SCANOSS

CODE FREELY. FINISH EARLY. TRUST COMPLETELY.

About SCANOSS

FIRST OPEN SOURCE RISK MANAGEMENT PLATFORM

github.com/scanoss

FIRST OPEN DATA OSS KNOWEDGEBASE

osskb.org

always-on

FREE AND OPEN SBOM

SPDX
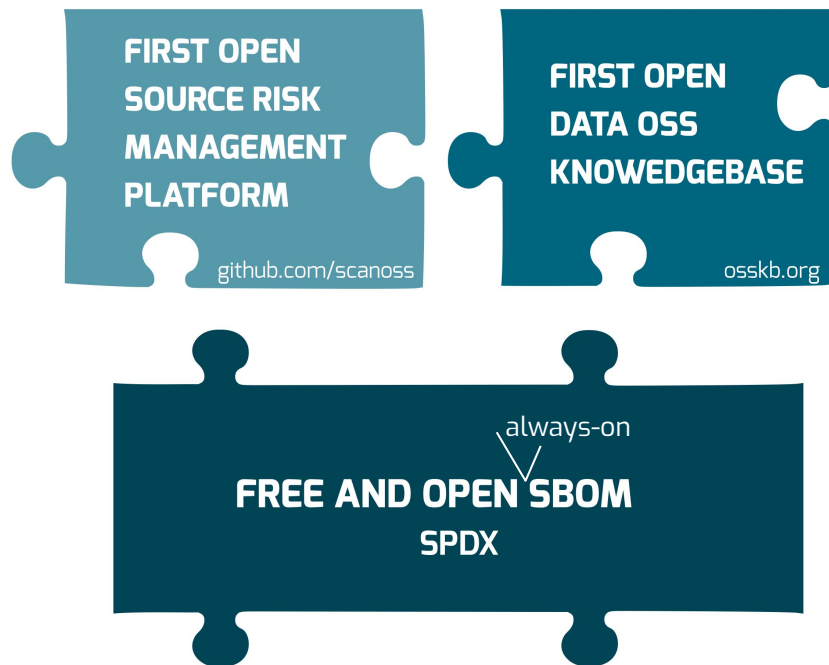
- Over a decade of SCA of experience as users & vendors

- Frustrated with legacy SCA vendors

- Three years of independent research and development

- Agile-driven, native DevOps support, **Open Source**

SCANOSS

Our mission

Democratise Open Source Risk Management

SCANOSS

Our vision: 360° Open Source Risk Management

LEGAL

License detection
Copyright detection
Dependency detection
Compliance notices
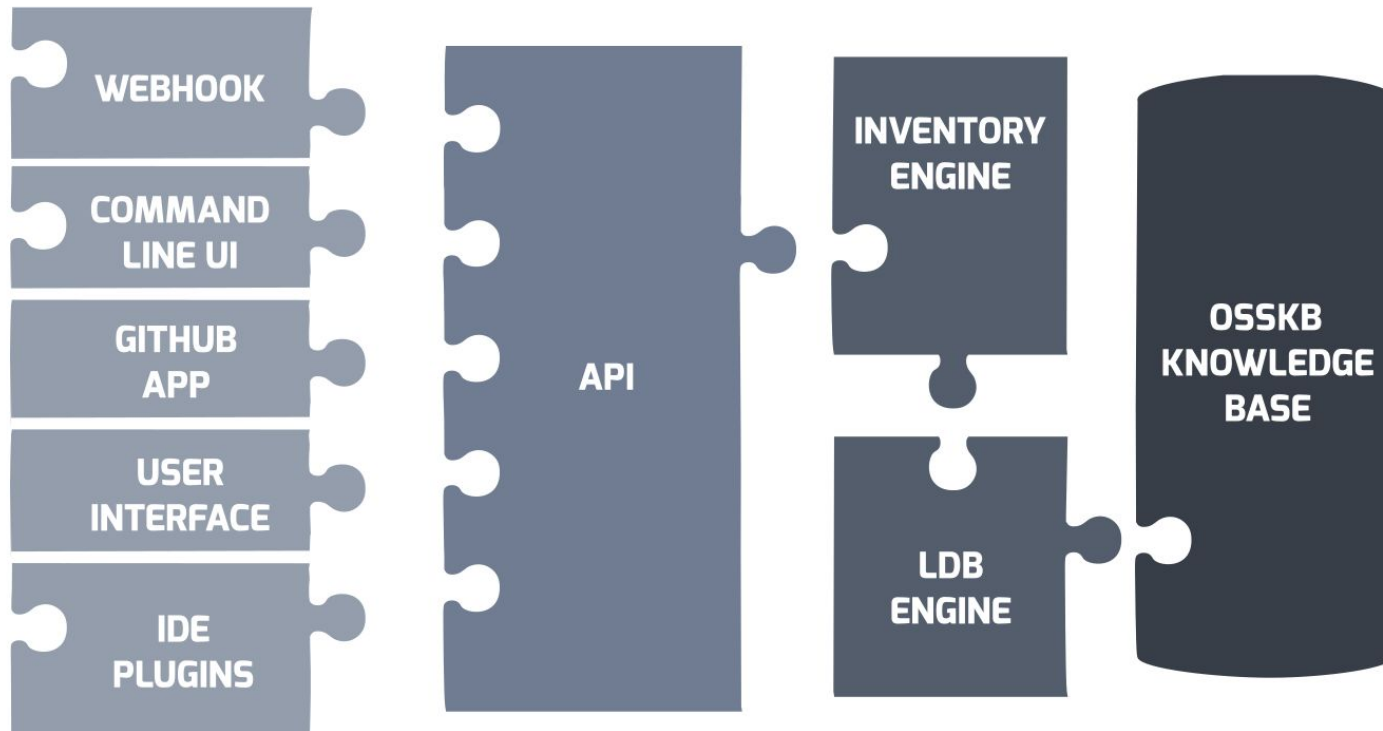Export control
Provenance
License compatibility

TECHNICAL

Project Health

Issues - Forks - Releases
Governance - Adoption

Project Quality

Best practices - Performance
Scalability - Stability
Documentation

SECURITY

NVD
NPM
VulnDB
Sonatype
Suse advisories
Github advisories

SCANOSS

We're different: 100% Open Source OSRM Platform

First public scanning & inventorying engine

100 million
One hundred million known OSS components in our knowledge base

50 billion
Fifty billion individual OSS files in our knowledge base

2 trillion
Two trillion lines of known OSS code in our knowledge base

20 microseconds
all it takes to scan a file and perform an identification could be just 0.00002 seconds

*https://osskb.org

Easy, rich SBOM for anyone: The QuickScan app

Available for Windows, Linux, Mac
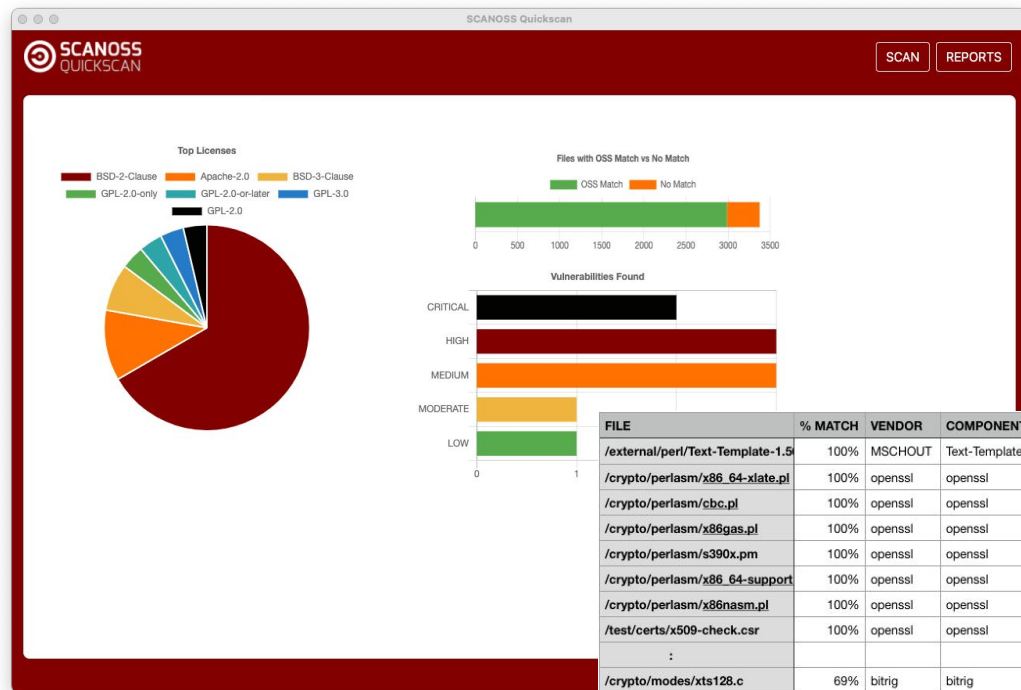
FILE	% MATCH	VENDOR	COMPONENT	VERSION	LICENSE	VULNERABILITIES	COPYRIGHT
/external/perl/Text-Template-1.5(	100%	MSCHOUT	Text-Template	1,56			Copyright 2013 M. J. Dominus.
/crypto/perlasm/x86_64-xlate.pl	100%	openssl	openssl	3.0.0~~alpha4.orig-openssl-	Apache-2.0		
/crypto/perlasm/cbc.pl	100%	openssl	openssl	3.0.0~~alpha1.orig-openssl-	Apache-2.0		Copyright 1995-2020 The OpenSSL Project Authors. All Rights Reserved.
/crypto/perlasm/x86gas.pl	100%	openssl	openssl	3.0.0~~alpha1.orig-openssl-	Apache-2.0		Copyright 2007-2020 The OpenSSL Project Authors. All Rights Reserved.
/crypto/perlasm/s390x.pm	100%	openssl	openssl	openssl-3.0.0-alpha4	Apache-2.0		Copyright 2018-2020 The OpenSSL Project Authors. All Rights Reserved.
/crypto/perlasm/x86_64-support	100%	openssl	openssl	openssl-3.0.0-alpha4	Apache-2.0		Copyright 2020 The OpenSSL Project Authors. All Rights Reserved.
/crypto/perlasm/x86nasm.pl	100%	openssl	openssl	3.0.0~~alpha1.orig-openssl-	Apache-2.0		Copyright 1999-2018 The OpenSSL Project Authors. All Rights Reserved.
/test/certs/x509-check.csr	100%	openssl	openssl	1.1.1g.orig	Apache-2.0	CVE-2007-5536	
:							
/crypto/modes/xts128.c	69%	bitrig	bitrig	sync_20140507	BSD-2-Clause		Copyright (c) 2011 The OpenSSL Project. All rights reserved.
/crypto/pem/pem_oth.c	30%	bitvisor	bitvisor	0.7-1.2	BSD-2-Clause		
/crypto/engine/eng_dyn.c	20%	bitrig	bitrig	sync_20150307-sync_2015(	BSD-2-Clause		Copyright (c) 1999-2001 The OpenSSL Project. All rights reserved.
:							
:							

SBOM standardized formats

```json
{
  "test.c": [
    {
      "id": "snippet",
      "lines": "1-10",
      "oss_lines": "175-184",
      "matched": "90%",
      "vendor": "unoconv",
      "component": "unoconv",
      "version": "0.9",
      "latest": "0.9",
      "url": "https://github.com/unoconv/unoconv/archive/0.9.zip",
      "file": "unoconv-0.9/unoconv",
      "component_id": "c6efa01ea8df7aca018b384a9ce26057",
      "file_id": "fbad29f459b5d52fce1e9596b50f3e8c",
      "dependencies": [],
      "licenses": [
        {
          "name": "GPL-2.0-only",
          "source": "component_declared"
        }
      ],
      "copyrights": [
        {
          "name": "Copyright 2007-2010 Dag Wieers <dag@wieers.com>",
          "source": "file_header"
        }
      ],
      "vulnerabilities": [
        {
          "ID": "GHSA-27p5-7cw6-m45h",
          "CVE": "CVE-2019-17400",
          "severity": "MODERATE",
          "reported": "2019-11-01T17:03:50Z",
          "introduced": "",
          "patched": "< 0.9.0",
          "summary": "Mishandled untrusted pathnames could lead to SSRF",
          "source": "github_advisories"
        }
      ],
      "quality": [
        {
          "score": "2/5",
          "source": "best_practices"
        }
      ],
      "elapsed": "0.002990s"
    }
  ]
}
```

RAW (JSON)

```json
"Document": {
  "specVersion": "SPDX-2.0",
  "creationInfo": {
    "creators": [
      "Tool: SCANOSS Inventory Engine",
      "Organization: http://scanoss.com"
    ],
    "comment": "This SPDX report has been automatically generated",
    "licenseListVersion": "1.19",
    "created": "2020-12-10T15:57:14+0000"
  },
  "spdxVersion": "SPDX-2.0",
  "dataLicense": "CC0-1.0",
  "id": "SPDXRef-DOCUMENT",
  "name": "SPDX-Tools-v2.0",
  "comment": "This document was automatically generated with SCANOSS.",
  "externalDocumentRefs": [],
  "documentDescribes": [
    {
      "Package": {
        "name": "unoconv",
        "versionInfo": "0.9",
        "supplier": "unoconv",
        "copyrightText": "Copyright 2007-2010 Dag Wieers <dag@wieers.com>",
        "downloadLocation": "https://github.com/unoconv/unoconv/archive/0.9.zip",
        "checksum": [
          {
            "algorithm": "checksumAlgorithm_md5",
            "value": "feac02b1ddc1556c2bd1361c4d6cc1b0"
          }
        ],
        "description": "Detected by SCANOSS Inventorying Engine.",
        "licenseConcluded": "",
        "licenseInfoFromFiles": "GPL-2.0-only"
      }
    }
  ]
}
```

SPDX (JSON)

```json
"bomFormat": "CycloneDX",
"specVersion": "1.2",
"serialNumber": "scanoss:prod04-5b1ebd38a30de6de4d4986b043b2420c",
"version": 1,
"components": [
  {
    "type": "file",
    "publisher": "unoconv",
    "group": "unoconv",
    "name": "unoconv",
    "version": "0.9",
    "hashes": [
      {
        "alg": "MD5",
        "content": "feac02b1ddc1556c2bd1361c4d6cc1b0"
      }
    ],
    "licenses": [
      {
        "license": {
          "id": "GPL-2.0-only"
        }
      }
    ],
    "purl":
    "https://github.com/unoconv/unoconv/archive/0.9.zip#unoconv-0.9/unoconv",
    "description": "Lines matched: 1-10"
  }
]
```

CycloneDX (JSON)

```xml
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:spdx="http://spdx.org/rdf/terms#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#">
  <spdx:SpdxDocument rdf:about="https://osskb.org/docs/spdx.rdf#SPDXRef-DOCUMENT">
    <spdx:specVersion>SPDX-2.1</spdx:specVersion>
    <spdx:dataLicense rdf:resource="http://spdx.org/licenses/CC0-1.0" />
    <spdx:creationInfo>
      <spdx:CreationInfo>
        <spdx:licenseListVersion>2.6</spdx:licenseListVersion>
        <spdx:creator>Person: OSSKB</spdx:creator>
        <spdx:creator>Organization: SCANOSS</spdx:creator>
        <spdx:creator>Tool: OSSKB</spdx:creator>
        <spdx:created>2020-12-10T16:00:26+0000</spdx:created>
      </spdx:CreationInfo>
    </spdx:creationInfo>
    <spdx:name>test.c</spdx:name>
    <rdfs:comment>
      This document was created by the SCANOSS engine by scanning against the OSSKB.ORG
    </rdfs:comment>
    <spdx:relationship>
      <spdx:Relationship>
        <spdx:relationshipType rdf:resource="http://spdx.org/rdf/terms#relationshipType_describes" />
        <spdx:relatedSpdxElement>
          <spdx:Package rdf:about="https://osskb.org">
            <spdx:name>test.c</spdx:name>
            <spdx:packageFileName>test.c</spdx:packageFileName>
            <spdx:downloadLocation rdf:resource="http://spdx.org/rdf/terms#noassertion" />
            <spdx:packageVerificationCode>
              <spdx:PackageVerificationCode>
                <spdx:packageVerificationCodeValue>0000000000000000000000000000000000000000</spdx:packageVerificationCodeValue>
              </spdx:PackageVerificationCode>
            </spdx:packageVerificationCode>
            <spdx:checksum>
              <spdx:Checksum>
                <spdx:algorithm rdf:resource="http://spdx.org/rdf/terms#checksumAlgorithm_md5" />
                <spdx:checksumValue>0000000000000000000000000000000000000000</spdx:checksumValue>
              </spdx:Checksum>
            </spdx:checksum>
            <spdx:licenseConcluded>
              <spdx:DisjunctiveLicenseSet>
              </spdx:DisjunctiveLicenseSet>
            </spdx:licenseConcluded>
            <spdx:licenseConcluded rdf:resource="http://spdx.org/rdf/terms#noassertion" />
            <spdx:licenseDeclared rdf:resource="http://spdx.org/rdf/terms#noassertion" />
            <spdx:licenseInfoFromFiles rdf:resource="http://spdx.org/rdf/terms#noassertion" />
            <spdx:copyrightText rdf:resource="http://spdx.org/rdf/terms#noassertion" />
            <spdx:hasFile>
              <spdx:File rdf:about="https://osskb.org/api/file_contents/fbad29f459b5d52fce1e9596b50f3e8c">
                <spdx:fileName>unoconv-0.9/unoconv</spdx:fileName>
                <spdx:checksum>
                  <spdx:Checksum>
                    <spdx:algorithm rdf:resource="http://spdx.org/rdf/terms#checksumAlgorithm_md5" />
                    <spdx:checksumValue>fbad29f459b5d52fce1e9596b50f3e8c</spdx:checksumValue>
                  </spdx:Checksum>
                </spdx:checksum>
                <spdx:licenseConcluded rdf:resource="http://spdx.org/rdf/terms#noassertion" />
                <spdx:licenseInfoInFile rdf:resource="http://spdx.org/rdf/terms#noassertion" />
                <spdx:copyrightText><![CDATA[
Copyright 2007-2010 Dag Wieers <dag@wieers.com>
                ]]></spdx:copyrightText>
              </spdx:File>
            </spdx:hasFile>
          </spdx:Package>
        </spdx:relatedSpdxElement>
      </spdx:Relationship>
    </spdx:relationship>
  </spdx:SpdxDocument>
</rdf:RDF>
```
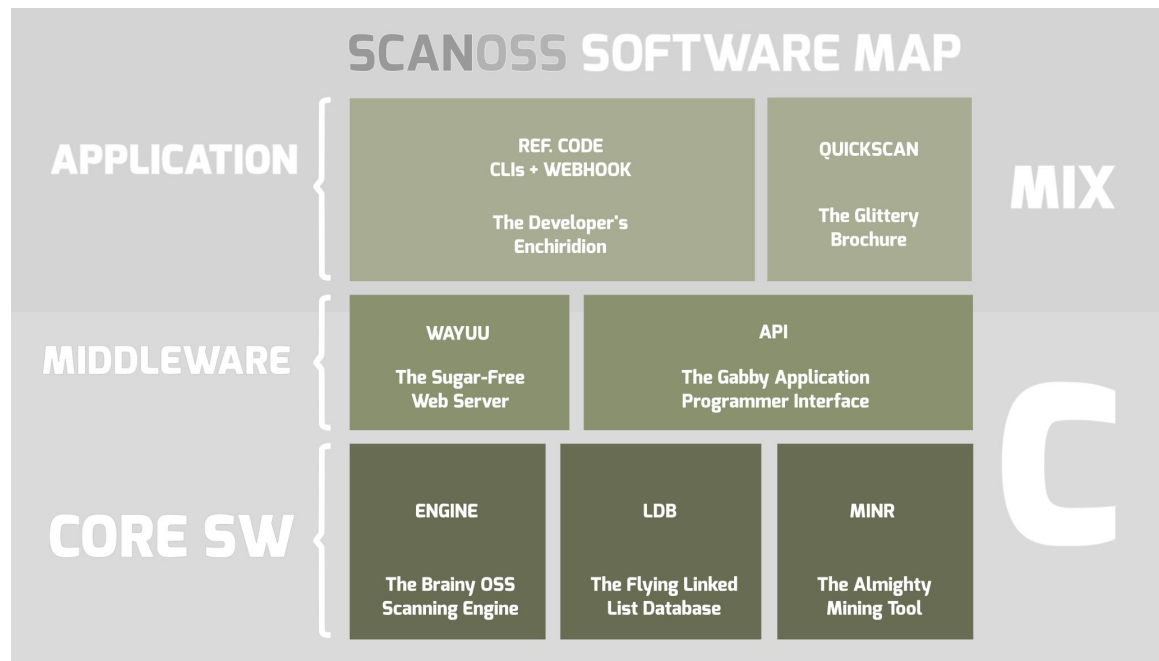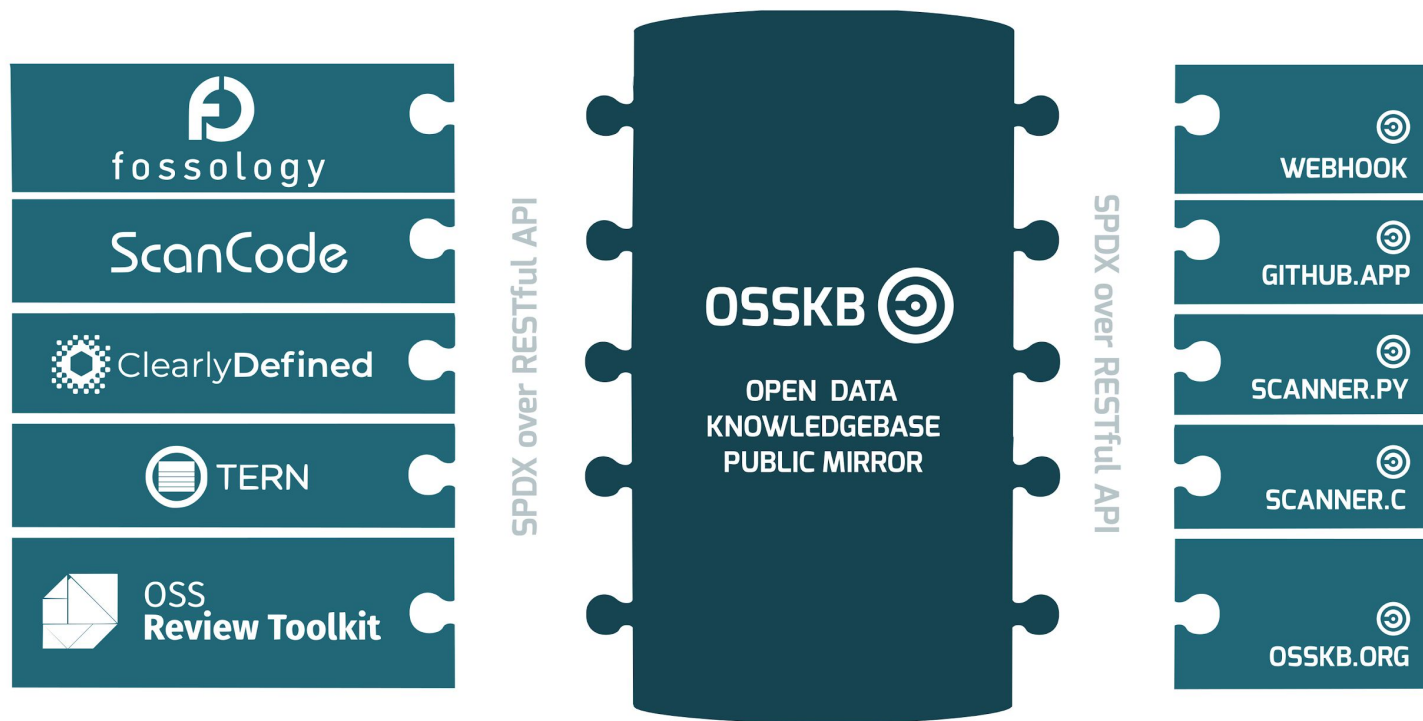
SPDX (RDF/XML)

Software contribution to the community

*https://github.com/scanoss
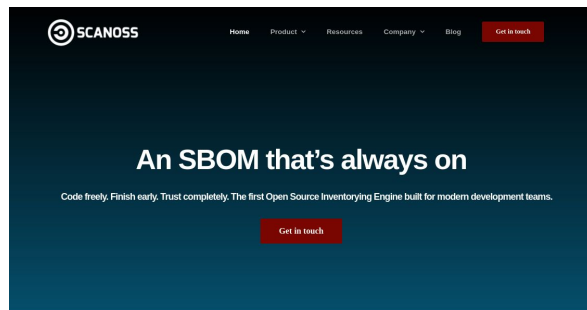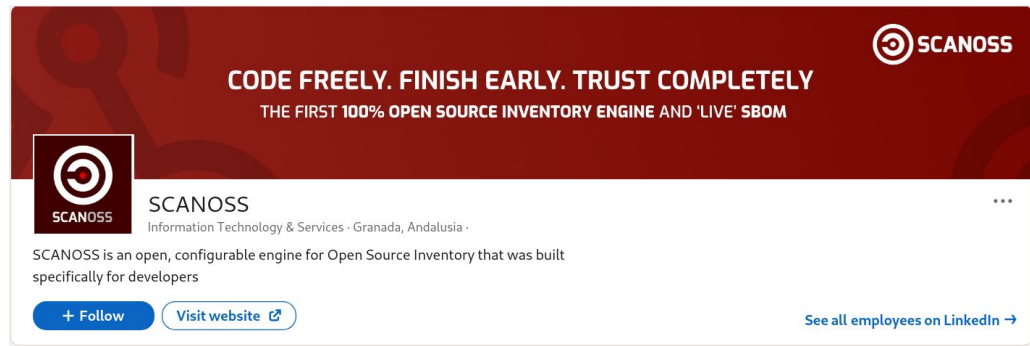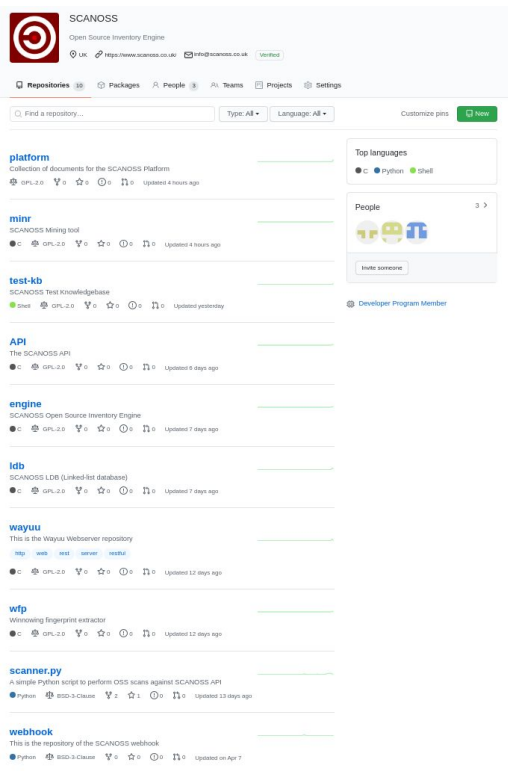
Bridging to the community

We're committed to being OPEN

- Non-profit organization
- Open governance model

- Opens sponsorship program
- Facilitates cooperation with other companies
- Facilitates community engagement

FOLLOW US, FORK, SHARE!

"Democratising Open Source
Risk Management"

Q&A