Blog Post 6: The Ironclad Gateway – Security, Identity, and Encryption

The Security Imperative Disaster data is sensitive. It reveals the vulnerabilities of critical infrastructure and the precise location of at-risk populations. PANTHEON implements a "Defense in Depth" security strategy aligned with GDPR and ISO 27001 standards.

Identity & Access Management (IAM) We utilize Keycloak as the central authentication broker.

- Single Sign-On (SSO): Users log in once to access dashboards, APIs, and simulation tools.
- Role-Based Access Control (RBAC): Access is strictly scoped. A "Researcher" may see historical anonymized data, while a "First Responder" sees live operational feeds.
- Token-Based API Access: All API calls require a valid JWT (JSON Web Token) in the header.

Encryption Standards

- In Transit: All data transmission—whether internal (Kafka streams) or external (User APIs)—is secured via TLS 1.2+.
- At Rest: Data stored in PostgreSQL and MinIO is encrypted using AES-256.
- Key Management: Cryptographic keys are rotated regularly (90-180 days) and stored in secure vaults.

System-Specific Hardening

- Kafka: Uses SASL/OAUTHBEARER for client authentication and ACLs (Access Control Lists) to restrict which components can write to specific topics.
- PostgreSQL: Implements Row-Level Security (RLS) to restrict access to sensitive table rows based on user roles.