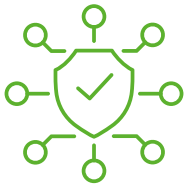
CYBER RESILIENCE ACT

IM PILOTPROJEKT VERWENDETE TOOLS.



Technologie-Stack des Piloten

- **Visual Studio** (kommerziell)
- **Azure DevOps** (kommerziell)
  https://azure.microsoft.com/
  Wird u.a. für die CI/CD Pipeline zur automatischen Erstellung des HMIs und der dazugehörigen SBOM genutzt.

SBOM Erstellung / Visualisierung

- **Syft** (Apache-2.0 License)
  https://github.com/anchore/syft
  Erstellt SBOMs
- **cyclonedx-dotnet** (Apache-2.0 License)
  https://github.com/CycloneDX/cyclonedx-dotnet
  Erstellt SBOMs
- **Sunshine** (Apache-2.0 License)
  https://github.com/CycloneDX/Sunshine/
  Visualisiert SBOMs

Threat-Modelling / Risiko- und Bedrohungsanalyse

- **OWASP Threat Dragon** (Apache-2.0 License)
  https://owasp.org/www-project-threat-dragon
  Verwendet zur Erstellung und Visualisierung von Bedrohungsmodellen.

Sicherheit der Lieferkette

- **grype** (Apache-2.0 License)
  https://github.com/anchore/grype
  Prüft die in einer SBOM angegeben Komponenten auf bekannte Schwachstellen
- **BOMnipotent** (kommerziell)
  https://www.bomnipotent.de/
  Hostet und verwaltet Dokumente rund um die Sicherheit der Lieferkette, z.B. Stücklisten (Bill of Materials), CSAF-Dokumente (Common Security Advisory Framework).
- **AUNOVIS Secure Sum** (MIT License)
  https://github.com/aunovis/secure_sum
  Bewertet eingebundene Pakete und kann auch zur Bewertung von Paketen verwendet werden, die zukünftig eingebunden werden sollen. Ruft intern OSSF Scorecard auf.

WIR BEGEISTERN AUTOMATISCH.

AUNOVIS