2024 North America Community Meeting

You Dropped a BOM on Me, Baby

PCI Security Standards Council

PCI Security Standards Council

Jake Marcinko

Senior Manager, Solution Standards
PCI Security Standards Council

PCI Security Standards Council®

```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: spdx-sbom-generator
DocumentNamespace: http://spdx.org/spdxpackages/spdx-sbom-generator--57918521-3212-4369-a8ed-3d681ec1d7a1
Creator: Tool: spdx-sbom-generator-XXXXX
Created: 2021-05-23 11:25:29.1672276 -0400 -04 m=+0.538283001

##### Package representing the Go distribution

PackageName: go
SPDXID: SPDXRef-Package-go
PackageVersion: v0.46.3
PackageSupplier: NOASSERTION
PackageDownloadLocation: pkg:golang/cloud.google.com/go@v0.46.3
FilesAnalyzed: false
PackageChecksum: TEST: SHA-1 224ffa55932c22cef869e85aa33e2ada43f0fb8d
PackageHomePage: pkg:golang/cloud.google.com/go@v0.46.3
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageLicenseComments: NOASSERTION
PackageComment: NOASSERTION

Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-go

##### Package representing the Bigquery Distribution

PackageName: bigquery
SPDXID: SPDXRef-Package-bigquery
PackageVersion: v1.0.1
PackageSupplier: NOASSERTION
PackageDownloadLocation: pkg:golang/cloud.google.com/go/bigquery@v1.0.1
FilesAnalyzed: false
PackageChecksum: TEST: SHA-1 8168e852b675afc9a63b502feeefac90944a5a2a
PackageHomePage: pkg:golang/cloud.google.com/go/bigquery@v1.0.1
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: NOASSERTION
PackageCopyrightText: NOASSERTION
PackageLicenseComments: NOASSERTION
PackageComment: NOASSERTION

Relationship: SPDXRef-Package-go CONTAINS SPDXRef-Package-bigquery
```

MAY 12, 2021

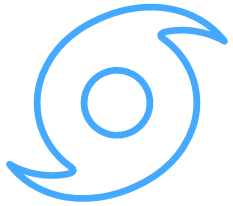
Executive Order on Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Security Requirements

Control Objectives	Test Requirements	Guidance
Control Objective C.1: Web Software Components & Services All components and services used by the software are identified and maintained in a manner that minimizes the exposure of vulnerabilities.		
C.1.1 All software components and services are documented or otherwise cataloged in a software bill of materials (SBOM).	**C.1.1** The assessor shall examine evidence to confirm that information is maintained that describes all software components and services comprising the software solution, including: • All proprietary software libraries, packages, modules, and/or code packaged in a manner that enables them to be tracked as a freestanding unit of software. • All third-party and open-source frameworks, libraries, and code embedded in or used by the software during operation. • All third-party software dependencies, APIs, and services called by the software during operation.	Modern software is rarely created entirely in-house and is typically composed of various bespoke code segments integrated with numerous components such as commercial and/or open-source frameworks, libraries, APIs, and services. Any part of this code may have or develop vulnerabilities over time that will require patching or mitigation. Knowing all of the components that comprise a software application or service, where they come from, and how they are updated and maintained is critical to minimizing and managing vulnerabilities in software applications. Without this information, it would be extremely difficult to identify and track vulnerabilities in software components that could expose the embedding software application to attacks. A Software Bill of Materials or "SBOM" services this purpose by documenting information about the software components and versions used to create a software product, their suppliers, and any third-party code that may also be embedded in these components. NIST refers to this information as "provenance data" and there are numerous standards and frameworks available, such as CycloneDX, SPDX and SWID, that describe how this information should be structured. For more information, refer to those standards and frameworks.

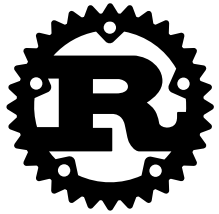


CycloneDX

PCI Security Standards Council


.NET


Maven




node
JS


Java


python


GO


CDXGEN

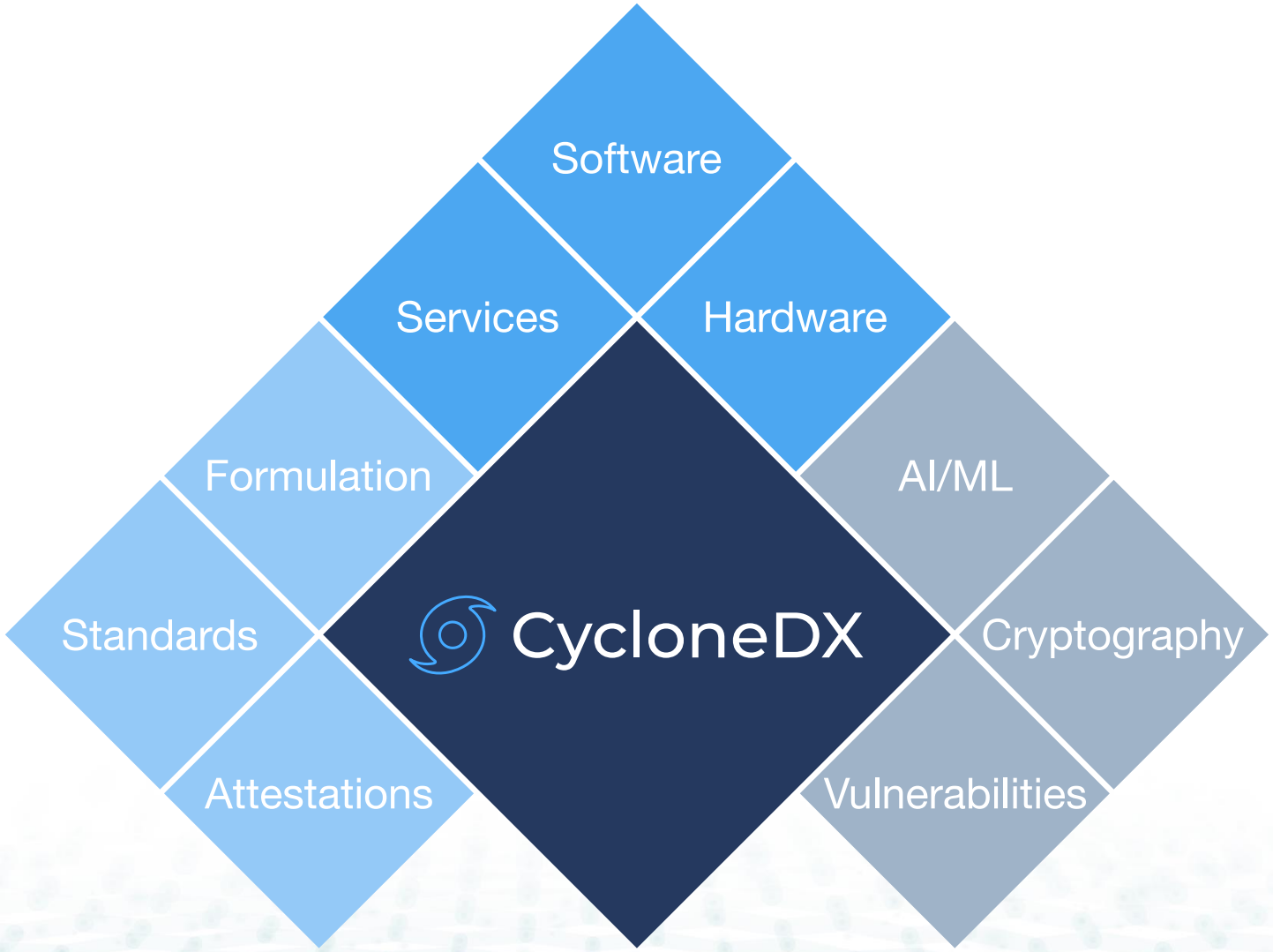

dependency track


Bitbucket

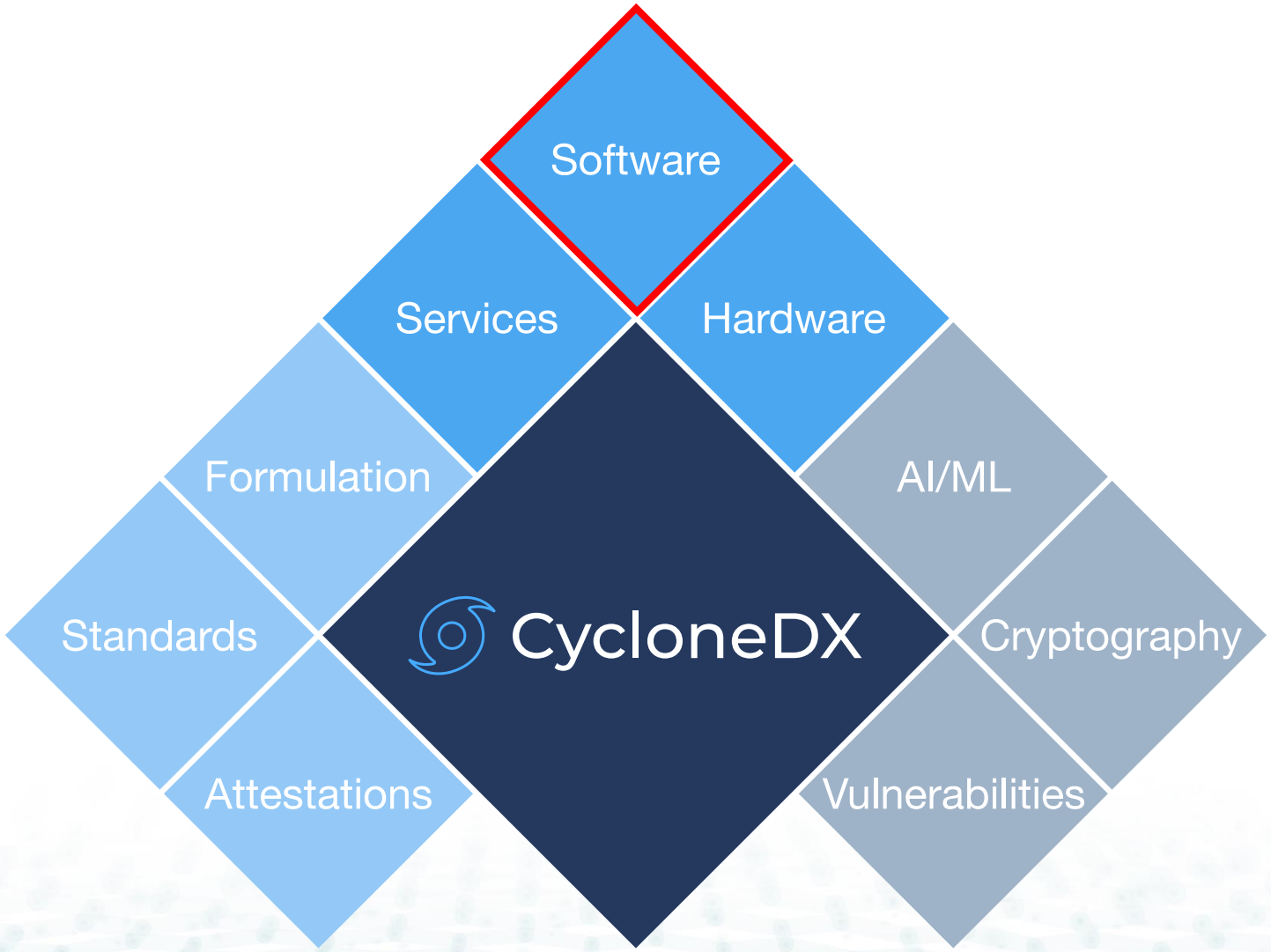

php


PCI
Security
Standards Council

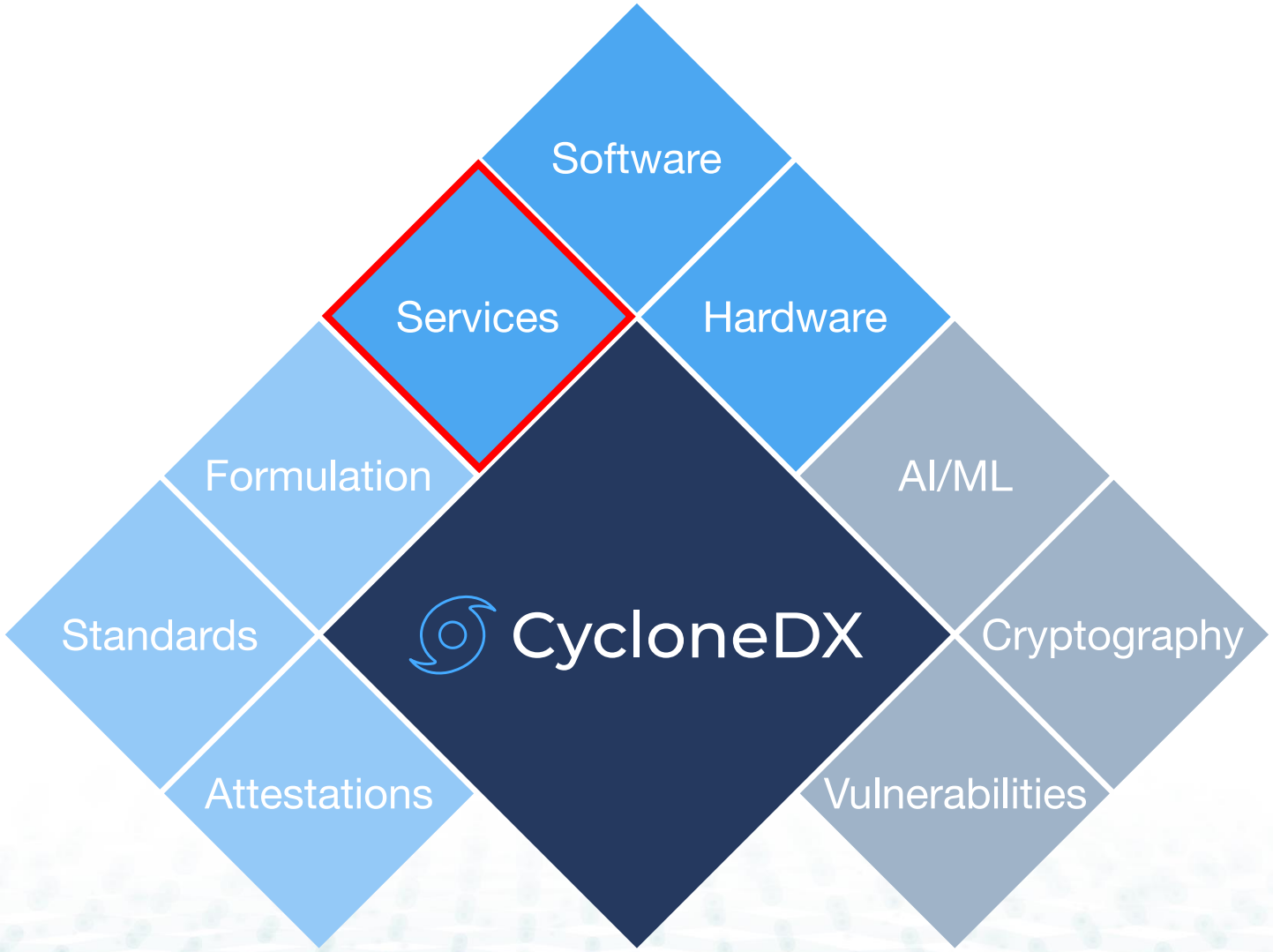
PCI Security Standards Council®



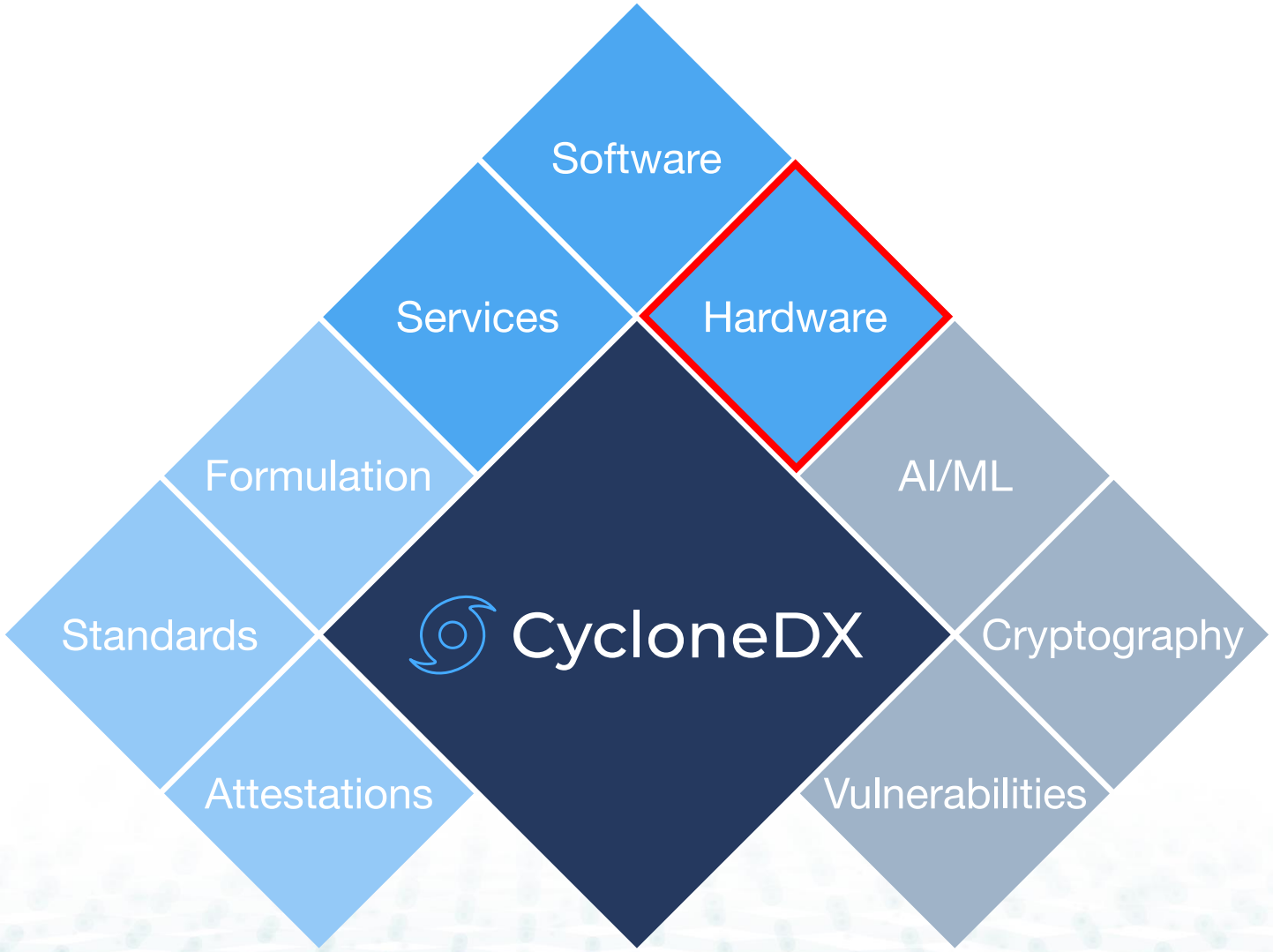
PCI Security Standards Council®



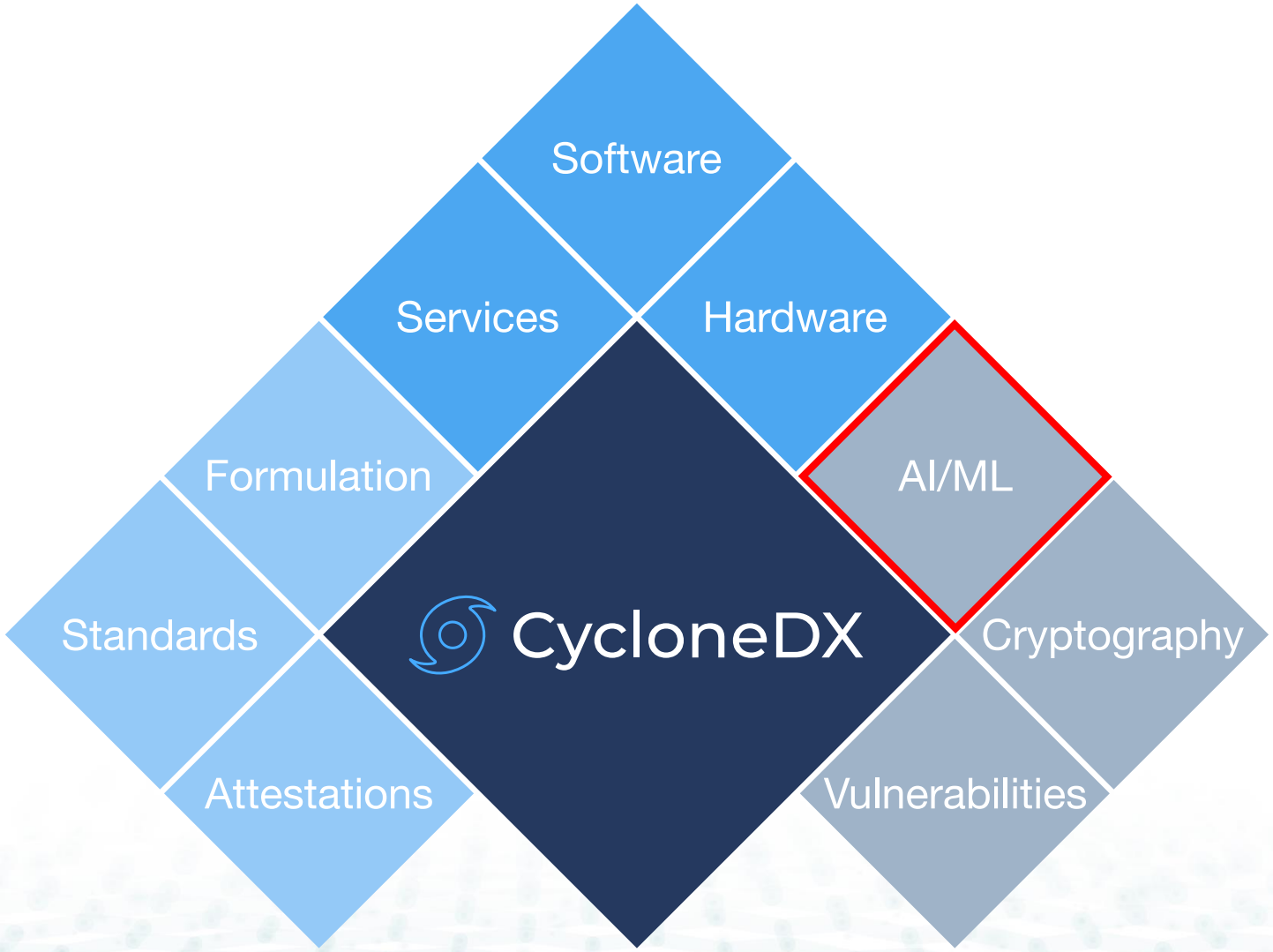
PCI Security Standards Council®



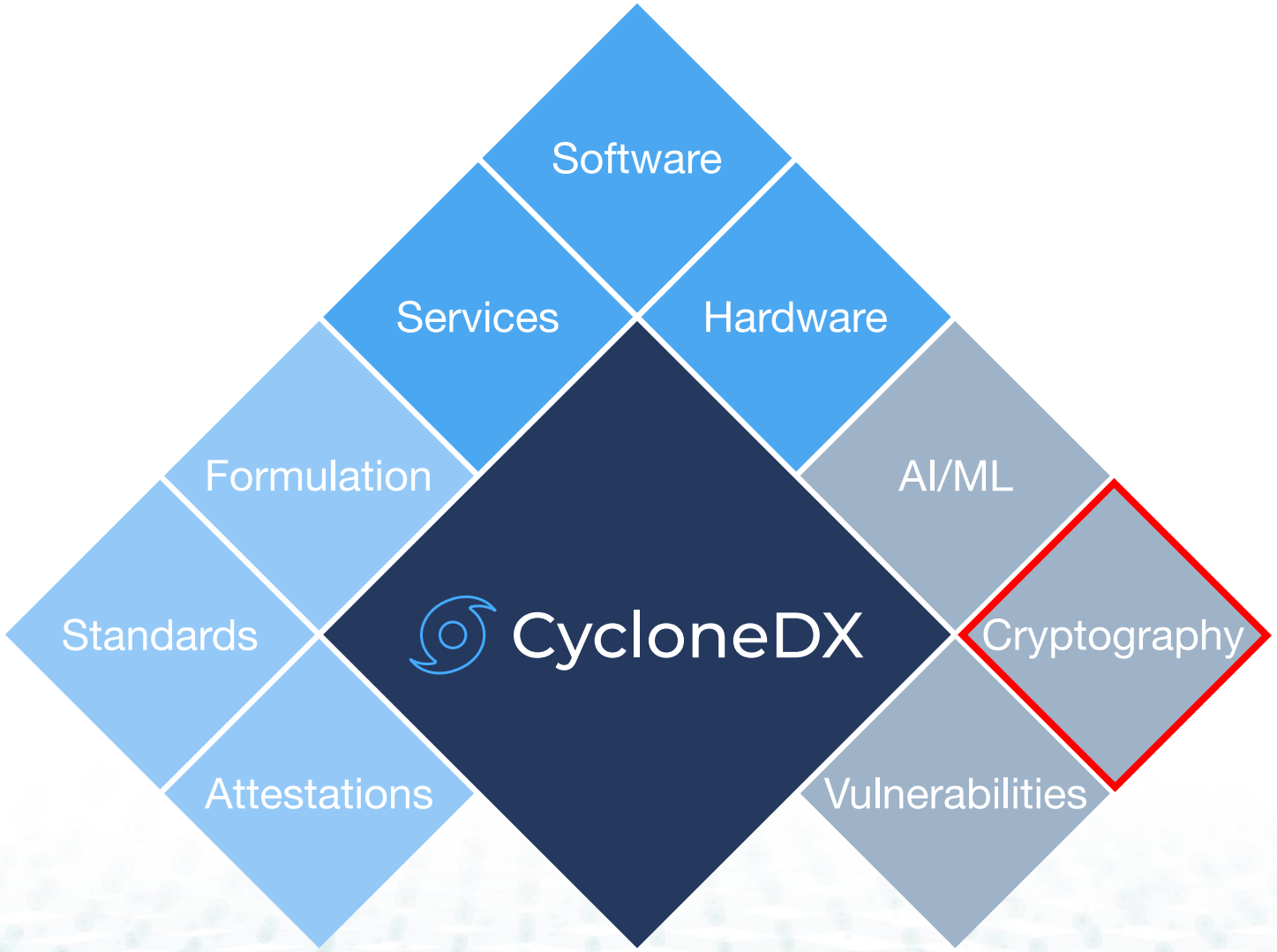
PCI Security Standards Council



PCI Security Standards Council



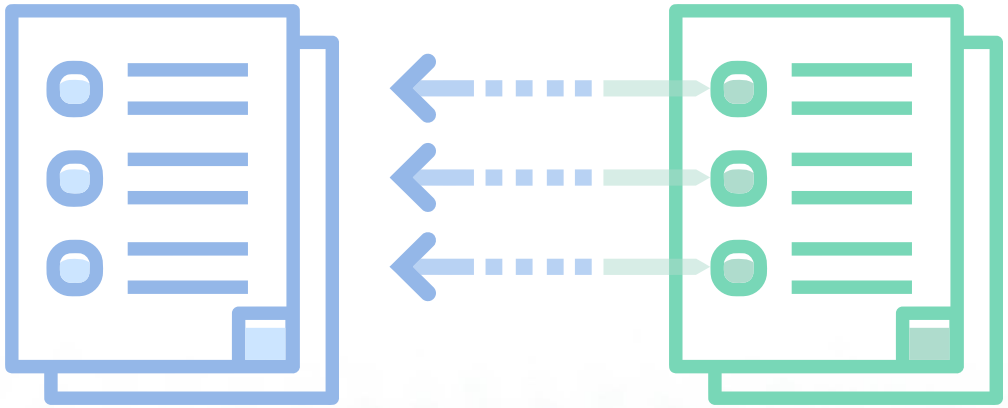
PCI Security Standards Council



PCI Security Standards Council

SBOM
+
SaaSBOM

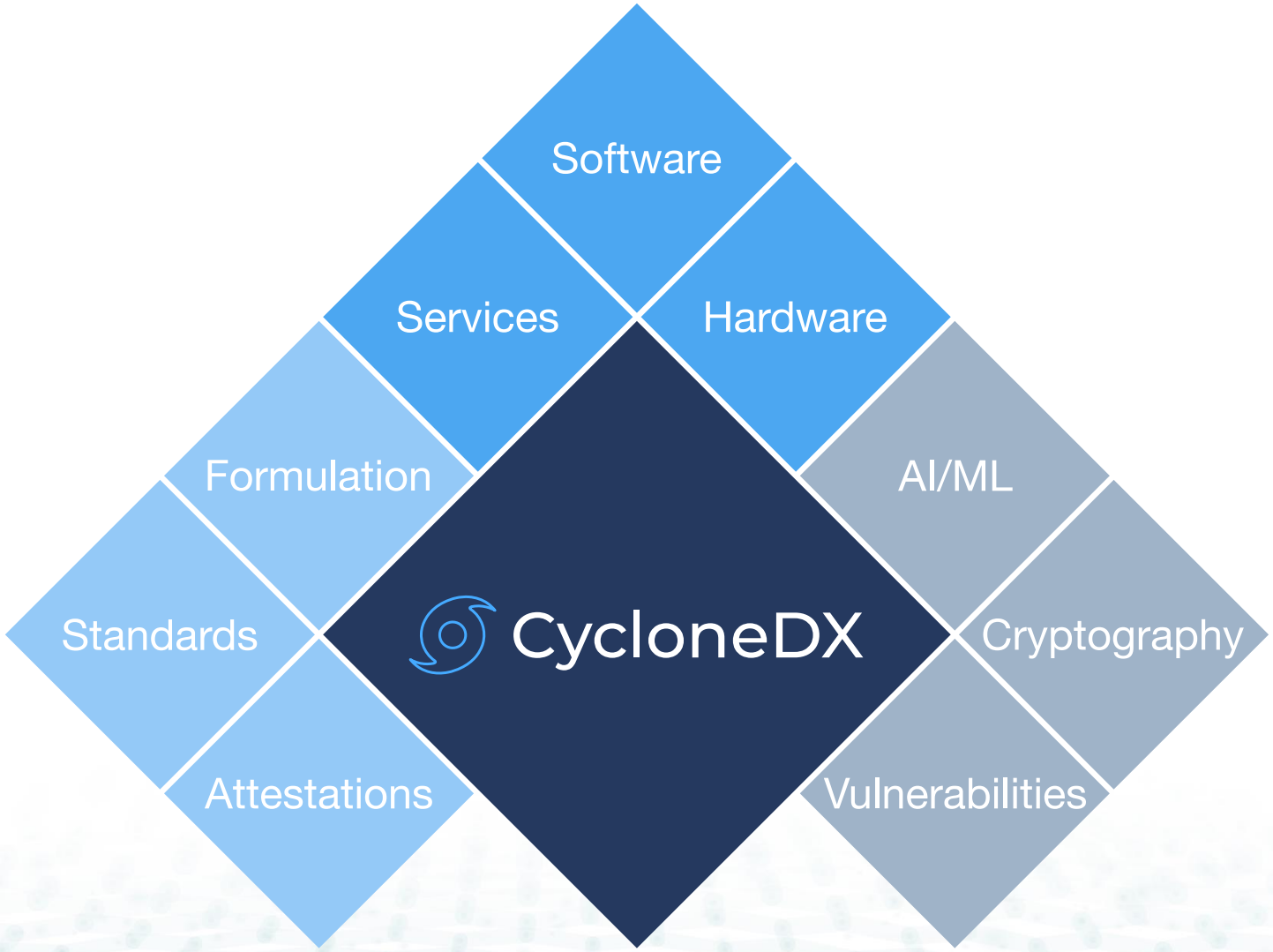
CycloneDX



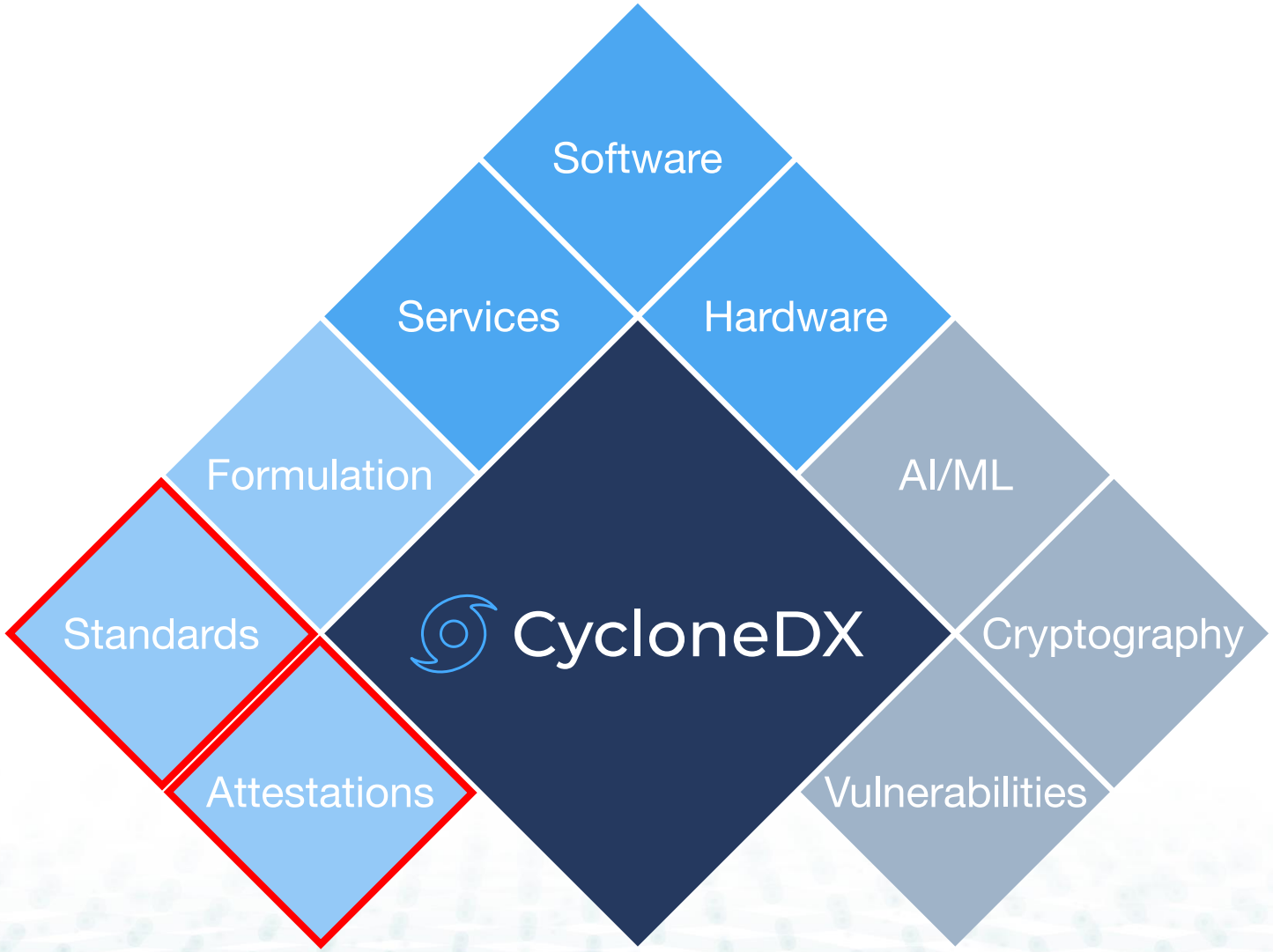
CycloneDX
SBOM

CycloneDX
SaaSBOM

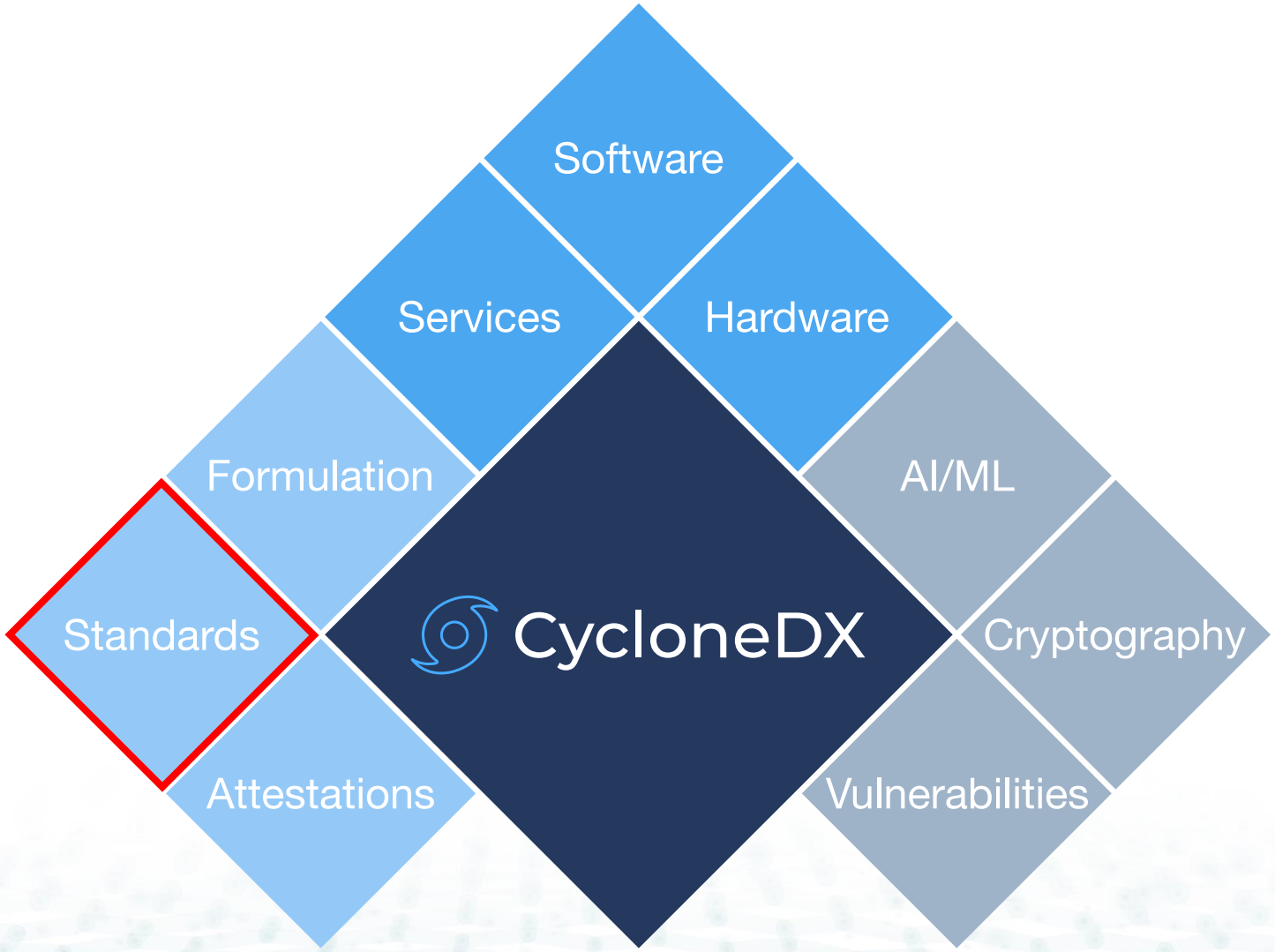
PCI Security Standards Council



PCI Security Standards Council®



PCI Security Standards Council®



PCI Security Standards Council

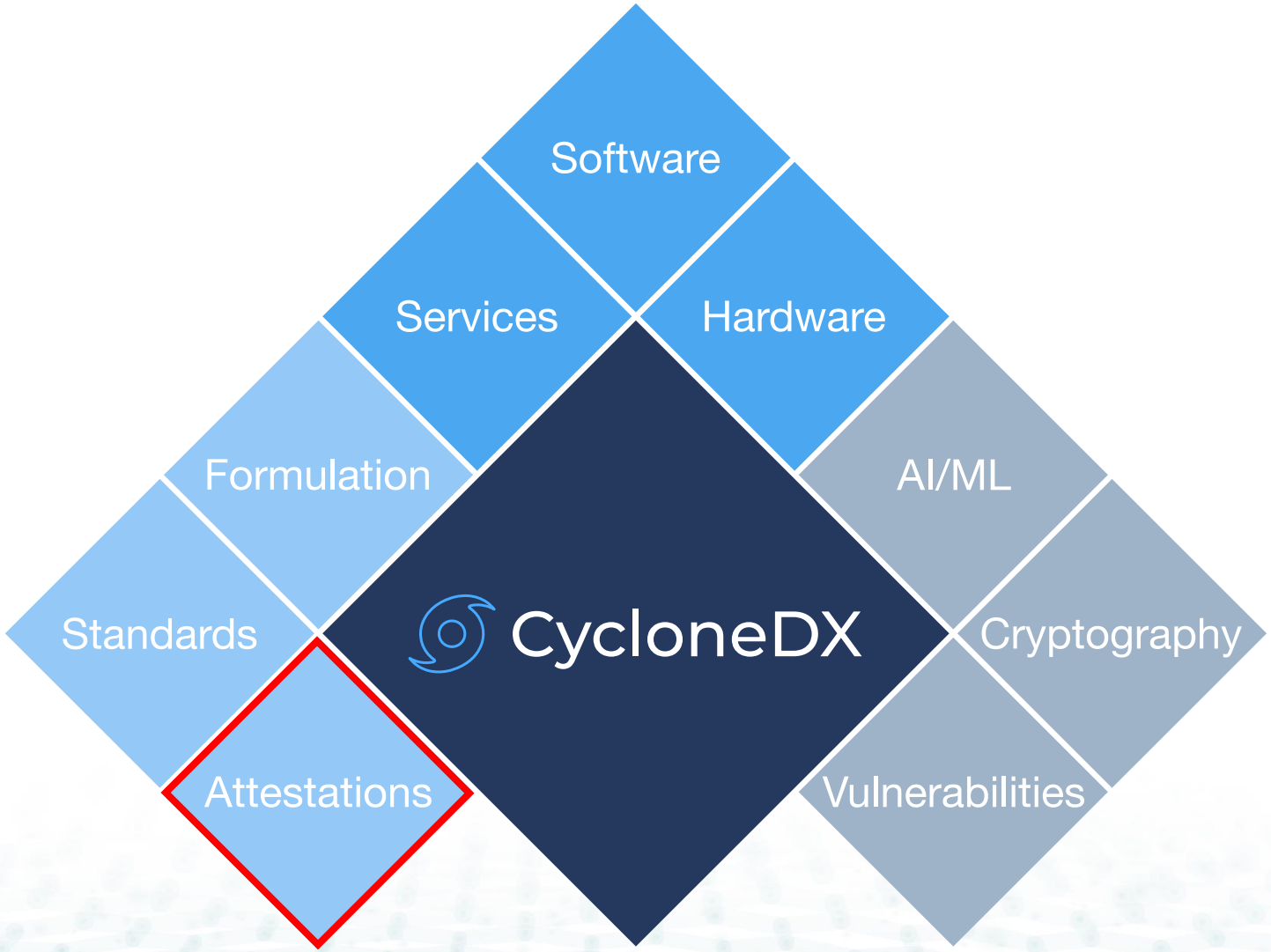
```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:f5224b09-170c-4e02-b7e8-98560d7acea6",
  "version": 1,
  "metadata": {
    "timestamp": "2023-10-04T00:37:13-05:00",
    "licenses": [],
    "supplier": {
      "name": "OWASP Foundation",
      "url": [
        "https://owasp.org"
      ]
    }
  },
  "definitions": {
    "standards": [
      {
        "bom-ref": "pcissc-sslc-1.1",
        "name": "PCI Secure Software Lifecycle (Secure SLC) Requirements and Assessment Procedures",
        "version": "1.1",
        "description": "PCI Secure SLC provides a baseline of security requirements with corresponding assessment procedures and guidance to help software vendors design, develop, and mainta
        "owner": "PCI Security Standards Council",
        "requirements": [
          {
            "bom-ref": "pcissc-sslc-1.1-1",
            "identifier": "1",
            "title": "Security Responsibilities and Resources",
            "text": "The software vendor's senior leadership team establishes formal responsibility and authority for the security of the software vendor's products and services. The softwar
          },
          {
            "bom-ref": "pcissc-sslc-1.1-1.1",
            "identifier": "1.1",
            "text": "Overall responsibility for the security of the software vendor's products and services is assigned by the vendor's senior leadership team.",
            "parent": "pcissc-sslc-1.1-1",
            "descriptions": [
              "The formal assignment of responsibility by the software vendor's senior leadership team ensures strategic-level visibility into and influence over the vendor's software securi
            ]
          },
          {
            "bom-ref": "pcissc-sslc-1.1-1.1.1",
            "identifier": "1.1.1",
            "text": "Accountability for ensuring the security of the software vendor's products and services is formally assigned to an individual or team by the software vendor's senior lea
            "parent": "pcissc-sslc-1.1-1.1"
          },
```


PCI Security Standards Council®

Machine Readable Standards

Benefits

- Simplifies updates to GRC systems when a new version of a standard is published.
- Facilitates more detailed analysis of changes from version to version.
- Enables organizations to display information in the standard in a manner that best suits their needs.
- Eliminates duplication errors across PCI documents.



PCI Security Standards Council

```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "declarations": {
    "assessors": [
      {
        "bom-ref": "assessor-1",
        "thirdParty": true,
        "organization": {
          "name": "Assessors Inc"
        }
      }
    ],
    "attestations": [
      {
        "summary": "Attestation summary here",
        "assessor": "assessor-1",
        "map": [
          {
            "requirement": "requirement-1",
            "claims": [ "claim-1" ],
            "counterClaims": [ "counterClaim-1" ],
            "conformance": {
              "score": 0.8,
              "rationale": "Conformance rationale here",
              "mitigationStrategies": [ "mitigationStrategy-1" ]
            },
            "confidence": {
              "score": 1,
              "rationale": "Confidence rationale here"
            }
          }
        ],
        "signature": {
          "algorithm": "ES256",
          "certificatePath": [ "MIIB...", "MIID..." ],
          "value": "tqIT..."
        }
      }
    ],
```


PCI Security Standards Council®

```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "declarations": {
    "assessors": [
      {
        "bom-ref": "assessor-1",
        "thirdParty": true,
        "organization": {
          "name": "Assessors Inc"
        }
      }
    ],
```



```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "declarations": {
    "assessors": [
      {
        "bom-ref": "assessor-1",
        "thirdParty": true,
        "organization": {
          "name": "Assessors Inc"
        }
      }
    ],
    "attestations": [
      {
        "summary": "Attestation summary here",
        "assessor": "assessor-1",
        "map": [
          {
            "requirement": "requirement-1",
            "claims": [ "claim-1" ],
            "counterClaims": [ "counterClaim-1" ],
            "conformance": {
              "score": 0.8,
              "rationale": "Conformance rationale here",
              "mitigationStrategies": [ "mitigationStrategy-1" ]
            },
            "confidence": {
              "score": 1,
              "rationale": "Confidence rationale here"
            }
          }
        ],
        "signature": {
          "algorithm": "ES256",
          "certificatePath": [ "MIIB...", "MIID..." ],
          "value": "tqIT..."
        }
      }
    ],
```

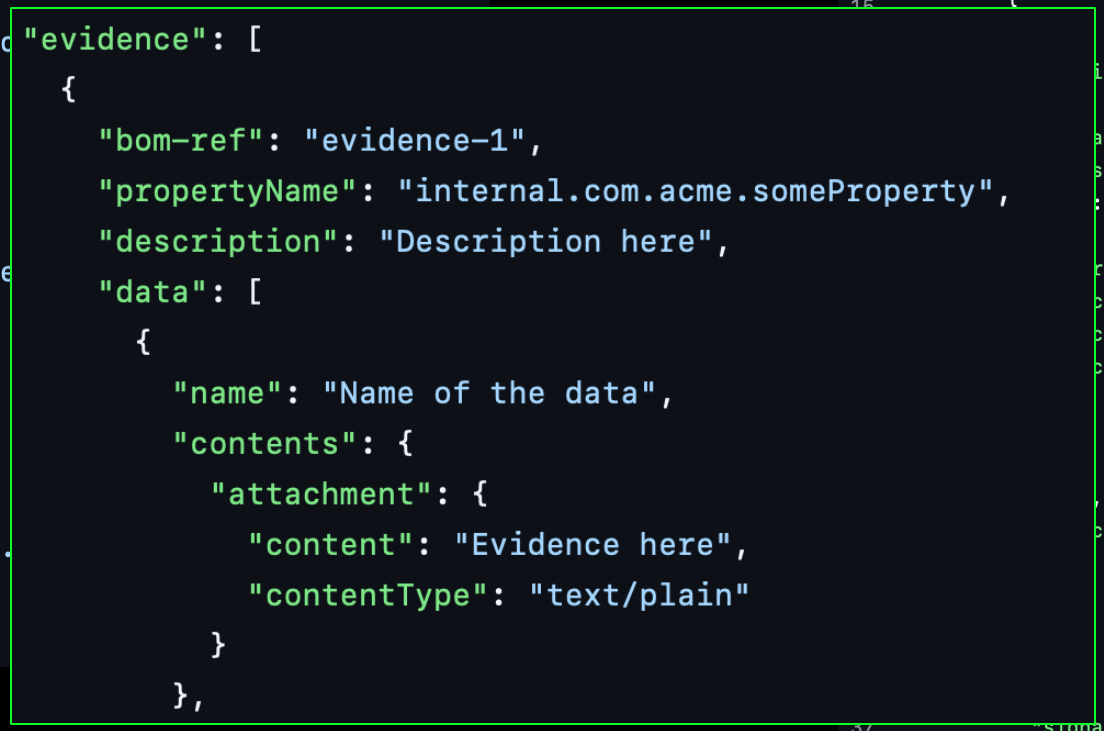

PCI Security Standards Council

```
"attestations": [
  {
    "summary": "Attestation summary here",
    "assessor": "assessor-1",
    "map": [
      {
        "requirement": "requirement-1",
        "claims": [ "claim-1" ],
        "counterClaims": [ "counterClaim-1" ],
        "conformance": {
          "score": 0.8,
          "rationale": "Conformance ratio
          "mitigationStrategies": [ "mitig
        },
        "confidence": {
          "score": 1,
          "rationale": "Confidence rationa
        }
      }
    ],
    "signature": {
      "algorithm": "ES256",
      "certificatePath": [ "MIIB...", "MIID..." ],
      "value": "tqIT..."
    }
  }
],
```

```
"assessors": [
  {
    "bom-ref": "assessor-1",
    "thirdParty": true,
    "organization": {
      "name": "Assessors Inc"
    }
  }
```

```
{
  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
  "bomFormat": "CycloneDX",
  "specVersion": "1.6",
  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
  "version": 1,
  "declarations": {
    "assessors": [
      {
        "bom-ref": "assessor-1",
        "thirdParty": true,
        "organization": {
          "name": "Assessors Inc"
        }
      }
    ],
    "attestations": [
      {
        "summary": "Attestation summary here",
        "assessor": "assessor-1",
        "map": [
          {
            "requirement": "requirement-1",
            "claims": [ "claim-1" ],
            "counterClaims": [ "counterClaim-1" ],
            "conformance": {
              "score": 0.8,
              "rationale": "Conformance rationale here",
              "mitigationStrategies": [ "mitigationStrategy-1" ]
            },
            "confidence": {
              "score": 1,
              "rationale": "Confidence rationale here"
            }
          }
        ],
        "signature": {
          "algorithm": "ES256",
          "certificatePath": [ "MIIB...", "MIID..." ],
          "value": "tqIT..."
        }
      }
    ],
```

PCI Security Standards Council



PCI Security Standards Council

PCI Security Standards Council®

Machine Readable Attestations

Benefits

Eliminates or minimizes the need for maintaining documentation in Word or PDF formats.

Enables the information to be formatted or displayed as needed.

Allows information to be appended and/or updated more easily.

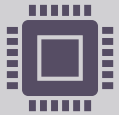
Supports the use of cryptographic signatures.

PCI Security Standards Council®

Machine Readable Attestations

Challenges & Other Considerations

Not all PCI SSC standards are structured to support machine-readable formats.



PCI SSC has not standardized on a particular schema.

Converting PCI SSC standards to these formats is not a top priority at this moment.

PCI Security Standards Council

Machine Readable Standards & Attestations

Next Steps

- Please be patient as PCI SSC continues to evaluate appropriate methods to provide these formats.
- Look for machine readable versions of the revised Secure Software and Secure SLC Standards in 2025 (v2.0).
- Leverage the RFC process as well as your PCI SSC contacts to submit requests and/or comments on machine readable versions of other PCI SSC standards.

PCI Security Standards Council

References

For more information on the SPDX and CycloneDX specifications, go to:

- SPDX website at: https://spdx.dev
- CycloneDX website at: https://cyclonedx.org

Thank You!


PCi
Security
Standards Council
®