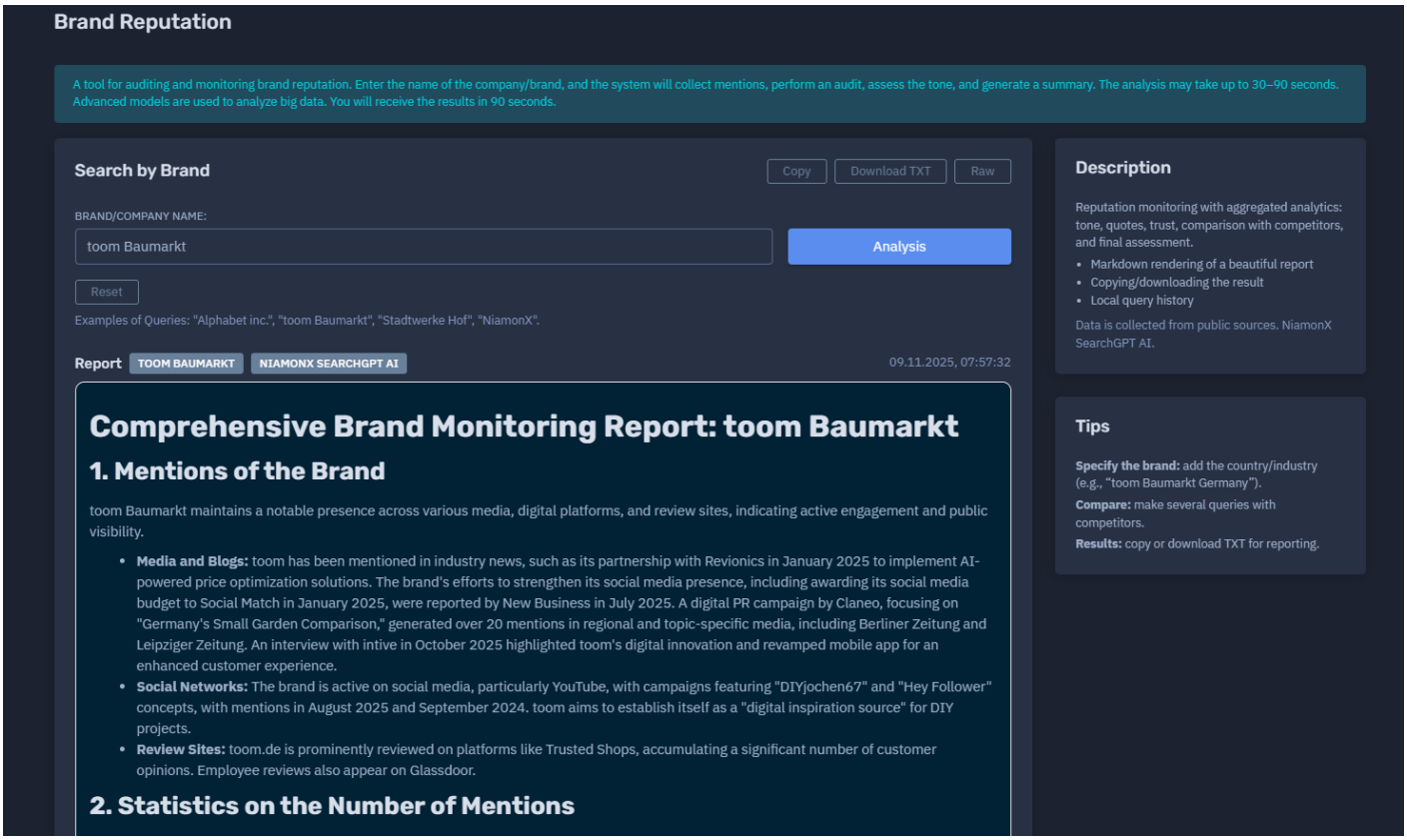
For any questions, reporting issues, or compliance requests, contact the NiamonX team:

- **support @ niamonx.io** — Technical Support
- **other @ niamonx.io** — General Inquiries

- **takedown @ niamonx.io** — Data removal / privacy takedowns
- **legal @ niamonx.io** — Legal / compliance

Alternative channel: **Helpdesk** → https://support.niamonx.io/

Brand Reputation



Brand Reputation — NiamonX

Link: https://dash.niamonx.io/brand_reputation

What it is
The **Brand Reputation** module is a next-generation AI-powered system for **brand perception auditing, sentiment tracking, and trust assessment**. It automatically gathers and analyzes public mentions of any company or brand name, evaluates overall tone and credibility, and generates a structured analytical report in under 90 seconds.

Built on top of **NiamonX SearchGPT AI**, it processes large datasets from multiple open sources, performing sentiment analysis, contextual clustering, and reputation scoring — all securely and locally processed with end-to-end encryption.

Key Functionality

- **Automated Brand Intelligence:** Enter a brand or company name; the system collects public mentions from online sources and performs semantic tone analysis.
- **Tone and Sentiment Detection:** Determines whether general sentiment is positive, neutral, or negative across aggregated mentions.
- **Trust and Risk Analysis:** Evaluates credibility of sources, consistency of tone, and potential risks to brand trust.
- **Comparative Analysis:** Allows comparing your brand's score with competitors (e.g., "toom Baumarkt Germany" vs. "OBI Germany").
- **Comprehensive Report Generation:** Produces a Markdown-formatted summary with sections for tone overview, key quotes, trends, competitor metrics, and final evaluation.
- **Local Query History:** Stores up to 200 recent searches locally (brand names and short previews only — no personal or external data).
- **Copy & Download Options:** Instantly copy or export the report in `.txt` format for presentations or documentation.

How It Works

1. You enter a **brand or company name** (e.g., "Alphabet Inc." or "NiamonX").
2. The engine collects relevant mentions from public data sources.
3. NiamonX AI performs a **multi-layer audit**: text clustering, tone detection, quote extraction, and trust scoring.
4. Within **30–90 seconds**, you receive a detailed Markdown report summarizing findings with sentiment breakdown, trend indicators, and confidence ratings.

What You Can Analyze

- **Corporate and consumer brands** (e.g., "IKEA", "Tesla", "Lufthansa").
- **Institutions or municipalities** (e.g., "Stadtwerke Hof").
- **Startups and emerging brands** (e.g., "NiamonX").
- **Cross-regional or industry-specific brands** ("toom Baumarkt Germany", "Volksbank Berlin").

Report Contents

- **Summary Overview** — concise snapshot of brand tone and reputation level.
- **Tone Analysis** — positive, neutral, negative tone distribution with percentages.
- **Quotes & Mentions** — key extracted phrases and examples.
- **Trust & Source Evaluation** — assessment of data credibility and bias level.

- **Competitor Comparison** — optional comparison with rival brands.
- **Final Assessment** — heuristic reputation score from 0–100 (aggregated).

Markdown rendering ensures each report is **visually clear, structured, and ready for presentation**.

Privacy & Security

- Data is **collected only from public sources** — no hidden APIs or unauthorized data scraping.
- All queries and results are processed through a **secure encrypted channel**.
- Local browser storage is used for history; no external telemetry or analytics.
- Generated reports are transient — not shared or indexed anywhere.

Tips for Best Results

- Add **geographical or industry context** to the query (e.g., “toom Baumarkt Germany”, “Airbus Aerospace”).
- Compare **multiple competitors** for benchmarking.
- Export results as `.txt` or copy Markdown directly into reports.
- Wait the full 90 seconds for the analysis to complete; large datasets require deep semantic evaluation.

Example Use Cases

- **PR & Marketing Teams:** Track brand health, press tone, and audience sentiment.
- **Corporate Analysts:** Monitor changes in brand perception or response to public events.
- **Investors:** Assess brand stability and public trust before funding decisions.
- **Reputation Management Firms:** Automate large-scale audits using AI-based contextual scoring.

Contact / Support

For issues, assistance, or legal inquiries:

Helpdesk: https://support.niamonx.io