CycloneDX

AI/ML Bill of Materials

Model and dataset transparency for security, privacy, safety, and ethical considerations

OWASP

OWASP FOUNDATION

®

Steve Springett

- Leader of OWASP Dependency-track
- Chair, OWASP CycloneDX Core WG
- Chair, Ecma Technical Committee 54
- Leader and co-author of OWASP SCVS
- Leader of Package URL standard
- OWASP Global Board of Directors
- Director, Product Security at ServiceNow

@stevespringett

@stevespringett

steve.springett@owasp.org

CycloneDX is a Full Stack BOM Standard

Provides advanced supply chain capabilities for cyber risk reduction

Community Driven

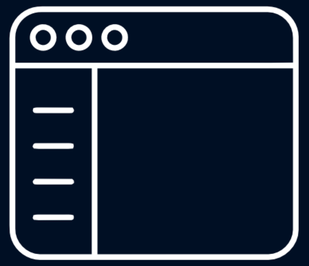
Standardization Through

In Production! At an estimated 100K organizations

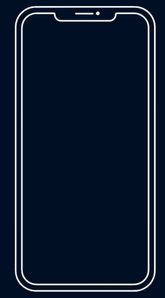
Over 500M components represented monthly

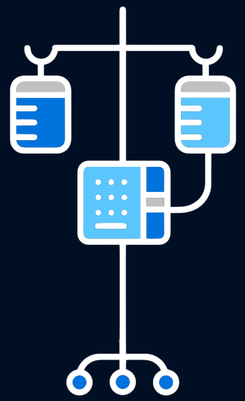
Source: Sonatype
One tool using a single source of vulnerability intelligence
Actual usage much greater

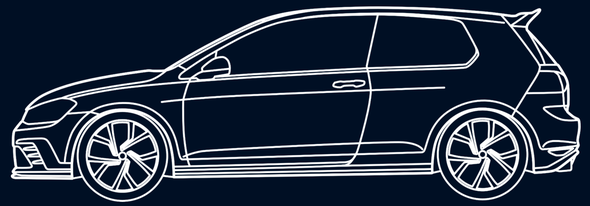
Vendor & Project Support

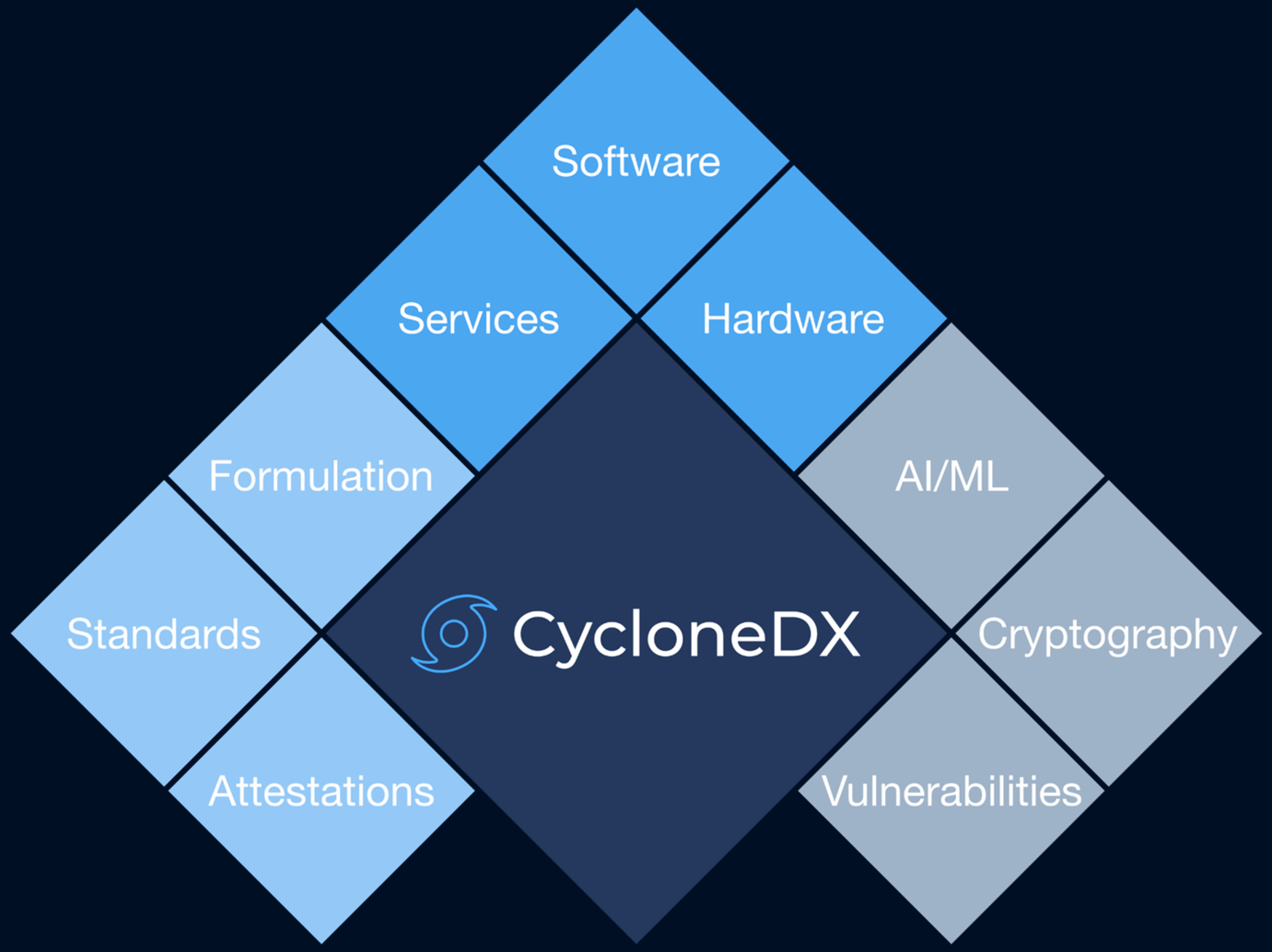


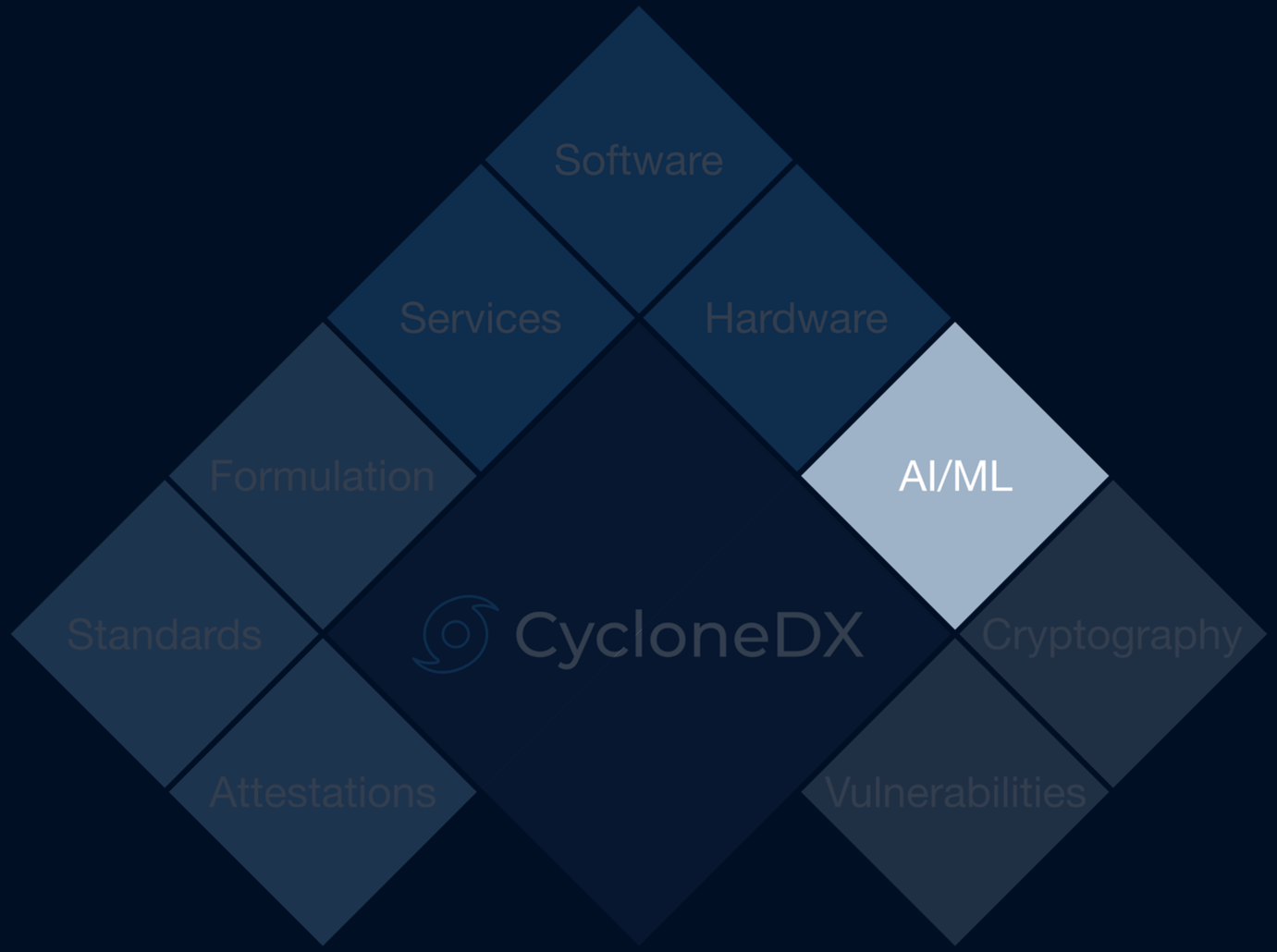

SaaS

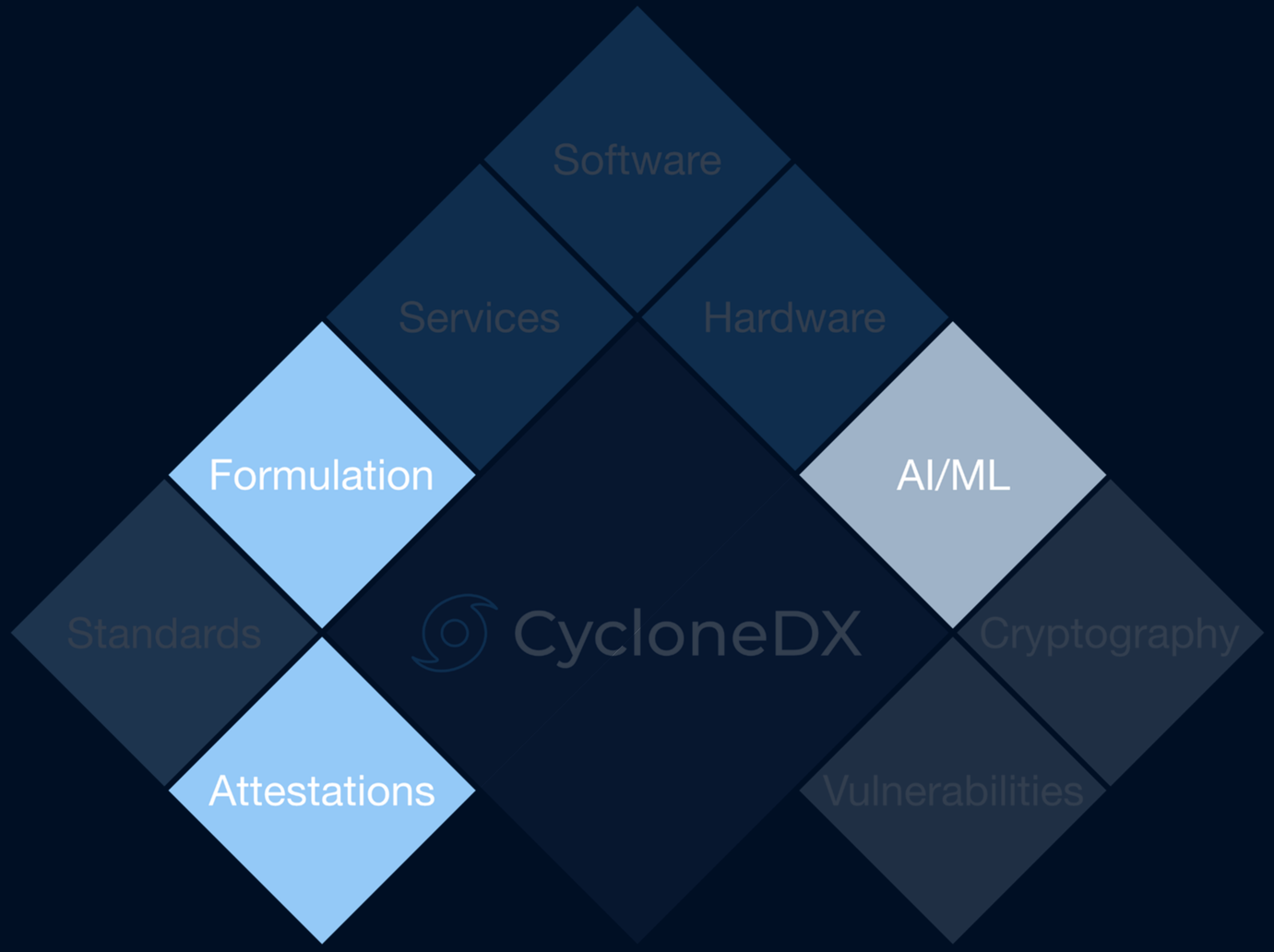







Software
Services
Hardware
Formulation
AI/ML
Standards
CycloneDX
Cryptography
Attestations
Vulnerabilities


Software
Services
Hardware
Formulation
AI/ML
Standards
CycloneDX
Cryptography
Attestations
Vulnerabilities


Software
Services
Hardware
Formulation
AI/ML
Standards
CycloneDX
Cryptography
Attestations
Vulnerabilities

CycloneDX Unified Model Cards

Inherits from the CycloneDX component model

- Provenance: supplier, author, publisher, manufacturer
- Identity: PURL, CPE, SWID, OmniBOR, SWHID, coordinates
- Licenses (open source and commercial) and copyrights
- Pedigree (ancestors, descendants, variants)
- External references (relationships and documentation)
- Release notes

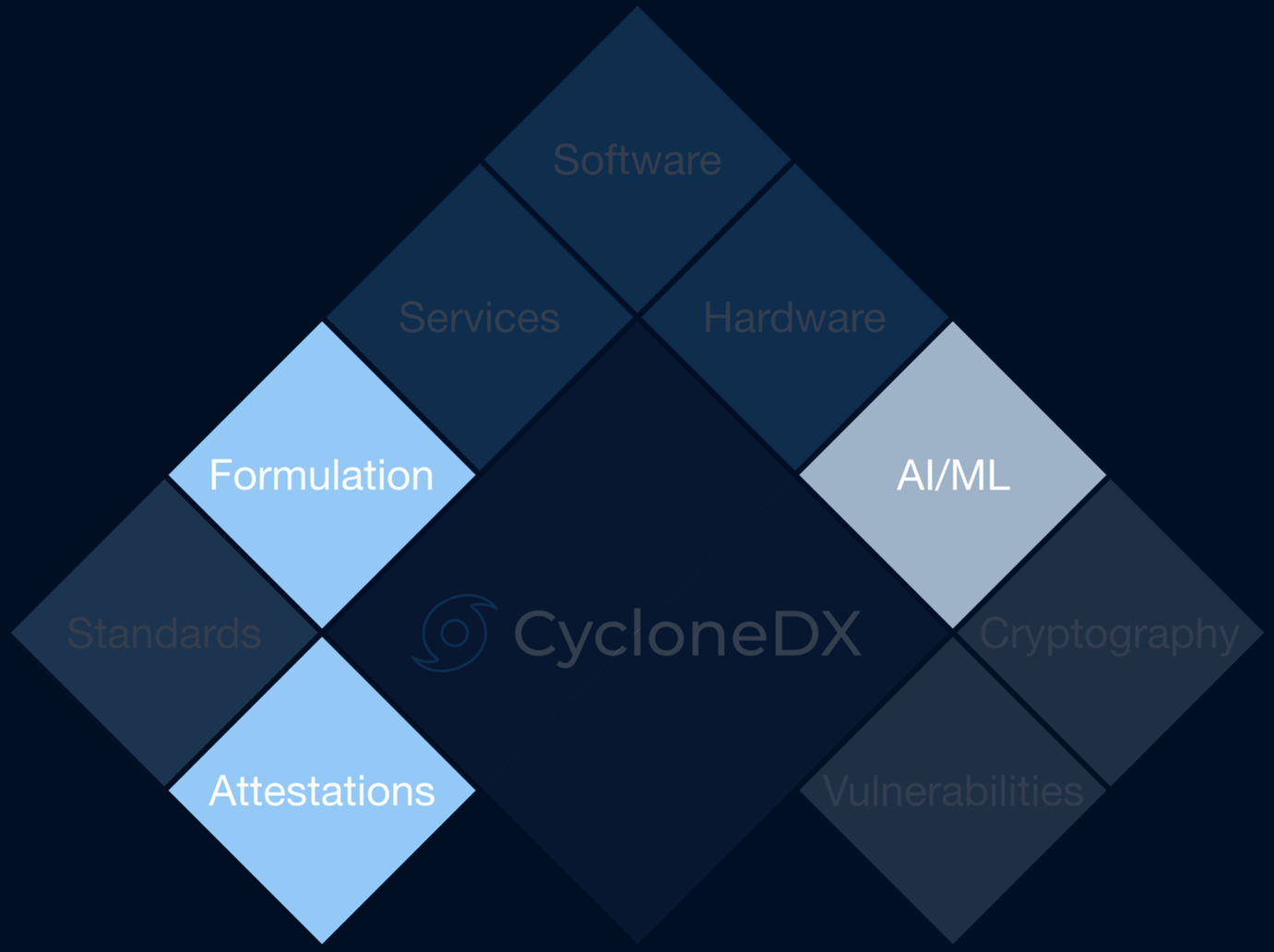
CycloneDX Unified Model Cards

Model Parameters	Approach Type	Task	Architecture Family
	Model Architecture	Datasets	I/O Formats
Quantitative Analysis	Performance Metrics	Graphics	
Considerations	Users	Use Cases	Technical Limitations
	Ethical	Environmental	Fairness

Perf Tradeoffs

CycloneDX

OWASP


Software
Services
Hardware
Formulation
AI/ML
Standards
CycloneDX
Cryptography
Attestations
Vulnerabilities

Proposed Enhancements for CycloneDX v1.7

Proposed Enhancements for CycloneDX v1.7

- Blueprints
- OTM → TM-BOM
- Sustainability