- PROBLEM STATEMENT ID : PS02
- TEAM NAME : HYDRA
- TEAM ID : HK-080
- TEAM MEMBERS : DISHA
  SARTHAK SINGH
  MANISH TIWARI
  AKSHITH

PROBLEM & SOLUTION

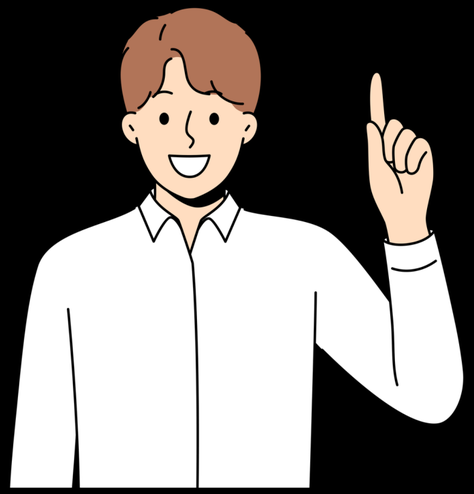
THE PROBLEM:

MANUAL OVERLOAD: SECURITY ANALYSTS CANNOT MANUALLY MONITOR THOUSANDS OF DARK WEB FORUMS, TELEGRAM CHANNELS, AND PASTE SITES FOR THREATS AGAINST INDIAN INFRASTRUCTURE

NOISE & FALSE POSITIVES: TRADITIONAL TOOLS STRUGGLE TO DISTINGUISH BETWEEN A "SCRIPT KIDDIE" BRAGGING AND A GENUINE COORDINATED ATTACK, LEADING TO ALERT FATIGUE

LINGUISTIC BARRIERS: EXISTING SYSTEMS OFTEN FAIL TO DETECT THREATS DISCUSSED IN REGIONAL INDIAN LANGUAGES (HINDI, TAMIL) OR CODE-MIXED "HINGLISH"

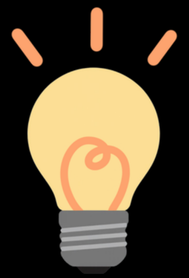
THE SOLUTION:



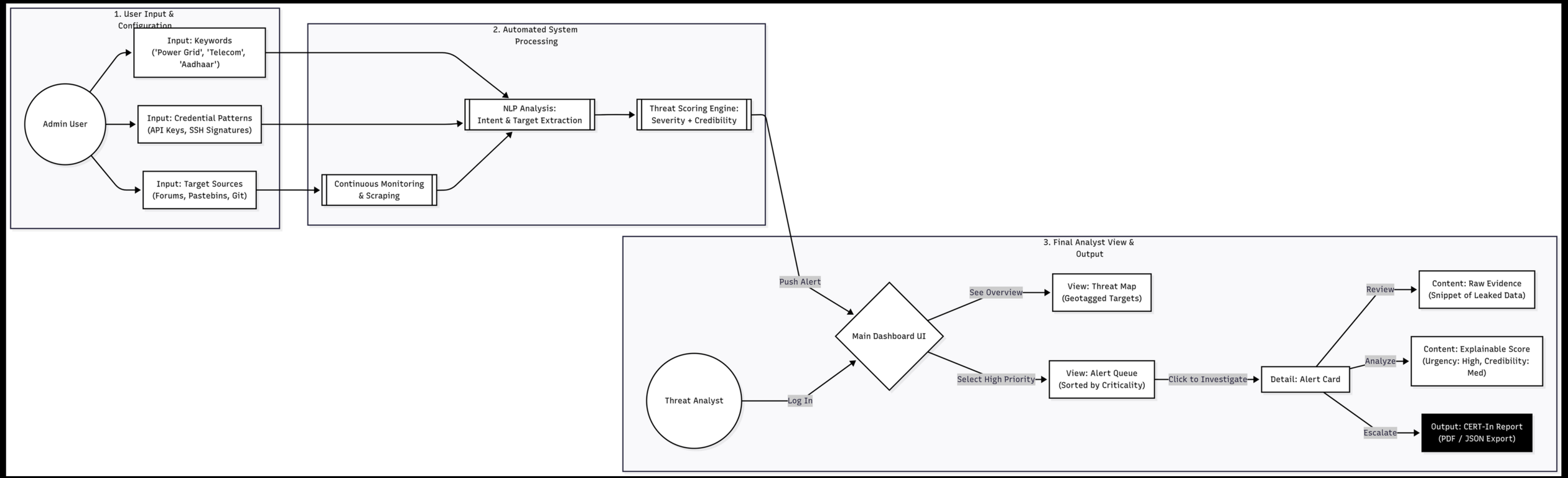
"TRINETRA " DASHBOARD: AN AUTOMATED "SINGLE PANE OF GLASS" THAT CONTINUOUSLY SCRAPES, PROCESSES, AND VISUALIZES THREATS IN REAL-TIME.

AI-POWERED CONTEXT: USES GOOGLE GEMINI 2.5 PRO TO ANALYZE THE INTENT OF DISCUSSIONS (E.G., PLANNING VS. SPAM) AND EXTRACT SPECIFIC TARGETS (E.G., "STATE POWER GRID")

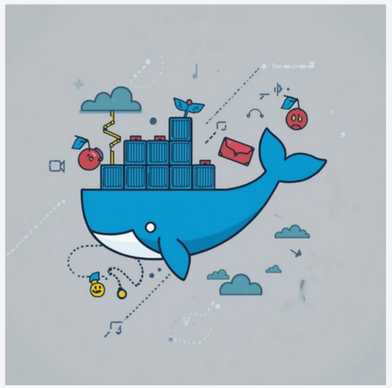
ACTIONABLE INTELLIGENCE: DELIVERS A COMPOSITE THREAT SCORE (SEVERITY, CREDIBILITY, URGENCY) AND RENDERS THREATS ON A 3D GEOSPATIAL MAP FOR IMMEDIATE SOC RESPONSE



FLOW OF SOLUTION



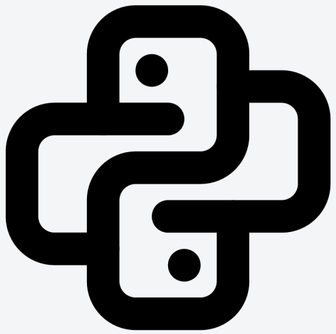
TECH STACK & APPROACH



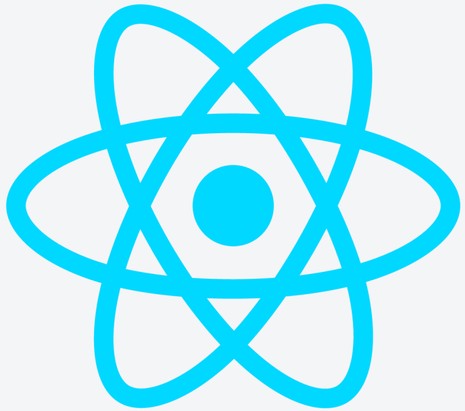
DOCKER

FIREBASE

JAVA-SCRIPT



PYTHON 3.X



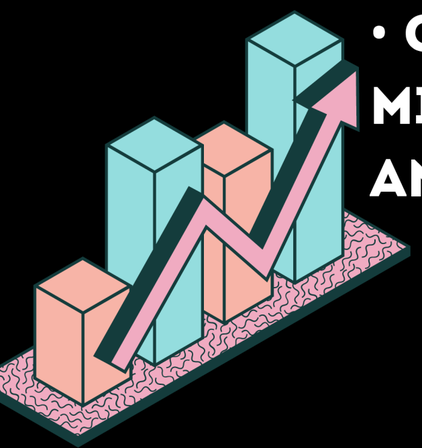
REACT

FEASIBILITY & CHALLENGES

- FEASIBILITY: BUILT ON A PHASED DEPLOYMENT ROADMAP, MOVING FROM A PROOF-OF-CONCEPT (3 SOURCES) TO A FULL-SCALE SOC-INTEGRATED ENGINE OVER 9-12 MONTHS.

- CHALLENGE - DATA NOISE: MANAGING HIGH-VOLUME STREAMS AND FALSE POSITIVES IS MITIGATED THROUGH HUMAN-IN-THE-LOOP VERIFICATION AND CONSERVATIVE SCORING THRESHOLDS.

- CHALLENGE - EVASION: SCRAPERS FACE BLOCKS/BANS; MITIGATED BY ADAPTIVE BACKOFF, PROXY ROTATION, AND PRIORITIZING OFFICIAL APIS WHERE POSSIBLE



RESEARCH & REFERENCE

1. SECURITY FRAMEWORKS & STANDARDS
• MITRE ATT&CK: WE MAP AI-DETECTED THREATS TO STANDARDIZED TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) TO ENSURE INDUSTRY-STANDARD CLASSIFICATION.
• CERT-IN COMPLIANCE: REPORTS ARE STRUCTURED TO MATCH INDIAN COMPUTER EMERGENCY RESPONSE TEAM FORMATS FOR IMMEDIATE OFFICIAL HANDOFF.
• OWASP GUIDELINES: ADHERENCE TO OWASP AUTOMATED THREAT STANDARDS TO ENSURE OUR SCRAPERS OPERATE ETHICALLY WITHOUT CAUSING DENIAL OF SERVICE (DOS).
2. TECHNICAL CITATIONS
• GOOGLE GEMINI 2.5 FLASH: SELECTED SPECIFICALLY FOR ITS HIGH-THROUGHPUT AND LOW-LATENCY CAPABILITIES, ALLOWING COST-EFFECTIVE "ON-DEMAND" ANALYSIS.
• FASTAPI & WEBSOCKETS: CHOSEN OVER FLASK/DJANGO FOR NATIVE ASYNCHRONOUS SUPPORT, ENABLING ZERO-LATENCY BROADCASTING OF THREATS TO THE DASHBOARD.
• REACT THREE FIBER: RESEARCH-BACKED CHOICE FOR HIGH-PERFORMANCE, GPU-ACCELERATED 3D VISUALIZATION OF GEOSPATIAL DATA IN THE BROWSER.
3. LEGAL & ETHICAL COMPLIANCE
• IT ACT 2000 (INDIA): STRICT COMPLIANCE WITH SECTION 43 & 66, ENSURING WE MONITOR ONLY PUBLIC OSINT SOURCES AND STRICTLY AVOID UNAUTHORIZED ACCESS ("HACKING BACK").
• ROBOTS.TXT PROTOCOL: ALL SCRAPERS ARE PROGRAMMED TO RESPECT THE USER-AGENT DIRECTIVES OF SOURCE WEBSITES TO MAINTAIN LEGAL STANDING.
• DATA PRIVACY: IMPLEMENTATION OF PII REDACTION (HASHING EMAILS/PHONES) BEFORE STORAGE TO PROTECT PRIVACY.
4. KEY LIBRARIES & APIS
• PRAW (REDDIT API): USES THE OFFICIAL PYTHON REDDIT API WRAPPER TO SCRAPE R/NETSEC LAWFULLY WITHOUT VIOLATING TERMS OF SERVICE.
• APSCHEDULER: UTILIZED FOR PRECISE CRON-STYLE BACKGROUND TASKS TO TRIGGER SCRAPING JOBS EXACTLY EVERY 60 SECONDS.
• FIREBASE FIRESTORE: CHOSEN FOR ITS NOSQL FLEXIBILITY TO STORE UNSTRUCTURED FORUM DATA AND RAPID REAL-TIME SYNCING.