TARA INNOVA

Integration Guide

Connecting TARA INNOVA to Your Existing Security Infrastructure

SIEM Integration

TARA INNOVA forwards security events and enforcement decisions to your existing SIEM platform. All major SIEM platforms are supported through standard log forwarding:

- **Syslog** — RFC 5424 structured syslog over TCP/TLS. Compatible with Splunk, QRadar, ArcSight, LogRhythm, and others
- **Webhook** — JSON-formatted events pushed to any HTTP endpoint. Real-time alerting for critical events
- **Log file export** — Structured JSON logs available for collection by any log shipper (Filebeat, Fluentd, Vector)
- **Native ClickHouse** — Direct query access for teams using ClickHouse as their analytics platform

SOAR and Automation

Full REST API enables integration with SOAR platforms and automation workflows:

Operation	API Capability
Policy management	Create, update, and deploy enforcement policies programmatically
Blocklist management	Add/remove IPs, domains, and patterns via API. Bulk operations supported
Incident response	Trigger automated responses — block IP, challenge subnet, escalate to monitor mode
Report generation	Generate compliance and incident reports on demand via API
Threat intelligence	Push and pull indicators through TI Cloud API. Manage feed configurations

Identity and Access Management

TARA INNOVA integrates with your existing identity infrastructure:

- **LDAP / Active Directory** — User authentication for Admin UI and CRP portal
- **SAML 2.0 / OIDC** — Single sign-on with your existing identity provider
- **RBAC** — Map your organizational roles to platform permissions. Least privilege enforcement
- **API keys** — Service-to-service authentication for automation and integration workflows

Monitoring and Observability

Export platform metrics to your existing monitoring stack:

- **Prometheus-compatible** — Metrics endpoint for scraping by Prometheus, Grafana, Datadog, or New Relic
- **Health endpoints** — Standard health check endpoints for load balancers and orchestrators
- **Custom dashboards** — Grafana dashboard templates provided for common monitoring scenarios
- **Alerting** — Webhook-based alerts for threshold breaches, anomalies, and critical security events

Network Infrastructure

Quicksand integrates with your existing network infrastructure:

- **Load balancers** — Works behind any L4/L7 load balancer. Health check endpoints provided
- **CDN compatibility** — Deploy behind or alongside CDN providers. X-Forwarded-For chain preserved
- **DNS integration** — Simple DNS change to route traffic through Quicksand. No application changes required
- **Certificate management** — Supports ACME (Let's Encrypt), custom certificates, and automated renewal

Data Export

All platform data is exportable in standard formats:

- **Reports** — PDF and JSON export for compliance, incident, and protection reports
- **Raw data** — ClickHouse SQL access for custom analytics and data warehouse integration
- **Threat intelligence** — Export indicators in standard formats for sharing with external platforms
- **Audit logs** — Full export capability for archival, legal hold, and external audit requirements

© 2026 TARA INNOVA. All rights reserved. European Union headquarters. EU data sovereignty by design.