FRAMEWORK #162

Security Entropy Accumulation

DEFINITION

Security posture degradation that accumulates while infrastructure remains fully converged with declared configuration state. Declared and actual state continue to match, but the security value of that state decays over time.

FRAMEWORK FLOW

01
Patch Latency Debt
Time since an available patch accumulates silently in fully converged infrastructure.

02
Credential Staleness
Unrotated secrets and certificates keep validating while their security value decays.

03
Permission Creep
Additive-only IAM and RBAC grants stay compliant with declared policy while violating least privilege.

04
Exposure Window Accumulation
Exceptions and legacy allowances persist past their justification, unflagged by reconciliation.

Failure State: Security Baseline Divergence

`Infrastructure fully converged` → `Every reconciliation check passes` →
`Reconciliation scoped to declared state only` → `Security value decays unobserved` →
`Posture diverges from design intent`

THE DIAGNOSTIC SIGNAL

CONVERGENCE IS NOT SECURITY
Ask what the drift detector actually measures. It measures state against declared state. Nothing in it measures state against the design intent.

PARALLEL DOMAINS
The four domains do not depend on each other firing first. Any one can degrade posture while the others stay clean.

TRIGGER CONDITION
Time. No change event occurs, so no origin exists to trace, and the degradation is invisible to every tool built to catch change.

REMEDIATION SHAPE
Point the reconciliation pattern that made configuration drift tractable at a different baseline, with one loop per entropy domain.

ONE RECONCILIATION LOOP PER DOMAIN

PATCH LATENCY DEBT
Security baseline reconciliation: check infrastructure against the current patch catalog, not only its own declared state.

CREDENTIAL STALENESS
Automated rotation enforcement. Rotation age becomes a checked property instead of an assumed one.

PERMISSION CREEP
Authorization recertification. Grants expire by default unless explicitly renewed, inverting the additive-only failure mode.

EXPOSURE WINDOW ACCUMULATION
Expiry-driven exception controls. Every exception carries a closure deadline enforced by the system.

ARCHITECTURAL RELATIONSHIPS

#4
Drift Origin Model
DEPENDENCY · STRONG

Without a traceable-origin drift taxonomy this framework has no baseline. It names degradation that produces no origin event.

#133
Policy Intent Drift
RELATED · MODERATE

Mirror-image failure: #133 is declared-versus-enforced divergence, #162 is declared and enforced agreeing while security value still worsens.

#151
Infrastructure Evidence Gap
RELATED · MODERATE

Shared pattern: a system reports healthy according to its own instrumentation while reality disagrees.

ANCHOR /security-drift/
FRAMEWORK HOME

One of two culminating frameworks in the Governance and Drift stage, alongside #159. A fully governed system failing quietly, because nothing ever drifted.

"Nothing drifted. The posture got worse anyway."