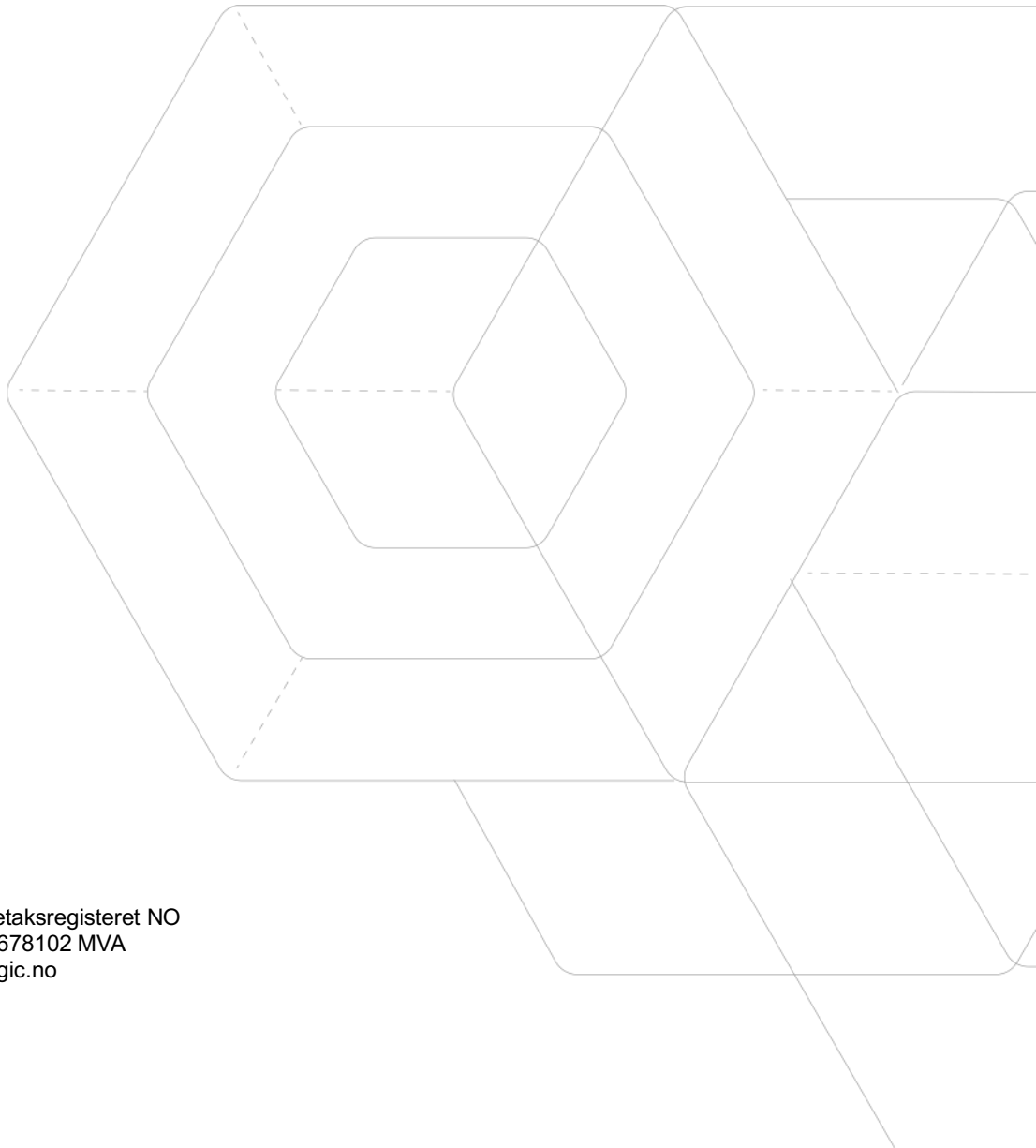
Powered by Knowledge.
Driven by Trust.

NIS2 Artikkel 21 – Teknisk referansearkitektur v. 2.0

Arkitekturen først, teknologivalget deretter.



nLogic AS

Foretaksregisteret NO
821678102 MVA
nLogic.no

Innhold

Sammendrag

Denne veiledningen oversetter NIS2-direktivets Artikkel 21 — ti minimumselementer for håndtering av cybersikkerhetsrisiko — til konkrete konfigurasjoner i Microsoft 365-plattformen, Microsoft Intune, og Microsoft Defender-suite. Den er bygget for norske virksomheter som driver Microsoft-baserte miljøer, og som forbereder seg på første tilsyn fra NSM under digitalsikkerhetsloven (forventet oktober 2026).

Arkitekturen først, teknologivalget deretter. Veiledningen åpner med en stakk-uavhengig referansearkitektur (Del 0) som beskriver hvilke seks komponenter en virksomhet trenger for å være i samsvar med NIS2 — uavhengig av leverandør. Deretter vises det hvordan disse komponentene leveres av Arctic Wolfs Security Operations Bundles som primær referansestakk, og hvordan Microsoft 365 / Intune / Defender kan dekke komponentene som alternativ eller komplement, med eksplisitt notat om svakhetene i Microsoft-leveransen der det er relevant. Hver virksomhet ender typisk med en hybrid — Microsoft som identitets- og endepunktstakk (komponent A og B), Arctic Wolf eller andre tilsvarende leverandører som SOC/MDR-tjeneste (komponent C, D, E, F).

Veiledningen forutsetter at organisasjonen har Microsoft 365 E5 eller tilsvarende lisensiering. Hvor E3-likeverdige tilnærminger finnes, er disse markert. Hvor Defender for Cloud, Sentinel eller Entra ID P2 kreves utover standard E5, er det også markert.

Den er ikke ment som en compliance-sjekkliste. Den er en teknisk implementeringsveiledning som forutsetter at organisasjonen allerede har gjort en formell scope-vurdering og en modenhetsanalyse mot Artikkel 21. Hvis ikke, se den operasjonelle NIS2-artikkelen som dette tekniske dokumentet følger opp.

Endringer i v2.0

- Ny **Del 1** — Overordnet teknisk arkitektur for NIS2-compliance (stakk-uavhengig referansemodell)
- Revidert **Del 2.3** — Deteksjonslag med Arctic Wolf SOC/MDR som primær, Defender XDR som datakilde og alternativ (med svakheter dokumentert)
- Revidert **Del 2.4** — Loggmottak med Arctic Wolf-plattformen som primær, Sentinel som alternativ (med svakheter dokumentert)
- Revidert **Del 3.2** — Hendelseshåndtering med Aurora MDR + JumpStart Retainer som primær leveranse

- Revidert **Del 3.3** — Driftskontinuitet med Cyber Resilience Assessment + Security Operations Warranty
- Revidert **Del 3.6** — Effektvurdering med Aurora Managed Risk + Cyber Resilience Assessment
- Revidert **Del 3.7** — Cyberhygiene med Aurora Managed Security Awareness and Training
- Lisensmatrise utvidet med **Microsoft Defender Suite** (bundle)

Endringer fra v1.0 til v1.1 (historisk)

- Ny **Del 2.6** — Hybrid sikkerhetsstack: Microsoft som baseline, men sjelden alene
- Ny **Del 3.7.5** — E-postflyt og e-postsikkerhetsarkitektur (Proofpoint to-topologi-modell, alternativer)
- Revidert **Del 2.3** og **3.9** — eksplisitt behandling av hybrid EDR (Microsoft Defender + CrowdStrike, Palo Alto Cortex XDR, SentinelOne)
- Revidert **Del 4.1** — logging og retensjon med MDR-leveransemodell som likeverdig arkitektur
- Ny **Del 4.5** — MDR/MR/IR som NIS2-utfyllende tjeneste

Hvordan bruke denne veiledningen

Veiledningen er strukturert i tre lag:

1. **Konseptuelt lag** (Del 2 og Del 4): Forklarer arkitekturvalgene som ligger til grunn for Tier-modellen, identitet som kontrollplan, deteksjons- og responsstruktur. Les denne delen først hvis du ikke har en moden Microsoft-sikkerhets-arkitektur fra før.
2. **Implementasjonslag** (Del 3): Per Artikkel 21-element gjennomgår vi krav, valg av Microsoft-produkter, konkrete konfigurasjoner med policy-stier og verifikasjonsskript. Hvert delkapittel kan leses uavhengig hvis du allerede har en moden arkitektur.
3. **Operasjonelt lag** (Del 5 og Del 6): Plan for utrulling, øvelser, og ferdige skript/maler.

Referansearkitektur — Microsoft-stakken mappet til Artikkel 21s ti elementer. Hvilket lag i stakken leverer hvilken Artikkel 21-funksjon, og hvor de overlapper.

Forutsetninger:

- Microsoft 365 E5 (eller E3 + tilleggslisenser for Defender for Endpoint, Defender for Identity, Defender for Office 365, og Entra ID P2)
- Microsoft Sentinel-instans i Azure (egen lisens, kost-basert)
- Defender for Cloud Plan 2 hvis serverarbeidsmengder skal inkluderes
- En etablert Tier 0-administrasjonsmodell, eller vilje til å etablere én

- En vakthavende-funksjon med myndighet til å kategorisere hendelser innen 24 timer

Lisensieringsmatrise:

Funksjon	E3	E5	Tilleggslisens
Defender for Endpoint Plan 1	✓	✓	—
Defender for Endpoint Plan 2	—	✓	Egen Plan 2-lisens
Defender for Identity	—	✓	Egen Defender for Identity-lisens (M365 E3-tillegg)
Defender for Office 365 Plan 1	—	—	Egen tilleggslisens
Defender for Office 365 Plan 2	—	✓	Egen Plan 2-lisens
Defender Vulnerability Management	Begrenset	Full	Standalone-lisens finnes
Microsoft Defender Suite (bundle)	—	—	Egen suite-lisens — inkluderer Defender for Endpoint P2 + Defender for Identity + Defender for Office 365 P2 + Defender for Cloud Apps + MDVM som en pakke (ofte rimeligere enn å kjøpe enkeltkomponenter). Anbefalt for virksomheter som ønsker full Microsoft Defender-dekning uten å gå hele veien til E5
Entra ID P1	✓	✓	Standalone
Entra ID P2 (PIM, Identity Protection)	—	✓	Standalone
Purview Compliance Manager — NIS2 premium template	3 gratis premium-maler	3 gratis premium-maler	~€500/mnd per template utover de tre
Microsoft Sentinel	—	—	Forbruks-basert (per GB ingestert)

1. Overordnet teknisk arkitektur for NIS2-compliance

1.1 Hvorfor arkitekturen kommer før teknologivalget

NIS2 Artikkel 21 er regelverks-styrt, ikke produkt-styrt. Direktivet beskriver ti minimumselementer som handler om *funksjoner som må være på plass* — risikohåndtering, hendelseshåndtering, driftskontinuitet, leverandørstyring, sikker utvikling, effektvurdering, opplæring, kryptografi, tilgangskontroll, og MFA/sikker kommunikasjon. Det sier ingenting om hvilke leverandører eller produkter som leverer disse funksjonene.

I praksis betyr det at hver virksomhet i scope må svare på det samme spørsmålet, *uavhengig av teknologivalg*: «Har vi en arkitektur som leverer alle de ti elementene, med navngitte eiere, dokumentert evidens, og kontinuerlig oppfølging?»

Veiledningen behandler dette i to lag:

- **En stakk-uavhengig referansearkitektur** (denne delen) som beskriver hvilke arkitektur-komponenter en virksomhet trenger for å være i samsvar med NIS2.
- **Konkrete implementeringsvalg per element** (Del 1–5) som viser hvordan disse komponentene kan realiseres — primært med Arctic Wolfs Security Operations-stakk som referansestakk, og med Microsoft 365 / Intune / Defender som alternativ eller komplement.

Valg av teknologistakk er en sekundær — men forretningskritisk — beslutning. Den må gjøres med åpne øyne om hva hver stakk faktisk leverer av NIS2-funksjoner ut av boksen, hva som krever betydelig egeninnsats å bygge ovenpå, og hva som ikke finnes uten supplerende tjenester.

1.2 De seks arkitektur-komponentene NIS2 krever

Når man brutalt forenkler de ti elementene til funksjonelle blokker, kan en virksomhet som er i samsvar med NIS2 beskrives som seks arkitektur-komponenter som må fungere sammen:

Komponent	Funksjon	NIS2-elementer dekket
A. Identitet og tilgang	Autentisering, autorisasjon, MFA, privilegert tilgang, joiner-mover-leaver	21(2)(i) Tilgangskontroll · 21(2)(j) MFA
B. Endepunkt og data	Endepunkt-EDR, kryptografi, asset management, sikker enhetskonfigurasjon	21(2)(h) Kryptografi · 21(2)(i) Asset mgmt
C. Deteksjon og respons (SOC)	24/7 overvåkning, hendelseshåndtering, 24/72-timers-varsling til NSM, forensikk	21(2)(b) Hendelseshåndtering
D. Loggmottak og retensjon	Sentralisert logging, retensjon ≥1 år, NSM-tilgang ved tilsyn, søkbarhet	21(2)(b) + (f) underbygging
E. Risikohåndtering og effektvurdering	Sårbarhetsplattform, attack surface management, kontinuerlig sikkerhetsrevisjon, pentest	21(2)(a) Risikoanalyse · 21(2)(f) Effektvurdering

F. Cyberhygiene og opplæring	Awareness-program, phishing-simuleringer, dokumentert deltakelse per bruker	21(2)(g) Opplæring

I tillegg ligger to tverrgående komponenter rundt disse:

- **Driftskontinuitet** (21(2)(c)) — backup, gjenoppretting, krisehåndtering — implementeres på tvers av komponentene
- **Leverandørkjede-sikkerhet** (21(2)(d)) — krav mot egne leverandører (inkludert de som leverer komponentene over)

Sikker utvikling (21(2)(e)) er en separat komponent for virksomheter som utvikler programvare.

1.3 Hvordan stakk-valget endrer arkitekturen

Det er to dominerende arkitektur-mønstre i norske mellomstore virksomheter:

Mønster A — Konsolidert Security Operations-leverandør med komplett dekning:

> En tjenesteleverandør som Arctic Wolf leverer komponentene C (SOC/MDR), D (loggmottak), E (Managed Risk), og F (Security Awareness Training) som integrert tjeneste. Virksomheten beholder ansvaret for A (identitet) og B (endepunkt) — men disse mates inn i leverandørens deteksjonsplattform. Konsekvens: én leverandør, én SLA, én dashboard, én rapporteringslinje.

Mønster B — Microsoft-baseline med flere supplerende verktøy og intern bemanning:

> Microsoft 365 + Intune + Defender XDR + Sentinel + Purview leverer A, B, og delvis C, D, E, F. *Men* — denne stakken forutsetter at virksomheten selv driver 24/7 SOC-funksjonen (eller kjøper Microsoft Defender Experts for XDR som tilleggstjeneste), tuner deteksjonsregler kontinuerlig, vedlikeholder Sentinel-workspacet, og kjører eget awareness-program via Attack Simulation Training. Konsekvens: høyere fleksibilitet, men betydelig egeninnsats — eller en supplerende MDR-leverandør som tette ut hullene.

Disse mønstrene er ikke gjensidig utelukkende. Mange virksomheter ender i en hybrid: Microsoft 365 + Defender for endepunkt og identitet (A og B), Arctic Wolf MDR som SOC + loggmottak (C og D), Arctic Wolf Managed Risk for sårbarhetsdekning (E), Arctic Wolf Managed Security Awareness for opplæring (F). Det er ikke en kompromiss-arkitektur — det er ofte den mest realistiske og optimale for å kunne være i samsvar med NIS2.

1.4 Sentralt prinsipp: «én arkitektur, mange implementeringer»

Resten av veiledningen behandler hver komponent for seg. For hver komponent vises:

1. **Hva NIS2 krever av komponenten** (regelverks-funksjon)
2. **Hvordan Arctic Wolfs Security Operations-stakk leverer komponenten** (primær referansestakk)
3. **Hvordan Microsoft 365 / Defender / Sentinel kan dekke komponenten** (alternativ — med eksplisitt notat om hva som mangler)
4. **Andre alternativer** der det er relevant (Tenable, CrowdStrike, Cortex XDR, Okta, etc.)
5. **Verifikasjon** (PowerShell, KQL, eller leverandørspesifikk evidens)

Hovedpoenget er ikke at Arctic Wolf eller Microsoft er det «rette» svaret.

> *Uten en bevisst arkitektur som dekker alle seks komponentene med dokumentert evidens og navngitt eier, er virksomheten ikke i samsvar med NIS2 — uavhengig av hvor mange Microsoft- eller AW-lisenser den har kjøpt.*

2. Grunnleggende arkitektur

2.1 Identitet som kontrollplan — Entra ID-sentrisk design

Den enkleste mentale modellen for moderne Microsoft-sikkerhet er at identitet erstatter nettverk som primær kontrollplan. Tradisjonelle perimetre — brannmurer, intern segmentering, VPN — er fortsatt relevante, men de er ikke lenger der den primære tilgangsbeslutningen tas. Den beslutningen tas i Entra ID hver gang en bruker, et endepunkt eller en applikasjon forsøker å autentisere.

I praktisk betydning: hvert NIS2-relevant tiltak du implementerer i Microsoft-økosystemet er en variant av enten *autentisering* (er du den du sier du er?), *autorisasjon* (har du rett til å gjøre dette?), eller *audit* (hva har du gjort?). Conditional Access, MFA, PIM, Defender for Identity, sensitivity labels — alle er manifestasjoner av disse tre.

Konkret betyr det:

- Conditional Access er der NIS2 Artikkel 21(2)(i) og (j) (tilgangskontroll og MFA) faktisk operasjonaliseres.
- Entra ID Privileged Identity Management (PIM) er der just-in-time-elevering faktisk implementeres.
- Microsoft Defender for Identity er der unormal Active Directory- og Entra ID-aktivitet faktisk oppdages.
- Microsoft Entra ID Identity Protection er der kompromitterte identiteter automatisk blokkeres eller utfordres.

Hvis Entra ID-rotmiljøet ditt er svakt — for eksempel: ingen MFA på Global Administrator, ingen Conditional Access på administrative roller, ingen PIM — kan ikke noen av de andre Microsoft-sikkerhetstiltakene levere mot Artikkel 21. Identitet er fundamentet. Alt annet er bygd på det.

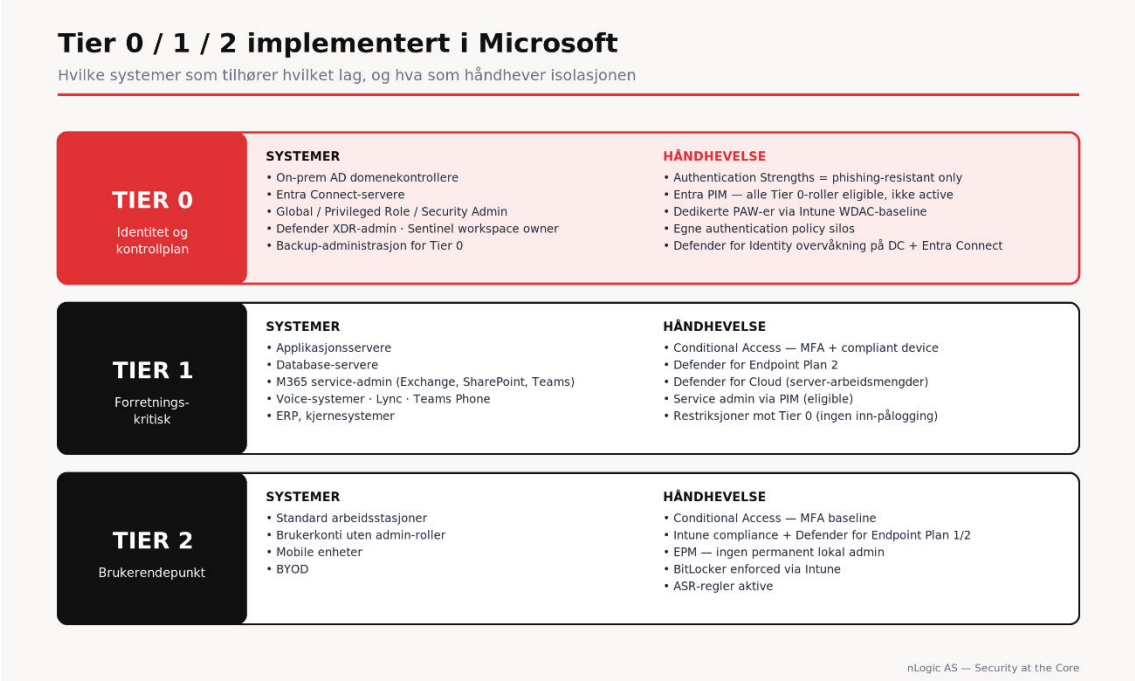
2.2 Tier 0/1/2-modellen implementert i Microsoft-stakken

Tier-modellen er et arkitekturvalg som NIS2 ikke eksplisitt krever, men som er den mest effektive måten å oppfylle Artikkel 21(2)(i) (personellsikkerhet og tilgangskontroll) i en Microsoft-basert virksomhet.

Tier 0 — Identitets- og kontrollplan-systemer: - On-premises Active Directory domenekontrollere (hvis hybrid) - Entra Connect-servere - Privilegerte Entra ID-roller (Global Admin, Privileged Role Admin, User Admin, Security Admin) - Defender XDR-administrator-roller - Microsoft Sentinel workspace owner-roller - Backup-administrasjon for Tier 0-systemer

Tier 1 — Forretningskritiske servere og tjenester: - Applikasjonsservere - Database-servere - Microsoft 365-administrator-roller (Exchange admin, Teams admin, SharePoint admin — *ikke* Global Admin) - Lync- og Teams Voice-systemer - ERP-systemer

Tier 2 — Brukerendepunkter: - Standard arbeidsstasjoner - Brukerkonti uten administrative roller - Mobile enheter – BYOD



Tier 0/1/2-modellen i Microsoft-stakken — hvilke systemer som tilhører hvilket tier, og hvilke Microsoft-teknologier som håndhever isolasjonen mellom tier-ene.

Håndhevelse via Authentication Policy Silos (Entra ID):

Bruk Authentication Policies og Authentication Strengths i Entra ID for å håndheve at Tier 0-kontoer bare kan autentisere fra Tier 0-arbeidstasjoner med phishing-resistant MFA:

```
# Eksempel: opprett en Authentication Strength som krever phishing-resistant
MFA
Connect-MgGraph -Scopes "Policy.ReadWrite.ConditionalAccess"

$tier0Strength = @{
    displayName = "Tier 0 – Phishing-resistant MFA only"
    description = "Krever FIDO2 eller Windows Hello for Business"
    policyType = "custom"
    requirementsSatisfied = "mfa"
    allowedCombinations = @("fido2", "windowsHelloForBusiness",
"x509CertificateMultiFactor")
}
New-MgPolicyAuthenticationStrengthPolicy -BodyParameter $tier0Strength
```

Privileged Access Workstations (PAW) via Intune:

Opprett en dedikert enhetskonfigurasjonsprofil i Intune for PAW-er som blokkerer alle ikke-administrative applikasjoner via AppLocker eller Windows Defender Application Control (WDAC):

- Intune → Devices → Configuration → Create policy → Windows 10/11 → Administrative templates
- Aktiver: Application Control Policies, WDAC i enforcement mode med en "Allow Microsoft signed only"-baseline
- Bind via dynamisk Entra-gruppe basert på enhetsattribute (f.eks. en custom property satt under enrollment)

PAW-ene må aldri brukes til e-post, web-surfing, eller noen aktivitet som ikke direkte er Tier 0-administrasjon. Bruker du PAW-en til å lese e-post, er den ikke lenger en PAW.

2.3 Deteksjonslag — Arctic Wolf SOC/MDR som primær, Defender XDR som datakilde

Komponent C (deteksjon og respons) i NIS2-arkitekturen er funksjonen som leverer 24/7 menneskelig overvåkning av sikkerhetsalarmer, triage, og initial respons. For norske mellomstore virksomheter er dette komponenten der gapet mellom regelverkskrav og operasjonell virkelighet er størst — fordi 24/7 SOC krever bemanning, kompetanse, og kontinuerlig tuning som de færreste virksomheter selv kan levere.

Primær referansearkitektur: Arctic Wolf Aurora MDR

Arctic Wolfs Aurora Managed Detection and Response leverer komponent C som tjeneste:

- **24/7 menneskelig overvåkning** av sikkerhetsalarmer på tvers av endepunkt, identitet, e-post, og sky — uten at virksomheten må bemanne SOC-en internt
- **Concierge Security Team (CST)** — én navngitt sikkerhetsingeniør som primær kontakt, ikke en anonym alarmkø. Dette matcher NIS2s krav om at hendelseskoordinering må skje med definerte mennesker

- **Multi-EDR-støtte** — Aurora-plattformen ingesterer fra Microsoft Defender for Endpoint, CrowdStrike Falcon, SentinelOne, Palo Alto Cortex XDR, Sophos Intercept X, Trend Micro Apex One, og flere. Virksomheten kan beholde eksisterende EDR-investeringer uten å låse seg til Microsoft
- **Multi-identitetsleverandør-støtte** — Microsoft Entra ID, Okta, Duo, Ping
- **Multi-e-postsikkerhet-støtte** — Proofpoint, Mimecast, Microsoft Defender for Office 365
- **Triage og initial respons** innen 15-30 minutter for kritiske alarmer (kontraktuell SLA), inkluderer aktive responshandlinger (block account, isolate endpoint, revoke session)
- **Active Response** — leverandøren kan utføre containment-handlinger direkte i kundens miljø, ikke bare gi anbefalinger

Aurora MDR er inkludert i alle Arctic Wolfs Security Operations Bundles (Core, Plus, Total). For NIS2-essensielle virksomheter er Total-bundle den mest naturlige fordi den i tillegg leverer JumpStart Retainer (IR-readiness) — som diskuteres i 2.2.

NIS2-kobling per Aurora MDR-leveranse

NIS2-element	Hvordan Aurora MDR leverer
21(2)(b) Hendelseshåndtering	Hele tjenesten — deteksjon, triage, respons, dokumentasjon
21(2)(f) Effektvurdering	Aurora-plattformen leverer kontinuerlig sikkerhetsovervåkning og månedlig rapportering
Artikkel 23 24/72-rapportering	CST har erfaring med varslingsfristene; eskaleres til virksomhetens CISO som tar beslutningen
Tabletop og IR-readiness	Inngår som del av Concierge Experience

Alternativ: Microsoft Defender XDR + Sentinel + Defender Experts for XDR

For virksomheter som velger Microsoft-stakken som komplett løsning, er kombinasjonen:

- **Defender XDR** (paraplyen) — samler Defender for Endpoint, Identity, Office 365, Cloud Apps, og Cloud
- **Microsoft Sentinel** — SIEM og SOAR-funksjon

- **Microsoft Defender Experts for XDR** — managed service der Microsoft selv leverer 24/7 SOC-funksjonen

Dette er en valid NIS2-arkitektur, men har konkrete svakheter som må adresseres:

Svakhet 1 — Defender XDR er en deteksjonsplattform, ikke en SOC. Plattformen samler alarmer; den triager dem ikke. Uten Defender Experts for XDR (egen lisens, betydelig kost) må virksomheten bemanne triagering internt. For mellomstore norske virksomheter er dette ikke realistisk.

Svakhet 2 — Multi-vendor EDR-støtte er begrenset. Defender XDR er bygget primært for Microsofts egne komponenter. Telemetri fra CrowdStrike, Cortex XDR, eller SentinelOne kan importeres via tredjepartskonnektorer i Sentinel, men korrelasjon på tvers av disse er manuelt arbeid — ikke ut-av-boksen-funksjonalitet.

Svakhet 3 — Sentinel-kostnaden er per-GB-ingestion. Logger fra hele Microsoft-økosystemet pluss tredjepartskilder kan raskt bli kostbart — flere hundre tusen kroner i året for en mellomstor virksomhet er ikke uvanlig. Dette er en uforutsigbar kost som vokser med trusselbildet.

Svakhet 4 — Defender Experts for XDR er fortsatt en tjeneste levert "fra-armlengdes-avstand". Det er ingen navngitt CST-modell. Hendelseskoordinering går via ticketing-system, ikke en navngitt sikkerhetsingeniør som kjenner virksomheten.

Svakhet 5 — Initial deployment-tid. En full Sentinel-utrulling med tuning av Analytics Rules tar typisk 3-6 måneder. Aurora MDR onboardes typisk på 1-2 uker.

Når Microsoft-only er likevel rett valg: Store virksomheter med eksisterende intern SOC, kompetanse på Sentinel/KQL, og budsjett for Defender Experts for XDR — eller virksomheter med en eksplisitt policy om "Microsoft-only" av suverenitetsgrunner.

Hybrid: Microsoft for A og B, Arctic Wolf for C og D

I praksis ser de fleste norske mellomstore virksomheter på en hybrid:

- Microsoft 365 + Entra ID + Defender for Endpoint som identitet- og endepunkt-stakk (komponent A og B)
- Arctic Wolf Aurora MDR som SOC og loggmottak (komponent C og D)
- Microsoft Defender for Office 365 *eller* Proofpoint for e-post — feedes inn i Aurora
- Microsoft Intune for enhets-konfigurasjon

Dette er ikke en kompromiss-arkitektur. Det er den modne arkitekturen, som er i samsvar med NIS2, for virksomheter som har Microsoft-investeringer men ikke

har 24/7 SOC-kapasitet selv. Arctic Wolfs CDR-plattform har dokumentert integrasjon mot Microsoft 365 audit, Entra ID, Defender XDR, og Defender for Cloud Apps via API-konnektorer.

2.4 Loggmottak og retensjon — Arctic Wolf-plattformen som primær

Komponent D (loggmottak og retensjon) i NIS2-arkitekturen krever sentral aggregering av sikkerhetsrelevante logger, retensjon ≥1 år, NSM-tilgang ved tilsyn, og evnen til å søke på tvers av logg-kilder innen 24 timer ved hendelse.

Primær referansearkitektur: Arctic Wolf-plattformen

Aurora MDR inkluderer som standard:

- **Log Retention** (en del av alle Security Operations Bundles) — historiske logger oppbevares for compliance og review, med mulighet for å oppgradere retensjonsperioden til virksomhetens krav (typisk 1-5 år, avtalefestes)
- **Data Explorer Lite** (alle bundles) — søkbart datasett for trusseljakt og hendelses-respons
- **Data Explorer (full)** — oppgradering for dyptgående KQL-lignende søk over hele datasettet
- **Aurora Threat Intelligence** — kuratert trusselsdata som beriker hendelser i sanntid

Sentralt for NIS2: **logg-retensjon, søkbarhet, og leverandørens tilgjengelighet for NSM-tilsyn er inkludert i tjenesten** — uten per-GB-ingestion-kost.

NIS2-kobling

Krav	Hvordan Arctic Wolf-plattformen leverer
Sentralisert logg-aggregering	Innebygd via Aurora-konnektorer for Microsoft 365, Entra ID, Defender XDR, tredjepartsleverandører
Retensjon ≥1 år	Standard i alle bundles; kan utvides ved behov, krever endring av kontrakt.
NSM-tilgang ved tilsyn	Klausulfestes i avtalen — leverandørplikt til å levere logguttrekk innen 72 timer på forespørsel
Søkbarhet under 24t SLA	Data Explorer Lite (standard) eller Data Explorer (oppgradert)
Loggintegritet	Plattformens lagring er immutabel etter ingest — bekreftet i Arctic Wolfs tekniske dokumentasjon

Alternativ: Microsoft Sentinel

Microsoft Sentinel er den native SIEM-løsningen og kan levere komponent D. Den har egne styrker (dyptgående KQL, omfattende konnektor-katalog, sterke workbooks) men også svakheter for mellomstore virksomheter:

Svakhet 1 — Forbruksbasert kostnadsmodell. Sentinel koster per GB ingestert. Logger fra Defender XDR, Entra ID, Microsoft 365 audit, samt syslog fra brannmurer og tredjepartsverktøy, kan raskt summeres til 100+ GB/dag i en mellomstor virksomhet. Det blir 50 000–200 000 NOK/måned i bare logg-kost — en kost som vokser med trusselbildet og som er vanskelig å forutsi presist.

Svakhet 2 — Retensjon krever aktiv konfigurasjon og kostnadsplanlegging. Standard hot-tier-retensjon er 30-90 dager; å holde logger i 1+ år krever Basic-tier eller Archive-tier, hver med egne søkebegrensninger og kostnader. Mange virksomheter oppdager dette først når kostnadene har eksplodert.

Svakhet 3 — Workspace-administrasjon krever kompetanse. Sentinel er et Azure-produkt med RBAC, identity-bindinger, og analytics rules som krever løpende vedlikehold. Det er ikke en tjeneste som «bare virker» — det er en plattform som må driftes.

Svakhet 4 — NSM-tilsyn må forberedes selv. Det er virksomhetens ansvar å konfigurere logguttrekk for NSM. Det er ikke en standardprosedyre i Sentinel.

Hybrid arkitektur: Sentinel for compliance-arkivet, Arctic Wolf for operasjon

For virksomheter med eksisterende Sentinel-investering kan en hybrid være:

- **Arctic Wolf-plattformen** som primær drift- og søke-plattform for SOC (24/7-overvåkning, hendelseshåndtering)
- **Sentinel** som langtidsarkiv (Basic eller Archive tier) for compliance-bevaring av logger som ikke trenger aktiv hunting

Dette gir det beste fra begge: AW-CSTs operasjonelle ekspertise på dagsaktive data, og Sentinel-arkivet for revisjons- og tilsynsformål når NSM ber om 18-måneders historikk.

Felles krav uavhengig av løsning

- **Loggintegritet** — logger må ikke kunne modifiseres etter ingest
- **Dokumentert retensjonspolicy** — skriftlig, godkjent av ledelsen, gjennomgått årlig
- **Tilgangskontroll** — hvem kan lese loggene? Hvem kan slette dem? Logg-tilgang skal selv være logget
- **Søkbarhet** — innen 24 timer skal SOC kunne svare på "hvilke påloggинger har bruker X hatt siste 90 dager?" og lignende
- **Exit-plan** — ved leverandørbytte må logger kunne eksporteres tilbake til virksomheten (gjelder begge mønstre)

2.5 Microsoft 365 mappet til Artikkel 21

Artikkel 21-element	Primær Microsoft-teknologi	Sekundær	Lisens
21(2)(a) Risikoanalyse-policy	Purview Compliance Manager + NIS2-template	Secure Score	Premium-template
21(2)(b) Hendelseshåndtering	Defender XDR + Sentinel	Service Trust Portal	E5 + Sentinel
21(2)(c) Driftskontinuitet	M365 Backup + Azure Backup	Retention Policies (Purview)	M365 Backup egen lisens
21(2)(d) Leverandørkjede	Conditional Access + Entra B2B + sensitivity labels	Defender for Cloud Apps	E5 + Defender for Cloud Apps
21(2)(e) Sikker utvikling	GitHub Advanced Security + Defender for DevOps	Azure DevOps	Egen lisens

21(2)(f) Effektvurdering	Defender Vulnerability Management + Microsoft Defender External Attack Surface Management (MDEASM)	Secure Score-trend	E5 / MDE ASM standalone
21(2)(g) Cyberhygiene	Attack Simulation Training (Defender for Office 365 Plan 2)	Viva Learning	E5
21(2)(h) Kryptografi	Purview Information Protection + BitLocker via Intune + Azure Key Vault	M365 Customer Key	E5
21(2)(i) Tilgang og asset	Conditional Access + Entra PIM + Intune compliance + Defender for Endpoint asset inventory	EPM (Endpoint Privilege Management)	E5 + Intune Suite
21(2)(j) MFA og kommunikasjon	Phishing-resistant MFA (FIDO2 / WHfB) + Conditional Access + Teams secure comms	Authenticator number matching	E5

Resten av denne veiledningen tar hvert av disse elementene i tur og dekker konfigurasjonen i detalj.

2.6 Hybrid sikkerhetsstack — Microsoft som baseline, men sjelden alene

Tabellen i 1.5 viser Microsoft-stakken som om den er hele bildet. I praksis er den det sjelden. De fleste norske virksomheter i NIS2-scope har en sammensatt sikkerhetsarkitektur der Microsoft 365 utgjør grunnmuren, men der spesifikke kontroller leveres av andre leverandører — av historiske grunner, lisensiering, fagkompetanse internt, eller bevisste arkitekturvalg.

Denne veiledningen er bygget for Microsoft-stakken fordi det er den vanligste startposisjonen, ikke fordi den er den eneste eller den beste. Hver av Artikkel 21-elementene dekkes operativt like godt — og i noen tilfeller bedre — av andre løsninger. Veiledningens praktiske verdi er at den beskriver hva som faktisk må være på plass for å oppfylle hvert element. Hvilket produkt som leverer det, er en arkitekturbeslutning.

Typiske alternativer per lag (ikke uttømmende):

Lag	Microsoft-baseline	Vanlige alternativer eller komplementer
Identitet og MFA	Entra ID + Conditional Access	Okta + Okta Adaptive MFA · Ping Identity · Duo Security
E-postsikkerhet	Defender for Office 365 Plan 2	Proofpoint Email Protection · Mimecast Email Security · Trend Micro Cloud App Security · Cisco Secure Email · Abnormal Security
Endepunkt-EDR/AV	Defender for Endpoint	CrowdStrike Falcon · Palo Alto Cortex XDR · SentinelOne Singularity · Sophos Intercept X · Trend Micro Apex One
Identitetsdeteksjon	Defender for Identity	Vectra AI · ExtraHop Reveal(x) · CrowdStrike Falcon Identity Protection
Sårbarhetsplattform	Defender Vulnerability Management	Tenable.io / Tenable.sc · Qualys VMDR · Rapid7 InsightVM
SIEM / SOAR	Microsoft Sentinel	Splunk Enterprise Security · IBM QRadar · Sumo Logic · Elastic Security
MDR (managed)	Defender Experts for XDR (Microsoft)	Arctic Wolf · andre tilsvarende leverandører (norsk) · Sophos MDR · CrowdStrike Falcon Complete
Privileged Access Management	Entra PIM	Delinea Secret Server · CyberArk PAM · BeyondTrust Password Safe
Sikker e-postarkivering	Purview Retention	Veritas Enterprise Vault · Mimecast Archive · Proofpoint Archive

Tabellen er ikke en anbefaling. Den er en realitetsbeskrivelse av at en sikkerhetsarkitektur som er i samsvar med NIS2. Den kan bygges på flere måter, men hovedspørsmålet er ikke «hvilken leverandør», men «hvilke funksjoner er på plass, hvem eier dem, og hvordan dokumenteres det at de virker».

Hva som faktisk endrer seg ved hybrid-stakk:

1. **Integrasjonsarbeid.** Microsoft-native gir minst integrasjonsfriksjon. Hver tredjeparts-løsning som introduseres må forsynes med logger fra Microsoft-laget (eller omvendt). Konnektorer, API-tilganger, og service-prinsipaler må styres.

2. **Logg-eierskap.** Hvis hovedlogg-aggregeringen er hos en MDR-leverandør (f.eks. Arctic Wolf-workspace) heller enn i Microsoft Sentinel, må retensjonsansvar, audit-tilgang for NSM, og e-discovery-ansvar tydeliggjøres i avtalen.

3. **Hendelseseierskap.** Hvis EDR er CrowdStrike og e-post er Proofpoint, vil to ulike alarm-køer eksistere. Disse må konsolideres et sted — enten i Sentinel som SIEM, i Microsoft Defender XDR via tredjepartskonnektor, eller hos MDR-leverandøren.

4. **Lisensoptimalisering.** E5 har redundans med flere tredjepartsprodukter. Hvis CrowdStrike er primær EDR, vurder om Defender for Endpoint Plan 2 fortsatt er nødvendig (i mange tilfeller ja, men ikke alltid). E3 + tilleggslisenser kan være rimeligere.

For resten av denne veiledningen markerer vi tydelig hvor Microsoft-implementeringen er én av flere veier. Del 3.5 spesielt behandler MDR/MR/IR-modellen som likeverdig arkitekturvalg når intern 24/7 SOC ikke er realistisk.

3. Implementering per Artikkel 21-element

3.1 Artikkel 21(2)(a) — Risikoanalyse-policy og informasjonssystem-sikkerhet

Hva regelverket krever: Skriftlige policyer for risikoanalyse og informasjonssystem-sikkerhet. Ledelses-godkjent, gjennomgått minimum årlig.

Microsoft-teknologier:

- **Microsoft Purview Compliance Manager** med NIS2-assessment-template
- **Microsoft Secure Score** som løpende styringssensor
- **Service Trust Portal** for å hente Microsofts egne sertifiseringsrapporter (ISO 27001, SOC 2 Type II, Cyber Essentials) som inngår i din risikoanalyse av Microsoft som leverandør

Steg-for-steg implementering:

Steg 1 — Aktiver NIS2-assessment-template:

1. Gå til Microsoft Purview-portalen → Compliance Manager → Assessment templates
2. Søk etter “NIS2”

3. NIS2-templaten er en premium-template. E5-kunder har tre gratis premium-template-aktiveringer; ellers koster den ~€500/mnd
4. Klikk “Create assessment” og velg M365-tenant og Azure-abonnementer som scope

Templaten inneholder ~200 kontroller mappet til Artikkel 21. Den scorer automatisk basert på din eksisterende M365-konfigurasjon, og foreslår tiltak for hver score under 100 %.

Steg 2 — Etabler baseline Secure Score:

1. Gå til Microsoft Defender-portalen → Secure Score
2. Eksporter nåværende score som baseline (bruk den innebygde export)
3. Sett et målnivå for 12 måneder fram — en typisk forbedring fra 50 % til 75 % er realistisk
4. Konfigurer ukentlig e-postrapport til sikkerhetsteamet
5. Bind én eier per “kategori” (Identity, Devices, Apps) for å eskalere stagnerte forbedringer

Steg 3 — Dokumenter sikkerhetspolicyen:

Bruk Compliance Manager-templaten som rammeverk for din skriftlige policy. Hver kontroll i templaten har et “implementation”-felt der du dokumenterer: - Hvilket M365-teknologivalg som dekker kontrollen - Hvem som er eier - Hvilken evidens som dokumenterer at kontrollen er på plass

Verifikasjon (PowerShell):

```
# Hent Secure Score over tid - tilstandssjekk
Connect-MgGraph -Scopes "SecurityEvents.Read.All"

Get-MgSecuritySecureScore -Top 30 |
    Select-Object CurrentScore, MaxScore, CreatedDateTime,
        @{N="ScorePercent";E={"{0:P1}" -f ($_.CurrentScore /
$_.MaxScore)}} |
    Sort-Object CreatedDateTime -Descending |
    Format-Table -AutoSize
```

CIS-mapping: 14.1, 14.4, 14.9 (Security Awareness and Skills Training Program), 17.1-17.9 (Incident Response Management)

3.2 Artikkel 21(2)(b) — Hendelseshåndtering (24t / 72t / 1mnd)

Hva regelverket krever: En dokumentert prosess for å oppdage, klassifisere, respondere på, og rapportere sikkerhetshendelser. Inkluderer 24-timers tidlig varsling, 72-timers hendelsesmelding, og 1-måneds sluttrapport til CSIRT (NSM).

Primær leveransemodell: Arctic Wolf Aurora MDR + JumpStart Retainer

Hendelseshåndtering er der få norske mellomstore virksomheter selv klarer å levere 24/7 — det er denne komponenten en konsolidert Security Operations-leverandør best dekker. Aurora MDR (inkludert i alle Security Operations Bundles fra Core og oppover) leverer hele kjeden:

- **24/7 menneskelig overvåkning** med Concierge Security Team som navngitt primær kontakt
- **Triage og initial vurdering** innen 15-30 minutter for kritiske alarmer
- **Active Response** — CST kan utføre containment-handlinger direkte (isolate endpoint, disable account, force MFA re-registration)
- **Eskalering** til virksomhetens vakthavende — CISO eller incident commander — med full kontekst og foreslått neste-steg
- **Dokumentasjon** av hendelsen i et format som direkte støtter Artikkel 23-rapportering

For NIS2-essensielle virksomheter er **JumpStart Retainer** (inkludert i Total-bundlen, oppgraderbar fra Core/Plus) den kritiske komponenten:

- Forhandshandlet IR-team aktivert med prioritert respons-SLA
- Battle-tested IR-plan utviklet og testet før hendelsen oppstår
- Sluttrapport som direkte kan inngå i Artikkel 23 1-måneds-rapport til NSM
- Tabletop-øvelser inkludert som del av forberedelsene

I tillegg gir Arctic Wolf Security Operations Warranty (finansiell risikooverføring opptil 3 mill. USD i Total-bundlen) en kompenserende økonomisk kontroll som ingen Microsoft-tjeneste tilbyr.

Hva dette betyr operativt for NIS2

NIS2-krav	Hva Arctic Wolf leverer
24-timers tidlig varsling	CST forbereder NSM-utkast basert på pågående hendelse; virksomhetens CISO godkjenner og sender
72-timers hendelsesmelding	CST + (om aktivert) JumpStart Retainer-IR-team leverer initial alvorlighetsgrad og IoC-er
1-måneds sluttrapport	Sluttrapport fra IR-engasjementet er strukturert for å oppfylle NSM-formatet
Aktiv respons	Inkludert i tjenesten — containment-handlinger utføres av CST/IR-team
Etterforskning	Aurora IR-tjeneste (oppgraderbar) eller standalone IR-retainer hos annen leverandør

Alternativ leveranse: Microsoft Defender XDR + Sentinel (intern SOC)

For virksomheter som velger å bygge intern SOC og bemanne den 24/7:

Microsoft-teknologier:

- **Defender XDR** — deteksjon og hendelseskonsolidering
- **Microsoft Sentinel** — SIEM, SOAR-playbooks, langtidsoppbevaring av logger
- **Microsoft Defender Experts for XDR** (valgfri tilleggslisens) — managed service hvis man ikke har intern 24/7-bemanning

Svakheter ved Microsoft-leveransen som virksomheter må adressere:

- Defender Experts for XDR er en *tilleggslisens* — den er ikke inkludert i E5
- Plattformen leverer alarmer, ikke ferdig vurderte hendelser; triagering må utføres av virksomheten selv (eller Defender Experts)
- Ingen Concierge-modell — alarmer kommer via portal og e-post, ikke navngitt sikkerhetsingeniør
- Ingen finansiell risikooverføring tilsvarende Security Operations Warranty
- IR-retainer må kjøpes som separat tjeneste (Microsoft Incident Response eller ekstern partner)

- Sentinel-kostnaden er per-GB-ingest, ikke flatpris

Steg-for-steg for de som likevel velger Microsoft-leveransen:

Steg 1 — Aktiver Defender XDR-hendelseskonsolidering:

1. Microsoft Defender-portalen → Settings → Microsoft Defender XDR → Account
2. Aktiver “Unified RBAC” for hele plattformen
3. Konfigurer “Incidents Auto-investigation” med Full automation for endpoints (krever Defender for Endpoint Plan 2)

Steg 2 — Sentinel data connectors og NIS2-spesifikk hendelses-tagging:

```
// Bekreft at de kritiske Sentinel-tilkoblingene er aktive
SentinelHealth
| where TimeGenerated > ago(7d)
| where SentinelResourceType == "Data connector"
| summarize LastUpdate = max(TimeGenerated),
            Status = arg_max(Status, TimeGenerated)
        by SentinelResourceName
| where Status != "Success" or LastUpdate < ago(24h)
| project SentinelResourceName, LastUpdate, Status
// Tagging av NIS2-rapporteringspliktige hendelser
SecurityIncident
| where Severity in ("High", "Medium")
| where Status == "New" or Status == "Active"
| where Title has_any (
    "ransomware", "data exfiltration", "credential theft",
"unauthorized access",
    "domain controller", "krbtgt", "DCSync", "golden ticket"
)
| extend NIS2_RelevanceCheck = "Verify within 24h — possible
significant incident"
| extend NSM_DeadlineEarly = format_datetime(now() + 24h, "yyyy-MM-dd
HH:mm")
| extend NSM_DeadlineNotification = format_datetime(now() + 72h,
"yyyy-MM-dd HH:mm")
```

Steg 3 — Dokumenter hendelsesrespons i virksomheten:

Tier 1 — Detection (24/7 dekning, intern SOC eller MSSP) Tier 2 — Triage (vakthavende sikkerhetsansvarlig, kan kategorisere alvorlighetsgrad) Tier 3 — Incident Commander (CISO eller designert vara, kan beslutte NSM-varsling) Tier 4 — Crisis Management (ledergruppe, juridisk, kommunikasjon, styre)

Hver tier må ha primær og minst én sekundær. Vakthavende-rolle må være kontaktbar 24/7.

Verifikasjon — MTTR-måling (KQL):

```
SecurityIncident
| where TimeGenerated > ago(90d)
| where Severity in ("High", "Medium")
| extend ResolutionTime_Hours = datetime_diff('hour', ClosedTime,
FirstActivityTime)
| where isnotempty(ClosedTime)
| summarize
    AvgResolutionHours = avg(ResolutionTime_Hours),
    MedianResolutionHours = percentile(ResolutionTime_Hours, 50),
    P90ResolutionHours = percentile(ResolutionTime_Hours, 90),
    HighSeverityCount = countif(Severity == "High")
    by bin(TimeGenerated, 7d)
| order by TimeGenerated desc
```

CIS-mapping: 17.1 (Incident Response Process), 17.4 (Establish and Maintain an Incident Response Process), 17.6 (Define Mechanisms for Communicating During Incident Response)

3.3 Artikkel 21(2)(c) — Driftskontinuitet og krisehåndtering

Hva regelverket krever: Backup, gjenoppretting, kontinuitetsplaner, kriseledelse. Testet minimum årlig, dokumentert.

Primær leveransemodell: Arctic Wolf Cyber Resilience Assessment + JumpStart Retainer

Driftskontinuitet er ikke en Arctic Wolf-tjeneste i seg selv (backup-løsningene leveres typisk separat), men *forberedelsen* til en kontinuitetshendelse er det Arctic Wolf-stakken adresserer:

- **Cyber Resilience Assessment** (inkludert i alle Security Operations Bundles) — vurderer virksomhetens sikkerhets-tilstand mot industri-rammeverk og identifiserer gap i kontinuitets-plan, IR-readiness, og recovery-modenhet. Det er den årlige dokumentasjonen som NIS2-tilsyn vil etterspørre
- **JumpStart Retainer** (Total-bundle) — battle-tested IR-plan, prioritert respons-SLA, tabletop-øvelser. Sluttrapporten fra en IR-aktivering er direkte input til 1-måneds NSM-rapport
- **Security Operations Warranty** — finansiell dekning for hendelses-relaterte kostnader, som kan fylle cyber-forsikringens deductible (opptil 3 mill. USD i Total-bundle med Aurora Managed Endpoint Defense-tillegg)

Hva virksomheten må levere selv (komplement til Arctic Wolf)

Funksjon	Anbefalt teknologivalg
Backup av Microsoft 365 (Exchange, SharePoint, OneDrive)	Microsoft 365 Backup ($0.15/GB/mnd) eller tredjeparts (Veeam, Veritas, AvePoint)
Backup av Azure-arbeidsmengder	Azure Backup eller tredjeparts
Backup av on-prem servere	Veeam, Commvault, Rubrik, eller liknende
AD-restore	Egne backup-prosedyrer, IFM (Install From Media)
Disaster recovery (DR)	Azure Site Recovery eller tilsvarende
Tabletop-øvelser	Inngår i Arctic Wolf Concierge Experience + JumpStart Retainer

NIS2-relevante kontroller — uavhengig av valg

1. **Test, ikke bare etabler.** Backup som ikke er testet er ikke backup. Sett opp et kvartalsvis vindu der vakthavende:
    - Restorer en utvalgt mailbox til en test-tenant
    - Restorer en SharePoint-site til en test-collection
    - Restorer en Tier 0-server til en isolert subnet
    - Verifiserer dataintegritet og dokumenterer tid til gjenoppretting

    Dokumentasjonen fra denne testen er det NSM ber om — ikke selve backup-policyen.
2. **Krisehåndteringsplan med definerte scenarioer:**
    - Ransomware som krypterer SharePoint og OneDrive
    - Domenekontroller-kompromittering med behov for AD-restore
    - M365-tenant-kompromittering (Global Admin har mistet kontroll)
    - Geografisk utfall av Azure-region (krever Multi-Region- eller hybrid-arkitektur)
3. **Tabletop-øvelse** der ledergruppen og IT-sikkerhet kjører igjennom hvert scenario minimum årlig.

Alternativ ren Microsoft-leveranse:

- **Microsoft 365 Backup** ($0.15/GB/mnd) for M365-data
- **Azure Backup** for serverarbeidsmengder
- **Azure Site Recovery** for failover-scenarier
- **Purview Retention Policies** for langtidsoppbevaring
- **Microsoft 365 Multi-Geo** for geografisk redundans (krever Multi-Geo-lisens)

Disse er gode tekniske komponenter, men de leverer ikke selve *prosessen* — tabletop-øvelsene, kriseplanen, og hendelsesresponsen som NSM ber om dokumentasjon på. Det må enten bygges internt eller leveres via et engasjement som Arctic Wolfs Cyber Resilience Assessment + JumpStart Retainer.

Verifikasjon — backup-jobs (KQL):

```
AddonAzureBackupJobs
| where TimeGenerated > ago(7d)
| where JobOperation == "Backup"
| summarize
    SuccessCount = countif(JobStatus == "Completed"),
    FailureCount = countif(JobStatus == "Failed"),
    LastSuccess = maxif(TimeGenerated, JobStatus == "Completed")
    by BackupItemFriendlyName
| where FailureCount > 0 or LastSuccess < ago(48h)
| project BackupItemFriendlyName, SuccessCount, FailureCount,
LastSuccess
| order by FailureCount desc
```

CIS-mapping: 11.1-11.5 (Data Recovery)

3.4 Artikkel 21(2)(d) — Leverandørkjede-sikkerhet

Hva regelverket krever: Vurdere, overvåke, og styre cybersikkerhetsrisiko fra leverandører — inkludert direkte leverandører og hele verdikjeden. Vurdering må inkludere leverandørens egne sikkerhetspraksiser, deres sikre utvikling, og deres egne underleverandører.

Microsoft-teknologier:

- **Microsoft Service Trust Portal** for Microsoft som leverandør
- **Conditional Access for external users** (Entra B2B)
- **Defender for Cloud Apps** for SaaS-leverandører
- **Microsoft Purview Information Protection** (sensitivity labels) for kontroll på data delt eksternt
- **Microsoft Entra Identity Governance for ekstern bruker-livssyklus**

Steg-for-steg:

Steg 1 — Etabler leverandørklassifisering:

Bygg en intern leverandørmatrise med fire klasser:

Klasse	Definisjon	Sikkerhetskrav
A — Kritisk	Driftsstans hos leverandøren stopper egen produksjon innen 24t	ISO 27001 + årlig sikkerhetsrevisjon + NIS2-samsvarserklæringer
B — Viktig	Driftsstans påvirker innen 7 dager	ISO 27001 eller likeverdig + SOC 2 Type II
C — Standard	Vesentlig, men erstattbar	Sikkerhetsklausuler i kontrakt
D — Marginal	Ikke kritisk	Standardvilkår

Steg 2 — Conditional Access for B2B-gjester:

Når en leverandør har behov for tilgang til ditt M365-miljø, må de inviteres som Entra B2B-gjest med strengere Conditional Access enn interne brukere:

```
# Eksempel: Conditional Access policy som tvinger MFA + Compliant
Device for B2B-gjester
# (Opprettes via Entra-portalen, dette er en JSON-skisse av policyen)

$policy = @{
    displayName = "CA: B2B Guests – MFA + Compliant Device"
    state = "enabled"
    conditions = @{
        users = @{ includeUsers = @("GuestsOrExternalUsers") }
        applications = @{ includeApplications = @("All") }
        clientAppTypes = @("all")
    }
    grantControls = @{
        operator = "AND"
        builtInControls = @("mfa", "compliantDevice")
    }
    sessionControls = @{
        signInFrequency = @{
            isEnabled = $true
            value = 1
            type = "hours"
        }
    }
}
```

Steg 3 — Data deling via sensitivity labels:

For data som deles med leverandører:

1. Microsoft Purview-portalen → Information Protection → Labels
2. Opprett en label kalt “Leverandør-konfidensiell” med:
   - Encryption: kun tilgjengelig for autoriserte B2B-gjester
   - Watermark: “Konfidensiell — leverandør”
   - Content marking: footer med leverandørnavn
   - Auto-applikasjon: når dokumenter deles til eksterne domener i en definert liste
3. Publiser label-policyen til relevante brukere

Steg 4 — Defender for Cloud Apps for SaaS-leverandører:

For hver SaaS-leverandør i M365-miljøet:

1. Microsoft Defender-portalen → Cloud Apps → Catalog
2. Sjekk Cloud App Catalog-vurderingen (Microsoft har en risikoscore på over 30 000 SaaS-apper)
3. For apps med score under 5 (lav modenhet), markere som “Unsanctioned” eller eskaler til evaluering
4. Konfigurer Conditional Access App Control for kritiske SaaS-apper for inline-overvåking

Steg 5 — Sikkerhetsklausuler i kontrakt:

For klasse A og B leverandører, krev følgende kontraktsmessige tilsagn:

- Skriftlig informasjonssikkerhetspolicy
- ISO 27001-sertifisering eller likeverdig
- Subprosessor-liste (deres egne leverandører) holdt oppdatert
- Hendelsesvarsling til deg innen 24 timer av oppdagelse
- Rett til revisjon (du eller en uavhengig revisor på din vegne)
- Avlevering eller sletting av data ved kontraktsslutt — dokumentert
- Kompenserende kontroller hvis sertifisering mangler

Verifikasjon:

```
// Hvilke eksterne brukere har vært aktive de siste 30 dager
AADSignInEventsBeta
| where TimeGenerated > ago(30d)
| where UserType == "Guest"
| summarize
    DistinctUsers = dcount(UserPrincipalName),
    SignInCount = count(),
    LastSignIn = max(TimeGenerated),
    Apps = make_set(AppDisplayName, 20)
    by UserPrincipalName
| order by SignInCount desc
```

CIS-mapping: 15.1-15.7 (Service Provider Management)

3.5 Artikkel 21(2)(e) — Sikkerhet i anskaffelse, utvikling og vedlikehold

Hva regelverket krever: Sikkerhetskrav som del av prosjektprosessen, ikke som etterpå-vurdering. Sikker utvikling der det utvikles programvare.

Microsoft-teknologier:

- **GitHub Advanced Security** (CodeQL static analysis, secret scanning, dependency scanning)
- **Microsoft Defender for DevOps** (i Defender for Cloud)
- **Azure DevOps Security**
- **Azure Pipelines** med sikkerhetstesting innebakt
- **Microsoft Entra Workload Identities** for tjenestebrukere

Steg-for-steg:

Steg 1 — Aktiver GitHub Advanced Security:

For virksomheter som bruker GitHub Enterprise Cloud:

1. GitHub.com → Organization Settings → Advanced Security
2. Aktiver for alle repositories — kost: per committer
3. Funksjoner som aktiveres:
    - **CodeQL** for static analysis (45+ kjente sårbarhetsmønstre)
    - **Secret scanning** for hardkoded credentials, API-nøkler
    - **Dependency scanning** for kjente sårbarheter i tredjepartsavhengigheter (Dependabot-alerts)
    - **Push protection** for å blokkere commits som inneholder secrets

Steg 2 Defender for DevOps i Defender for Cloud:

1. Defender for Cloud → Environment settings → Add environment → GitHub eller Azure DevOps
2. Auth via GitHub App eller Azure DevOps personal access token
3. Aktiverer kontinuerlig scanning av repositories for:
   - Misconfigurations i IaC (Terraform, Bicep, ARM)
   - Eksponerte secrets
   - Sårbarheter i avhengigheter
   - CI/CD pipeline-sikkerhet

Steg 3 Branch protection:

I hvert kritisk repository:

- Krev pull request før merge til main
- Krev minst én kodegjennomgang
- Krev at status checks passerer (CodeQL, Secret scanning, build, tests)
- Krev signerte commits
- Begrens push til admin-roller direkte mot main

Steg 4 Secure SDLC-policy:

Dokumenter at hver utviklingsprosess inkluderer:

Fase	Sikkerhetskrav
Design	Threat modeling for nye features (Microsoft Threat Modeling Tool er gratis)
Implementering	Code review, CodeQL pass, secret scan
Testing	SAST (CodeQL), DAST der relevant, dependency check
Deployment	IaC scanning, signerte artefakter, no-direct-push til prod
Drift	Runtime monitoring (Defender for Cloud), patch management

Verifikasjon:

```
// Kjør jevnlig: GitHub Advanced Security-funn
GitHubAdvancedSecurity_CL
| where TimeGenerated > ago(30d)
| where State_s == "open"
| summarize
    OpenFindings = count(),
    HighSeverity = countif(Severity_s == "high"),
    CriticalSeverity = countif(Severity_s == "critical")
    by RepositoryName_s, Tool_s
| order by CriticalSeverity desc, HighSeverity desc
```

CIS-mapping: 16.1-16.14 (Application Software Security)

3.6 Artikkel 21(2)(f) — Effektvurdering av sikkerhetstiltak

Hva regelverket krever: Løpende sårbarhetshåndtering, penetrasjonstesting og sikkerhetsrevisjoner. Ikke som engangsaktiviteter — som kontinuerlige prosesser.

- **Primær leveransemodell: Arctic Wolf Aurora Managed Risk + Cyber Resilience Assessment**

Aurora Managed Risk (inkludert i Plus- og Total-bundlene) leverer komponent E (risikohåndtering og effektvurdering) som tjeneste:

- **Kontinuerlig sårbarhetsskanning** — internt og eksternt, agent-basert og nettverks-skanning
- **Risikobasert prioritering** — ikke bare CVSS, men kontekstualisert mot virksomhetens miljø, eksponering, og kritikalitet
- **Account takeover-eksponering** — løpende sjekk mot lekkede passord, kompromitterte kontoer på dark web
- **System misconfigurations** — sikkerhetskonfigurasjons-baseline mot CIS Benchmarks og liknende
- **Månedlig eller kvartalsvis rapportering** med ledelsesvennlig presentasjon, sammen med Concierge-leveranse

I tillegg leverer **Aurora Attack Surface Management** (en del av AW-plattformen som standalone produkt) oppdagelse av internet-fasende eiendeler og deres sårbarhets-status — særlig nyttig for virksomheter med distribuert infrastruktur.

Cyber Resilience Assessment (inkludert i alle bundles) gir den årlige strukturerte vurderingen mot industri-rammeverk (NIS2, ISO 27001, CIS Controls, og forsikrings-frameworks) som NIS2-tilsyn ber om dokumentasjon på. Det er ikke en engangsleveranse — det er en gjentakende vurdering som flytter virksomheten gjennom modnings-trappen.

NIS2-kobling

NIS2-krav	Hvordan Arctic Wolf leverer
Løpende sårbarhetshåndtering	Aurora Managed Risk (24/7 monitoring)
Penetrasjonstesting	Ikke en AW-tjeneste — kjøpes separat (se under)
Sikkerhetsrevisjon	Cyber Resilience Assessment + Concierge Security Team-løpende-vurdering
Attack surface management	Aurora Attack Surface Management
Effektvurdering av tiltak	Månedlig Concierge-rapportering med trend-data
Rapportering til styret	Inkludert i Concierge-leveransen, ledelsesvennlig presentasjon

Komplementaritet: Tenable for OT/ICS-spesifikk skanning

For norske virksomheter med industriell infrastruktur (energi, vann, produksjon) er Tenable.io / Tenable.sc ofte foretrukket for OT/ICS-skanning fordi den har bedre dekning av industrielle protokoller (Modbus, DNP3, S7) enn rene IT-vulnerability-plattformer. Aurora Managed Risk kan injeste Tenable-data via API, slik at man får én konsolidert risiko-rapportering selv om underliggende skanning gjøres med Tenable.

Penetrasjonstesting — separat fra Arctic Wolf

Pentest er en aktivitet som krever uavhengighet fra dem som drifter sikkerheten. Arctic Wolf gjør derfor ikke pentest selv — det skal være en uavhengig tredjeparts-aktivitet. Anbefal:

- Årlig ekstern pentest fra en uavhengig tredjepart for NIS2-essensielle virksomheter
- Kvartalsvis er bedre for høyrisiko-sektorer (energi, helse, kritisk infrastruktur)
- Pentest-rapporter mates inn i Aurora Managed Risk-prosessen for prioritert remediering

Alternativ leveranse: Microsoft Defender Vulnerability Management

Microsoft-teknologier:

- **Microsoft Defender Vulnerability Management (MDVM)** — sårbarhetsskanning av endepunkter
- **Microsoft Defender External Attack Surface Management (MDEASM)** — internet-fasende eiendel-discovery
- **Microsoft Secure Score** — løpende baseline-trend
- **Purview Compliance Manager** — kontinuerlig compliance-score

Svakheter ved Microsoft-leveransen:

- MDVM dekker primært endepunktene Defender for Endpoint er installert på — *ikke* OT/ICS, *ikke* nettverksenheter (med mindre Authenticated Scan er konfigurert), *ikke* internet-fasende infrastruktur uten MDEASM-tillegg
- Ingen risikobasert prioritering basert på account-takeover-eksponering
- Ingen menneskelig kontekstualisering — listen av CVSS-er må prioriteres av virksomheten selv
- Ingen integrert månedlig styresak-rapportering — det må bygges fra Compliance Manager-eksport
- MDEASM er en separat lisens, ikke inkludert i E5

Verifikasjon — sårbarhetsstatus mot SLA (KQL)

```
DeviceTvmSoftwareVulnerabilities
| where Timestamp > ago(1d)
| extend AgeDays = datetime_diff('day', now(), FirstSeenTimestamp)
| extend Breach =
    case(
        VulnerabilitySeverityLevel == "Critical" and AgeDays > 7,
"Critical SLA breached",
        VulnerabilitySeverityLevel == "High" and AgeDays > 14, "High
SLA breached",
        VulnerabilitySeverityLevel == "Medium" and AgeDays > 30,
"Medium SLA breached",
        "Within SLA"
    )
| where Breach != "Within SLA"
| summarize BreachCount = count() by VulnerabilitySeverityLevel,
Breach
```

CIS-mapping: 7.1-7.7 (Continuous Vulnerability Management), 18.1-18.5 (Penetration Testing)

3.7 Artikkel 21(2)(g) — Grunnleggende cyberhygiene og opplæring

Hva regelverket krever: Brukeropplæring, awareness-program, phishing-simuleringer. Dokumentert deltakelse for hver bruker.

Primær leveransemodell: Arctic Wolf Aurora Managed Security Awareness and Training

Aurora Managed Security Awareness and Training (inkludert i Total-bundlen) leverer hele opplæringsprogrammet som tjeneste:

- **Fullt managed microlearning content** — virksomheten administrerer ikke kursinnhold, opplastings-kalender, eller phishing-mal-bibliotek. Arctic Wolf leverer det
- **Månedlige phishing-simuleringer** med automatisk eskalering til opplærings-modul for brukere som klikker
- **Rolle-spesifikk opplæring** — Tier 0-administratorer, økonomiske roller, HR, og utviklere får tilpasset innhold
- **Compliance-rapportering** — dokumentert deltakelse per bruker, klar for NSM-tilsyn og styre-rapportering
- **Styremedlems-opplæring** — Innhold som er i samsvar med artikkel 20 designet for styre-medlemmer

Som standard-leveranse er dette mer komplett enn Microsoft-alternativet — fordi den faktisk er en *leveranse*, ikke et verktøy som virksomheten må drifte selv.

NIS2-kobling

NIS2-krav	Hvordan Arctic Wolf leverer
Brukeropplæring	Månedlig microlearning, automatisk levert
Phishing-simuleringer	Inkludert i tjenesten — månedlig kadens
Dokumentert deltakelse	Compliance-dashbord + eksport
Rolle-spesifikk opplæring	Tier 0, HR, økonomi, utviklere, styre — alle dekket
Article 20 styre-opplæring	Inkludert som spesifikk modul

Alternativ leveranse: Microsoft Attack Simulation Training + Viva Learning

Microsoft-teknologier:

- **Attack Simulation Training** (i Defender for Office 365 Plan 2)
- **Microsoft Viva Learning** for integrert opplæringsplattform
- **Microsoft Entra Identity Governance** for compliance-attestering

Svakheter ved Microsoft-leveransen:

- Attack Simulation Training er et verktøy — virksomheten må selv designe kampanjer, velge mal, planlegge kadens, og følge opp brukere
- Innholdet er generisk; det er ikke leveranse-tilpasset rolle eller risikoprofil uten betydelig egeninnsats
- Ingen managed delivery — det er ingen som ringer og sier «her er august-kampanjen, vi har testet den»
- Viva Learning krever separat content-strategi
- Article 20 styre-opplæring er ikke inkludert; må kjøpes som ekstern tjeneste eller bygges internt

Steg-for-steg for Microsoft-leveransen

For virksomheter som velger å drifte opplæring internt:

Steg 1 — Etabler Attack Simulation Training:

1. Defender-portalen → Email & Collaboration → Attack simulation training
2. Opprett en baseline-simulering for alle brukere — typisk en credential harvest
3. Kjør simuleringen — målfase
4. Identifiser brukere som klikket eller leverte credentials
5. Auto-assign training til de som feilet ("Phish landing page" → 5-minutts video)

Steg 2 — Etabler en månedlig kadens:

Måned	Simuleringstype	Treningsfokus
Måned 1	Credential harvest	Hvordan oppdage phishing-mail
Måned 2	Malware-vedlegg	Vedlegg-hygiene
Måned 3	OAuth consent	"Permission scams" — apper som ber om tilgang
Måned 4	CEO fraud	Sosial ingeniørkunst
Måned 5	Drive-by URL	Web-baserte angrep
Måned 6	Repeat baseline	Mål forbedring versus måned 1

Steg 3 — Spesialisert opplæring for risikogrupper:

- Tier 0-administratorer: kvartalsvis dypere opplæring om identitets-angrep
- Styremedlemmer: årlig opplæring som er i samsvar med artikkel 20 (typisk ikke dekket av Microsoft — krever ekstern leverandør)
- HR / økonomi: månedlig social engineering-fokus
- Utviklere: secure coding (kvartalsvis)

Steg 4 — Dokumentasjon:

NIS2 krever dokumentasjon på at hver bruker har gjennomgått opplæring. Bruk:

- Viva Learning-rapporter for individuell deltakelse

- Compliance Manager for å spore virksomhetsnivået i prosent
- Eksport til Sentinel via Microsoft Graph API for langtidsoppbevaring

Verifikasjon — KQL hunt for failed phishing-simuleringer

```
AttackSimulation_CL
| where TimeGenerated > ago(90d)
| where SimulationStatus == "Failed"
| summarize
    FailedSimulations = count(),
    LastFailure = max(TimeGenerated),
    SimulationsCompleted = make_set(SimulationName_s, 10)
    by UserPrincipalName_s
| extend RiskLevel = case(
    FailedSimulations >= 3, "High",
    FailedSimulations == 2, "Medium",
    "Low"
)
| where RiskLevel in ("High", "Medium")
| order by FailedSimulations desc
```

CIS-mapping: 14.1-14.9 (Security Awareness and Skills Training)

3.7.1 E-postflyt og e-postsikkerhetsarkitektur

Hvorfor dette er en NIS2-relevant seksjon: E-post er den dominerende angrepsvektoren mot norske virksomheter — BEC, phishing, malware, og kompromittert kommunikasjon. NIS2 dekker e-post implisitt gjennom flere Artikkel 21-elementer: (b) hendelseshåndtering, (g) cyberhygiene, (h) kryptografi, og (j) sikker kommunikasjon. I praksis krever det at virksomheten har en bevisst e-postsikkerhetsarkitektur — ikke bare den default-konfigurasjonen Exchange Online leveres med.

Denne seksjonen er bevisst lagt mellom 2.7 (opplæring) og 2.8 (kryptografi) fordi e-postsikkerhet binder begge. Awareness-trening uten god teknisk e-post-filtrering er ikke nok. E-post-filtrering uten brukeropplæring er heller ikke nok.

Tre topologier å velge mellom

I norske mellomstore virksomheter ser jeg tre dominerende oppsett:

Topologi A — Microsoft-native: Defender for Office 365 Plan 2 alene
Topologi B — Tredjeparts gateway foran Exchange Online (MX-topologi): Proofpoint / Mimecast / annet er primær MX, prosesserer all e-post, ruter til Exchange Online **Topologi C — Inline / API-integrasjon ved siden av Exchange Online:** Tredjepart kobles via API til Exchange Online uten å være i MX-kjeden (også kalt ICES — Integrated Cloud Email Security)

Hver topologi har konsekvenser for NIS2-relevante kontroller:

Aspekt	A (Microsoft-only)	B (gateway-foran)	C (inline/API)
DNS-endring	Ingen	Ja, MX peker til gateway	Ingen, MX peker til M365
Spool ved utfall	M365 standard 24t	Gateway-leverandørens spool (lengre)	M365 standard 24t
Forensisk analyse av blokkerte meldinger	Defender XDR	Hos gateway-leverandør (ofte bedre verktøy)	Hos ICES-leverandør
Tredjepart kan se klartext-innhold?	Nei	Ja (gateway dekrypterer TLS)	Ja (API-tilgang)
Kompleksitet for tilsyn	Lavest — én leverandør	Høyest — to logg-kjeder	Middels
TLS-kjede	M365 ende-til-ende	Gateway terminerer TLS	M365 ende-til-ende, ICES sjekker postdokumenter

Topologi A — Microsoft-native (Defender for Office 365 Plan 2)

For virksomheter som har full E5-lisensiering og ikke har en historisk gateway-leverandør, kan Defender for Office 365 Plan 2 alene være en løsning som er akseptabel og i samsvar med NIS2.

Konfigurasjon:

1. **Anti-phishing-policy:**
   - Threshold: 3 (Most aggressive)
   - Impersonation protection: aktivert for nøkkelpersoner (CEO, CFO, økonomi-team, HR-team)
   - Mailbox intelligence: aktivert
   - Spoof intelligence: aktivert
2. **Safe Links-policy:**
   - URL rewriting for alle innkommende meldinger
   - Real-time URL scanning
   - Dynamic delivery (avhengig av lyst på forsinkelse)
3. **Safe Attachments-policy:**

- Dynamic Delivery: lever e-post umiddelbart, hold vedlegg under detonation
- Block: ikke lever meldingen før vedlegg er klarert

4. **DKIM/DMARC/SPF:**
   - SPF: v=spf1 include:spf.protection.outlook.com -all
   - DKIM: aktiver via Defender → Email & Collaboration → Policies → DKIM
   - DMARC: start på p=none, monitor i 30 dager, escalér til p=quarantine, deretter p=reject
5. **Attack Simulation Training:** (allerede dekket i 2.7)

Topologi B — Proofpoint (eller Mimecast) som gateway foran Exchange Online

Den vanligste topologien hos større norske virksomheter — særlig der det er historisk Proofpoint-investering. MX peker på Proofpoint som mottar all innkommende e-post, prosesserer (anti-spam, anti-phishing, sandboxing, archive), og ruter klarert e-post videre til Exchange Online via SMTP-konnektor.

NIS2-relevante konfigurasjonspoeng:

1. **Send connectors** i Exchange Online må begrenses til Proofpoints IP-rangevirksomheten — slik at angripere ikke kan omgå Proofpoint ved å sende direkte til M365-tenant-endepunkter:

```
# Konfigurer transport rule i Exchange Online for å avvise e-post som ikke
kommer fra Proofpoint
New-TransportRule -Name "Block direct mail bypassing Proofpoint" `
    -SenderAddressLocation "Header" `
    -FromScope "NotInOrganization" `
    -ExceptIfSenderIPRanges "PROOFPOINT_IP_RANGES" `
    -RejectMessageReasonText "All inbound mail must route via the corporate
email gateway" `
    -RejectMessageEnhancedStatusCode "5.7.1"
```

2. **Defender for Office 365 i sekundærrolle:** Defender skal fortsatt være aktiv som et dypere lag — slik at ikke gateway-leverandøren blir det eneste sikkerhetslaget. Konfigurer Defender for å:
   - Sjekke meldinger som har passert gateway (sjekk på nytt internt)
   - Skanne innebygd intern-til-intern e-post (gateway ser ikke dette)
   - Skanne SharePoint, OneDrive, og Teams (utenfor gateways scope)
3. **Logg-konsolidering for hendelseshåndtering:**

- Proofpoint TAP-logger må enten eksporteres til Sentinel (via Proofpoint TAP/EFD API-konnektor) eller til MDR-leverandørens workspace
- Defender for Office 365-logger må også havne samme sted
- For Artikkel 23-rapportering må SOC kunne søke på tvers av begge kilder innen 24 timer

4. **Mail-spool-konsekvens:** Proofpoint som gateway gir typisk lengre spool-evne (typisk 5-14 dager, men kan endres etter egne definisjoner) enn M365 default. Det er en NIS2-fordel under et Exchange Online-utfall (Artikkel 21(2)(c) driftskontinuitet).

Topologi C — Inline / API-integrasjon (ICES)

Trenden 2024-2026 har vært bort fra MX-gateway og mot ICES-modellen — Proofpoint Integrated, Abnormal Security, IRONSCALES, Microsoft-konfigurerte API-koblinger. MX peker fortsatt på M365, men en tredjepart har API-tilgang til mailbox-content for å:

- Identifisere allerede leverte phishing-meldinger og fjerne dem post-delivery
- Analysere sender-mottaker-mønstre for BEC-deteksjon
- Skanne historisk korrespondanse for å trene atferdsmodellen

NIS2-konsekvenser:

- Bedre internkommunikasjon-beskyttelse (kjenner all e-post, ikke bare innkommende)
- Forenklet DNS-administrasjon (ingen MX-endring)
- Mister gateway-spool (e-post leveres direkte til M365)
- ICES-leverandøren har **bred API-tilgang til mailbox-content** — dette må vurderes som risiko og dekkes av leverandørklausuler under Artikkel 21(2)(d) leverandørkjede-sikkerhet

Sikker kommunikasjon for sensitive samtaler

Uavhengig av topologi, krever NIS2 at sensitive samtaler har en sikker kanal. For e-post spesifikt:

- **S/MIME** for ende-til-ende-signerte og krypterte meldinger til klarerte mottakere — krever sertifikat-utrulling
- **Microsoft Purview Message Encryption (OME)** for adhoc-kryptert e-post med sensitivity label (enklere å rulle ut enn S/MIME)

- **Out-of-band-kanal** for absolutt sensitivt: Signal eller annen E2EE-løsning, ikke e-post

For NSM-varsling under en e-postkompromittering: ikke send varslet på e-post. Bruk en out-of-band-kanal (telefon, krypterte meldinger, NSMs alternative kontaktkanal).

Verifikasjon — uavhengig av topologi:

```
# Sjekk DMARC-konfigurasjon for virksomhetens domener
Connect-ExchangeOnline

Get-AcceptedDomain | ForEach-Object {
    $domain = $_.DomainName
    $dmarc = Resolve-DnsName -Name "_dmarc.$domain" -Type TXT -
ErrorAction SilentlyContinue
    [PSCustomObject]@{
        Domain = $domain
        DMARC = if ($dmarc) { $dmarc.Strings -join "" } else { "NOT
SET" }
    }
} | Format-Table -AutoSize

# Sjekk om transport rules blokkerer mail-bypass
Get-TransportRule | Where-Object { $_.Name -match
"bypass|gateway|Proofpoint|Mimecast" } |
    Select-Object Name, State, Priority |
    Format-Table -AutoSize
```

KQL — Cross-topology e-posthunting:

```
// Identifiser meldinger som har passert e-post-laget men har URLer
som ble klikket etterpå
EmailEvents
| where TimeGenerated > ago(7d)
| where DeliveryAction == "Delivered"
| join kind=inner (
    UrlClickEvents
    | where TimeGenerated > ago(7d)
    | where ActionType == "ClickAllowed"
) on $left.NetworkMessageId == $right.NetworkMessageId
| project Timestamp, SenderFromAddress, RecipientEmailAddress,
Subject, Url, ThreatTypes
| where ThreatTypes has_any ("Phish", "Malware", "Spam")
| order by Timestamp desc
```

CIS-mapping: 9.1-9.7 (Email and Web Browser Protections)

3.8 Artikkel 21(2)(h) — Kryptografi og kryptering

Hva regelverket krever: Policy for hva som skal krypteres når, og hvordan nøkler håndteres. Inkluderer både data at rest og data in transit.

Microsoft-teknologier:

- **Microsoft Purview Information Protection** — sensitivity labels med kryptering
- **BitLocker** via Intune på endepunkter
- **Azure Key Vault** for nøkkellagring
- **Microsoft 365 Customer Key** (for kunder som ønsker bring-your-own-key)
- **Azure Confidential Computing** for spesielle use-cases

Steg-for-steg:

Steg 1 — Sensitivity labels:

Definer minimum 4 nivåer av sensitivity labels:
(Dette er eksempler på bruk, definer dette etter virksomhetens behov)

Label	Encryption	Watermark	Auto-apply
Public	Nei	Nei	—
Internal	Nei	“Internal Use Only”	Default for alt nytt
Confidential	AES-256	“Confidential”	Auto-detect kredittkort, personnummer
Highly Confidential	AES-256 + content-restricted	“Highly Confidential”	Manuell

Publiser labels via Purview-portalen → Information Protection → Labels og Label policies.

Steg 2 — BitLocker via Intune:

Intune → Endpoint Security → Disk encryption → Create Policy → Windows 10 and later → BitLocker

Innstillinger:

```
- BitLocker Drive Encryption: Enabled
- Drive Encryption Method: XTS-AES 256-bit
- System Drives Require Startup Authentication: Enabled
- Configure TPM Startup: Required
- Configure TPM Startup PIN: Required (for kritiske enheter)
- Minimum PIN Length: 8
- Recovery key backup: Azure AD
```

Steg 3 — Azure Key Vault for sentralisert nøkkelhåndtering:

```
# Opprett en Key Vault med RBAC-basert tilgang (anbefalt over access
policies)
$rg = "rg-keyvault-prod"
$location = "norwayeast"
$kvName = "kv-prod-nis2"

New-AzKeyVault `
    -Name $kvName `
    -ResourceGroupName $rg `
    -Location $location `
    -EnableRbacAuthorization `
    -EnablePurgeProtection `
    -EnableSoftDelete `
    -SoftDeleteRetentionInDays 90

# Tildel RBAC-rolle for nøkkel-administrator
$kvId = (Get-AzKeyVault -Name $kvName).ResourceId
New-AzRoleAssignment `
    -ObjectId (Get-AzADGroup -DisplayName "KeyVault-
Administrators").Id `
    -RoleDefinitionName "Key Vault Administrator" `
    -Scope $kvId
```

Steg 4 — Customer Key (valgfritt):

Hvis virksomheten har krav om å eie sine egne krypteringsnøkler for Microsoft 365-data:

1. Anskaff Customer Key-lisens
2. Opprett 2 Key Vaults i to forskjellige Azure-regioner
3. Generer “data encryption policy” som peker på begge KV-er
4. Bruk for Exchange Online-mailboxer og SharePoint Online-sites

Merk: dette gir kontroll, ikke nødvendigvis økt sikkerhet. Microsoft kan fortsatt lese dataene; Customer Key gir deg muligheten til å revoke tilgang gjennom å slette nøkkelen.

Verifikasjon:

```
# Sjekk BitLocker-status på alle Intune-enheter
Connect-MgGraph -Scopes "DeviceManagementManagedDevices.Read.All"

Get-MgDeviceManagementManagedDevice -All |
    Where-Object { $_.OperatingSystem -eq "Windows" } |
    Select-Object DeviceName, UserPrincipalName,
        @{N="BitLockerStatus";E={
            (Get-MgDeviceManagementManagedDeviceComplianceState `
                -ManagedDeviceId $_.Id).BitLockerStatus
        }} |
    Where-Object { $_.BitLockerStatus -ne "On" } |
    Format-Table -AutoSize
```

CIS-mapping: 3.6, 3.11 (Data Protection)

3.9 Artikkel 21(2)(i) — Personellsikkerhet, tilgangskontroll og asset management

Hva regelverket krever: Det største og mest komplekse området. Hvem har tilgang til hva, hvorfor, og hvordan kontrolleres det? Asset management, joiner-mover-leaver, prinsippet om minste rettighet.

Microsoft-teknologier:

- **Microsoft Entra Privileged Identity Management (PIM)** — JIT-elevasjon for administrative roller
- **Microsoft Entra ID Identity Governance** — access reviews, entitlement management
- **Microsoft Intune** — enhet-tilgangskontroll, compliance policies
- **Microsoft Endpoint Privilege Management (EPM)** — JIT for lokale administratorrettigheter på Tier 2-endepunkter
- **Microsoft Defender for Endpoint** — asset inventory
- **Conditional Access** — kontekstuell tilgangsbeslutning

Steg-for-steg:

Steg 1 — Aktiver PIM for alle privilegerte roller:

1. Entra-portalen → Identity Governance → Privileged Identity Management
2. Konfigurer hver høyt-privilegerte rolle (minimum: Global Admin, Privileged Role Admin, Security Admin, User Admin, Exchange Admin, SharePoint Admin):

   Eligibility: Eligible (ikke Active)
   Activation max duration: 4 timer
   Activation requires:
   ☑ Justification
   ☑ MFA
   ☑ Approval (for Global Admin)
   ☑ Ticket information (Jira/ServiceNow-ID)
   Notification: Send e-post til sikkerhetsteamet ved aktivering

Steg 2 — Aktiver Identity Protection:

1. Entra-portalen → Identity Protection
2. Sign-in risk policy: Krev MFA ved Medium og High risk
3. User risk policy: Krev passord-reset ved High risk
4. Bind via Conditional Access for granulær kontroll

Steg 3 — Access Reviews kvartalsvis:

For hver privilegert rolle, sett opp en kvartalsvis access review:

1. Entra → Identity Governance → Access reviews
2. Opprett review per rolle
3. Reviewer: enten manager eller en designert sikkerhetsansvarlig
4. Action on results: Auto-apply (fjern brukere som ikke ble approved)
5. Mail-påminnelser: 7, 3, 1 dag før deadline

Steg 4 — Endpoint Privilege Management for Tier 2:

EPM er en del av Intune Suite — krever egen tilleggslisens:

1. Intune → Endpoint security → Endpoint Privilege Management
2. Opprett en policy som fjerner lokale administratorrettigheter fra alle vanlige brukere

3. Opprett “elevation rules” for apper som legitimt trenger admin-rettigheter (f.eks. ScreenConnect-konsulent-verktøy med signert sertifikat)
4. Slik kan brukere kjøre spesifikke apper med elevation uten å være lokal admin

Steg 5 — Asset inventory via Defender for Endpoint:

Defender for Endpoint vedlikeholder en automatisk inventory av: - Endepunkter (Windows, macOS, Linux, mobile) - Installert programvare per enhet - Brukere som er logget på - Nettverkstilkoblinger

Bruk dette som primær asset inventory; eksporter til Sentinel for langtidsoppbevaring og korrelasjon.

```
// Asset inventory: enheter som ikke har vært online i 30 dager
DeviceInfo
| summarize LastSeen = max(Timestamp) by DeviceName
| where LastSeen < ago(30d)
| extend Finding = "Device offline >30 days — investigate
(lost/decommissioned/dormant)"
| project DeviceName, LastSeen, Finding
| order by LastSeen asc
```

Verifikasjon (PowerShell):

```
# Sjekk at PIM er aktivert for alle høyt-privilegerte roller
Connect-MgGraph -Scopes "RoleManagement.Read.Directory"

$criticalRoles = @(
    "Global Administrator",
    "Privileged Role Administrator",
    "Security Administrator",
    "User Administrator"
)

foreach ($roleName in $criticalRoles) {
    $role = Get-MgRoleManagementDirectoryRoleDefinition -Filter
"displayName eq '$roleName'"
    $activeAssignments = Get-MgRoleManagementDirectoryRoleAssignment `
        -Filter "roleDefinitionId eq '$($role.Id)'"
    $eligibleAssignments = Get-
MgRoleManagementDirectoryRoleEligibilitySchedule `
        -Filter "roleDefinitionId eq '$($role.Id)'"

    Write-Host "$roleName — Active: $($activeAssignments.Count),
Eligible: $($eligibleAssignments.Count)"

    if ($activeAssignments.Count -gt 0) {
        Write-Warning "$roleName has STANDING active assignments —
should be eligible via PIM"
    }
}
```

CIS-mapping: 5.1-5.6, 6.1-6.8 (Account Management og Access Control Management)

3.10 Artikkel 21(2)(j) — MFA og sikker kommunikasjon

Hva regelverket krever: MFA på alt — ikke bare admin-kontoer. Definerte krypterte kommunikasjonsvalg for sensitive samtaler. Nødkommunikasjon i tilfelle ordinære kanaler er kompromittert.

Microsoft-teknologier:

- **Microsoft Entra ID Authentication Methods** (FIDO2, Windows Hello for Business, Authenticator)
- **Authentication Strengths** for phishing-resistant MFA-policyer
- **Microsoft Teams** med E2EE-meldinger og samtaler
- **Microsoft Authenticator number matching** (standard nå)

Steg-for-steg:

Steg 1 — Phishing-resistant MFA for Tier 0:

Entra → Protection → Authentication strengths → Create
Name: "Phishing-resistant MFA"

Allowed methods:
☑ FIDO2 security key
☑ Windows Hello for Business
☑ Certificate-based authentication (Multi-Factor)

Bind via Conditional Access:

CA Policy: "Require phishing-resistant MFA for Tier 0 roles"
Users: All users in role "Global Administrator", "Privileged Role Administrator", etc.
Apps: All cloud apps
Grant: Require authentication strength → Phishing-resistant MFA

Steg 2 — Standard MFA for alle andre:

Selv om phishing-resistant er ideelt, er standard MFA via Authenticator app et minimum:

CA Policy: "MFA for all users"
Users: All users (exclude break-glass accounts)
Apps: All cloud apps
Conditions: Exclude trusted locations (optional)
Grant: Require multi-factor authentication

Steg 3 — Disable legacy authentication:

Legacy auth (Basic Auth, IMAP, POP, SMTP AUTH) er ikke MFA-kompatibel og må blokkeres:

CA Policy: "Block legacy authentication"
Users: All users
Apps: All cloud apps
Conditions: Client apps → Other clients (legacy)
Grant: Block access

Steg 4 — Authenticator number matching:

Aktivert som default siden 2023, men verifiser:

Entra → Authentication methods → Microsoft Authenticator
Microsoft Authenticator → Configure → Require number matching for push notifications: Enabled
Geographic location in push notifications: Enabled
App name in push notifications: Enabled

Steg 5 — Teams sikker kommunikasjon:

For sensitive samtaler:

- Aktivér Teams E2EE for 1:1-samtaler (Teams Admin Center → Voice → Enhanced encryption policies)
- Konfigurer DLP-policyer for å oppdage og blokkere sending av klassifisert data i Teams-chat
- For særlig sensitive samtaler, bruk Signal eller annen tredjeparts E2EE-løsning (Teams E2EE er kun for media stream, ikke chat-historikk)

Steg 6 — Nødkommunikasjon:

For NSM-varsling under en M365-hendelse hvor primær e-post er kompromittert:

- Etabler “out-of-band”-kontakt med NSM (telefon, krypterte meldinger via Signal)
- Konfigurer alternative kontaktopplysninger i NSM-registrering
- Vakthavende har tilgang til alternative kommunikasjonsverktøy fra personlige enheter (Signal-grupper med kommandostrukturen)

Verifikasjon:

```
// Brukere som har autentisert med MFA siste 30 dager
SigninLogs
| where TimeGenerated > ago(30d)
| where ResultType == 0
| extend MFAUsed = AuthenticationDetails contains "succeeded"
       and AuthenticationDetails contains "MFA"
| summarize
    TotalSignIns = count(),
    MFASignIns = countif(MFAUsed),
    MFAPercentage = todouble(countif(MFAUsed)) / count() * 100
    by UserPrincipalName
| where MFAPercentage < 100
| project UserPrincipalName, TotalSignIns, MFASignIns, MFAPercentage
| order by MFAPercentage asc, TotalSignIns desc
```

CIS-mapping: 6.3, 6.4, 6.5 (Multi-Factor Authentication)

4. Tverrgående tema

4.1 Logging, audit og retensjon — Microsoft Sentinel vs MDR-leveransemodell

NIS2 krever ikke en eksplisitt retensjonstid for logger, men kombinasjonen av Artikkel 21(2)(b) (hendelseshåndtering), 21(2)(f) (effektvurdering), og praktiske krav til tilsynsdokumentasjon betyr at logger bør lagres minimum 1 år. For tilsynsbevis 2 år. For finansielle og helse-sektorer, ofte 5 år eller mer.

Det viktige er ikke *hvor* loggene oppbevares, men at retensjonen er definert, at NSM kan få tilgang til loggene ved tilsyn, og at virksomheten kan svare på Artikkel 23-rapporteringskravene innen 24/72-timers-fristene basert på logg-analyse.

To likeverdige arkitekturmønstre

Mønster A — Microsoft Sentinel som primær logg-aggregator (virksomhetseid):

Loggene injestes direkte i et Sentinel workspace eid av virksomheten. Virksomheten har full kontroll over retensjon, søk, og analyse. Egen SOC eller intern sikkerhetsorganisasjon driver Sentinel.

Mønster B — MDR-leverandørens workspace som primær (tjenesteleverert):

Loggene rutes til en MDR-leverandør (Arctic Wolf eller andre tilsvarende leverandører — Sophos MDR, CrowdStrike Falcon Complete, eller liknende) som vedlikeholder workspace og leverer 24/7 deteksjon og respons. Virksomheten har tilgang ihht. kontrakt, men eier ikke selve plattformen.

For norske mellomstore virksomheter uten eget 24/7 SOC er Mønster B ofte mer realistisk enn Mønster A. Hovedfeilen som gjøres er å tro at Mønster A er den eneste veien som er i samsvar med NIS — det er den ikke. Mønster B er også i samsvar med NIS2, forutsatt at retensjons- og tilgangskravene er forankret i kontrakter.

Mønster A — Microsoft-loggkilder og standard retensjon

Kilde	Standard retensjon	Hvor det utvides
Entra ID Sign-in logs	30 dager (P1/P2)	Eksporter til Sentinel/Storage
Entra ID Audit logs	30 dager (P1/P2)	Eksporter til Sentinel/Storage
Microsoft 365 Audit Log	180 dager (E5) / 1 år (Audit Premium)	Eksporter til Sentinel
Defender XDR Advanced Hunting	30 dager	Eksporter til Sentinel for lengre
Sentinel Log Analytics	30-730 dager (konfigurerbart)	Archive-tier opp til 12 år

Anbefalt arkitektur for logging i samsvar med NIS2 (Mønster A):

1. **Hot tier (Sentinel Analytics):** 90 dager — aktiv hunting, alarmering, KQL-analyse
2. **Warm tier (Sentinel Basic):** 1 år — tilgjengelig for søk men ikke alarmering, lavere kost
3. **Archive tier (Sentinel Archive):** 7 år — bevart for revisjon, kan hentes fram med “search jobs”
4. **Storage Account backup:** 10+ år for de mest sensitive loggene

```
// Sentinel-tabell-retensjon-status
Usage
| where TimeGenerated > ago(30d)
| where IsBillable == true
| summarize TotalGB = sum(Quantity) / 1024 by DataType
| order by TotalGB desc
```

Mønster B — MDR-leverandørens plattform som primær

I dette mønsteret leveres deteksjons- og retensjonsfunksjonen som tjeneste. MDR-leverandørens egen Cloud Detection and Response-plattform (slik Arctic

Wolfs CDR-arkitektur eksemplifiserer, men prinsippet gjelder for alle seriøse MDR-leverandører) tar imot logger via dedikerte konnektorer:

Kildetype	Hvordan ingest skjer
Microsoft 365 audit / Entra ID	API-konnektor (Microsoft Graph + Office Activity API)
Microsoft Defender XDR	Defender API / Microsoft Sentinel integration
Tredjeparts EDR (CrowdStrike, Cortex XDR, SentinelOne)	Native EDR-konnektor
E-postsikkerhet (Proofpoint, Mimecast)	API-konnektor
SaaS (Okta, Duo, Google Workspace, AWS, Azure)	API-konnektor
On-prem / brannmurer	Syslog forwarder eller leverandørens egen agent

NIS2-konsekvenser av Mønster B:

1. **Retensjon styres av kontrakt, ikke av Azure-policy.** Verifiser at MDR-leverandørens standard er minimum 365 dager (alle seriøse leverandører tilbyr dette). For finans- og helse-sektor, forhandle inn 2-5 års retensjon i kontrakten.
2. **NSM-tilgang til logger må være sikret i kontrakten.** Klausul: “Leverandøren skal levere logguttrekk innen 72 timer ved tilsynsforespørsel fra norske myndigheter (NSM, sektormyndighet, eller relatert).” Dette er ikke standard — det må eksplisitt avtales. Et DORA addendum til en kontrakt vil ta høyde for dette for finansvirksomheter.
3. **Hendelses-eierskap:** Ved en signifikant hendelse må det være klart hvem som tar Artikkel 23-rapporteringsbeslutningen — leverandøren foreslår, virksomheten avgjør. Leverandørens IR-team kan ha NSM-mal og prosess klar, men virksomhetens CISO må trykke på knappen. Dette må stå i kontrakten.
4. **Datasouvereignitet:** For norske virksomheter, kontroller hvor MDR-leverandørens workspace er hostet. Arctic Wolf har Europa-region, men ikke nødvendigvis Norge eller Norden. For NIS2-essensielle virksomheter med suverenitetskrav, sjekk dette.
5. **Exit-plan:** Når kontrakten med MDR-leverandøren utløper, må logger kunne eksporteres tilbake til virksomheten — minimum siste 12 måneder, helst hele retensjonsperioden. Klausul kreves.

Hva som er likt i begge mønstre

Uavhengig av om Mønster A eller B velges, må følgende være på plass:

- **Loggintegritet:** Logger må ikke kunne modifiseres etter ingest. Sentinel beskytter dette via Azure-storage-immutability; MDR-leverandører gjør tilsvarende. Bekreft i kontrakt.
- **Dokumentert retensjonspolicy:** Skriftlig, godkjent av ledelsen, gjennomgått årlig.
- **Tilgangskontroll:** Hvem kan lese loggene? Hvem kan slette dem? Tilgang skal logges, og loggene over logg-tilgang er selv loggdata.
- **Søkbarhet:** Innen 24 timer skal SOC kunne svare på "hvilke påloggинger har bruker X hatt siste 90 dager?" og lignende spørsmål. Test dette periodisk.

4.2 Hendelsesresponsorganisasjon

For virksomheter med intern 24/7 SOC ser organisasjonen typisk slik ut. For virksomheter som benytter MDR-modell (Del 3.5), erstattes SOC Tier 1 og deler av Tier 2 av MDR-leverandørens funksjon. Begge mønstrene er i samsvar med NIS2.
Rolle-rolle-matrise — NIS2-tilpasset (intern SOC):

Rolle	Primær ansvar	Backup	24/7-kontaktbar
SOC Tier 1 Analyst	Initial deteksjon, triage	MSSP fallback	Ja (24/7-vakt)
Incident Commander	Klassifisering, koordinering	Vara	Ja (vakttelefon)
CISO	Beslutning om NSM-varsling	CIO	Ja
Juridisk	Rådgivning rundt rapportering	Ekstern juridisk rådgiver	I åpningstid + telefon
Kommunikasjonsansvarlig	Intern + ekstern kommunikasjon	CEO som backup	I åpningstid + telefon
Tekniske spesialister	Forensisk analyse, gjenoppretting	Eksterne IR-konsulenter	På anrop
Styreleder	Informert ved alvorlige hendelser	Nestleder	På anrop

Rolle-rolle-matrise — MDR-leveransemodell:

Rolle	Primær ansvar	Hvem leverer	24/7-kontaktbar
Initial deteksjon og triage	Identifiser, klassifiser, varsle	MDR-leverandørens SOC	Ja (kontraktuell SLA)
MDR-koordinator (intern)	Mottaker av MDR-alarmer	Vakthavende sikkerhetsansvarlig	Ja
Incident Commander	Beslutning om respons	Intern, eskaleres fra MDR	Ja
CISO	Beslutning om NSM-varsling	Intern (kan ikke delegeres)	Ja
MDR-IR-team	Forensikk og containment	MDR-leverandør (typisk del av avtalen)	Ja (aktiveres on-demand)
Juridisk, kommunikasjon, styre	Som over	Intern	I åpningstid + telefon

I MDR-modellen er det viktig at virksomhetens **MDR-koordinator** er definert med navngitt primær og backup. Når MDR-leverandøren ringer kl. 03:00 fredag natt, må noen ta telefonen, og den noen må ha myndighet til å iverksette respons-beslutninger umiddelbart (isolere endepunkt, deaktivere konto, eskalere til CISO).

Eskaleringsmatrise:

Severity 1 (kritisk, NIS2-rapporteringspliktig):
T+0: SOC oppdager → Incident Commander varslet
T+15min: Initial vurdering — er dette NIS2-relevant?
T+1h: CISO + juridisk + kommunikasjon på på telco
T+4h: Beslutning om NSM-varsling
T+24h: NSM tidlig varsling sendt
T+72h: NSM hendelsesmelding sendt
T+1uke: Styremedlem informert (ikke nødvendigvis hele styret)
T+1mnd: Sluttrapport til NSM

Severity 2 (alvorlig, ikke nødvendigvis NIS2):
T+0: SOC → Tier 2 sikkerhetsansvarlig
T+1h: Initial vurdering
T+4h: Hvis eskaleres til Sev 1, følg over

Severity 3+ (rutine): SOC-egen håndtering, rapporter månedlig

4.3 Microsoft Secure Score som styringssensor

Secure Score gir en kvantifisert tilstand av M365-sikkerhetsmodenheten. For NIS2-formål bruk det som:

- Månedlig styringsindikator til CISO (mål: stigende trend)
- Kvartalsvis rapportering til styret (sammen med Compliance Manager-score)
- Sammenligning mot benchmark — Microsoft viser “industry average”

Typisk modningstrappen vi har sett hos norske mellomstore virksomheter:

Fase	Secure Score-prosent	Innhold
Baseline	30-45 %	Default M365-konfigurasjon
Innsats 1	50-60 %	MFA overalt, Conditional Access standardpolicy, Defender XDR aktiv
Innsats 2	65-75 %	PIM, Identity Protection, Defender Vulnerability Management, sensitivity labels
Innsats 3	75-85 %	Phishing-resistant MFA, EPM, Defender for Cloud Apps, Customer Key
Moden	85 %+	Sjeldent uten dedikert sikkerhetsteam og kontinuerlig optimalisering

4.4 Purview Compliance Manager — NIS2-template

Som nevnt i 2.1 har Microsoft levert en NIS2-template i Compliance Manager. Denne er den enkleste måten å spore Artikkel 21-implementeringen mot en strukturert kontroll-katalog.

Bruksmønster:

1. Bind hver kontroll i templaten til en intern eier
2. Dokumenter implementasjon med M365-spesifikk evidens (skjermbilder, PowerShell-output, KQL-resultater)
3. Sett oppfølgingsdato per kontroll
4. Eksporter rapport månedlig til ledergruppen, kvartalsvis til styret
5. Bruk eksporten som vedlegg til styreprotokollen — det er den dokumentasjonen NSM kan be om

4.5 MDR / MR / IR som NIS2-utfyllende tjeneste

For mange norske virksomheter er én av de største praktiske barrierene mot NIS2-compliance ikke teknisk — det er bemanning. NIS2 Artikkel 21(2)(b) krever effektiv hendelseshåndtering, inkludert evnen til å vurdere alvorlighetsgrad og varsle NSM innen 24 timer. Det forutsetter en deteksjonsfunksjon som er operativ 24/7. De aller fleste norske mellomstore virksomheter har ikke en intern 24/7 SOC, og de fleste vil ikke ha det i 2026 heller.

Denne seksjonen behandler hvordan eksterne sikkerhetstjenester — MDR, MR, og IR-retainer — kan levere de funksjonene som en intern virksomhet ikke når. Seksjonen er bevisst leverandør-uavhengig: Arctic Wolf eller andre tilsvarende leverandører — Sophos MDR og CrowdStrike Falcon Complete er eksempler på tjenester som passer modellen, og veiledningen behandler dem som tjeneste-modell heller enn produkt-valg.

MDR — Managed Detection and Response

Hva tjenesten faktisk leverer:

- 24/7 menneskelig overvåkning av sikkerhetsalarmer på tvers av endepunkt, identitet, e-post, og sky
- Triage og initial responsbeslutning innen leverandørens SLA (typisk 15-30 minutter for kritiske alarmer)
- Koordinert respons med kundens IT-organisasjon
- Integrasjon med kundens egen ticketing og kommunikasjon
- Månedlig rapportering på hendelses-volum, MTTR, og trender

NIS2-kobling:

- Direkte adresserer Artikkel 21(2)(b) hendelseshåndtering
- Støtter Artikkel 23 24-timers-rapporteringskravet ved å levere en alltid-på vurderingsfunksjon
- Leverer Artikkel 21(2)(f) effektvurdering gjennom løpende sikkerhetsovervåkning og rapportering

Kontraktsklausuler som er kritiske for NIS2:

Krav	Hvorfor
Initial respons-SLA på kritiske alarmer (≤ 30 min)	Må holde 24-timers-fristen til NSM
Eskaleringsmatrise med navngitt CST/SOC-kontakt	"Concierge"-modellen som Arctic Wolf og enkelte andre tilbyr; sikrer at riktig person nås raskt
Rett til å aktivere IR-retainer på MDR-leverandør	Sømløs overgang fra deteksjon til respons
Logguttrekk innen 72 timer på forespørsel	NSM-tilsyn
Dataresidens i EU/EØS (helst Norden)	Datasouvereignitet for sensitive sektorer
Hendelseskommunikasjon på norsk	NSM-rapportering må være på norsk

MR — Managed Risk (sårbarhetshåndtering som tjeneste)

Hva tjenesten faktisk leverer:

- Kontinuerlig sårbarhetsskanning (internt og eksternt)
- Risikobasert prioritering (ikke bare CVSS, men kontekstualisert mot virksomhetens miljø)
- Account takeover-eksponering (lekkede passord, kompromitterte kontoer)
- System misconfigurations
- Månedlig eller kvartalsvis rapportering med ledelsesvennlig presentasjon

NIS2-kobling:

- Direkte adresserer Artikkel 21(2)(f) effektvurdering — kontinuerlig sårbarhetshåndtering er kjernen
- Støtter Artikkel 21(2)(i) tilgangskontroll ved å identifisere kontoer med kompromittert eksponering
- Eksempler på leverandører: Arctic Wolf Managed Risk, Tenable som managed service via partner, Rapid7 Managed Vulnerability Management

Komplementaritet med Microsoft-stakken: MR-tjenester gir verdi utover Defender Vulnerability Management ved å:

- Skanne hele angrepsoverflaten, ikke bare endepunktene Defender ser
- Tilby kontekstualisering ("denne CVE-en er kritisk for deg fordi den treffer ditt eksponerte system, ikke fordi CVSS sier 9.8")
- Inkludere identitet-/account-takeover-overvåkning som Defender ikke dekker

IR — Incident Response (retainer-basert)

Hva tjenesten faktisk leverer:

- Forhandshandlet IR-team som kan aktiveres under en alvorlig hendelse
- Forensisk analyse og containment
- Koordinering med juridisk og kommunikasjon
- Sluttrapport som kan inngå i Artikkel 23 1-måneds-rapport til NSM

NIS2-kobling:

- Adresserer den siste fasen av Artikkel 21(2)(b) — håndtering og gjenoppretting etter en alvorlig hendelse
- Støtter Artikkel 21(2)(c) driftskontinuitet gjennom strukturert recovery-prosess
- Den 1-måneds sluttrapporten som NIS2 Artikkel 23 krever er ofte produkt av IR-arbeidet

To IR-modeller:

1. **Standalone IR-retainer:** Mandiant, CrowdStrike Services, Arctic Wolf IR, andre lokale IR-tjenesteleverandører. Aktiveres on-demand under hendelse. Kost typisk per time eller forhåndskjøpt timer.
2. **IR inkludert i MDR-tjeneste:** Sømløs overgang fra MDR-deteksjon til IR-respons innenfor samme leverandøravtale. Reduserer friksjon, men låser deg til én leverandør.

For NIS2-essensielle virksomheter anbefales en IR-retainer **i tillegg til** primær MDR-leverandørens IR-kapabilitet. Det gir en backup hvis primær leverandør selv blir kompromittert eller har kapasitetsproblemer under en bransje-bred hendelse.

Hvordan vurdere om virksomheten bør bruke MDR-modellen

Beslutningstre:

Spørsmål	Hvis ja →
Har du intern 24/7 SOC med minst 6 dedikerte analytikere?	Mønster A (intern Sentinel, eget SOC)
Har du intern SOC, men kun arbeidstidsbasert?	Hybrid: intern i dagtid, MDR for kveld/helg/natt
Har du ingen intern SOC, men IT-drift med sikkerhetsoppmerksomhet?	Mønster B (full MDR)
Er du essensiell virksomhet i sektor som krever 24/7 respons (energi, vann, helse)?	MDR + IR-retainer fra to ulike leverandører
Er virksomheten under 50 ansatte, men leverer til NIS2-virksomhet?	Vurder MDR for å oppfylle leverandørklausuler, selv om dere ikke er i scope selv

Felles arkitektur uavhengig av leverandørvalg

Uansett hvilken MDR-leverandør som velges, må følgende være på plass for at tjenesten faktisk skal levere på NIS2:

1. **Definert primær kontakt hos virksomheten.** Vakthavende-rolle med myndighet til å motta MDR-alarmer 24/7 og iverksette respons. Dette er ikke en e-postadresse — det er en navngitt person med backup.
2. **Forhåndsdefinert Article 23-prosess.** Hva utløser at NSM varsles? Hvem trykker på knappen — virksomheten eller leverandøren? Hva er NSM-malen, og hvor er den lagret? Dette skal være kjørt gjennom som tabletop minst én gang før første tilsyn.
3. **Koordinert kommunikasjonsplan.** Når MDR-leverandøren ringer kl. 03:00, hvem ringer de? Hvilken bridge eskalerer de til? Hvordan informeres styret og ledergruppen?
4. **Klargjorte data-deling-rutiner.** Hvilke logger og artefakter får MDR-leverandøren tilgang til? Hvor lenge oppbevarer de dem? Hva skjer ved kontraktsslutt?
5. **Test, ikke bare etabler.** En MDR-tjeneste som ikke har vært stresset i et reelt scenario er en hypotese, ikke en kontroll. Kvartalsvise tabletop-øvelser med leverandøren som deltaker er minimum.

Konkret om Arctic Wolf som leverandøreksempel

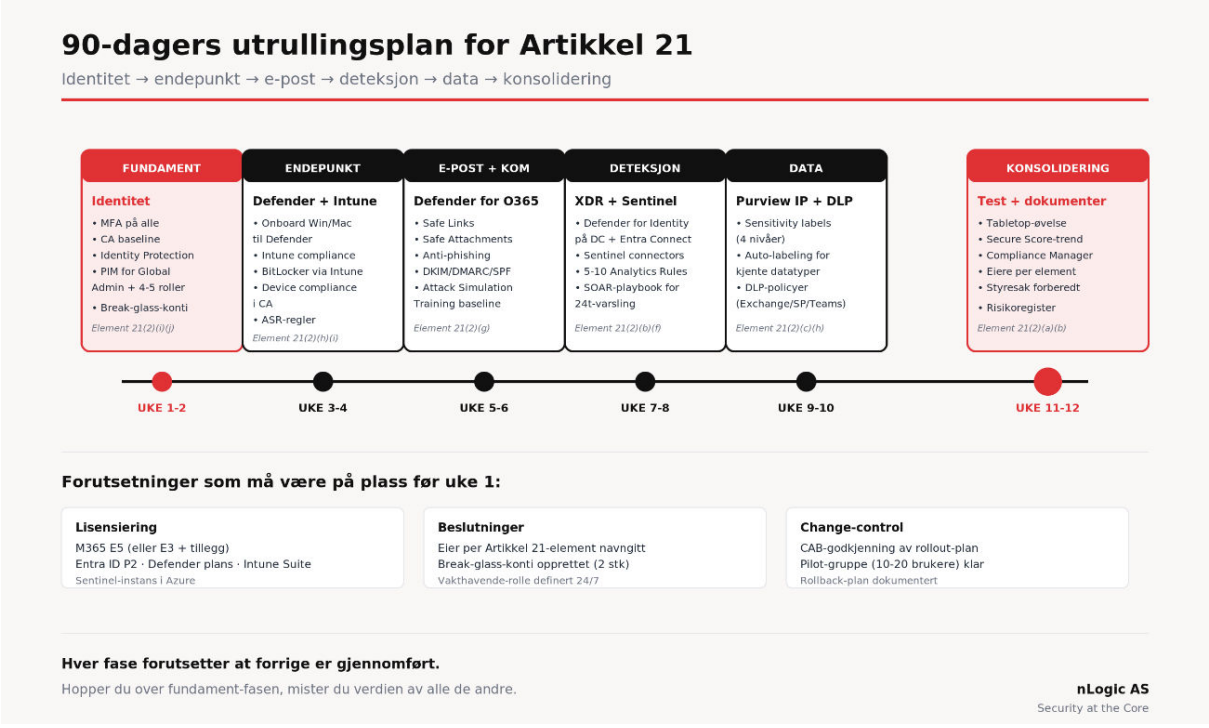
Arctic Wolf brukes hyppigst som referansepunkt i denne typen veiledning fordi deres CDR-plattform har den mest dokumenterte integrasjonsmatrisen mot Microsoft 365 (se referanser). Plattformen injester logger fra Microsoft 365 audit, Entra ID, Defender XDR, Defender for Cloud Apps, samt fra tredjeparts EDR, e-postsikkerhet, og SaaS-applikasjoner. Concierge Security Team-modellen — der hver kunde får en navngitt sikkerhetsingeniør som primær kontakt — passer godt med NIS2s krav til at hendelseskoordinering må skje med definerte mennesker, ikke med en e-postkø.

Dette betyr ikke at Arctic Wolf er det riktige valget for alle. Norske alternativer finnes og også andre tilsvarende nordiske MDR-leverandører. CrowdStrike Falcon Complete er et godt valg der CrowdStrike allerede er primær EDR. Sophos MDR passer der Sophos-stakken er etablert. Valget bør være kontekstuelt — størrelse, sektor, eksisterende investeringer og geografisk preferanse.

Hovedpoenget er: NIS2 forutsetter 24/7 deteksjonsevne. Få norske virksomheter kan etablere det internt. MDR-modellen er den mest realistiske veien dit for de fleste.

5. Implementering

5.1 90-dagers utrullingsplan



90-dagers utrullingsplan med ukentlige milepæler. Fokus på rekkefølge: identitet → deteksjon → respons → leverandør → opplæring. Hva som må være på plass før neste fase kan starte.

Uke 1-2 — Fundament (Identity-først):

- Aktiver MFA på alle brukere
- Etabler Conditional Access baseline (MFA, block legacy auth, require compliant device for admin)
- Aktiver Identity Protection
- Konfigurer PIM for Global Admin og 4-5 andre kritiske roller
- Onboard break-glass-kontoer (2 stk, dokumentert)

Uke 3-4 — Endepunktbeskyttelse:

- Onboard alle Windows-endepunkter til Defender for Endpoint via Intune
- Konfigurer baseline Intune compliance policies
- Aktivér BitLocker via Intune-policy
- Etablér device compliance som krav i Conditional Access
- Konfigurer ASR-regler (Attack Surface Reduction) i Defender XDR

Uke 5-6 — E-post og samarbeid:

- Konfigurer Defender for Office 365 Safe Links + Safe Attachments
- Aktivér Anti-phishing-policyer
- Etablér DKIM, DMARC, SPF (egne domener)
- Aktiver Attack Simulation Training med baseline-test

Uke 7-8 — Deteksjon og respons:

- Aktivér Defender for Identity på alle DC-er og Entra Connect
- Onboard Sentinel med kjernekonnektorer (Defender XDR, Entra ID, M365)
- Implementer 5-10 high-value Analytics Rules
- Bygg SOAR-playbook for 24-timers-varslingsklargjøring

Uke 9-10 — Data og kryptografi:

- Publiser sensitivity label-strategi
- Konfigurer Information Protection auto-labeling for kjente data-typer
- DLP-policyer for Exchange, SharePoint, Teams
- Aktiver Microsoft Information Protection scanner for on-prem data hvis relevant

Uke 11-12 — Konsolidering:

- Kjør tabletop-øvelse (se 4.2)
- Gjennomgå Secure Score-trend, Compliance Manager-score
- Dokumenter alle eiere per Artikkel 21-element
- Forbered første styremøtepresentasjon (se 4.3)

5.2 Tabletop-øvelse for 24/72-varsling

Følgende scenario brukes for kvartalsvis tabletop-øvelse:

Scenario: Fredag kl. 16:45 oppdager SOC Tier 1 at en bruker i finansavdelingen har klikket på en phishing-mail og oppgitt credentials. Innen minutter ser de unormal aktivitet på brukerens konto — påloginger fra en utenlandsk IP, opprettelse av en mail forwarding-regel som videresender all innkommende e-post til en gmail-konto, og forsøk på å sende noen titalls e-poster eksternt.

Spørsmål til øvelsen:

1. Hvem skal Tier 1 ringe? Er nummeret i en kommunikasjonsmal som er tilgjengelig kl. 16:45 fredag?
2. Hvilken playbook i Sentinel skal trigge automatisk? Hva slags handlinger gjør den (block account, isolate device, revoke sessions)?
3. Innen 1 time: hvem deltar på telco-en? Hvor er telco-bridge-nummeret dokumentert?
4. Innen 4 timer: hva er CISO-ens beslutning — er dette NSM-rapporteringspliktig?
5. Innen 24 timer (lørdag kl. 16:45): hvis CISO konkluderer “ja”, hvem sender det første NSM-varselet? Hvor er malen?
6. Innen 72 timer (mandag morgen): som koordinerer hendelsesmelding 2?

7. Når informeres styreleder? Når informeres hele styret?

Vanlige funn fra første tabletop:

- Ingen vet hvem den vakthavende CISO-en faktisk er på en fredag kveld
- NSM-malen finnes ikke ennå
- Telco-bridge-nummeret er hardkodet i én Outlook-kalenderoppfølging — ikke i en mal
- Det er uklart om Sentinel-playbook'en faktisk blokkerer kontoen, eller bare logger at den ble forsøkt blokkert
- Juridisk er ikke informert om NIS2-rapporteringskrav før øvelsen

Det er det øvelsen er for. Fix funnene, kjør om igjen om tre måneder.

5.3 Måling og rapportering til styret

Kvartalsvis styresak — strukturen:

Element	Innhold	Datakilde
Trend siste kvartal	Secure Score, Compliance Manager-score, NIS2 readiness %	Sentinel workbook
Hendelser siste kvartal	Antall, alvorlighetsgrad, MTTR, lærdom	Defender XDR-rapport
Risiko-godkjenninger som krever vedtak	Konkrete saker	Risikoregister
Status på pågående tiltak	Per Artikkel 21-element	Compliance Manager
Leverandørstatus	Topp 20 leverandører — sikkerhetsmodenhet	Internt register
Opplæring	% deltakelse, phishing-failure-rate	Attack Simulation Training
Investeringsbehov	Hva mangler ressurser	Plan

Årlig styresak:

- Vedtak: oppdatert cybersikkerhets-strategi
- Vedtak: budsjett for kommende år
- Gjennomgang av forrige års hendelser
- Tabletop-øvelse-funn og forbedringstiltak
- NIS2 tilsynsstatus

---

6. Vedlegg

6.1 Vedlegg A — PowerShell-baseline-skript for tilstandssjekk

```
# NIS2 Artikkel 21 – Microsoft 365 baseline tilstandssjekk
# Krever: Microsoft.Graph, Az PowerShell
# Kjøres med Global Reader-rolle eller høyere

Connect-MgGraph -Scopes
"User.Read.All","Policy.Read.All","SecurityEvents.Read.All",
                      "DeviceManagementConfiguration.Read.All",
                      "RoleManagement.Read.Directory","Reports.Read.All"

$report = @()

# 21(2)(a) Secure Score
$score = Get-MgSecuritySecureScore -Top 1
$report += [PSCustomObject]@{
    Article = "21(2)(a)"
    Check = "Microsoft Secure Score"
    Value = "$($score.CurrentScore) / $($score.MaxScore)"
    Status = if (($score.CurrentScore / $score.MaxScore) -ge 0.7) { "OK" }
else { "Improvement needed" }
}

# 21(2)(d) Conditional Access for B2B
$caPolicies = Get-MgIdentityConditionalAccessPolicy
$b2bPolicy = $caPolicies | Where-Object {
    $_.Conditions.Users.IncludeUsers -contains "GuestsOrExternalUsers"
}
$report += [PSCustomObject]@{
    Article = "21(2)(d)"
    Check = "Conditional Access for B2B guests"
    Value = if ($b2bPolicy) { "Found $($b2bPolicy.Count) policy" } else { "NOT
FOUND" }
    Status = if ($b2bPolicy) { "OK" } else { "Action required" }
}


# 21(2)(h) BitLocker compliance via Intune
$devices = Get-MgDeviceManagementManagedDevice -All -Filter "operatingSystem
eq 'Windows'"
$encrypted = ($devices | Where-Object { $_.IsEncrypted -eq $true }).Count
$total = $devices.Count
$report += [PSCustomObject]@{
    Article = "21(2)(h)"
    Check = "BitLocker on Windows devices"
    Value = "$encrypted / $total"
    Status = if ($total -gt 0 -and ($encrypted / $total) -ge 0.95) { "OK" }
else { "Action required" }
}


# 21(2)(i) PIM aktivert for Global Admin
$globalAdminRole = Get-MgRoleManagementDirectoryRoleDefinition -Filter
"displayName eq 'Global Administrator'"
$standingAssignments = Get-MgRoleManagementDirectoryRoleAssignment `
    -Filter "roleDefinitionId eq '$($globalAdminRole.Id)'"
$report += [PSCustomObject]@{
    Article = "21(2)(i)"
    Check = "Global Administrator standing assignments"
    Value = "$($standingAssignments.Count) standing"
    Status = if ($standingAssignments.Count -le 2) { "OK (break-glass)" } else
{ "Move to PIM-eligible" }
}
```

```
# 21(2)(j) MFA - alle brukere
$mfaReport = Get-MgReportAuthenticationMethodUserRegistrationDetail `
    -Filter "isMfaRegistered eq false" -All
$report += [PSCustomObject]@{
    Article = "21(2)(j)"
    Check = "Users without MFA registered"
    Value = "$($mfaReport.Count) users"
    Status = if ($mfaReport.Count -eq 0) { "OK" } else { "Action required" }
}

$report | Format-Table -AutoSize
$report | Export-Csv -Path "nis2-baseline-$(Get-Date -Format 'yyyyMMdd').csv"
-NoTypeInformation
```

6.2 Vedlegg B — KQL-jaktpakke

Hunt 1: Privilegerte kontoer med standing assignments:

```
IdentityInfo
| where TimeGenerated > ago(7d)
| extend AssignedRoles = todynamic(AssignedRoles)
| mv-expand AssignedRoles
| extend RoleName = tostring(AssignedRoles)
| where RoleName has_any (
    "Global Administrator", "Privileged Role Administrator",
    "Security Administrator", "User Administrator",
    "Exchange Administrator", "SharePoint Administrator"
)
| distinct AccountUPN, RoleName, AccountObjectId
| extend Finding = "Standing assignment — should be PIM-eligible"
```

Hunt 2: Brukere uten MFA siste 30 dager:

```
SigninLogs
| where TimeGenerated > ago(30d)
| where ResultType == 0
| extend AuthDetails = parse_json(AuthenticationDetails)
| extend HasMFA = AuthDetails has "MFA"
| summarize
    TotalSignIns = count(),
    MFASignIns = countif(HasMFA),
    Apps = make_set(AppDisplayName, 10)
    by UserPrincipalName
| where MFASignIns == 0 and TotalSignIns >= 5
| project UserPrincipalName, TotalSignIns, MFASignIns, Apps
```

Hunt 3: Mistenkelig data-eksfiltrering (Article 21(2)(b)):

```
CloudAppEvents
| where TimeGenerated > ago(7d)
| where Application in ("Microsoft SharePoint", "Microsoft OneDrive",
"Microsoft Teams")
| where ActionType in~
("FileDownloaded","FileSyncDownloadedFull","FileAccessed")
| summarize
    DownloadCount = count(),
    UniqueFiles = dcount(ObjectName),
    TotalSize =
sum(toint(coalesce(tostring(parse_json(RawEventData).ObjectSize), "0")))
    by AccountObjectId, AccountDisplayName, bin(TimeGenerated, 1h)
| where DownloadCount > 100 or UniqueFiles > 50
| extend Finding = "Possible mass download — investigate"
| order by DownloadCount desc
```

Hunt 4: Conditional Access bypass-forsøk:

```
SigninLogs
| where TimeGenerated > ago(7d)
| where ConditionalAccessStatus == "failure"
| summarize
    FailureCount = count(),
    UniqueIPs = dcount(IPAddress),
    PoliciesTriggered = make_set(ConditionalAccessPolicies, 10)
    by UserPrincipalName
| where FailureCount >= 10 or UniqueIPs >= 3
| extend Finding = "Possible MFA bombing or policy evasion"
```

Hunt 5: Defender for Identity høyverdis-deteksjoner:

```
AlertInfo
| where TimeGenerated > ago(30d)
| where DetectionSource == "MicrosoftDefenderForIdentity"
| where Severity in ("High", "Medium")
| join kind=inner (
    AlertEvidence
    | where EntityType == "User"
) on AlertId
| project Timestamp, Title, Severity, AccountName, DomainName, Categories
| order by Timestamp desc
```

6.3 Vedlegg C — Conditional Access policy-maler

Mal 1: MFA for alle brukere (baseline):

Name: CA001 - Baseline MFA
State: Enabled
Users: All users
  Exclude: Break-glass accounts, Service accounts (named)
Applications: All cloud apps
  Exclude: (none — alle apps)
Conditions:
  Client app: All
Grant: Require MFA

Mal 2: Block legacy authentication:

Name: CA002 - Block Legacy Auth
State: Enabled
Users: All users
Applications: All cloud apps
Conditions:
  Client app: Exchange ActiveSync clients, Other clients
Grant: Block access

Mal 3: Phishing-resistant MFA for Tier 0:

Name: CA003 - Tier 0 PRMFA
State: Enabled
Users: Role-based group "Tier 0 Administrators"
Applications: All cloud apps
Grant: Require authentication strength = "Phishing-resistant MFA"
Session:
  Sign-in frequency: 1 hour
  Persistent browser session: Never persistent

Mal 4: B2B Guests — compliant device + MFA:

Name: CA004 - B2B Guests Compliance
State: Enabled
Users: All guests and external users
Applications: All cloud apps (or scope to specific apps)
Grant: Require MFA AND Require compliant device

Session:
  Sign-in frequency: 1 hour

Mal 5: Block from non-trusted countries:

Name: CA005 - Geographic Restriction
State: Enabled (or Report-only first)
Users: All users
  Exclude: Travel exception group
Applications: All cloud apps
Conditions:
  Locations: Include "All locations", Exclude "Trusted countries" (definert i Named locations)
Grant: Block access

6.4 Vedlegg D — Dokumentmaler

Mal 1: NSM 24-timers tidlig varsling

Til: NSM CSIRT — incident@nsm.no (eller via NSM-portal)
Fra: [Virksomhetsnavn — registreringsnummer i NSM-portal]
Dato/tid for varsling: [YYYY-MM-DD HH:MM]
Dato/tid for første observasjon: [YYYY-MM-DD HH:MM]

1. Hendelsens art (kort beskrivelse):
   [En til to setninger]

2. Mistenkt årsak:
   [ ] Mistenkt ulovlig/ondsinnet aktivitet
   [ ] Ikke fastslått
   [ ] Teknisk feil/menneskelig feil

3. Mulig grenseoverskridende konsekvens:
   [ ] Ja — beskriv hvilke EU-/EØS-land som kan være berørt
   [ ] Nei
   [ ] Ikke fastslått

4. Initial vurdering av alvorlighetsgrad:
   [ ] Kritisk — betydelig drift-/data-/tjenestepåvirkning
   [ ] Alvorlig — vesentlig påvirkning
   [ ] Moderat

5. Kontaktinformasjon:
   Navn: [Incident Commander]
   Telefon: [+47 XXX XX XXX]
   E-post: [navn@virksomhet.no]
   Alternativ kontakt: [stilling, navn, telefon]

6. Forventet oppfølging:
   [En setning om når neste oppdatering forventes — typisk innen 72t]

Mal 2: Risikoregister — én rad per risiko

Risiko-ID: R-2026-001
Område: [Eks: Identitet og tilgang]
NIS2-element: [Artikkel 21(2)(i)]
Beskrivelse: [Klar, kort beskrivelse av risikoen]
Trusselskilde: [Eks: ekstern angriper, intern feilbruk]
Sannsynlighet: [Lav / Middels / Høy / Svært høy]
Konsekvens: [Lav / Middels / Høy / Svært høy]
Risikoscore: [Sannsynlighet × Konsekvens]
Eier: [Navngitt rolle]
Tiltak:
- [Tiltak 1] — Status: [Pågående/Vedtatt/Implementert] — Frist: [Dato]
- [Tiltak 2] ...

Restrisiko etter tiltak: [Lav / Middels / Høy]
Styregodkjenning: [Dato — protokoll-referanse]
Neste gjennomgang: [Dato]

6.5 Vedlegg E — Referanser

- Microsoft — *NIS2 Compliance & Cybersecurity Solutions* — https://www.microsoft.com/en-us/trust-center/compliance/nis2-compliance
- Microsoft Learn — *Microsoft Purview Compliance Manager regulations list* — https://learn.microsoft.com/en-us/purview/compliance-manager-regulations-list
- Microsoft Learn — *Build and manage assessments in Microsoft Purview Compliance Manager* — https://learn.microsoft.com/en-us/purview/compliance-manager-assessments
- Microsoft Learn — *Incident Response in Microsoft Defender Portal* — https://learn.microsoft.com/en-us/security/zero-trust/respond-incident-defender
- Microsoft Learn — *Microsoft Defender for Identity overview* — https://learn.microsoft.com/en-us/defender-for-identity/what-is
- Microsoft Learn — *Microsoft Defender XDR* — https://learn.microsoft.com/en-us/defender-xdr/
- Microsoft Learn — *Microsoft Sentinel* — https://learn.microsoft.com/en-us/azure/sentinel/
- Microsoft Learn — *Entra Privileged Identity Management* — https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/

- Microsoft Learn — *Conditional Access* — https://learn.microsoft.com/en-us/entra/identity/conditional-access/
- Microsoft Learn — *Securing privileged access (Tier 0/1/2 model)* — https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-strategy
- NIS-2 Directive — Article 21 — https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html
- NIS-2 Directive — Article 23 — https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html
- Nasjonal sikkerhetsmyndighet — *Ny digitalsikkerhetslov i Norge* — https://nsm.no/aktuelt/ny-digitalsikkerhetslov-i-norge
- NSMs Grunnprinsipper for IKT-sikkerhet 2.1 — https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/
- CIS Critical Security Controls v8 — https://www.cisecurity.org/controls/v8
- NIST Cybersecurity Framework 2.0 — https://www.nist.gov/cyberframework
- ENISA — *Mapping NIS 2 obligations with ECSF role profiles* — https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%202%20obligations%20with%20ECSF%20role%20profiles.pdf

MDR / MR / IR-modell — eksempler på leverandører og dokumentasjon:

- Arctic Wolf — *Cloud Detection and Response Integrations* — https://docs.arcticwolf.com/en/active-response-log-forwarding-and-security-monitoring/cloud-detection-and-response-integrations/cloud-detection-and-response-integrations
- Arctic Wolf — *Managed Detection and Response* — https://arcticwolf.com/solutions/managed-detection-and-response/
- Arctic Wolf — *Managed Risk* — https://arcticwolf.com/solutions/managed-risk/
- Sophos — *Managed Detection and Response* — https://www.sophos.com/en-us/products/managed-detection-and-response
- CrowdStrike — *Falcon Complete (Managed XDR)* — https://www.crowdstrike.com/services/managed-services/falcon-complete/

E-postsikkerhet — leverandører:

- Proofpoint — *Microsoft 365 Integration (MX Deployment)* — https://help.proofpoint.com/Essentials/Product_Documentation/Account_Management/Integrations/Microsoft_365_Integration_MX

- Proofpoint — *Integrated Deployment (ICES)* — https://www.proofpoint.com/us/products/email-security-and-protection
- Mimecast — *Email Security for Microsoft 365* — https://www.mimecast.com/products/email-security/
- Microsoft Defender for Office 365 Plan 2 — https://learn.microsoft.com/en-us/defender-office-365/

Sårbarhetshåndtering — alternativer:

- Tenable — *Tenable Vulnerability Management* — https://www.tenable.com/products/tenable-io
- Qualys — *VMDR* — https://www.qualys.com/apps/vulnerability-management-detection-response/
- Rapid7 — *InsightVM* — https://www.rapid7.com/products/insightvm/
-

EDR-alternativer:

- CrowdStrike Falcon — https://www.crowdstrike.com/platform/endpoint-security/
- Palo Alto Cortex XDR — https://www.paloaltonetworks.com/cortex/cortex-xdr
- SentinelOne Singularity — https://www.sentinelone.com/platform/

7. nLogic Security

nLogic er en pålitelig nordisk partner for nettverks- og sikkerhetsløsninger med høy ytelse, og hjelper virksomheter med å bygge sikkerhet som et system — ikke bare som compliance.

Denne artikkelen om NIS2 og styreansvar er utarbeidet av nLogic Security, sikkerhetsteamet i nLogic.

Teamet arbeider med sikkerhetsarkitektur, governance, regulatoriske sikkerhetskrav, risikoanalyse og operasjonell sikkerhet i komplekse virksomhetsmiljøer.

Arbeidet handler ikke bare om teknologi, men om hvordan virksomheter faktisk styrer, dokumenterer og følger opp cyberrisiko når regulatoriske krav, trusselbildet og forretningsrisiko møtes i praksis.

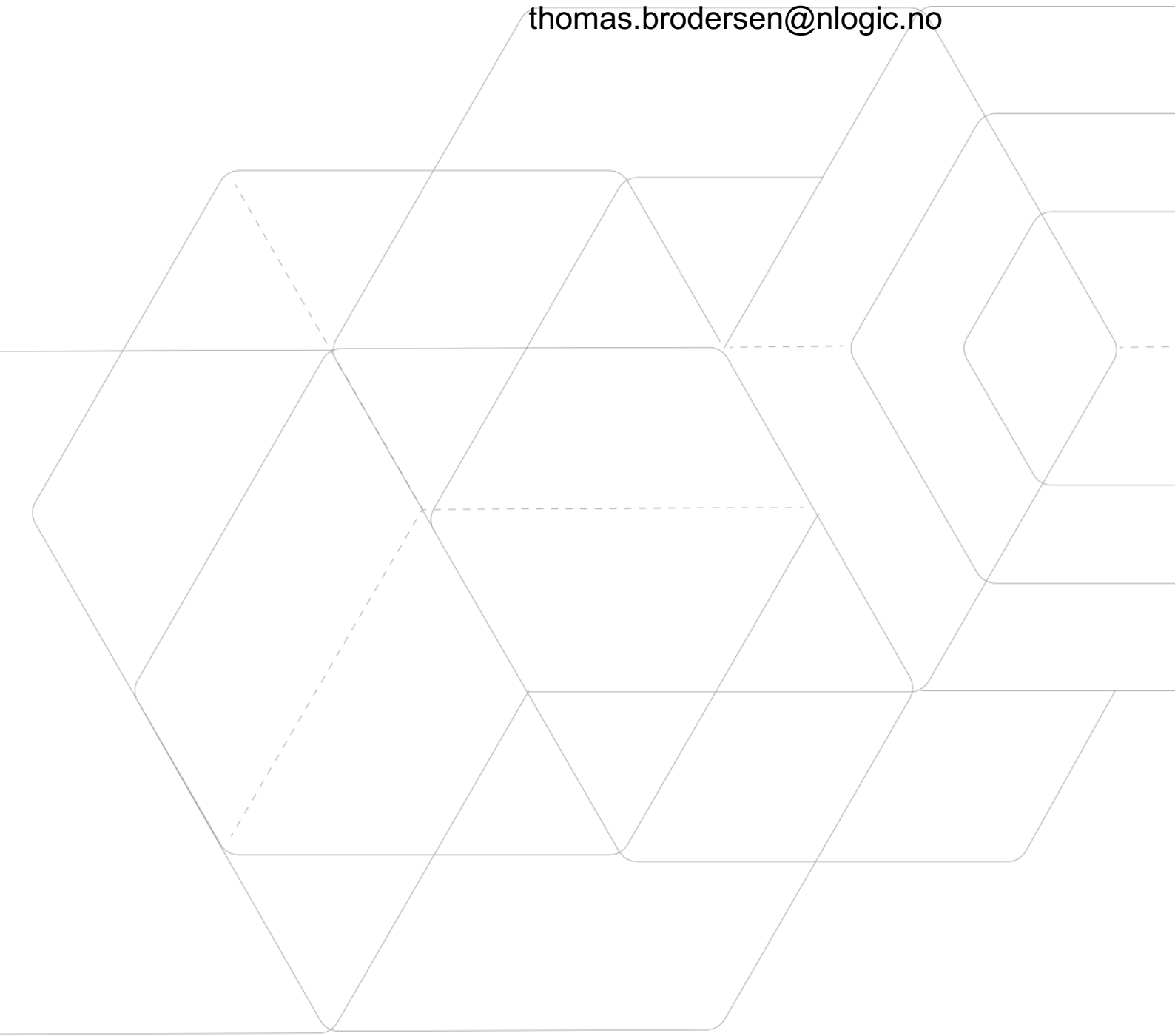
Disse artiklene er en del av nLogics arbeid med kunnskapsdeling, analyse og praktisk risikoreduksjon i moderne virksomhetsmiljøer — med fokus på hvordan sikkerhetskontroller faktisk fungerer når de møter reelle trusler, operative kompromisser og nye angrepsmetoder.

Powered by Knowledge. Driven by Trust.

Dette dokumentet er en teknisk implementeringsveiledning, ikke en juridisk eller compliance-uttalelse. Microsoft 365- og Azure-konfigurasjoner som beskrives skal valideres mot egen risikoprofil, change-control-prosedyrer, og operasjonell beredskap før produksjonsutrulling. Lisensieringsoversikten reflekterer Microsoft-priser per mai 2026 og kan endres. nLogic AS tar ikke ansvar for anvendelse av denne veiledningen utenfor et dedikert prosjekt/oppdrag med våre konsulenter.

Thomas Brodersen

IT Security Advisor
+47 95830108
thomas.brodersen@nlogic.no



Kontakt oss

nLogic AS
Karenslyst Allé 20, 0278 Oslo
Org.nr.: 821 678 102
info@nlogic.no

Powered by Knowledge.
Driven by Trust.