

Trusselformidling i Equinor: Hva skal formidles, og til hvem?

Anne Synnøve Harestad og Linn Øvestad Eikeland
Cyber Security Awareness, Cyber Defense Center





Agenda

1. Hva er trusselformidling?
2. Trusselanalyse i Equinor:
Trusselformidling som **beslutningsstøtte**
3. Security Awareness i Equinor:
Trusselformidling som **sikringstiltak**



Hva mener vi egentlig
når vi snakker om
trusselformidling?

Threat Dissemination
+
Security Awareness
=
Trusselformidling?

Threat Analysis → **Cyber** Threat Analysis
Security Awareness → **Cyber** Security Awareness

Threat Dissemination: å sikre at informasjon om trusler når frem til beslutningstakere og stakeholders

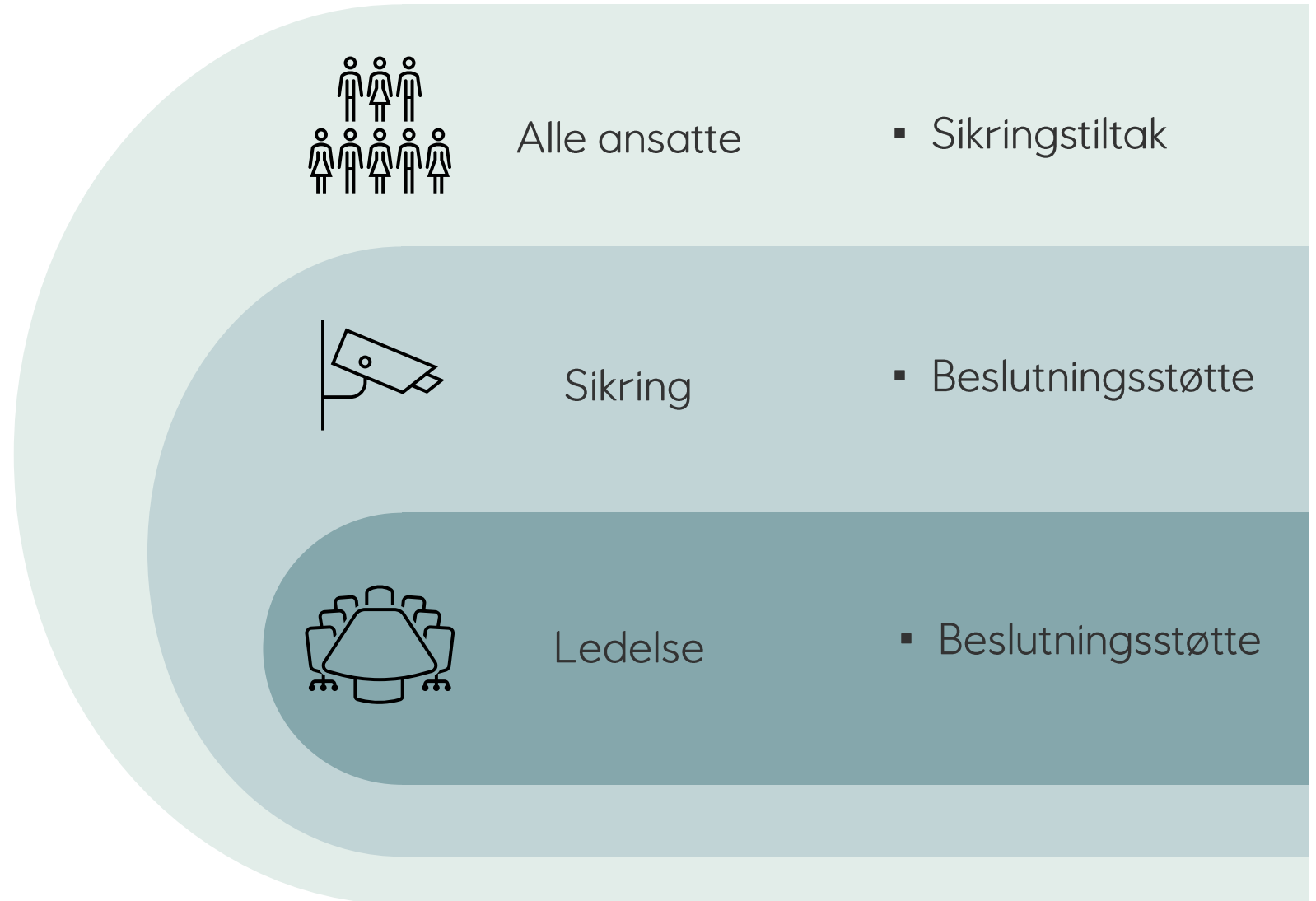
Security Awareness: å sikre at alle har tilstrekkelig kunnskap til å håndtere og varsle om sikkerhetstruende hendelser de kan bli utsatt for



Hva formidles til hvem,
og hvorfor?

Trusselformidling som
beslutningsstøtte

Trusselformidling som en
del av **sikringstiltak**





Security Threat Analysis

Sikringsrisiko er definert som forholdet mellom **trussel**, sårbarhet og konsekvens

En trussel mot Equinor innebærer at noen har **intensjon** og **kapabilitet** til å skade oss



Militær konflikt
og sabotasje



Cyber og
spionasje



Kriminalitet



Aktivism



Maritim
kriminalitet



Sivil uro og
opptøyer

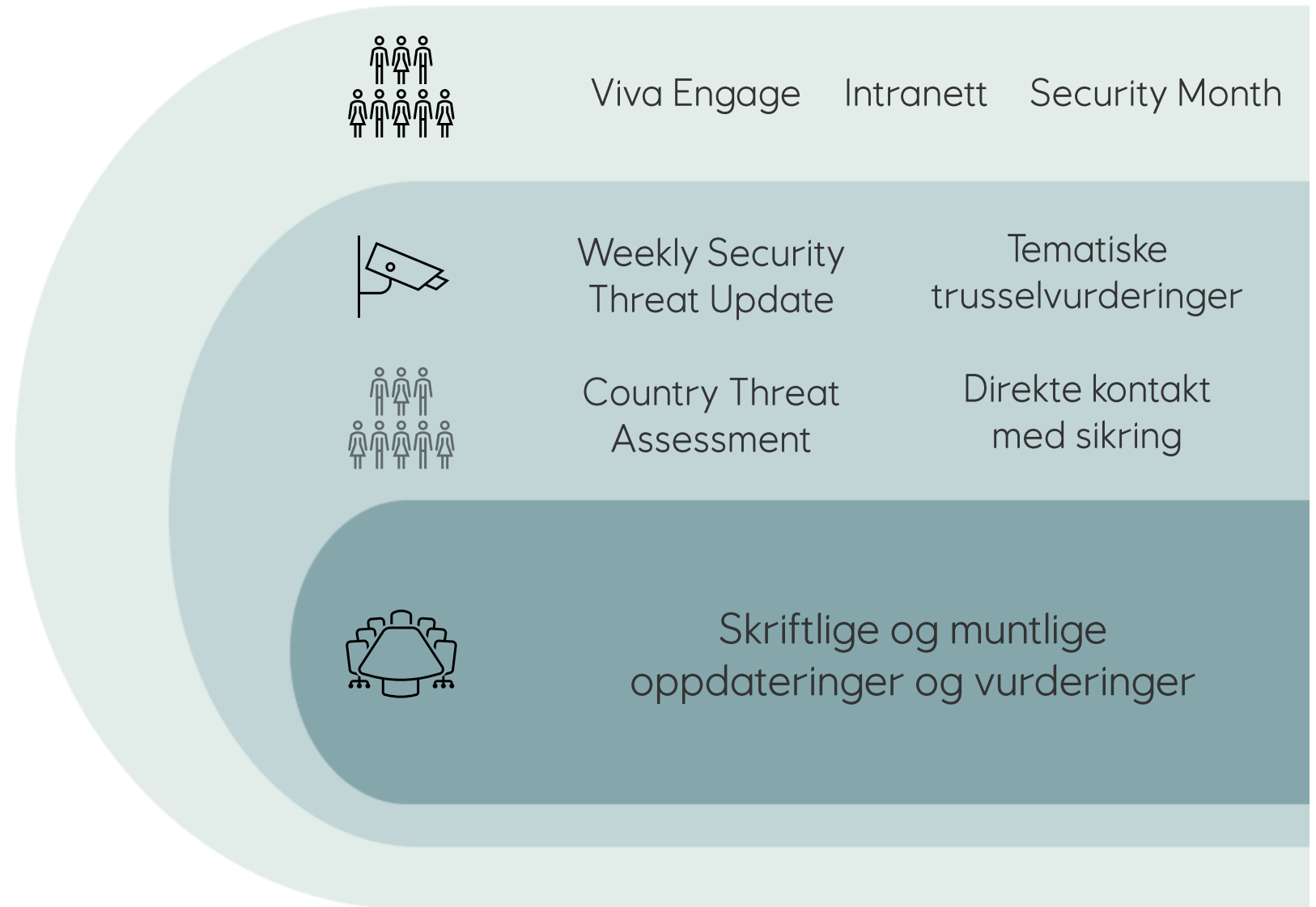


Terrorisme



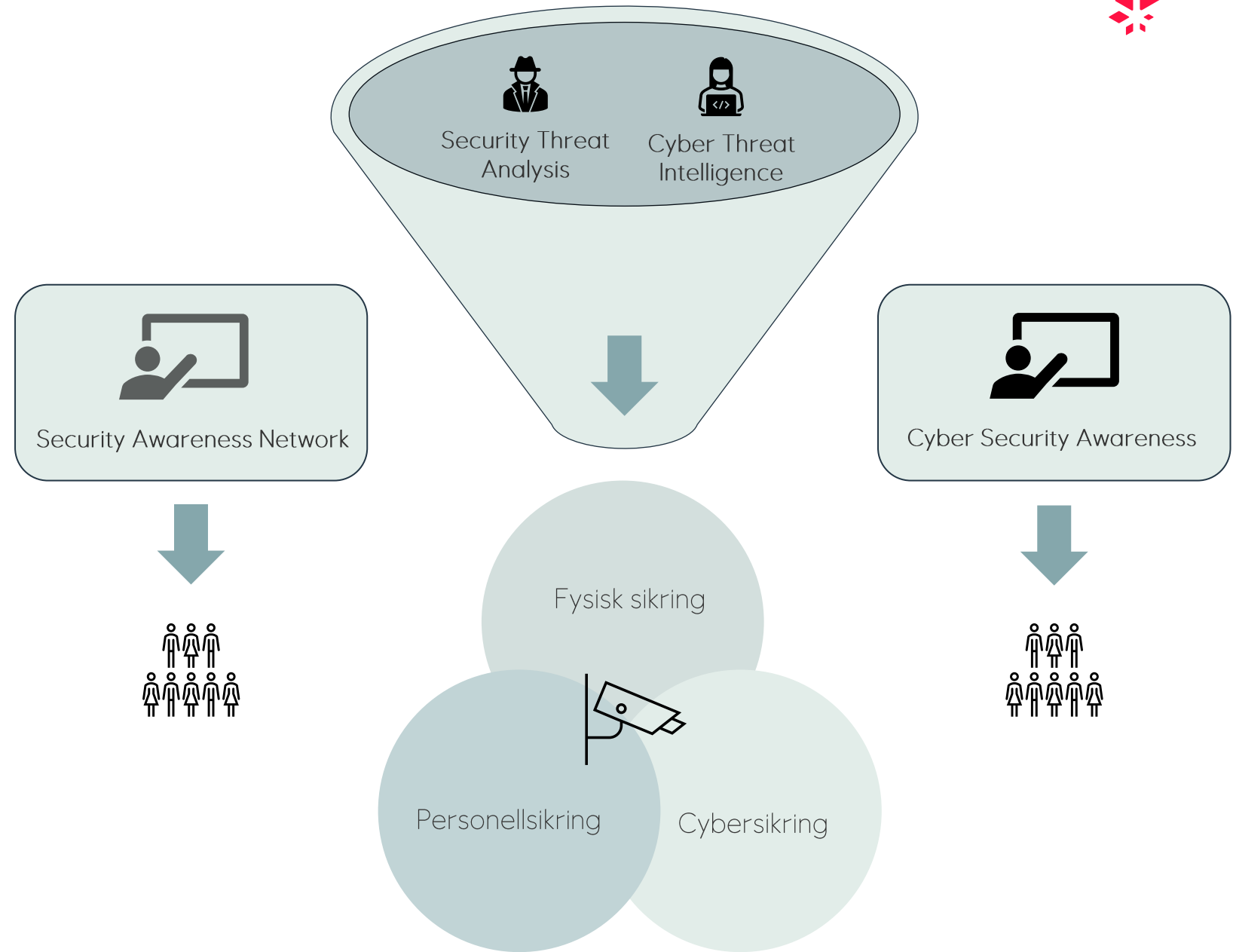
Security Threat Analysis

Identifisering, vurdering og **kommunikasjon** av sikringstrusler er det første steget i å håndtere sikringsrisiko



Trussel og sikring i Equinor

- Trusselformidling til beslutningstakere og sikringsmiljø som iverksetter sikringstiltak
- Innen cybersikring har trusselformidling til alle ansatte lenge vært et viktig sikringstiltak
- Endringer i trusselbildet har medført et økende behov for formidling av flere typer trusler til alle ansatte





Security Awareness: Verktøy og virkemidler

Overordnet tilnærming

Formål:

- Endring i holdninger
- Endring i adferd

Forståelse

Safety/Security
moments

Artikler på intranett
– «nyhetssaker»

Plakater, visuelt
materiell

Kampanjer

Kunnskap

Security awareness:
Kursportefølje

Kampanjer

Trusseloppdatering

Presentasjoner

Ferdigheter

Table-tops/
diskusjonsøvelser

Støtte/Fasilitering

Kampanjer

Simuleringer



Hvordan tilpasse budskapet?

Effektiv formidling av trusler og sikringstiltak må ta hensyn til:

- Forretningsområde
- Geografi
- Kultur

Men hvordan vet man om man har lyktes?

- Engasjement – uten å skremme
- Skape forståelse – uten å overvelde
- Nyansere – uten å forvirre
- Tilpasse budskapet – uten å bruke for mye tid
- Ansvarliggjøring – uten ansvarsfraskriving
- Oppdatert – men ikke for ofte



Hva må til for å lykkes?

- Tilstrekkelig Ledelsesinvolvering/ ledelsesstøtte
- Tett samarbeid med HR-funksjonen og Kommunikasjonsavdelingen(e)
- Riktig fagkompetanse og erfaring internt i teamet
- Høy kvalitet i leveransene
- Kjennskap til brukergruppenes problemstillinger og ulike kulturer
- Risikobasert/metodisk tilnærming til målgrupper

Trusselformidling i Equinor: Hva skal formidles, og til hvem?

Anne Synnøve Harestad og Linn Øvestad Eikeland
Cyber Security Awareness, Cyber Defense Center

© Equinor ASA

This presentation, including the contents and arrangement of the contents of each individual page or the collection of the pages, is owned by Equinor. Copyright to all material including, but not limited to, written material, photographs, drawings, images, tables and data remains the property of Equinor. All rights reserved. Any other use, reproduction, translation, adaption, arrangement, alteration, distribution or storage of this presentation, in whole or in part, without the prior written permission of Equinor is prohibited. The information contained in this presentation may not be accurate, up to date or applicable to the circumstances of any particular case, despite our efforts. Equinor cannot accept any liability for any inaccuracies or omissions.

