SBOM: Cyclone DX Generator vs Trivy

CycloneDX includes all the packages available in the GitHub repository that were used.

Trivy, on the other hand, only detects packages that have vulnerabilities and does not list all the packages. It also includes CVE information, and by using this CVE, we can fetch further details directly via the APIs that I have sent in QSekOps Channel.

In comparison, Trivy is considered better than the CycloneDX generator. Additionally, we can check for vulnerabilities in the CycloneDX-generated SBOM JSON using Trivy.

However, it's important to note that the results might be inaccurate when we use cyclone's SBOM json with Trivy, as Trivy has informed us about this limitation.

Both tools have the same language support, but **CycloneDX** supports **Erlang**.

SAST : SemGrep vs HoruSec

Horusec identifies some files that are not present in the Semgrep report, which are shown critical by Horusec.

Similarly, **Semgrep** reports more vulnerabilities that are not found in the files scanned by **Horusec**.

Based on the rule sets, both tools may detect different vulnerabilities, as **Horusec** includes some rules not present in **Semgrep** and vice versa.

Semgrep generates more findings than **Horusec**, but **Horusec** is not a complete subset of **Semgrep**.

Semgrep supports more programming languages than **Horusec**.

However, **Horusec** covers 3 areas that **Semgrep** does not: **Kubernetes**, **Shell**, and **Nginx**.

Even in the same file, **Semgrep** and **Horusec** may report vulnerabilities at different lines, sometimes for different vulnerabilities.

In some cases, both tools report the same issue. For example, **Semgrep** detects hard-coded credentials using GitLeaks, which is also detected by **CWE**.

Both tools provide reference links, but **Horusec** includes the reference URL along with details(Contains message and the link related to the vulnerability).

If we need to merge the reports, we can do so by cross-checking vulnerabilities based on the line number and filename present in both JSON files.

SAST VS SBOM : Trivy vs Semgrep and Horusec

Semgrep and Horusec do not provide any reports related to the packages that were used.

However, Trivy provides detailed reports, including the installed package version and its corresponding fixed version.

Also Trivy Provides Reference Links related to the packages.

Conclusion

While checking **Semgrep**, **Horusec**, **Trivy**, and **CycloneDX**:

We should use **Semgrep**, **Horusec**, and **Trivy**, as **CycloneDX** is covered by **Trivy**.

TOOLS USED

1.SemGrep

2.HoruSec

3.Cyclone DX Generator

4.Trivy SBOM