NORGES BANK

# TIBER – avansert trusseltesting for bedre cybersikkerhet

Threat Intelligence-Based Ethical Red-teaming

Andreas Havsberg
Anders Olaus Granerud

# Innhold

Hvem er vi?

Hva er TIBER

Verdien av TIBER

Utfordringer

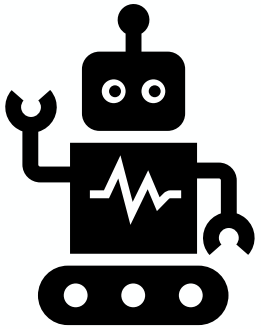
Spørsmål

# TIBER-NO Cyber Team (TCT)

Anders Olaus Granerud
Team Manager TIBER-NO

Andreas Havsberg
Security Test Manager

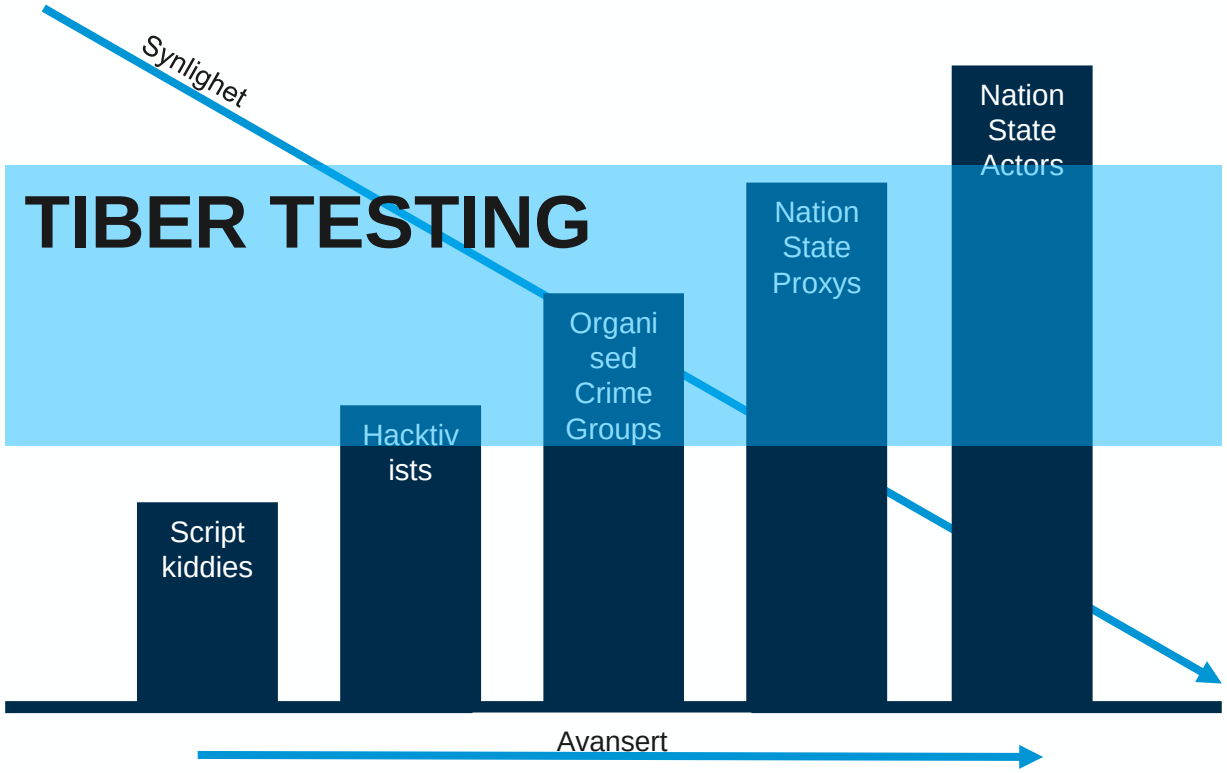
Øystein Sangolt
Security Test Manager



Konsulent

# Kort om TIBER

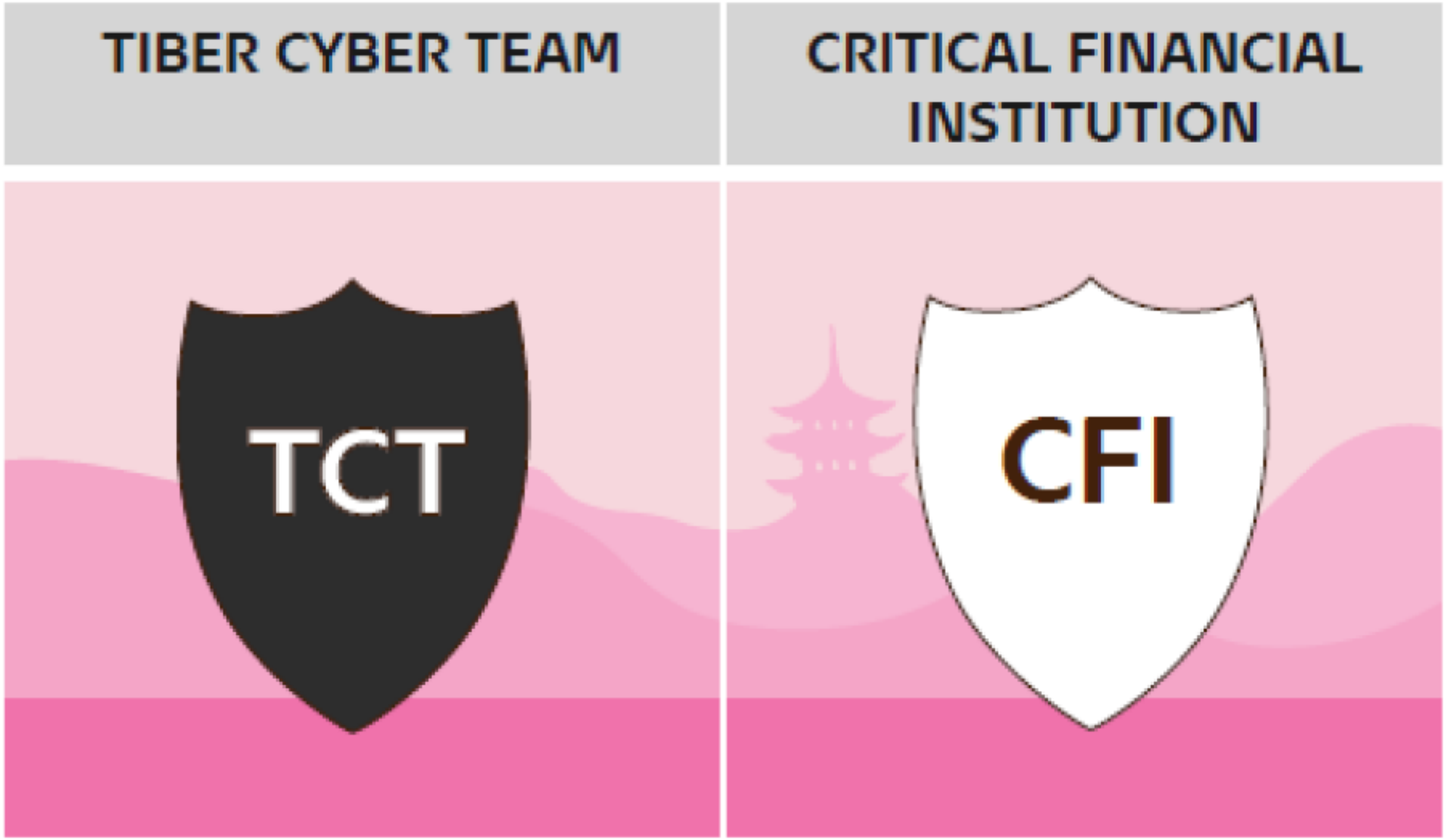
- **Avansert sikkerhetstesting**
- Kritiske funksjoner skal testes
- Etterretningsdrevet (trusselbasert)
- Mest mulig realistisk
- Foretakene eier selv testene
- Bidra til styrke robusthet i finansiell sektor og finansiell stabilitet



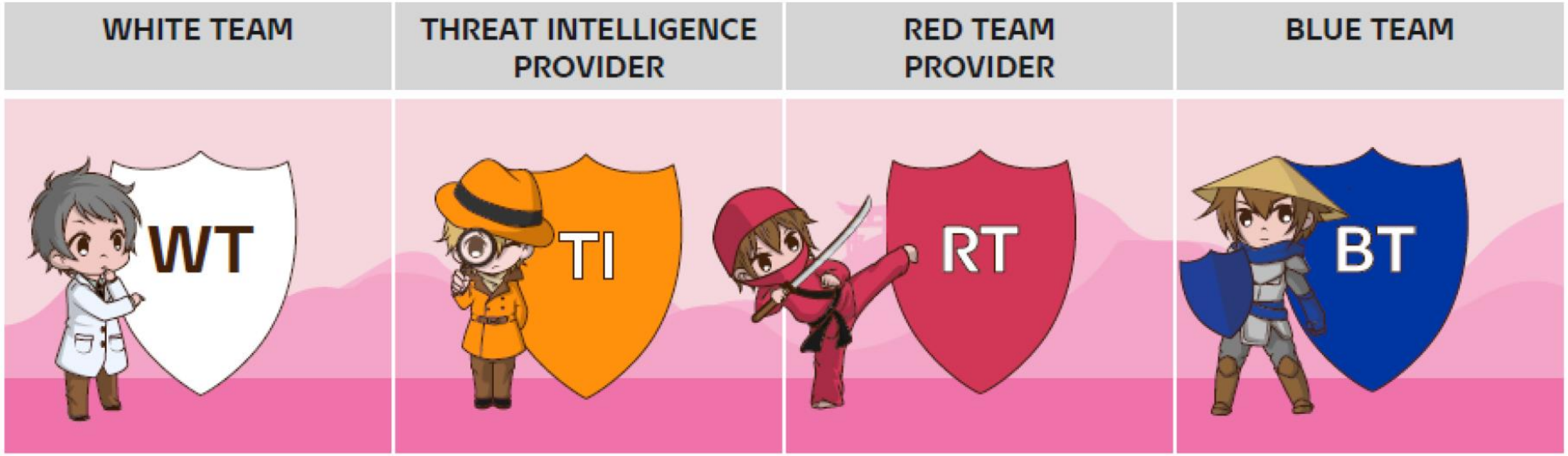
# Organisering

- TIBER-EU: Rammeverk utviklet av European Central Bank
- TIBER-NO: Norsk implementasjon etablert av Norges Bank og Finanstilsynet
- Frivillig - ikke et verktøy for tilsyn
- Informasjonsdeling fra en test
- TIBER-NO Forum: Deling av erfaringer fra testing

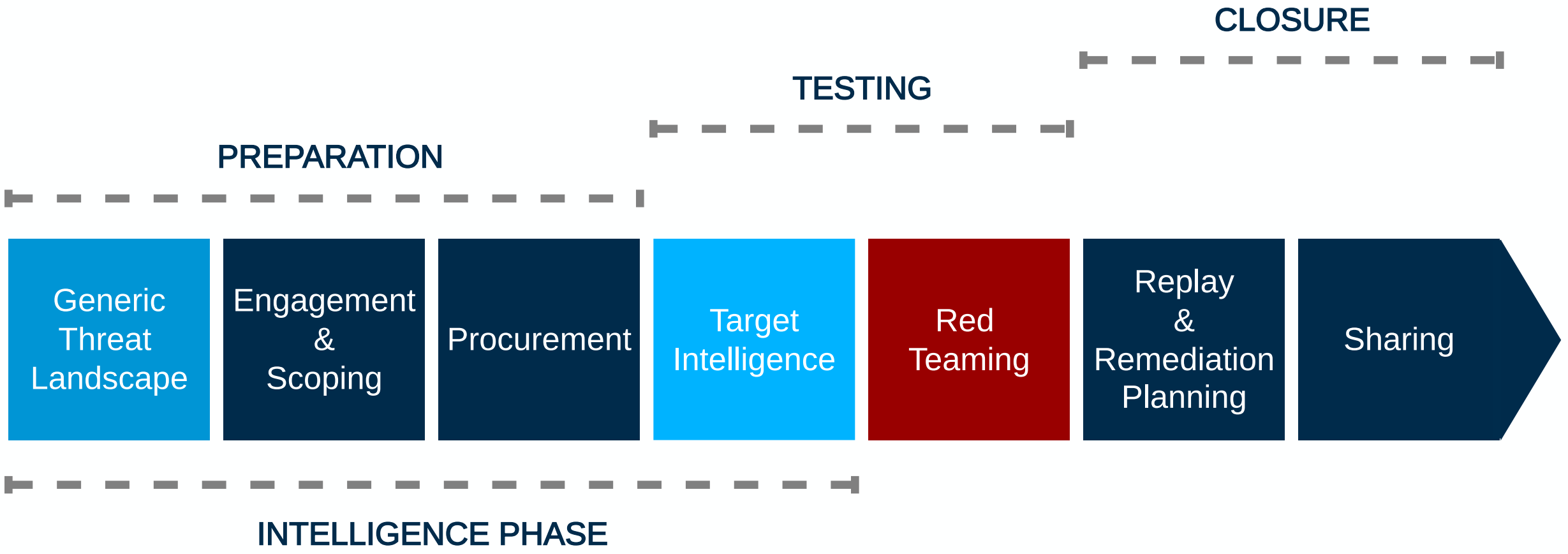
# Roller i en TIBER-test



# Roller i en TIBER-test



# TIBER-NO prosjekt



# Hvorfor TIBER?

Økt motstandskraft
styrker finansiell stabilitet

Testing gir
god læring

På tvers av
landegrenser

# Verdien av TIBER

## For foretaket

- Omfattende testing
- Hvilke trusselaktører kan utgjøre en risiko for foretaket?
- Hvilke sårbarheter fant red team og hvordan reagerte foretaket på angrep?

## For samfunnet

- Trygge felles infrastruktur og stabilitet
- Mye er likt på tvers av foretak
- Påvirkes en, påvirkes tilliten til alle

Klikk for å legge til tekst

# Samarbeid

Norges Bank TCT-NO
Finanstilsynet

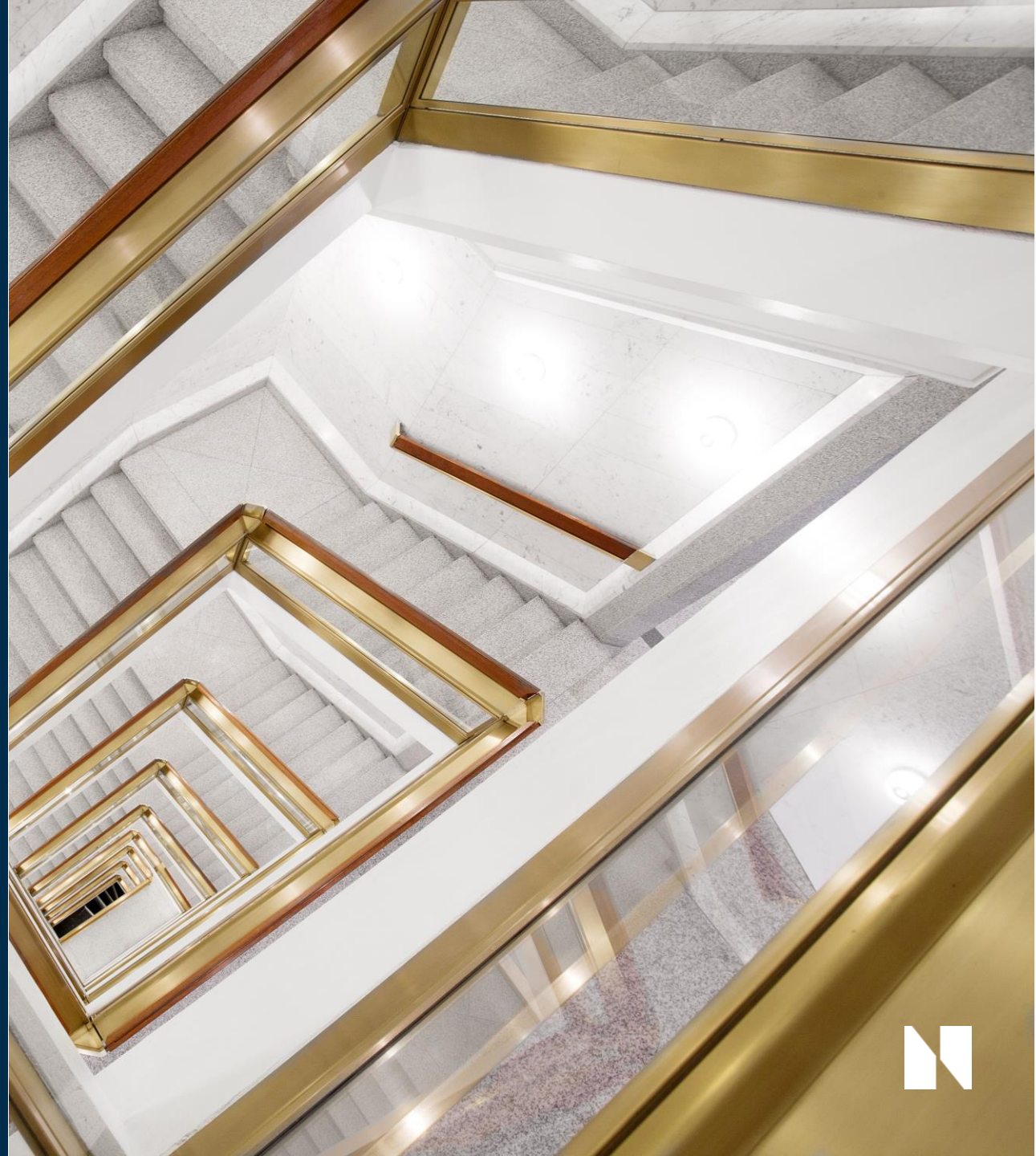
Foretaket som testes
- White team
- Blue team

NFCERT
Red Team leverandør
Trusseletterretning leverandører

# Utfordringer

## Hvilke erfaringer har vi?

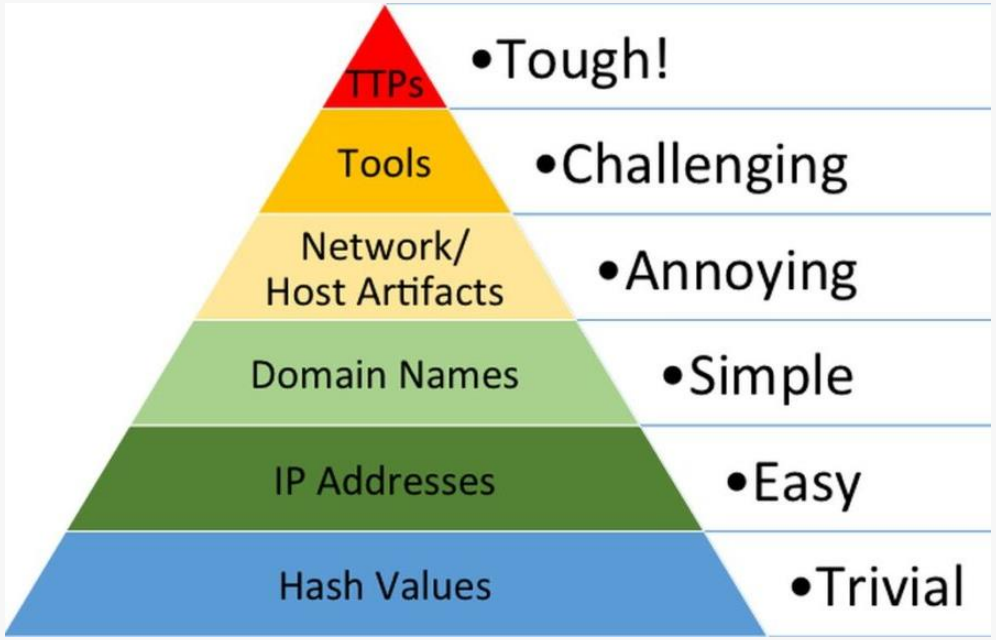
- Hemmelighold og OPSEC
- Fallgruven ved definering av kritiske funksjoner
- Lage realistiske scenarioer
- Når skal testen avsløres?
- Venter for lenge med å bruke legups



# Trussel-emulering

Hvordan emulere en trusselaktør presist med begrenset tid og ressurser?

- Zero Trust og NSM Grunnprinsipper
- Generic Threat Landscape fra NFCERT
- MITRE TTPs
- Tenk som en angriper og vær kreativ
- En ekte angriper har ubegrenset tid forberedelse
- TIBER testing er forskjellig fra sikkerhetstesting



# Oppsummering

Samarbeid

Høy kvalitet

TIBER passer for flere enn finanssektoren

# TIBER

TIBER står for Threat Intelligence-Based Ethical Red-teaming, og er et felles-europeisk rammeverk der myndigheter, finansforetak og leverandører samar-beider om testing av cybersikkerhet i det finansielle systemet.

## TIBER-EU

TIBER-EU er retningslinjer utarbeidet av ECB for å teste finansielle institusjoners evne til å oppdage, beskytte seg mot og reagere på avanserte cyberangrep.

Bruk av målrettet trusseletterretning og eksterne testspesialister («Red Team») bidrar til at testingen blir realistisk. Viktige IKT-systemer testes ved å etterligne taktikk, teknikk og prosedyrer som benyttes av reelle trusselaktører. Hensikten er å oppdage sårbarheter slik at risikoreduserende tiltak kan iverksettes.

Et standardisert oppsett for testing i Europa bidrar til sammenlignbare vurderinger av

## Last ned

- Implementeringsveiledning TIBER-NO (pdf)
- Angrep for bedre forsvar - presentasjon av TIBER-NO på Betalingsformidlingskonferansen 2021 - Av direktør Anna Grinaker (pdf)
- TIBER-NO Leg-Up Guidance 1.1 (pdf)
- TIBER-NO Scope specification - TEMPLATE - v1.2 (pdf)
- TIBER-NO Test Process Overview v1.0 (pdf)
- TIBER-NO WT and TCT Rules of Engagement - TEMPLATE 1.2 (pdf)

# Spørsmål?