Blog Post 5: The Technical Backbone – Infrastructure and Security

Ensuring PANTHEON runs reliably requires a robust underlying IT infrastructure, focusing on secure, asynchronous communication and scalable deployment.

Asynchronous Messaging with Kafka

Given the non-deterministic nature of disaster data processing (some tasks take milliseconds, others hours), PANTHEON uses an asynchronous messaging broker. **Apache Kafka** was selected over alternatives like RabbitMQ because of its persistence capabilities—Kafka acts as a log, retaining messages by default, which is crucial for data recovery and audit trails in disaster scenarios.

Orchestration and Security

- **Containerization:** The platform uses **Docker Swarm** for service orchestration, favoured for its simplicity and ease of setup compared to Kubernetes for this specific implementation context.
- **Workflow Management: Apache Airflow** manages complex data pipelines, chosen for its extensibility and dynamic Python-based pipeline generation.
- **User Management:** Security is managed via **Keycloak**, providing Single-Sign-On (SSO), OAuth 2.0 support, and role-based access control (RBAC) to ensure sensitive disaster data is only accessible to authorized personnel.

This infrastructure allows PANTHEON to be deployed on-premises (for maximum data security within a first responder organization) or in a hybrid cloud environment to leverage greater computational resources for heavy simulations.