unit it

Thomas Boe
Security

Incident response

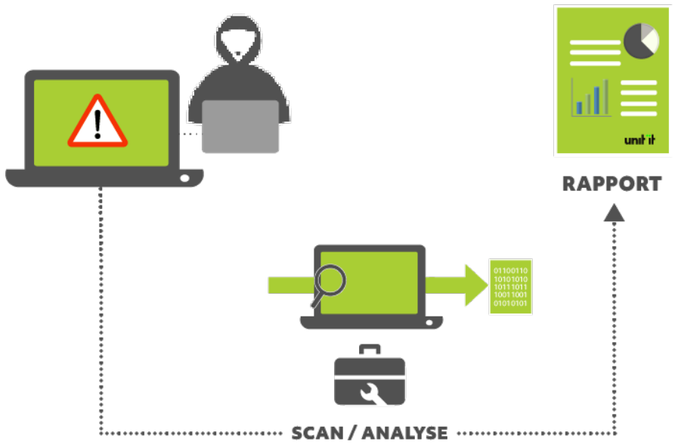
Strategi (en lille smule teknik)

DATA & CLOUD DAGEN VEST
Aarhus
28. september

Incident response..

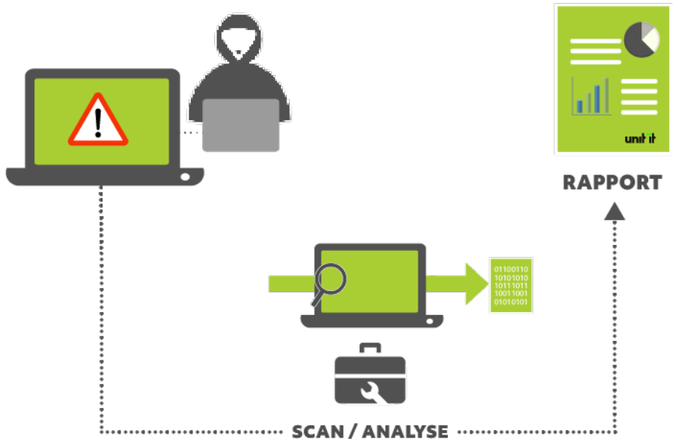
Hvordan håndterer Unit IT kompromitteringer?

Hvilke ressourcer kræver en kompromittering?



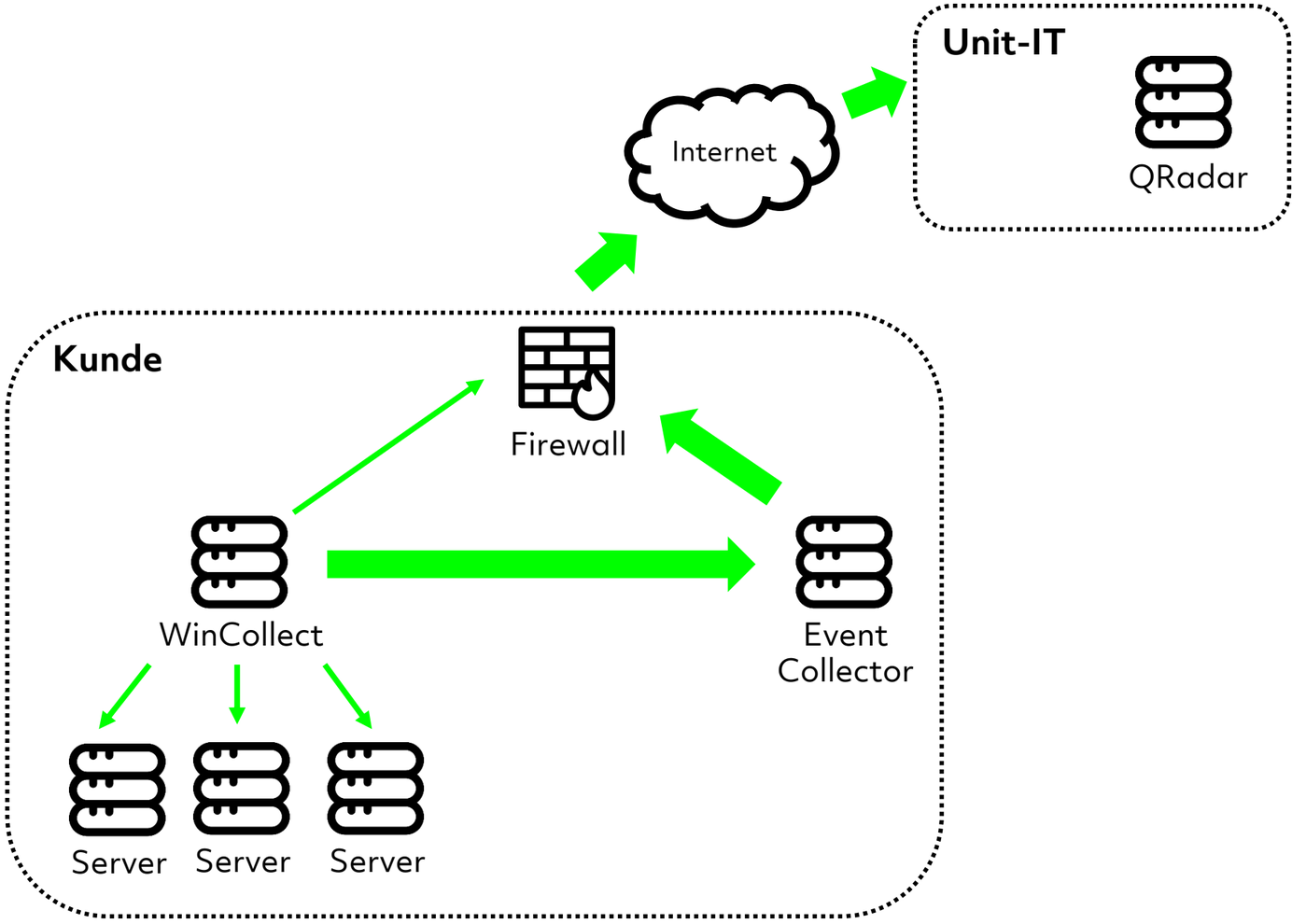
2 veje ind

- Kunden er kendt hos Security
- Kunden er IKKE kendt hos Security



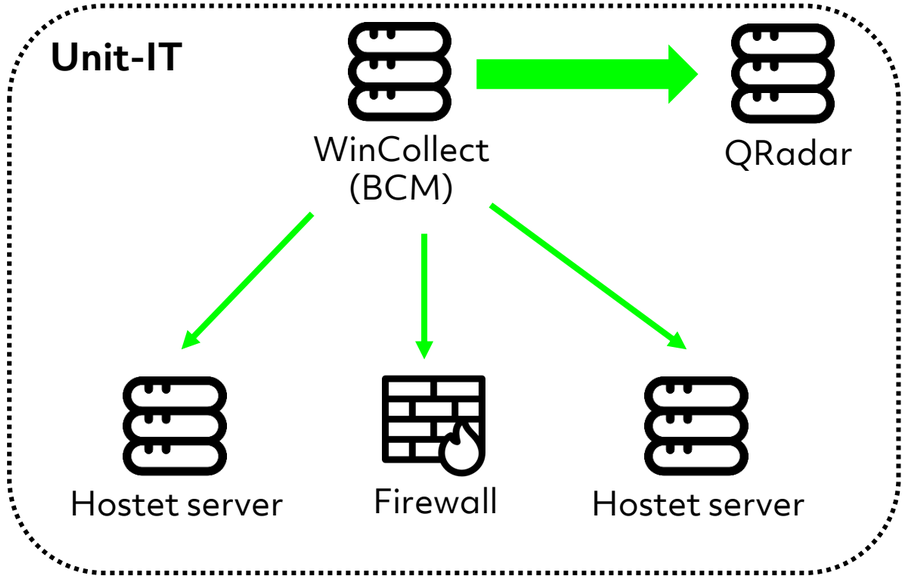
Ikke hostet kunde - servere og udstyr

- Event Collector (appliance)
  - 12 GB RAM, 4 CPU kerner
  - VMware image (skal hostes via VMware)
- WinCollect
  - Installeres på en Windows server (behøver ikke være dedikeret)
- Servere
  - Kan udrulles via GPO eller Endpoint Manager
  - Servicekonto oprettes i AD (Domain Users og Event Log Readers på maskiner)
  - 3 Remote Event Log Management firewall regler aktiveres (*NP-in, RPC, RPC-EPMAP*)
- Firewall
  - Syslog



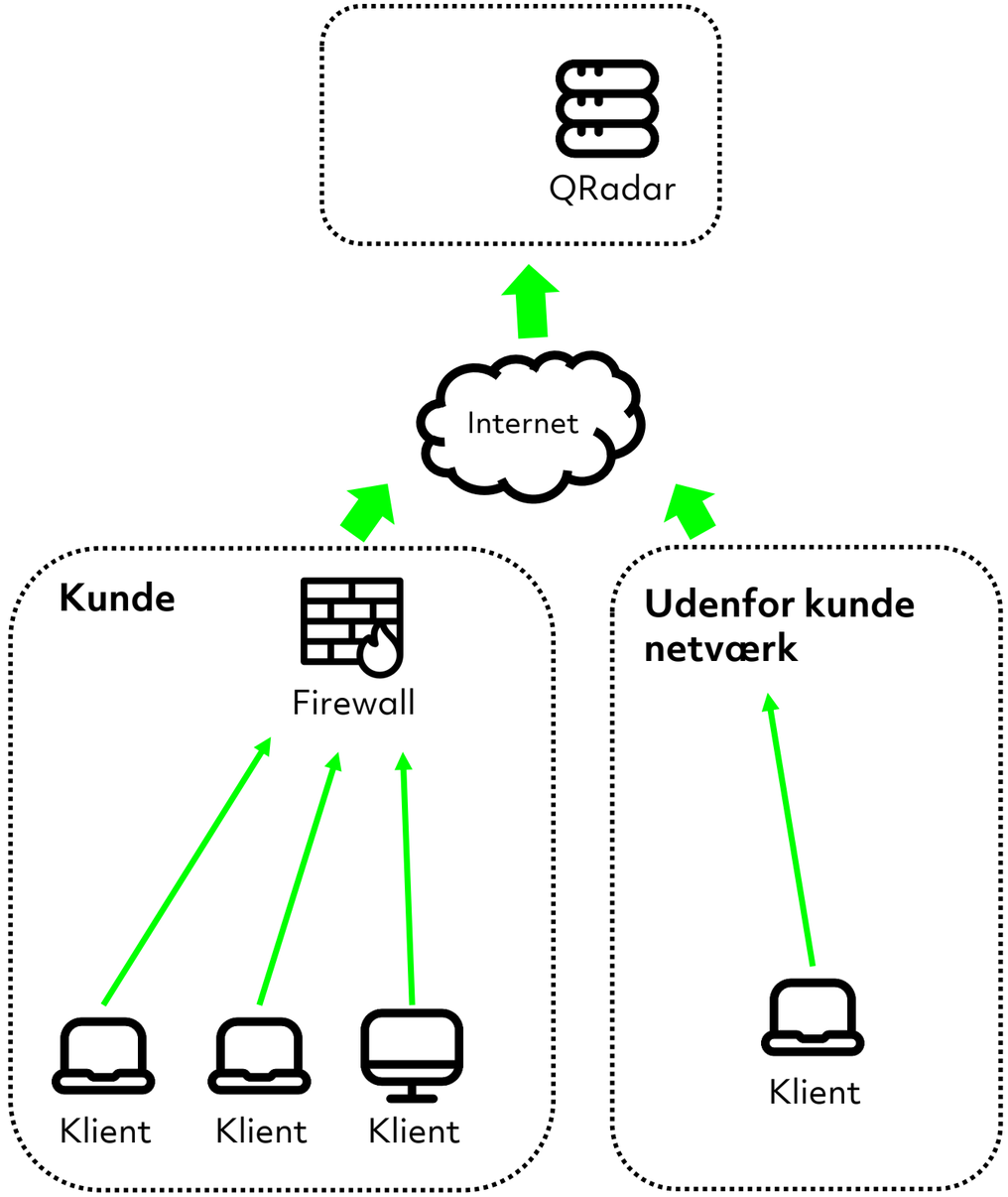
Hostet kunde – servere og udstyr

- WinCollect
  - Installeres på en Windows server typisk BCM
- Servere
  - Kan udrulles via GPO eller Endpoint Manager
  - Servicekonto oprettes i AD (Domain Users og Event Log Readers på maskiner)
  - 3 Remote Event Log Management firewall regler aktiveres (*NP-in, RPC, RPC-EPMAP*)
- Firewall
  - Syslog



Klientmaskiner

- Klientmaskiner
  - Agent installeres på her maskine
  - Kan udrulles via GPO
  - Port 6514 (Syslog over TLS)



Kunde kompromittering

Hvad er udgangspunktet?

Unit har eget CDC

- Vi anvender vores egen velafprøvede model med 6 faser
- Råder over et team af specialister til at igangsætte logindsamling og analyse
- Er man kunde i forvejen kan vi være operationelle på under 2 timer
- Bagudrettet efterforskning mod 'patient ZERO' og tyveri af data
- Fremadrettet efter forsøg på ny kompromittering
- Vi stiller med 24/7 hold bestående af Situation Manager, Team lead, analytikere, AD specialister, forensics m.v.

Overordnet plan fase 1

Vores 6 fasede model er tilpasset gennem anvendelse

- **Forberedelse**: Roller, ansvar, kommunikation*, risk**

Dette er KAOS fasen. **Vi lytter**

Hvornår started det?
Hvem opdagede det?
Hvad er det gjort indtil nu?
Hvilke systemer er involveret nu?
Hvilke ressourcer har kunden selv?
Hvilke teknologier er der tale om? (ICS)

Der laves risikovurdering:
Kan vi komunikere sikkert?
Har der været fysisk kontakt?
Kan Teams være kompromitteret?
Input fra SDM
Har vi ressourcer nok nu?

Overgang til fase 2

Eksempel: Kan vi kommunikere sikkert? alternativt (Signal, Telegram)

Lights Out: Holder nogen øje med jer? Nye tilføjelser på LinkedIn, fysisk sikkerhed – rogue udstyr

Overordnet plan fase 2

Vores 6 fasede model er tilpasset gennem anvendelse

- **Indsamling**: Kritiske systemer, patient zero, IOC, indsaml logs, berig SIEM

Vi kan ikke arbejde uden valide data.

Ordsproget (Så trækker vi netstikket) er noget vås.

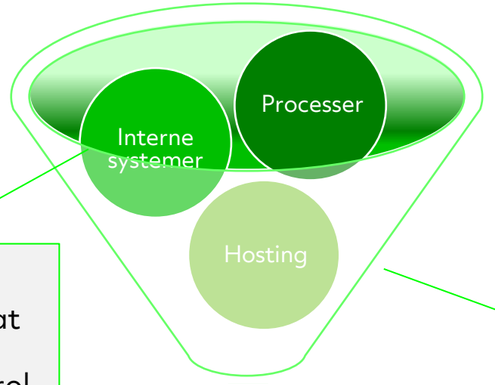
Mini BIA
Forudsætninger for at deploye agents
Etablering af nødvendige adgange
Jagten på patiens ZERO
IOC'er på storyboard så regler kan tunes

SDM er situation manager
Etablering af kommunikationskanaler
Mødeintervaller
Tekniske teams (hvem skal friholdes)

Overgang til fase 3

Business Impact Assessment

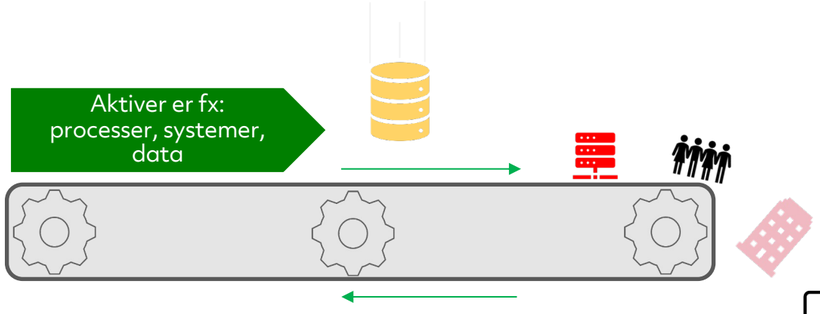
I bør have kontrol over et aktiv og være i stand til at overvåge og udnytte aktivet fuldt ud.



Hvad er der behov for, for at kunne drive og have fuld kontrol over et aktiv?

Hvilke informationsaktiver (komponenter) hjælper med at opfylde målsætningen og hvilke kan muligvis forhindre jer i at nå målsætningen, i tilfælde af, at aktivet bliver beskadiget, forsvinder eller kompromitteres?

Hvad er kritisk for at opfylde målsætningen?



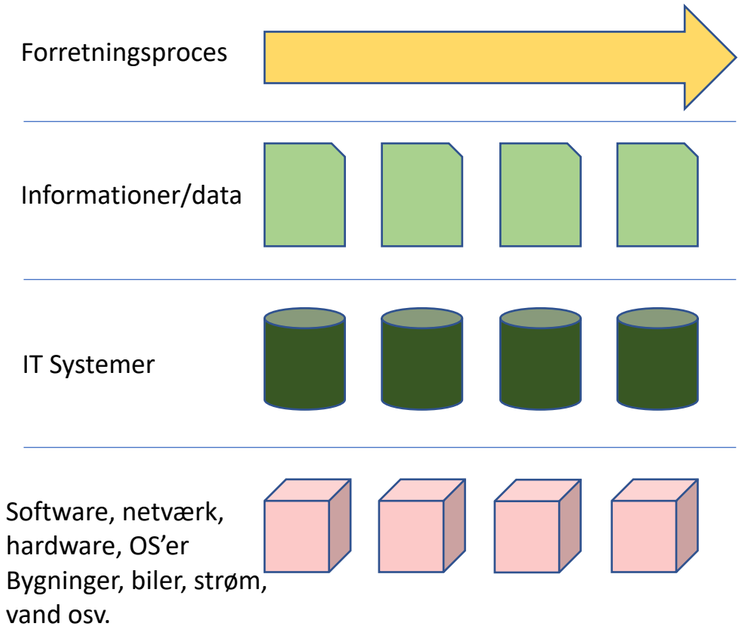
BIA er en metode og proces der følger **ISO31010**, og anvendes til **at vurdere potentielle konsekvenser for forretningskritiske aktiver**, som følge af en katastrofe, ulykke eller nødsituation.

Vi skal bruge data i vurderingen af mulig impact af hændelsen.

Business Continuity

Risikovurdering

Nedbrydningen



Primære aktiver

BYG HUS

Kontrakt, tegning, beregning

Korrespondance, aftale, afvigelse

Projektetablering, styring, ændring

Levering etc.

Supporterende aktiver

CAD program, materialeberegningsportal
Office.

PC'er, telefoner, biler, bygninger
Servere, Unit IT, netværk,

Først skalaer

Skala	Skala til konsekvens ved tab af fortrolighed	Skala til konsekvens ved tab af integritet	Skala til konsekvens ved tab af tilgængelighed
5	Rygtet om kompromittering vil påvirke omdømme ekstremt og medføre målbart tab samt bod/bøde og straf.	0 fejltolerance	Tidskritisk under 1 time
4	Kompromittering af få data vil påvirke kraftigt og medføre tab af omdømme og brud på kontrakter og lovgivning	Promiller op til 1% fejltolerance	Tidskritisk efter 4 timer
3	Kompromittering af alle data fra én eller flere kilder vil medføre lovgivningsmæssige og kontraktlige brud samt tab af omdømme	1-10% fejltolerance	Tidskritisk efter 24 timer
2	Kompromittering af alle data fra flere kilder, vil kunne påvirke omdømme i nogen eller mindre grad	Over 10% fejltolerance	Tidskritisk efter 7 dage
1	Brud kompromitterer ikke fortrolige eller persondata, lav eller mindre mærkbare konsekvenser	Data har ingen signifikant værdi og kan genskabes fra offentlige kilder ved lav til middel indsats	Man kan fungere uden systemet i en længere periode

Lad os tage et eksempel

Kritisk forretningsproces	Information	IT system(er)	Software, applications etc.	Asset / Forretnings Ejer	Konfidalitet	Integritet	Tilgængelighed	Kommentarer	Kritisk?
Hvilke forretningsprocesser	Kritisk forretningsinformation og data: Hvilke informationer er vigtige for forretningsprocessen?	Hvilke(t) system(er) er vigtige for at få udført forretningsprocessen?	Hvilke IT systemer, software, platforme, bygninger og personer der understøtter forretningsprocessen	Hvem er forretningsejer? (Afdeling/Business Unit etc.)	1 (Ingen) 2 (Lav) 3 (Medium) 4 (Høj) 5 (Kritisk)	1 (Ingen) 2 (Lav) 3 (Medium) 4 (Høj) 5 (Kritisk)	1 (Ingen) 2 (Lav) 3 (Medium) 4 (Høj) 5 (Kritisk)	Vil aktivændringen ændre sin kritikalitet baseret på andre faktorer?	Er det et meget kritiske asset?
Bygning Privat									
Bygge Hus	Tegning af hus	CAD Program	PC'er	Projektafdelingen	**2 (Lav)**	**2 (Lav)**	**4 (Høj)**	Nej	
Bygge Hus	Beregning af materialeforbrug	Telefoner	Servere	Finance	**4 (Høj)**	**4 (Høj)**	**3 (Medium)**	Ja	
Bygge Hus	Kontrakt	Office	Telefoner	Salg	**5 (Kritisk)**	**5 (Kritisk)**	**2 (Lav)**	Nej	

Overordnet plan fase 3

Vores 6 fasede model er tilpasset gennem anvendelse

- **Stands ulykken**: Adgange, MFA, systemkonti, legacy, patchniveau, netværk

AD skal have grov gennemgang
Kerberos skiftes
Admin konti gennemgås og skiftes
Systemkonti gennemgås (red flags?)
Dataanalyse, SIEM kommer med resultater

Der kommer nye oplysninger
Kunden opdager hidtil ukendte fakta
Alle opdager uhensigtsmæssigheder
Ingen slår nogen I hovedet

Overgang til fase 4

Overordnet plan fase 4

Vores 6 fasede model er tilpasset gennem anvendelse

- **Fjern årsagen**: Efterretninger, data, filer, spor, forensics data

Patient Zero formodes eller kendes
Hvad er der gået galt (proces, teknologi, menneske)
Hvem er aktøren
Er der etableret bagdøre
Er data stjålet (BIA)
Screenshots
Hackeren tager måske kontakt
Evt. Involvering af gidselforhandler (Ekstern)
Triage af servere og klienter

SDM holder overblikket
Laver liste med arbejdspunkter
Leder og fordeler opgaver mellem Unit
IT og kunden

Overgang til fase 5

Overordnet plan fase 5

Vores 6 fasede model er tilpasset gennem anvendelse

- **Genskab**: Sikre zoner, hærdede enheder, korrekte adgange, hele systemer

Kræver involvering af Operations og Platform teams

Brugere de-aktiveres
Netværk og firewalls genbesøges hvis nødvendigt
Legacy systemer (kan de undværes)
Sårbarheder fjernes (patch)
Test, glemte og ikke anvendte lukkes ned
Backup indlæses i sikker enclave

Her kommer BIA'en til hjælp sammen med CMDB

Overgang til fase 6

Overordnet plan fase 6

Vores 6 fasede model er tilpasset gennem anvendelse

- **Læring**: Hvad er lært, hvad mangler, hvad lykkedes ikke

Arbejde med hærdning fortsættes
Bistand til anmeldelse til Datatilsyn og forsikring
Daglige møder med kundens team
Evaluering fra start til slut
Hvad lykkedes vi ikke med
Hvad gik godt
Hvad skulle vi have gjort anderledes

SDM udarbejder hændelsesrapport med tidslinje

Overgang til 30 dages 24/7

Spørgsmål ?

- **Forberedelse**: Roller, ansvar, kommunikation*, risk**
- **Indsamling**: Kritiske systemer, patient zero, IOC, indsaml logs, berig SIEM
- **Stands ulykken**: Adgange, MFA, systemkonti, legacy, patchniveau, netværk
- **Fjern årsagen**: Efterretninger, data, filer, spor, forensics data
- **Genskab**: Sikre zoner, hærdede enheder, korrekte adgange, hele systemer
- **Læring**: Hvad er lært, hvad mangler, hvad lykkedes ikke

Tak for opmærksomheden

Næste session her starter kl. 10:15
Det bedste forsvar er et angreb!

Muligheder:

Lokale M1 – Skab Effektive Digitale Transformationer
Lokale M2 – Audit og sikkerhed i dit SQL setup
Lokale M4 – Få styr på dine følsomme data (Detectia)

TAK!

Thomas Boe

Mehmet Dagli