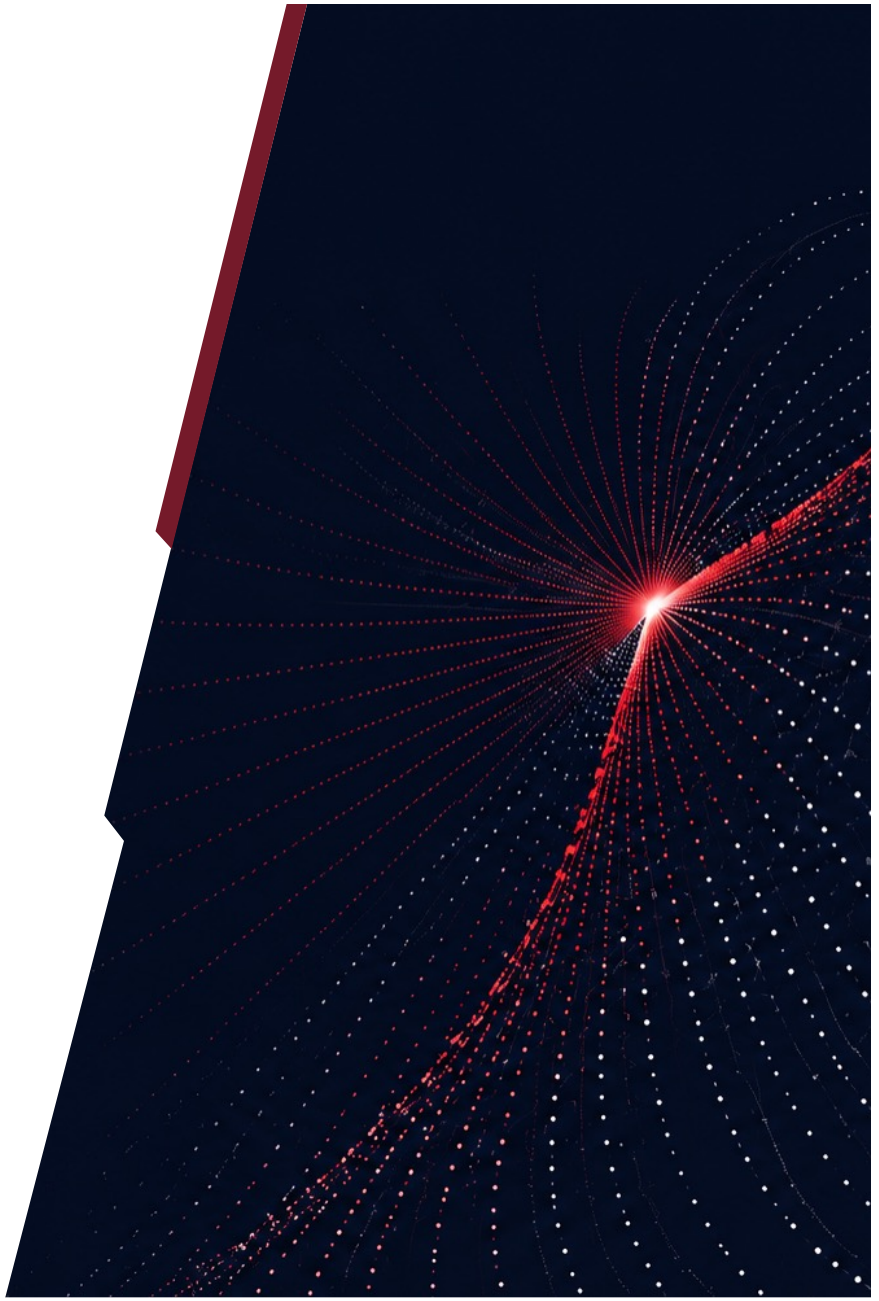
ARLO
DECISIONBEACON

BEYOND COMPLIANCE:

THE FUTURE OF CYBER RISK DECISION MAKING

August 2026

CUTTING THROUGH THE CYBER NOISE



SESSION ROADMAP

Where We're Headed



1 The Limits of the Point-in-Time ATO

- Slide 4: The Snapshot Problem
- Slide 5: The Environment Moves

2 Turning Cyber Data into Decision Advantage

- Slide 6: The Decision Gap
- Slide 7: Beyond Reporting
- Slide 8: The Decision Loop

3 Building a Continuous Decision Loop

- Slide 9: The Mission View
- Slide 10: Role-Based Decisions
- Slide 11: Practical Takeaways
- Slide 12: The Solution
- Slide 13: cATO Framework

4 A Practical Example: DecisionBeacon

- Slide 14: DecisionBeacon Practical Example
- Slide 15: Mission Partner Opportunities

ARLO
DECISIONBEACON

LONYE FORD

U.S. Air Force Veteran | Co-founder |
CEO, Arlo Solutions

- Served in Information Assurance for the U.S. Air Force
- Co-authored the U.S. Air Force Fast Track ATO process
- Developed and streamlined the USDA's Risk Management Framework process

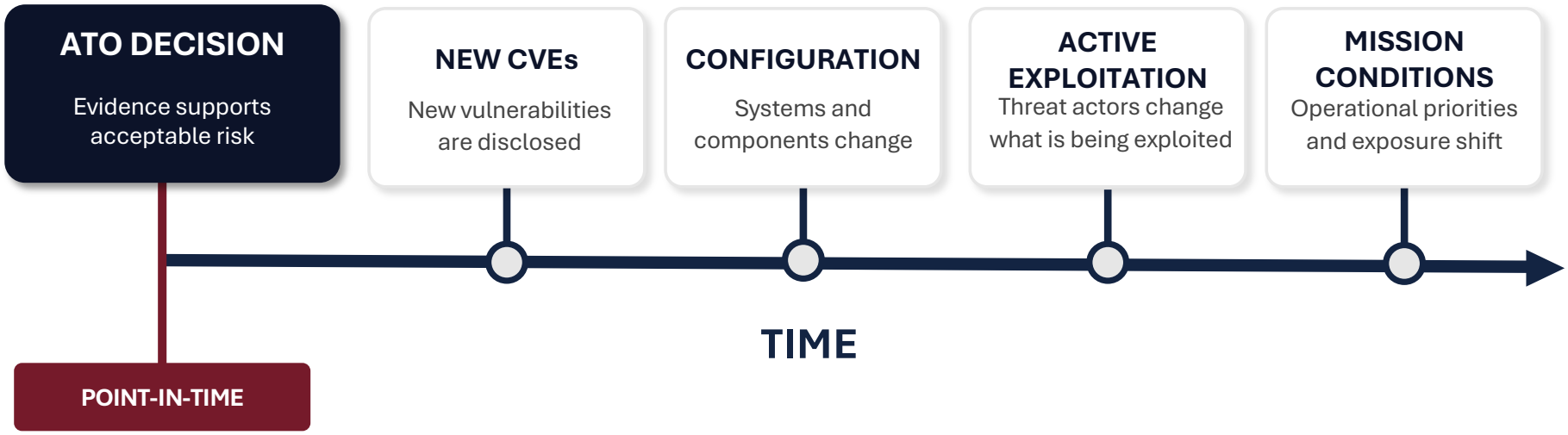






The Snapshot Problem

THE AUTHORIZATION IS A SNAPSHOT. THE ENVIRONMENT KEEPS MOVING.



Leaders are forced into critical decisions with noisy, incomplete information.

- The result is misaligned decisions and costs amid growing threats and vulnerabilities

THE DECISION QUESTION CHANGES:

Does the original risk decision still hold?

The Environment Moves

Cyber risk changes constantly—faster than traditional authorization cycles



CHANGE IS CONSTANT. RISK IS DYNAMIC.

- >30,000 CVEs published in 2024
- Median time to exploit < 5 days
- >70% of organizations changed cloud configurations in the past 30 days*
- User and access changes happen daily

THE CONSEQUENCE

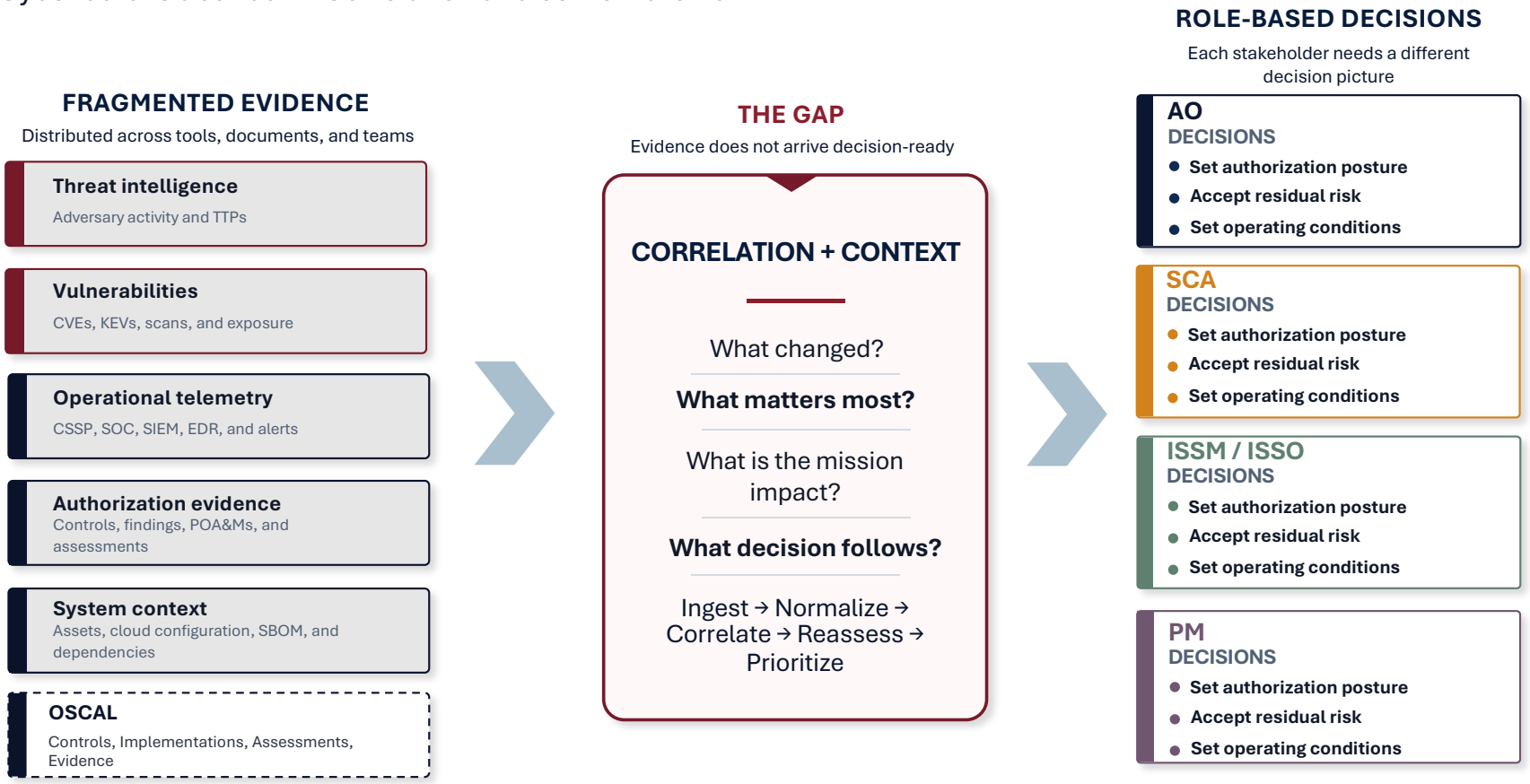
What was an acceptable risk yesterday may be an unacceptable risk today.

Point-in-time reviews can't keep up. You need continuous visibility and continuous context to make timely, defensible risk decisions.

* Source: Gartner, 2024; CISA KEV Catalog; Tenable Vulnerability Intelligence Report 2024

The Decision Gap

Cyber data is abundant. Correlation and context are not.



MACHINES FOR VOLUME. HUMANS FOR JUDGMENT.

The challenge is not visibility — it is connecting fragmented evidence to the context each role needs to make a timely decision

Beyond Reporting

Current State

Continuous Reporting:

- More dashboards
- More alerts
- More status updates
- More data to interpret

Data

Desired State

Continuous Monitoring:

- Detect changes
- Determine risk impact
- Prioritize action
- Validate response

Decision

Continuous Monitoring is a decision process – not a reporting cadence

The Decision Loop

Continuous Monitoring should create decision advantage—not just more reporting.

Use automation to compress the cycle:
observe the environment, orient risk in context, decide what matters, and act with defensible evidence.

AF connection

OODA was developed by U.S. Air Force Col. John Boyd to explain decision advantage in a changing environment.



SO WHAT?

A faster OODA loop.

Continuous monitoring should shorten the time between change and action.

Goal: faster decisions with current context, clear ownership, and evidence that keeps the authorization defensible.

The Mission View

Cyber data is abundant. Correlation and context are not.

Decision question

Why does this vulnerability matter to the mission?

Severity is only the starting point. Mission context determines priority. The goal is operational risk, not just technical risk.

So What?
You cannot prioritize cyber risk correctly unless you know what the affected system enables.

From technical signal to mission consequence

Threat / Vulnerability	Affected Asset / System	Control / Safeguard	Mission Function	Operational Impact
Active CVE exploit activity	Mission app cloud service	Mitigation control status	Capability supported	Identify mission risk

Context lens

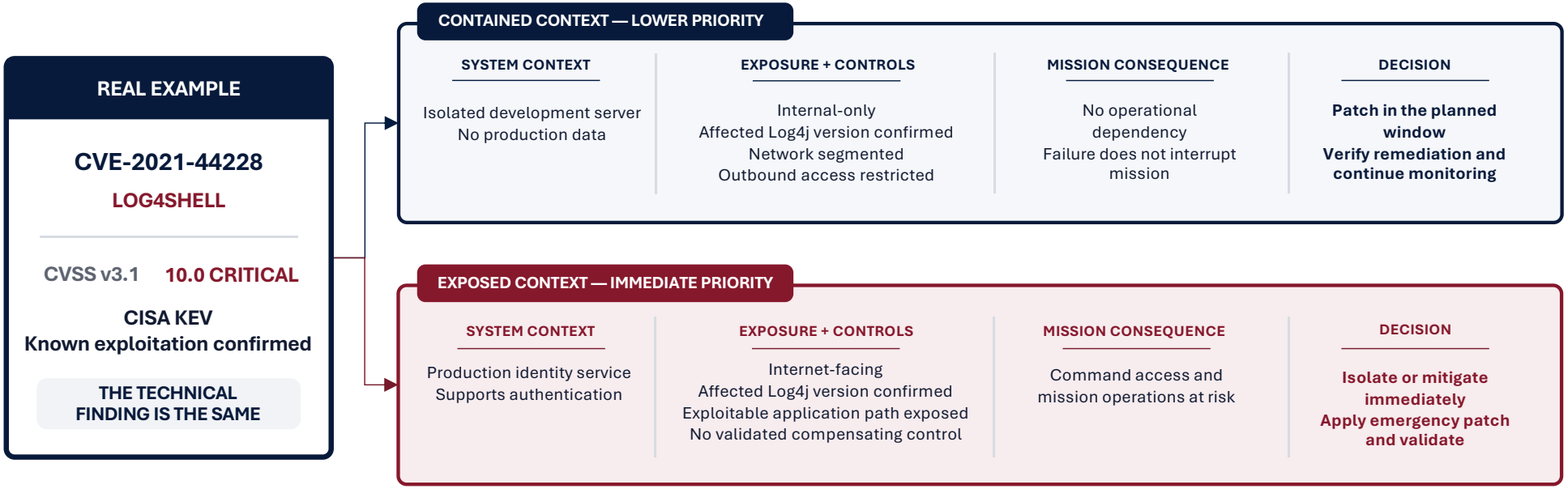
Present? Reachable? Actively exploited? Mission-critical? Effective control?

A critical CVE is not automatically the highest mission risk.

Continuous Monitoring becomes decision support when cyber data is connected to mission impact.

Role-Based Decisions (example)

Severity describes the vulnerability. Mission context determines what deserves attention first.



THE SAME EVIDENCE DRIVES DIFFERENT ROLE-BASED ACTIONS

ISSO	Validate affected instance and exposure	**ISSM**	Set priority, escalation, and tracking	**SCA**	Assess controls and residual risk	**AO**	Set conditions or accept risk	**PM**	Align resources, outage, and schedule

The vulnerability and threat are the same. Context determines priority, action, and ownership.

What You Can Do Now

Practical steps to mature Continuous Monitoring before any new tool is added.

1

Build the Continuous Monitoring Strategy

Define what to monitor, why it matters, and which changes should trigger review, escalation, or action.

2

Prioritize What You Patch

Focus remediation on vulnerabilities that are present, exploitable, actively targeted, mission-relevant, and fixable.

3

Exercise the Decision Process

Use realistic tabletops to test people, information flow, authorities, communications, and response timing.

4

Validate Incident Response & Controls

Treat incident response as part of Continuous Monitoring. Prove safeguards, escalation paths, and recovery actions work.

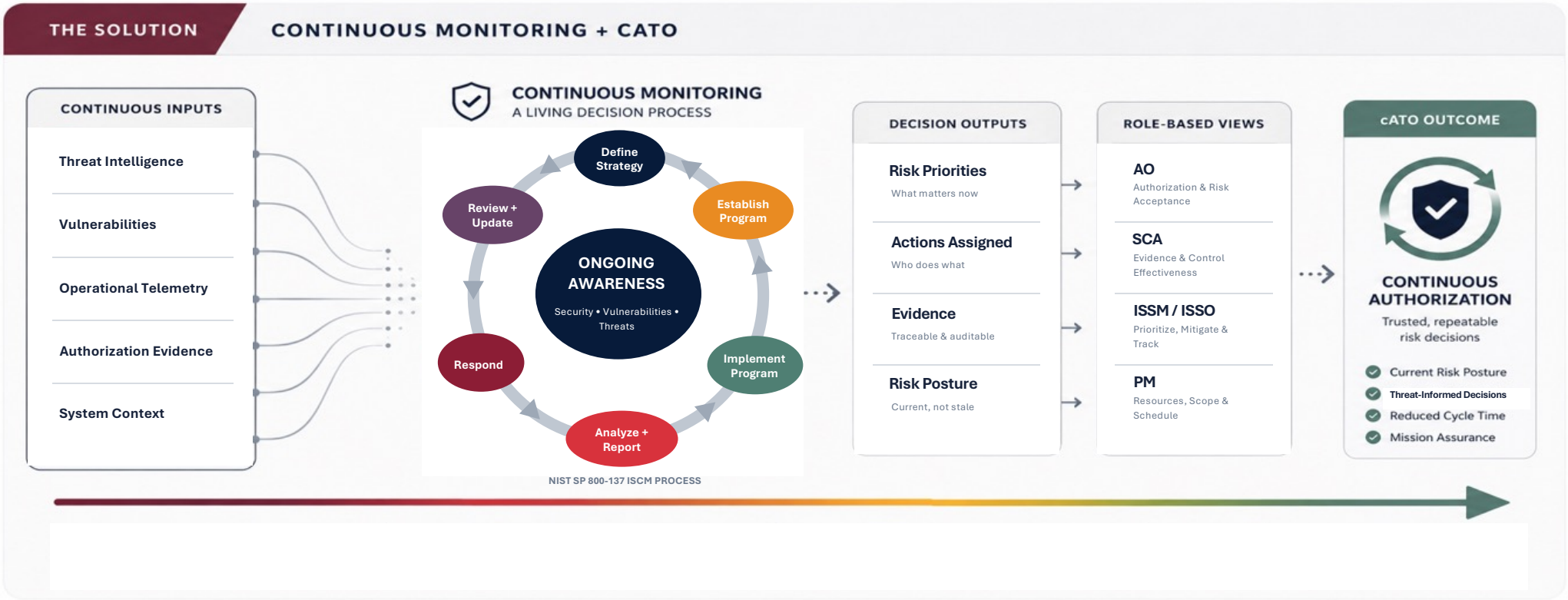
5

Capture Evidence & Improve

Document decisions, measure outcomes, and feed lessons learned from incidents and exercises back into the monitoring cycle.

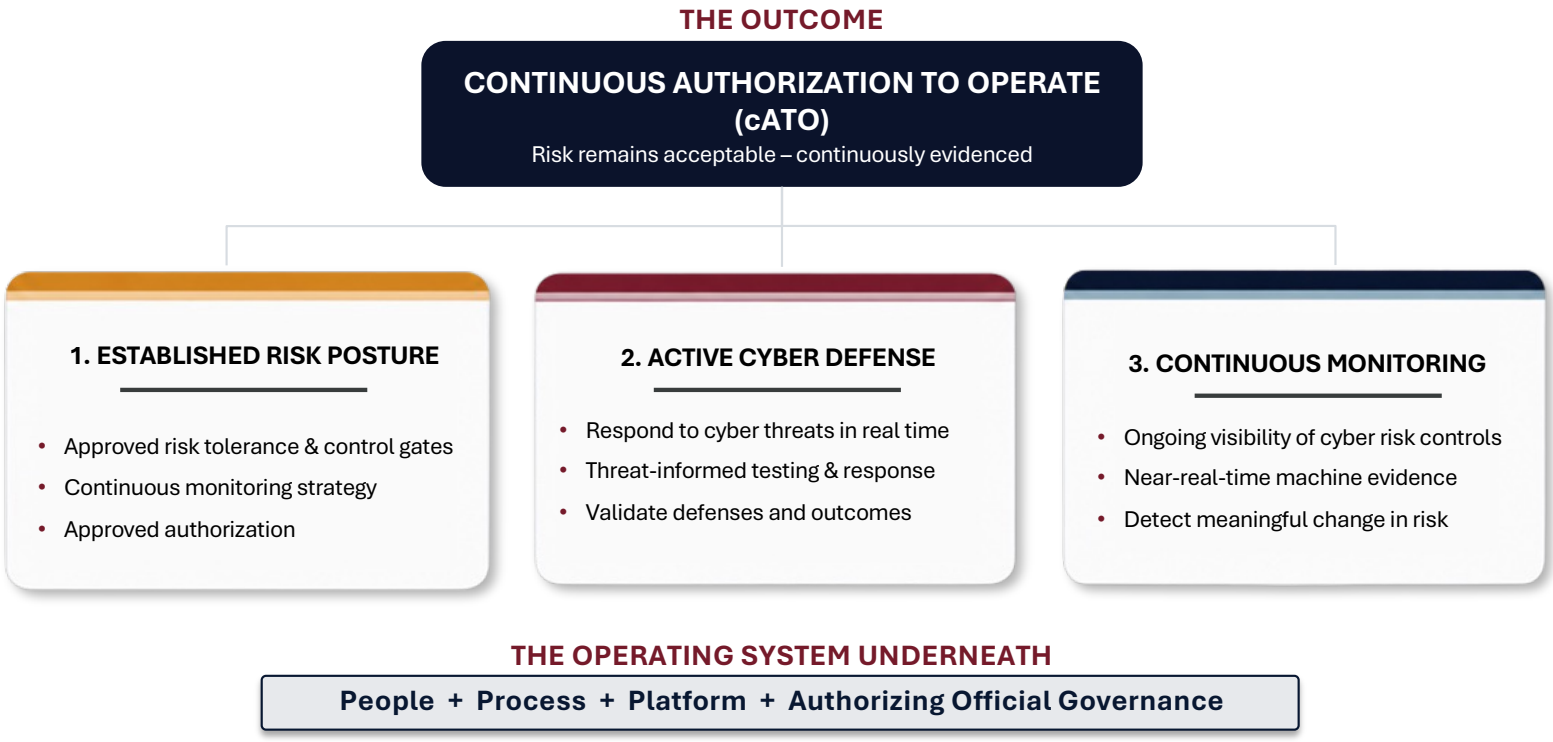
Continuous Monitoring is an operating discipline: know what changed, what matters, and what action reduces risk.

The Solution



A Framework for Continuous Authorization

Continuous authorization is an operating state – not a faster approval cycle.



Automation enables continuous authorization—but governance, context, and human judgment sustain it.

DecisionBeacon (Practical Example)

The decision layer for continuous monitoring & continuous authorization

WHAT DECISIONBEACON IS

DecisionBeacon is a threat-informed operational decision platform that continuously correlates cyber, threat, vulnerability, authorization, and mission data—helping stakeholders make faster, more confident operational decisions.

- Continuous Monitoring Intelligence
- Continuous Authorization Support
- Threat-Informed Risk Evaluation
- Mission-Aware Prioritization
- AI-Assisted Decision Support
- Operational Risk Visibility
- Human-Governed Cyber Reasoning
- Actionable Mitigation Guidance

FROM DATA TO DECISIONS

Threat Intel | CVEs / CPEs | SBOM / HBOM | Controls | Telemetry | POA&Ms | Authorization Conditions

DECISIONBEACON

CORRELATE | CONTEXTUALIZE | VALIDATE | PRIORITIZE | RECOMMEND

BETTER DECISIONS. STRONGER MISSIONS.

Decision Clarity | Operational Confidence | Continuous Authorization | Actionable Response | Mission Resilience

WHAT DECISIONBEACON IS NOT

- Not a SIEM
- Not a SOAR
- Not a Vulnerability Scanner
- Not a GRC Replacement
- Not an eMASS Replacement
- Not a Compliance Dashboard
- Not a Ticketing System
- Not an Autonomous AI Agent
- Not Another Cyber Portal

DECISIONBEACON EXISTS TO ANSWER FOUR QUESTIONS.

1. What changed?
2. Why does it matter?
3. What decision is required?
4. What should happen next?

DecisionBeacon does not replace existing monitoring or governance tools.
It sits above them—correlating, contextualizing, validating, and prioritizing information to accelerate operational and authorization decisions.

ARLO
DECISIONBEACON

Partner With Us

We came to DAFITC to find mission partners. Three ways to engage:

01 **Pilot / cATO proof-of-concept** — stand up DecisionBeacon against a live system boundary.

02 **SBIR / OTA pathway** — a funded transition vehicle to mature and field the tool.

03 **eMASS integration** — map DecisionBeacon outputs directly into your authorization workflow.