SecurityBoat Community

Connect, Learn & Grow!!

Seeing the Hidden Crypto: Why CBOM Matters Now

SecurityBoat Community
Connect, Learn & Grow!!

About Me

Shyam Kumar Arshid
Cybersecurity researcher

Works at an International bank

14 years of professional experience

Previous org: Siemens, NTRO & ISRO

LinkedIn: www.linkedin.com/in/shyam-kumar-arshid

Cryptographic Bill of Materials (CBOM)

SecurityBoat Community
Connect, Learn & Grow!!

- Cryptography is everywhere
- But often invisible
- PQC makes that a problem
- CBOM makes it visible

Why should we care?

SecurityBoat Community
Connect, Learn & Grow!!

- Where are we using RSA, ECC, SHA-1, TLS ciphers?
- Which systems depend on them?
- Which ones are quantum-vulnerable?
- What breaks if we change them?

BOM → SBOM → CBOM

SecurityBoat Community
Connect, Learn & Grow!!

- BOM: what parts make up a product
- SBOM: what software components are inside
- CBOM: what cryptography is inside

SBOM sees software, not crypto intent

SecurityBoat Community
Connect, Learn & Grow!!

Why CBOM matters now

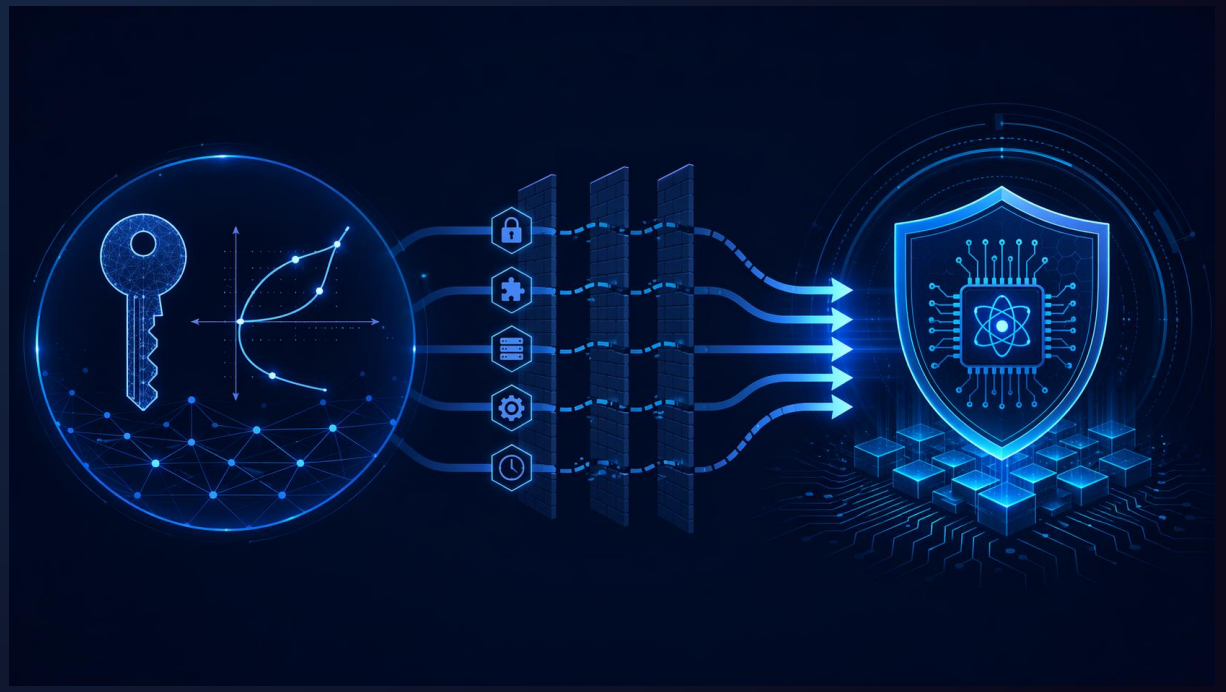
SecurityBoat Community
Connect, Learn & Grow!!

- Weak / legacy crypto still exists
- Crypto agility is becoming necessary
- PQC migration starts with discovery
- Regulation is pushing inventory and planning

PQC changes the question

SecurityBoat Community
Connect, Learn & Grow!!

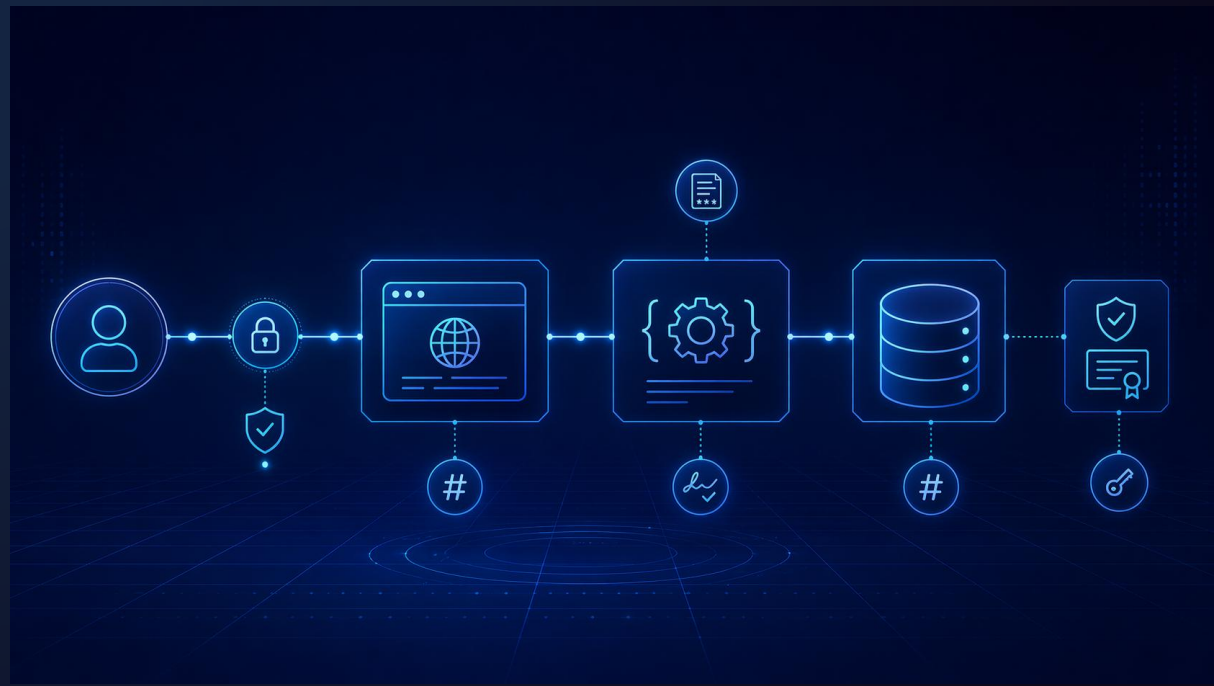
- Not: Do we use cryptography?
- But: Where do we use vulnerable public-key crypto?
- And: How hard is it to replace?
- Discovery becomes the first migration step



Example: one application, many crypto dependencies

SecurityBoat Community
Connect, Learn & Grow!!

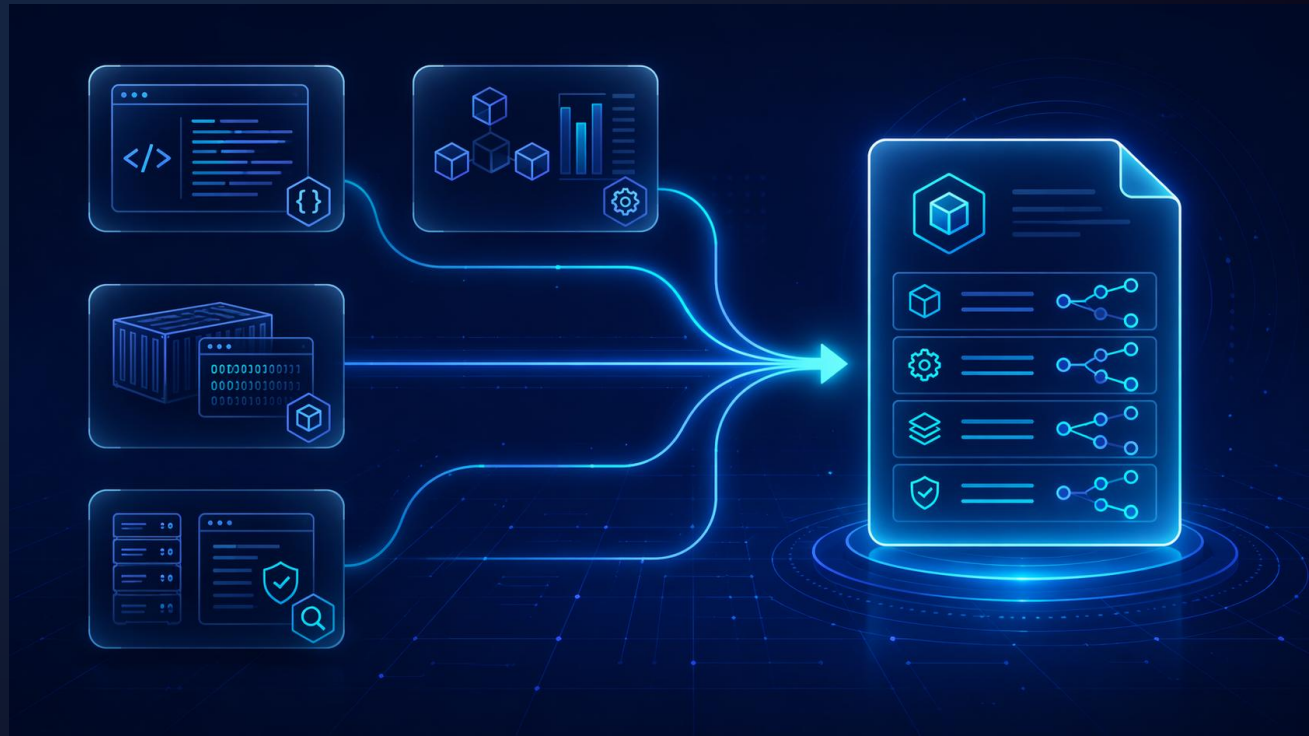
- Web app uses TLS
- Backend signs tokens
- Library performs hashing
- Certificate chain anchors trust
- Container may include extra crypto libraries



Discovery comes from multiple places

SecurityBoat Community
Connect, Learn & Grow!!

- Source code scanning
- Binary/executables scanning
- Network traffic
- Filesystem and Containers



How can we generate CBOMs today?

SecurityBoat Community
Connect, Learn & Grow!!

Open source tools

1. CBOMkit
2. CodeQL

Demo

Where the ecosystem is heading

SecurityBoat Community
Connect, Learn & Grow!!

- Inventory of cryptographic systems is now expected
- PQC migration guidance stresses discovery
- Standards are moving toward machine-readable structure
- NIST, OMB, ETSI, NCSC, ENISA
- From India: CERT-In

Final takeaway

SecurityBoat Community
Connect, Learn & Grow!!

- You cannot migrate what you cannot see
- You cannot enforce what you cannot describe
- Visibility enables agility
- Agility enables PQC readiness

SecurityBoat Community

Connect, Learn & Grow!!

Questions?

SecurityBoat Community

Connect, Learn & Grow!!

Thank You!