LIONSPACE — Unified Master Plan

מסמך זה מאחד את כל תכניות העבודה הקיימות (MEGA/UNIFIED/COMPLETE, system_design, feature_status, technical_debt, phase reports, deployment summaries) למסמך־על אחד, קוהרנטי וברור. הוא כתוב בעברית עם מונחים טכניים באנגלית היכן שנדרש. אין נספחים; אין שכפולים; אין אזכורי רג׳קס/כללי מסווג — רק התוכן הקנוני.

גרסת מסמך: 07-09-2025 • מצב: Pre-Production (עם חסרים מהותיים)

---

1) חזון ומטרות הפלטפורמה

LIONSPACE היא פלטפורמת Cognitive Warfare/OSINT מודרנית שמעניקה למשתמש מקצועי "עמדת מודיעין" אזרחית מתקדמת: איסוף, ניתוח, זיהוי נרטיבים, ניטור איומים, ובניית קמפייני השפעה נגדיים (Prebunk/Debunk/Counter-Narrative) — בממשק Web טרמינלי מהיר ונקי.

עיקרי החזון:
- "Arm Yourself with the Truth" — מנוע אמת פרגמטי הבנוי על Data + AI + ניתוח אנושי.
- חוויית "War-Room Terminal" עם Dashboard חי, Threat Feed, ו־Workflows סדורים.
- שקיפות מלאה: כל טענה נשענת על מקורות ניתנים לאימות (OSINT + לוגים מערכתיים).

יעדים טכניים (יעדי ליבה):
- מובייל/דסקטופ מהירים (LCP ≤ 1.5s, Lighthouse ≥ 95), אבטחה חזקה (RBAC, CSP, Rate-Limit), ותצורת פרודקשן ניתנת לסקייל.
- אינטגרציה ל-(Google Generative AI) Gemini כ־Analysis Engine, עם יכולת החלפה/ריבוי מודלים בהמשך.

---

2) תחום וכיסוי (In-Scope / Out-of-Scope)

In-Scope (שלב V1):

- Web App רספונסיבי (Next.js 15, App Router) + API Routes.
- מנוע זיהוי/מעקב נרטיבים (AI + חוקים), OSINT Intake/Archive, Threat Feed חי.
- קמפייני נגד (Counter/Prebunk/Debunk) עם תבניות מבוססות נתונים.
- Dashboard מדדים + אנליזות (KPIs, תובנות AI, מצב מערכת).
- Auth (OAuth Google) + RBAC בסיסי; PostgreSQL + Prisma; Observability בסיסי.

Out-of-Scope (V1):

- מובייל native; ML מודל־בית; תשלומים; הרחבות Marketplace; Kubernetes מלא (אלא אם יידרש סקל).

---

3) יכולות ליבה ו-Use-Cases

יכולות:

1. Threat Intelligence: זיהוי נרטיבים/איומים, תיוג חומרה, מעקב בזמן אמת, והיסטוריית אירועים.
2. OSINT Operations: איסוף ממקורות פתוחים, אימות, ארכוב, חיפוש מתקדם, הפקה לדוחות.
3. Counter-Operations: יצירת קמפייני השפעה נגדיים (תבניות, פרסונות, ערוצים) עם A/B ו-KPIs.
4. Analytics & Reporting: דשבורדים חיים, דוחות PDF/HTML, יצוא נתונים.
5. Governance & Security: הרשאות תפקידיות, לוגים, מעקב פעילות, ניהול סודות.

Use-Cases טיפוסיים:

- Analyst בודק גל דה-מידע, מפיק הערכת מצב, ומפעיל קמפיין נגד.
- Team Lead פוקח דשבורד מטריקות (Threats/Campaigns) ומאשר פעולות.
- OSINT Operator מעלה מקורות, מתייג ומאמת, ומייצא ראיות לדוח.

---

4) ארכיטקטורה לוגית (ללא קוד)

שכבות מערכת:

1. Client (Next.js Web): ממשקי Dashboard/War-Room/OSINT/Reports; state קל; i18n + RTL.

2. API Gateway (Next.js API Routes): אימות, Rate-Limit, ולידציה (Zod), תקנון תגובות/שגיאות.
3. Services (Business Layer):
- IntelligenceEngine (AI orchestration, narrative tracking, threat scoring)
- OSINTService (ingest, verify, archive, search)
- CampaignService (generate/optimize/track)
- AnalyticsService (metrics/events/dashboards)
4. Data Layer: PostgreSQL (Prisma), Redis (cache), Object Storage לקבצים (GCS/S3).
5. Integrations: Google OAuth, Gemini API, News APIs, Sentry, Vercel Analytics.

עקרונות:
- "API-First": כל פעולה נסגרת ב-API עם סוגי נתונים קבועים.
- "Secure by Default": RBAC, CSP, CSRF, ולידציה קפדנית, Rate-Limit.
- "Observability-Ready": טרייסים, לוגים מבניים, מטריקות עסקיות וטכניות.

---

5) מודולים/שירותים ותפקידם (תיאורי)

- AuthService: OAuth Google (NextAuth), JWT/Sessions, RBAC (roles: admin, analyst, viewer), ניהול פרופיל.
- IntelligenceEngine: ניתוחי Gemini, חישוב Threat Score, קלסטר נרטיבים, עדכוני real-time (SSE/WebSocket).
- OSINTService: איסוף/ייבוא, אימות, ארכוב, אינדוקס חיפוש; ניהול מקורות ותיעוד אמינות.
- CampaignService: תבניות Counter/Prebunk/Debunk, יצירה וטיוב, ניטור ביצועים, יצוא.
- AnalyticsService: KPIs/metrics, Dashboards, Alerts; שילוב Vercel Analytics + Sentry.
- AdminService: ניהול משתמשים/תפקידים, קונפיג, לוגים, יצוא ביקורות.

---

6) נתונים ושכבת אינטגרציה (בקצרה)

מודל בסיסי (טבלאי):
- users, sessions — חשבונות וגישה.

- intelligence_reports — דוחות ניתוח (content, analysis, threat_level, status).
- campaigns — קמפיינים (objectives, audiences, channels, metrics).
- osint_data — נתוני OSINT (source, content, metadata, verified, indicators).

זרימות עיקריות:
- Client → API → IntelligenceEngine (AI call) → persist report → Dashboard/Threat Feed מתעדכן.
- Ingest → Verify → Archive → Search/Export (OSINT lifecycle).

אינטגרציות:
- Google OAuth (Auth), Gemini (AI), Sentry (Errors), News APIs (איסוף), GCS/S3 (קבצים).

---

7) אבטחה, הרשאות ומדיניות

Authentication/Authorization:
- OAuth2 (Google), NextAuth, JWT/Sessions; RBAC תפקידים; MFA בהמשך.

Application Security:
- ולידציה (Zod), הגנת CSRF, Rate-Limit, כותרות אבטחה (CSP/Strict-Transport-Security/Frame-Options), הימנעות מחשיפת מפתחות בקוד/מסמכים.

Data Security:
- הצפנה בתעבורה (TLS 1.3) ובמנוחה (AES-256), מסכות PII, Audit Logs, מדיניות שמירה/מחיקה, גיבויים מוצפנים.

Privacy/Compliance:
- הכנה ל-GDPR/CCPA (זכויות גישה/מחיקה, שקיפות עיבוד, DPA).

---

8) תפעול, ניטור ו-SLO/KPIs

SLO יעד:
• זמינות 99.9%, זמן תגובה API p95 < 200ms, שגיאות < 0.1%.

Observability:
• Sentry (שגיאות), Vercel Analytics (ביצועים), לוגים מבניים, מטריקות מותאמות (activeUsers, analysisCount, threatDetections, cpu/mem/db).

KPIs עסקיים/שימוש:
• Engagement (>5m session), Retention (>40% WAU), שימוש ≥ 3 פיצ׳רים לסשן, קצב גידול 20% MoM.

---

9) מפת דרך מרוכזת (Roadmap)

Phase 0 — Stabilize (Days 1-3)
• תיקון build, סיום exports/Routes/TS, סידור env, ריצת smoke על כל המסכים.

Phase 1 — Auth + Data (Week 1)
• NextAuth עם Google, מודל users/sessions, הגנת RBAC; בחירת DB (PostgreSQL/Supabase), Prisma + מיגרציות.

Phase 2 — Intelligence Core (Weeks 2-3)
• חיבור /intelligence endpoints, Gemini/*, שמירת Threat Feed, reports חי, Dashboard אמיתי.

Phase 3 — OSINT + Archive (Week 4)
• Intake/Verify/Archive/Search, ניהול מקורות, יצוא דוחות.

Phase 4 — Campaigns (Weeks 5-6)
• תבניות Generator, Counter/Prebunk/Debunk, ניטור ביצועים.

Phase 5 — Hardening & QA (Week 7)
• בדיקות (Unit/Int/E2E), ביצועים (Code-split/Lazy), אבטחה (CSP/Rate-Limit), Docs.

Phase 6 — Launch (Week 8)

- Deploy מלא, דומיין, מטמונים/CDN, גיבויים, מעקב פוסט-השקה.

---

10) סיכוני מפתח והנחות עבודה

סיכונים:

- חשיפת סודות/מפתחות היסטוריים — נדרש סקר סודות והחלפה.
- תלות גבוהה במודל יחיד (Gemini) — יש להכין ממשק pluggable לריבוי מודלים.
- חסר Backend/Data כיום — דורש תיאום זמנים ומשאבים (3–6 שבועות).
- ביצועים/סקיילינג — ללא Cache/Queue תיתכן שחיקה ב-p95.

הנחות:

- Vercel + GCP זמינים; PostgreSQL מנוהל (Supabase) מועדף ל-TTV מהיר; Redis מנוהל (Upstash).
- צוות 3–4 מפתחים בספרינט דו-שבועי; תעדוף אבטחה/תפעול מוקדם.

---

11) מפת שמות מאוחדת (Alias Map)

שם במקורות	שם קאנוני	הערות
LIONSPACE	LionSpace / LIONSPACE / lionspace-next	שם הפלטפורמה
Intelligence Engine	cognitive-warrior	רכיב/יכולת ניתוח ואיתור נרטיבים
War-Room	War Room	מסך/אזור מבצעי בזמן אמת
Platform	Unified Platform / platform	אזור מאוחד בתוך האפליקציה
Analytics	News Pulse / Analytics	מודול מדדים/ניתוח חדשותי
Investigation Terminal	Investigation Terminal	טרמינל חקירתי (CLI UI)
Counter Ops	Prebunk/Debunk/Counter-Narrative	משפחת יכולות לקמפיינים נגדיים

הערה: טבלת הכינויים תתרחב תוך כדי אינטגרציה מול הקוד והקונפיג (שלב הבא).

סוף מסמך. זהו הקאנון המאוחד — ניסוח אחד, רציף וברור, שמרכז את כל המקורות לתכנית עבודה אחת. השלב הבא יהיה לגזור ממנו דיאגרמות (ארכיטקטורה/זרימות/CI-CD), טבלאות ENV/Routes, וצעדי מימוש ממוקדים.