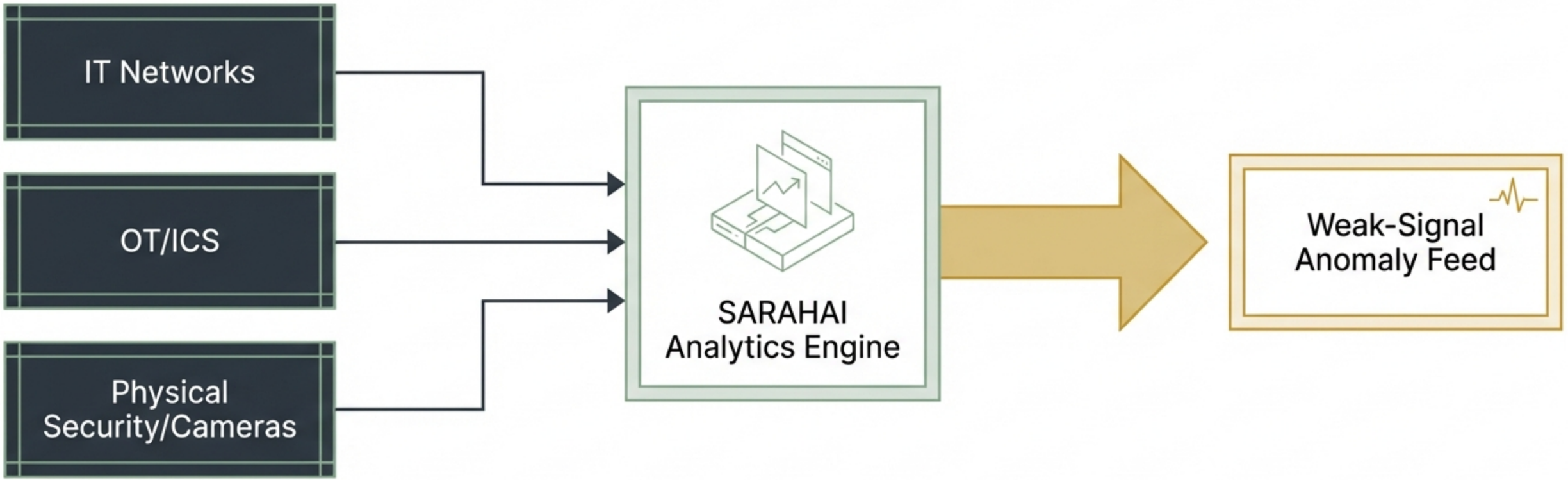
TENSOR NETWORKS

SARAHAI™: Predictive Pattern-of-Life Analytics for Critical Infrastructure

A Strategic Evaluation Brief for Federal, SLED, and Utility Operations

The Core Thesis: Mixed-Data Convergence



The Converged Risk

Adversaries exploit seams between physical, facility, and cyber systems across 16 CISA sectors.

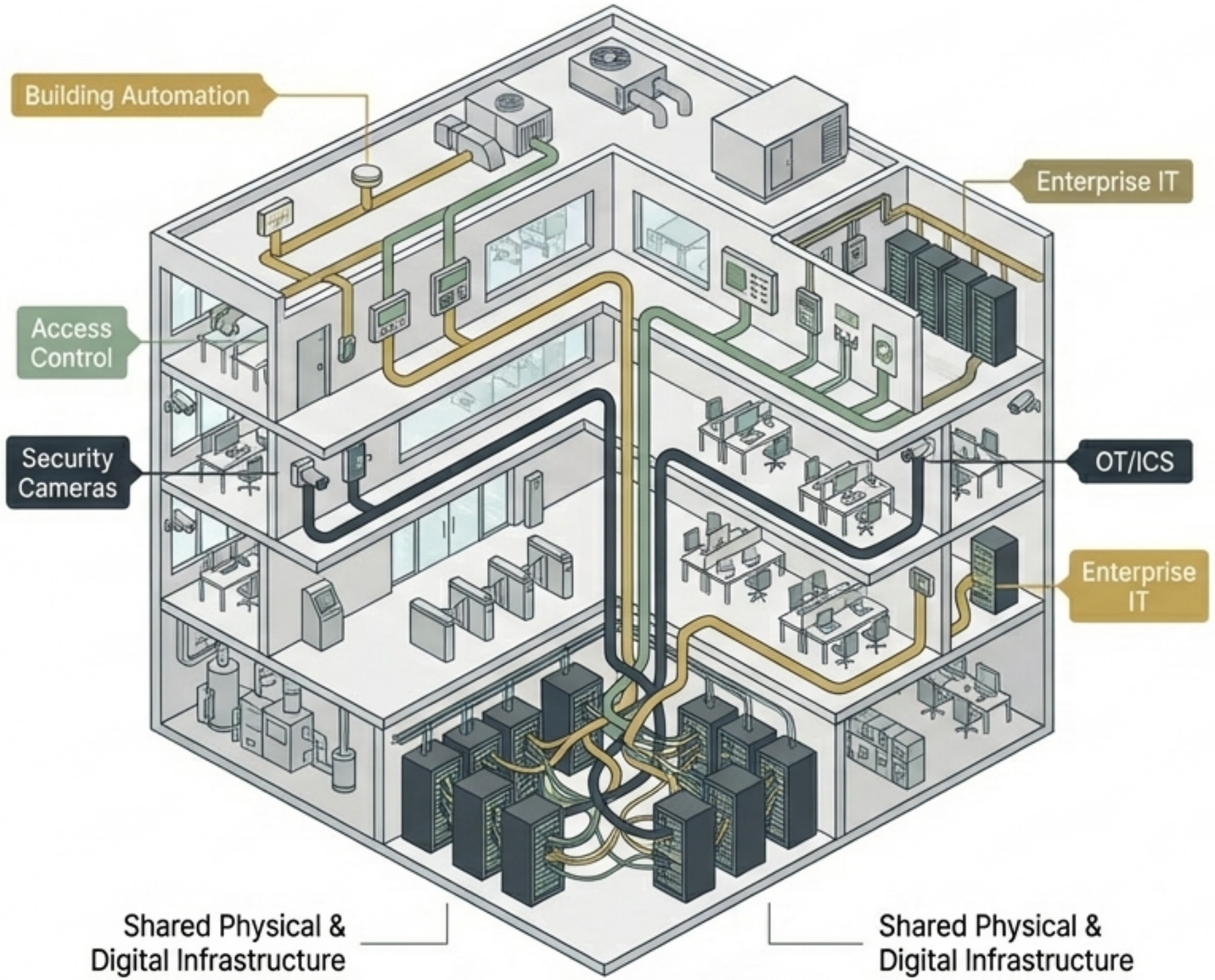
The Capability

A predictive Pattern-of-Life (PoL) layer that learns local normalcy and prioritizes weak-signal anomalies.

The Strategy

An overlay that compresses heterogeneous data into actionable events without replacing incumbent SIEM or OT tools.

The Reality of Cyber-Physical Convergence



Expanded Definition

NIST SP 800-82 explicitly treats physical access-control and building automation as Operational Technology (OT).

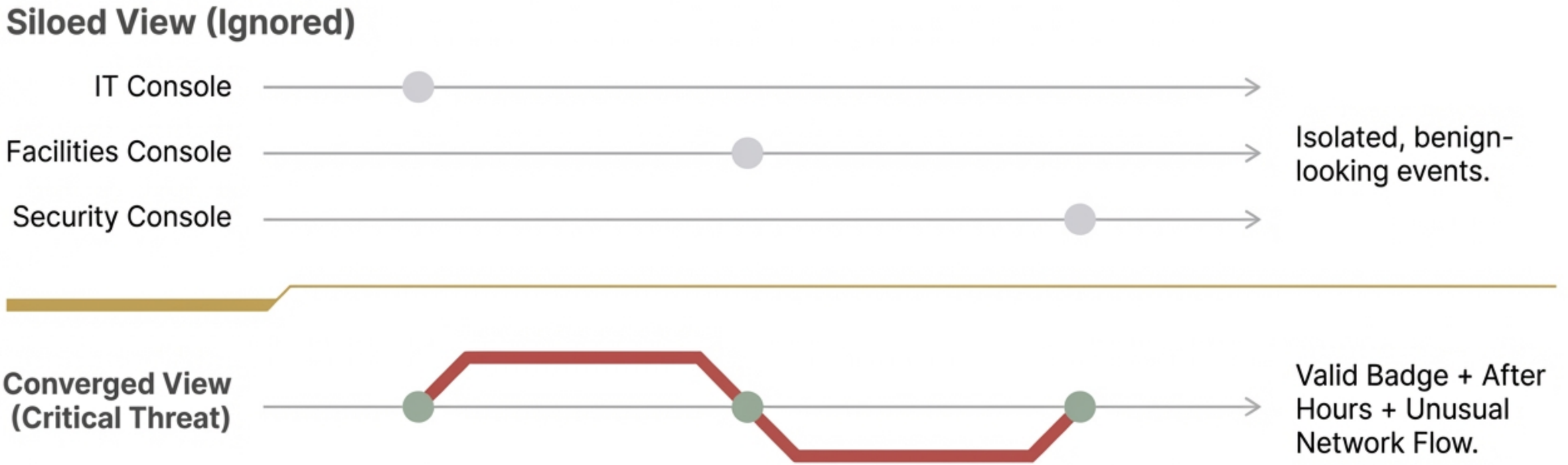
Federal Reality

GAO-15-6 findings confirm building and access-control systems are increasingly Internet-connected, heightening mission vulnerability.

National Policy

NSM-22 and DHS 2024 guidance demand cross-sector resilience, not just isolated, one-off protection efforts.

The Threat in the Seams

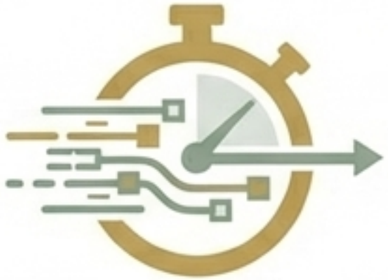


The Context: Long-dwell, low-noise access campaigns (e.g., Volt Typhoon) evade static signatures.

The Failure: Conventional monitoring misses slow, contextual deviations across domains.

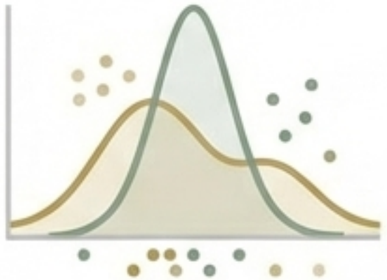
The Core Problem: Protecting modern infrastructure requires identifying normal-looking events occurring in abnormal combinations.

Demystifying SARAHAI™



Real-Time Detection

Continuous monitoring that reduces latency between event emergence and operator awareness.

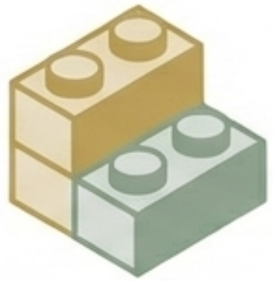


Pattern-of-Life Baselining

Uses kernel density estimation to model local statistical normalcy across the environment.

Mixed-Data Handling

Processes categorical (user role, asset type) and non-categorical (temperature, frequency) data directly.



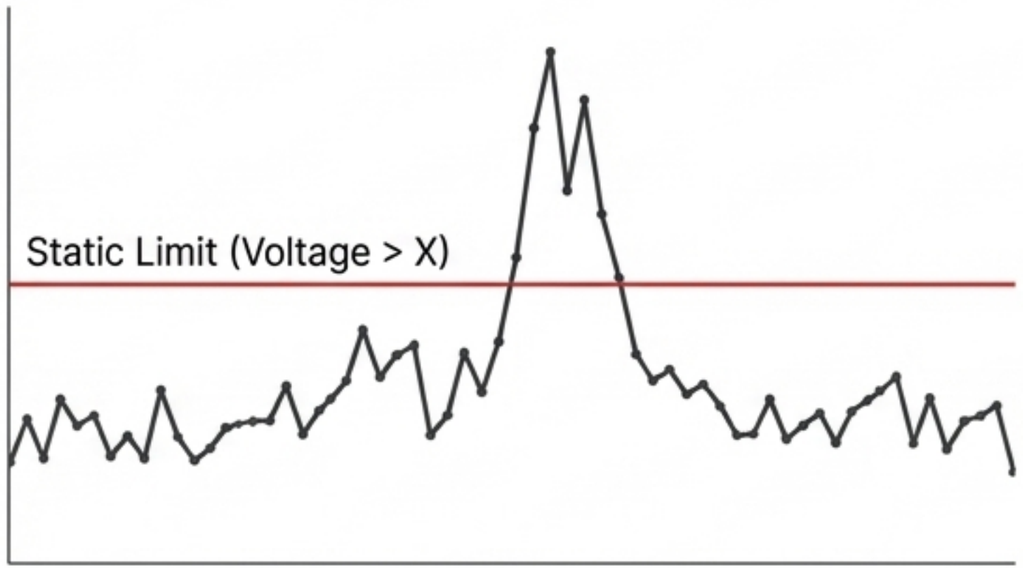
Low-Code Usability

Enables non-experts to build streaming analytics, reducing dependence on specialized data-science talent.

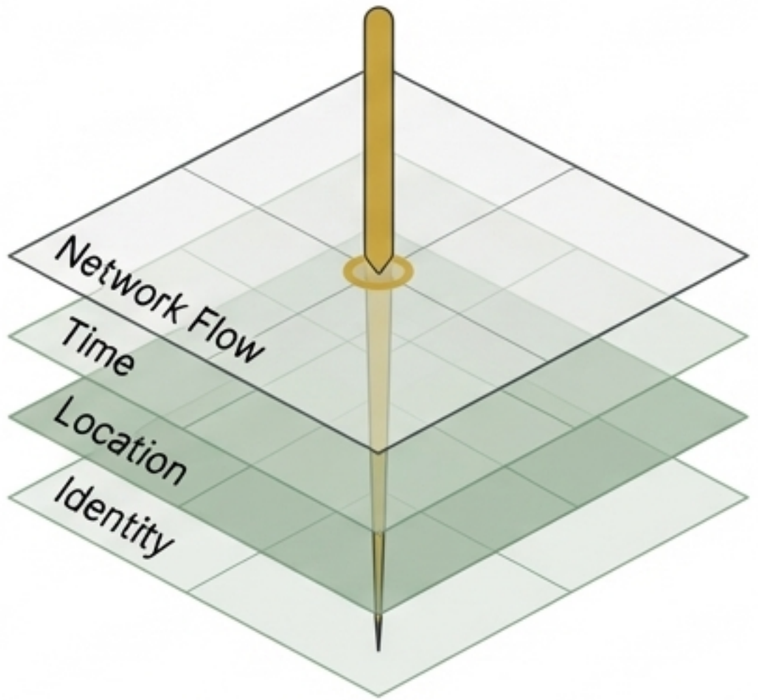
Static Thresholds vs. Pattern-of-Life (PoL)

Many of the most damaging critical infrastructure incidents are not initial threshold violations. They are subtle **pattern deviations**. SARAHAI shifts defense from fixed rules to local operational context.

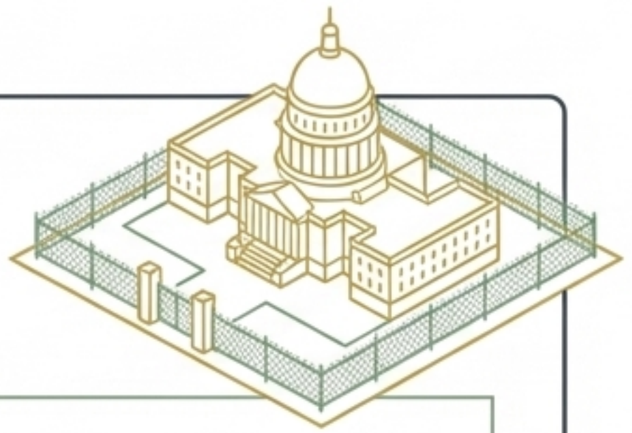
Did something happen?



Given this asset, place, time, role, and history... should a human care?



Operating Profile: Federal Facilities



Inter

Primary Focus: Mission Continuity

The Problem	Managing converged building, access, cyber, and mission-continuity risk under ISC mandates.
The Value Driver	Local normalcy models reduce cross-console triage. SARAHAI elevates meaningful cyber-physical anomalies to protect network-connected facility control systems.
Acquisition Path	Available via SEWP V, ITES-SW2, NASPO, and OMNIA.

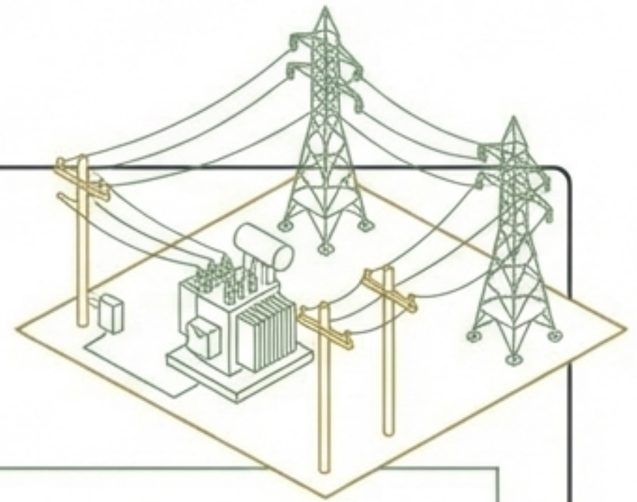
Operating Profile: State, Local, & Education (SLED)

Inter

Primary Focus: Force Multiplication

The Problem	Fragmented civic infrastructure (K-12 campuses to municipal operations centers), lean staffing, and asymmetric risk. GAO notes K-12 incidents cause up to 9 months of recovery time.
The Value Driver	Low-code/no-code usability compresses complexity. Lean teams can monitor more sites and signals with vastly reduced manual triage.
Acquisition Path	Aligns with State and Local Cybersecurity Grant Program (SLCGP) funding paths.

Operating Profile: Utilities

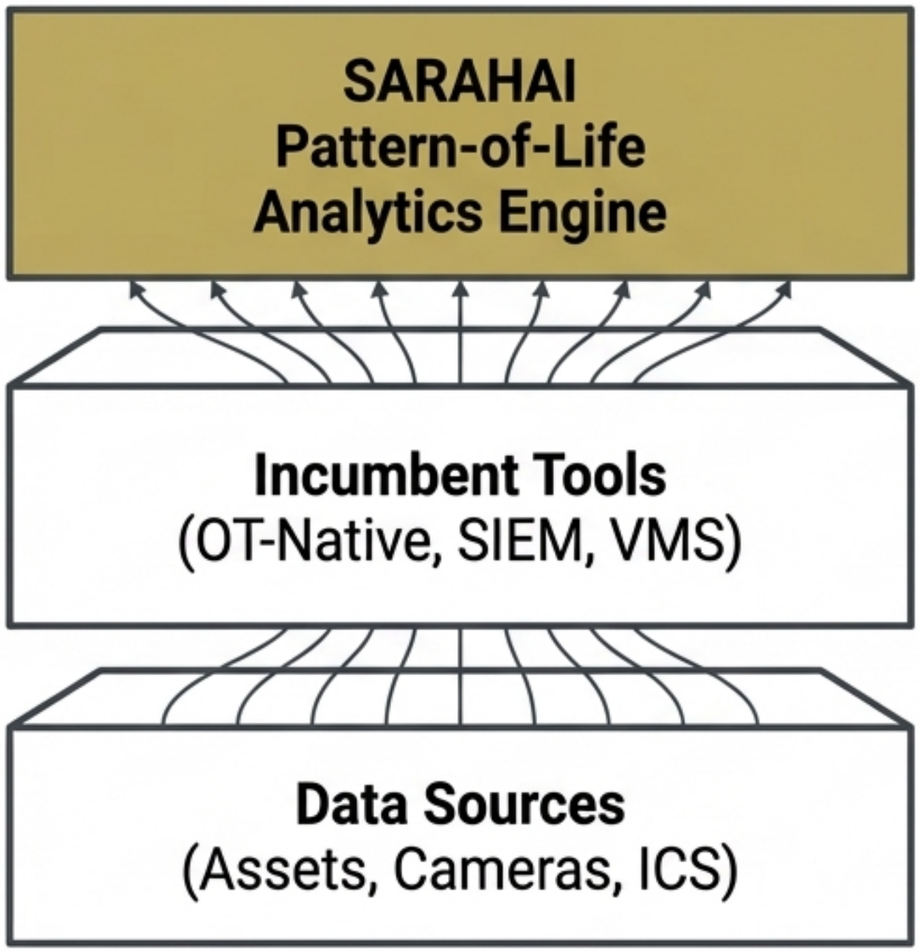


Inter

Primary Focus: Outage Economics & Resilience

The Problem	High-consequence OT environments requiring cross-domain correlation (NERC CIP-015-1). ORNL reports the U.S. annual cost of major outages reached **$121 billion** in 2024.
The Value Driver	Acts as a cross-domain overlay for anomaly confirmation. The economic case is driven by **avoided or shortened outages**, where tiny reductions in downtime justify the investment.

The Convergence Overlay Strategy



The Coexistence Posture: Do not rip and replace.

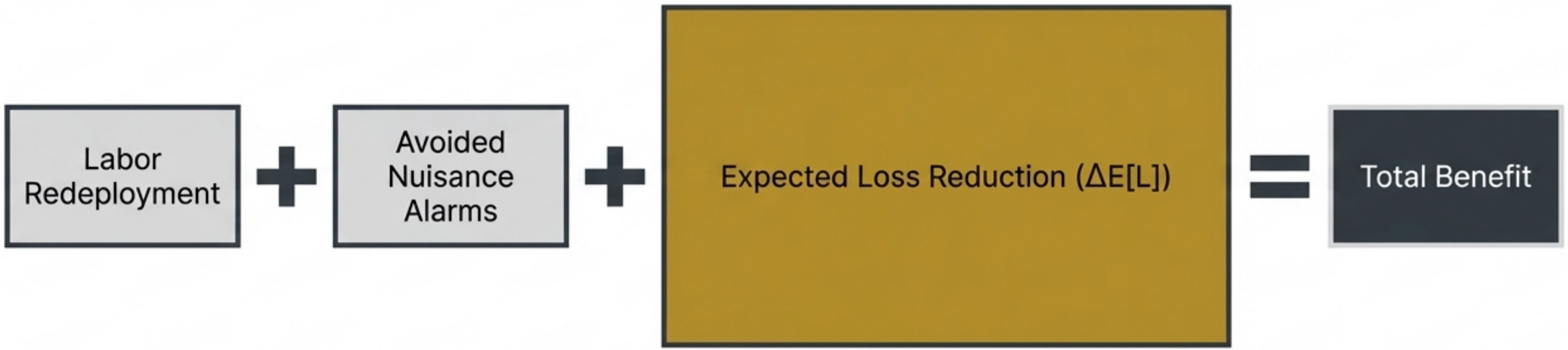
Keep OT-native tools for protocol depth.
Keep SIEMs for enterprise log orchestration.
Keep VMS for camera management.

Deploy SARAHAI strictly as the convergence engine to fuse heterogeneous data and surface cross-domain anomalies.

Architectural Fit & Competitive Coexistence

Category	Incumbent Strength	SARAHAI Advantage
OT-Native (e.g., Dragos, Claroty)	Deep OT protocol coverage.	**Cross-domain PoL** across cyber, physical, and operational data.
Enterprise SIEM (e.g., Sentinel)	Massive log aggregation and SOC playbooks.	Learning "normal" physical/operational combinations without heavy rule engineering.
Physical Security (e.g., Genetec)	Camera management and operator ergonomics.	**Broader telemetry** and PoL analysis beyond video.
Custom ML Data Lakes	Maximum bespoke flexibility.	**Lower deployment friction** for non-expert teams.

The Resilience ROI Equation



The Logic: For critical infrastructure, labor savings rarely justify the program alone. The true business case relies on expected-loss reduction: identifying pre-incident indicators earlier and accelerating triage to prevent or shorten high-consequence disruption.

Break-Even Sensitivity

The Reality: You do not need to prevent every incident. Preventing a single high-impact near-miss or drastically cutting false-triage time validates the investment.

Outage Hours Avoided	
At a $250k program cost and a $1M/hour outage consequence, the platform breaks even by preventing just **0.25 hours** of downtime annually.	
$1M/hour Consequence	0.25 hours

Labor Redeployment	
At a **$250k program cost**, the platform breaks even by saving the equivalent of 1.67 loaded FTEs (at $150k/FTE) from manual triage.	
$150k/FTE Cost	1.67 FTEs

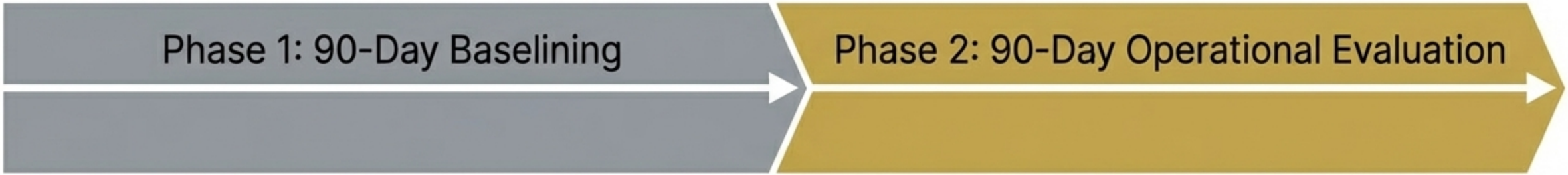
Framework Alignment & AI Governance

NIST CSF 2.0 Fit: Core SARAHAI maps directly to continuous monitoring, anomaly discovery (**Detect**), and cross-domain triage context (**Respond**). It is a decision-support capability, not a compliance panacea.

Mandatory Guardrails (DHS 2024)

- ✓ **Human Decision Authority**: SARAHAI supports human triage; it does not autonomously adjudicate response.
- ✓ **Baseline Management**: Controlled schedules for re-baselining to manage operational drift.
- ✓ **Evidence Integrity**: Retains timestamped logs and provenance for defensible after-action reviews.

The 180-Day Pilot Framework



A structured, KPI-driven evaluation against existing baseline alert streams.

Federal Success Metrics

Time-to-triage, nuisance-alert reduction, cross-domain correlations surfaced.

SLED Success Metrics

Analyst hours redeployed, alert relevance, potential downtime avoided.

Utility Success Metrics

Lead time on abnormal events, remote-session anomaly yield, operationally meaningful correlations.

The Decision Criterion: Continue to scale only if SARAHAI materially improves early warning and prioritization across the seams existing tools leave exposed.