1) Qué es realmente Palantir (visión rápida y correcta)

Palantir es un fabricante de software de misión crítica para gobierno y empresa. Sus tres pilares tecnológicos son:

- **Gotham**: "OS" de analistas y operaciones para defensa/inteligencia (fusión de datos operativos, investigación, targeting, misión). Última generación: **Gotham Europa** para colaboración segura multi-dominio y datos sensibles.
- **Foundry**: plataforma de datos/operaciones que normaliza, gobierna y **operacionaliza** IA sobre una **Ontología** (modelo operativo del negocio que conecta datos, modelos y acciones).
- **Apollo**: "mission control" de **DevSecOps** para desplegar, monitorizar y **actualizar software en el edge y en dominios clasificados** (incluye mecanismos para entornos air-gapped).
- **AIP (Artificial Intelligence Platform)**: capa para **agentes de IA** (LLMs) operando sobre la Ontología con **acciones controladas, auditoría y sandboxing**; integra SDKs (Python/Java/TypeScript) y herramientas para construir asistentes que **leen y escriben** sobre procesos reales.

En defensa, Palantir lidera programas como **TITAN** (nodo táctico de targeting con IA, prototipos financiados por el US Army) y **Project Maven / Maven Smart System** (expandido a miles de usuarios DoD).

---

2) La tecnología clave (para que podamos "hablar Palantir")

2.1 Ontología (Foundry)

- Es la **capa operativa** que mapea entidades reales (activos, unidades, sensores, incidencias, órdenes, pagos) y sus relaciones/acciones; enlaza datos crudos + modelos + workflows con **controles de acceso a nivel de objeto/acción**.
- Ventajas: **trazabilidad** (Data Lineage), **retenciones lineage-aware**, rollback transaccional, **materializaciones** para estado "vivo".
- **Interoperabilidad**: arquitectura abierta, integración con IDEs (Jupyter/RStudio) vía Code Workspaces y SDK/OSDK; integra fuentes REST/Webhooks y "external transforms" para sistemas externos.

Traducción a tu caso: nuestra Ontología modelaría **trazabilidad logística/militar** (personas/roles, unidades, dispositivos IoT/drones, lotes, eventos de cadena de

suministro, evidencias, contratos, tokens on-chain, KYC/AML), y **acciones** (por ejemplo: “emitir alerta”, “abrir expediente”, “bloquear activo”, “generar parte”, “firmar hash on-chain”).

2.2 Seguridad y gobernanza

- **Modelo de seguridad granular** (obligatorio/discrecional), **marcados y roles**, **restricted views** (filtrado a nivel de fila/objeto), **cifrado**, **audit logging** exhaustivo.
- **Data Lineage** interactivo y gobierno de lifecycle para datos y modelos (histórico, releases, métricas).
- En AIP, los **Agentes** se “encierran” en un **control plane** de acciones/recursos con permisos mínimos necesarios.

Traducción a tu caso: podemos certificar **quién vio/accionó qué** (cadena de custodia), aplicar **políticas ABAC/RBAC** (por unidad, rango, país, contrato) y **doble control humano** para acciones críticas (por ejemplo, “desplegar alerta táctica” o “congelar un lote").

2.3 AIP y Agent Studio (IA operativa)

- Construyes **Agentes de IA** que consultan la Ontología, ejecutan **acciones** (con confirmación humana opcional) y llaman herramientas (retrieval, consultas de objetos, edición). **APIs/SDK** para integrarlos en apps externas.
- Toolchain con **AIP Logic** (funciones agentic), **Ontology SDK** (Py/Java/TS) y **MCP** para conectar IDEs/otros agentes a tu Ontología.

Traducción a tu caso: agentes que **vigilan sensores**, consolidan **anomalías** de múltiples fuentes, **reconcilian** eventos con evidencia on-chain, y proponen **resoluciones** (abrir investigación, bloquear proveedor, ordenar inspección) para **aprobación humana**.

2.4 Apollo (DevSecOps + Edge + dominios clasificados)

- Despliegues **autónomos** y observabilidad en flotas heterogéneas, **rollback** seguro, operación en **entornos desconectados/air-gapped** con **Binary Transfer Service** para mover binarios/metadatos entre dominios.
- **Edge AI**: entrenar, gestionar y desplegar modelos donde corren los sensores; “write once, deploy anywhere”.

Traducción a tu caso: paquetes de IA/analítica al **borde** (bases, vehículos, UAV/UxV, puestos de control) con **rutas de actualización controladas** y **canales entre dominios** (no clasificado → clasificado).

2.5 Casos y contratos de defensa (contexto)

- **TITAN (US Army)**: nodo táctico de targeting multi-sensor con IA; contrato de **178,4 M$** para 10 prototipos.
- **Project Maven / Maven Smart System**: contrato DoD de **480 M$** para escalar uso global; ampliación de usuarios de "cientos" a "miles".
- Uso en **Ucrania** (fusión de inteligencia, targeting, desminado, crímenes de guerra) — útil para entender **capacidad real en zona de conflicto**.

---

3) Qué necesitamos dominar (lista de conocimientos y decisiones previas)

A. Dominio y Ontología operacional

1. Mapa de **entidades**: unidades, roles/rangos, instalaciones, dispositivos (drones/sensores), proveedores, rutas, activos, lotes, incidentes, órdenes, contratos, **tokens** y wallets, evidencias.
2. **Relaciones** y **acciones**: quién puede hacer qué (acciones aprobables), flujos de **investigación** y **resolución**.
3. **Esquema de datos**: fuentes (SIGINT/OSINT/IMINT, IoT, ERP/SCM, logs blockchain, KYC), **frecuencias** y **SLAs**.

B. Seguridad, cumplimiento y gobernanza
4) **Política de accesos** (RBAC/ABAC por misión/país/contrato); **marcados** y **restricted views** por necesidad.
5) **Auditoría** y **cadena de custodia** (lineage, retenciones, export de evidencias).
6) **Operación en dominios clasificados y edge** (rutas BTS, espejos air-gapped, releases y rollback).

C. IA operativa (AIP)
7) **Casos de agente** (detección/alerta, correlación multi-sensor, priorización, propuesta de medidas, verificación humana).
8) **Tooling** (AIP Logic, OSDK, APIs) y **reglas de seguridad** del agente (acciones permitidas; confirmación obligatoria).
9) **Datasets de entrenamiento/validación** y **métricas** (recall/precision por tipo de amenaza, latencias en edge).

D. Integración blockchain (tu ventaja competitiva)
10) **Modelo on-chain**: qué se firma/hash-ea (evidencias, órdenes, inventario, hand-over), qué se tokeniza (identidades soberanas, permisos de acceso, activos logísticos/contratos), cómo se reconcilia **off-chain↔on-chain** en la Ontología.
11) **Cumplimiento**: KYC/AML, privacidad, jurisdicciones (ES/EU/UAE/US), retención de datos, redacción de **SOPs** (por ejemplo, "cada apertura de expediente

genera hash y NFT de prueba de existencia con policy X").
12) **Integraciones**: indexado de cadenas (Polygon, Base, Arbitrum…), **webhooks/ETL** a Foundry, claves y HSM, **segregación de permisos** para agentes.

E. DevSecOps con Apollo
13) **Arquitectura de despliegue** (cloud soberano / on-prem / edge mixto).
14) **Estrategia de dominios** (N, S, TS…), **BTS** y ciclo de parches; telemetría y **SLOs** en cada teatro.

F. Alianzas y "go-to-market" defensa
15) **Interoperabilidad** con contratista militar (estándares STANAG/NATO, formatos MISB/COT, ATAK, Link-16* si aplica) y **documentación** para ATO/autoridad certificadora.
16) **Casos de uso ancla**: seguridad de instalaciones, **trazabilidad de suministros críticos**, anti-fraude mantenimiento, contra-dron/UxS (sensor fusion), **compliance y auditoría** multi-actor.

---

4) Propuesta de integración (cómo encajaría nuestra tecnología con Palantir)

Capa de datos y Ontología (Foundry):

- Indexar **telemetría de sensores**, logs de UAV/UxV, ERP/SCM del contratista, documentos tácticos, **eventos on-chain** (hashes/evidencias, tokens), y fuentes OSINT.
- Ontología con objetos **Asset, Unit, Device, Route, Incident, Evidence, Contract, Token, Wallet, Alert, Inspection**, etc., y **acciones**: open_case, lock_asset, escalate, issue_token, verify_hash, flag_provider.

Agentes AIP:

- Agente **"Fusion & Triage"**: correlaciona anomalías (sensor + OSINT + ERP + on-chain), puntúa riesgo, **propone** medidas.
- Agente **"Evidence & Compliance"**: mantiene **cadena de custodia**, firma hash on-chain, verifica permisos, prepara dossier **audit-ready**.
- Agente **"Supply Shield"**: trazabilidad de **piezas y mantenimiento** con señales de manipulación; cruza con inventario/tokenización.

DevSecOps (Apollo):

- Paquetes de agentes y módulos de ingestión a **edge** (puertas de base, convoyes, drones), con **rutas BTS** para promover releases entre dominios y **observabilidad** continua.

---

5) Esqueleto del dosier para socios (listo para redactar)

1. **Resumen ejecutivo** (objetivo, impacto, ROI operativo)
2. **Contexto de mercado defensa** (tendencias IA/edge, compliance, riesgos éticos → "human-in-the-loop") con referencias actuales (TITAN/Maven).
3. **Arquitectura propuesta** (diagrama de 3 capas: datos/Ontología, IA/AIP, despliegue/Apollo)
4. **Casos de uso prioritarios** (3–5 quick wins medibles en 90 días)
5. **Diseño de Ontología** (objetos, links, acciones, permisos)
6. **IA operativa (AIP)**: agentes, prompts controlados, validaciones, auditoría
7. **Seguridad y gobernanza** (RBAC/ABAC, lineage, retenciones, export forense)
8. **Blockchain & trazabilidad** (qué se tokeniza/hashea, reconciliación Foundry↔chain)
9. **DevSecOps (Apollo/Edge)**: dominios clasificados, air-gapped, BTS, SLOs
10. **Plan de integración con contratista militar** (estándares, roles, RACI, plan de pruebas en campo)
11. **Roadmap 0-12 meses** (Fase 0 PoC → Fase 3 despliegue multibase)
12. **Riesgos y mitigaciones** (técnicos/legales/éticos)
13. **Anexos**: fichas técnicas, políticas de acceso, matrices de permisos, KPIs, glosario

Si te va bien, en la siguiente respuesta te lo **redacto completo** en formato presentación o documento (ES/EN), con tablas y anexos.

---

6) Detalle ampliado

- **Plataforma y docs oficiales**: visión de AIP/Foundry/Apollo, incluyendo SDKs y features para crear apps y agentes con control de permisos y auditoría.
- **Europa (Gotham)**: colaboración segura **multi-dominio** sobre datos muy sensibles; útil para coaliciones y contratistas.
- **Edge AI**: despliegues en sensores y plataformas tácticas; entreno/gestión de modelos en campo.

- **Air-gapped y dominios clasificados**: estrategia **BTS** para mover binarios/metadata entre niveles; operaciones “Day-2” en entornos desconectados.
- **Contratos relevantes** (señal de capacidad en defensa): **TITAN** (178,4 M$ prototipos), **Maven** (480 M$, expansión usuarios).