Trusselmodellering ved bruk av skytjenester

Håkon Nikolai Stange Sørum
Principal Security Architect
+47 902 63 400 | hakon@o3c.no

Sikkerhetsfestivalen
29.08.2023

O3 CYBER

To guide the global community toward a more secure utilization of cloud technologies

HVA ER TRUSSELMODELLERING?

HVORDAN GJØR MAN DET?

HVA ER FORSKJELLEN NÅR MAN TRUSSELMODELLERE SYSTEMER SOM BENYTTER SEG AV SKYTJENESTER?

AGENDA

01

- BAKGRUNN

02

- ANGREPSPRIMITIVER

03

- CONTROL PLANE
- MANAGEMENT PLANE
- DATA PLANE

04

- HVORDAN GJØR VI SKY I VÅR ORGANISASJON?

05

- HELHETLIG TRUSSELMODELLERING

06

- OPPSUMMERING

Bakgrunn

Trusselmodell

En forenklet representasjon av alle de potensielle årsakene til uønskede hendelser som kan skade våre verdier

Trusselmodellering

En mer eller mindre strukturert prosess for å analysere arkitekturen eller designet til et system for å avdekke disse potensielle årsakene.
Kartlegger design- og arkitekturfeil på bakgrunn av analysen.

Hvorfor

Fremmer kvalitet i systemutvikling, muliggjør innebygd sikkerhet og bygger sikkerhetskultur.

Hvordan

Skap felles forståelse for arkitekturen.
Forstå verdiene i systemet.
Diskuter mulige uønskede hendelser og deres potensielle årsak.
Lag sikkerhetskontroller som fjerner eller reduserer muligheten for at de inntreffer.

Angrepsprimitv

“En konfigurasjonstilstand som kan misbrukes under visse forhold, men som ikke er en implentasjonsfeil”

1. Billigere for en angriper
2. Blir ikke patchet
3. Vanskelig å oppdage

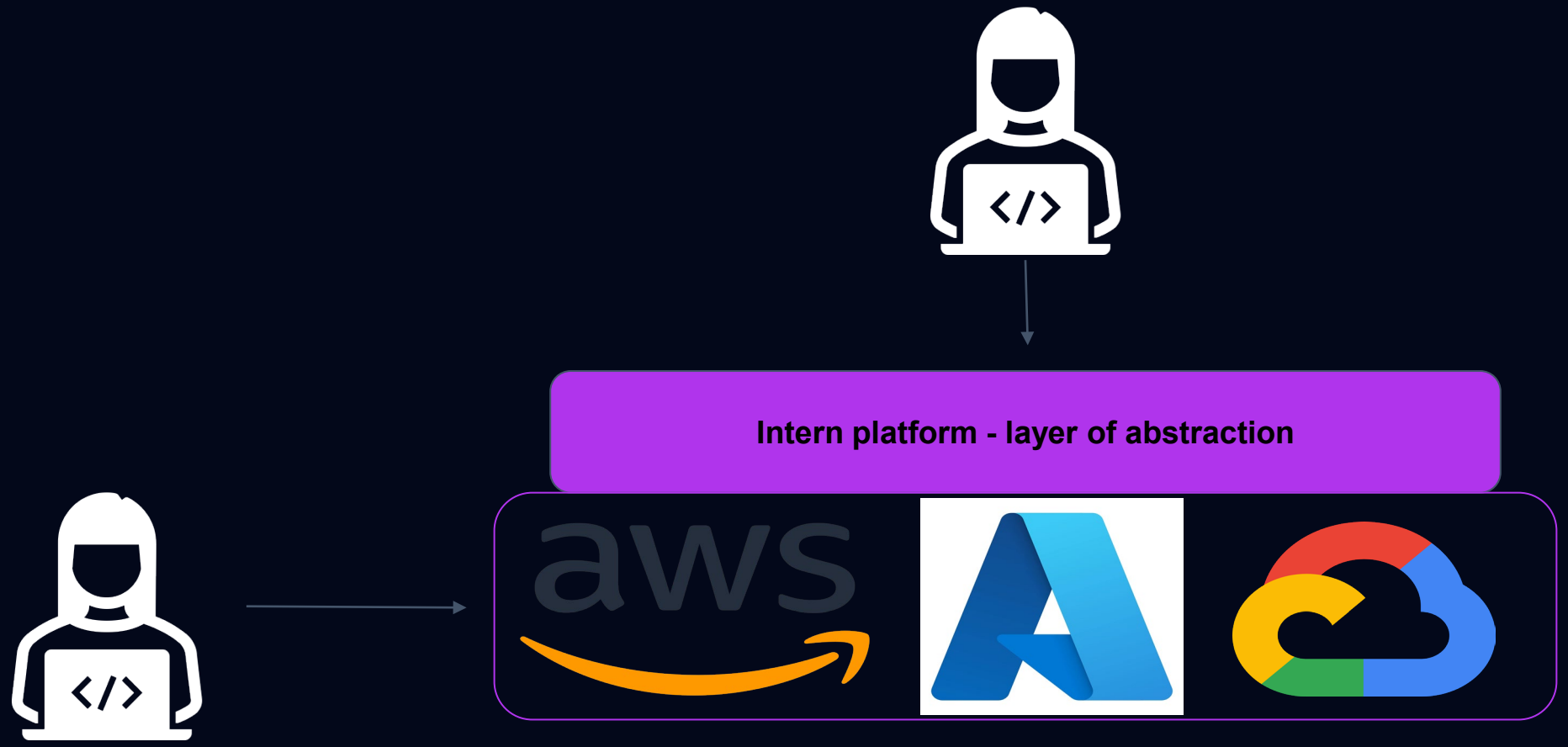
Control plane, Management plane, og data plane

Control plane
Sentraliserte sikkerhetskontroller:
- **Tilgangstrying**
- **Nettverkskontroll**

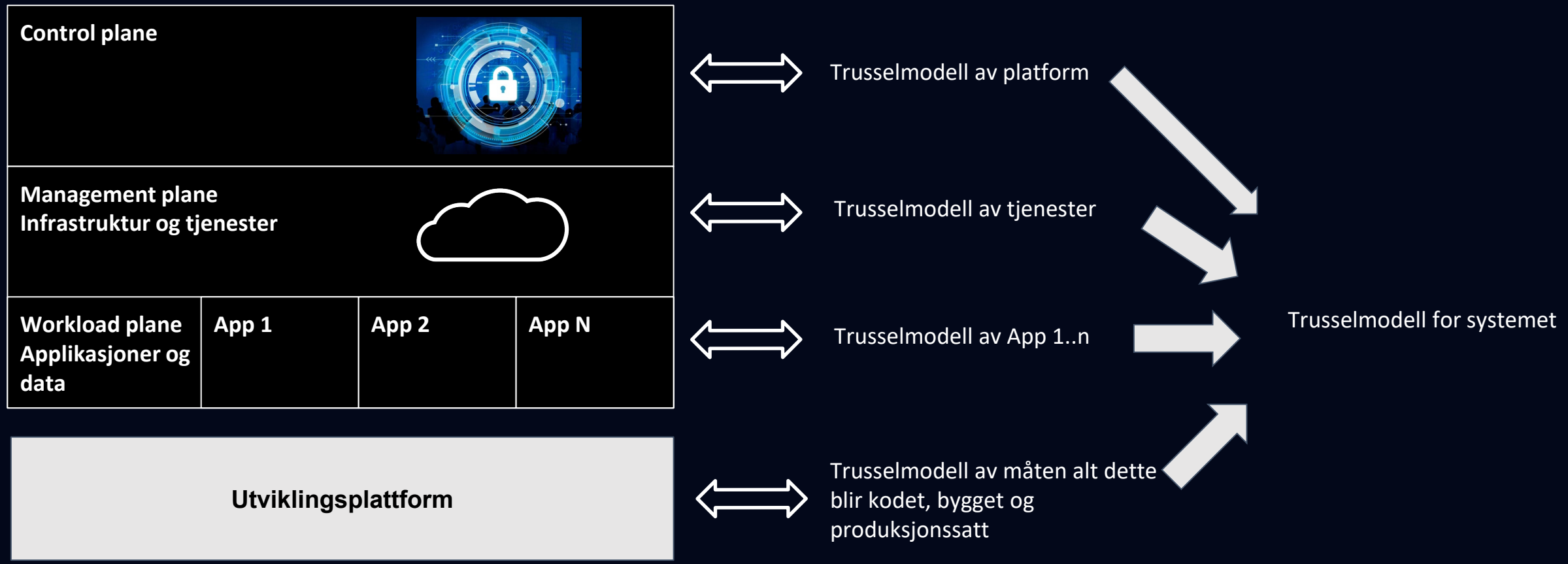
Management plane
Drift av infrastruktur og tjenester

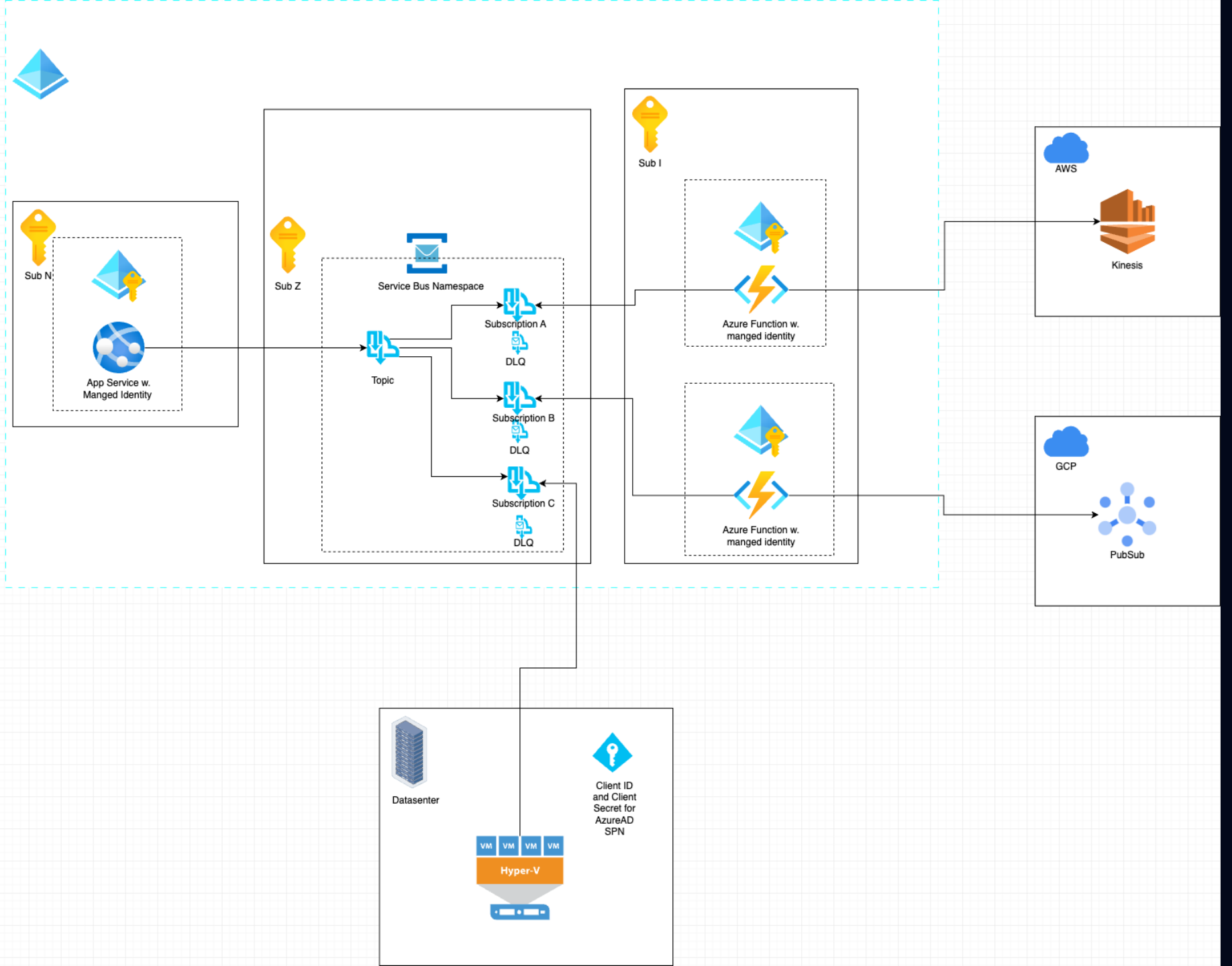
Workload plane **Applikasjoner og data**	**App 1**	**App 2**	**App N**	

Hvordan gjør du sky?



Helhetlig TM




Sub N
App Service w.
Manged Identity
Sub Z
Service Bus Namespace
Topic
Subscription A
DLQ
Subscription B
DLQ
Subscription C
DLQ
Sub I
Azure Function w.
manged identity
Azure Function w.
manged identity
AWS
Kinesis
GCP
PubSub
Datasenter
Client ID
and Client
Secret for
AzureAD
SPN
VM
VM
VM
VM
Hyper-V

Annerledes

Krever kunnskap om potensielle årsaker i skyen
Lag med abstraksjoner og ny dynamikk i tjenesteleveranse

Domenekunnskap

Bruk av native funksjoner i offentlige skytjenester
Fundamentale forskjeller påvirker angrepsveier
Kode skrevet internt med mulige feil

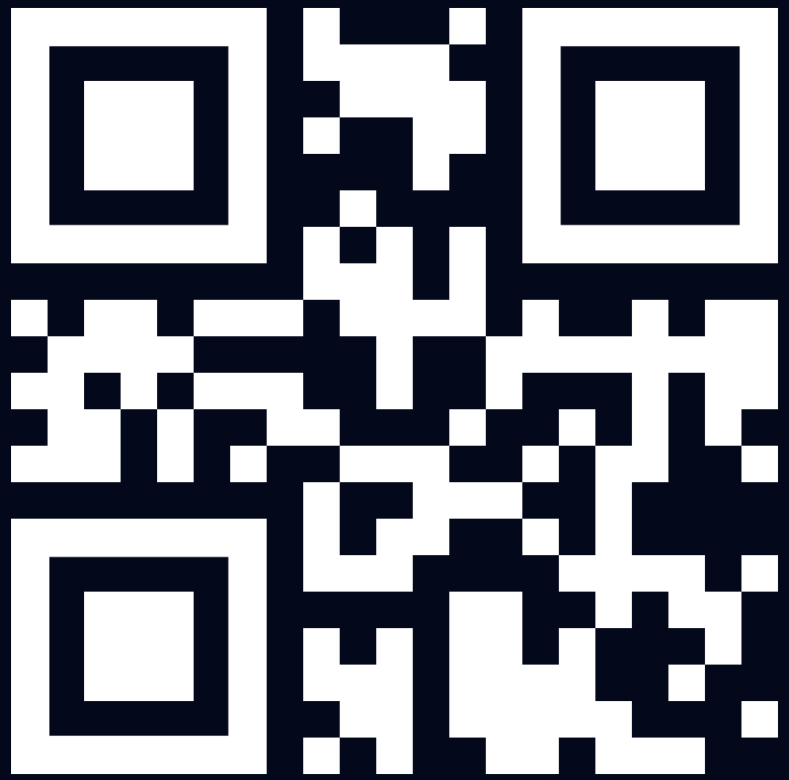
Utfordrende

Din modell kan endre seg som følge av endringer i underliggende tjenester
Trusselmodellering er utfordrende allerede - enda mer komplekst nå

Delt ansvar

Hvem har ansvar for å vedlikeholde modellen for de forskjellige abstraksjonslagene?
Hvem har mandat og eller ansvar for å faktisk utbedre sårbarhetene?

hakon@o3c.no



O3C.NO