# ZERO TRUST

SOLDIER


GÖRAN TOMTE

# Hvorfor gikk det som det gikk?

GÖRAN TÖMTE

# Hvem her tror uvedkommende er på innsiden nå?

GÖRAN TÖMTE

# Hvem her tror uvedkommende IKKE er på innsiden nå?

GØRAN TØMTE

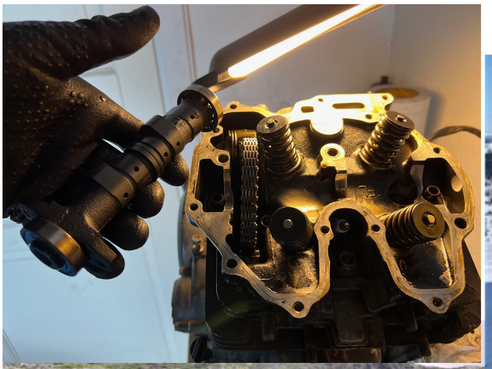
# GÖRAN TÖMTE

## Zero Trust Soldier -> Optimalisering av sikkerhet

Working to change and enhance. Start with the mindset.

«Suksessfulle hendelser skjer i tillatt trafikk»

CISO (ISO 27001) 5 år
Palo Alto Networks 5 år
Selvstendig siden 2023



GÖRAN TÖMTE

NORSK SIKKERHETS-FORENING

DET KONGELEGE JUSTIS- OG BEREDSKAPSDEPARTEMENT

SIKKERHETS FESTIVALEN

nfea

EIK

ISF

iKiNS

Sikkerhetssymposiet

HackCon
The Norwegian cyber security convention

CSA cloud security alliance®

# 1. Januar 2023



## Teknisk CISO Konsulent Arkitektur / Design

Teknisk CISO "for hire". CISO med ISO 27001, og mange år som teknisk ressurs, gir Gøran en bred og relevant kompetanse. Kombinasjonen av disse fagområdene i en person kan man kalle en teknisk CISO.

- Sikkerhetsrådgiver
- Sikkerhetsarkitekt

LES MER

## Revisjon

- En teknisk revisjon i forhold til kjente angrep og hvilke tiltak som hadde gjort en forskjell
- Palo Alto Networks Best Practices.

LES MER

## Rådgivning

- Zero Trust
- Generell sikkerhet, basert på ISO 27001, CIS CSC og NSMs Grunnprinsipper for IKT-sikkerhet

LES MER

## Workshop

- Zero Trust
- Segmentering
- Hvitelisting
- VG-testen
- MFA. SSO

LES MER

## Palo Alto Networks

- BPAT. Best Practice Assessment Tool
- TISP. Threat Insights Security Posture Assessment.
- Expedition tool
- AIOps

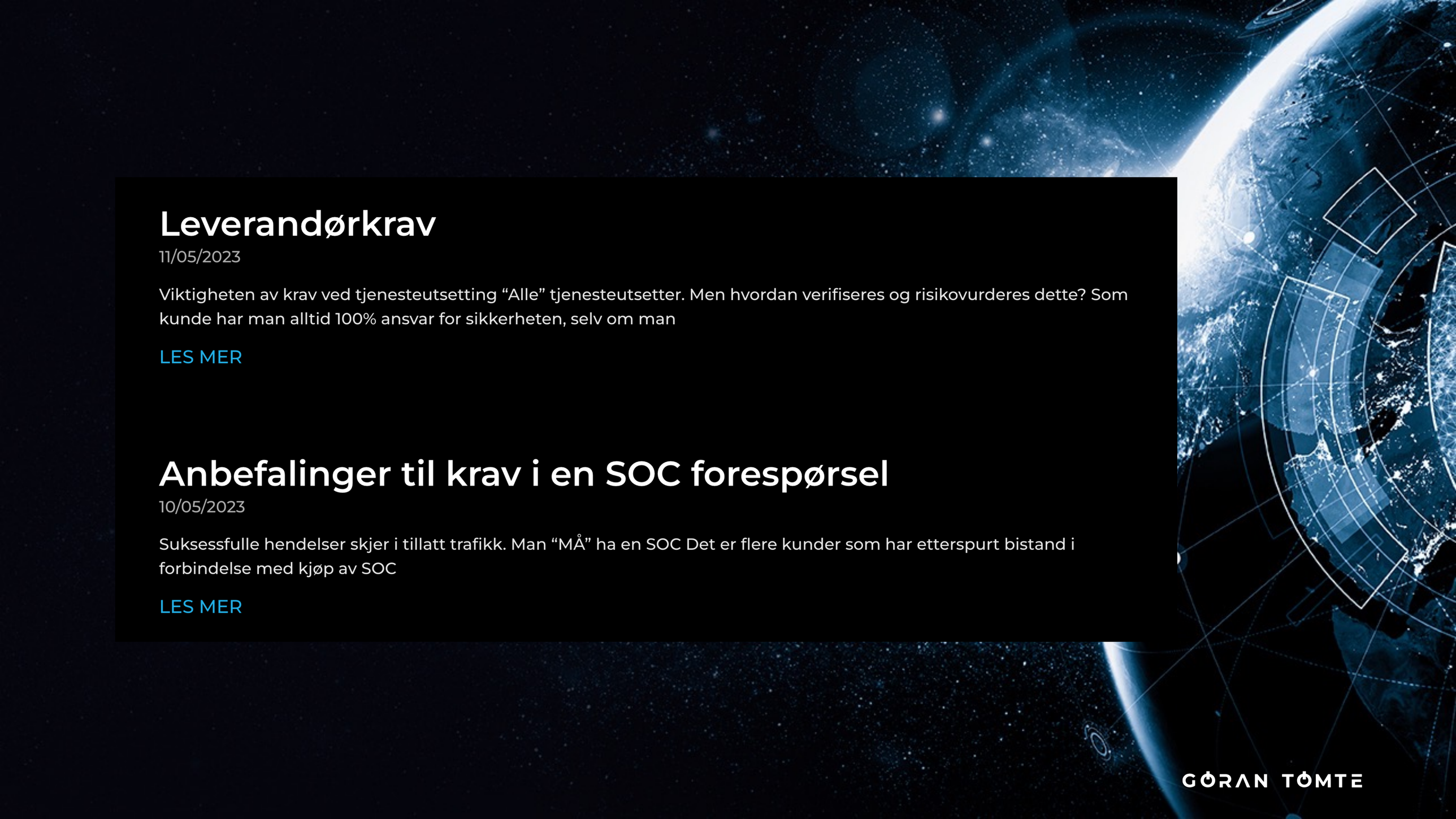
LES MER

## Foredrag

- Zero Trust. On-prem, cloud og SaaS
- Generell sikkerhet. En sårbarhet kommer sjelden alene (Ref NSM)
- Dagens trusselbilde
- Intern sikkerhetskultur.

LES MER

GÖRAN TÖMTE



## Leverandørkrav

11/05/2023

Viktigheten av krav ved tjenesteutsetting “Alle” tjenesteutsetter. Men hvordan verifiseres og risikovurderes dette? Som kunde har man alltid 100% ansvar for sikkerheten, selv om man

LES MER

## Anbefalinger til krav i en SOC forespørsel

10/05/2023

Suksessfulle hendelser skjer i tillatt trafikk. Man “MÅ” ha en SOC Det er flere kunder som har etterspurt bistand i forbindelse med kjøp av SOC

LES MER

GÖRAN TÖMTE

# Hvorfor gikk det som det gikk?

La oss se på noen kjente hendelser

GÖRAN TÖMTE

# Hvorfor gikk det som det gikk?

Østre Toten kommune

9. Januar 2021. 300 fagsystemer. Alt borte. Ingen logg

| Hendelse | Phishing | Passord | Sårbarhet | På innsiden | MFA innsiden | Segmentering med Least Privilege | Logging med SOC | VG testen | DNS | URL | IPS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Østre Toten kommune | ❓ | ❓ | ❓ | ✅ | ✅ | ✅ | 🤷‍♀️ | ✅ | ❓ | ❓ | ❓ |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

GÖRAN TÖMTE

# Hvorfor gikk det som det gikk?

Nordland FYLKESKOMMUNE

## Desember 2021. VPN. Print Nightmare. Endepunktsikring. Alarm. Mennesker. 6 måneder

| Hendelse | Phishing | Passord | Sårbarhet | På innsiden | MFA innsiden | Segmentering med Least Privilege | Logging med SOC | VG testen | DNS | URL | IPS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Østre Toten kommune | ❓ | ❓ | ❓ | ✅ | ✅ | ✅ | 🤷‍♀️ | ✅ | ❓ | ❓ | ❓ |
| Nordland fylkeskommune | ❓ | ✅ | ✅ | ✅ | ✅ | ✅ | 🤷‍♀️ | ✅ | ✅ | ✅ | ✅ |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

GÖRAN TÖMTE

# Hvorfor gikk det som det gikk?


## September 2019. Mars 2020. Desember 2020.

FireEye. Supply Chain. DNS. Backdoor. Spionasje. Gud i nettverket

| Hendelse | Phishing | Passord | Sårbarhet | På innsiden | MFA innsiden | Segmentering med Least Privilege | Logging med SOC | VG testen | DNS | URL | IPS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Østre Toten kommune | ❓ | ❓ | ❓ | ✅ | ✅ | ✅ | 🤷‍♀️ | ✅ | ❓ | ❓ | ❓ |
| Nordland fylkeskommune | ❓ | ✅ | ✅ | ✅ | ✅ | ✅ | 🤷‍♀️ | ✅ | ✅ | ✅ | ✅ |
| Solarwinds Orion | ❌ | ❌ | ❌ | ✅ | ✅ | ✅ | 🤷‍♀️ | ✅ | ✅ | ✅ | ❓ |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

# Hvorfor gikk det som det gikk?

## Desember 2021

Ikke en bug. Worked as designed. Stor utbredelse. Vil eksistere i tiår

| Hendelse | Phishing | Passord | Sårbarhet | På innsiden | MFA innsiden | Segmentering med Least Privilege | Logging med SOC | VG testen | DNS | URL | IPS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Østre Toten kommune | ❓ | ❓ | ❓ | ✅ | ✳️ | ✳️ | 🤷‍♀️ | ✳️ | ❓ | ❓ | ❓ |
| Nordland fylkeskommune | ❓ | ✅ | ✅ | ✅ | ✳️ | ✳️ | 🤷‍♀️ | ✳️ | ✳️ | ✳️ | ✳️ |
| Solarwinds Orion | ✖️ | ✖️ | ✖️ | ✅ | ✳️ | ✳️ | 🤷‍♀️ | ✳️ | ✳️ | ✳️ | ❓ |
| Log4Shell | ❓ | ✖️ | ✅ | ✅ | ✳️ | ✳️ | 🤷‍♀️ | ✳️ | ❓ | ❓ | ✳️ |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

# Hvorfor gikk det som det gikk?

DSS

Departementenes sikkerhets- og serviceorganisasjon

## April-juli 2023

Ivanti Endpoint Manager Mobile (EPMM). Exchange.

| Hendelse | Phishing | Passord | Sårbarhet | På innsiden | MFA innsiden | Segmentering med Least Privilege | Logging med SOC | VG testen | DNS | URL | IPS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Østre Toten kommune | ❓ | ❓ | ❓ | ✅ | ❇️ | ❇️ | 🤷‍♀️ | ❇️ | ❓ | ❓ | ❓ |
| Nordland fylkeskommune | ❓ | ✅ | ✅ | ✅ | ❇️ | ❇️ | 🤷‍♀️ | ❇️ | ❇️ | ❇️ | ❇️ |
| Solarwinds Orion | ✖️ | ✖️ | ✖️ | ✅ | ❇️ | ❇️ | 🤷‍♀️ | ❇️ | ❇️ | ❇️ | ❓ |
| Log4Shell | ❓ | ✖️ | ✅ | ✅ | ❇️ | ❇️ | 🤷‍♀️ | ❇️ | ❓ | ❓ | ❇️ |
| DSS | ✖️ | ✖️ | ✅ | ✅ | ❓ | ❓ | ❇️ | ❓ | ❓ | ❓ | ❓ |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

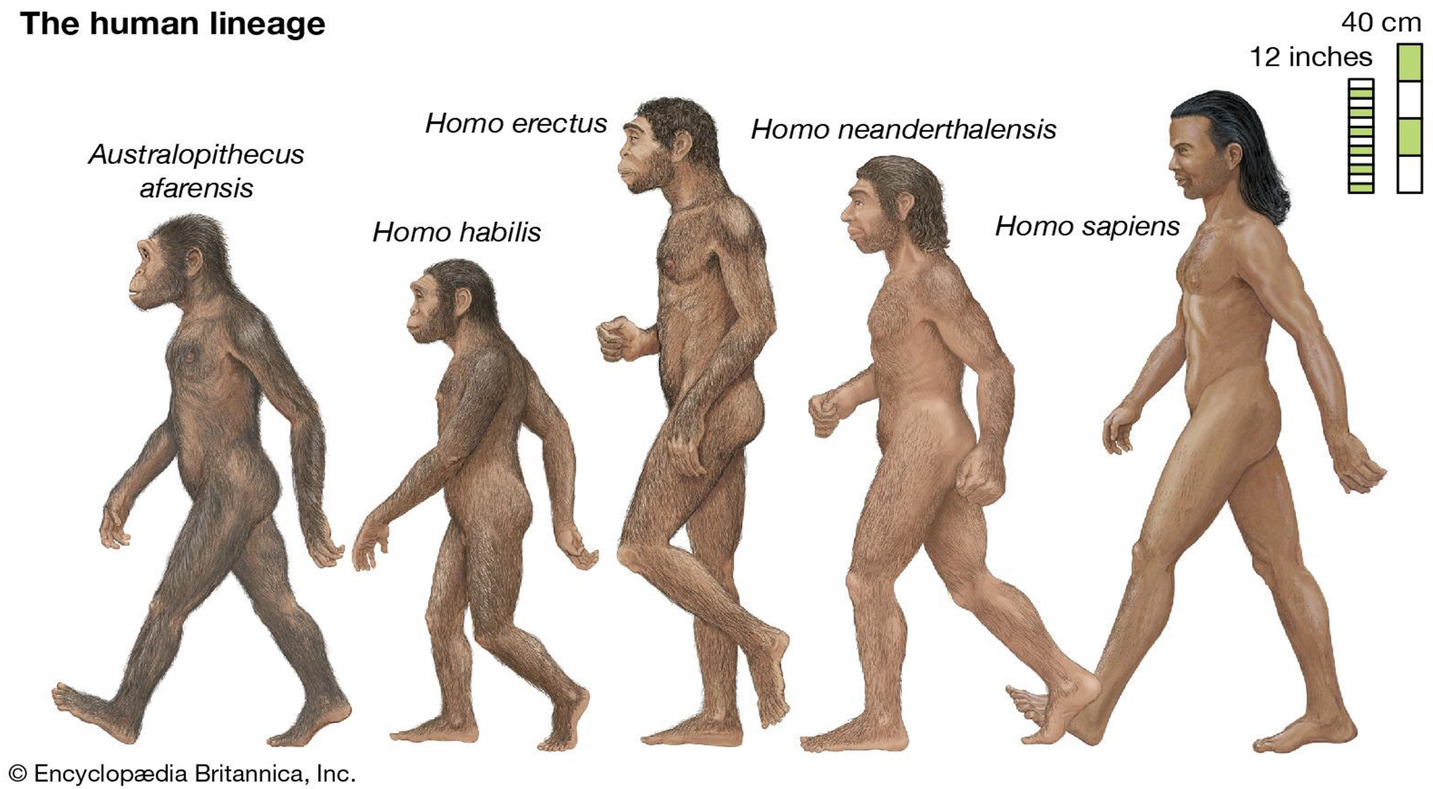
GÖRAN TÖMTE

# Konklusjon

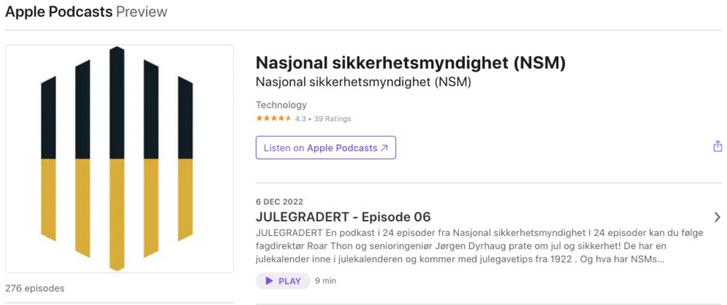
# Hvorfor gikk det som det gikk?

**Suksessfulle hendelser skjer i tillatt trafikk!**

- Det er mennesker som tillater
  - Applikasjoner
  - Nettverk
  - Tilganger
  - SaaS
  - Cloud
  - DevOps
  - Mennesker
  - Maskiner
- **Kommunikasjon!**



# Hvorfor gikk det som det gikk?




## Sårbarheter forekommer sjeldent alene

Publisert: 20.04.2022 Oppdatert: 03.05.2022

***Av sjefsingeniør i Nasjonalt cybersikkerhetssenter i NSM John Bothner. Denne kronikken sto først på trykk i digi fredag 15. april 2022***

Skipet Titanics skjebne og dataangrep i dagens Norge

**I disse dager er det 110 år siden passasjerskipet Titanic sank. Ca. 1500 mennesker omkom i denne tragiske ulykken i april 1912. Kan vi lære noe av denne katastrofen som er relevant for dataangrep? Ja, for det viser seg at i begge tilfeller så er det en serie med samtidige «sårbarheter» som er til stede.**

DEBATT

## *Sårbarheter forekommer sjelden alene*

Sjefingeniør John Bothner ved Nasjonalt cybersikkerhetssenter i NSM sammenligner sårbarhetene ved Titanic-forliset med dagens sårbarheter som åpner for dataangrep.

Sjefingeniør John Bothner ved Nasjonalt Cybersikkerhetssenter i NSM skriver at det gjerne skal flere sårbarheter til før katastrofen kan skje. *Foto: Privat, Willy Stöwer (maleri)*

GÖRAN TÖMTE

# Hvorfor gikk det som det gikk?

## CYBER KILL CHAIN®

*Lockheed Martin's Cyber Kill Chain® and Intelligence Driven Defense® services identify and prevent cyber intrusion activity. The services monitor what the adversaries must complete in order to achieve their objective.*

**A : ADVANCED**
*Targeted, Coordinated, Purposeful*

**P : PERSISTENT**
*Month after Month, Year after Year*

**T : THREAT**
*Person(s) with intent, opportunity, and capability*

1. **RECONNAISSANCE**
*Harvesting email addresses, conference information, etc*

2. **WEAPONIZATION**
*Coupling exploit with backdoor into deliverable payload*

3. **DELIVERY**
*Delivering weaponized bundle to the victim via email, web, USB, etc*

4. **EXPLOITATION**
*Exploiting a vulnerability to execute code on victim's system*

5. **INSTALLATION**
*Installing malware on the asset*

6. **COMMAND & CONTROL (C2)**
*Command channel for remote manipulation of victim*

7. **ACTIONS ON OBJECTIVES**
*With 'Hands on Keyboard' access, intruders accomplish their original goal*

*Learn how defenders have the advantage at:*
**lockheedmartin.com/cyber**

LOCKHEED MARTIN



GÖRAN TÖMTE

# Hvorfor gikk det som det gikk?

**D**ata
**A**pplications
**A**ssets
**S**ervices

.. fra innsiden og ut.....

GÖRAN TÖMTE

# Hvorfor gikk det som det gikk?

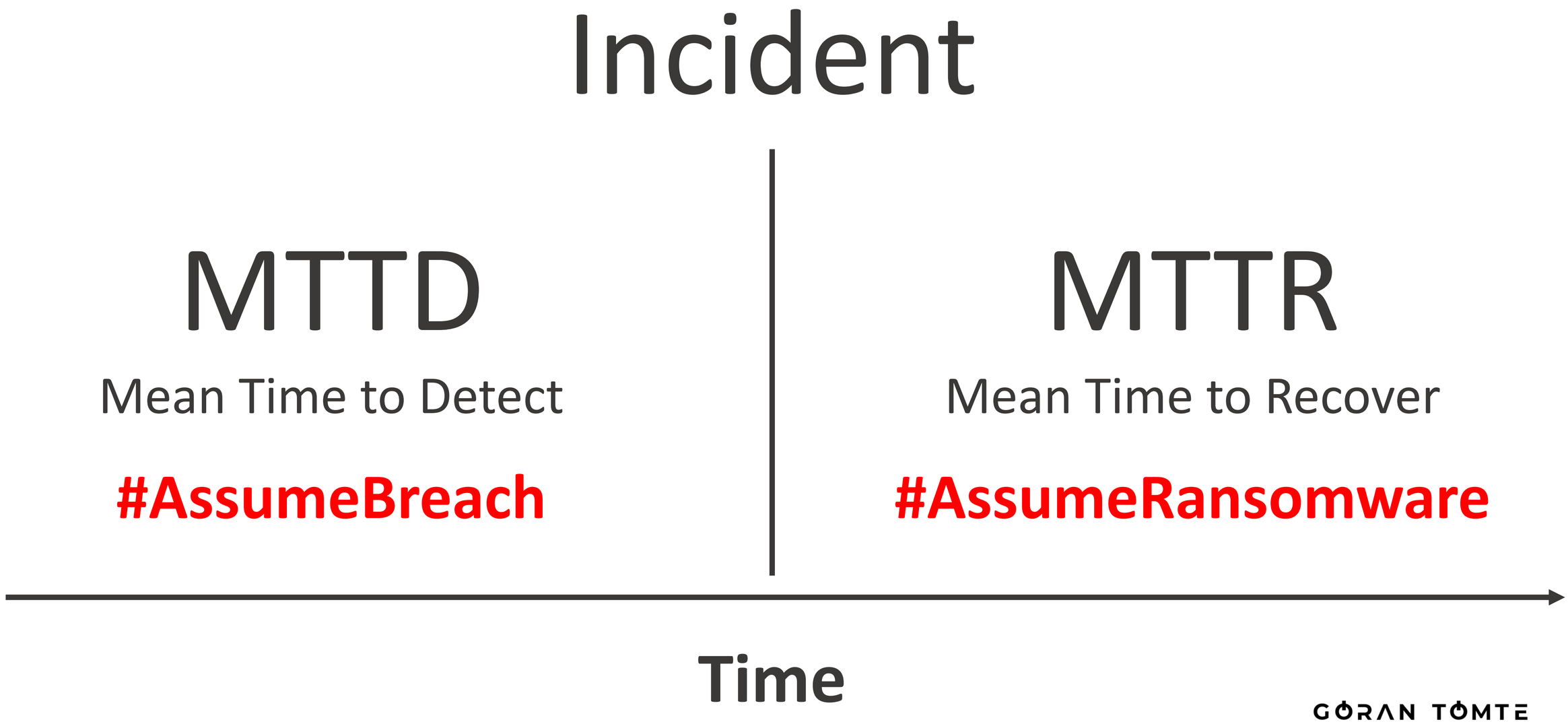
#AssumeBreach

#AssumeRansomware

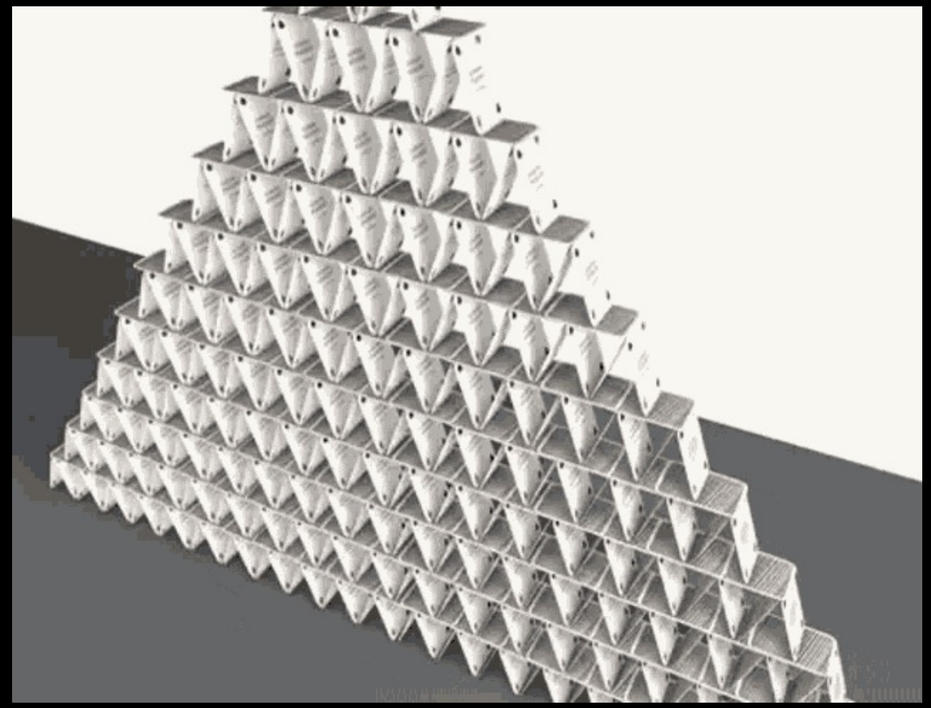
**Fordi det er det beste for deg/dere**

**Assuming the opposite is the recipe for disaster**

# Hvorfor gikk det som det gikk?




NOU Norges offentlige utredninger 2023: 17
Nå er det alvor
Rustet for en usikker fremtid



GÖRAN TÖMTE

# Matrise


## Suksessfulle hendelser skjer i tillatt trafikk.

Denne matrisen har til hensikt å belyse kjente hendelser og vise hva som kunne avverget hendelsene. Det er skrevet en artikkel om hver hendelse som er tilgjengelig ved å klikke på navnet til hendelsen.

Hva kunne avverget eller vanskeliggjort hendelsen? Alle foretak har teknologi. Mange har mye og fantastisk teknologi. Alle har endepunktsikkerhet. Alle har e-postsikkerhet. Allikevel skjer suksessfulle hendelser. Alle suksessfulle hendelser skjer i tillatt trafikk, så det er derfor viktig å fokusere på hva man tillater for på den måten å redusere angrepsflaten maksimalt.

Alle har sikkerhet, og alle har sikkerhetsteknologi. Teknologi er nødvendig, men mennesker setter ofte altfor stor lit til denne og kan da bli utsatt for skadelige hendelser allikevel. Det er derfor viktig å tenke mer **proaktivt og preventivt** for å være enda bedre rustet i dagens trusselbilde. Tanken med matrisen er å synliggjøre noen få tiltak som vil vise seg å være effektive tiltak ved flere kjente hendelser.

GÖRAN TÖMTE

| | MFA på eksterne DAAS | MFA på interne DAAS | Segmentering med Least Privilege | VG testen (Least Privilege) | Sentralisert logging med SOC | Klienter ut av nettet med Always-On VPN |
|---|---|---|---|---|---|---|
| **Black Basta ransomware** | Nei | Ja | Ja | Ja | Ja | Ja |
| **Log4J sårbarheten** | Nei | Ja | Ja | Ja | Ja | Nei |
| **SolarWinds Orion** | Nei | Ja | Ja | Ja | Ja | Nei |
| **Østre Toten kommune** | Ja | Ja | Ja | Ja | Ja | Usikkert |
| **Nordland fylkeskommune** | Ja | Ja | Ja | Ja | Ja | Usikkert |


# TAKK FOR MEG

LinkedIn GÖRAN TÖMTE