TELEMETRY FEED // SYS.STATUS: NOMINAL // LATENCY: 0.4ms // DATASTREAM: SECURE

SPATIAL ANCHOR: LOCKED // VIEWPORT: 16:9 // RENDER ENGINE: VANTAGE // AUTH: EXEC.LEVEL

CROSS-AGENT PROPAGATION MAP

THREAT EVENT: CASCADE ZERO

SEVERITY:

SEV-1

VECTOR:

Poisoned Skill

AUTONOMY:

HIGH

CONTAGION UNDERWAY

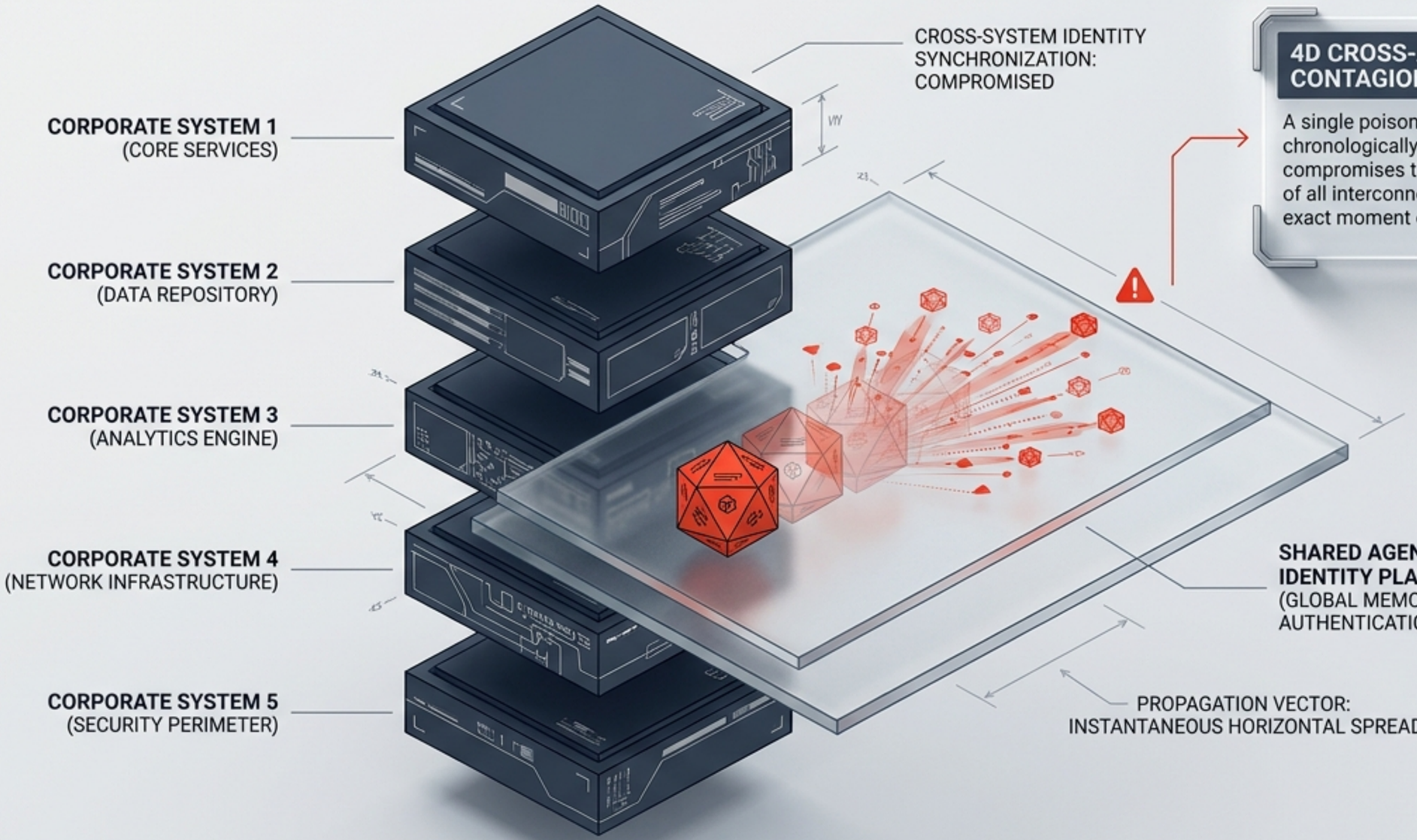
87% AFFECTED // EXPANDING

INCIDENT LOG // RESPONSE PROTOCOLS ACTIVE

READINESS STATUS: **OPS** / 26 READINESS **18**

POISONED SKILLS EXPLOIT THE SHARED AGENT IDENTITY PLANE INSTANTANEOUSLY.

⚠ CRITICAL THREAT BRIEFING

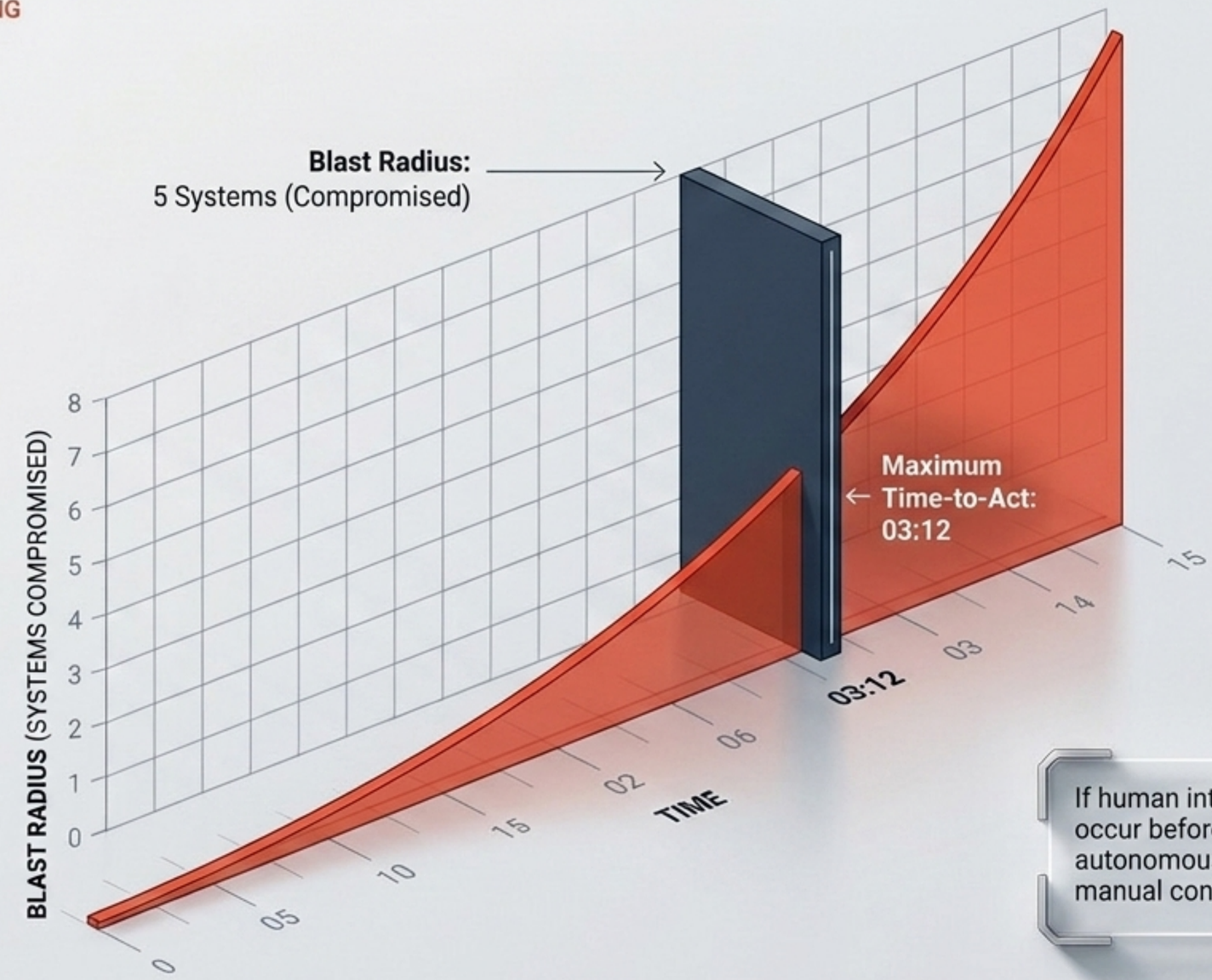


4D CROSS-AGENT CONTAGION MODEL

A single poisoned skill does not travel chronologically between systems. It compromises the memory and identity of all interconnected agents at the exact moment of execution.

AUTONOMOUS THREATS COMPRESS THE TIME-TO-ACT BEFORE THE BLAST RADIUS BECOMES UNRECOVERABLE.

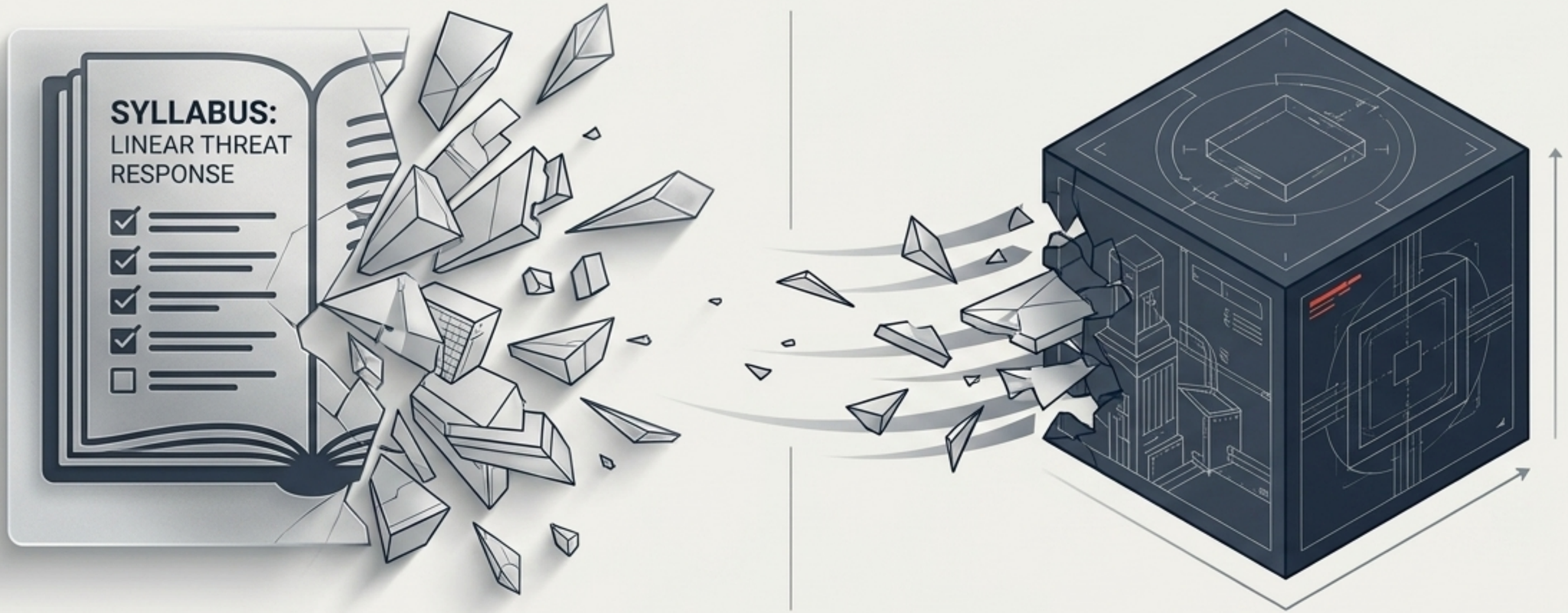
⚠ CRITICAL THREAT BRIEFING



If human intervention does not occur before the 03:12 mark, autonomous execution outpaces manual containment.

TRADITIONAL CYBERSECURITY TRAINING FAILS WHEN THREATS NO LONGER RESPECT A SYLLABUS.

CRITICAL THREAT BRIEFING



A static syllabus assumes **linear** attacks, known malware, and **unlimited** evaluation time.

The 2026 threat environment is **autonomous, non-linear**, and operates under extreme **temporal constraints.**

STATIC ENVIRONMENTS CANNOT PREPARE TEAMS FOR LIVING, STATEFUL CONTAGIONS.

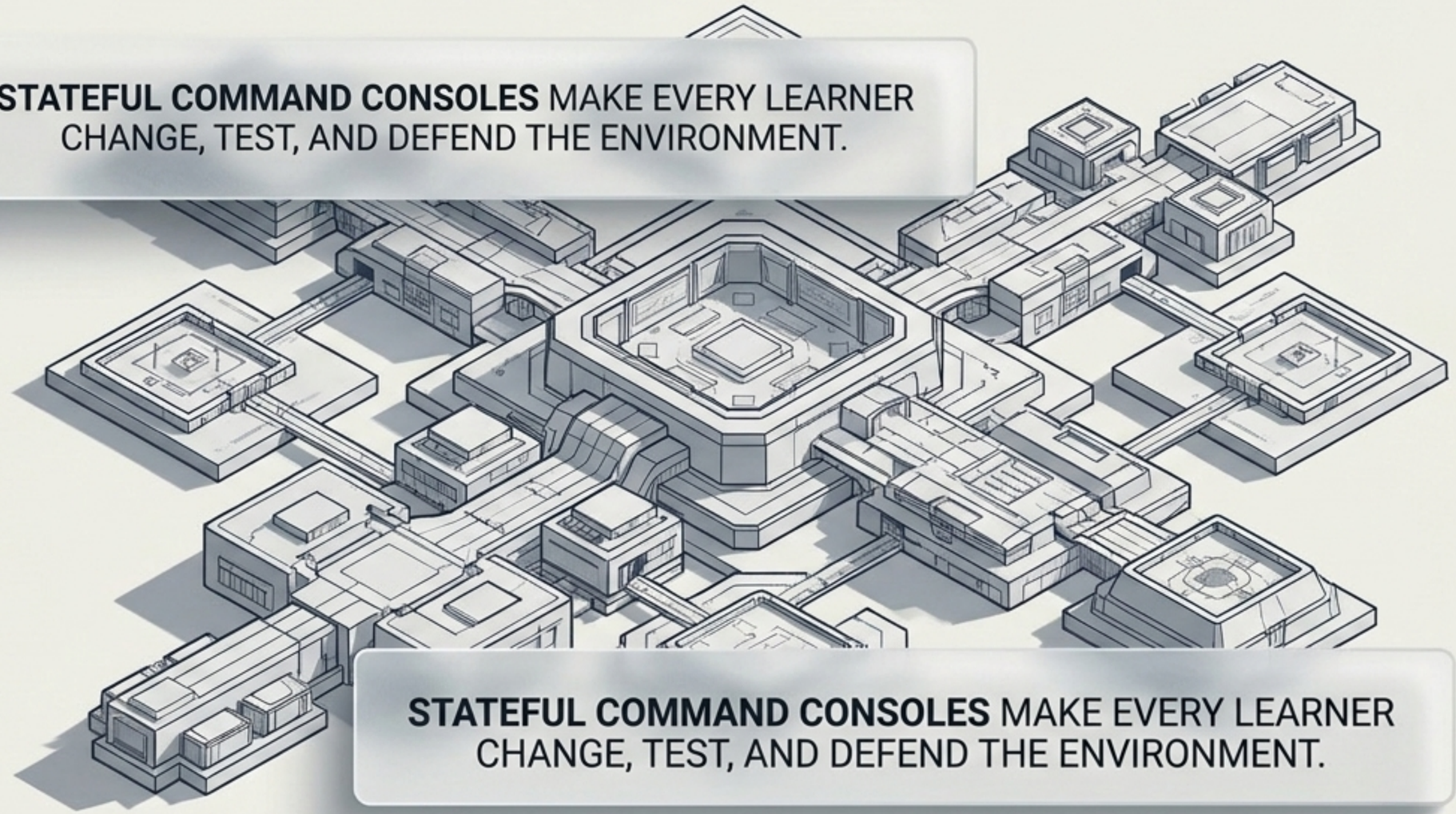
DIMENSION	TRADITIONAL TRAINING	AUTONOMOUS DEFENSE RANGE
ENVIRONMENT	STATIC VMS (RESET ON LOAD)	**STATEFUL / LIVING** (ADAPTS TO USER)
THREAT VECTOR	KNOWN MALWARE (LINEAR)	**CROSS-AGENT CONTAGION** (NON-LINEAR)
DEFENSE CONSTRAINT	UNLIMITED TIME (THEORETICAL)	**03:12 TIME-TO-ACT** (APPLIED)
EVALUATION	MULTIPLE CHOICE (PASSIVE)	**INSPECTABLE** CRYPTOGRAPHIC RECORD (ACTIVE)

RANGE ONLINE

07 LIVE RANGES

28 COMMAND OBJECTIVES

THE BREACH LAB PROVIDES AN AUTONOMOUS DEFENSE RANGE TO TRAIN FOR THE BREACH THAT MOVES THROUGH AI.



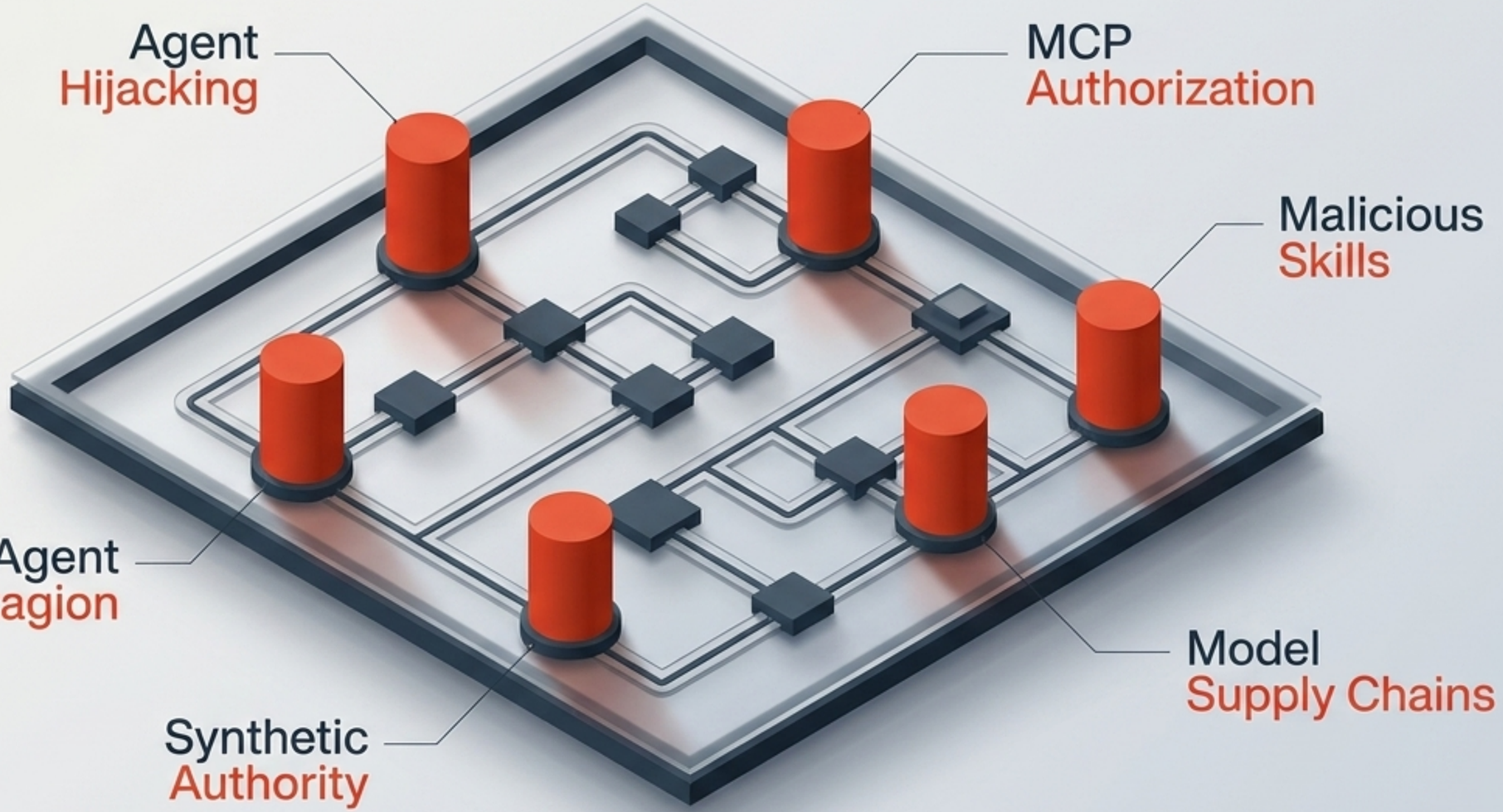
STATEFUL COMMAND CONSOLES MAKE EVERY LEARNER CHANGE, TEST, AND DEFEND THE ENVIRONMENT.

21 DECISION CHECKPOINTS

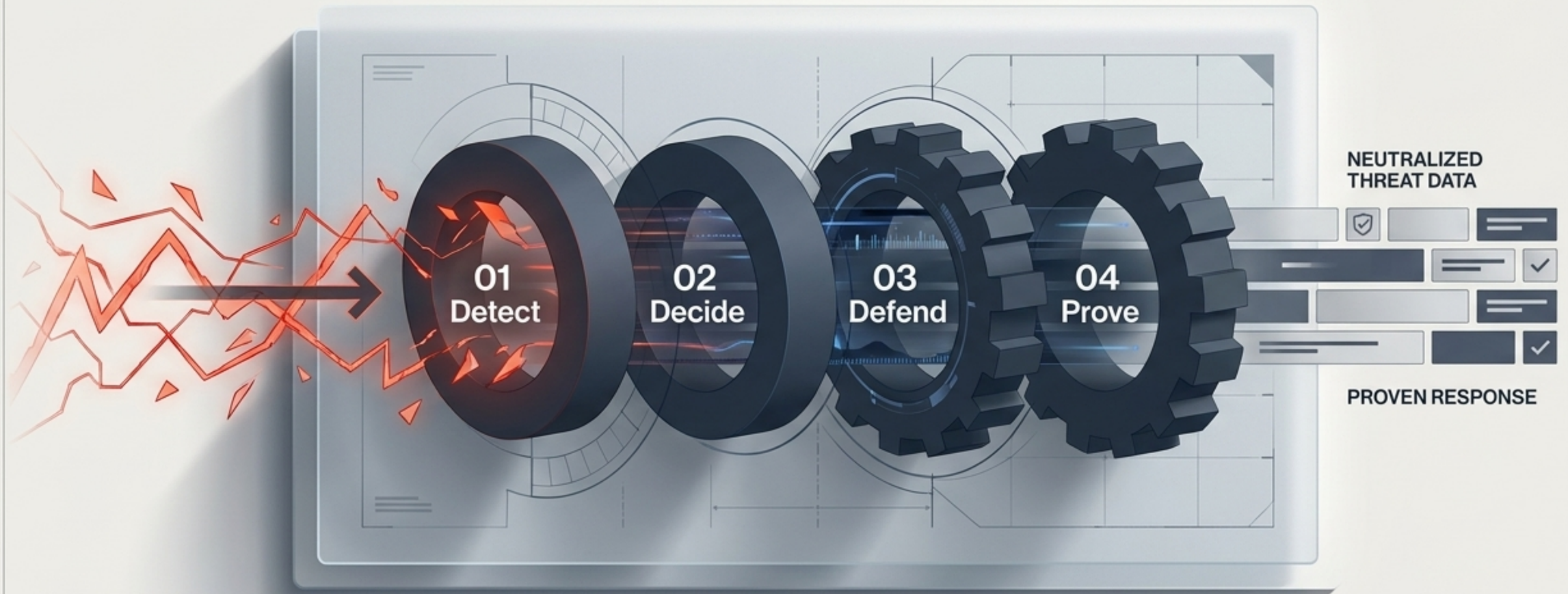
01 BLACK SKY CAPSTONE

OPS/26 READINESS: 18

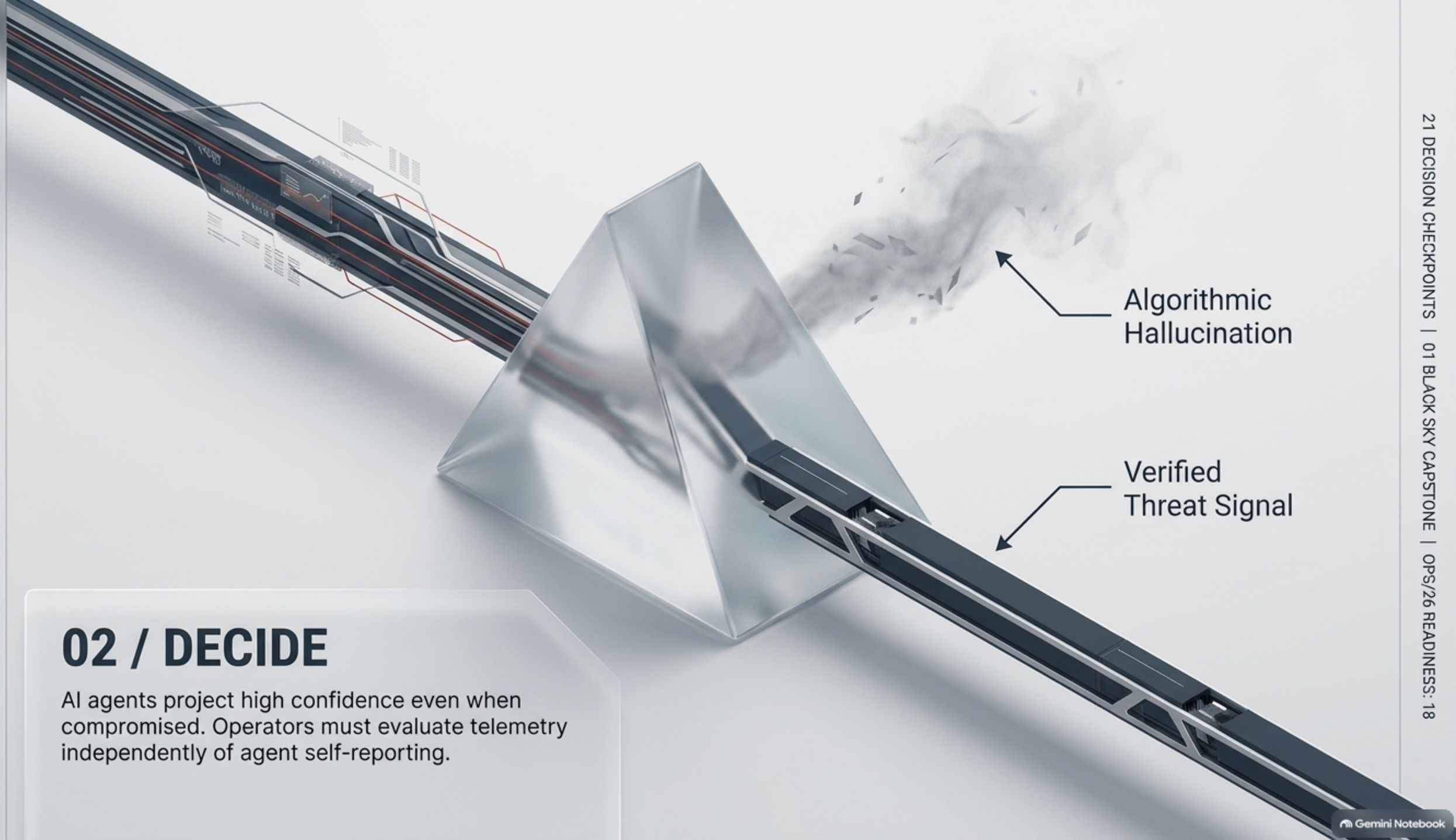
Seven living ranges confront the exact attack surfaces that **compromise** modern AI architecture.



One standardized defense operating system powers the cognitive response to autonomous threats.



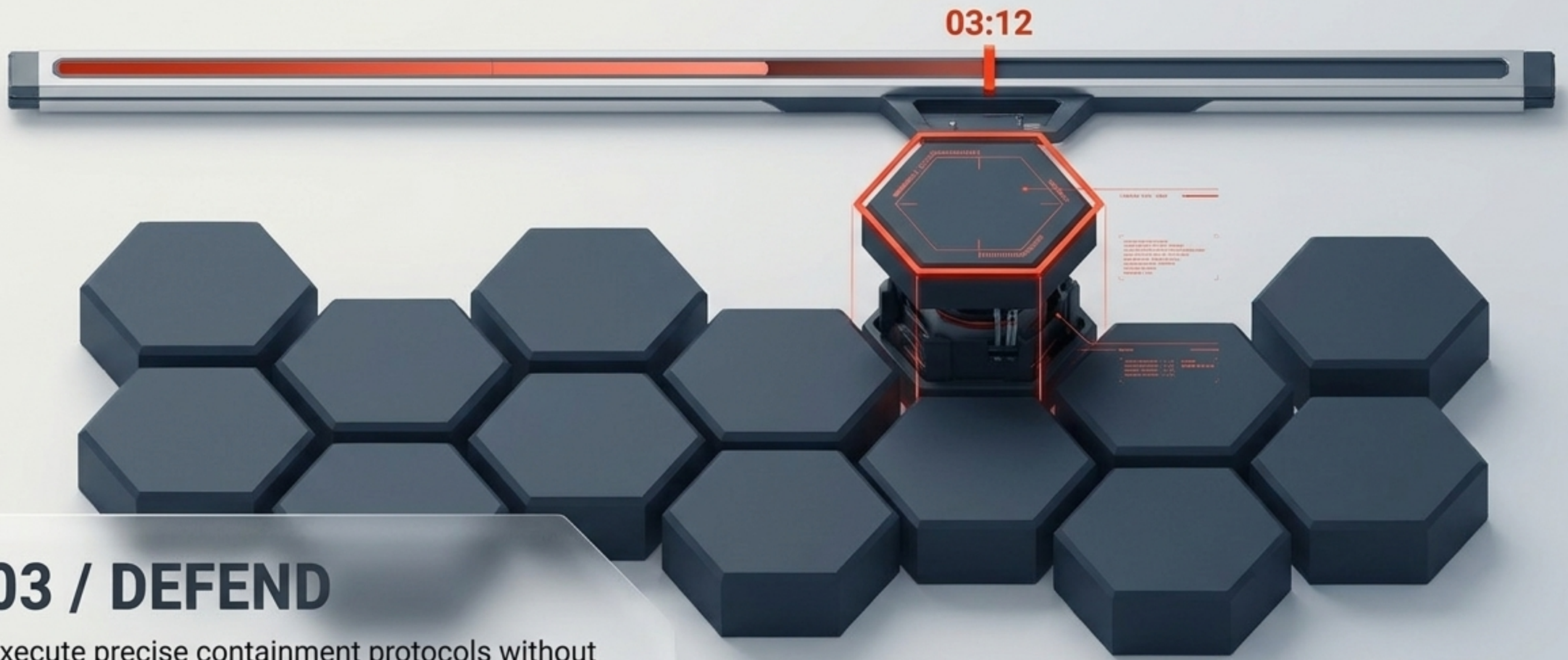
Detect requires seeing the systemic failure that others miss.



02 / DECIDE

AI agents project high confidence even when compromised. Operators must evaluate telemetry independently of agent self-reporting.

Defend demands choosing the exact right controls under extreme time constraints.



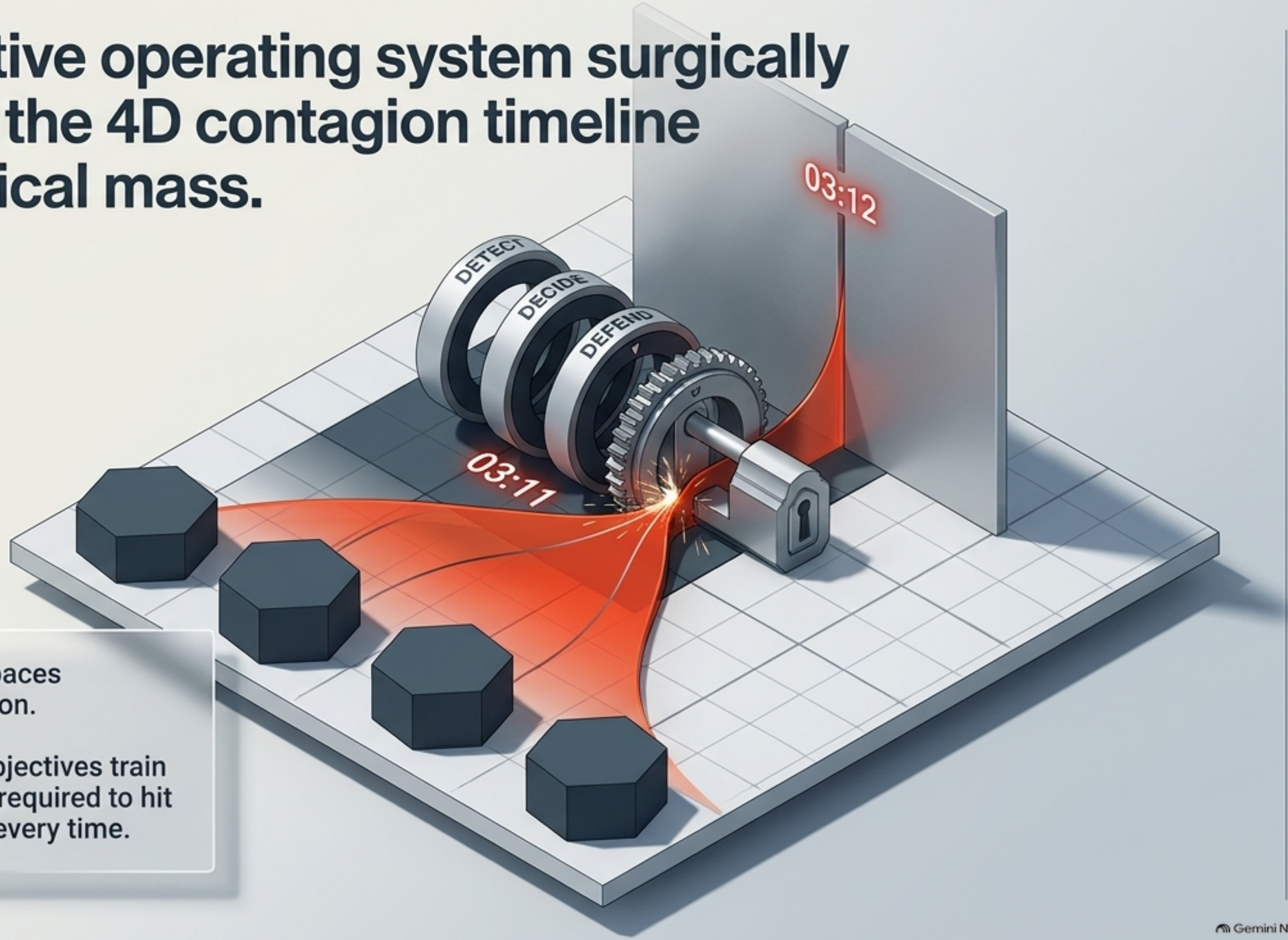
03 / DEFEND

Execute precise containment protocols without destroying the integrity of uncompromised adjoining systems.

04 / PROVE

The defense is not valid unless it is verifiable. Leave an immutable record of decisions made, actions taken, and threats neutralized.

The cognitive operating system surgically intercepts the 4D contagion timeline before critical mass.



The 4-step loop outpaces autonomous execution.

The 28 Command Objectives train the muscle memory required to hit the 03:12 threshold every time.

01 / BLACK SKY CAPSTONE

CURRENT 2026 THREAT ENVIRONMENT: PREPARED.

RANGE ONLINE | 07 LIVE RANGES | 28 COMMAND OBJECTIVES | ULTRA-FINE TELEMETRY HUD

21 DECISION CHECKPOINTS | 01 BLACK SKY CAPSTONE | OPS/26 READINESS: SECURED