ATEA TECH TOUR

Henrik E. H. Nielsen

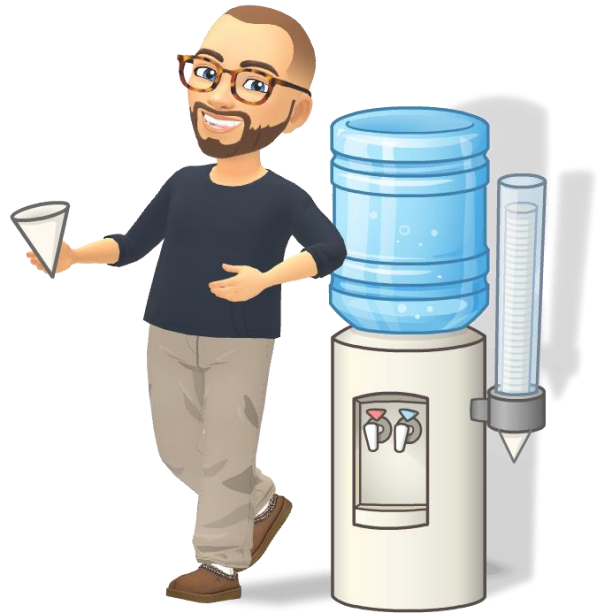
Lead Architect, Secure Workplace, Atea A/S

Thomas G. Rysgaard

Lead Architect, Strategic Security & Advisory, Atea A/S

Microsoft Solutions Partner

- Microsoft Secure Future Initiative
- NIS2 fylder – men hvad med SFI og identitetshygiejne?
- Security Exposure Management
- Defender for Cloud
- Afrunding



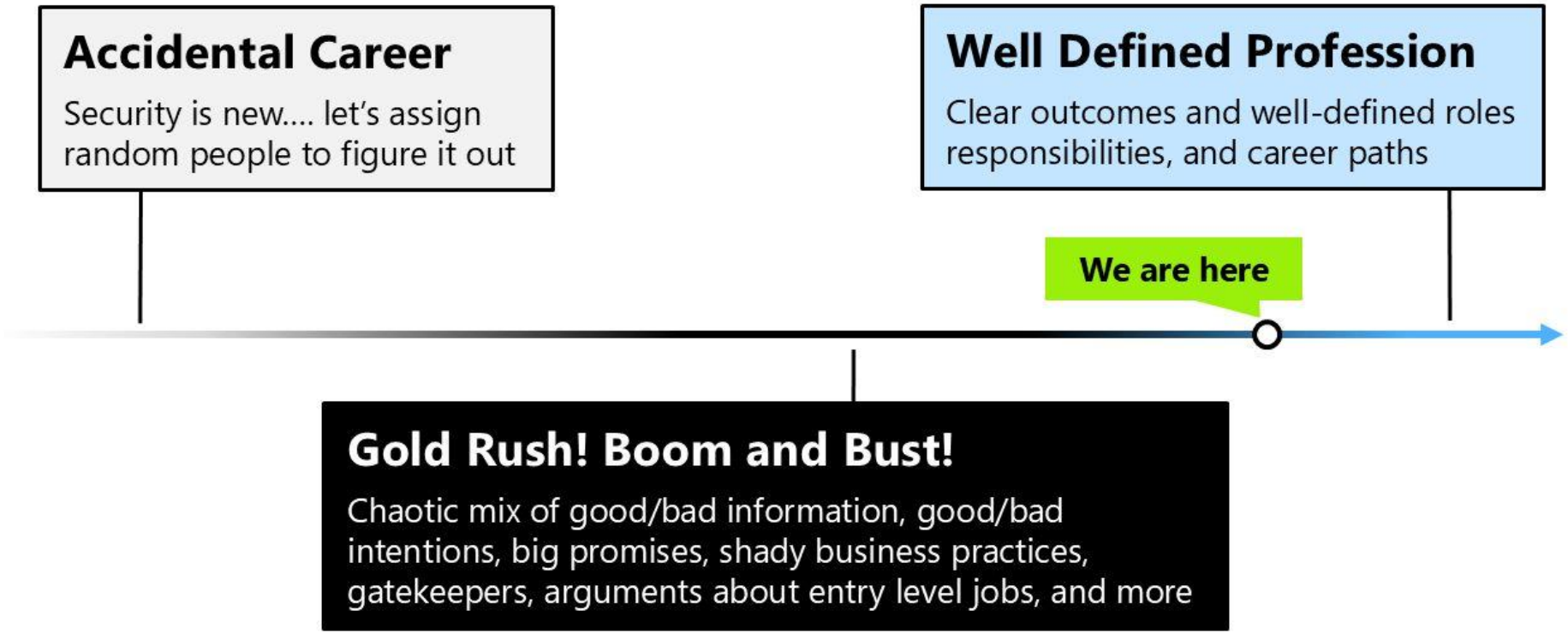
CIO Analytics 2025

- **Nordeuropas største it-undersøgelse**
  - Næsten 1.300 CIO'er og it-beslutningstagere deltager
  - Dækker Danmark, Norge, Sverige, Finland og Baltikum
  - Fokus på prioriteringer, teknologier og udfordringer i 2025
- **Vigtig læsning for IT teknikere**
- **Sikkerhed et gennemgående tema**

https://www.atea.dk/cio-analytics-2025/

ATEA TECH TOUR

Cybersecurity Industry Maturity



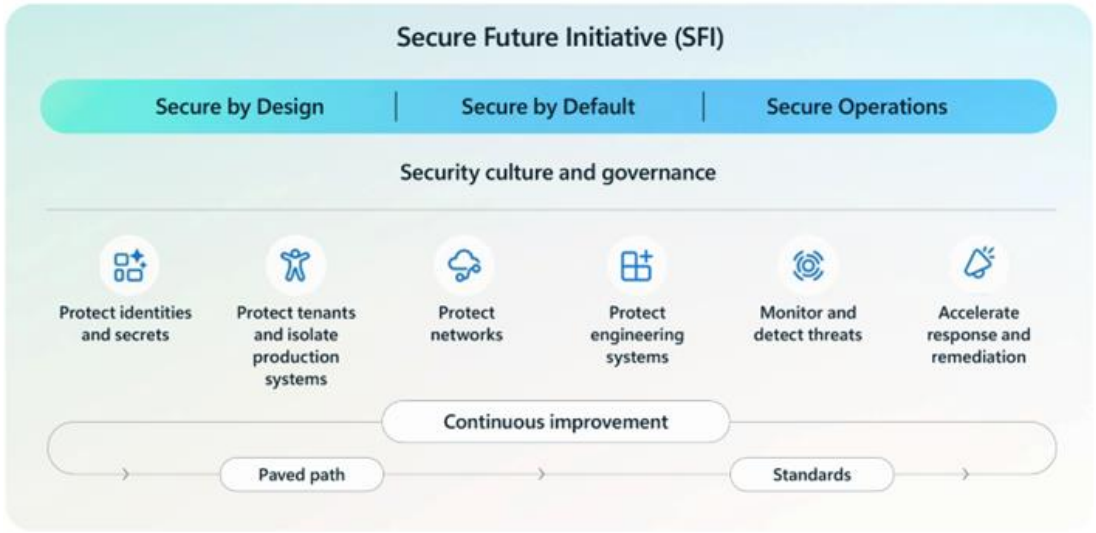
How One Bad Password Ended a 158-Year-Old Business

Sep 24, 2025 The Hacker News Password Security / IT Compliance

- Uden basic security falder alt
- Manglende MFA + gættet password gav adgang
- Ransomware lammede hele infrastrukturen
- Backups og recovery blev destrueret
- Total stop: ingen drift, ingen data

How One Bad Password Ended a 158-Year-Old Business

Hvad SFI (Secure Future Initiative) *egentlig* er



- **SFI = Microsofts flerårige sikkerhedsprogram**: *secure-by-design*, *secure-by-default*, *secure operations*.
- Praktisk oversættelse for organisationer: **identitet først, mindst mulige rettigheder, antag brud** (Zero Trust) – og automatisér evidens.
- SFI's principper **understøtter** NIS2-foranstaltninger; det er ikke reklame for Microsoft, det er *metoden*.

April 2025 rapport

Vi løber efter NIS2 – men ignorerer SFI og basal sikkerhedshygiejne. Hvorfor?

- **Compliance driver budget – ikke risiko.** NIS2 har personligt ledelsesansvar og håndhævelse, derfor får det flyvehøjde. Hygiejnen har ingen pisk.
- **De samme kontroller går igen.** MFA, PIM, patch, logging/IR – NIS2 kalder det governance/foranstaltninger; SFI kalder det secure-by-default; nogen kalder det drift.
- **Uden identitetshygiejne er NIS2-planen tom.** Hvis Global Admins ikke er på phishing-resistent MFA og CA, er art. 21 bare papir.

NIS2 principle	Microsoft solutions
Governance	Microsoft Defender CSPM, Entra, Microsoft Purview Compliance Manager
Risk management	Microsoft Defender XDR, Microsoft Purview Insider Risk Management
Asset management	Microsoft Defender XDR, Microsoft Purview Data Lifecycle Management
Supply chain	Microsoft Defender XDR, Entra, Microsoft DevOps
Service protection	Microsoft Defender XDR
Identity & access	Entra
Encryption	Microsoft Purview Information Protection
System security	Microsoft Defender XDR
Resilient networks	Azure Network Security
Staff awareness	Office 365 Phishing Simulation and Learning Paths, Microsoft Purview in-app notification & policies
Security monitoring	Microsoft Sentinel, Microsoft Purview Insider Risk Management Data Security Posture Management (DSPM)
Proactive security	Microsoft Defender XDR
Response and recovery	Microsoft Defender XDR, Azure Backup and Recovery, Microsoft Purview Insider Risk Management (Adaptive Scop
Incident reporting	Microsoft Purview e-Discovery & Audit

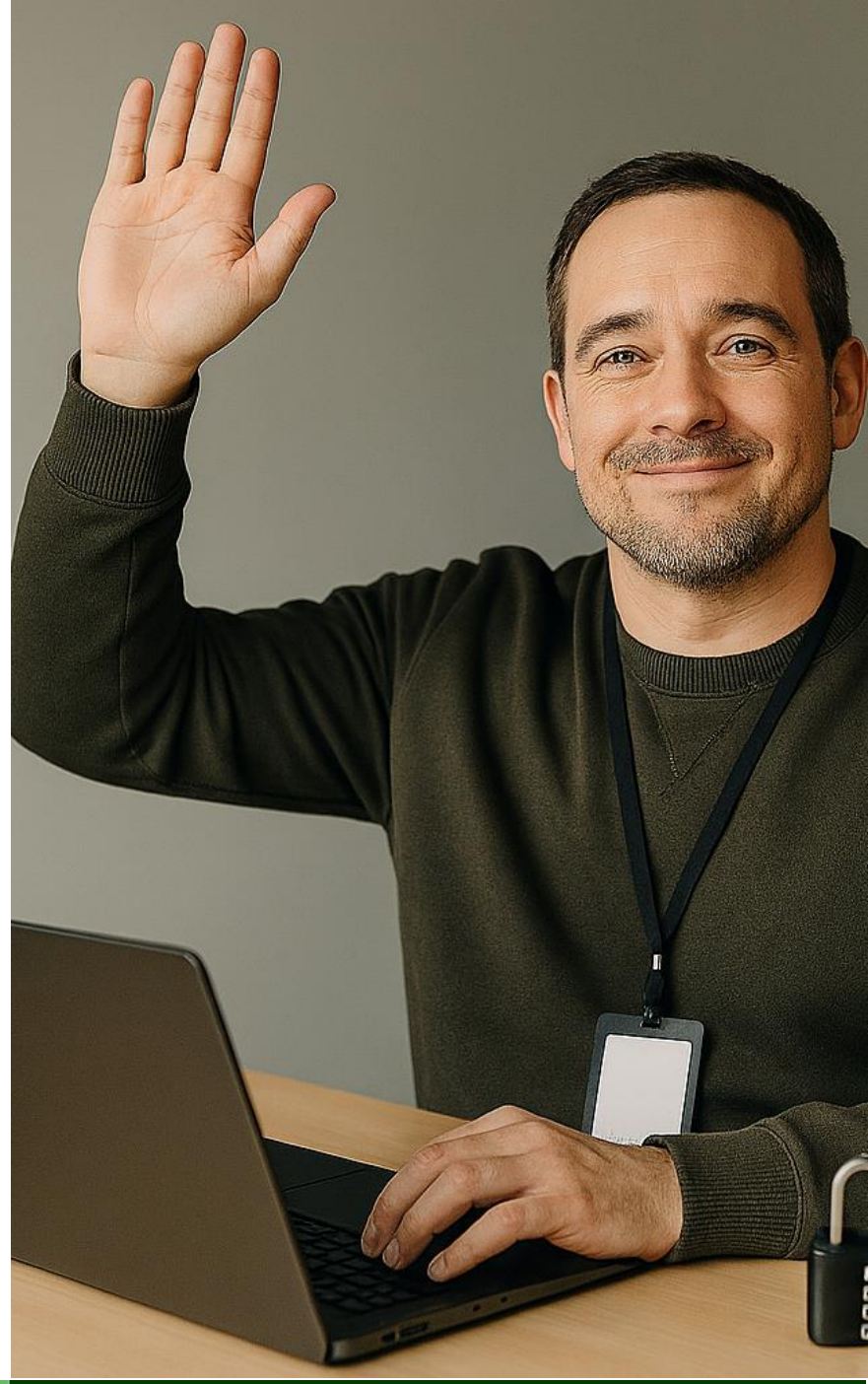
Håndsoprækning

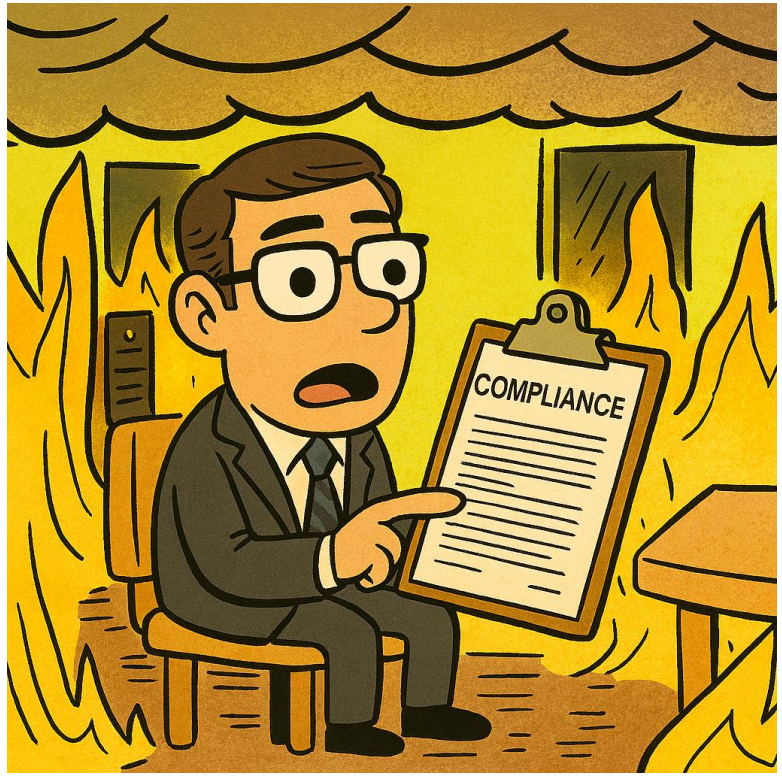
Folketælling:

- **Hvem har en leder-rolle?**
- **Hvem har en operationel rolle?**

Ræk hånden op hvis:

- **I har en dokumenteret NIS2-politik godkendt og forankret i ledelsen.**
- **Alle Global Admins kører phishing-resistent MFA?**
- **I har testet jeres beredskabsplan i år.**



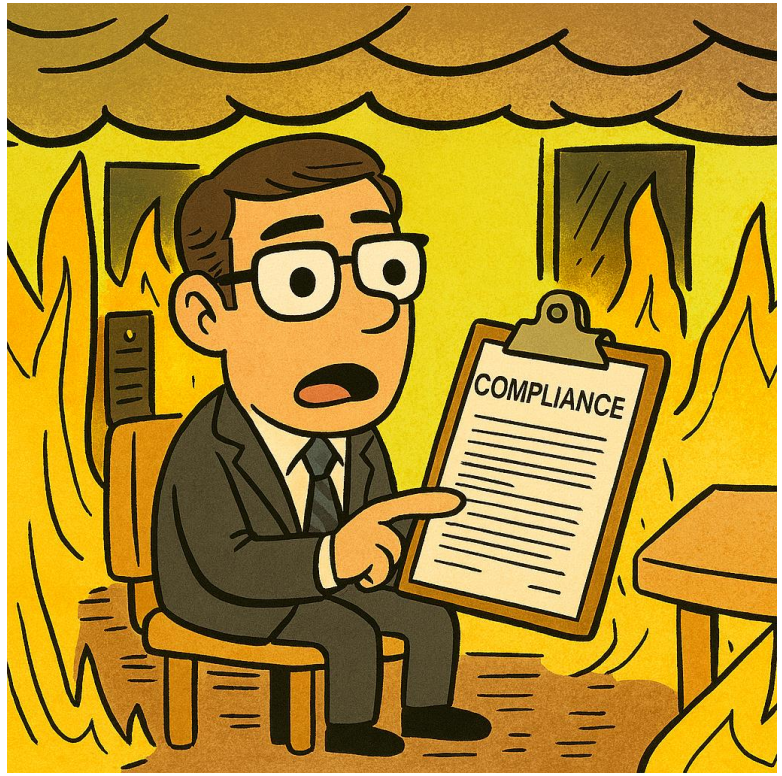


”Men det er compliant...”

Sikkerhed og compliance i balance

Forestil jer tilsynet i næste kvartal:

Vi kan vise politikker og planer (NIS2), men når de spørger efter evidens for **‘hvem kan hvad, hvornår’** og ‘**hvordan stopper I laterale bevægelser**’, peger vi så på **CA-politikker, PIM-logs og Sentinel-playbooks**—eller på et Excel-ark?



”Men det er compliant...”

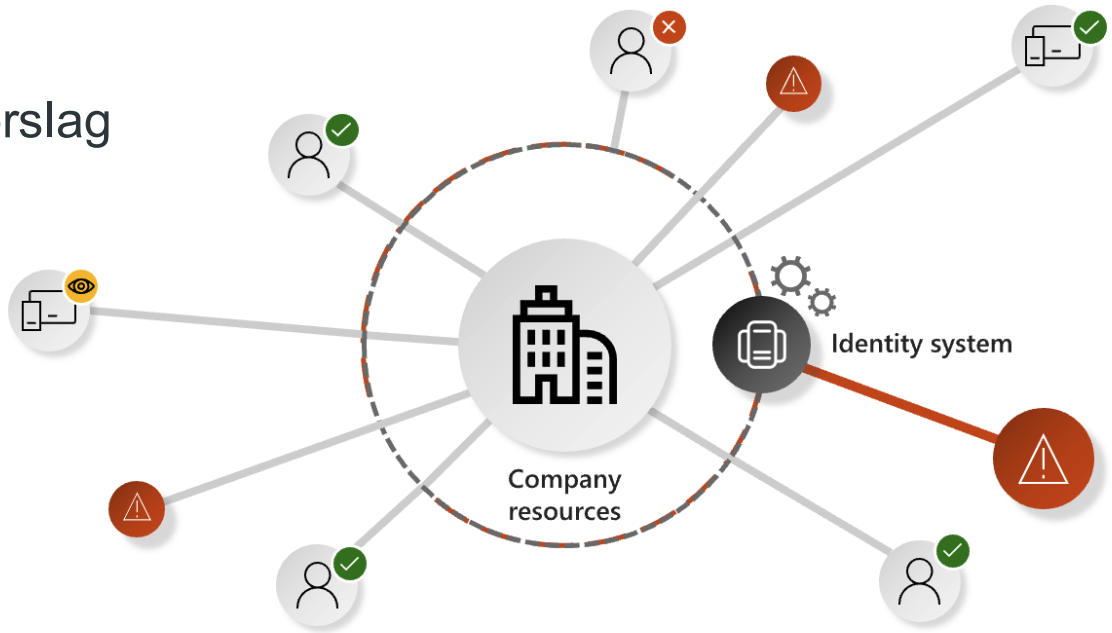
Vores budskab i dag:

Hvis ikke vi kan dokumentere **hvem der har privilegier hvornår**, **hvordan vi stopper et brud**, og **hvordan vi genopretter**—så er NIS2 bare pæne slides og dokumenter.

Vil vi måles på papir eller på reduceret risiko?

Begynd at arbejde med IT hygiejnen –
XDR, Security Posture og Exposure Management

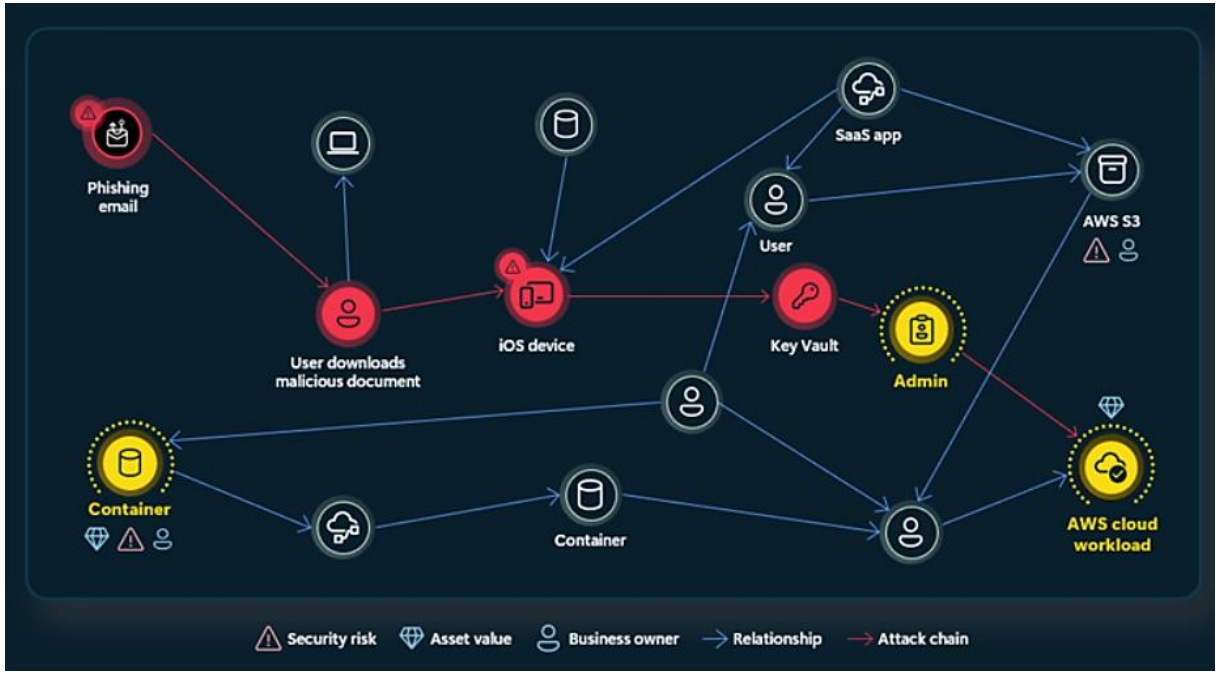
- Data samles og udstilles med operationelle forslag til forbedring
- Assessments i Secure Score Dashboard
- Attack paths, udsatte identiteter eller assets
- En proaktiv tilgang, hjælper med hygiejnen



Microsoft Security Exposure Management (MSEM)

(Indsigt & Overblik)

- Med Defender XDR & Unified SecOps forbinder vi trusler og infrastrukturen.
- MSEM registrerer aktiviteter og angrebsoverflader, og udstiller lateral bevægelse.
- Kritiske aktiver, dem vi kender og dem vi fremadrettet vil kende og klassificere.



https://techcommunity.microsoft.com/blog/securityexposuremanagement/proactive-security-with-continuous-threat-exposure-management-ctem/4452149

Hvem kan bruge Exposure Management?

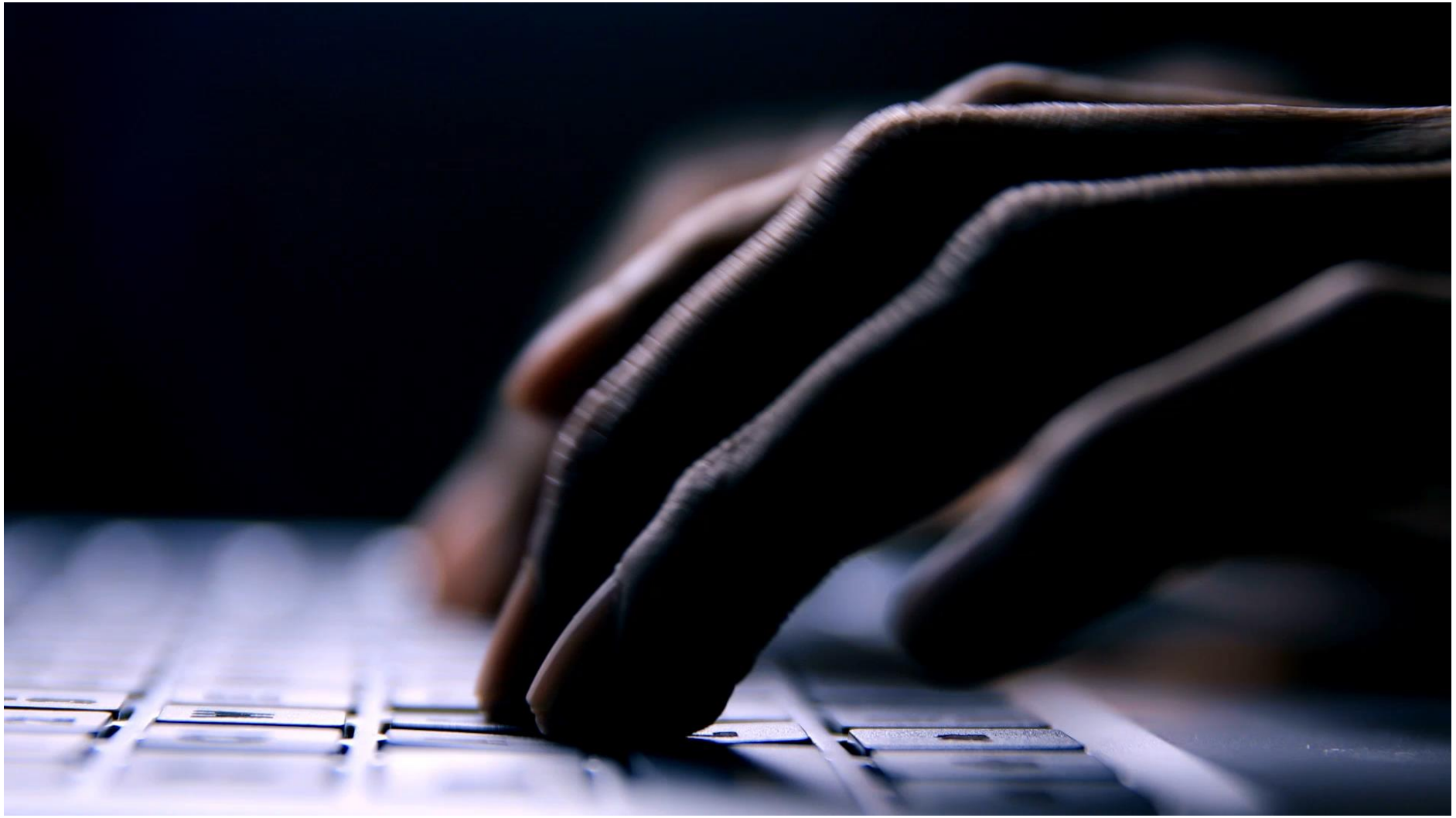
- **Sikkerheds administratorer der arbejder med sikkerhed** og overholdelse af angivne standarder. Ansvarlige for at vedligeholde og kontinuerligt forbedre en organisations security-posture.

- **SOC teams**, der har brug for synlighed i data og aktiviteter på tværs af en organisation, for at registrere, undersøge, mitigere og afhjælpe sikkerhedstrusler.

- **Sikkerhedsarkitekter**, som er ansvarlige for at løse systematiske problemer i den overordnede sikkerhedsholdning.

- **CISO og beslutningstagere**, der har brug for indsigt i overflader og eksponering af organisatoriske angreb for at forstå sikkerhedsrisikoen inden for en organisationens rammer.

Demo – Lad os kigge på det.

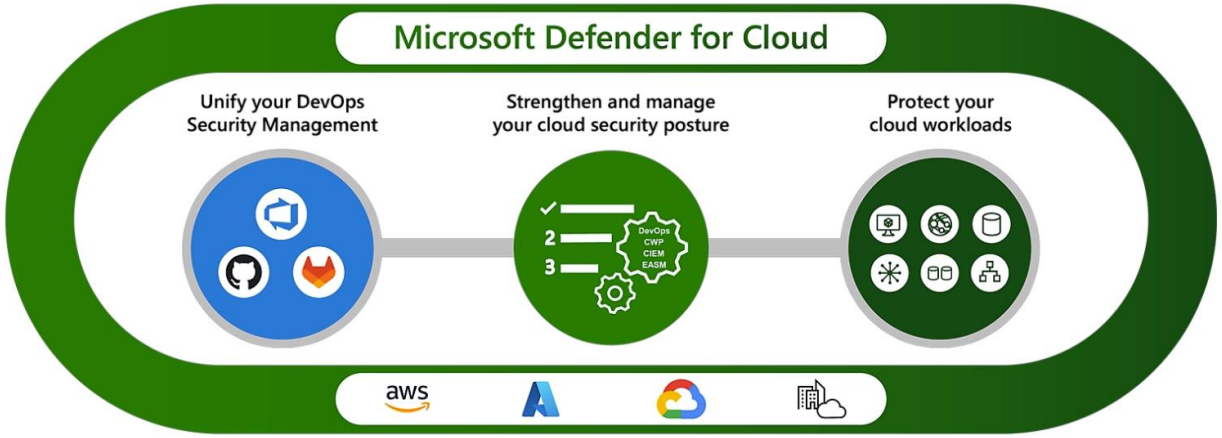


Defender for Cloud

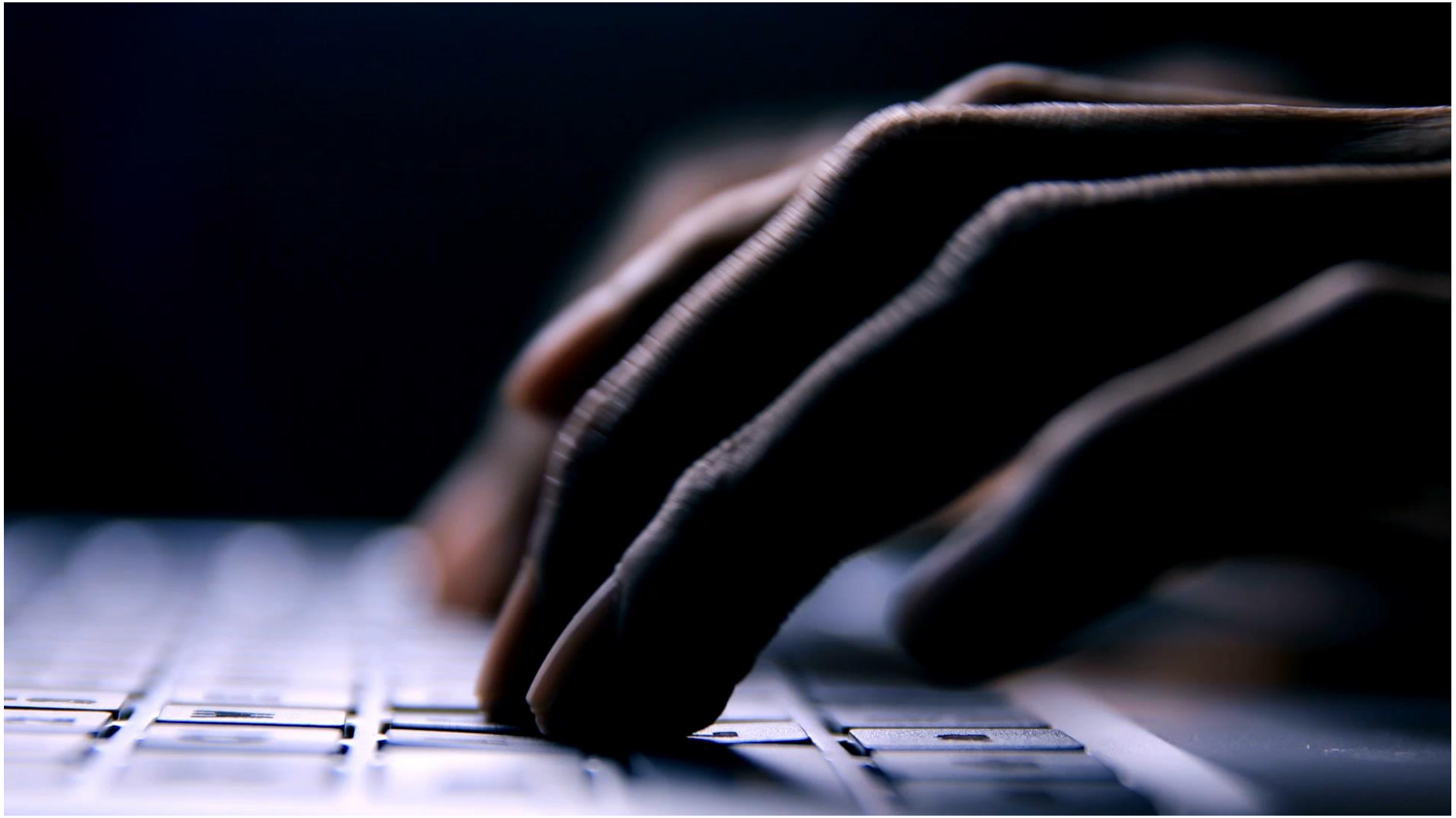
Sikkerhed på tværs af Cloud + Hybrid infrastrukturen:

- Development Security Operations (DevSecOps)
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP):
  - Virtual machines (VMs)
  - Containers
  - Storage
  - Databases

Vi skal kontrollere og sikre vores Cloud platforme, også selvom det er Multi-Cloud.



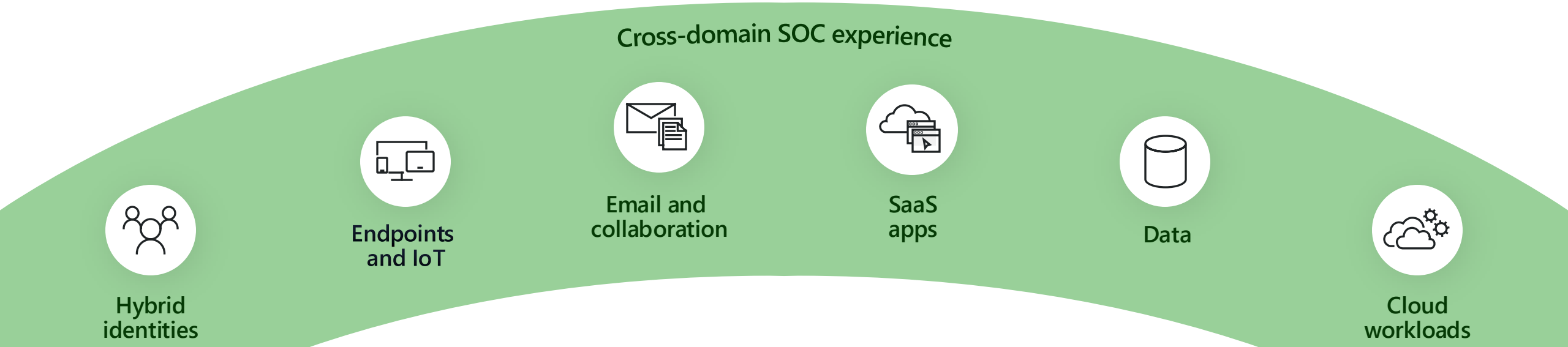
Demo – Lad os kigge på det.



ATEA TECH TOUR

Microsoft Unified Security

Build a unified defense with XDR, Defender for Cloud & Sentinel



Prevent

Reduce attack surface with threat-based configuration recommendations and built-in vulnerability management

Protect

Automatically contain and remediate compromised assets

Detect and respond

Use incidents to respond to cross-workload threats from a single portal

Speed up response with an experience designed for SOC efficiency

Extend

Unified APIs and connectors

ATEA TECH TOUR

Fra brute-force til brain-force hacking!

Edward Nygma's invention, ***"The Box."***

- ***What it is:*** *A 3-D/VR "TV enhancer" that beams entertainment straight into your brain.*

- ***What it actually does:*** *While projecting images, it* ***siphons users' brainwaves*** *their thoughts, knowledge, and neural energy* ***into Nygma****, making him progressively* ***smarter and able to read minds****.*

- ***Purpose****: By eavesdropping on minds, he amasses power, money, and secrets.*

ATEA TECH TOUR

*Security is part of **everyone's** job ~~the security team's job~~*

*Assets must be protected **wherever** they are ~~behind the security perimeter is safe~~*

ATEA TECH TOUR

Næste indlæg:

Indsigt i Windows endpoint-beskyttelse mod målrettede cyberangreb