Automated Evidence & Cryptographic Integrity

Achieving Data-Centric cAT0 across the CJADC2 Kill Web

BZESOE008?+j/|]3ctp+#B2BA月9AH6RInSt8AC1I-VINRCEA++-+FeMIARGEAoSNIQHEHeGA-FIIEAEKA...EUDA5j/12EcIn21

X02A36z7RE004Bcd4TABGA21Nhaa'635MbbzEZ+2c0d5QY28G£0b00GHT34d2y879EM8M2CND318RDBbhu0kJwQEJAMNE3c89SK20a1NDE4ePs7oqn38e:00Er

6306ATRPcdU6C=3.5886436923Ep03K753U4N_U1DTE])+1]//---

Travis Steele

Chief Architect & Field CTO - Defense, Red Hat

The Reality

Legacy paper-based RMF packages cannot scale to threats across distributed combat networks.

The Mandate

Continuous Authority to Operate (cATO) requires automated, cryptographically signed evidence instead of subjective checkboxes.

The Mission

Deliver tamper-evident, verifiable code integrity from enterprise software factories to the tactical edge.

Software as an Operational Vulnerability

Supply Chain Risk Across Distributed Kill Webs

Open-Source Reliance

98% & 9.8T

Modern tactical and C2 baselines rely heavily on open-source components. Unvetted upstream ingestion creates a large attack surface.

Emerging Attack Vectors

177K & $4.9M

Repository poisoning, dependency confusion, typosquatting, and malicious packages inject risk into build pipelines. Adversaries move faster than manual patch cycles.

Operational Consequences

75% Surge

Static baselines leave systems exposed in contested multi-domain environments.

Why Point-in-Time ATO Fails Modern Mission Delivery



The 12-18 Month Manual Cycle

Static System Security Plans (SSPs) are disconnected from live baselines. Accreditation reflects a historical moment, not current posture.



Machine-Speed cATO

Fear of re-accreditation freezes updates. Engineering effort must shift from generating paperwork to delivering capability.

Operationalizing Data-Centric cATO

Anchored to Official Dow Guidance

01. Continuous Monitoring

Near real-time visibility into system posture, configurations, and vulnerabilities.

02. Active Cyber Defense

Ability to detect, contain, and respond to threats at operational speed.

03. Secure Software Supply Chain

End-to-end provenance signed attestations, and verifiable build evidence from source through deployment.



Isolating Tactical Pipelines from Public Risk



Public Ingestion

(PyPI, npm, Maven, Crates, OCI)

Clearinghouse Buffer

(AI-assisted automated filtering, multi-engine vulnerability & malware triage, and validated signed remediation feeds)

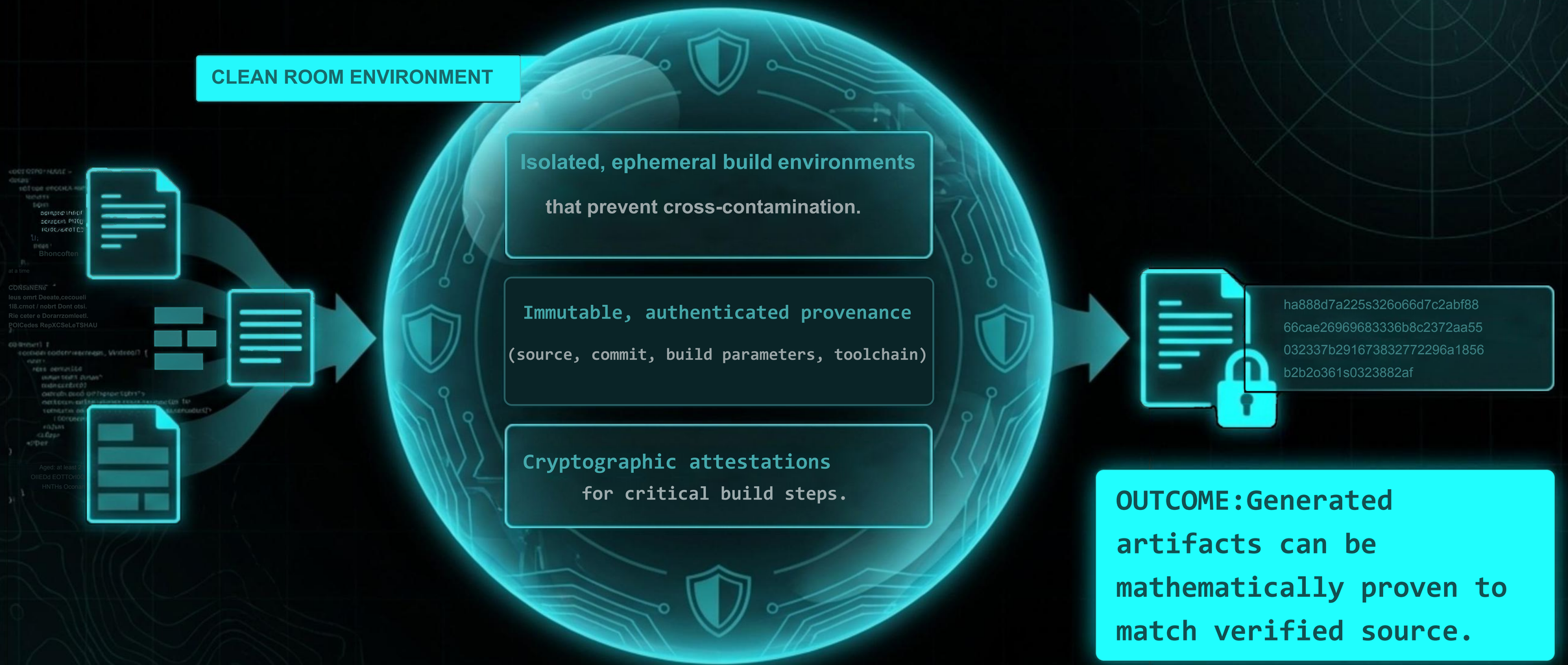
Curated Internal Registries

(that feed enterprise software factories)

STRATEGIC RULE: `Weapons systems software pipelines should never pull directly from unvetted public registries.`

Tamper-Resistant Build Pipelines

Supply Chain Integrity – SLSA Level 3



Cryptographic Proof of Integrity

Cryptographic Signing & Key Management



HSM-backed protection of root signing keys (FIPS-validated)

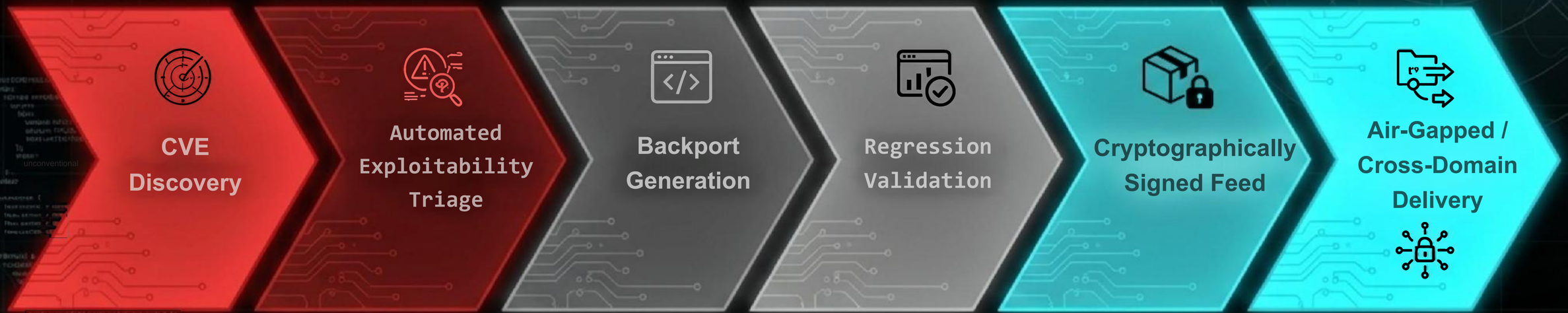
Support for keyless / short-lived signing tied to workload identity.

Hybrid classical + post-quantum dual signing now in practical early production use as the recommended transition approach for long-lifecycle systems facing Harvest Now, Decrypt Later (HNDL) risk.

Transparency logging of signing events.

Automated Embargo, Triage & Patch Distribution

Rapid Vulnerability Response



03:00:00

TARGET METRIC: Critical vulnerability isolation and patched feed delivery measured in hours while preserving platform stability.

Feeding Verified Content into Platform One and Iron Bank-Style Pipelines

Integration with Enterprise Software Factories



Pre-validated, continuously scanned base artifacts are injected into approved enterprise pipelines.

Downstream programs inherit scanning results, SBOMs, and hardening evidence.

Reciprocity reduces duplicated effort across the Department.

Preserving Provenance Across Domain Boundaries

Disconnected & Air-Gapped Synchronization

Staging

Mirror, sign, and package verified artifacts + SBOMs + attestations.



Transfer with signature and schema validation.

Disconnected Tactical Edge

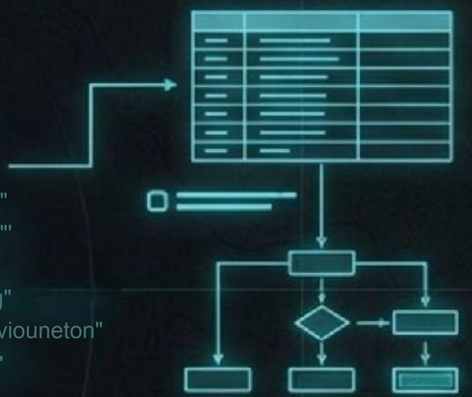
Air-gapped factory operates local registries and pipelines with no reach-back while retaining cryptographic chain of custody.

KEY TAKEAWAY: Provenance must survive the domain crossing.

From Static Documents to Automated Evidence

Machine-Readable Compliance





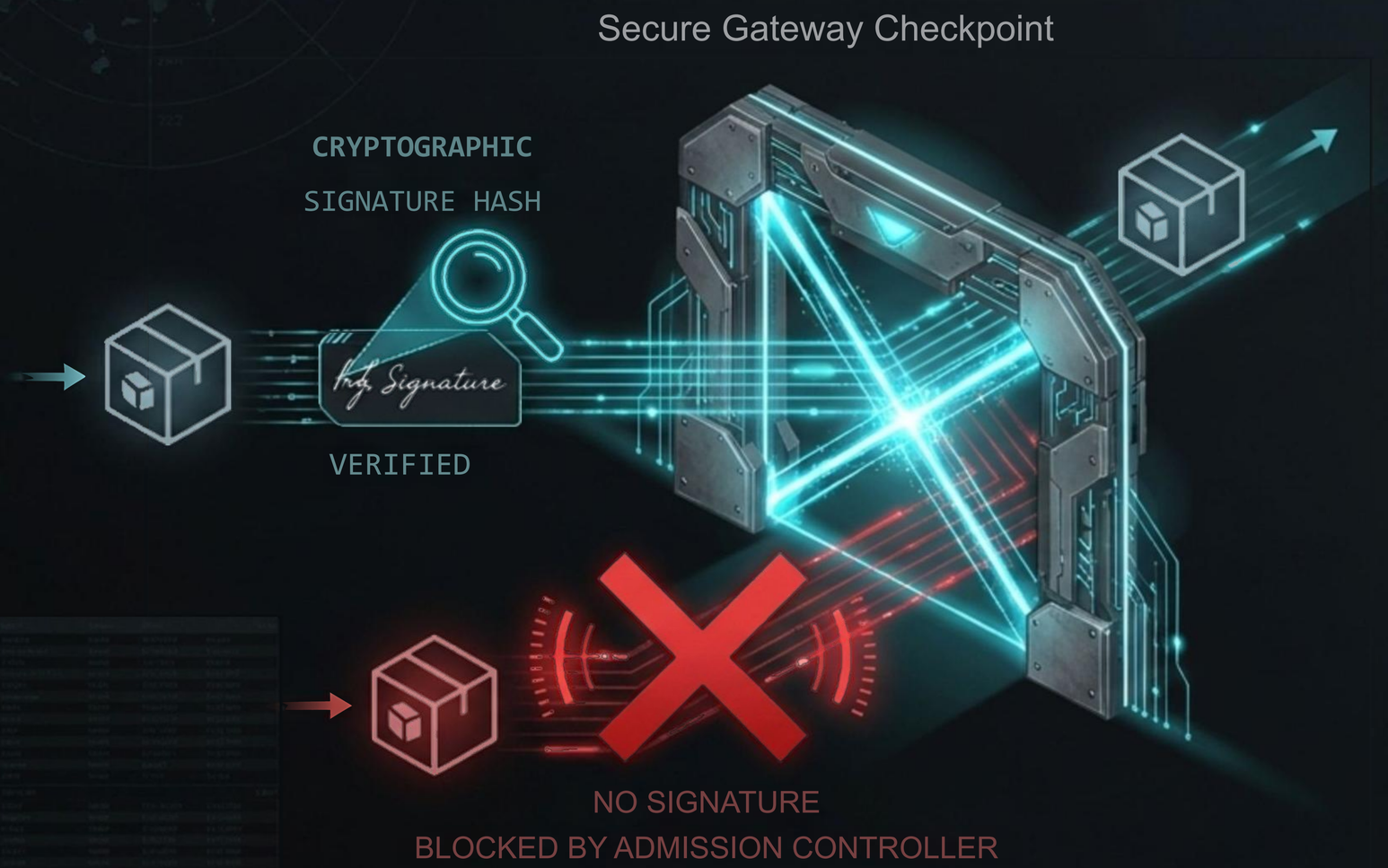
Comprehensive SBOM generation (CycloneDX / SPDX) at every layer.

Mapping of security controls into machine-readable formats (OSCAL and emerging continuous authorization standards).

Policy-as-code enforcement at admission time.

Continuous Enforcement at the Tactical Edge

Zero-Trust Runtime Protection



Admission control that rejects unsigned or insufficiently attested images.

Mutual TLS and strong workload identity for service-to-service communication.

Runtime visibility and anomaly detection for process, memory, and network deviation.

What Authorizing Officials and Program Offices Gain

Operational Impact Metrics

	Traditional ATO	Data-Centric cATO
Update Frequency	12-18 month manual cycles.	Continuous delivery via CI/CD pipelines.
Evidence Type	Subjective self-attestation.	Unforgeable cryptographic attestations.
Security Posture	Point-in-time historical snapshot.	Real-time active defense and monitoring.
Engineering Focus	Generating compliance paperwork.	Delivering war-winning capabilities.

- Continuous, evidence-based accreditation
- Source-to-runtime cryptographic provenance
- Critical vulnerability response in hours
- Policy-enforced rejection of unsigned artifacts

Practical Path to Continuous Authorization

Phased Adoption Roadmap

Phase 1(Months 1-3)

Curated registries, block direct public pulls, mandate SBOM generation.

Phase 2(Months 4-6)

SLSA Level 3 build practices, cryptographic signing (including hybrid post-quantum), machine-readable control mapping.

Phase 3 (Months 7+)

Admission gates, continuous runtime monitoring, real-time visibility for Authorizing Officials.

Principles for Defense Program Leadership

Strategic Takeaways



Evidence over documentation

Continuous authority requires automated, cryptographically verifiable proof from source to deployment.



Buffer the supply chain

A controlled clearinghouse and rapid signed remediation protect weapon system pipelines from public risk.



Mission-speed delivery

Strong integrity controls enable faster, safer delivery of capability to the warfighter.

Q & A