**Værdien af vores SAI-SDLC: Tryghed gennem industriel modenhed**

For en offentlig kunde er software ikke bare et værktøj, men en del af den kritiske infrastruktur, der forvalter borgernes retssikkerhed. Vores proces er designet til at adressere netop dette ansvar.

**1. Radikal gennemsigtighed (Ingen "Sort Boks")**

Mange frygter, at AI træffer beslutninger på et uigennemsigtigt grundlag.

* **Værdi for kunden:** Gennem vores faste brug af **SHAP/LIME** og **Model Cards** får kunden fuld indsigt i, hvilke parametre der vægter i en afgørelse. Det betyder, at sagsbehandleren altid kan forklare en borger, *hvorfor* systemet foreslår en bestemt handling. Det sikrer den menneskelige kontrol, som lovgivningen kræver.

**2. Økonomisk ansvarlighed via FAIR**

Traditionel sikkerhed handler ofte om mavefornemmelser.

* **Værdi for kunden:** Ved at anvende **FAIR-metoden** omsætter vi it-risici til kroner og ører. Vi kan præsentere kunden for et beslutningsgrundlag, der siger: *"Denne sårbarhed koster potentielt 2 mio. kr. i tabt omdømme, derfor prioriterer vi den nu."* Det giver kunden vished for, at deres budget bruges der, hvor det gør den største forskel for sikkerheden.

**3. "Audit-Ready" fra dag ét**

Revision og tilsyn fra myndigheder (fx Digitaliseringsstyrelsen eller DNV) kan være en tung proces for kunden.

* **Værdi for kunden:** Fordi vores Azure DevOps-miljø automatisk kobler krav, risikovurdering, kodestandard (SEI CERT Java) og testresultater, er dokumentationen altid klar. Kunden skal ikke bruge uger på at indsamle beviser til en ITGC- eller GDPR-erklæring; de kan blot få udleveret en eksport af vores sporbarhedsmatrix.

**4. Overholdelse af kommende lovgivning (EU AI Act)**

AI-lovgivningen er i hurtig udvikling.

* **Værdi for kunden:** Vores SDLC bygger direkte på **ISO 42001**, som er den standard, EU AI Act i høj grad læner sig op ad. Ved at vælge denne model er kunden ikke blot compliant i dag, men er også på forkant med de krav, der bliver obligatoriske i de kommende år. Det beskytter kundens investering mod pludselige lovkrav.

**5. Sikkerhed uden hastighedstab**

Mange frygter, at tunge sikkerhedskrav bremser udviklingen.

* **Værdi for kunden:** Vores brug af **Security Champions** og automatiseret scanning betyder, at sikkerheden "bygges ind" i stedet for at "klistres på" til sidst. Kunden får hurtige leverancer, men med den indbyggede garanti for, at hver eneste linje kode er tjekket mod de højeste internationale standarder.

**Den skarpe "Elevator Pitch" til kunden:**

*"Vi leverer ikke bare en AI-model; vi leverer en industriel og revisionssikker fabrik. Med vores SAI-SDLC får I en løsning, hvor etik er kvantificeret, sikkerhed er automatiseret, og hvor enhver beslutning kan forklares til både borgere og revisorer. I køber ikke bare software – I køber ro i maven over for jeres digitale ansvar."*

| **KOMBIT Princip** | **Beskrivelse** | **Hvordan SAI-SDLC opfylder det** |
| --- | --- | --- |
| **P1-3: Relevans & Værdi** | AI skal skabe værdi og have et klart formål. | **Forretningssporet (3 mdr.)** screener alle Epics mod disse mål, før de prioriteres i backloggen. |
| **P4-5: Lovlighed & Retssikkerhed** | Skal overholde gældende ret og borgernes rettigheder. | **FAIR-risikovurderingen** kvantificerer juridiske risici, og **ASVS-kontroller** sikrer teknisk efterlevelse. |
| **P6: Gennemsigtighed** | Det skal være tydeligt, hvordan AI anvendes. | **Model Cards** dokumenterer modellens opførsel, og **XAI (SHAP/LIME)** forklarer de specifikke output. |
| **P7-8: Bias & Diskrimination** | Modvirke utilsigtede forskelle i output. | **SHAP/LIME-valideringen** i pipelinen overvåger løbende feature-vægtning for at spotte proxy-bias. |
| **P9-10: Menneskelig kontrol** | AI må aldrig stå alene i en afgørelse. | Vores **Security Champions** og **Definition of Done** sikrer, at der altid er indbygget "human-in-the-loop" i kritiske flows. |
| **P11: Datasikkerhed** | Beskyttelse af borgernes data. | **ISO 27001**, **SEI CERT Java** og automatiseret **PII-maskering** i alle logs jf. OWASP standarder. |
| **P12-13: Datakvalitet** | Data skal være korrekte og repræsentative. | **Open Metadata** og **CycloneDX (ML-BOM)** sikrer fuld sporbarhed (proveniens) af træningsdata. |
| **P14: Forklarlighed** | Beslutninger skal kunne forklares. | **XAI-rapporter** og tekniske Model Cards oversættes til forståelig information i løsningens UI. |
| **P15: Placeret ansvar** | Der skal altid være et entydigt ansvar. | Vores **Account Security Manager (ASM)** og den uafhængige **revision** sikrer en klar audit-trail for alle beslutninger. |