

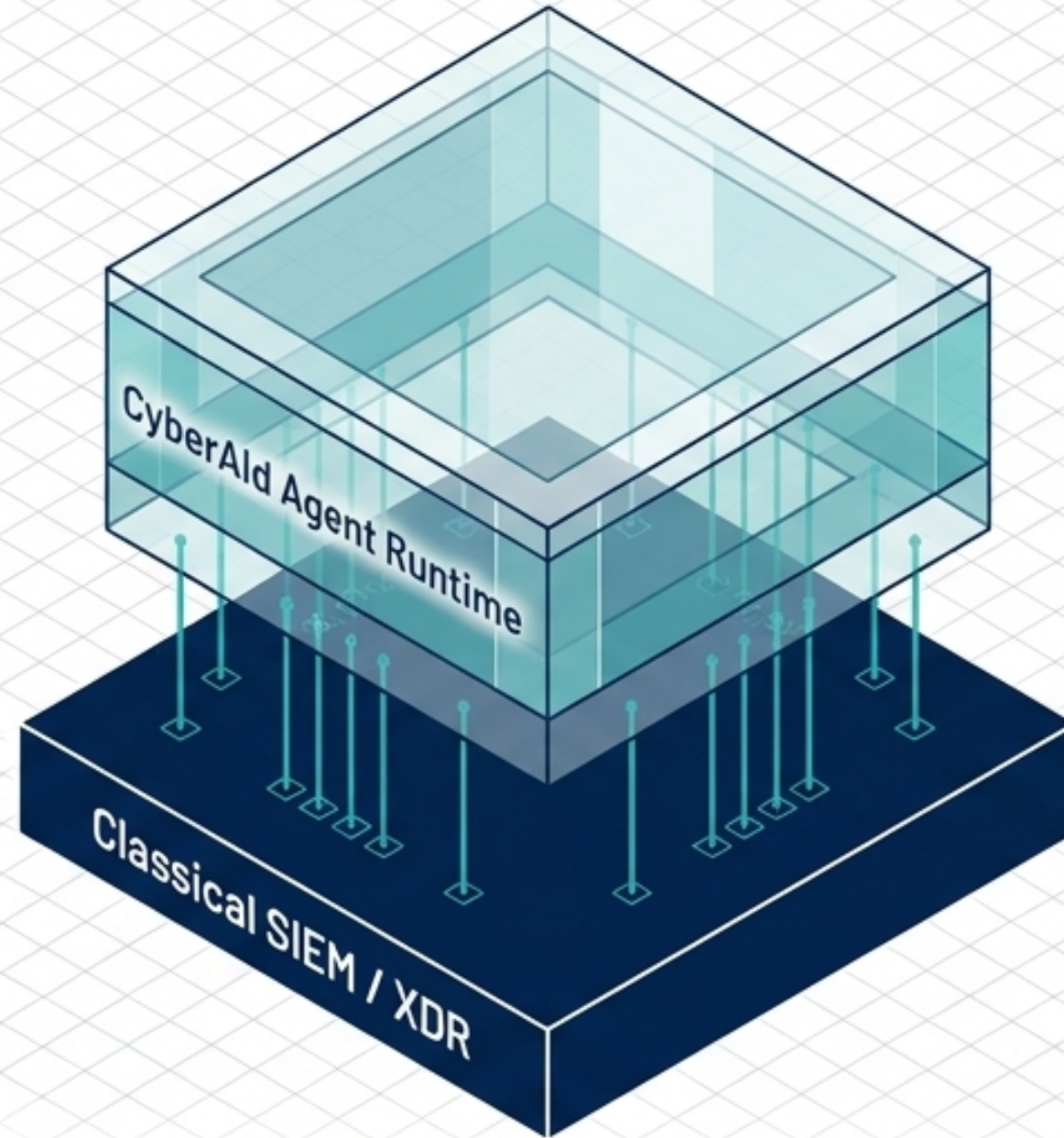


AI-Driven Cybersecurity for
Financial Service Providers

Learning Center

Tutorial 3 | CyberAid: The Architecture of AI-driven
Financial Cybersecurity

A Hybrid Multi-Agent System for Regulated Operations (DORA,
NIS2, EU, AI, Act)



CyberAid: The Architecture of AI-Driven Financial Cybersecurity

A Hybrid Multi-Agent System for Regulated Operations (DORA, NIS2, EU AI Act)

DATA INGESTION

CONTEXT: EUROPEAN
FINANCE: €100T ASSETS,
400k+ TRANSACTIONS/DAY.

THE SURGE: +238%
CYBERATTACK GROWTH
SINCE 2020.

ANALYST REASONING BOTTLENECK

UNINVESTIGATED BREACHES

THE FAILURE: UNINVESTIGATED
BREACHES (BREACHES PRECEDED
BY ALERTS GENERATED BUT
NEVER INVESTIGATED).

~21%



MITRE ATT&CK TECHNIQUES ACTUALLY
DETECTED BY ENTERPRISE SIEMs
DESPITE MASSIVE DATA INGESTION.

2/3



SOC TEAMS FAILING TO KEEP PACE
WITH INCOMING ALERT VOLUMES.



THE REALITY



THE CONSTRAINT IS ANALYTIC
REASONING, NOT SENSOR DATA
OR STAFFING.

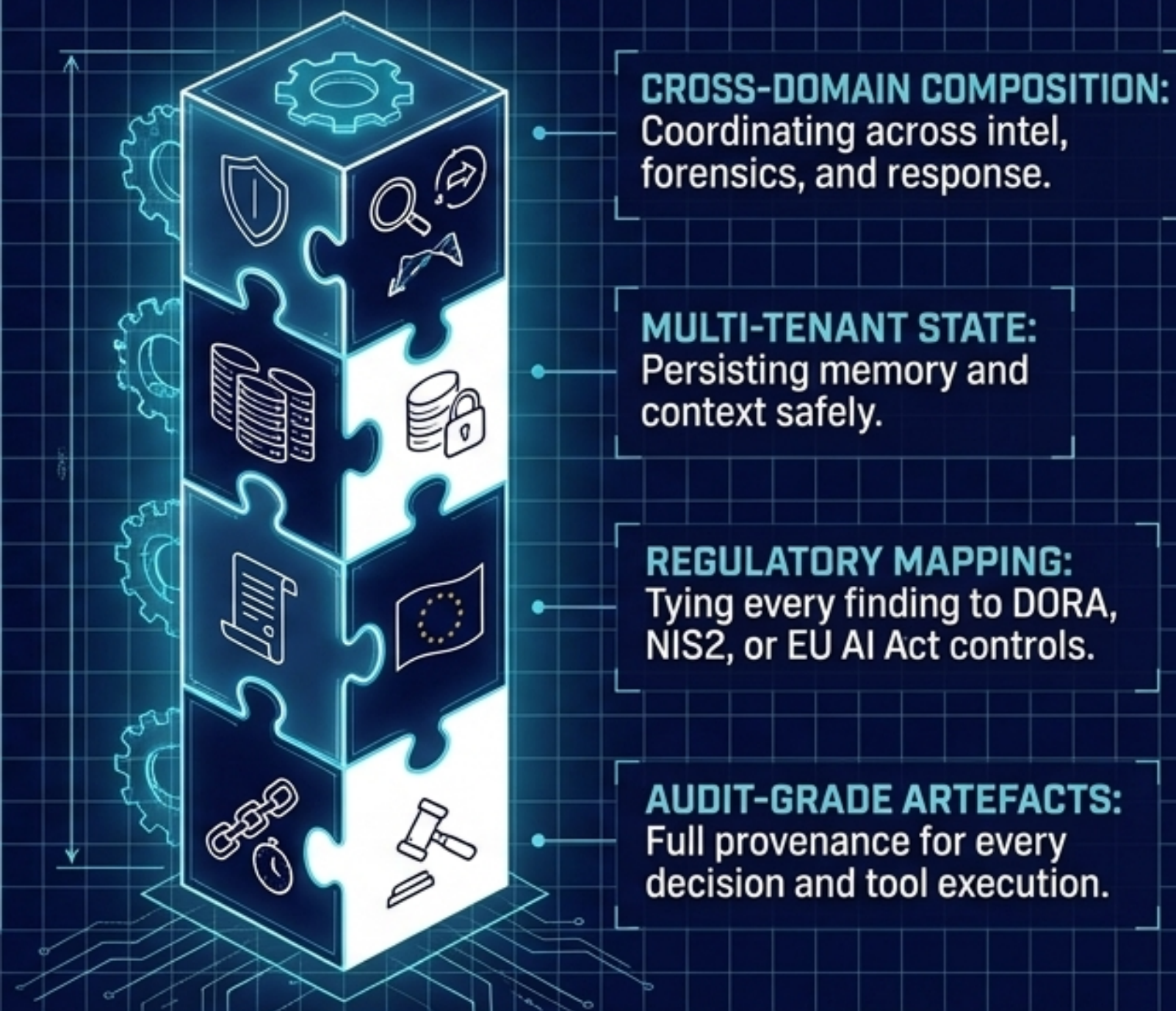


THE ARCHITECTURAL CONTRAST: ISOLATED TOOLS vs. INTEGRATED PLATFORM

THE NARROW LLM WIN (ISOLATED)

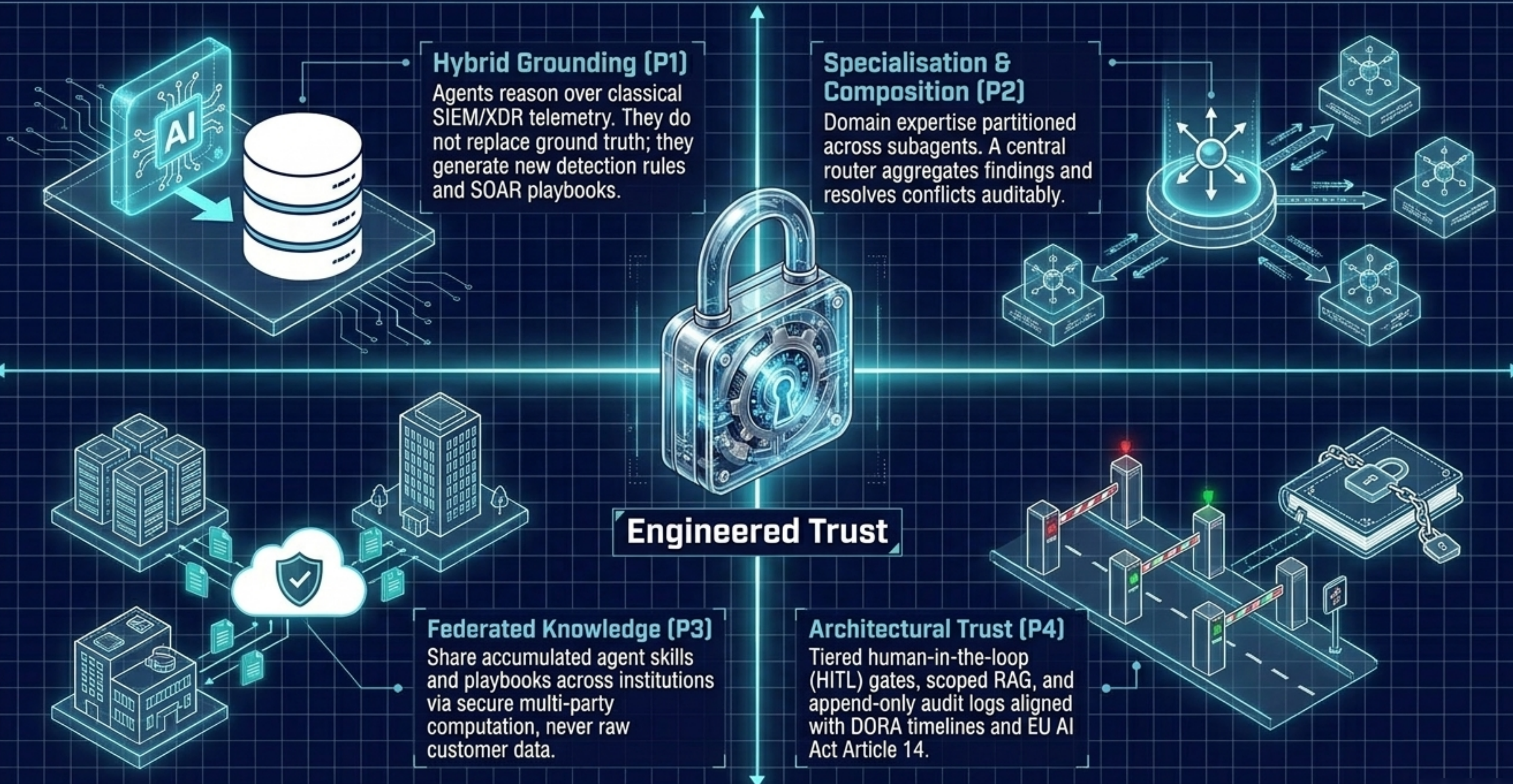


THE PLATFORM REALITY (INTERLOCKED)

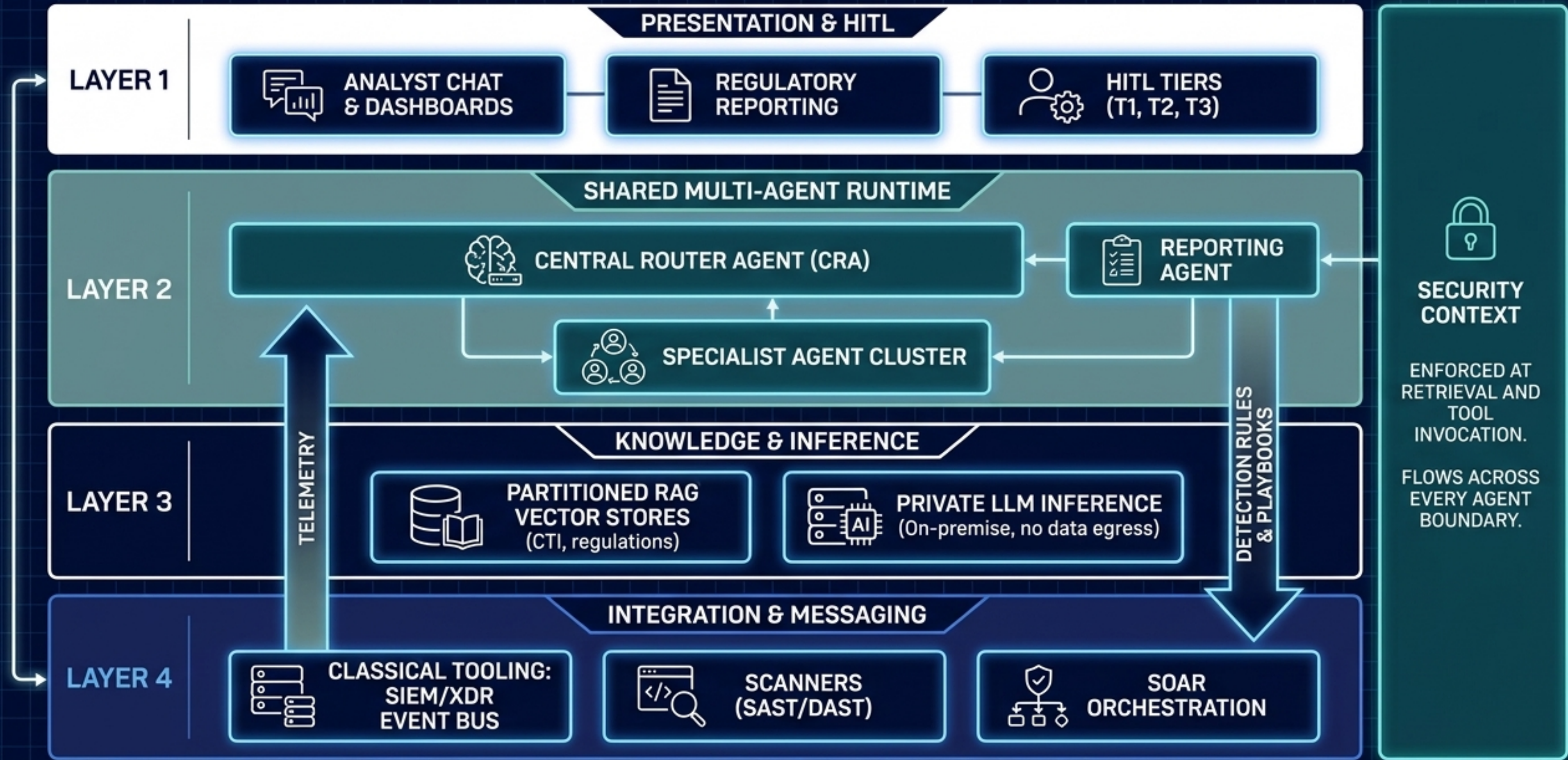


A MONOLITHIC LLM IS A TOOL. A SOC REQUIRES A PLATFORM.

THE FOUR PILLARS OF ENGINEERED TRUST: A CONCEPTUAL FRAMEWORK



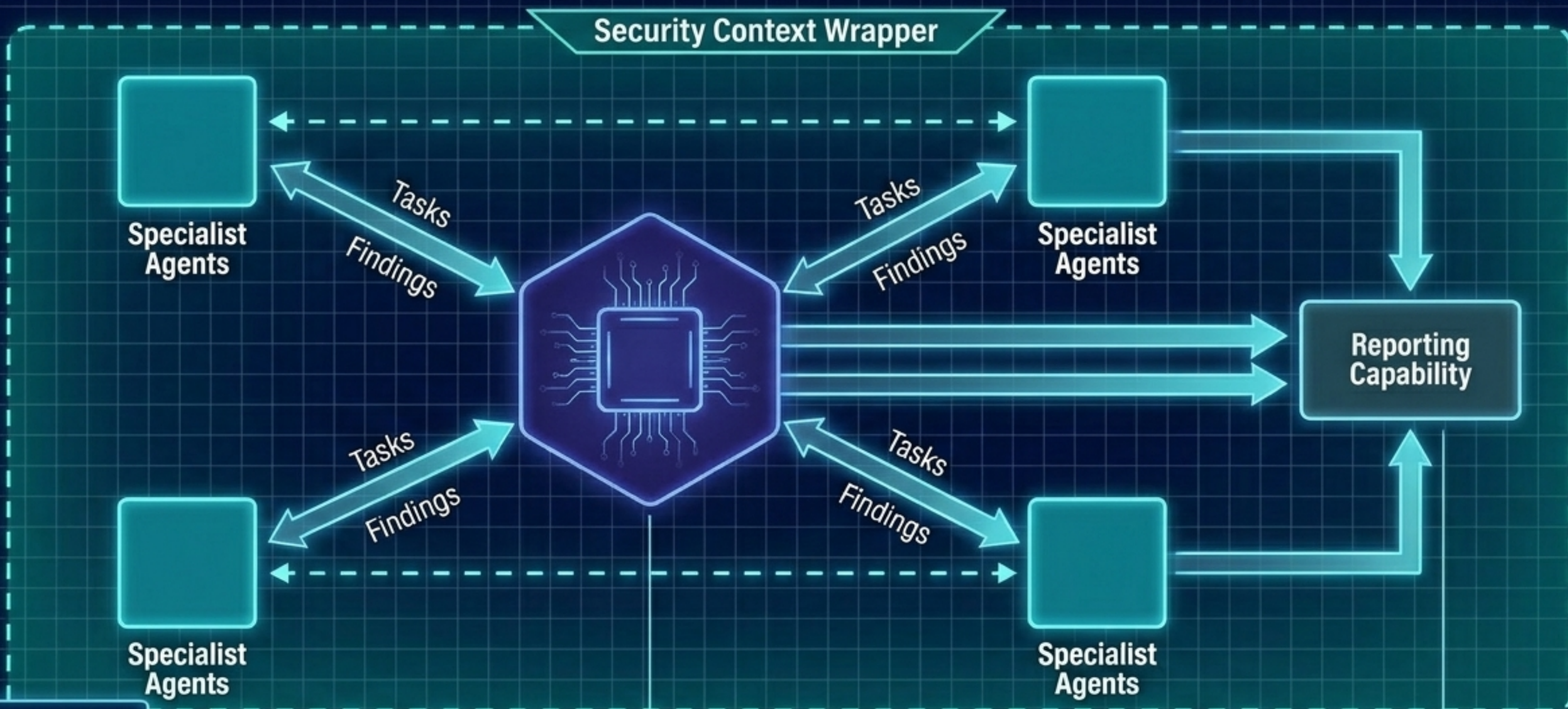
THE SOC ARCHITECTURE: A RIGID 4-LAYER TECHNICAL STACK



THE RUNTIME LAYER: CENTRAL ROUTER & SPECIALIST AGENTS TOPOLOGY

18:9 ASPECT RATIO

TECHNICAL SCHEMATIC V1.2



```
{
  "finding_id": "...",
  "source_agent": "...",
  "severity_score": 8.5,
  "evidence": [ ... ],
  "confidence": 0.92,
  "schema_version": "v2.1"
}
```

The Standard Finding Schema
Forces all specialists to return evidence in a unified, deterministic format for the CRA to synthesize.

Central Router Agent (CRA)
Function: Analyst-facing triage and dispatch layer.
Mechanics: Performs initial severity scoring, activates specialists in parallel, resolves analytical conflicts via calibrated confidence scores.

The Reporting Capability (Low-Latency Bypass)
Function: Direct query path to specialists, bypassing CRA contention.
Mechanics: Ensures regulatory templates (DORA 4-hr, NIS2 24-hr) are drafted concurrently with active incident response.

TECHNICAL SCHEMATIC V1.2

THE AGENTIC SOC PERIODIC TABLE: MODULAR CAPABILITIES MATRIX

18:9 ASPECT RATIO

TECHNICAL SCHEMATIC V1.2

Deep Navy

CRA

**CENTRAL ROUTER
AGENT**

Triage, parallel dispatch,
conflict resolution,
HITL escalation.

Muted Teal

TIA

**THREAT INTEL
AGENT**

Maps IoCs to MITRE ATT&CK,
correlates campaigns across
external CTI feeds.

Cyan

VAA

**VULNERABILITY
ASSESSMENT**

Scores exploitability against
actual exposure; merges
SAST/DAST with LLM static
analysis.

Cyan

CVA

**COMPLIANCE
VERIFICATION**

Maps findings directly to
DORA, NIS2, GDPR, PSD2,
and AI Act controls.

Muted Teal

BAA

**BEHAVIOURAL
ANALYSIS**

UEBA over kernel telemetry
and transactions; surfaces
subtle insider threats.

Deep Navy

IRA

**INCIDENT
RESPONSE**

Generates containment
playbooks, coordinates
isolation, manages recovery.

Deep Navy

FAA

**FORENSIC
ANALYSIS**

Reconstructs timelines,
preserves evidence chains to
legally admissible standards.

Cyan

DCA

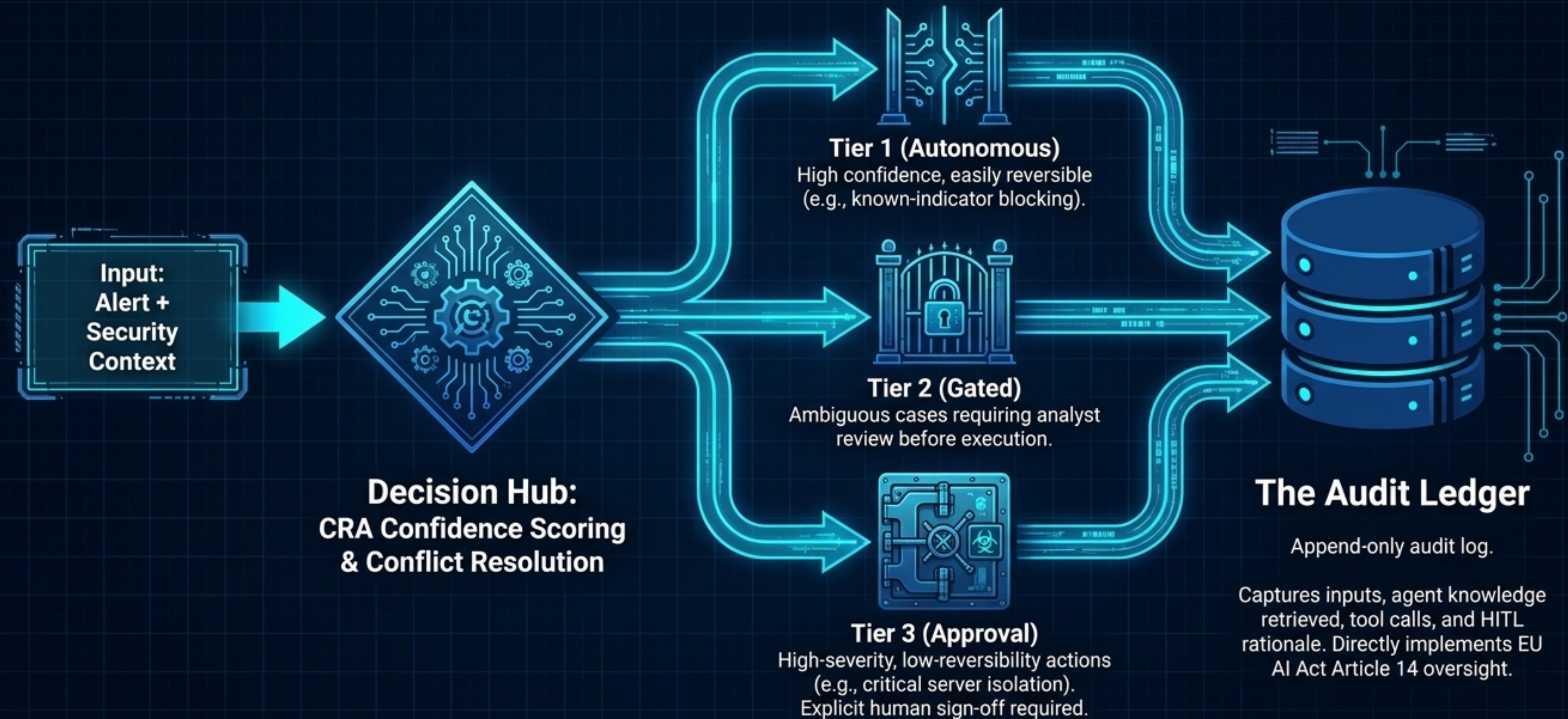
**DEVSECOPS
& CODE**

CI/CD static/dynamic
analysis; enforces SDLC and
PCI-DSS compliance.

18:9 ASPECT RATIO

TECHNICAL SCHEMATIC V1.2

THE AGENTIC SOC DECISION FLOW: CRA CONFIDENCE & HITL TIERS



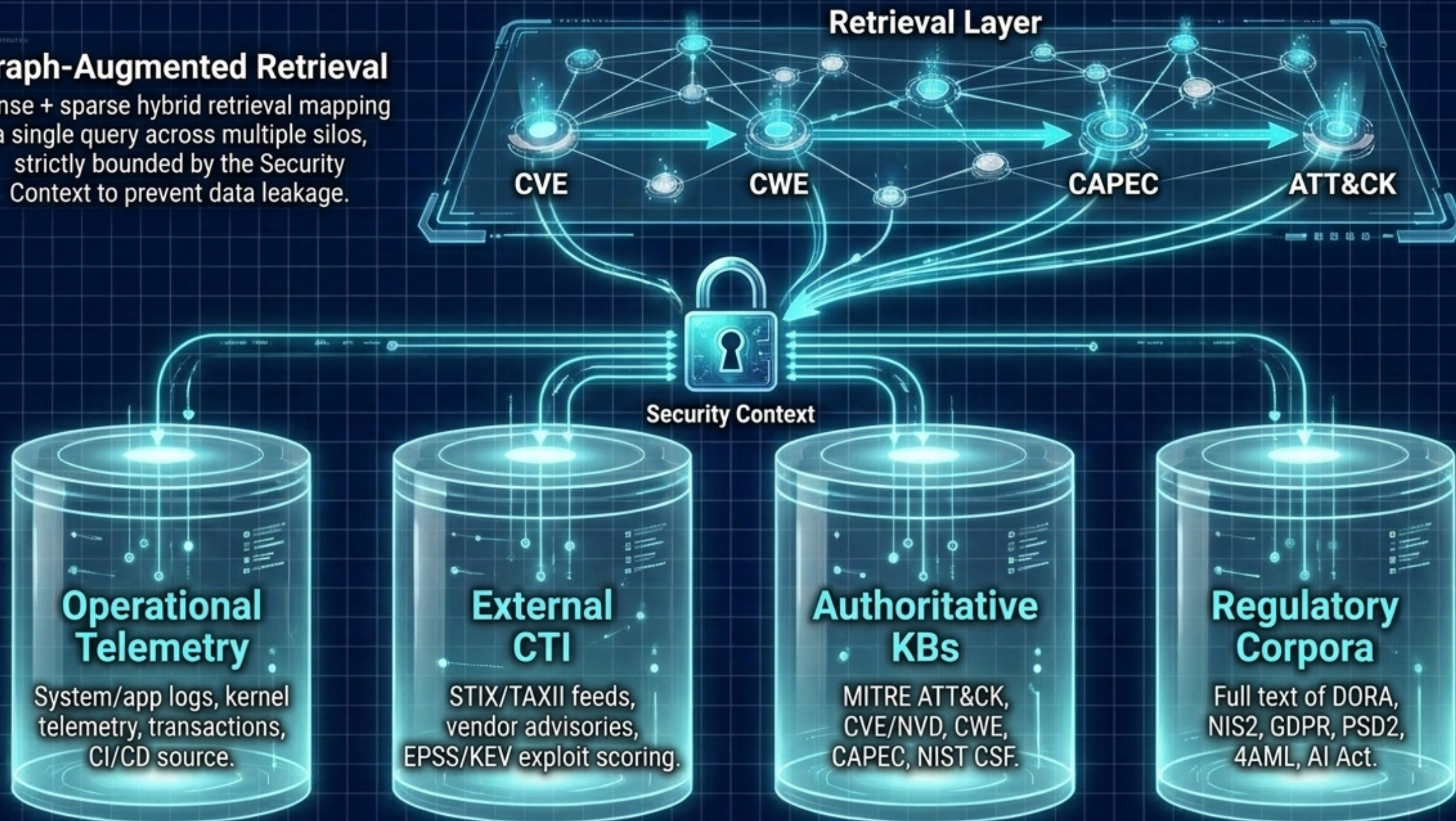
GRAPH-AUGMENTED DATA RETRIEVAL: UNIFIED ACCESS ACROSS SILOS

18:9 ASPECT RATIO

TECHNICAL SCHEMATIC V1.2

Graph-Augmented Retrieval

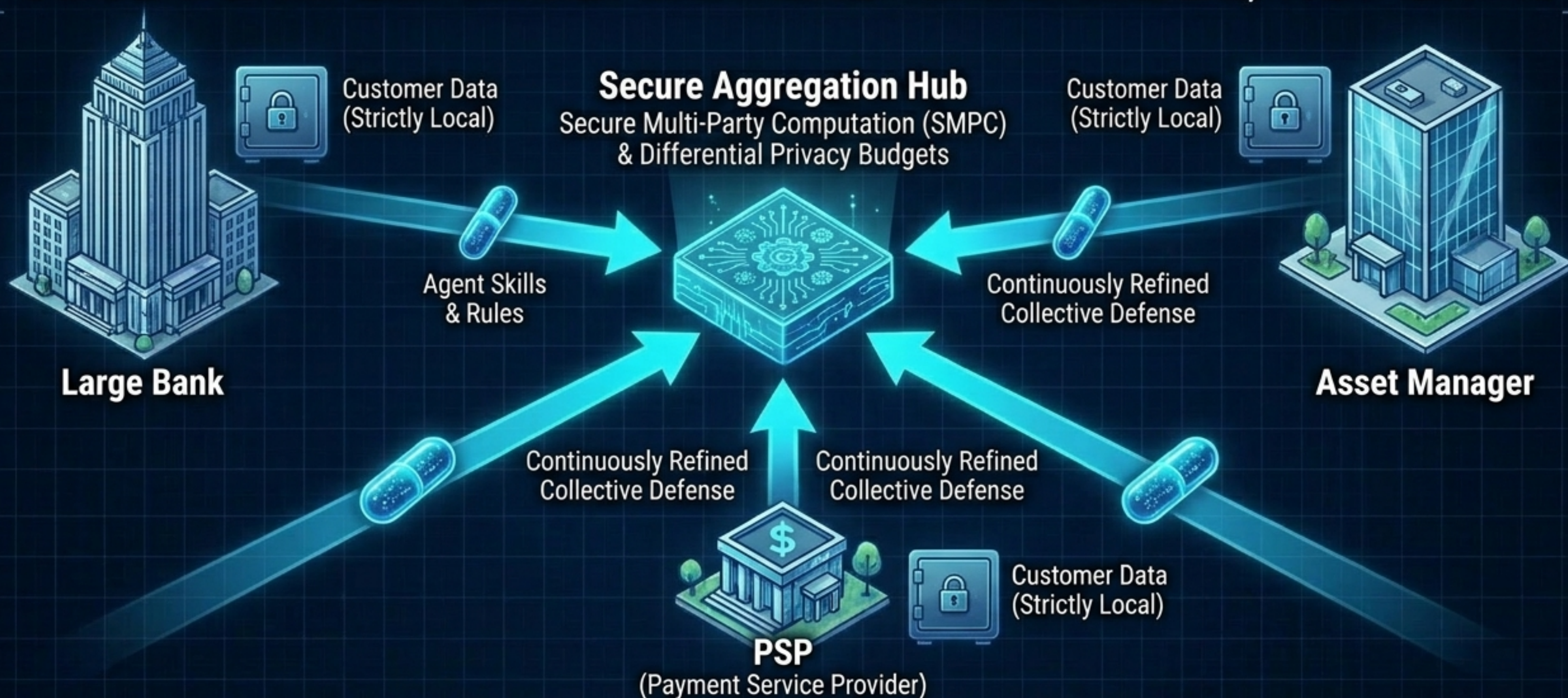
Dense + sparse hybrid retrieval mapping a single query across multiple silos, strictly bounded by the Security Context to prevent data leakage.



18:9 ASPECT RATIO

TECHNICAL SCHEMATIC V1.2

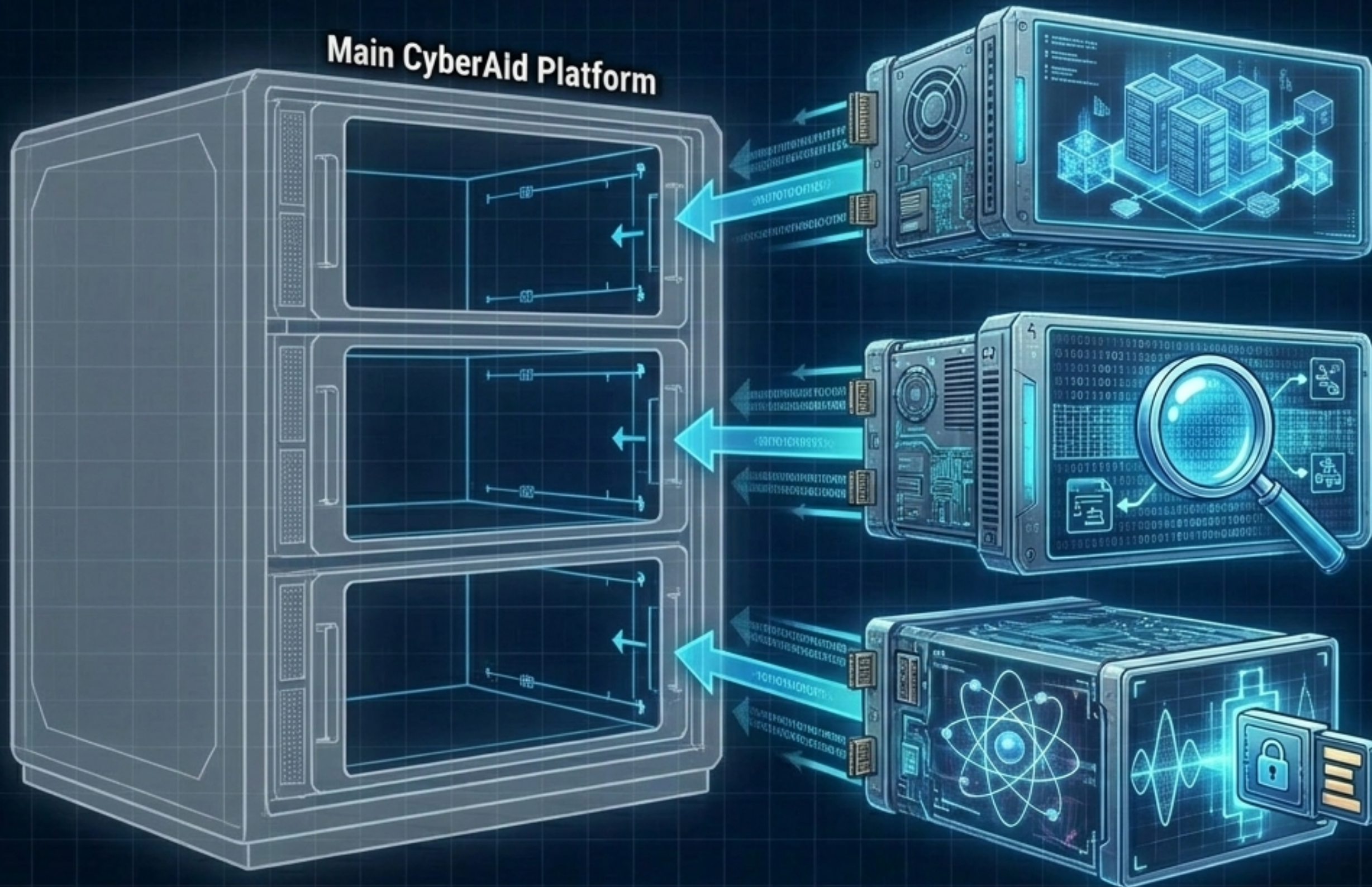
FEDERATED DEFENSE: SHARING KNOWLEDGE, NOT DATA



Federated Defense: Sharing Knowledge, Not Data

Institutions share accumulated agent knowledge (detection rules, behavioural baselines, response playbooks)—never raw data. Smaller institutions instantly inherit big-bank detection capabilities.

MODULAR CYBER DEFENSE: FLEXIBLE EXPANSION CARTRIDGES



Digital Twins

(Adversarial Validation)

LLM red-team agents safely attack an infrastructure replica. Successful exploit paths automatically generate new VAA priorities and SIEM detection rules.

eBPF Instrumentation

(Kernel Telemetry)

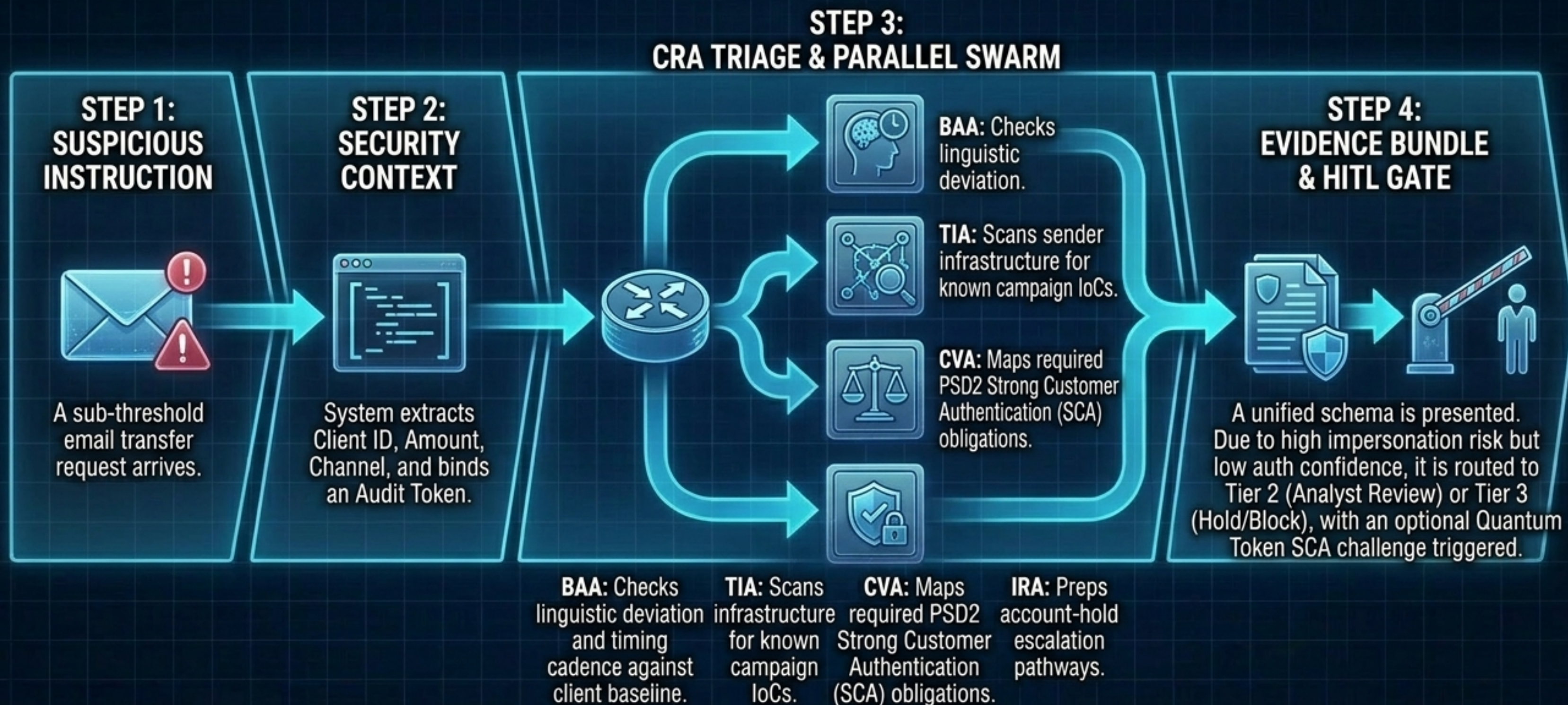
Low-overhead syscall and network visibility on edge devices (ATMs, POS, gateways), feeding the BAA with sub-second behavioral telemetry.

Quantum Tokens

(Unforgeable 2FA)

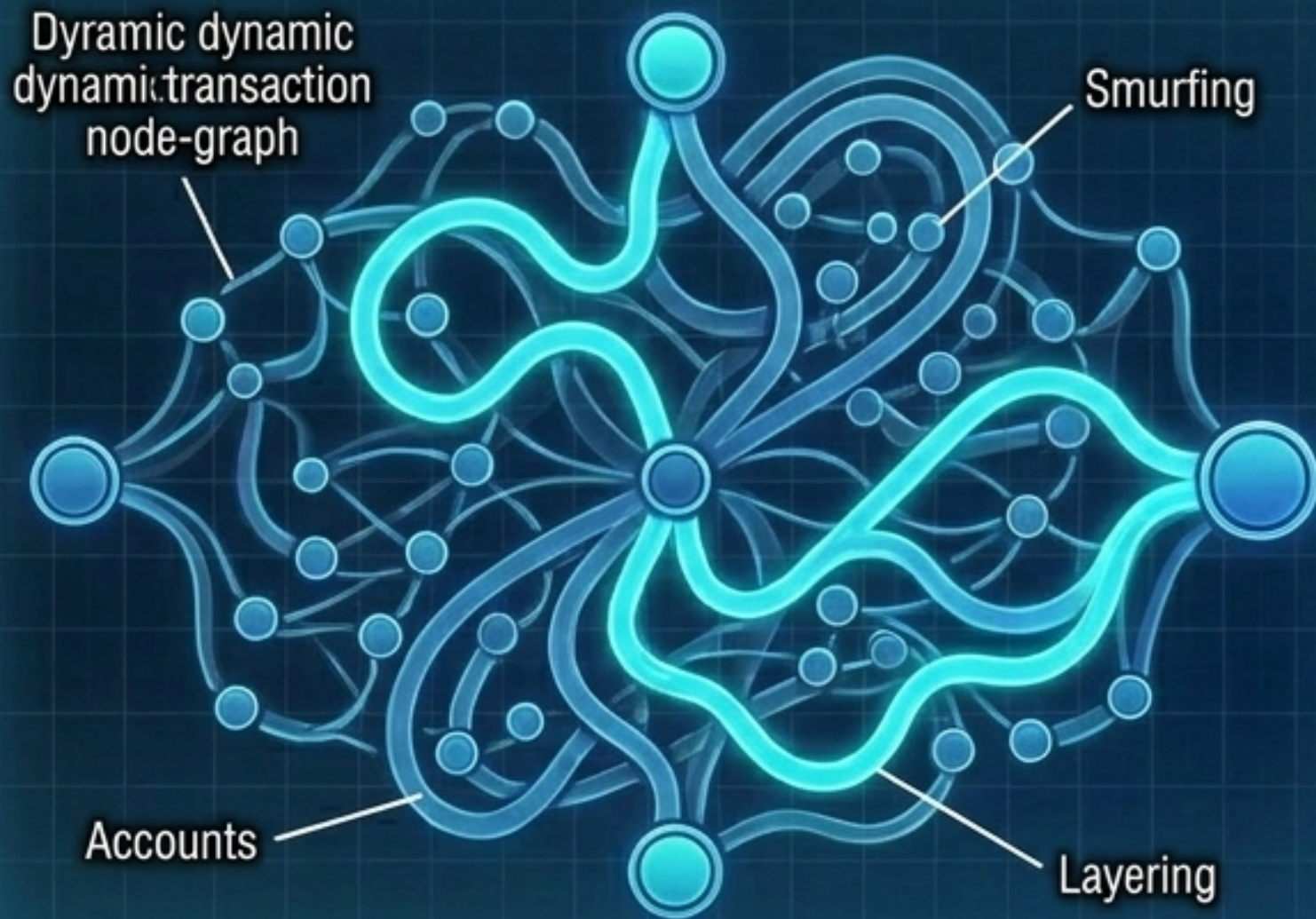
Exploiting the no-cloning theorem for physically unforgeable, single-use authentication on high-value bank-to-bank and custodian transactions.

ARCHITECTURE IN ACTION: CLIENT IMPERSONATION (PRIVATE BANKING)



ANALYTICAL CONCEPTS: NETWORK VS. VELOCITY

Use Case 2 - PSP Anti-Money Laundering



Bypassing the 95% false-positive rate of legacy rule-based AML.

BAA and TIA build dynamic transaction graphs across e-wallet and IBAN ecosystems to surface shell-account patterns hidden across institutions.

Use Case 3 - Retail Banking Scale



10k+ servers, **Petabytes** of logs. eBPF kernel telemetry feeds pipelined CRA triage at sub-second latency. Confirmed incidents trigger autonomous Tier-1 IRA containment while the Reporting Agent drafts mandatory DORA notifications within the strict 4-hour window.

THE HORIZON: SKILL-BASED AGENT ADAPTATION



**MONOLITHIC
SYSTEM PROMPT**

aml-eu-emoney

kyc-global

**AGENT
CORE**

fraud-detection-v3

pci-dss-v4

fraud-detection-v3

Moving away from monolithic system prompts to composable, versioned, cryptographically signed Skill Packages.

⚠️ CONFLICT RESOLUTION ⚠️

How to auditably resolve disputes when an AML skill flags what a PCI-DSS compliance skill suppresses.

⚠️ SKILL POISONING ⚠️

Expanding RAG defenses to protect against malicious external skill authors.

⚠️ FEDERATED CONSISTENCY ⚠️

Balancing differential-privacy budgets when multiple institutions update shared skills simultaneously.



Securing financial critical infrastructure does not require a smarter monolithic LLM.
It does not require a completely new SIEM.
It requires a hybrid, multi-agent runtime.



Thank you!

Connect With CyberAid:

Linkedin: CyberAid



The project funded under Grant Agreement No 101249596 is supported by the European Cybersecurity Competence Centre