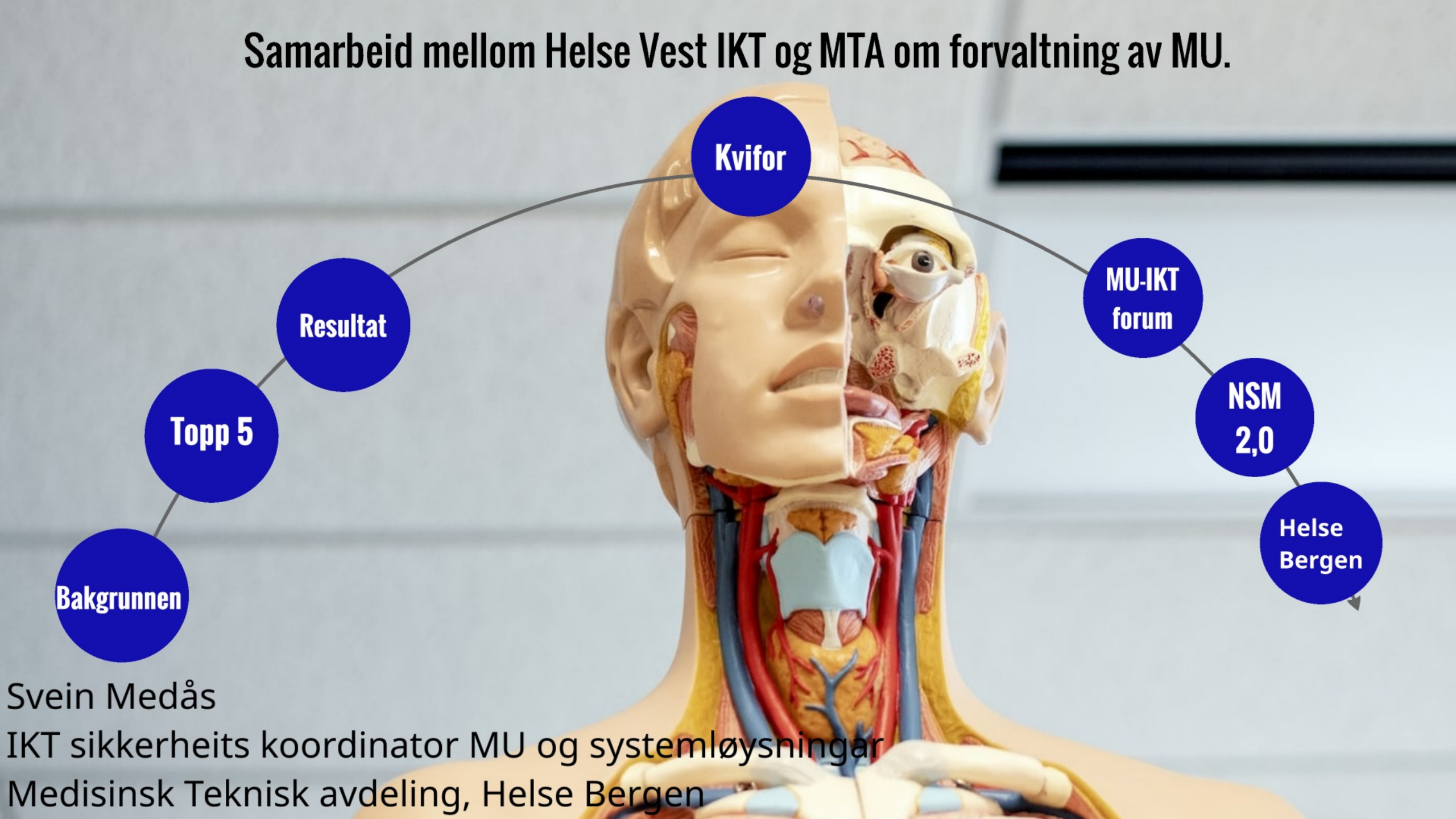
Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen

Bakgrunnen til prosjektet

Bakgrunnen til prosjektet

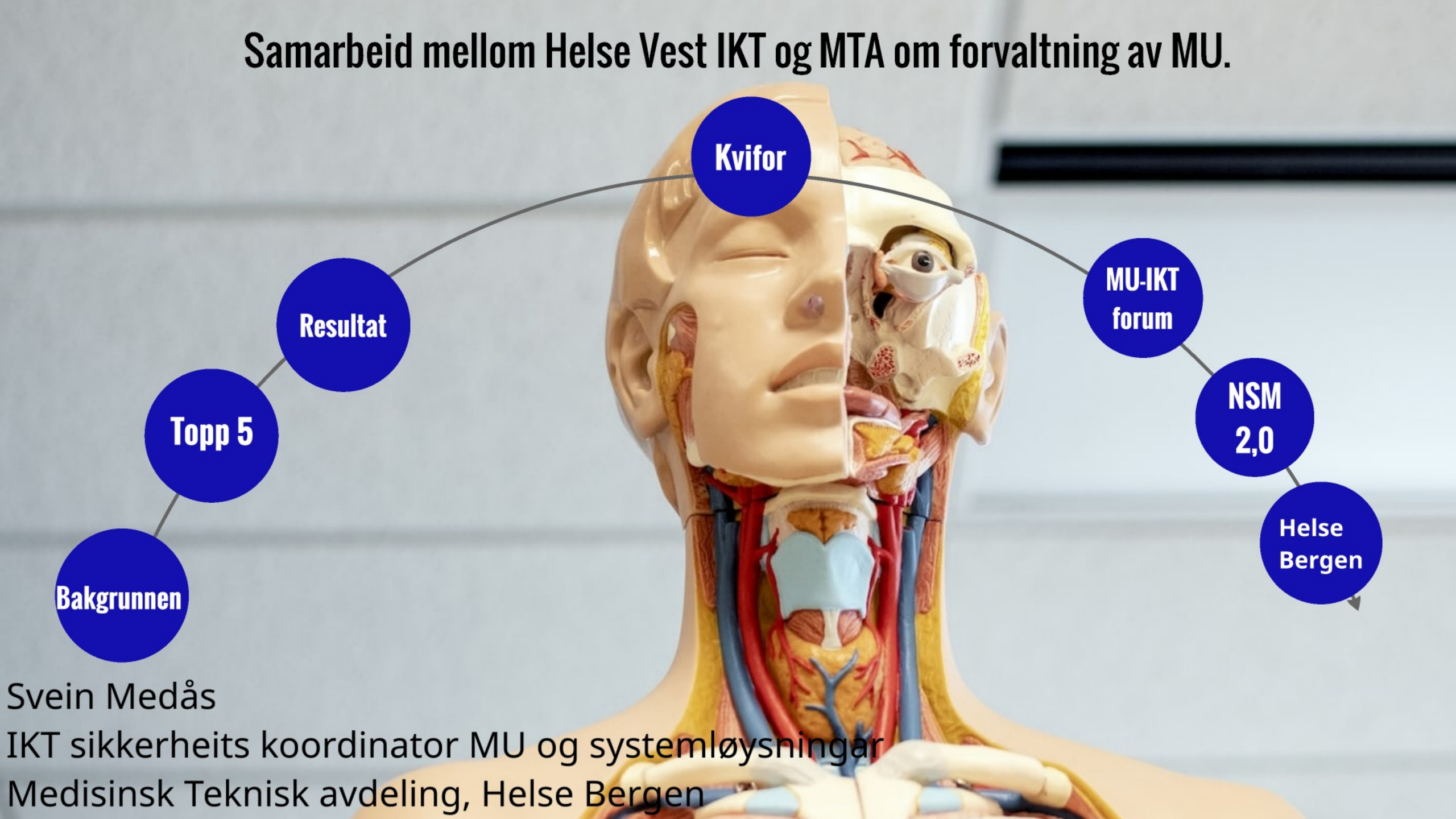
Riksrevisjonsrapport 2014-2015

Bakgrunnen til prosjektet

Riksrevisjonsrapport 2014-2015

Riksrevisjonsrapport 2020-2021

Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen

Informasjonsikkerheit prosjekt i Helse Vest RHF

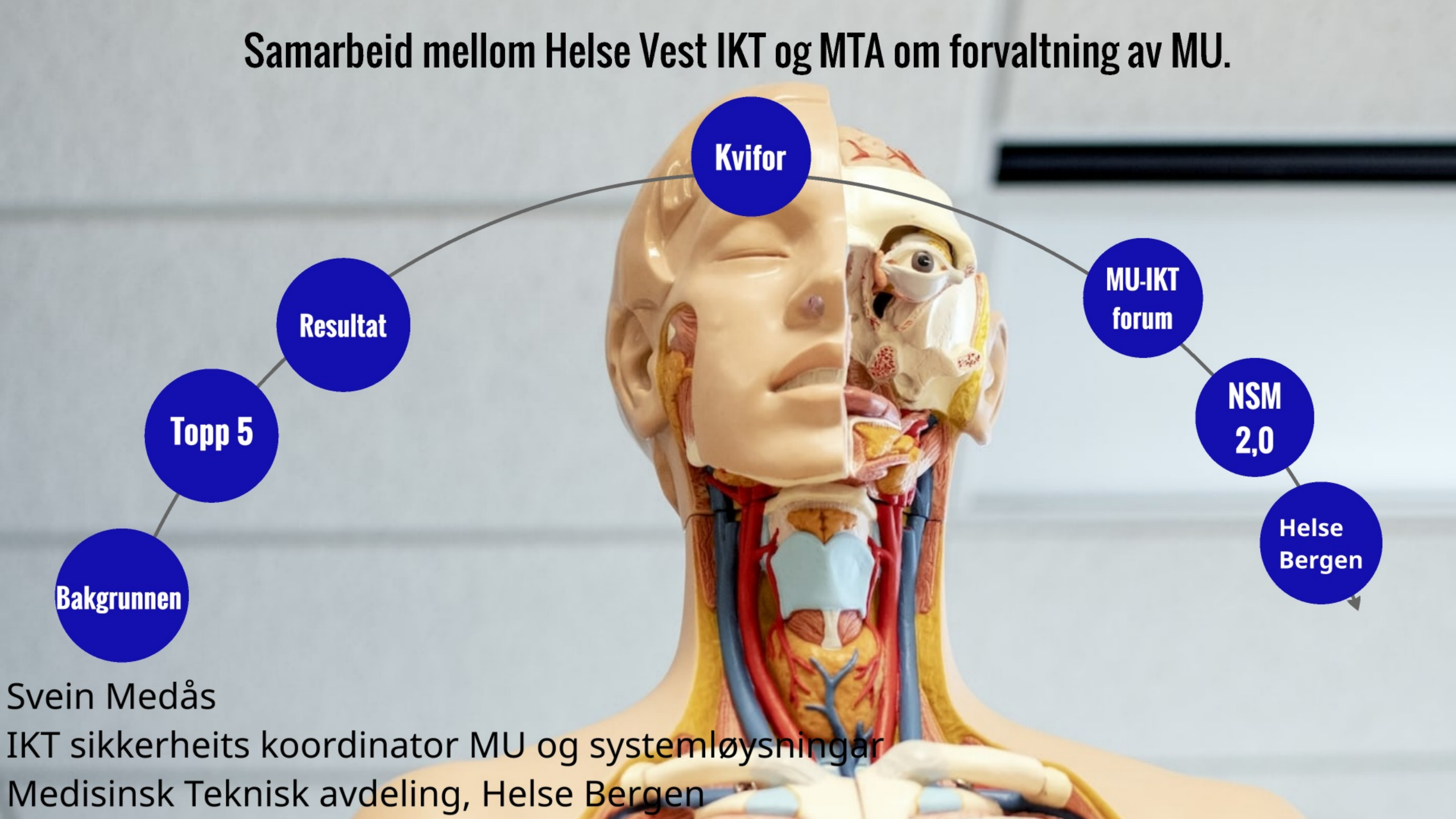
6 stk

1. Felles tilnærming til NSM 2.0.
2. Informasjonssikkerhet som del av virksomhetsstyringen.
3. Videreutvikling av sikkerhetskultur.
4. Tiltak for IKT-sikkerhet i regi av Helse Vest IKT.
5. Felles tiltak for økt IKT-sikkerhet for MU og TU
6. Tiltak for økt IKT-sikkerhet for lokal IKT

Informasjonsikkerheit prosjekt i Helse Vest RHF

6 stk

Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen

Resultat av kartlegginga

MU

MTA driftar både fysiske og virituelle servarar

MTA driftar pc og brukarar

MTA har domene med ein vegs trust mot AD

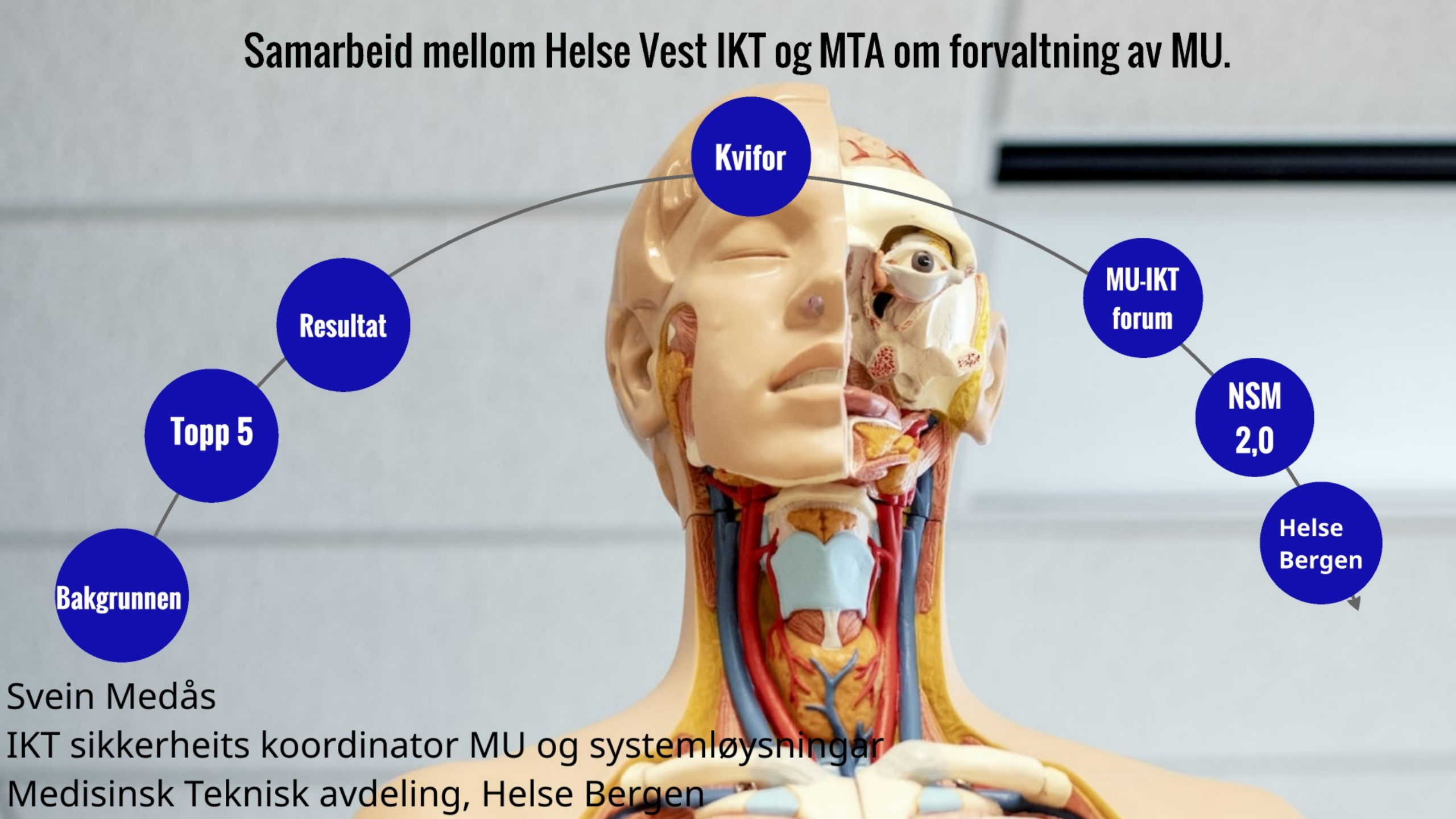
MTA leverer tjenester til andre HF i regionen

Alle hadde system som var drifta i samarbeid mellom HF, leverandør og Helse Vest IKT i ukjent ansvarsforhold

Resultat av kartlegginga

MU

Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen

Kvifor skjedde dette.

Helse Vest IKT har prioritert stordrift og standarisering og har lykkast med dette på mange områder.
MU og TU er områder der dette er problemfylt pga sertifisering, godkjenning, CE merking, levetid, utviklingsalder....

Lokal IKT

Lokal IKT

Helse Bergen

Medisinteknisk Avdeling
60+ systemer, 60 servere, 200 klienter, 110 brukere
Laboratorieklinikken
Ca. 35 servere og klienter
Drift/teknisk divisjon
Bygg og infrastruktur
Radiologisk avdeling
Forskning og opplæring
Avdeling for kreftbehandling og medisinsk fysikk
Systemer knyttet til stråleterapi
FoU-avdelingen
Virksomhetsstyring, forskning og opplæring
Kvalitetsregistre
Analyse og rapportering

Skygge IT

Dropbox, Facebook, WhatsApp, Google Apps, …
PC/Mac uten forvaltning

Lokal IKT

Som ein stor norsk bedrift

Helse Bergen

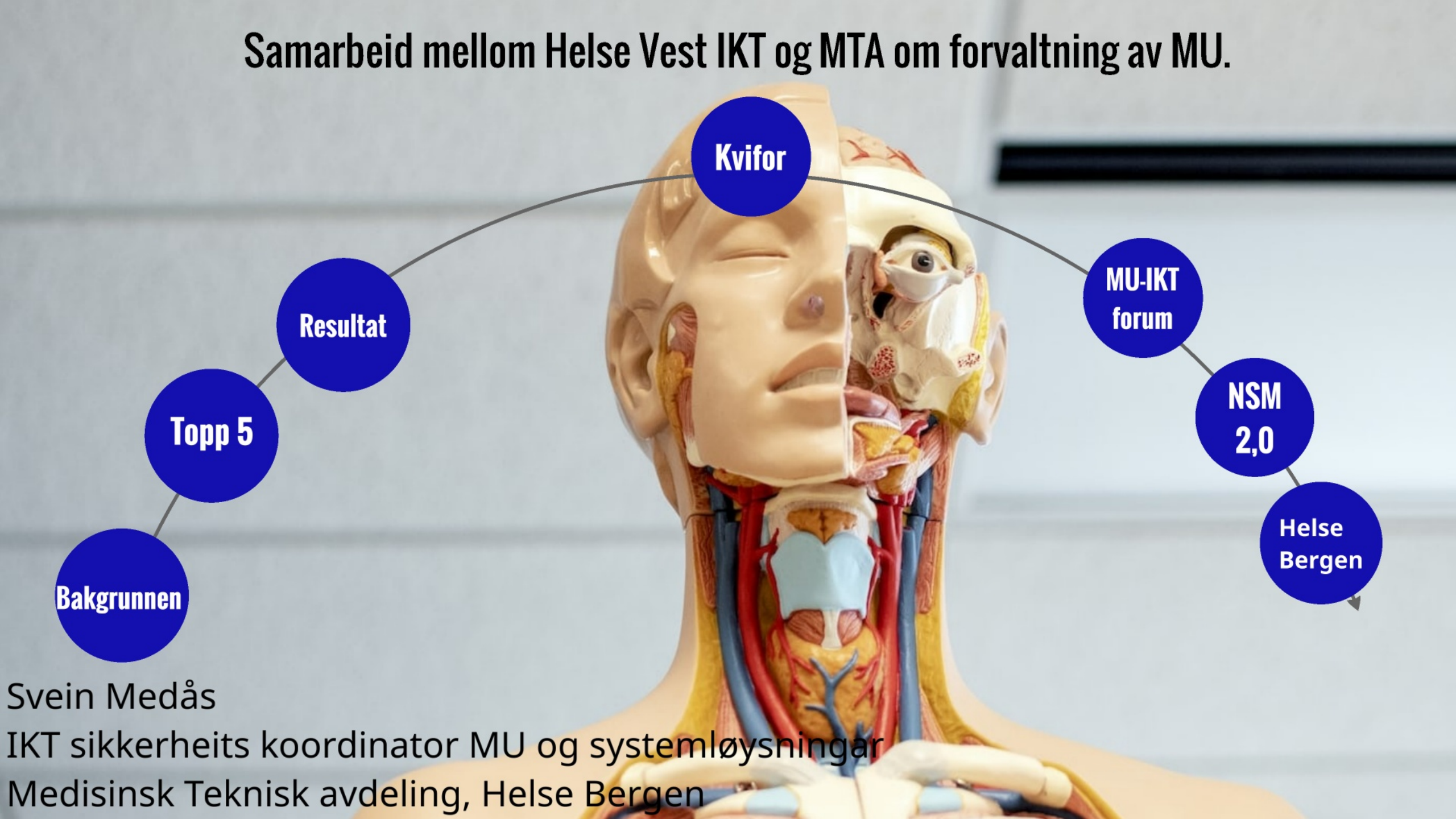
Medisinteknisk Avdeling
60+ systemer, 60 servere, 200 klienter, 110 brukere
Laboratorieklinikken
Ca. 35 servere og klienter
Drift/teknisk divisjon
Bygg og infrastruktur
Radiologisk avdeling
Forskning og opplæring
Avdeling for kreftbehandling og medisinsk fysikk
Systemer knyttet til stråleterapi
FoU-avdelingen
Virksomhetsstyring, forskning og opplæring
Kvalitetsregistre
Analyse og rapportering

Skygge IT

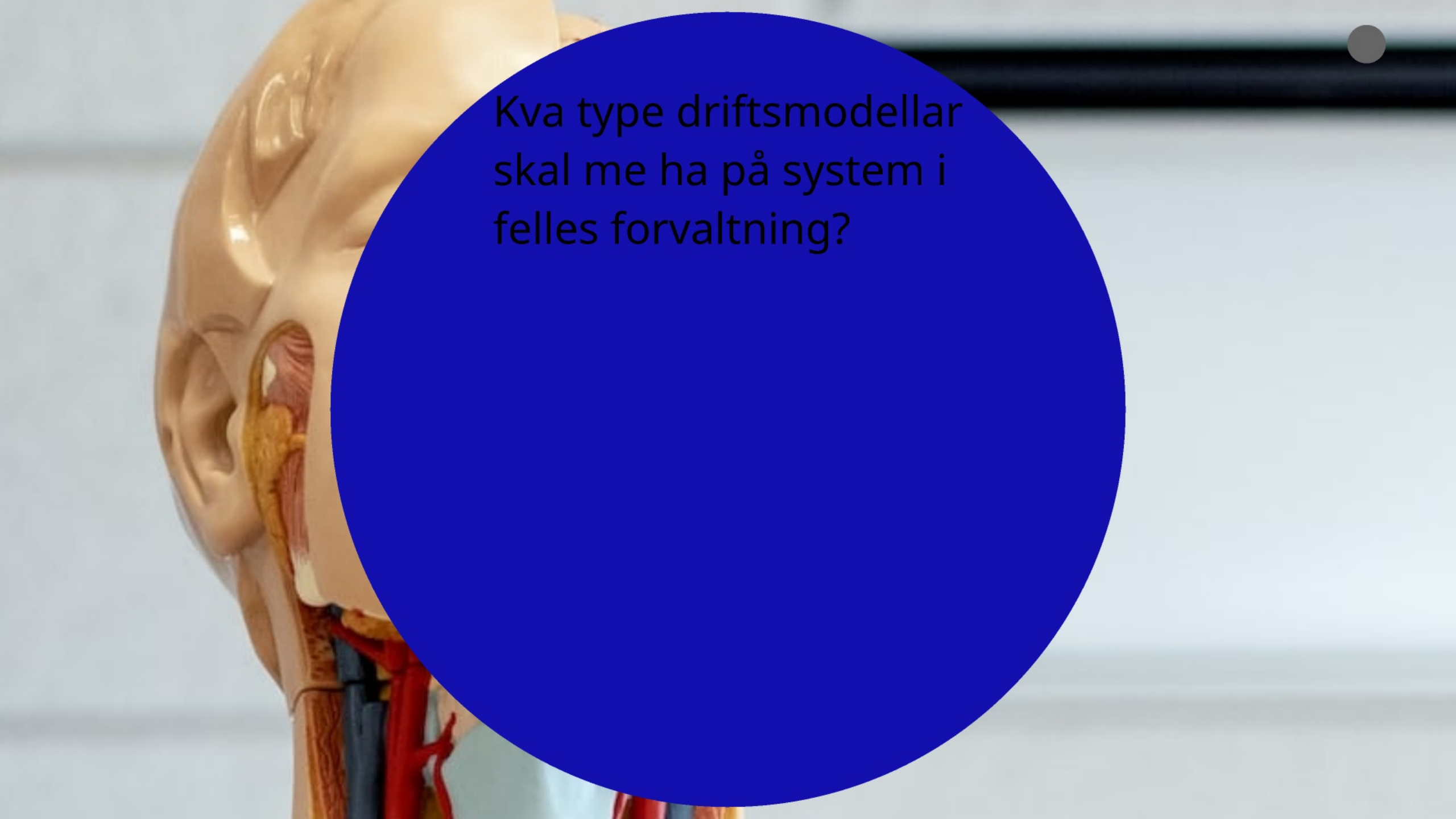
Dropbox, Facebook, WhatsApp, Google Apps, …
PC/Mac uten forvaltning

Kvifor skjedde dette.

Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen



Kva type driftsmodellar skal me ha på system i felles forvaltning?

Kva type driftsmodellar skal me ha på system i felles forvaltning?

saas-1	saas-2	saas-3	PaaS-1	Paas-2	Paas-3	IaaS-1	Iaas-2	NaaS	Separat HF-nett
App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv
Klient App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift
Klient App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.
Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift
Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon
OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift
OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon
Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)
Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup
Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk
Fysisk lokasjon m/strøm/kjøling/vann og fastmontert kabling									

Kva type driftsmodellar skal me ha på system i felles forvaltning?

saas-1	saas-2	saas-3	PaaS-1	Paas-2	Paas-3	IaaS-1	Iaas-2	NaaS	Separat HF-nett
App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv
Klient App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift
Klient App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.
Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift
Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon
OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift
OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon
Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)
Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup
Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk
Fysisk lokasjon m/strøm/kjøling/vann og fastmontert kabling									

Helse Vest IKT

Kva type driftsmodellar skal me ha på system i felles forvaltning?

HF

saas-1	saas-2	saas-3	PaaS-1	Paas-2	Paas-3	IaaS-1	Iaas-2	NaaS	Separat HF-nett
App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv
Klient App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift
Klient App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.
Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift
Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon
OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift
OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon
Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)
Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup
Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk
Fysisk lokasjon m/strøm/kjøling/vann og fastmontert kabling									

Helse Vest IKT

Ansvarsmatrise Viewpoint

Hoved Aktivitet	Delaktivitet	Sysemeier	Sysemansvarlig	Medisinsk Teknisk Avdeling	Nærmeste leder	Bruker	Sysemansvarlig-forum	Sysemforvalter	Kundesenter	Server og lagring	Klientdrift	Kommunikasjon	Leverandør
Modalitet	Konfigurering på modalitet				U								r
	Lage AE-tittel				U				I				
	Opprette ressurs			Iu	U								
	Konfigurering på server			U	Iu								r
	X-Tray				IU								
	Viewpoint			U	Iu			B					u
	Feilsøking			u	U		I						ru
	Koble opp i nettverk			I	U				I				
Applikasjonsforvaltning													
	Avtale- og lisensadministrasjon		B	U					I				
	Leverandørkontakt og -oppfølging			U					u				
	Overvåking av feil og problemer			u					U				
	Feilsøking og -retting			uI	u		I		U				ur
	Endringshåndtering		B	I			I	u	U	I			Iur
	Rapporter og statistikker			Bu					u				U
	Håndtering av feilsituasjoner			Iu			I		U	I			Ir
	Databaseforvaltning												U
Applikasjondrift													
	Aksess for programvareleverandør			I					U				
	Overvåking av ytelse og stabilitet			u					U				
	Integrasjonsforvaltning			U					u				
	Viewpoint - X-tray (begge)			U									
	Viewpoint - DMA			U									
	Viewpoint - Synego			U									
	Viewpoint HBE - Viewpoint HST			U									
	Bruker- og rolle-styring gjennom Samlepunktet					BU	I						
	Konfigurasjon av programvaren			Bu			I		I				U
	Oppgradering på servere og klienter			B			I		u	I			U
	Dokumentasjon			u					U				u
App Installasjon (klient)													
	Pakke og distribuere klientprogramvare			B			I		Iu			U	r
	Installere / aktivere lisenser			U					Iu				ur
Klient, server og lagring													
	Drift og vedlikehold av OS på server og klient			B			I		U	I		u	R
	OS installasjon på server og klient										U	u	
	Administrasjon, drift og vedlikehold av server og										U		
	Administrasjon, drift og vedlikehold av lagring lokalt på server			U			I		u	I			
	Overvåkning av server, lagrings- og virtualiseringsteknologi										U		
	Administrasjon, drift og vedlikehold av klient											U	

B	Beslutninger
U	Utfører arbeidet
u	Bidrar i utførelsen
I	Må informeres
R	Må rådspørres
r	Kan tilkalles for diskusjon

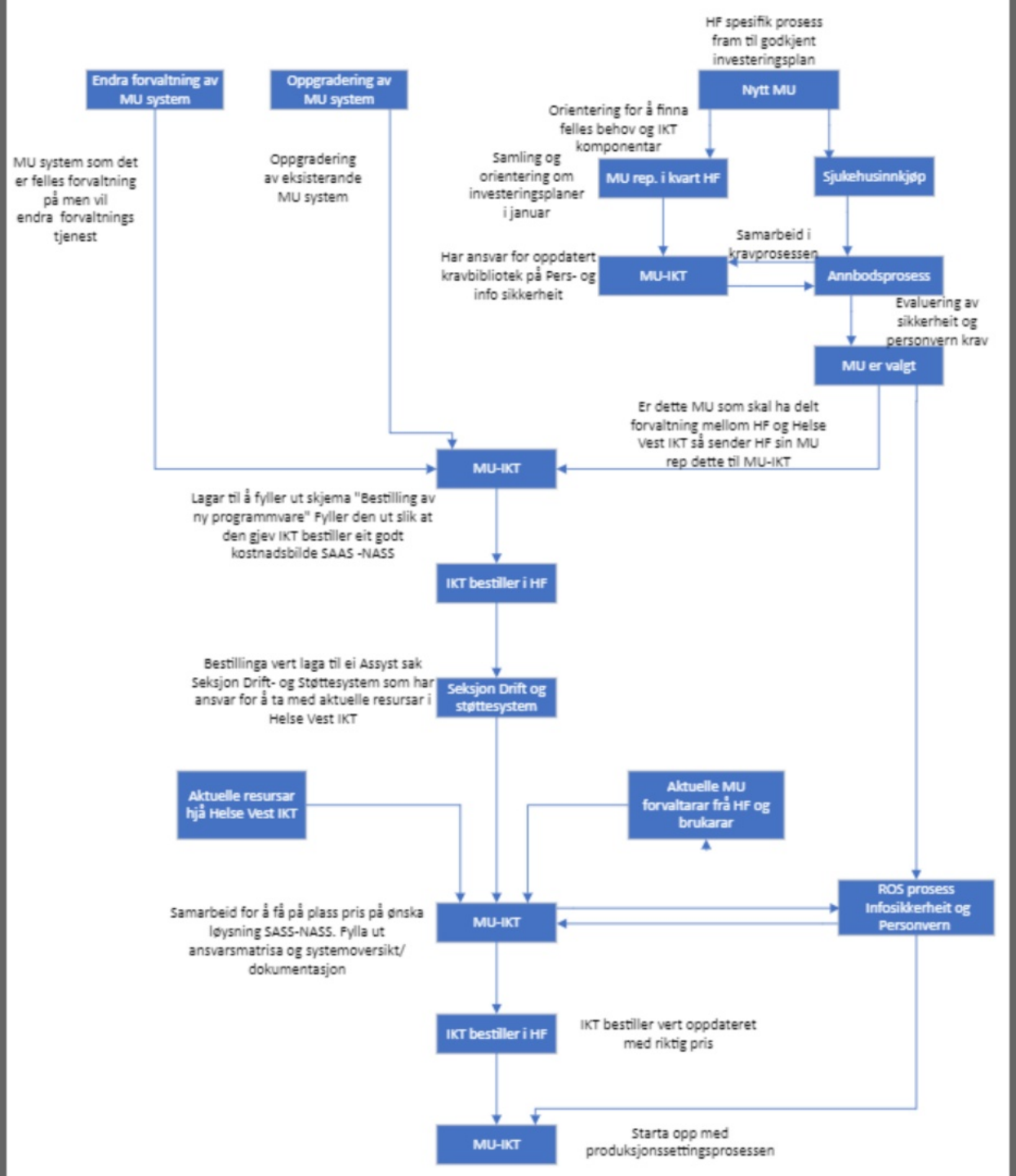
Foretak
RHF/Regionalt
Helse Vest IKT
Ekstern

MU-IKT forum

Samansetning og Mandat.

Mandat:

Det er etablert en gruppe som heter MU-IKT forum som består av personar frå MU-forvalter og Drift og støttesystem hos Helse Vest IKT. Det er MU-IKT forum som skal vera det operative samhandlingsforumet som skal brukas ved etablering og sikker drift av MU systemer med delt forvaltning. Delt forvaltning betyr at MU-forvaltar setter vekk drift av IKT komponent i MU til Helse Vest IKT. Det avtalast ein forvaltningsmodell og ansvarsmatrisa for kvart system som har delt forvaltning.


HF spesifik prosess fram til godkjent investeringsplan
Endra forvaltning av MU system
Oppgradering av MU system
Nytt MU
Orientering for å finna felles behov og IKT komponentar
MU system som det er felles forvaltning på men vil endra forvaltnings tjenest
Oppgradering av eksisterande MU system
Samling og orientering om investeringsplaner i januar
MU rep. i kvart HF
Sjukehusinnkjøp
Samarbeid i kravprosessen
Har ansvar for oppdatert kravbibliotek på Pers- og info sikkerheit
MU-IKT
Annbodsprosess
Evaluering av sikkerheit og personvern krav
MU er valgt
Er dette MU som skal ha delt forvaltning mellom HF og Helse Vest IKT så sender HF sin MU rep dette til MU-IKT
MU-IKT
Lagar til å fyller ut skjema "Bestilling av ny programmvare" Fyller den ut slik at den gjev IKT bestiller eit godt kostnadsbilde SAAS -NASS
IKT bestiller i HF
Bestillinga vert laga til ei Assyst sak Seksjon Drift- og Støttesystem som har ansvar for å ta med aktuelle resursar i Helse Vest IKT
Seksjon Drift og støttesystem
Aktuelle resursar hjå Helse Vest IKT
Aktuelle MU forvaltarar frå HF og brukarar
ROS prosess Infosikkerheit og Personvern
Samarbeid for å få på plass pris på ønska løysning SASS-NASS. Fylla ut ansvarsmatrisa og systemoversikt/ dokumentasjon
MU-IKT
IKT bestiller i HF
IKT bestiller vert oppdateret med riktig pris
MU-IKT
Starta opp med produksjonssettingsprosessen

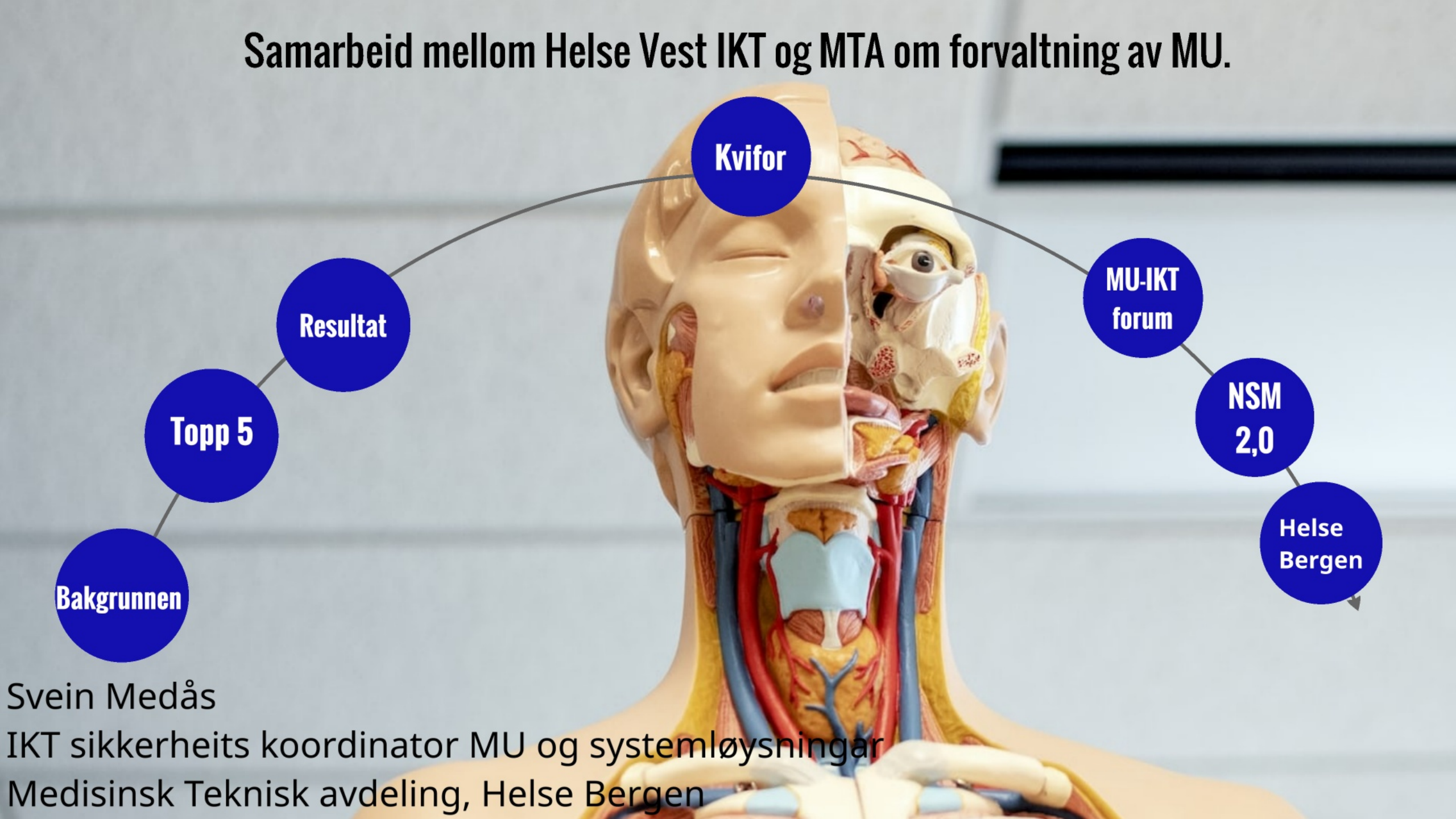
Kva type driftsmodellar skal me ha på system i felles forvaltning?

HF

saas-1	saas-2	saas-3	PaaS-1	Paas-2	Paas-3	IaaS-1	Iaas-2	NaaS	Separat HF-nett
App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv	App. Forv
Klient App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift	App. Drift
Klient App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.	App. Inst.
Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift	Server App. Inst og drift
Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon	Integrasjon
OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift	OS drift
OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon	OS Installasjon
Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)	Server&Klient (Fys/Virt)
Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup	Lagring & Backup
Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk	Nettverk
Fysisk lokasjon m/strøm/kjøling/vann og fastmontert kabling									

Helse Vest IKT

Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen

1. Identifisere og kartlegge

- 1.1 Kartlegg styringsstrukturer, leveranser og understøttende systemer
- 1.2 Kartlegg enheter og programvare
- 1.3 Kartlegg brukere og behov for tilgang

2. Beskytte og opprettholde

- 2.1 Ivareta sikkerhet i anskaffelses- og utviklingsprosesser
- 2.2 Etabler en sikker IKT-arkitektur
- 2.3 Ivareta en sikker konfigurasjon
- 2.4 Beskytt virksomhetens nettverk
- 2.5 Kontroller dataflyt
- 2.6 Ha kontroll på identiteter og tilganger
- 2.7 Beskytt data i ro og i transitt
- 2.8 Beskytt e-post og nettleser
- 2.9 Etabler evne til gjenoppretting av data
- 2.10 Integrer sikkerhet i prosess for endringshåndtering

3. Oppdage

- 3.1 Oppdag og fjern kjente sårbarheter og trusler
- 3.2 Etabler sikkerhets-overvåkning
- 3.3 Analyser data fra sikkerhets-overvåkning
- 3.4 Gjennomfør inntrengings-tester

4. Håndtere og gjenopprette

- 4.1 Forbered virksomheten på håndtering av hendelser
- 4.2 Vurder og klassifiser hendelser
- 4.3 Kontroller og håndter hendelser
- 4.4 Evaluer og lær av hendelser

Har me oversikt over kva me har i nettet vårt?

Har me oversikt over kva me har i nettet vårt?

Me har ikkje ein samla oversikt over alt me har i nettet vårt.

Har me oversikt over kva me har i nettet vårt?

Me har ikkje ein samla oversikt over alt me har i nettet vårt.

Me har MAC og IP på mykje MU men manglar info om type utstyr, OS, versjon, kjende sårbarheiter

Oversikt over oversikt

En samling over de ulike oversiktene med informasjon om lokal IKT i Helse Bergen HF. Lokal IKT er IKT-enheter, -utstyr, -komponenter, -infrastruktur og programvare som enheter i Helse Bergen HF har ansvar for utvikling, forvaltning eller drift alene eller i samarbeid med Helse Vest IKT og andre leverandører. Dette gjelder i hovedsak Drift/teknisk divisjon, Laboratorieklinikken, Kreftavdelingen, Radiologisk avdeling og FoU-avdelingen.

Systemlisten Helse Vest IKT - Oversikt over alle systemer som er forvaltet av Helse Vest IKT. Listen inneholder ikke systemer som er forvaltet av enheter i Helse Bergen. Listen inneholder heller ikke oversikt over tjenester levert av Helse Vest IKT etter MU-bilaget (virtuelle servere eller lagring). Det er ingen god oversikt over leveranser fra Helse Vest IKT over MU-bilaget.

\\ihelse.net\medisinteknisk - MU filområde levert av Helse Vest IKT etter MU-bilaget. Helse Vest IKT leverer også andre filområder etter MU-bilaget. Det er ingen god oversikt over slike filområder.

Utstyrsportalen Helse Vest IKT - Oversikt over enheter og utstyr som er tilknyttet ulike nettverk levert av Helse Vest IKT. Dekker ikke gjestenett fra Helse Vest IKT. Det er noe varierende hvilke opplysninger som er registrert per enhet. Det fremgår i mindre grad hvilken tjeneste eller system enheten er del av.

System Informasjon MTA - Oversikt over IKT-systemer forvaltet av medisinsk-teknisk avdeling i HBE (pålogging)

Medusa Helse Vest MTA - Oversikt over medisinsk utstyr i HBE (pålogging). Detaljert oversikt over medisinsk utstyr men mindre oversikt over tilhørende IKT-enheter og systemer.

Programvare i kreftavdelingen - Oversikt over ansvarsfordeling for programvare i kreftavdelingen HBE (noe overlapp med systemlisten og MTA-oversikt)

IKT-systemer og datalagring ved MGM - Oversikt over systemer i bruk ved MGM (noe overlapp med systemlisten og MTA-oversikt)

Gitlab MGM - Oversikt over egenutviklet programvare ved MGM (pålogging)

Sikker Lagring - Oversikt over lagringsområder på Sikker Lagring på \\ihelse.net\SL\HBE

PET-senteret, radiologisk avdeling - mangler oversikt

Programvare utviklet av forskningsprosjekter - mangler oversikt

Helsetjenesteutvikling, virksomhetsstyring og rapportering (forløpsdabasen) - mangler oversikt

Kvalitetsregistre - mangler oversikt

Fagsentre, nettverk og kompetansesentre - mangler oversikt

Nessus Scan

VPR Top Threats

Assessed Threat Level: Critical

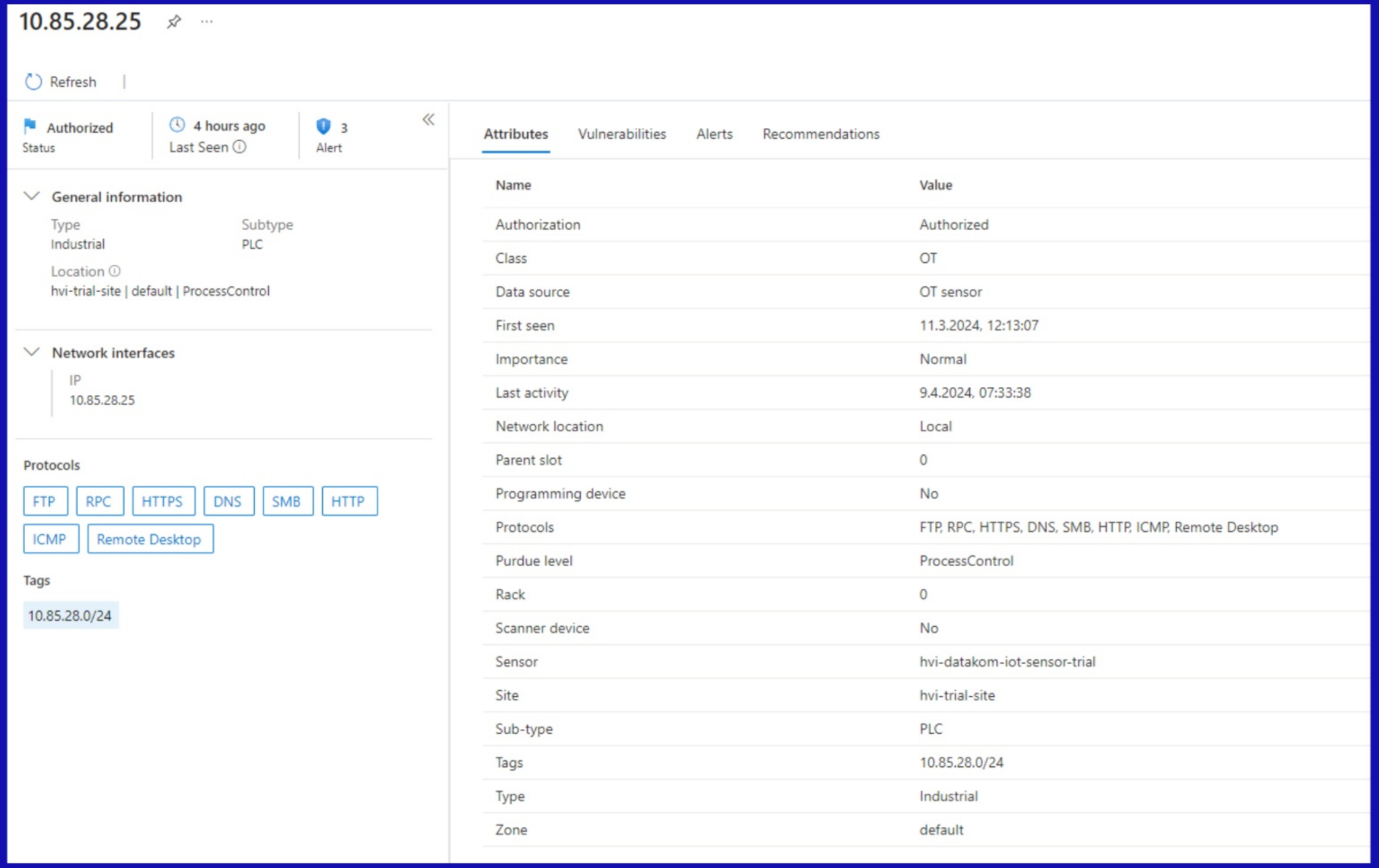
The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk. To learn more about Tenable's VPR scoring system, see: https://www.tenable.com/predictive-prioritization

severity	pluginname	host_count
4	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	5
4	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	2
3	Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper)	4
2	Apache Tomcat 9.0.0.M1 < 9.0.81 multiple vulnerabilities	1
2	Microsoft Windows SMBv1 Multiple Vulnerabilities	4
2	SMB NULL Session Authentication	1
2	SSL Medium Strength Cipher Suites Supported (SWEET32)	43
2	OpenSSH X11 Forwarding Session Hijacking	1
2	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	4
2	CodeMeter Runtime Buffer Over-read (WIBU-210423-01)	1

Andre løysningar

Me har testa ut andre løysningar som har sensor/utstyr i nettet vårt som registrerer og nyttar kommunikasjonsprotokollar til å utføra deep packet inspection (DPI) for å gjenkjenna og gruppera utstyr. Systema koplar saman type utstyr og kjente sårbarheitar og hjelpa oss å prioritera desse oppgåvene.

Sensor og plassering

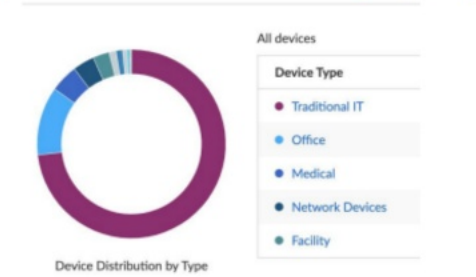


Medical IoT Security accelerates your device zero trust journey

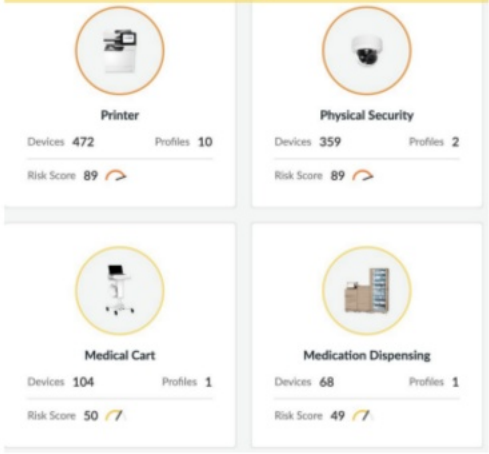
Comprehensive visibility & risk assessment

Discover and classify all your connected devices by type & risk profile

View Device distribution by type



Device inventory, Rich context

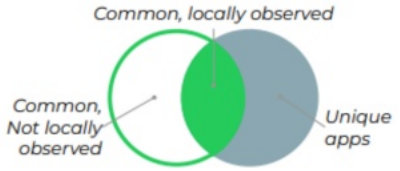


Segmentation & least privilege access

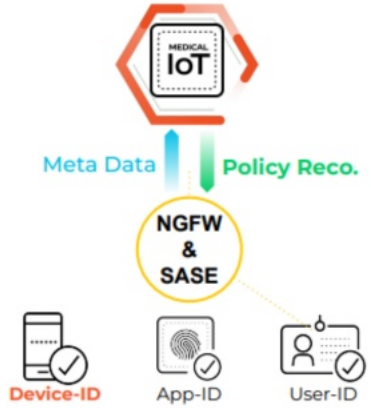
Segment critical or risky medical devices from the rest & enforce least privilege access controls

Analyse device behaviors

Compare device data with crowdsourced telemetry data



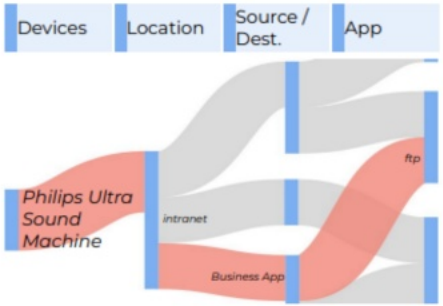
Enforce recommended policies



Continuous monitoring, Adv. security inspection

Monitor device communications for continuous trust verification & security inspection

Identify abnormal connections



Block known and unknown threats

Security Inspection

MIoT Asset Integrity (sample criteria)

1. IDENTIFY ANOMALOUS BEHAVIORS:
   - Deviation from OEM (e.g., remote SW updates)
   - Unexpected Apps (e.g., FTP on XRAY)
2. ADD ACTION: GENERATE ALERT AS PRIORITY AND SEND TO 3RD PARTY AND/OR ASSIGN TO USER

Pre-built integrations & Automation

Simplify operations and automate workflows

Eliminate Medical IoT blind spots

Prioritized list of all vulnerabilities

10,234 instances were identified for the following vulnerabilitie

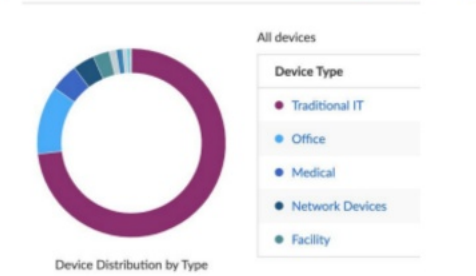
Priority	Vulnera...	Severity	CVSS
To	CVE-2021-...	V	7.8
To	CVE-2016-...	V	7.8
To	CVE-2016-...	V	8.8
To	CVE-2019-...	V	7.8
To	CVE-2018-...	V	9.8
To	CVE-2018-...	V	9.8
Me	CVE-2019-...	V	7.1

Medical IoT Security accelerates your device zero trust journey

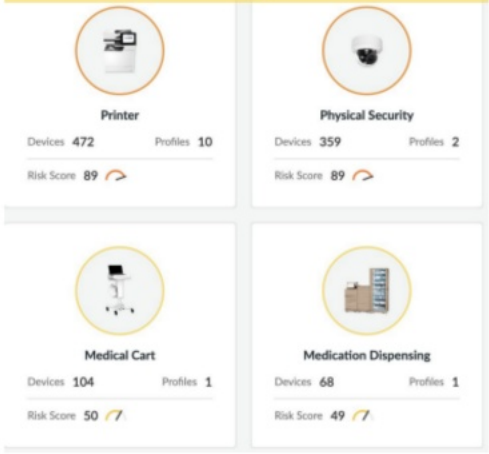
Comprehensive visibility & risk assessment

Discover and classify all your connected devices by type & risk profile

View Device distribution by type



Device inventory, Rich context

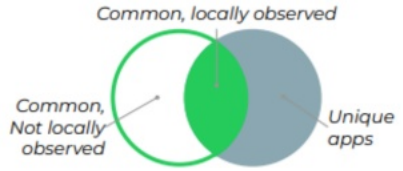


Segmentation & least privilege access

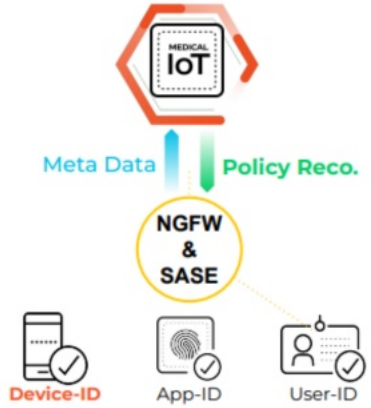
Segment critical or risky medical devices from the rest & enforce least privilege access controls

Analyse device behaviors

Compare device data with crowdsourced telemetry data



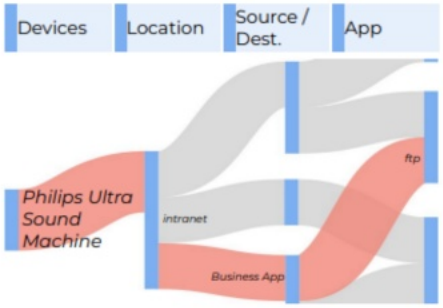
Enforce recommended policies



Continuous monitoring, Adv. security inspection

Monitor device communications for continuous trust verification & security inspection

Identify abnormal connections



Block known and unknown threats

Security Inspection

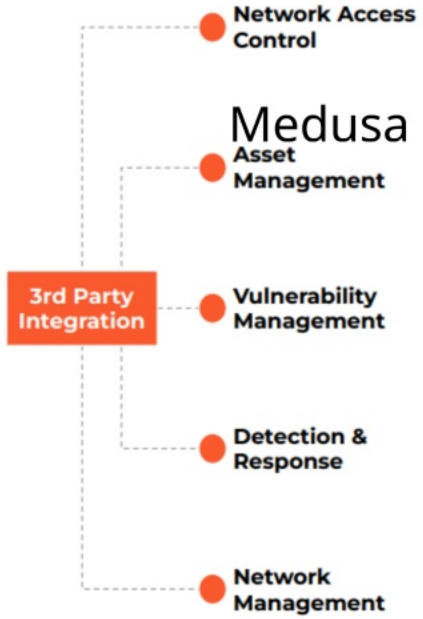
MIoT Asset Integrity (sample criteria)

1. IDENTIFY ANOMALOUS BEHAVIORS:
   - Deviation from OEM (e.g., remote SW updates)
   - Unexpected Apps (e.g., FTP on XRAY)
2. ADD ACTION: GENERATE ALERT AS PRIORITY AND SEND TO 3RD PARTY AND/OR ASSIGN TO USER

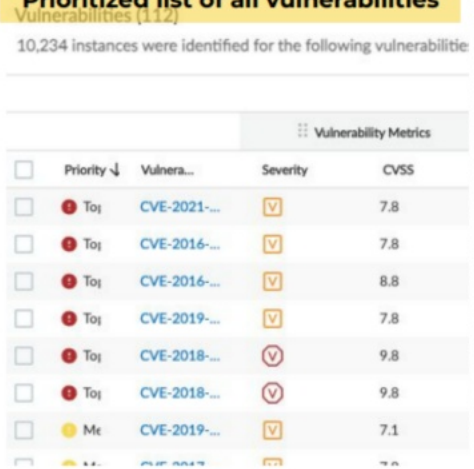
Pre-built integrations & Automation

Simplify operations and automate workflows

Eliminate Medical IoT blind spots



Prioritized list of all vulnerabilities



MDS2 og SBOM

Asset Types, Card View (Total: 764)

Blood Gas Analyzer

23

C-Arm

9

Chemistry Analyzer

7

CR

27

CR/DR

7

CT

10

CVIS Server

2

DICOM Workstation

38

Fluoroscopy

2

Gateway

53

Glucometer

28

Hematology Analyzer

7

Hemodialysis

22

Hemostasis Analyzer

1

Immunoassay

3

IoT Device

45

IVUS

3

LIS Server

4

Mammography

1

Medical Device

6

Mobile DR

1

Molecular Testing

1

MRI

6

NAS

1

Network Device

3

OIS Server

3

PACS Server

8

PCR Analyzer

5

Point of Care Analyzer

1

Printer

8

Top 10 Risks

Risk Title	Asset Type	Count	Risk Score
CVE-2015-1497	CT	1	9.9
URGENT/11	C-Arm	1	9.9
Legacy OS	C-Arm	3	9.8
Legacy OS	Chemistry Analyzer	1	9.8
Legacy OS	CR	18	9.8
Legacy OS	CT	3	9.8
Legacy OS	Fluoroscopy	1	9.8
Legacy OS	MRI	4	9.8
Legacy OS	Network Device	1	9.8
Legacy OS	Blood Gas Analyzer	3	9.7

Name **CVE-2015-1497** Risk Group **Vuln. Services** ••• IDENTIFIED

Impact (environmental score)	
Confidentiality	Medium
Patient Safety	High
Service Disruption	Medium

Base Score	10
Confidentiality	Complete
Integrity	Complete
Availability	Complete

Type	Vulnerability
Vendor	N/A
CVE	CVE-2015-1497
CWE	Improper Control of Ge...
Publish Date	16/02/2015

Description

radexecd.exe in Persistent Systems Radia Client Automation (RCA) 7.9, 8.1, 9.0, and 9.1 allows remote attackers to execute arbitrary commands via a crafted request to TCP port 3465.

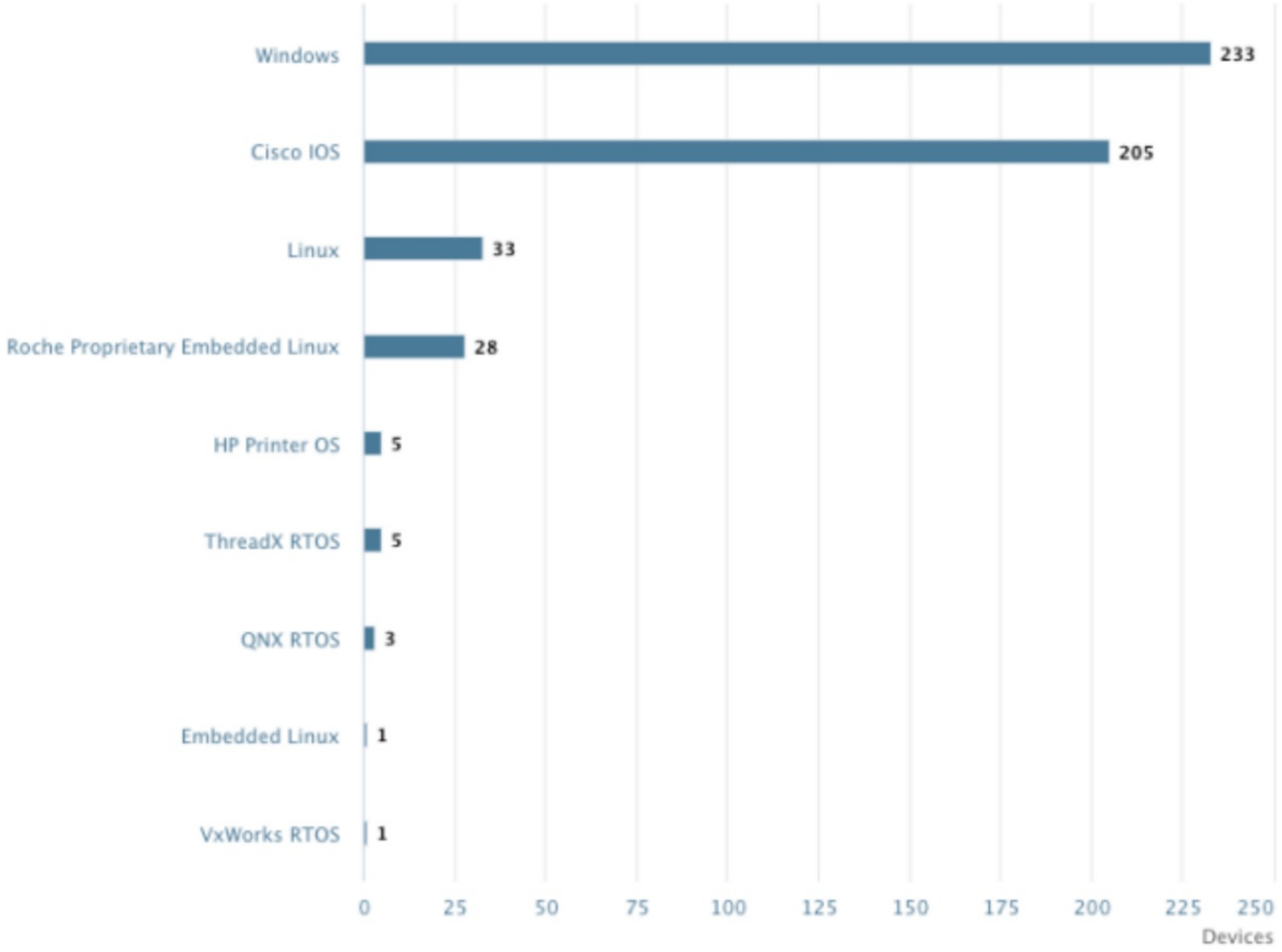
Mitigation

1 . Apply East-West Segmentation: It is advised to run the devices in a dedicated network segment and protected IT environment.
2 . Apply North-South Segmentation: It is advised to run the devices in a dedicated network segment and protected IT environment.

More Details

CVE-2015-1497 (NVD) , CVE-2015-1497 (MITRE) , CC-1568 (NHS Digital)

OS Distribution



Operating System	Number of Assets
Windows 2000	3
Windows 7	22
Windows 7/Server 2008	1
Windows 7 Embedded	1
Windows 7 SP1	3
Windows 8.1	3
Windows CE	1
Windows CE 7.0	1
Windows Embedded Compact 7	2
Windows Embedded Std 2009	1
Windows Embedded Std 7 SP1	19
Windows Embedded Std 7 X64 SP1	1
Windows XP	3
Windows XP Embedded	20
Windows XP Embedded SP3	1
Windows XP SP2	11

Kva kan hjelpa oss når me må leva med slikt utstyr i nettet vårt?

Kva kan hjelpa oss når me må leva med slikt utstyr i nettet vårt?

Segmentering

Kva kan hjelpa oss når me må leva med slikt utstyr i nettet vårt?

Segmentering

Segmentering

Kva kan hjelpa oss når me må leva med slikt utstyr i nettet vårt?

Segmentering

Segmentering

Segmentering

Kva kan hjelpa oss når me må leva med slikt utstyr i nettet vårt?

Segmentering

Segmentering

Segmentering

Cisco SDA

Kva kan hjelpa oss når me må leva med slikt utstyr i nettet vårt?

Segmentering

Segmentering

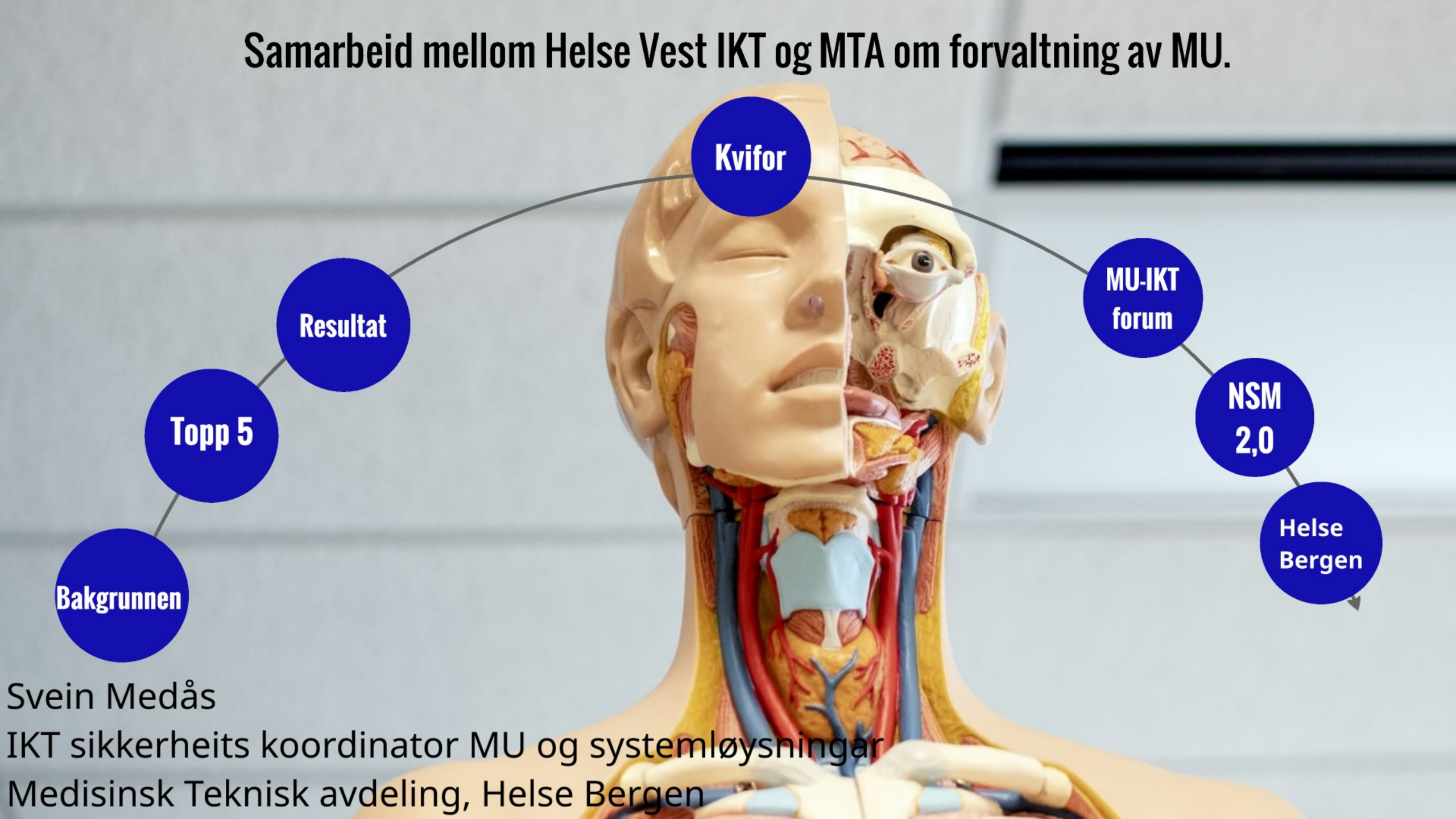
Segmentering

Cisco SDA

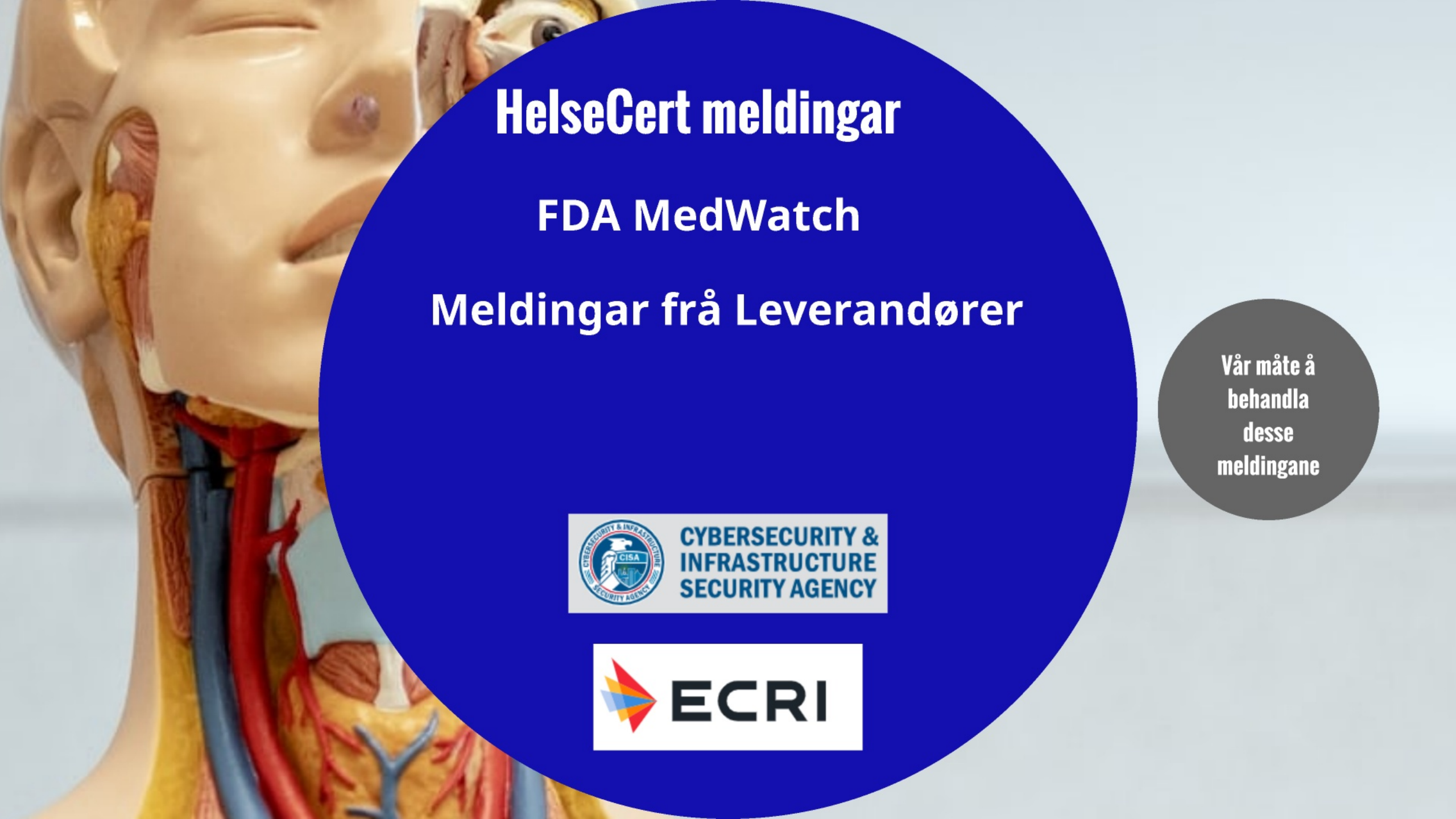
Dyrt å oppgradera nettverksutstyr og mykje arbeid

Sikkerheit kostar

Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen



HelseCert meldingar

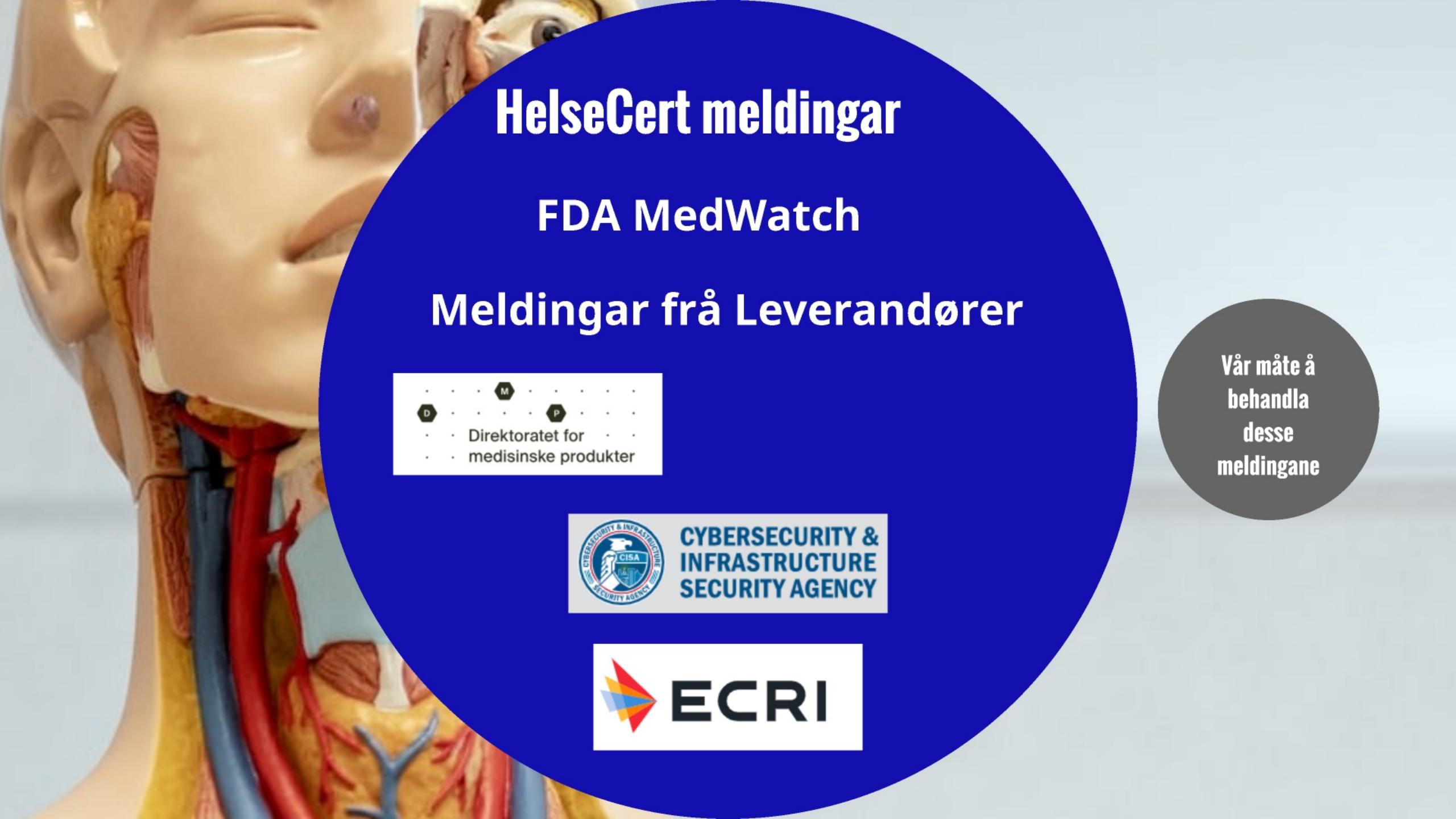
FDA MedWatch

Meldingar frå Leverandører

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ECRI

Vår måte å behandla desse meldingane



HelseCert meldingar

FDA MedWatch

Meldingar frå Leverandører

Direktoratet for medisinske produkter

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ECRI

Vår måte å behandla desse meldingane

HelseCert meldingar

FDA MedWatch

Meldingar frå Leverandører

Direktoratet for medisinske produkter

Helsetilsynet

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ECRI

Vår måte å behandla desse meldingane

HelseCERT sårbarhet-patch

+ Legg til oppgave

Kritisk CVSS 9-10

[NBP-saarbarhet-patch] [HelseCERT#10058796] Kritisk sårbarhet i Cisco IOS XE-webgrensesnitt

16.11.

Kritisk CVSS 9-10

[NBP-saarbarhet-patch] [HelseCERT#10058681] Microsoft patchetirsdag oktober 2023

11.11.

Høy/Alvorlig CVSS ...

[NBP-saarbarhet-patch] [HelseCERT#10058629] Kommende oppdateringer for curl- sårbarheter

HelseCERT Medtek

+ Legg til oppgave

Fullførte oppgaver 31

HelseCERT trussel

+ Legg til oppgave

[NBP-trussel] [HelseCERT#10050672] Varsel om USB-spredt skadevare - Raspberry Robin

2

13.10.

+1

Fullførte oppgaver 24

HelseCERT inntrengningstest

+ Legg til oppgave

Kritisk CVSS 9-10

Kamera

17.11.

Kritisk CVSS 9-10

Liebert UPS

10.11.

Hospitaldrift Sikker...

Sikkerhet - håndter...

Hospitaldrift Sikkerhet (Kamera og adgangskontroll)

3

17.11.

Kritisk CVSS 9-10

Ikke i utstyrsportalen

MTA Bilde

HelseCert meldingar

FDA MedWatch

Meldingar frå Leverandører

Direktoratet for medisinske produkter

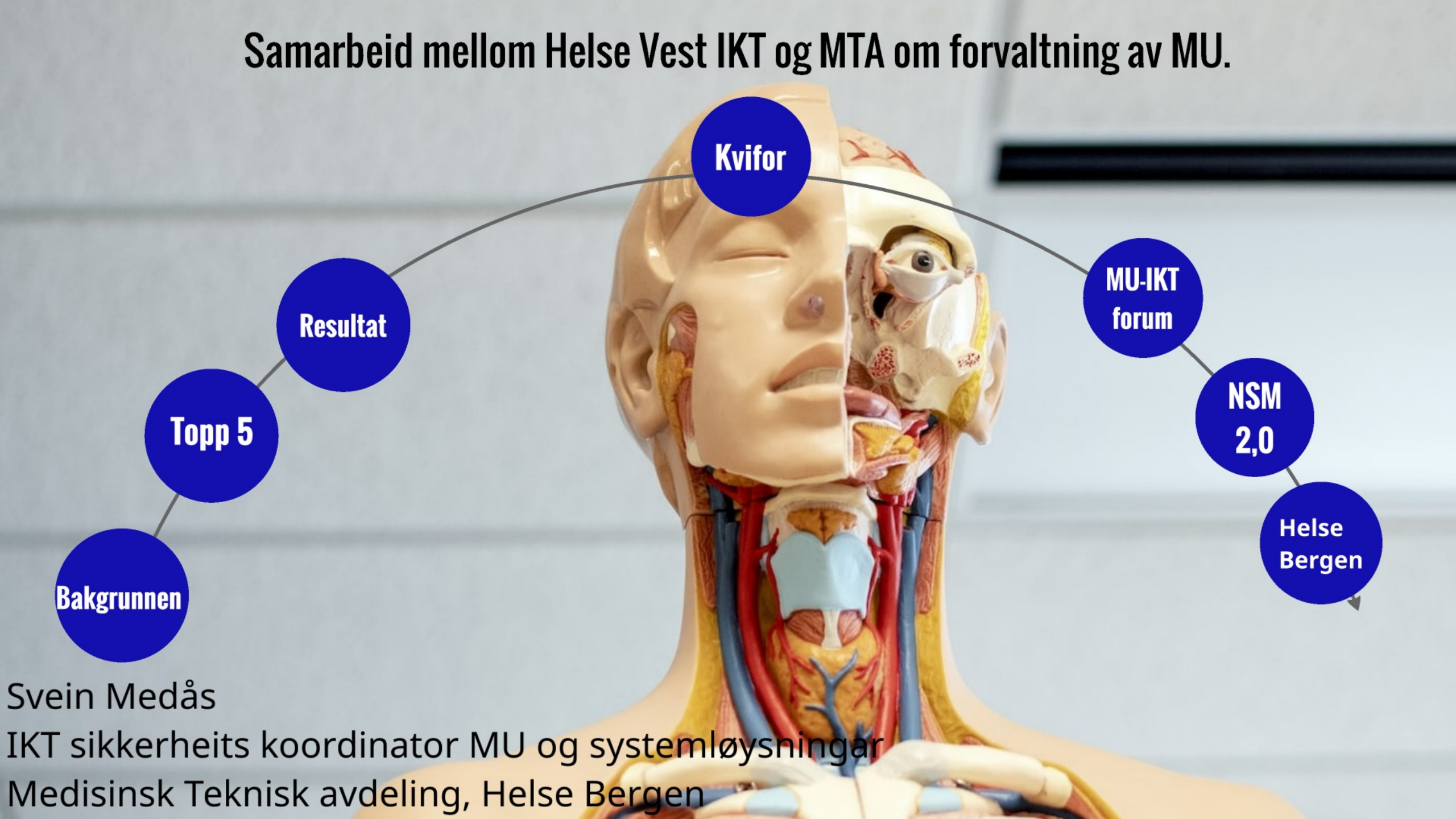
Helsetilsynet

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ECRI

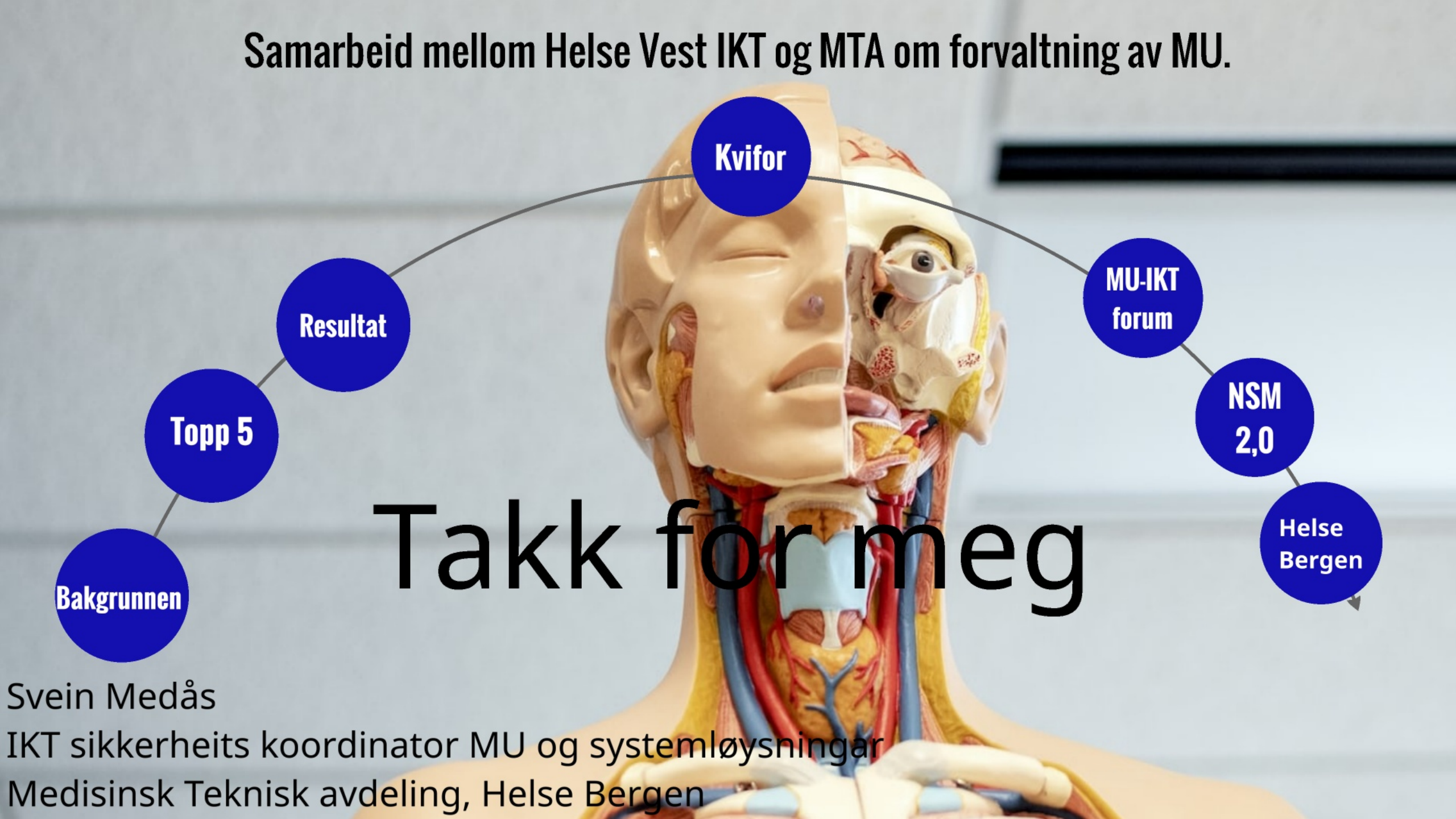
Vår måte å behandla desse meldingane

Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen

Samarbeid mellom Helse Vest IKT og MTA om forvaltning av MU.



Takk for meg

Svein Medås
IKT sikkerheits koordinator MU og systemløysningar
Medisinsk Teknisk avdeling, Helse Bergen