2-faktor –
en falsk trygghet

Jens Dale Røttereng
Jens@atea.no

Jens Dale Røttereng

Sjefskonsulent

Hendelseshåndterer

Microsoft 365 Certified Enterprise Administrator Expert

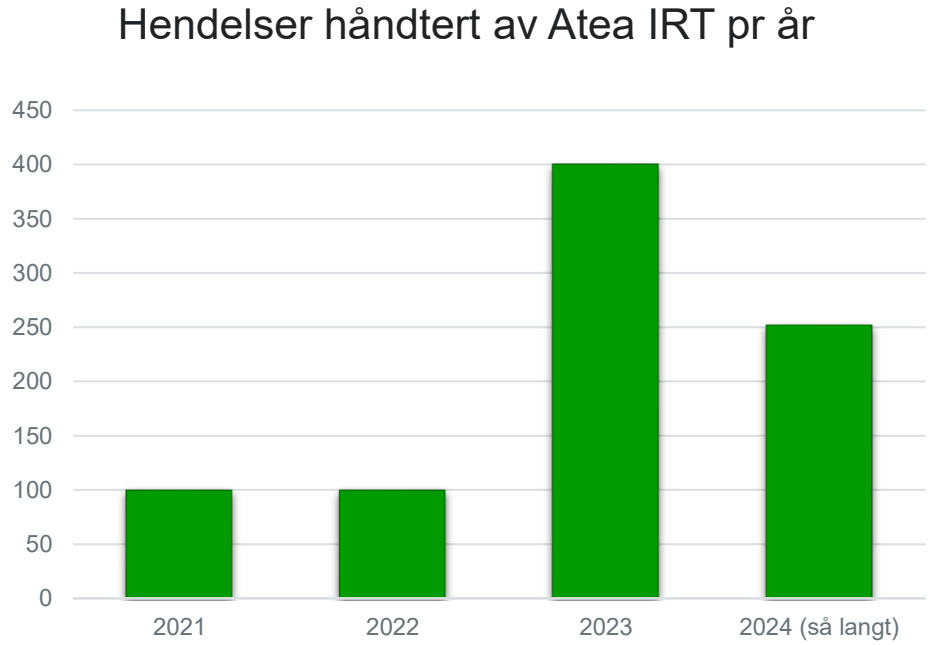
Microsoft 365 Certified Security Administrator

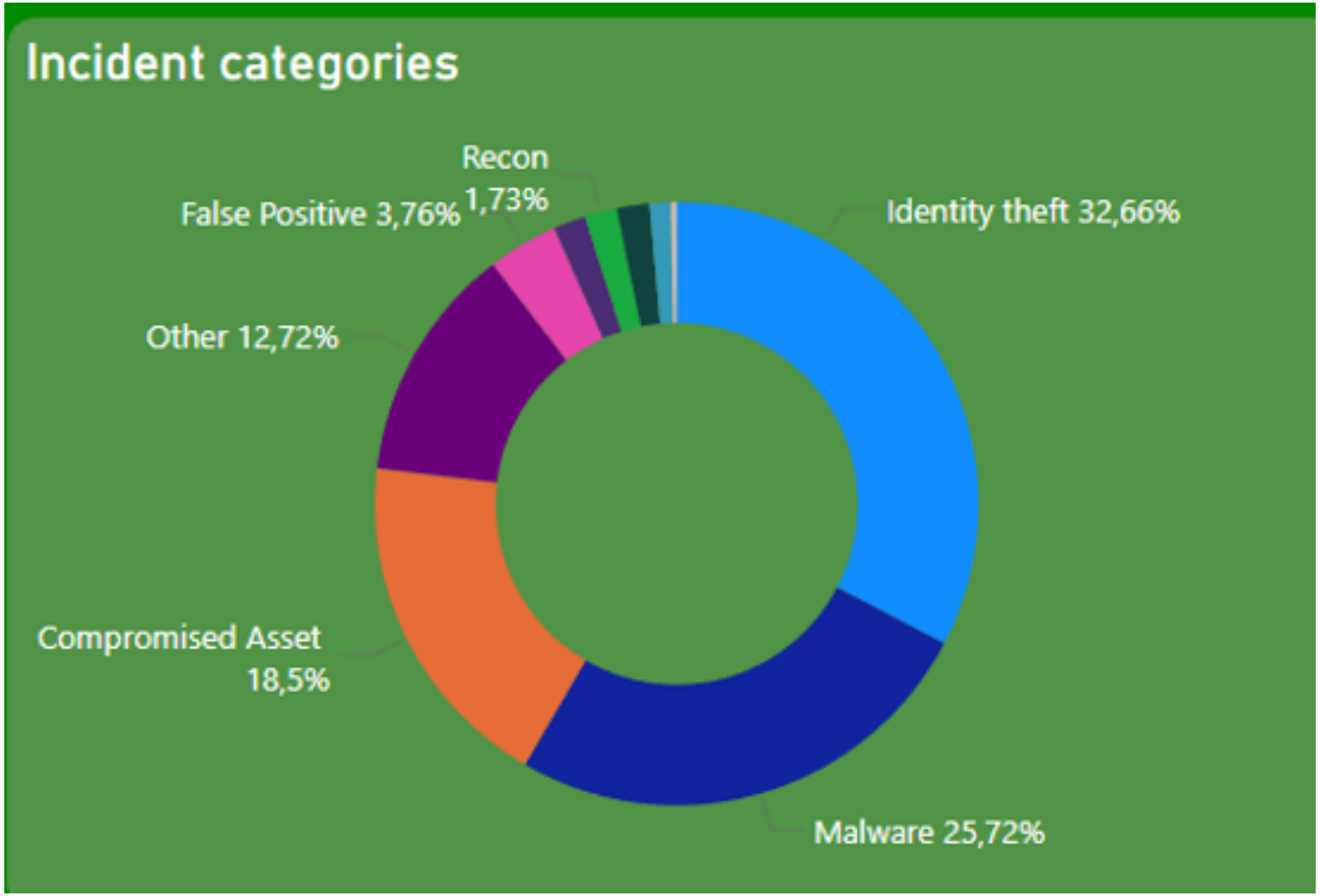
Microsoft 365 Certified Messaging Administrator

Blue Team Level 1

Atea IRT – Incident Response Team

- Team fordelt i hele Norge.
  - 16 konsulenter
- Spesialisert på kritisk hendelseshåndtering i forbindelse med datakriminalitet og angrep.
- Inngår i NSMs ordning for Hendelseshåndtering.
- Dyp innsikt i det gjeldende trusselbildet og bred erfaring fra hendelseshåndtering i kompromitterte miljøer.





Ordbok

- **AiTM** – Adversary In The Middle
- **BEC** - Business Email Compromise
- **Reverse proxy** – Tjeneste for publisering av tjenester (Netscaler, BigIP, etc.)
- **Evilginx** – Reverse proxy laget for phishing
- **Token/Session token** – «Billett» lagret i browseren din for tilgang til en løsning.

Hensikten med AiTM-phishing

https://www.nrk.no/norge/nrk-svindlet-for-naer-en-million-kroner-1.16621474

AiTM - Hvordan fungerer det

Brukers enhet

Bruker går på en lenke og får spørsmål om å godkjenne pålogging

Angripers enhet

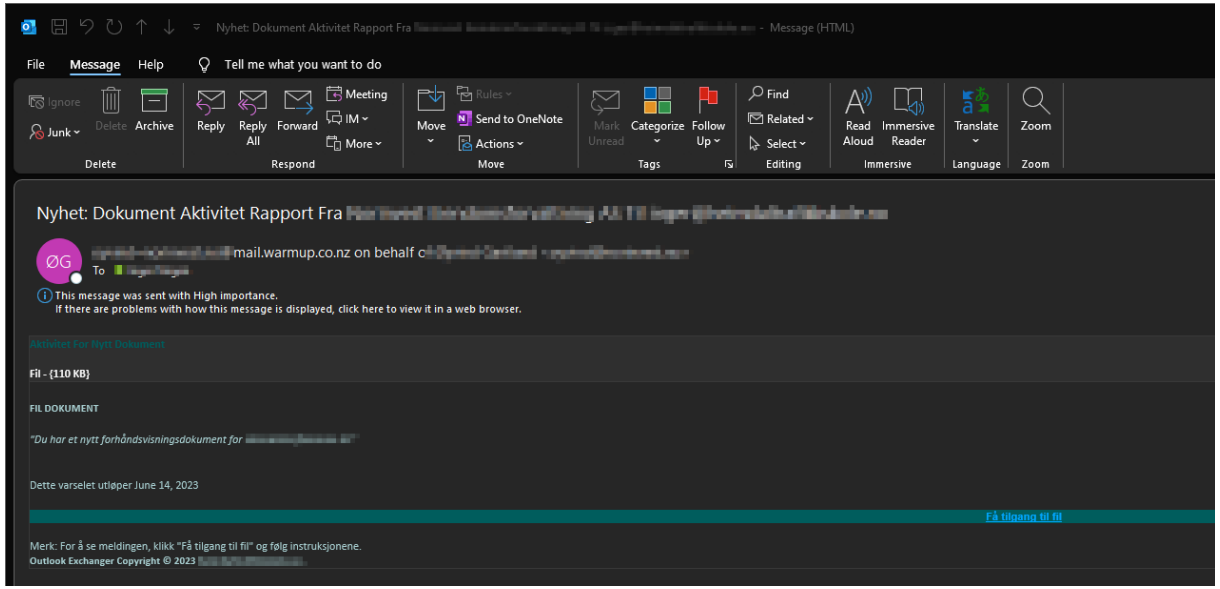
Pålogging utføres på angripers enhet i stedet for brukerens, uten at bruker merker det.

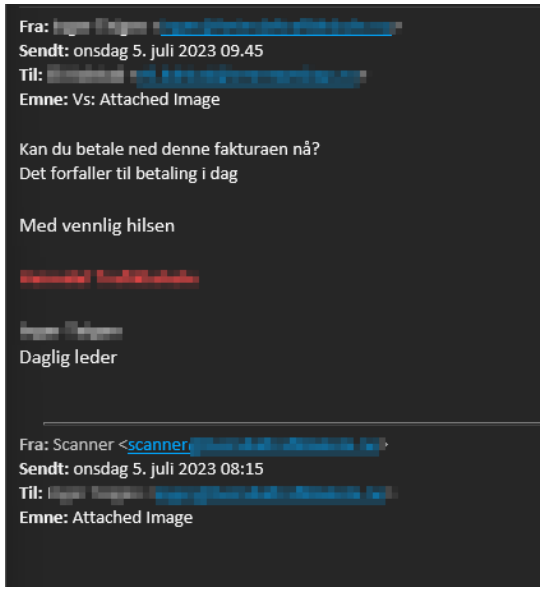
Skytjeneste

Skytjenesten ser bare påloggingsforsøk fra angripers enhet, ikke fra brukerens enhet

Case - AiTM

Dato	Klokka	Hendelse
13.06	12:54	Mottok mail som utga seg for å være huseier. "Nyhet: Dokument Aktivitet Rapport Fra <firma>"
13.06		Klikket på link. URL går mot https://app.seesaw[.]me/#/item/item.f2cb6a67-47f1-8872-4fde0757d531/share/H-Oi_OskQFiaJgvbRigJ4A
13.06	13:02	Generert inboxregel for å gjemme mailer fra utleier.
15.06	07:42	Generert inboxregel for å gjemme mailer med subject/body som inneholder "Visma".
04.07	20:10	Innlogging fra Oslo (VPN server) (146[.]70.103.88)
04.07	20:00	Innlogginger fra Toronto Ontario CA (149[.]57.28.216)
05.07	07:53	Innlogging fra Oslo (VPN server) (82[.]102.27.101)
05.07	08:13	Generert inboxregel for å gjemmer mailer fra "josephdunbar0@gmail.com".
05.07	08:15	Mottok mail fra josephdunbar0@gmail.com. "Attached Image". Dette er mailen som er videresendt etterpå. Inneholder en PDF med en falsk faktura.
05.07	08:36	Lagt til regnskapsfører i inboxregel for å gjemme mailer.
05.07	09:45	Mail sendt til regnskapsfører. Emne "vs:attached Image".
05.07	10:00	Regnskapsfører lukter lunta og kontakter kunde. Først på mail, som blir gjemt, deretter på telefon.
05.07	13:00	Kunde kontakter Atea.

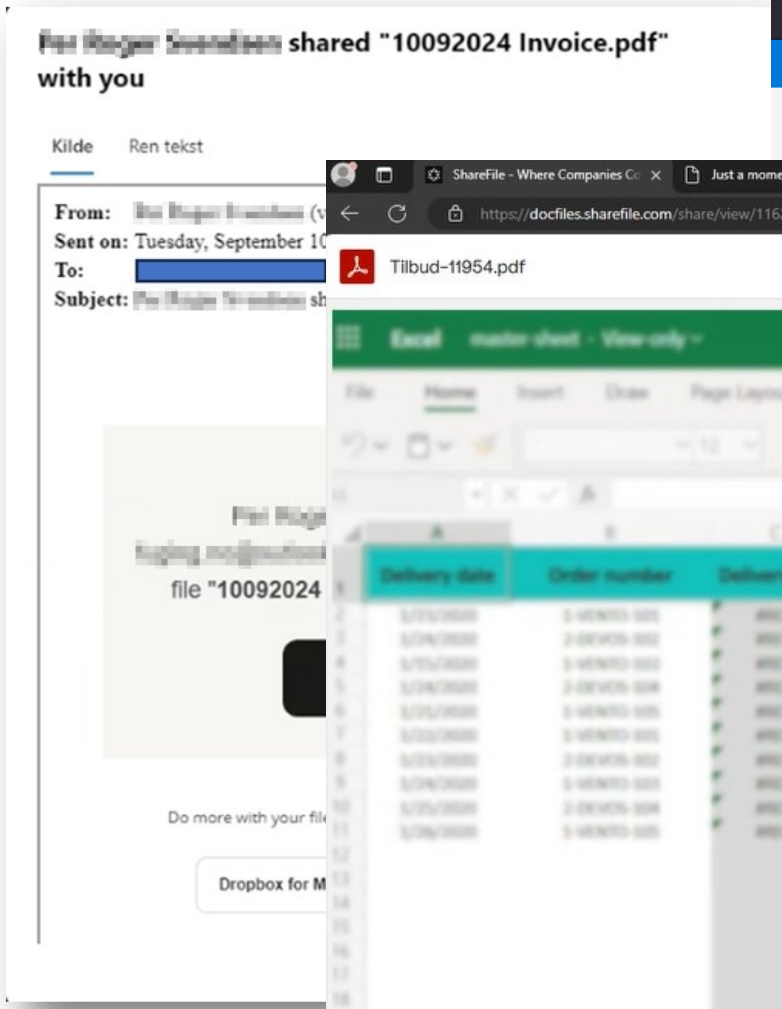


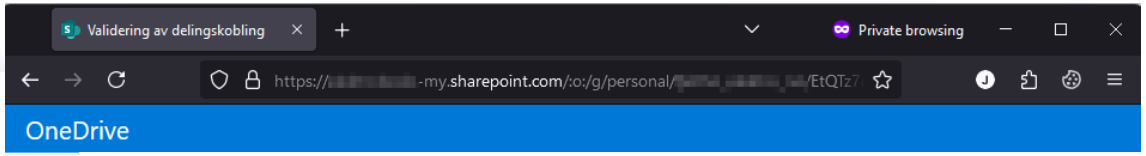


ATEA Incident Response Team

AiTM – Levering av link

Generasjon	Hva	Beksyttelse
G1	Linker direkte i mail	Safe links, EOP ++
G2	Mailvedlegg med link	Safe Attachments, Safe Links, EOP ++
G3	Teams	Tetting av sikkerehtshull
G4	QR-kode	Utvidelse til Safe Links som leser QR-koder
G5	Legitime fildeltingstjenester delt med kun bruker. Delt fil sender videre til phishing-link.	????
Annet	SMS	





Vennligst finn vedlagte faktura fra

Last ned fakturaen din så snart som mulig.

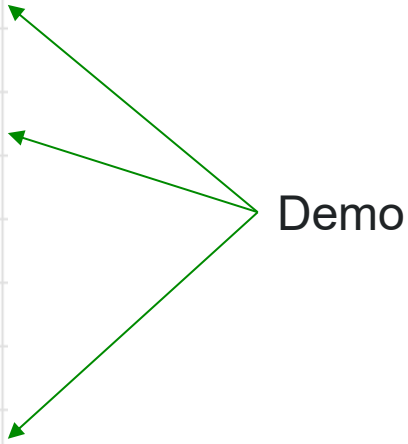
Se vedlagte faktura # 4484747.

Ikke nøl med å kontakte oss hvis du har noen bekymringer eller trenger ytterligere informasjon.

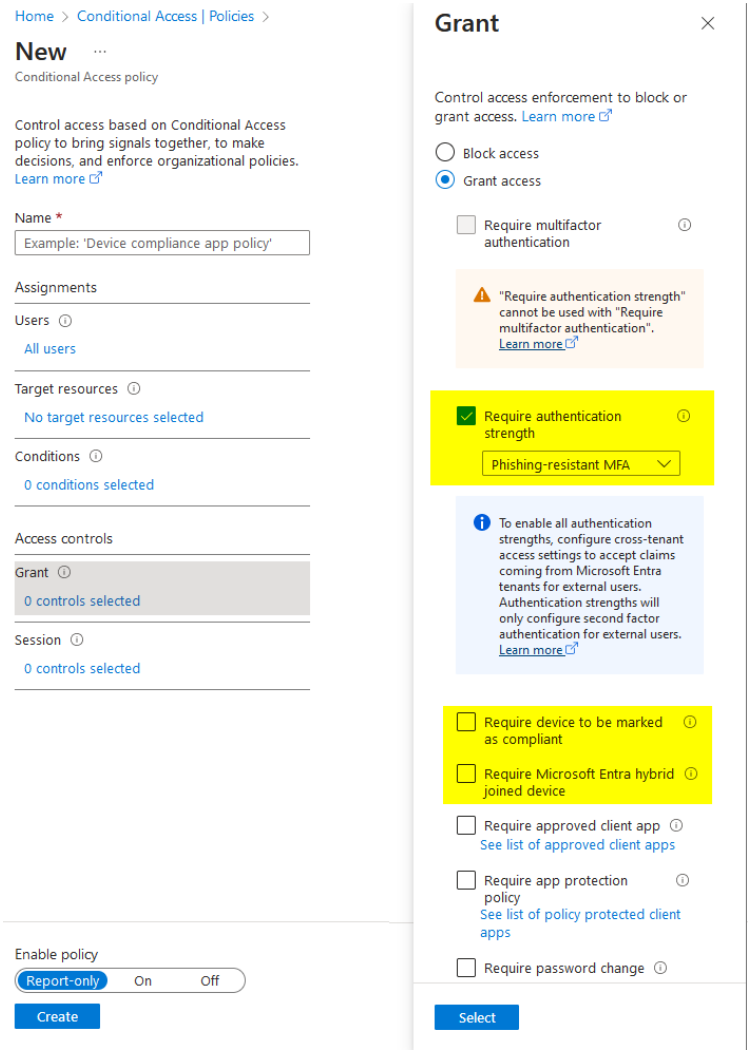
Hilsen.

AiTM – beskyttelse

Metode	Beskyttelse/mitigering mot AiTM
SMS/telefon/Authenticator App	X
Passwordless authenticator/sms	X
Krev compliant/hybrid joined device	✓
AiTM kanari	Varsler ved angrep
Defender for Endpoint	X (Kun varsling ved kjente angreps-nettsider)
Require token protection for sign-in sessions	X
Defender for Office 365	X (Kun ved kjente angreps-nettsider)
FIDO2 sikkerhetsnøkler	✓
Windows Hello for Business	✓
Sertifikatbassert autentisering	✓
Custom Tenant Branding	X



AiTM – beskyttelse – Conditional Access



FIDO/PassKey, Hello For Business, etc

Require Compliant/hybrid joined

AiTM – Oppsummering

Vi har sett følgende demos

- Demo 1: Token hijacking med MFA
- Demo 2: Forsøk på token hijacking med FIDO
- Demo 3: Forsøk på token hijacking med Require Compliant Device

Beskyttelse (som fungerer):

- KREV FIDO 2.0
  - Eller sertifikatbasert autentisering, Windows Hello etc.
- Require compliant/hybrid joined device.
  - Passord er på avveie…

Forberendende tiltak

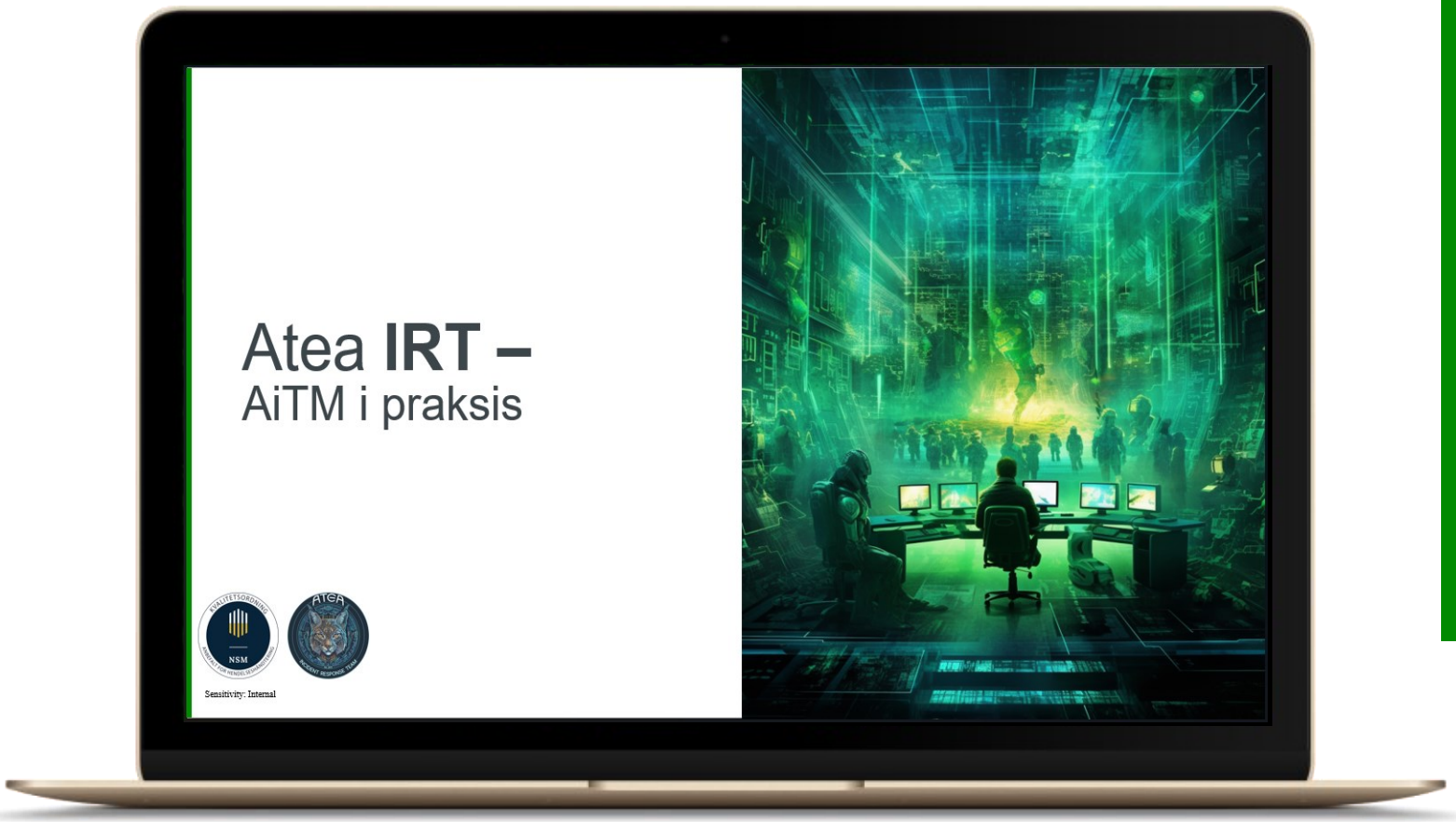
- Sørg for at Audit-logging er aktivert

Hvis uhellet er ute

- Bytt passord og revoke sessions
- Sjekk audit logger
  - Lagt til Authenticator
  - Lagt til inbox-regler
  - Lagt til Enterprise Apps
- Slett mail fra inbox til alle mottakere

ATEA

Jens Dale Røttereng
Jens@atea.no
97764890



Stoler du ikke på QR-koden? Søk etter «Webinar med Atea IRT» på YouTube