



An AI-Assisted Framework for Post-Quantum Cryptography Bill Of Materials (CBOM) Discovery

Paper Presentation

Varun Grover • Prachi Gupta • Debasish Deb • Padmalav Sahoo
Wipro Innovation Network

CHALLENGE

URGENCY

REQUIREMENTS

AI ASSISTED FRAMEWORK

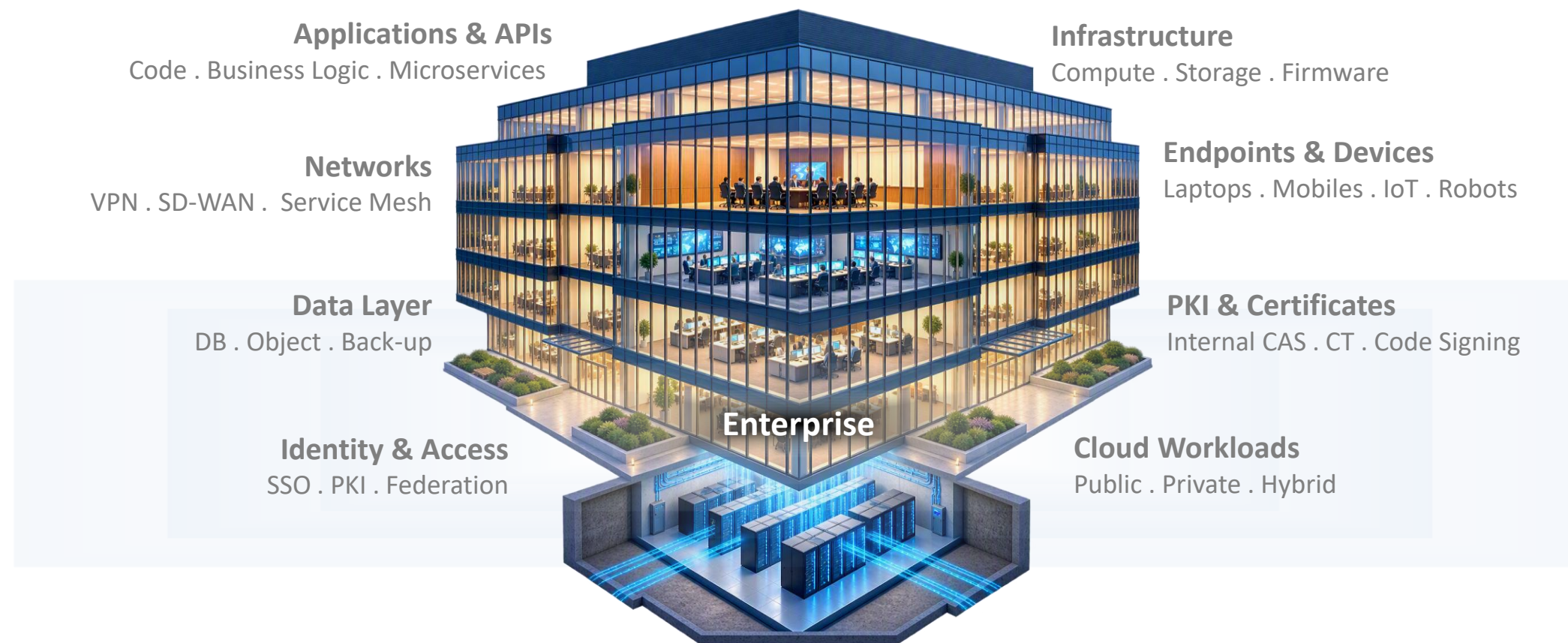
MEASUREMENT MATRICS

ADOPTION

WE KNOW WE NEED TO ADOPT POST-QUANTUM CRYPTOGRAPHY

but HOW ? what & where ?

Enterprise Today = Digital (Crypto-Guarded)



rarely visible in one inventory | almost no enterprise can list it with confidence

“ YOU CANNOT MIGRATE WHAT YOU CANNOT SEE !! ”

CHALLENGE

URGENCY

REQUIREMENTS

AI ASSISTED FRAMEWORK

MEASUREMENT MATRICS

ADOPTION

Mosca's inequality has turned quantum uncertainty into a readiness test

MOSCA'S
INEQUALITY:

$$X + Y > Z \rightarrow \text{asset is exposed}$$

X = secrecy or trust lifetime Y = migration time Z = years until CRQC



COMPLIANCE

Technology standards & **regulatory mandates** are set

- ML-KEM, ML-DSA, SLH-DSA finalized (Aug 2024)
- CNSA 2.0 mandates migration by 2033
- OMB M-23-02 & CERT-In v2 require cryptographic inventories



TIMELINE

Risk window accelerated as CRQC forecasts continue to move closer

- Timeline compressed - Shifted from a distant 2035+ window to as early as 2028–2029.
- Qubit threshold slashed - Physical qubit requirements dropped from 20 Mn to under 1 Mn due to better error correction.



EVOLVING AI

AI challenges cryptographic assumptions

- AI accelerates cryptanalysis and vulnerability discovery
- Emerging algorithms can fail much faster
- Crypto-agility becomes essential



THREATS

Adversary Threats are **active across time** (Today + Q-Day)

- HNDL (Harvest Now, Decrypt Later)
- TNFL (Trust Now, Forge Later)
- Long-lived data and trust assets already exposed
- Q-Day



NEW ATTACK VECTORS

Migration introduces **new risks**

- Hybrid downgrade attacks
- Supply-chain manipulation
- Algorithm substitution attacks

Compliance + Timeline + AI + Threats + Attack Surface = Need for Cryptographic Visibility

CHALLENGE

URGENCY

REQUIREMENTS

AI ASSISTED FRAMEWORK

MEASUREMENT MATRICS

ADOPTION

ENTERPRISE NEEDS

Complex Cryptography Inventory Dimensions



Algorithm inventory: Every algorithm across code, PKI, network, data, signing

Code-layer usage: User vs. provider methods at each tech layer

Structural dependency: In-house, vendor, licensed tools, devices

Business mapping: Which functions and services each asset serves

Time relevance: Secrecy and trust lifetime vs. exposure risk

Threat & vector exposure: Adversary threats today vs. Q-Day; new attack vectors

MULTIPLE DIMENSIONS, ONE DEPENDENCY GRAPH — VISIBILITY FAILS IF ANY DIMENSION IS MISSING.

Cryptography Bill of Material (CBOM) Framework

CycloneDX as foundation model

- convert cryptography into a machine-readable template

Algorithms

RSA · AES · ML-KEM

Protocols

TLS · SSH · IPsec

Certificates

issuer · validity · sigAlg

Key material

state · context · attestation

Implementations

OpenSSL · HSM firmware

Usage sites

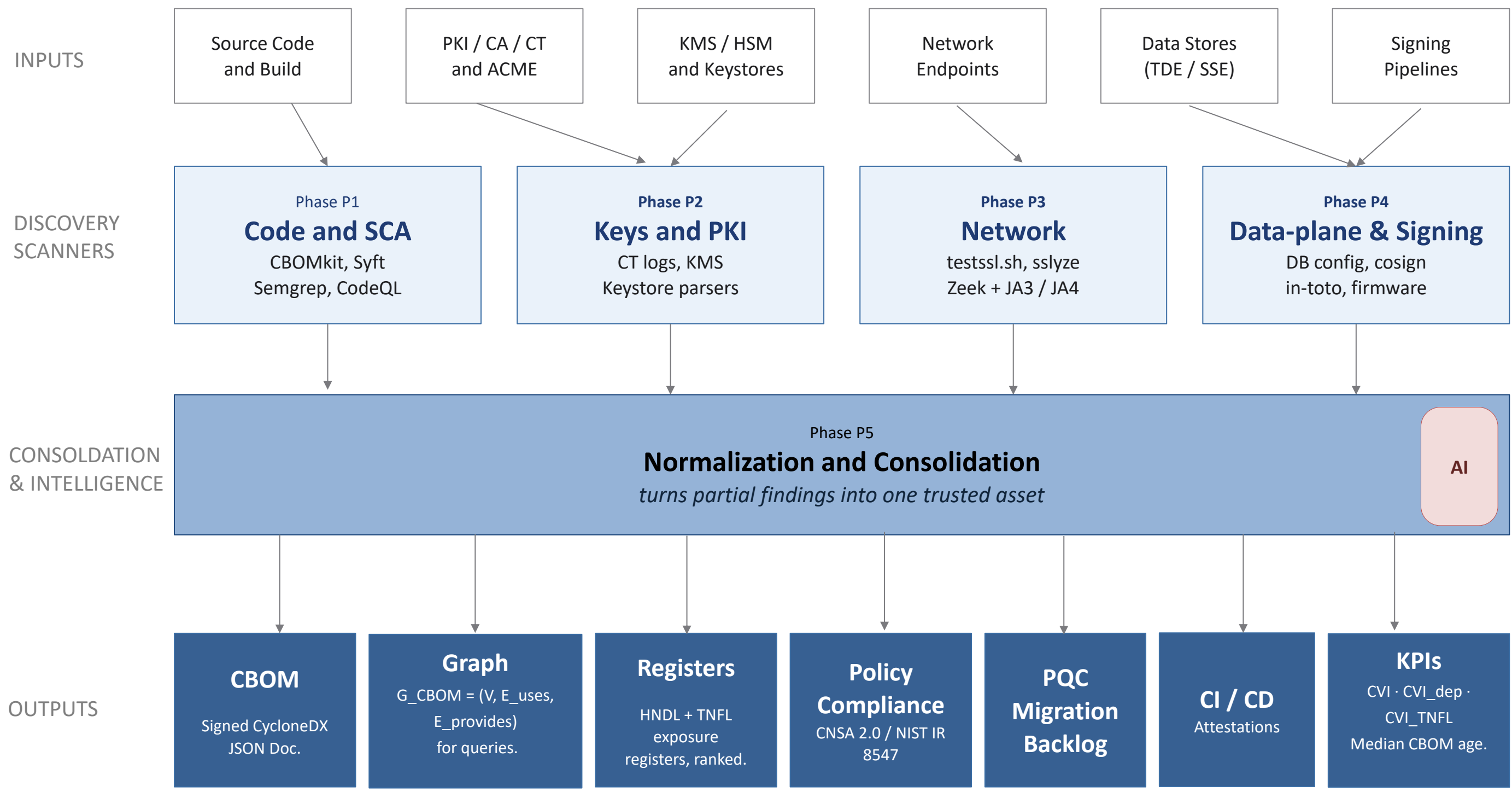
apps · services · devices

SBOM - Dependency Graph Tracking

- align migration needs regarding cryptographic assets and dependencies



Multi-Layer CBOM Discovery Pipeline with AI-Assisted Module



AI-ASSISTED MODULE

AI closes blind spots, but does not replace scanners

- **LLM static analysis**
Find obfuscated, manually implemented and runtime-selected cryptography that signature-based scanners miss.
- **TLS fingerprint embeddings**
Infer likely protocol assets where active probing is restricted by projecting JA3/JA4 observations into an embedding space.
- **Cross-source linking**
Link the same certificate or key across PKI, secrets, endpoints and downstream artefacts to improve TNFL lineage.

Open-Weight AI models v/s API

- Data sovereignty
- Cost + latency
- Safety Guardrails

CHALLENGE

URGENCY

REQUIREMENTS

AI ASSISTED FRAMEWORK

MEASUREMENT MATRICS

ADOPTION

Coverage measurement metrics

makes “we scanned the estate” reproducible

Report recall together with precision and F1 so that higher coverage does not hide noisy or duplicated findings.



Cryptography Visibility Index

Asset recall

$$\text{CVI} = \frac{\text{discovered} \cap \text{ground truth}}{\text{ground truth}}$$

Fraction of ground-truth assets the pipeline finds.
The headline metric for discovery completeness.



Precision

$$\text{Precision} = \frac{\text{discovered} \cap \text{ground truth}}{\text{discovered}}$$

Fraction of discovered assets that are real.
Counters AI-module hallucination and false positives.



F1 score

Quality balance

$$\text{F1} = \frac{2 * \text{CVI} * \text{Precision}}{\text{CVI} + \text{Precision}}$$

Harmonic mean. Balances recall-vs-precision trade-off.
Used for cross-pipeline benchmarking.

Variants: CVI_dep (uses/provides edge recall) | CVI_TNFL (long-trust signing-key recall) -- both required for migration impact analysis

ground truth = set of known cryptographic assets in scope | discovered = set discovered assets by the pipeline

CHALLENGE

URGENCY

REQUIREMENTS

AI ASSISTED FRAMEWORK

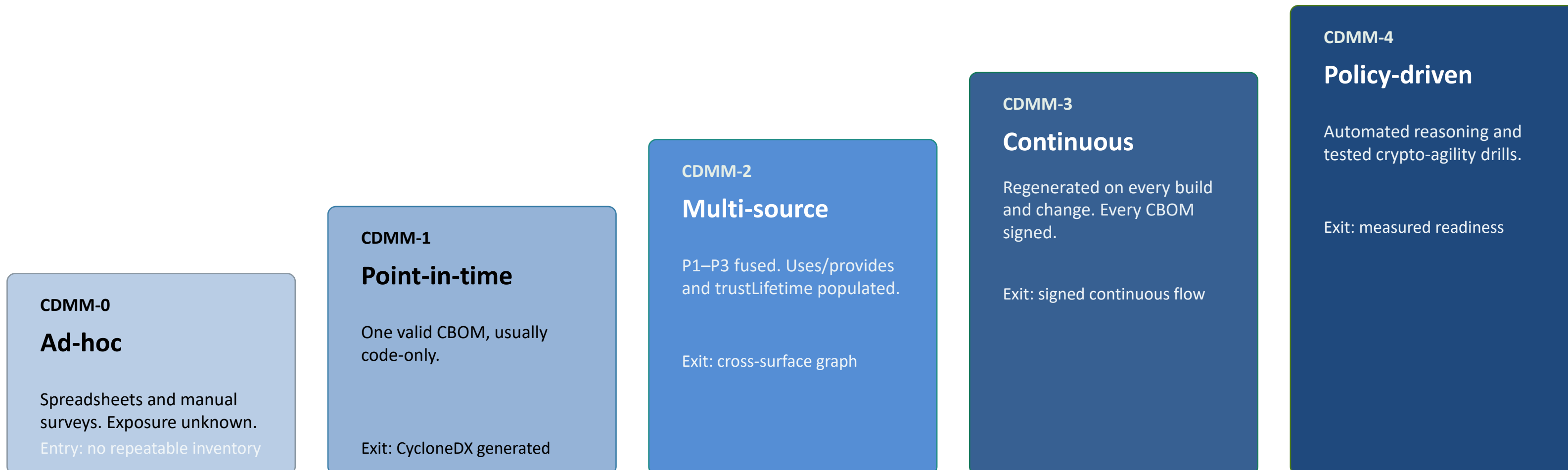
MEASUREMENT MATRICS

ADOPTION

Cryptography Discovery Maturity Model - CDMM

turns the framework into an enterprise capability

CVI proves what the pipeline finds; CDMM shows how the organization operationalizes it.



Each level shortens the time between a cryptographic change happening and the CBOM knowing about it.

Lower discovery latency → smaller Y → lower HNDL and TNFL exposure

Key Contributions

Multi-layer CBOM discovery framework

Aligns CycloneDX 1.6 asset and dependency semantics with five enterprise discovery surfaces (P0-P4 + P5 fusion).

AI-assisted module

LLM classifier + JA4 fingerprint embeddings + sentence-transformer cross-source linking; recovers obfuscated and non-API crypto.

Crypto Visibility Index (CVI)

Reproducible coverage metric with HNDL- and TNFL-specific variants; supports precision/F1 reporting per asset type.

CBOM Discovery Maturity Model (CDMM)

Five levels CDMM-0..4; entry/exit criteria, KPIs, and tooling support per level.

Explicit threat model

Four adversary classes; six attack classes including HNDL, TNFL, store-now-forge-later docs, hybrid downgrade, agility upgrade-path, and ASA.

Concrete artefacts

CycloneDX 1.6 emission, consolidation algorithm, architecture asset dependency, existing cbom tool comparison

An AI-assisted Framework for Post-Quantum Cryptography Bill Of Materials (CBOM) Discovery



THANK YOU

An AI-assisted Framework for Post-Quantum Cryptography Bill Of Materials (CBOM) Discovery

Varun Grover • Prachi Gupta • Debasish Deb • Padmalav Sahoo

Wipro Innovation Network