JIZÔ AI

THE ONLY FULL OPTIONS & ALL-IN-ONE OBSERVABILITY AND DEFENSE PLATFORM.

Based on **in-house Artificial Intelligence**, Jizô AI delivers the most comprehensive visibility into your network with **zero data sharing**, covering both **IT and OT** traffic within a single platform. It unifies advanced **threat detection**, clear **explainability** of ongoing attacks, full network **observability** and deep **forensic visibility**.

The integrated **Response module** enables automated, orchestrated actions across your entire network and cybersecurity ecosystem.

UNMATCHED DETECTION CAPACITIES

> **Built on complete network traffic flow analysis, Jizô AI approaches digital omniscience and omniscience is how you win in cyber defence.**

Jizô AI transforms your network data into actionable intelligence, helping reduce your **time of repair (MTTR) from a day to an hour.**

contact@jizo.ai

.02

CYBER DEFENCE CENTER
SEE EVERYTHING UNDERSTAND EVERYTHING

Jizô AI maps every threat in real time using a natural-language interface, MITRE ATT&CK matrix views, and AI-driven detection that adapts to your network no pre-training, no data sharing.

BEHAVIORAL ANOMALY DETECTION

+ No pre-training required
+ No external data sharing
+ ML confidence score (0–1) per alert
+ Exfiltration, port scan, DDoS detection

MITRE ATT&CK FRAMEWORK

+ 130+ techniques detected in real time
+ Kill chain visualisation
+ Campaign correlation across techniques
+ Enterprise IT and ICS/OT matrices

THREAT INTELLIGENCE

+ Real-time IoC matching
+ IPs, domains, URLs, file hashes
+ STIX 2.1 / TAXII integration
+ Automatic IoC lifecycle management

Monitors 5,000+ metrics : detecting what EDRs and agent-based solutions miss

/ ALERT MANAGEMENT

/ CLASSIFICATION

Critical / High / Medium / Low / Info with automatic escalation and false-positive tuning.

/ NOTIFICATIONS

Email, Slack, webhooks, SMS. Customisable templates per severity.

/ REPORTING & EXPORT

Daily SOC reports, executive weekly summaries, compliance monthly reports PDF, CSV, JSON.

contact@jizo.ai

OBSERVABILITY CENTER

SPOT AND UNDERSTAND ANOMALIES AND MISCONFIGURATION IN YOUR NETWORK

Jizô AI delivers a unified view of your network: topology, AI-driven analytics, performance metrics, DNS supervision and automatic asset discovery all in one platform. Resolve hygiene issues and misconfigurations before they become incidents.

/ NETWORK ANALYTICS

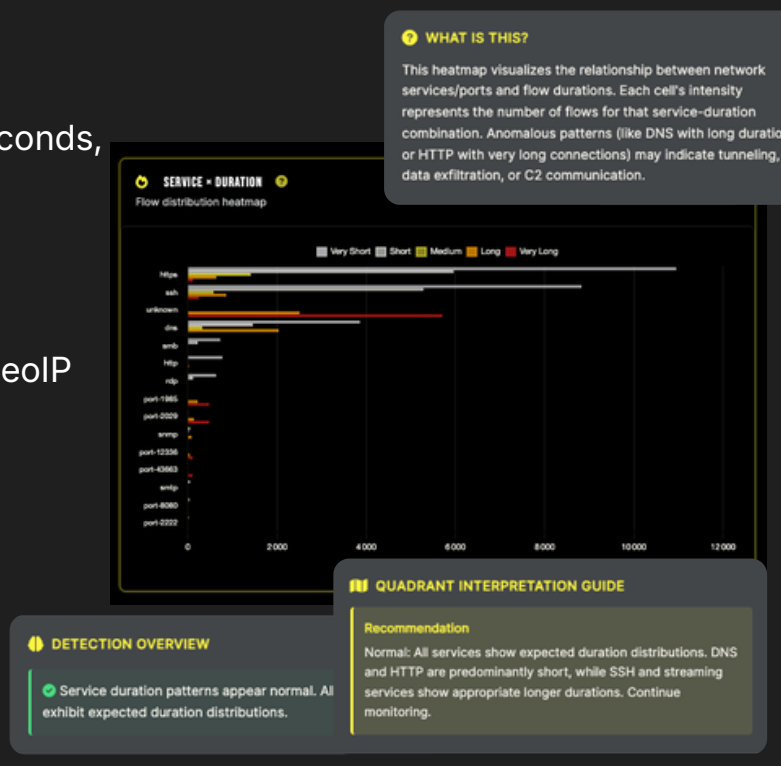
Bandwidth, latency, packet loss in real time. Correlate performance with security events. Prove root cause in seconds, not hours.

/ ASSET ANALYTICS

Auto device enumeration, no agents. Fingerprinting and GeoIP enrichment. Shadow IT exposed

/ CYBER ANALYTICS

ML models profile normal behaviour. Detects exfil, C2 beaconing and lateral movement, no signatures.



THREAT HUNTING AND FORENSICS

Hunt threats across historical data. Reconstruct sessions, decode packets, export forensic evidence : precision capture and scalable retention built into your workflows.

+ DEEP PACKET INSPECTION

Full packet capture, metadata extraction, protocol ID, TLS/SSL fingerprinting.

+ SESSION RECONSTRUCTION

Interactive TCP timeline, colour-coded flows, export to SVG for forensic reporting

+ SESSION VIEWER

Wireshark-style syntax, real-time payload decoding, one-click contextual filtering.

+ FLOW ANALYSIS

NetFlow v5/v9, IPFIX, sFlow sampling, subnet-to-subnet communication matrix.

contact@jizo.ai

JIZÔ ADVISOR

AI THAT TURNS ALERTS INTO DECISION

One question. Full context. Instant decision support without any data leaving your perimeter. Combines your environment (assets, topology, configs, history) with threat intel and known attack techniques.

SAMPLE QUERIES

"What is happening on my network right now?"

"What is my current threat level and risk?"

"Who could be behind this activity?"

"What should I do now?"

+ ADVANCED ANALYSIS

Rapidly understand complex incidents, reduce investigation time, prioritise effectively.

+ DECISION SUPPORT

Structured, explicit analysis enabling confident, informed response decisions.

+ AUTO TICKET GENERATION

Incident summary, risk level, technical description and remediation actions ready to use.

CREATE CASES TO COLLABORATE ON REMEDIATION

Engage your team in investigations and resolutions directly through the platform. Assign, comment, qualify and generate follow-up reports on ongoing threats.

NEW → ASSIGNED → IN PROGRESS → ESCALATED → CLOSED

/ CASE MANAGEMENT

+ Assign cases to analysts
+ Comment and qualify detections
+ Track status with full history

/ REPORTING

+ Structured follow-up reports
+ Linked to ATT&CK detections
+ Full audit trail for compliance

/ INTEGRATIONS

+ Auto ticket creation in Jira
+ Consistent documentation
+ Reduces manual overhead

contact@jizo.ai