TARA
INNOVA

Compliance Report Portal

From Enforcement to Evidence — Automated Compliance Proof

The Challenge

Security works. Threats are blocked. Policies enforced. Incidents handled. But when the auditor arrives and asks "Show me evidence of your access controls" — teams scramble. Logs are exported. Screenshots captured. Spreadsheets assembled. Weeks of manual work to prove what happened in seconds. The gap between security operations and provable compliance costs time, money, and credibility.

The Solution

The Compliance Report Portal turns every security decision across the TARA INNOVA platform into audit-grade evidence — continuously, automatically, and mapped to the regulatory frameworks you operate under. Security without proof does not protect leadership.

Key Capabilities

- **Automatic Evidence Capture** — Every enforcement action becomes an evidence record with tamper-evident integrity, synchronized timestamps, and complete decision context
- **Regulatory Framework Mapping** — Evidence automatically mapped to NIS2, DORA, GDPR, ISO 27001, SOC 2, PCI DSS, NIST CSF, and custom control frameworks
- **Incident Traceability** — Chronological timelines, causal relationships, cross-system correlation across Quicksand, Oasis, and TI Cloud
- **One-Click Report Generation** — Protection, incident, compliance, and audit reports in PDF or JSON with scheduled delivery
- **Role-Based Views** — Security operations, compliance officers, executives, MSP operators, auditors, and regulators each see the right perspective

Report Types

Type	Contents
Protection	Traffic processed, threats blocked by category, protection rates, geographic distribution
Incident	Detection timestamp, classification, impact assessment, response timeline, remediation actions
Compliance	Framework-specific control mapping, evidence inventory, gap analysis
Audit	Evidence packages prepared for external review, auditor access provisions

Use Cases

- **Regulated Enterprises** — Banks, insurers, and healthcare organizations with continuous compliance obligations under NIS2 and DORA
- **Critical Infrastructure** — Energy, utilities, and telecoms operators under heightened regulatory scrutiny
- **Managed Security Providers** — Multi-tenant evidence isolation and client-specific reporting at scale

Why CRP

- **Evidence, Not Reports** — Proof generated at enforcement time, not assembled after the fact.
- **Continuous, Not Periodic** — Compliance documented every moment, automatically. Not quarterly exercises.
- **Immutable Records** — Timestamps that cannot be adjusted. Evidence that cannot be altered or backdated.
- **Cross-Platform Correlation** — Quicksand + TI Cloud + Oasis in a single evidence chain.