Risikostyring af open source pakker i STAR

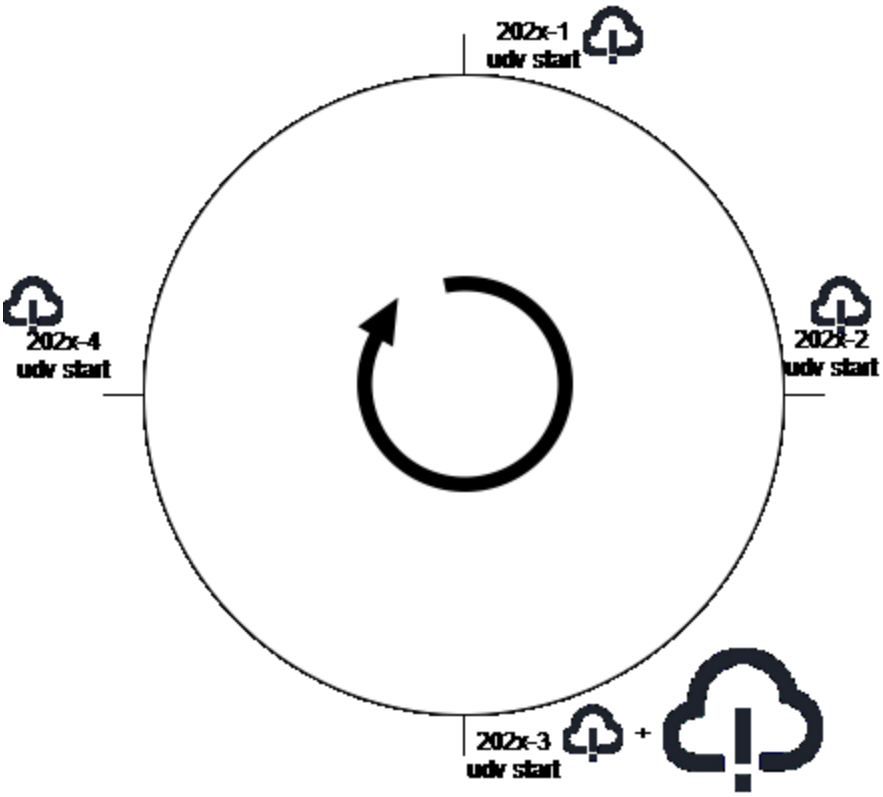
Baggrund

I STAR's systemer anvendes open source komponenter og frameworks. Denne side beskriver risikostyringsprocessen for brugen af open source pakker i STAR således at både STAR, Systemforvalter og udviklingsleverandører er afstemte omkring STARs forventning til risikohåndtering af open source komponenter og frameworks, der anvendes som en del af den leverede kode.

Kontekst:

Risikoanalysen opdeles i to niveauer som begge baserer sig på SIG's Open-source health metrikker. Eksempel for JobNet.

1. **Kvartalsvis**: Overordnet risikovurdering af eksisterende pakker udføres ved 1. sprint for hver hoved-release
2. **Årlig**: Bredere risikovurdering af eksisterende pakker (illustreret ved stort ikon herunder) udføres ved 1. sprint for 202x-3 hoved-release



Afgrænsning

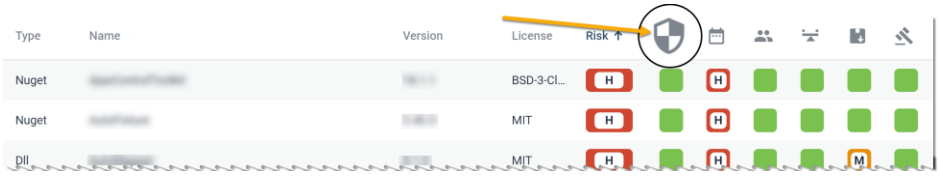
Open source pakker risikovurderes primært i forhold til nedenstående vektorer

- **Kendte sårbarheder**. Kendte sårbarheder i open source pakker udgør en sikkerhedsrisiko.
- **Support og community**. Support, vedligehold og udvikling af open source pakker er afhængige af et aktivt community.

Overordnet kvartals risikovurdering

I forbindelse med udviklingsstart af hver hovedrelease gennemgår Udviklingsleverandøren SIG's Open-source health metrikken for sårbarhed (Vulnerability) og identificerer

- de pakker, der har en High risk på Vulnerability



Pakker med kritiske sårbarheder (læs: HIGH risk) skal efter aftale med CPO og Systemforvalter umiddelbart opgraderes af Udviklingsleverandøren til en version uden kritiske sårbarheder. Hvis opgraderingen vurderes at have et "større" omfang aftales nærmere forløb.

For pakker med kritiske sårbarheder, der ikke umiddelbart kan opgraderes, skal risikovurdering og -håndtering ske i samarbejde mellem Udviklingsleverandøren, CPO og STAR's arkitektgruppe under hensyntagen til

- kritikalitet,
- kodebasens forholdsmæssige afhængighed af pakken,
- om pakken anvendes i produktionskode,
- forventet pris for opgradering eller migrering
- kompleksitet

Afrapportering

Til udførelse af risikovurderingen anvendes Confluence-skabelonen *"STAR City: Kvartalsvis risikovurdering af Open Source komponenter"*

Risikovurderingen gemmes på den interne del af STAR WIKI (fx under Udviklerhåndbøger) og afrapporteres på et møde med STAR's arkitekter.

Bredere årlig risikovurdering

I forbindelse med den årlige risikovurdering af systemer i STAR foretager Udviklingsleverandøren, **ud over den kvartalsvise overordnede risikovurdering**, også en bredere risikovurdering af anvendelsen af open source pakker i systemerne, herunder support og community. Baseret på

- udviklingen i pakker, der har en samlet High risk på tværs af SIG's Open-source health metrikker,
- udviklingen i det samlede antal pakker anvendt i systemet
- en vurdering af om der er enkelte pakker eller frameworks, som Udviklingsleverandøren anbefaler, at STAR af andre grunde foretager en grundigere risikovurdering af

STARs arkitektgruppe udarbejder på baggrund af vurderinger og anbefalinger fra udviklingsleverandørerne og med input fra Systemforvaltningen en plan for risikostyring og herunder forslag til eventuelle opgraderinger.

Afrapportering

Til udførelse af risikovurderingen anvendes Confluence-skabelonen *"STAR City: Årlig risikovurdering af Open Source komponenter"*

Risikovurderingen gemmes på den interne del af STAR WIKI (fx under Udviklerhåndbøger) og afrapporteres på et møde med STAR's arkitekter.

Ansvar og forankring

- STARs arkitektgruppe har ansvar for etablering og vedligeholdese af denne risikostyringsproces.
- Udviklingsleverandørerne har ansvar for at foretage risikovurderinger og udarbejde anbefalinger inden for deres eget systemansvarsområde.
- STARs arkitekturgruppe, CPO'er og Udviklingsleverandører håndterer i fællesskab de identificerede risici.

Kommunikation og godkendelse af risikohåndteringsplan

Den årlige risikovurdering af open source pakker og aftaler om håndtering og implementering af kontroller dokumenteres i en risikohåndteringsplan, som afrapporteres af STARs arkitekter til DOS' ledelse.

Der udarbejdes et resumé af den årlige risikovurdering til it-sikkerhedssekretariatet i STAR, som kan anvende den i forbindelse med it-sikkerhedssekretariatets årsrapport.