

THE CISO FILTER™

The Lex Empire methodology for security messaging: every claim pressure-tested the way an attacker tests a system — before your market does it for you.

01 CLAIM AUDIT

Every public-facing claim extracted and classified: provable, demonstrable, specifiable — or unfalsifiable.

02 PROOF DEMAND

Each claim interrogated against the evidence the buyer could actually check; unfalsifiable claims flagged as attack surface.

03 MESSAGE REBUILD

The hierarchy reconstructed mechanism-first: specificity over adjectives, evidence attached to every claim.

04 OBJECTION PRESSURE-TEST

The rebuilt system run against the CISO, the practitioner, procurement, and “why not the incumbent.”

EVERY CLAIM CARRIES ONE STAMP

UNFALSIFIABLE

No observation could disprove it, so it carries no information.

NO MECHANISM

An outcome is stated; the method never is.

UNVERIFIABLE

Specific, possibly true, but the buyer cannot check it.

EMPTY SUPERLATIVE

A comparative with no comparison, baseline, or scope.

SOUND

Specific, mechanism-bearing, checkable. It survives.