

2024 Europe Community Meeting

You Dropped a BOM on Me, Baby



Jake Marcinko

Senior Manager, Solution Standards
PCI Security Standards Council







```
1 SPDXVersion: SPDX-2.2
2 DataLicense: CC0-1.0
3 SPDXID: SPDXRef-DOCUMENT
4 DocumentName: spdx-sbom-generator
5 DocumentNamespace: http://spdx.org/spdxpackages/spdx-sbom-generator--57918521-3212-4369-a8ed-3d681ec1d7a1
6 Creator: Tool: spdx-sbom-generator-XXXXX
7 Created: 2021-05-23 11:25:29.1672276 -0400 -04 m=+0.538283001
8
9 ##### Package representing the Go distribution
10
11 PackageName: go
12 SPDXID: SPDXRef-Package-go
13 PackageVersion: v0.46.3
14 PackageSupplier: NOASSERTION
15 PackageDownloadLocation: pkg:golang/cloud.google.com/go@v0.46.3
16 FilesAnalyzed: false
17 PackageChecksum: TEST: SHA-1 224ffa55932c22cef869e85aa33e2ada43f0fb8d
18 PackageHomePage: pkg:golang/cloud.google.com/go@v0.46.3
19 PackageLicenseConcluded: NOASSERTION
20 PackageLicenseDeclared: NOASSERTION
21 PackageCopyrightText: NOASSERTION
22 PackageLicenseComments: NOASSERTION
23 PackageComment: NOASSERTION
24
25 Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-Package-go
26
27 ##### Package representing the Bigquery Distribution
28
29 PackageName: bigquery
30 SPDXID: SPDXRef-Package-bigquery
31 PackageVersion: v1.0.1
32 PackageSupplier: NOASSERTION
33 PackageDownloadLocation: pkg:golang/cloud.google.com/go/bigquery@v1.0.1
34 FilesAnalyzed: false
35 PackageChecksum: TEST: SHA-1 8168e852b675afc9a63b502feefac90944a5a2a
36 PackageHomePage: pkg:golang/cloud.google.com/go/bigquery@v1.0.1
37 PackageLicenseConcluded: NOASSERTION
38 PackageLicenseDeclared: NOASSERTION
39 PackageCopyrightText: NOASSERTION
40 PackageLicenseComments: NOASSERTION
41 PackageComment: NOASSERTION
42
43 Relationship: SPDXRef-Package-go CONTAINS SPDXRef-Package-bigquery
```





MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

[BRIEFING ROOM](#)[PRESIDENTIAL ACTIONS](#)

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.

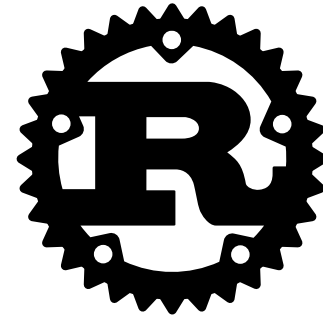
Security Requirements

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: <ul style="list-style-type: none"> • 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. <p>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.</p> <p>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.</p>

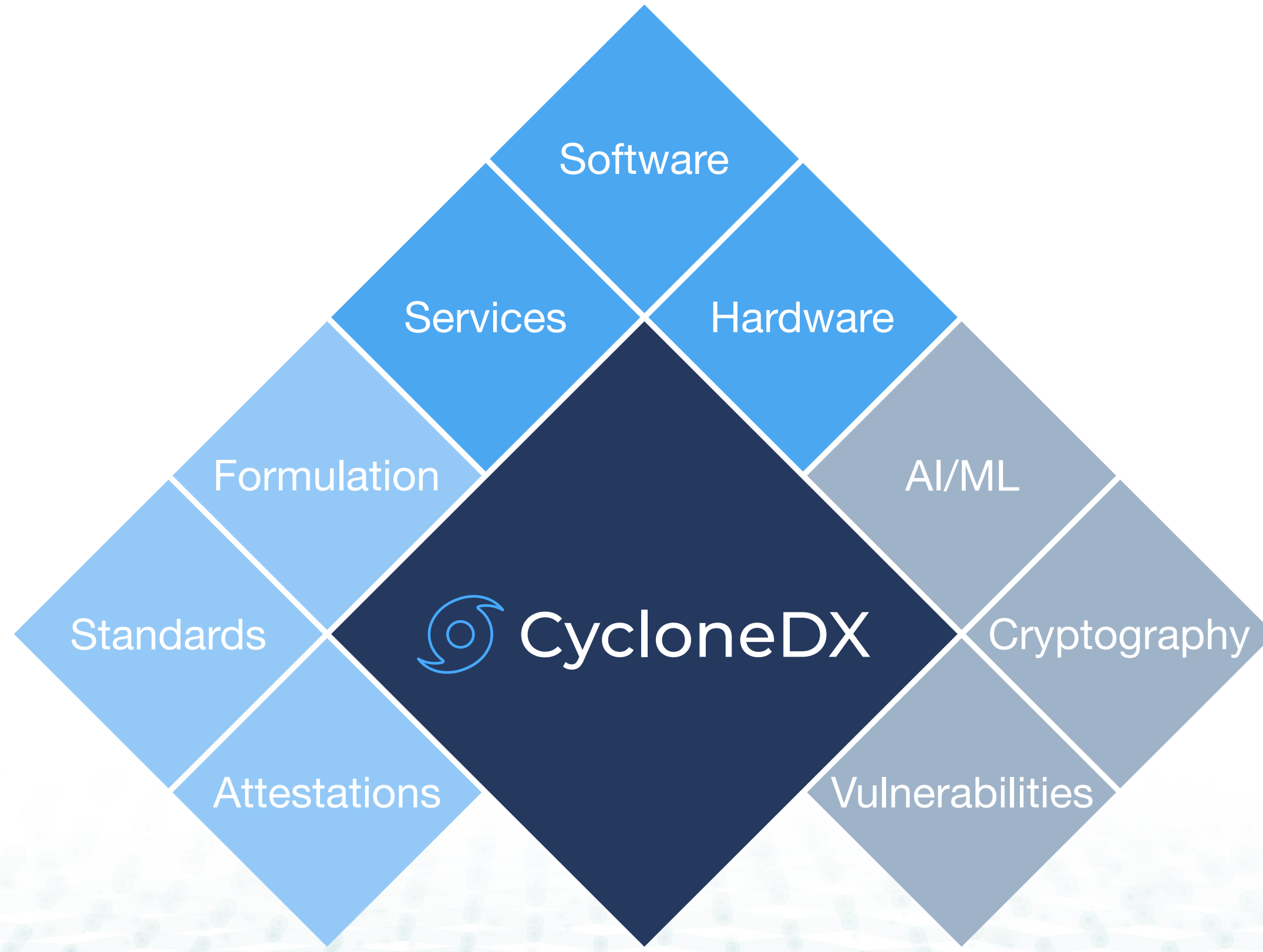


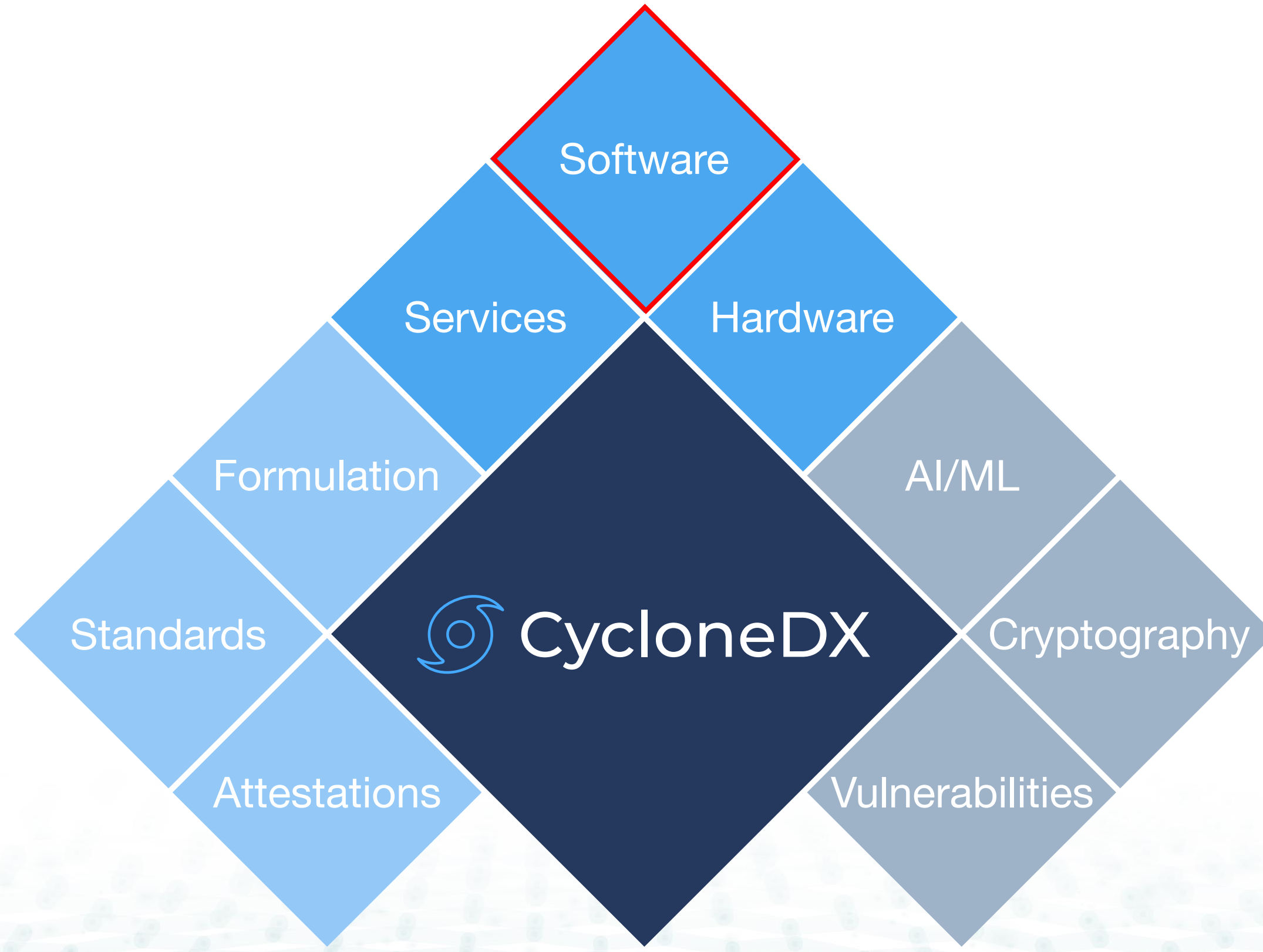


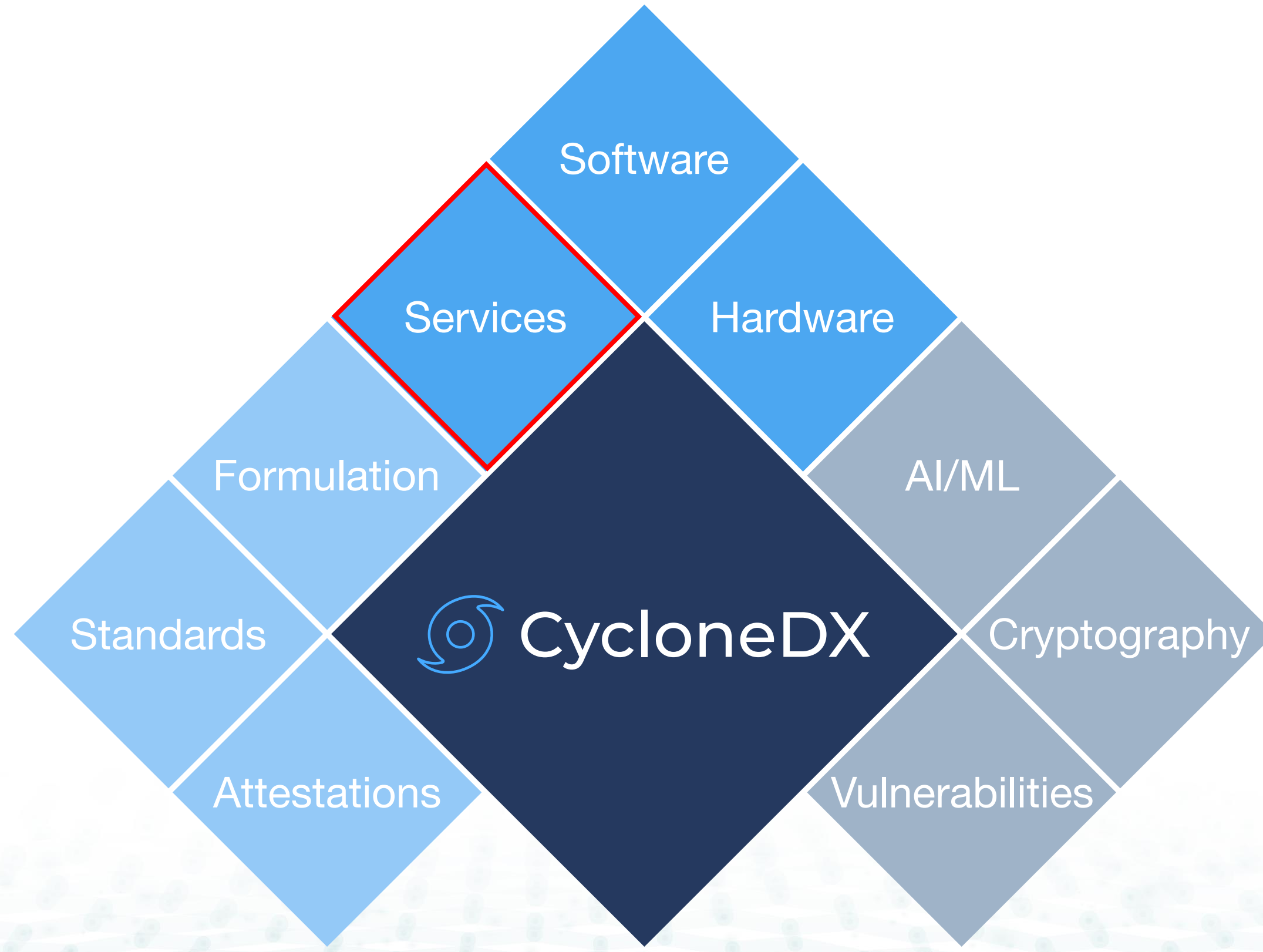
Maven

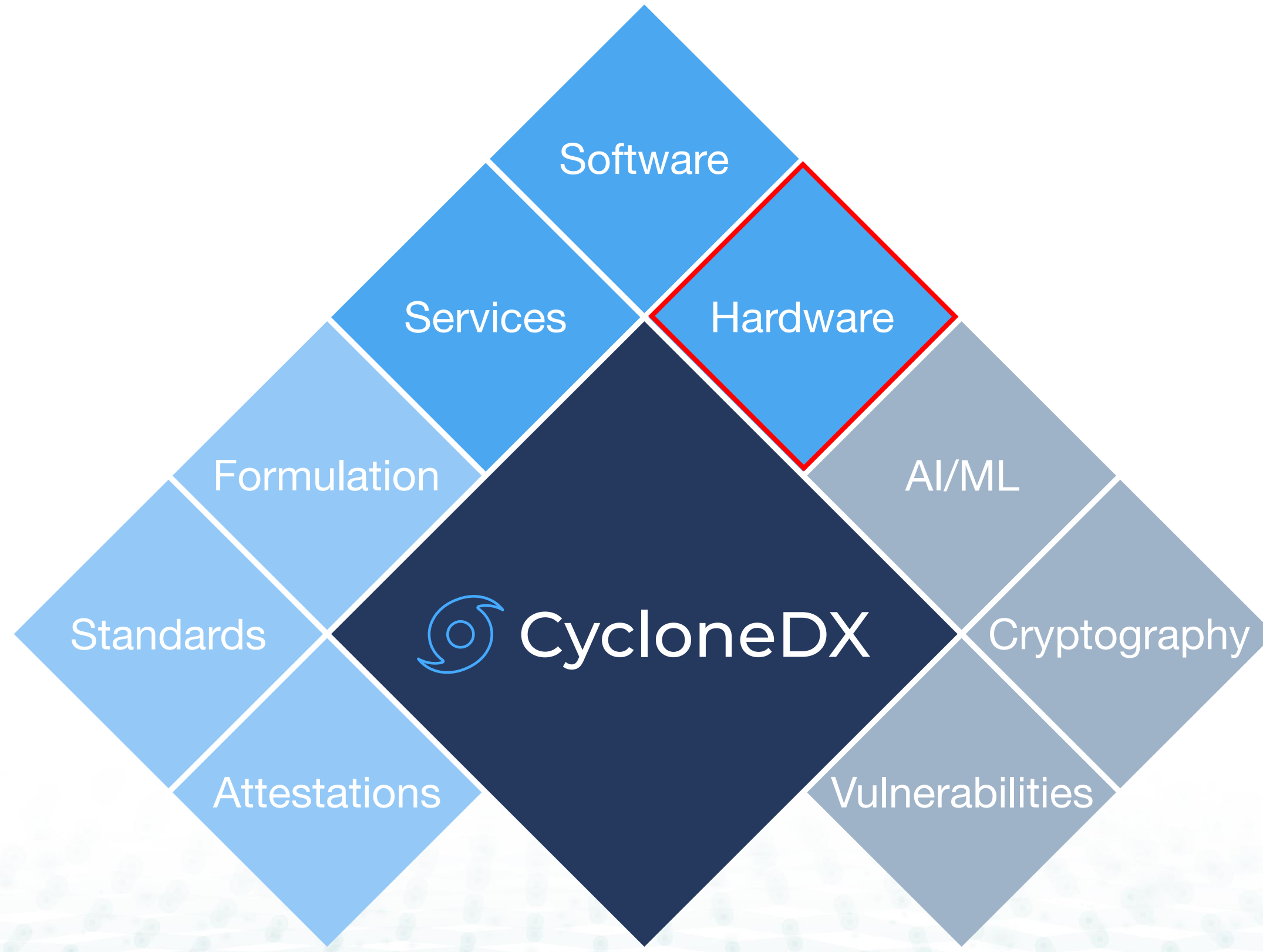


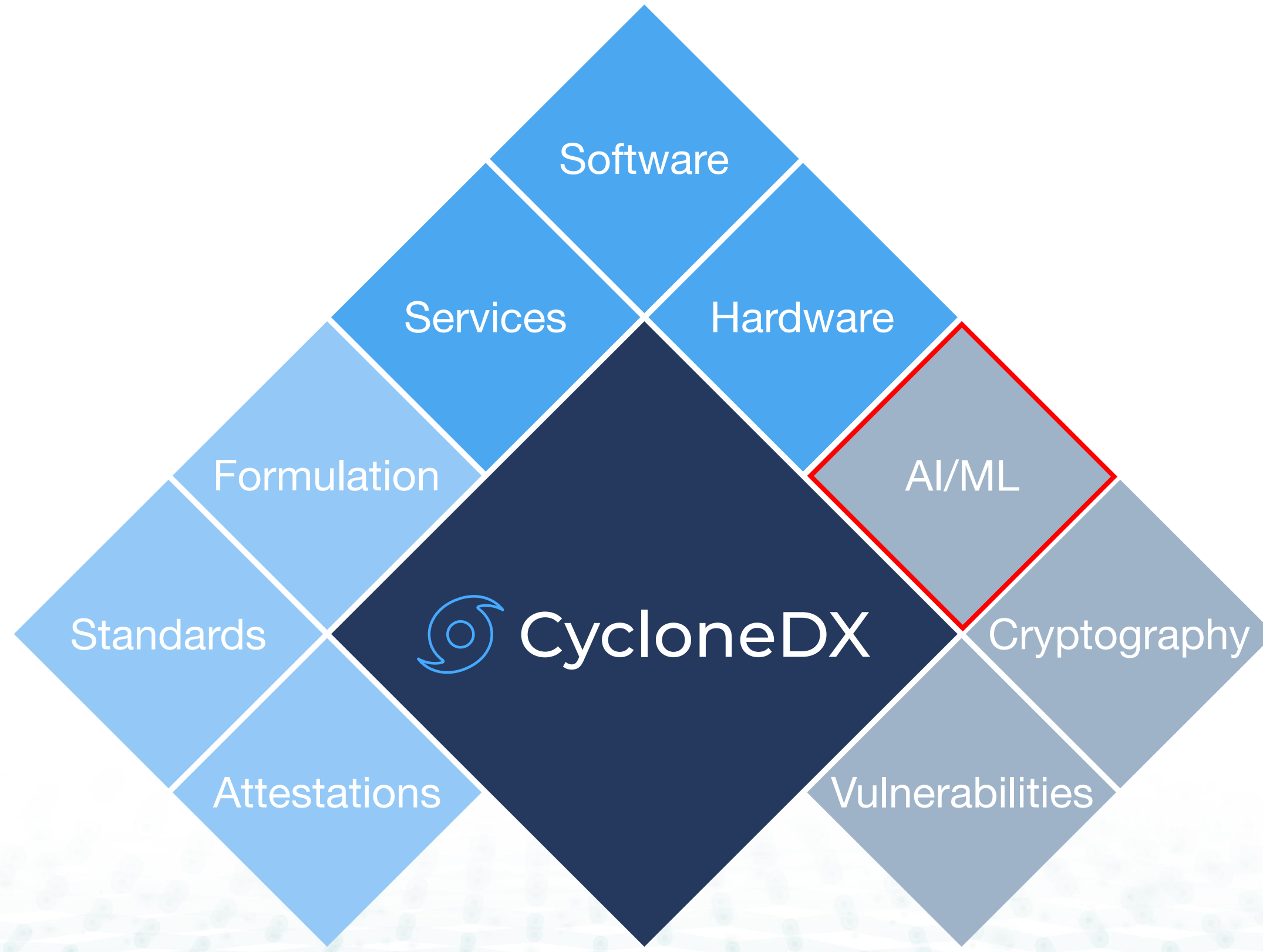


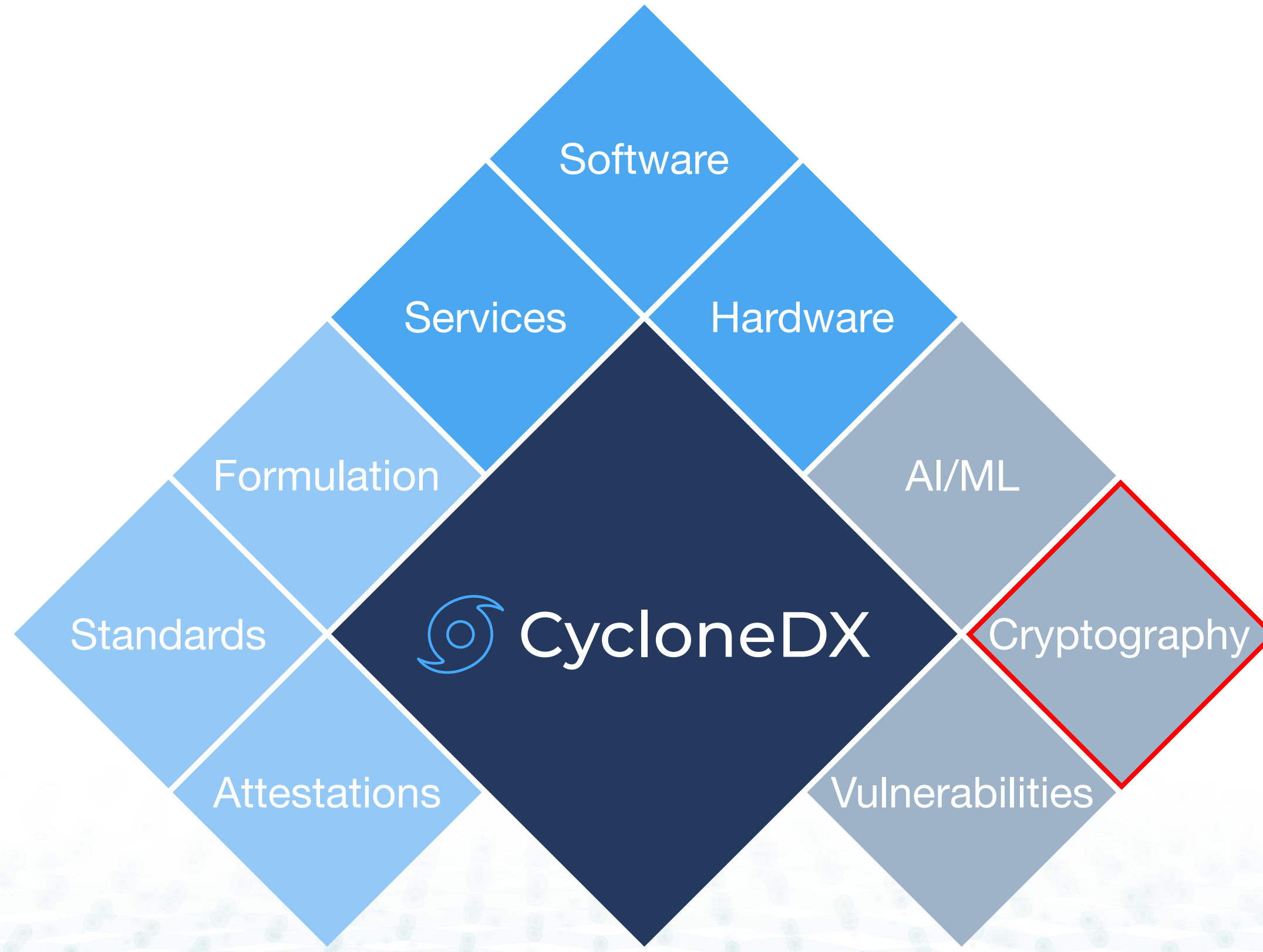












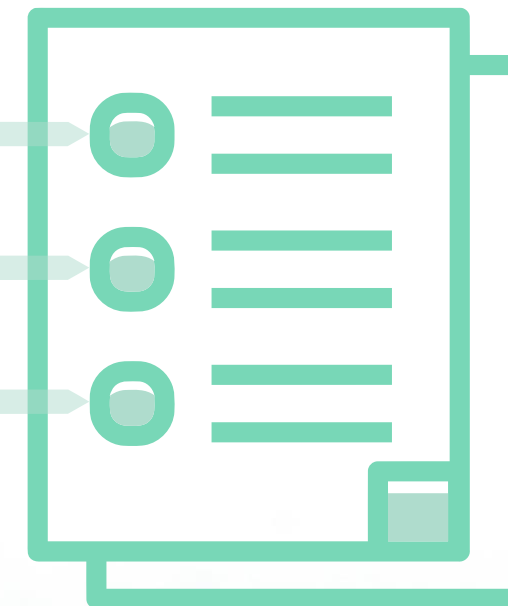
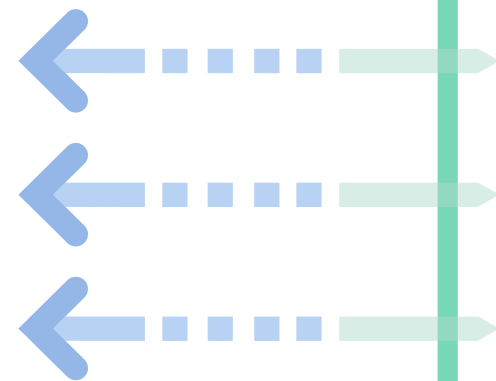


SBOM
+
SaaSOM

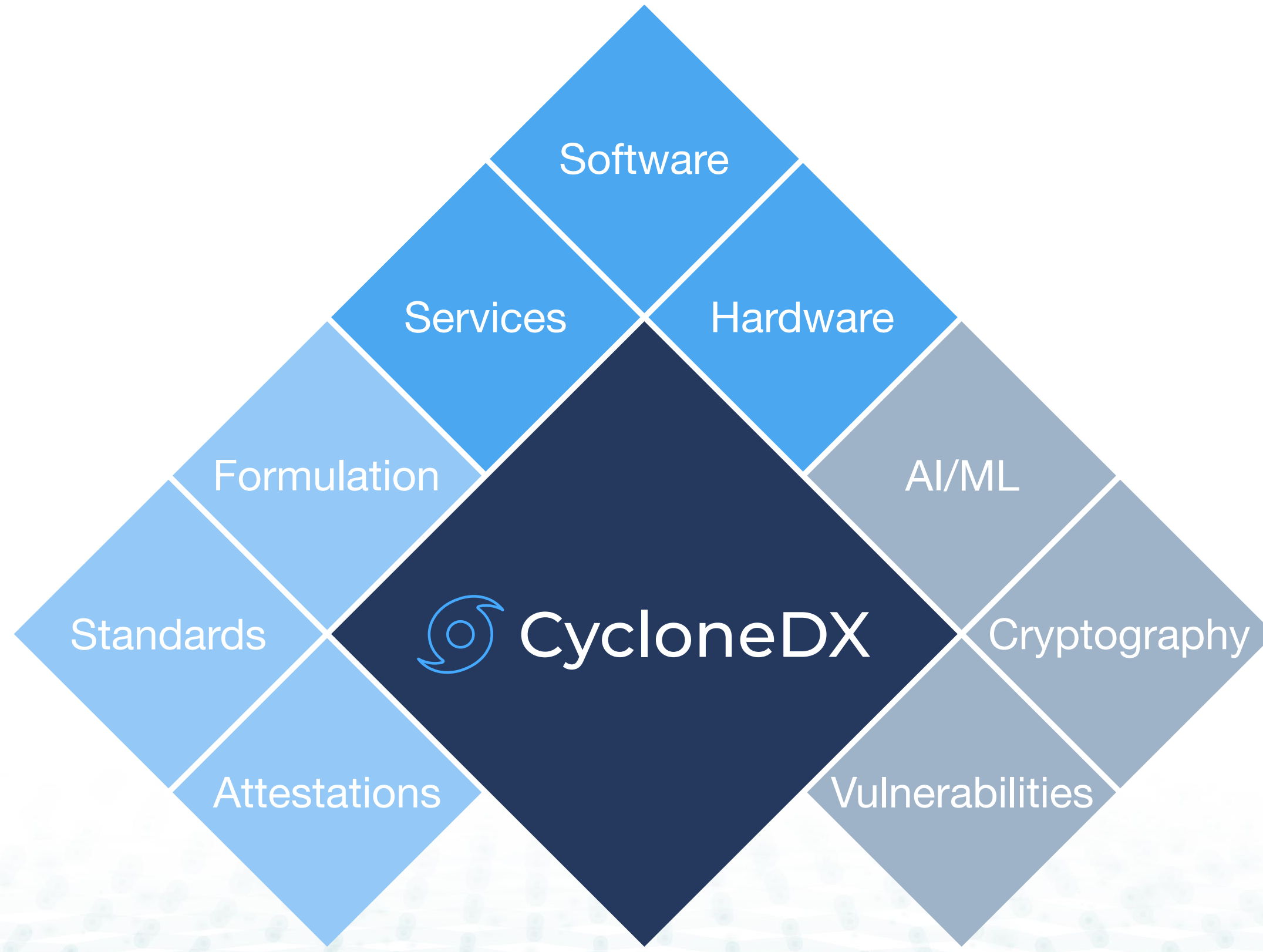
 CycloneDX

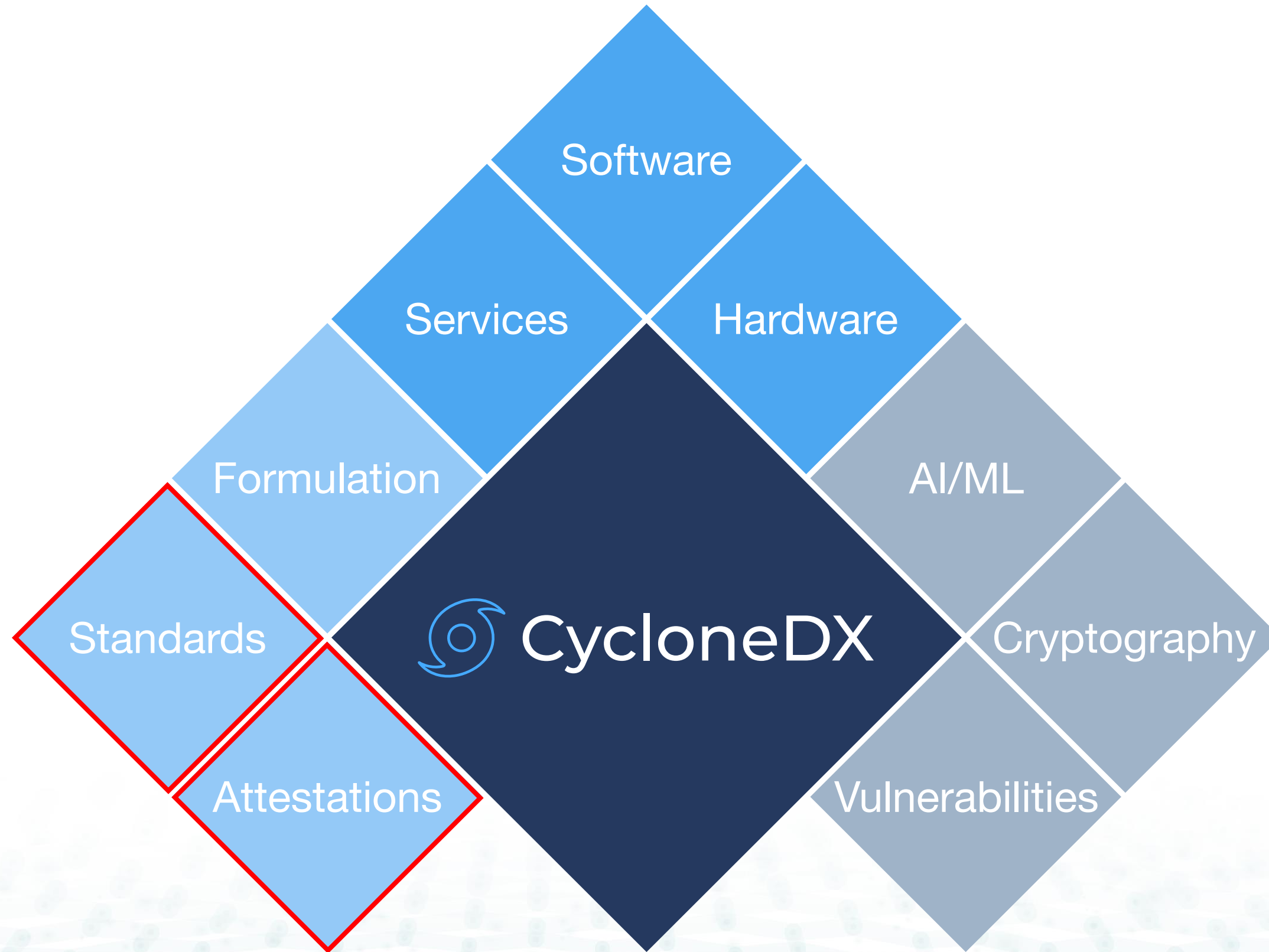


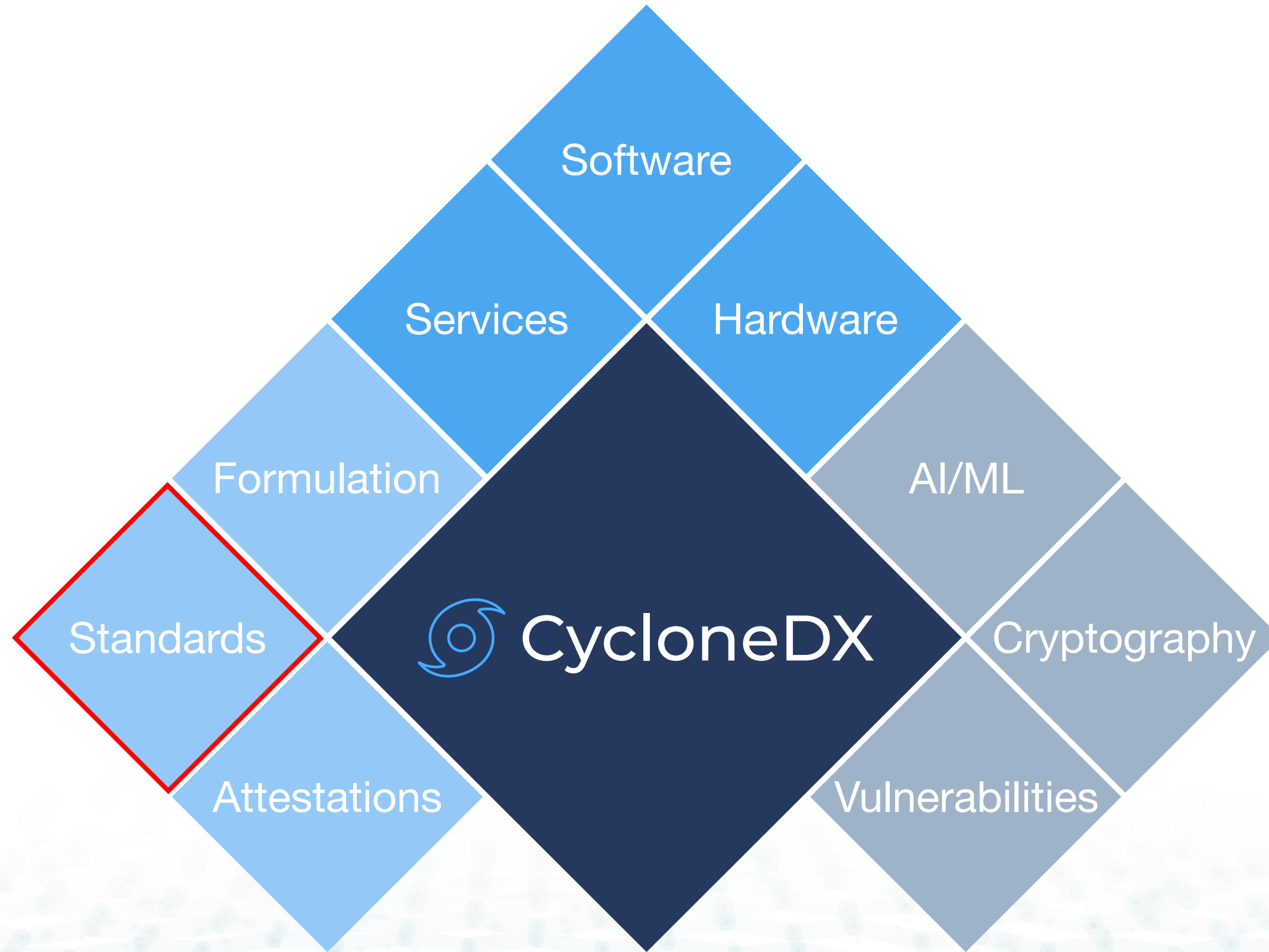
 CycloneDX
SBOM



 CycloneDX
SaaSOM







```

1  {
2    "bomFormat": "CycloneDX",
3    "specVersion": "1.6",
4    "serialNumber": "urn:uuid:f5224b09-170c-4e02-b7e8-98560d7acea6",
5    "version": 1,
6    "metadata": {
7      "timestamp": "2023-10-04T00:37:13-05:00",
8      "licenses": [],
9      "supplier": {
10       "name": "OWASP Foundation",
11       "url": [
12         "https://owasp.org"
13       ]
14     }
15   },
16   "definitions": {
17     "standards": [
18       {
19         "bom-ref": "pcissc-sslc-1.1",
20         "name": "PCI Secure Software Lifecycle (Secure SLC) Requirements and Assessment Procedures",
21         "version": "1.1",
22         "description": "PCI Secure SLC provides a baseline of security requirements with corresponding assessment procedures and guidance to help software vendors design, develop, and maintain",
23         "owner": "PCI Security Standards Council",
24         "requirements": [
25           {
26             "bom-ref": "pcissc-sslc-1.1-1",
27             "identifier": "1",
28             "title": "Security Responsibilities and Resources",
29             "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 software",
30           },
31           {
32             "bom-ref": "pcissc-sslc-1.1-1.1",
33             "identifier": "1.1",
34             "text": "Overall responsibility for the security of the software vendor's products and services is assigned by the vendor's senior leadership team.",
35             "parent": "pcissc-sslc-1.1-1",
36             "descriptions": [
37               "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 security",
38             ]
39           },
40           {
41             "bom-ref": "pcissc-sslc-1.1-1.1.1",
42             "identifier": "1.1.1",
43             "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 leadership",
44             "parent": "pcissc-sslc-1.1-1.1"
45           },

```

Machine Readable Standards

Benefits

Machine Readable Standards

Benefits

- Simplifies updates to GRC systems when a new version of a standard is published.

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.

Machine Readable Standards

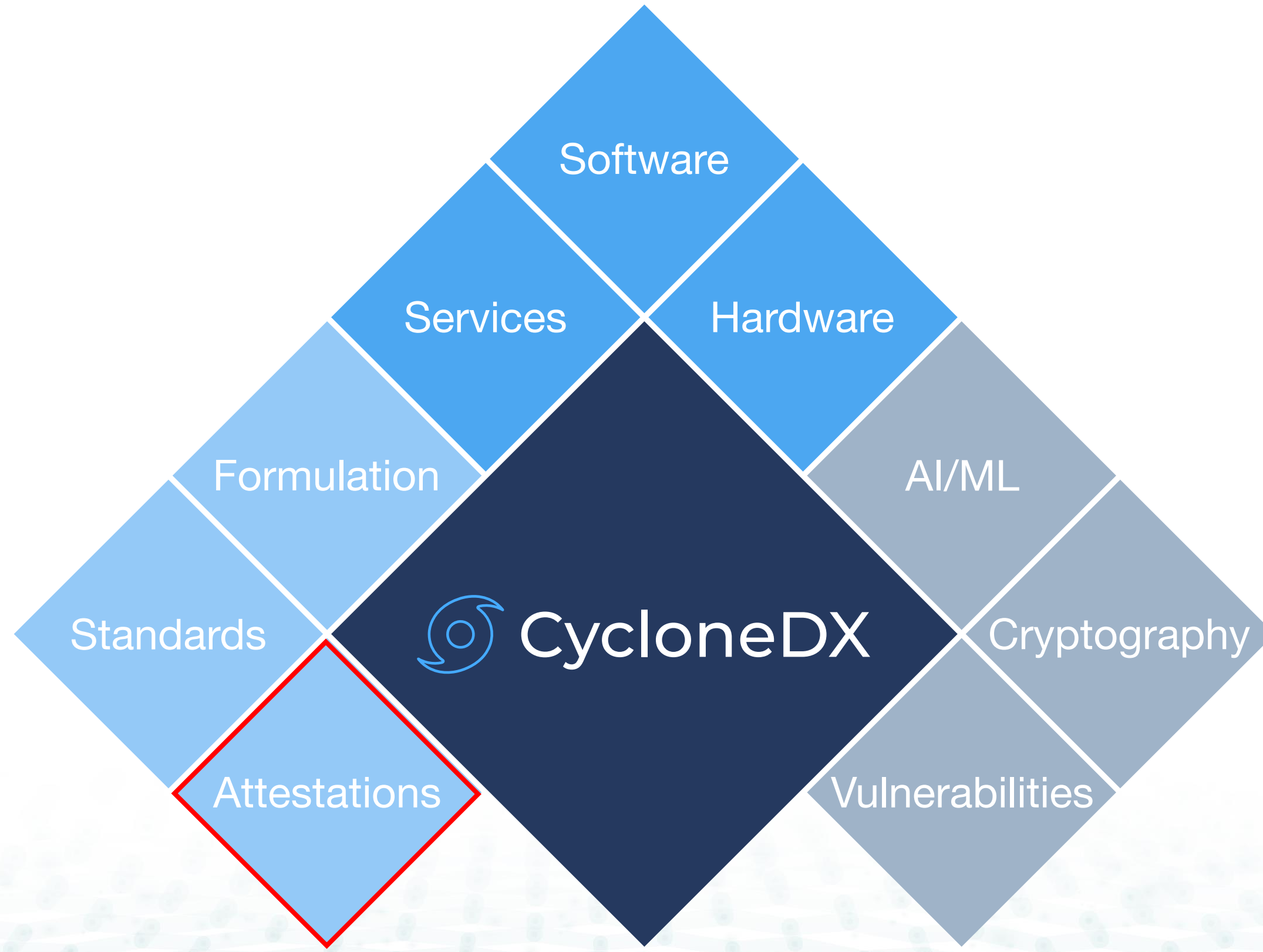
Benefits

- 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.

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.



```
1 {
2   "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
3   "bomFormat": "CycloneDX",
4   "specVersion": "1.6",
5   "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
6   "version": 1,
7   "declarations": {
8     "assessors": [
9       {
10        "bom-ref": "assessor-1",
11        "thirdParty": true,
12        "organization": {
13          "name": "Assessors Inc"
14        }
15      }
16    ],
17    "attestations": [
18      {
19        "summary": "Attestation summary here",
20        "assessor": "assessor-1",
21        "map": [
22          {
23            "requirement": "requirement-1",
24            "claims": [ "claim-1" ],
25            "counterClaims": [ "counterClaim-1" ],
26            "conformance": {
27              "score": 0.8,
28              "rationale": "Conformance rationale here",
29              "mitigationStrategies": [ "mitigationStrategy-1" ]
30            },
31            "confidence": {
32              "score": 1,
33              "rationale": "Confidence rationale here"
34            }
35          }
36        ],
37        "signature": {
38          "algorithm": "ES256",
39          "certificatePath": [ "MIIB...", "MIID..." ],
40          "value": "tqIT..."
41        }
42      }
43    ],
```

```

{
  "$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"
        }
      }
    ],
  },

```

```

1  {
2  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
3  "bomFormat": "CycloneDX",
4  "specVersion": "1.6",
5  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
6  "version": 1,
7  "declarations": {
8    "assessors": [
9      {
10       "bom-ref": "assessor-1",
11       "thirdParty": true,
12       "organization": {
13         "name": "Assessors Inc"
14       }
15     }
16   ],
17   "attestations": [
18     {
19       "summary": "Attestation summary here",
20       "assessor": "assessor-1",
21       "map": [
22         {
23           "requirement": "requirement-1",
24           "claims": [ "claim-1" ],
25           "counterClaims": [ "counterClaim-1" ],
26           "conformance": {
27             "score": 0.8,
28             "rationale": "Conformance rationale here",
29             "mitigationStrategies": [ "mitigationStrategy-1" ]
30           },
31           "confidence": {
32             "score": 1,
33             "rationale": "Confidence rationale here"
34           }
35         }
36       ],
37       "signature": {
38         "algorithm": "ES256",
39         "certificatePath": [ "MIIB...", "MIID..." ],
40         "value": "tqIT..."
41       }
42     }
43   ],

```

```

"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..."
    }
  }
],

```

```

1  {
2  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
3  "bomFormat": "CycloneDX",
4  "specVersion": "1.6",
5  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
6  "version": 1,
7  "declarations": {
8    "assessors": [
9      {
10         "bom-ref": "assessor-1",
11         "thirdParty": true,
12         "organization": {
13           "name": "Assessors Inc"
14         }
15       }
16     ],
17     "attestations": [
18       {
19         "summary": "Attestation summary here",
20         "assessor": "assessor-1",
21         "map": [
22           {
23             "requirement": "requirement-1",
24             "claims": [ "claim-1" ],
25             "counterClaims": [ "counterClaim-1" ],
26             "conformance": {
27               "score": 0.8,
28               "rationale": "Conformance rationale here",
29               "mitigationStrategies": [ "mitigationStrategy-1" ]
30             },
31             "confidence": {
32               "score": 1,
33               "rationale": "Confidence rationale here"
34             }
35           }
36         ],
37         "signature": {
38           "algorithm": "ES256",
39           "certificatePath": [ "MIIB...", "MIID..." ],
40           "value": "tqIT..."
41         }
42       }
43     ],

```

```

"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..."
    }
  }
],

```

```

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

```

```

1  {
2  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
3  "bomFormat": "CycloneDX",
4  "specVersion": "1.6",
5  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
6  "version": 1,
7  "declarations": {
8    "assessors": [
9      {
10       "bom-ref": "assessor-1",
11       "thirdParty": true,
12       "organization": {
13         "name": "Assessors Inc"
14       }
15     }
16   ],
17   "attestations": [
18     {
19       "summary": "Attestation summary here",
20       "assessor": "assessor-1",
21       "map": [
22         {
23           "requirement": "requirement-1",
24           "claims": [ "claim-1" ],
25           "counterClaims": [ "counterClaim-1" ],
26           "conformance": {
27             "score": 0.8,
28             "rationale": "Conformance rationale here",
29             "mitigationStrategies": [ "mitigationStrategy-1" ]
30           },
31           "confidence": {
32             "score": 1,
33             "rationale": "Confidence rationale here"
34           }
35         }
36       ],
37       "signature": {
38         "algorithm": "ES256",
39         "certificatePath": [ "MIIB...", "MIID..." ],
40         "value": "tqIT..."
41       }
42     }
43   ],

```

```

"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..."
}

```

```

1  {
2  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
3  "bomFormat": "CycloneDX",
4  "specVersion": "1.6",
5  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
6  "version": 1,
7  "declarations": {
8    "assessors": [
9      {
10         "bom-ref": "assessor-1",
11         "thirdParty": true,
12         "organization": {
13           "name": "Assessors Inc"
14         }
15       }
16     ],
17     "attestations": [
18       {
19         "summary": "Attestation summary here",
20         "assessor": "assessor-1",
21         "map": [
22           {
23             "requirement": "requirement-1",
24             "claims": [ "claim-1" ],
25             "counterClaims": [ "counterClaim-1" ],
26             "conformance": {
27               "score": 0.8,
28               "rationale": "Conformance rationale here",
29               "mitigationStrategies": [ "mitigationStrategy-1" ]
30             },
31             "confidence": {
32               "score": 1,
33               "rationale": "Confidence rationale here"
34             }
35           }
36         ],
37         "signature": {
38           "algorithm": "ES256",
39           "certificatePath": [ "MIIB...", "MIID..." ],
40           "value": "tqIT..."
41         }
42       }
43     ],

```

```
"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...", "MID..." ],
  "value": "tqIT..."
}
```

```
"claims": [
  {
    "bom-ref": "claim-1",
    "target": "acme-inc",
    "predicate": "Predicate here",
    "mitigationStrategies": [ "mitigationStrategy-1" ],
    "reasoning": "Reasoning here",
    "evidence": [ "evidence-1" ],
    "counterEvidence": [ "counterEvidence-1" ],
    "externalReferences": [
      {
        "type": "issue-tracker",
        "url": "https://alm.example.com"
      }
    ]
  }
],
```

```
1  {
2    "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
3    "bomFormat": "CycloneDX",
4    "specVersion": "1.6",
5    "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
6    "version": 1,
7    "declarations": {
8      "assessors": [
9        {
10         "bom-ref": "assessor-1",
11         "thirdParty": true,
12         "organization": {
13           "name": "Assessors Inc"
14         }
15       }
16     ],
17     "attestations": [
18       {
19         "summary": "Attestation summary here",
20         "assessor": "assessor-1",
21         "map": [
22           {
23             "requirement": "requirement-1",
24             "claims": [ "claim-1" ],
25             "counterClaims": [ "counterClaim-1" ],
26             "conformance": {
27               "score": 0.8,
28               "rationale": "Conformance rationale here",
29               "mitigationStrategies": [ "mitigationStrategy-1" ]
30             },
31             "confidence": {
32               "score": 1,
33               "rationale": "Confidence rationale here"
34             }
35           }
36         ]
37       },
38       {
39         "summary": "Attestation summary here",
40         "assessor": "assessor-1",
41         "map": [
42           {
43             "requirement": "requirement-1",
44             "claims": [ "claim-1" ],
45             "counterClaims": [ "counterClaim-1" ],
46             "conformance": {
47               "score": 0.8,
48               "rationale": "Conformance rationale here",
49               "mitigationStrategies": [ "mitigationStrategy-1" ]
50             },
51             "confidence": {
52               "score": 1,
53               "rationale": "Confidence rationale here"
54             }
55           }
56         ]
57       }
58     ],
59     "signature": {
60       "algorithm": "ES256",
61       "certificatePath": [ "MIIB...", "MID..." ],
62       "value": "tqIT..."
63     }
64   }
65 ],
```



```

"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..."
}

```

```

1  {
2  "$schema": "http://cyclonedx.org/schema/bom-1.6.schema.json",
3  "bomFormat": "CycloneDX",
4  "specVersion": "1.6",
5  "serialNumber": "urn:uuid:3e671687-395b-41f5-a30f-a58921a69b79",
6  "version": 1,
7  "declarations": {
8    "assessors": [
9      {
10         "bom-ref": "assessor-1",
11         "thirdParty": true,
12         "organization": {
13           "name": "Assessors Inc"
14         }
15       }
16     ],
17     "attestations": [
18       {
19         "summary": "Attestation summary here",
20         "assessor": "assessor-1",
21         "map": [
22           {
23             "requirement": "requirement-1",
24             "claims": [ "claim-1" ],
25             "counterClaims": [ "counterClaim-1" ],
26             "conformance": {
27               "score": 0.8,
28               "rationale": "Conformance rationale here",
29               "mitigationStrategies": [ "mitigationStrategy-1" ]
30             },
31             "confidence": {
32               "score": 1,
33               "rationale": "Confidence rationale here"
34             }
35           }
36         ],
37         "signature": {
38           "algorithm": "ES256",
39           "certificatePath": [ "MIIB...", "MIID..." ],
40           "value": "tqIT..."
41         }
42       }
43     ],

```

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.



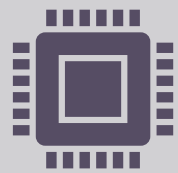
Supports the use of cryptographic signatures.

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.

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!





Security
Standards Council®