OBOS S-SDLC og veien til et Security Champions program

Hans Ove Ringstad // OBOS
Sarmilan Gunabala // Bekk

OBOS

OBOS er mer enn du tror

Norges største boligutbygger
Stor boligutbygger i Sverige
Næringseiendom
OBOS Bank
OBOS Eiendomsmeglere
Boligforvaltning
Hammersborg inkasso
OBOS OpenNet
og enda mer …

Sikkerhetsteamet i OBOS konsernet

	GRC	Rådgivning og støtte	IAM	OBOS SOC
FOKUS	Styre, Ha oversikt	Beskytte	Ha oversikt, Beskytte	Detektere, Håndtere
MENNESKER	**Informasjonssikkerhetsleder**	**Informasjonssikkerhetsrådgiver**	**IAM ansvarlig**	**SOC ansvarlig**

TJENESTER	› Styrende dokumenter (sentrale krav og føringer) inkl. oversikt over lover og regler
	› Overordnet risiko- og trusselbildet
	› Veikart for informasjonssikkerhet inkl. oppfølging og løpende vurdering
	› Opplæring- og bevisstgjøring
	› Strategisk rådgivning
	› Rapportering
		› Rådgivning og støtte til org. enheter (inkl. enheter i IT og digital) i deres arbeid med å operasjonalisere og etterleve føringer i styringssystemet:
		  › Generell rådgivning
		  › Verdivurdering
		  › Penetrasjonstest
		  › Sikkerhetsrevisjon
		  › Sentrale prosedyrer, instrukser, veiledere og arkitekturmønstre
		  › mv.
			› Privilegerte identiteter og tilganger
			› Arbeidsstyrke (ansatte og innleide) identiteter og tilganger
			› Forbruker (kunder og medlemmer) identiteter og tilganger
				› Sikkerhetsovervåkning
				› Hendelseshåndtering og -koordinering
				› Trusseletterretning
				› «Vulnerability management»

Produkt-/utviklingsteam i OBOS

Data	Interne tjenester	Kundetjenester
CRM/Marketing	Legacy	Medlem
BI/Datavarehus	ERP	OBOS-appen
	Integrasjon	Nettsted
	Tjenesteplattform	Forkjøp
	Automatisering	Nærkontoret
		Boligjakten
		Homerun
		Styrerommet
		Vibbo
		OBOS-nøkkel
		Living Lab

~150 teammedlemmer

OBOS’ krav til sikkerhet er grunnleggende

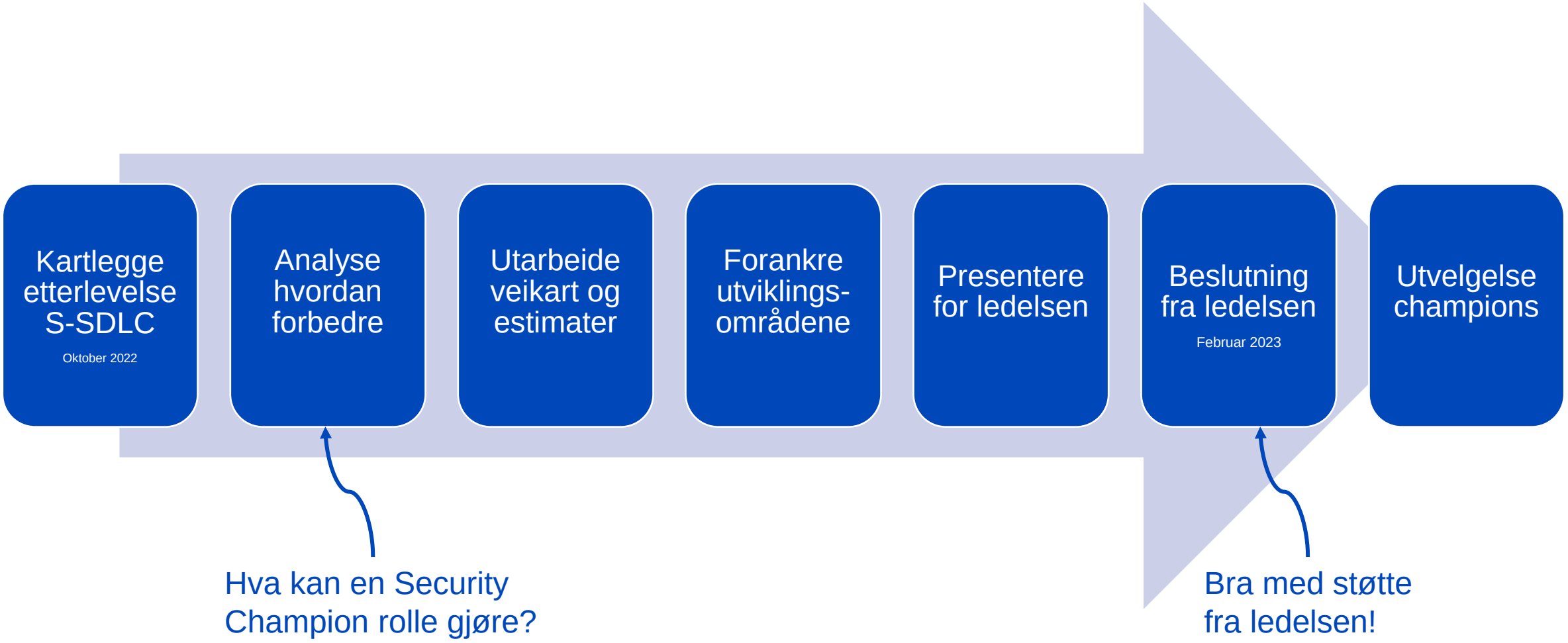
Hva er sikkert nok for OBOS? Hva må vi gjøre for å være så sikre som vi ønsker å være?

- Informasjonssikkerhetspolicy for OBOS-konsernet
- Krav til sikker administrasjon av informasjonsverdier
- Krav til sikker innføring, oppgradering og utvikling av IT-systemer (OBOS S-SDLC)
- Krav til sikker drift av IT-systemer og –infrastruktur
- Krav til teknisk beskyttelse av informasjonsverdier og digital kommunikasjon
- Krav til identitets- og tilgangskontroll (IAM)
- Krav til passord (passordstandard for OBOS)

OBOS S-SDLC


Konsekvens-/verdivurdering
Ansvars-/rollefordeling
Endringskontroll
Identifikasjon sikkerhetskrav og -tiltak
Sikkerhetsrisikovurdering
Trusselmodellering
Kodegjennomgang/SAST
Kontroll 3.partskode/SCA
Dynamisk sikkerhetstesting/DAST
Penetrasjonstesting

Etablering av OBOS Security Champions



Verdiforslaget for OBOS Security Champions

- Skaper en ny ressursgruppe for å etterleve S-SDLC
- Gir oss et forum for å hjelpe hverandre på sikkerhet
- Gir økt kompetanse på sikkerhet i teamene
- Gjør at sikkerhetsoppgaver kommer i backlog
- Bedre samarbeid med oss i sikkerhetsteamet
- Øker sikkerheten for OBOS

→ Operasjonalisere OBOS S-SDLC

Sikkerhetsteamets rolle i programmet

→ Drive Security Champions programmet

Hva skal en Security Champion i OBOS være

- [x] En i teamet som både kan og har tid til å ta på seg oppgaver i OBOS S-SDLC
- [x] En som ønsker å lære om mer sikkerhet
- [x] En som ønsker å hjelpe andre med sikkerhetsoppgaver

Konkrete oppgaver Sarmilan gjør

- Risikoanalyser ved nye features
- Poster på #sikkerhet på Slack ved store og små oppdateringer
- Holder i sikkerhetsrelaterte saker ved for eksempel pen.test
- Beredskapsplan
- Prioritere opp mot forretningens ønsker
- Jobber en del med å knytte sammen sikkerhetsavdelingen og utviklerne

Lærdom så langt

☹ Utfordrende å få folk til å faktisk prioritere oppgavene som følger med rollen

☹ Fellesmøter ikke så produktive fordi teamene jobber så forskjellige

☹ Markedsføring av programmet

😳 Skulle ønske at det var mer selvgående

😊 Konkrete oppgaver hjelper med å forklare hva vi skal få til

😊 Forankring i ledelsen essensielt for OBOS

😊 Utholdenhet og kontinuitet er viktig

Veien videre

- ✨ Utvide antall champions og aktiviteter
- ✨ Enda mer kompetanseutvikling på sikkerhet
- ✨ Bedre verktøystøtte
- ✨ Øke verdsettelsen av sikkerhet hos teamene

Takk for oss!

hans.ove.ringstad@obos.no

sarmilan.gunabala@bekk.no