Deployment Topology (Center + Optional Clients)

Client Nodes (Linux only)

Sensors
Falco / Filebeat / Suricata → RabbitMQ
(data.* queues) → Pull API
Go backend
GET /falco /filebeat /suricata

Center Node (macOS/Linux)

poll incremental
(client_poller)

Host Processes

Frontend UI
Next.js
:3000 —HTTP→ Backend API
FastAPI
:8001 —ECS→Graph / queries→

Docker Compose (backend/docker-compose.yml)

Neo4j
HTTP :7474
Bolt :7687

OpenSearch Dashboards
HTTP :5601 —dev UI→ OpenSearch
HTTPS :9200

store/search