

— PRODUCT SHEET · WEB3 MONITORING

Web3 *Monitoring* **On-chain market abuse detection**

Regulatory-grade market abuse detection for crypto-asset service providers under MiCA and ESMA RTS. Monitor on-chain activity and document abusive behaviours in a compliant, audit-ready workflow.

PRODUCT

Web3 Monitoring

CATEGORY

Product sheet

VERSION

2026

FRAMEWORK

MiCA · ESMA RTS

ORIGIN

France · EU

Market abuse detection *for crypto*

Web3 Monitoring detects, explains and documents abusive on-chain behaviours in a compliant, audit-ready workflow, designed for crypto-asset service providers under MiCA and ESMA RTS.

Detection combines deterministic regulatory rules with statistical and AI-assisted behavioural models, reducing false positives while remaining fully explainable. Now with custom detection rules tailored to your own risk profile.

18

BLOCKCHAIN NETWORKS

5

ABUSE TYPOLOGIES

100%

HOSTED IN EUROPE

AUDIT-READY

Every finding is consolidated into audit-ready outputs: STOR-compatible reports (aligned with ESMA RTS Article 16), evidence packs and immutable audit trails, for full traceability and regulatory defensibility.

How *Web3 Monitoring* works

A structured, auditable workflow. Each step transforms raw on-chain activity into actionable, regulator-ready evidence.

01 **Scan request**

Initiated by the compliance team or triggered automatically (API call, dashboard, customer deposit or withdrawal). Defines scope, wallets and risk parameters.

02 **Data ingestion**

Real-time or batch collection of transactions, token transfers and smart contract interactions, sourced from SeqLense's proprietary blockchain indexer.

03 **Normalisation & contextualisation**

Raw data is normalised and enriched: wallet clustering, sequence reconstruction and market context. Transactions are never analysed in isolation.

04 **Behavioural analysis**

Behavioural baselines are established per wallet and group, identifying deviations, coordination patterns and abnormal activity over time.

05 **Abuse detection engine**

Detected behaviours are evaluated through MiCA / ESMA RTS-aligned rules and statistical models, reducing false positives while remaining explainable.

06 **Alert & case management**

When a threshold is met, an alert is generated with reasoning, timelines and evidence. Analysts review, comment, escalate or close cases.

07 **Reporting & regulatory evidence**

All findings are consolidated into audit-ready outputs: STOR-compatible reports, evidence packs and immutable audit trails.

Types of market abuse *detected*

A combination of regulatory rule sets and behavioural analysis covering the full spectrum of on-chain market abuse.



Insider trading

Detection of abnormal trading behaviour potentially linked to the use of non-public or privileged information.

On-chain · Behavioural · MiCA-aligned



Wash trading

Identification of artificial volume generated through self-trading or controlled counterparties.

On-chain · Rule-based · Market integrity



Pump & dump

Detection of rapid price inflation followed by coordinated sell-offs across multiple wallets or entities.

On-chain · Pattern detection · Behavioural



Smurfing

Identification of fund fragmentation across multiple wallets to disguise intent or avoid detection thresholds.

On-chain · Transaction analysis · Risk-based



AI behavioural clustering

Advanced clustering to surface coordinated wallet behaviour, hidden relationships and emerging manipulation patterns.

AI-driven · Behavioural · Explainable

MiCA *market abuse coverage*

Mapping MiCA market abuse monitoring expectations to current Web3 Monitoring capabilities.

MICA REQUIREMENT	REGULATORY EXPECTATION	WEB3 MONITORING COVERAGE
Market abuse signal detection	Identify and monitor indicators of potential market abuse on an ongoing basis.	Continuous on-chain monitoring via behavioural analysis and rule-based models.
Insider trading indicators	Identify transactions potentially executed using inside or non-public information.	Detection of abnormal pre-event behaviour, wallet deviations and temporal correlation.
Market manipulation	Detect manipulative behaviours affecting price formation or market integrity.	Identification of wash trading, pump & dump and coordinated wallet activity.
Transaction structuring	Identify fragmented transactions intended to bypass monitoring thresholds.	Wallet clustering, transaction splitting analysis and cross-wallet linkage.
Monitoring & alerting	Ongoing surveillance mechanisms and timely alerts when risks are identified.	Automated alert generation, risk scoring and analyst review workflows.
Investigation & traceability	Justify decisions, reconstruct events and maintain traceable records.	Evidence timelines, decision logs and immutable audit trails.

This coverage focuses on detection and investigation support. Reporting obligations should be assessed per each organisation's internal compliance procedures.

Architecture & *integration*

Fully managed SaaS platform. Fast, secure and compatible with existing compliance workflows.



Fully managed SaaS

Scanning, analysis, detection and alerting handled within SeqLense infrastructure hosted in Europe.



MCP-ready

An in-house MCP server connects Web3 Monitoring to your AI assistants and agents, with no custom integration.



API & web interface

Submit scans and review alerts via secure API or directly through the SeqLense web interface.

∞ Unified processing

📄 Real-time alerting

EU Hosted in Europe

➔ Secure & scalable

NATIVE MCP

The Model Context Protocol standardises the connection between your AI agents and Web3 Monitoring: your compliance workflows reach detection and alerts directly, within minutes.

Who is *Web3 Monitoring* for

For organisations subject to market abuse monitoring obligations under MiCA and related European frameworks.



Exchanges & trading platforms

Continuous monitoring of on-chain flows; detection of insider trading, wash trading and pump & dump, with escalation-ready evidence.



Custodians & wallet providers

Monitoring of customer deposits and withdrawals, detection of abnormal wallet behaviour and fund fragmentation.



Brokers & intermediaries

Risk-based monitoring aligned with MiCA, without manual transaction review.



Compliance & risk teams

Clear alerts with contextual evidence, structured case management and regulator-ready reporting.

GET STARTED

Launch Web3 Monitoring via MCP, API, webhook or managed onboarding. ·

contact@seqlense.com · seqlense.com

© 2026 Seqlense S.A.S · Making compliance easier.