DAFITC 2026 · TRACK 2

DECISION AUTHORITY

AT MACHINE SPEED

Securing the Human Edge in Agentic Cyber Operations

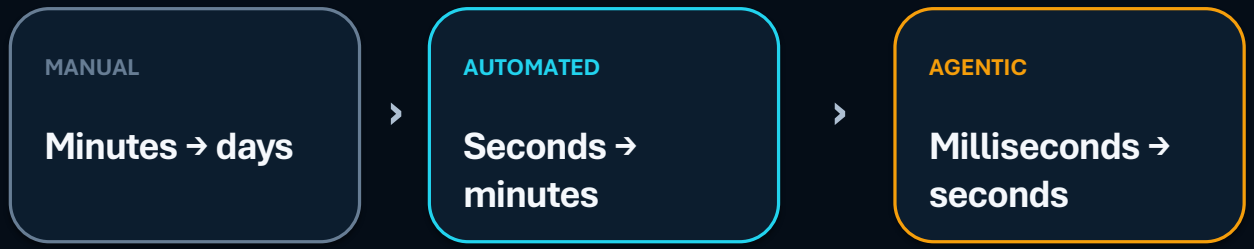
Allen Westley
Director, Cyber Intelligence

Agile. Assured. Accountable—from enterprise to orbit.



THE ASSURANCE GAP

Machine-speed action is outrunning human-speed accountability.



The critical question is no longer only "Did the system perform?"

It is also: Who owned the decision when the machine acted before the human fully understood?

ASSURANCE EVOLUTION

From compliance-centric authorization to continuous, data-centric assurance.

Traditional governance remains necessary. It is no longer sufficient by itself.

01
PROFILE
Mission context

›

02
CONTINUOUS
Risk signals

›

03
PREDICT
Emerging exposure

›

04
ASSURE
Accountable action

Automate evidence collection and response—not accountability.

DECISION AUTHORITY MAPPING

Separate what the machine can see, suggest, decide, and execute.

SENSE	Observe and summarize activity
RECOMMEND	Prioritize options and explain rationale
DECIDE	Select an action within delegated bounds
EXECUTE	Act with technical or operational effect

Control principle: Higher-impact action requires clearer context, tighter decision bounds, and explicit ownership.

PRACTICAL METHOD

Agentic Role Mapping clarifies responsibility before deployment.



Authority
What may the agent do?

Evidence
What must it show?

Escalation
When must a human intervene?

Accountability
Who answers for the outcome?

HUMAN EDGE UNDER PRESSURE

Three failure modes hide behind “human in the loop.”

01

APPROVAL FATIGUE

Repeated prompts become ritual. Review turns into reflexive consent.

02

COGNITIVE DRIFT

Operators gradually inherit the machine’s framing of risk.

03

ACCOUNTABILITY GAP

Authority is distributed, but responsibility remains unresolved.

A human click is not evidence of meaningful human judgment.

OPERATIONAL VISIBILITY

Cognitive Indicators of Compromise expose degradation in human judgment.

Override collapse	Humans stop challenging recommendations.
Rationale decay	Explanations become thinner as action speeds up.
Escalation avoidance	Ambiguous cases remain inside automated flows.
Frame convergence	Teams adopt the same machine-generated interpretation.
Decision latency inversion	Humans delay only after the machine has acted.
Ownership ambiguity	No one can state who held final authority.

Treat these indicators as operational signals—not personnel failures.

APPLIED SCENARIO

A machine-speed defensive action across the kill web.

DETECT

Agent correlates anomalous activity

RECOMMEND

Isolate node and revoke credentials

DECIDE

Policy permits autonomous containment

EXECUTE

Access is severed across mission systems

POLICY

Was the authority delegated?

EVIDENCE

Was the rationale visible?

RESILIENCE

Could the action be reversed?

ACCOUNTABILITY

Who owned mission impact?

PRESERVE SPEED WITHOUT SURRENDERING OWNERSHIP

An AI-fluent cyber team combines delegation, evidence, and disciplined intervention.

BOUND

Define authority before deployment.

Mission owners set decision limits and prohibited effects.

OBSERVE

Instrument the human-machine workflow.

Capture rationale, confidence, overrides, and escalation behavior.

INTERVENE

Rehearse exceptional conditions.

Design reversible actions and practice authority recovery.

The objective is not slower automation. It is faster, explainable, recoverable decision-making.

QUESTIONS?

The technology may move at machine speed.

Responsibility still belongs to people.

CALL TO ACTION

Map one human-machine decision path before your next agentic deployment.



Allen Westley | Director, Cyber Intelligence

DAFITC 2026 · Automated, Agile, and Assured