NOZOMI NETWORKS

WHITE PAPER

Compliance Assessment of Vantage IQ's Clustering Functionality in Context of the EU AI Act

1. Introduction

This white paper presents the findings of a recent audit on the AI-based clustering functionality embedded within Nozomi Networks' Vantage IQ platform. The audit was conducted by an independent third-party auditor based in the European Union to ensure impartiality and alignment with international best practices. The primary objective was to evaluate the system's compliance with the European Union Artificial Intelligence Act (EU AI Act).

Nozomi Networks has proactively addressed these challenges through its AI Governance Program, which establishes internal policies and oversight mechanisms to ensure that AI development aligns with regulatory expectations and organizational values. A cornerstone of this program is transparency—ensuring that AI outputs are explainable, traceable, and auditable. This commitment enhances stakeholder confidence and supports informed decision-making across operational and compliance teams.

2. Context: The EU Artificial Intelligence Act

The European Union Artificial Intelligence Act (EU AI Act) is the world's first comprehensive legal framework for regulating artificial intelligence. Officially adopted in 2024, the Act introduces a risk-based classification system for AI systems, ranging from minimal to unacceptable risk. It mandates stricter requirements for high-risk AI applications, including transparency, human oversight, data governance, and documentation. The regulation aims to ensure that AI technologies deployed within the EU are safe, ethical, and aligned with fundamental rights.

For organizations like Nozomi Networks, which develop AI-driven cybersecurity tools used in critical infrastructure, the EU AI Act provides a clear compliance roadmap. It emphasizes the importance of explainability, traceability, and human-in-the-loop controls—principles that are central to Nozomi's AI Governance Program. Understanding and aligning with the Act is essential not only for legal compliance but also for maintaining trust with customers and regulators across the European market.

3. About Vantage IQ

Vantage IQ is an AI-powered cybersecurity analytics engine designed specifically for Operational Technology (OT) and Internet of Things (IoT) environments. It functions as an add-on to the Nozomi Vantage platform and acts as a virtual SOC analyst in the cloud. Vantage IQ leverages machine learning and generative AI to deliver deep insights, root-cause analysis, and alerts, helping security teams respond faster and more effectively to threats.

4. Audit Overview

The audit focused on assessing the current functional state of Vantage IQ, its level of autonomy, and the potential evolution of its risk classification.

The primary goal was to determine whether Vantage IQ qualifies as an autonomous or high-risk AI system under the EU AI Act.

5. Audit Results

Current Classification

Vantage IQ does not qualify as an autonomous or high-risk AI system. It is categorized under the limited or minimal-risk AI classification, subject to specific governance and transparency measures.

Functional Assessment

Vantage IQ uses unsupervised machine learning (clustering) to identify behavioral similarities among assets, detect anomalies in OT network sessions, and support operator investigations through asset grouping and session classification. The outputs are delivered via visual dashboards that provide actionable insights to support informed decision-making; however, they do not trigger automated enforcement actions and require human review and intervention for execution.

Operational Autonomy

The system is non-autonomous and functions strictly in a decision-support role. There is no automated enforcement based on clustering output, no real-time feedback loops, and no dynamic re-training in production.

Deployment Context

Vantage IQ is used in OT/ICS visibility and triage, not in real-time control or automated mitigation. Clustering outputs are not involved in legally binding or regulatory decision processes.

6. Conclusion

The audit confirms that Vantage IQ currently aligns with the characteristics of a limited-risk AI system. As Nozomi Networks continues to evolve its AI capabilities, particularly in areas such as automated response mechanisms or general-purpose AI, the company remains committed to proactively tracking regulatory developments. A risk-based approach will continue to guide the AI Governance Program, ensuring that future innovations maintain compliance, transparency, and ethical integrity.

For further inquiries regarding this white paper on Nozomi Networks' data protection practices, please contact the compliance team at **compliance@nozominetworks.com**

NOZOMI
NETWORKS

Cybersecurity for OT, IoT and Critical Infrastructure

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com