

The background of the image is a dark blue, almost black, field filled with a dense, ethereal cloud of white and light blue particles. These particles appear to be in motion, creating a sense of depth and dynamic energy. The particles are more concentrated in some areas, forming soft, glowing clouds, while other areas are darker and more sparse.

intility | The Enterprise  
Cloud Solution

# Om Intility



- En ende-til-ende **plattformtjeneste**
- **650** selskaper på **2 500** lokasjoner
- **600+** medarbeidere (snittalder 28 år)
- Organisk **vekst**. Langsiktig **eierskap**



# En urolig verden



Brukerkontoer  
på avveie



Phishingangrep



Angrep over  
flere medier



Fremtreden av  
KI i angrep



Utnyttelse av  
sårbarheter

## EU cyber strategy for the digital decade

*«The threat landscape is compounded by geopolitical tension over the global and open internet and over control of technologies across the whole supply chain»*

EU cyber strategy for the digital decade

*«EU Should drive standards and norms for world class solutions and standards of cyber security»*

# EU som premissleverandør



Høye ambisjoner



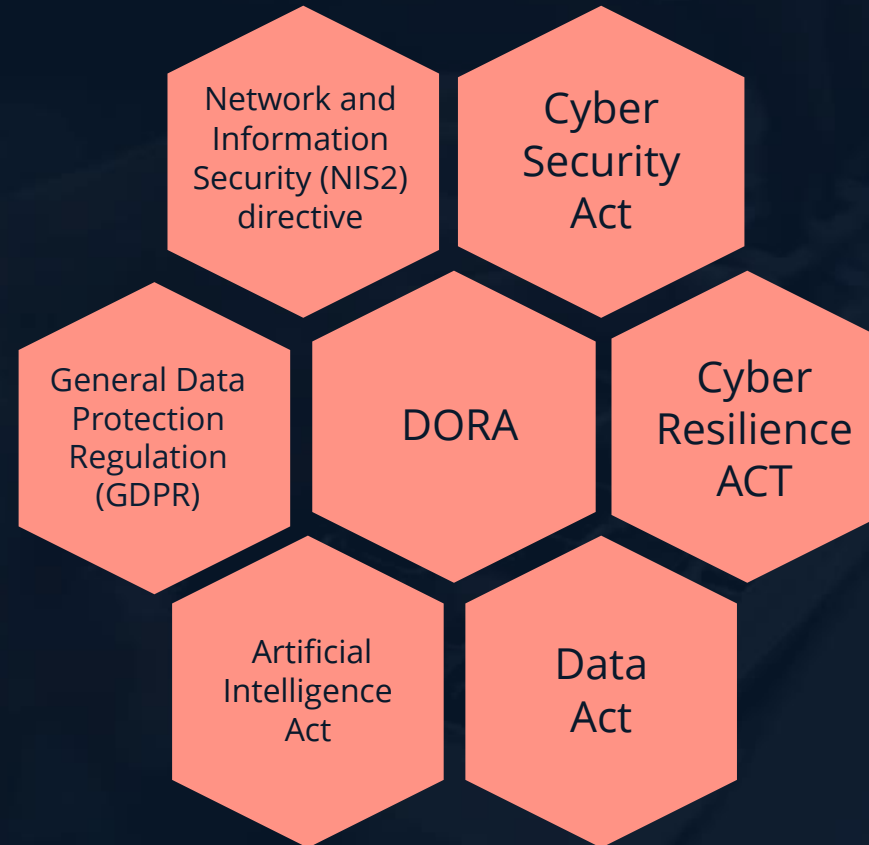
Etterlevelse gjennom reguleringer



På tvers av sektorer



# Regelmaskinen EU



DORA



Digital Operational  
Resilience Act

NIS 2



Network and  
Information  
Security Directive

# Største **risikoer** ved kjøp av **tjenester**



Tilgjengelighet



Sikkerhet



Compliance



Lock-in



Kontraktrisiko\*

\*Komplekse og lite forståelige kontrakter

## Største **risikoer** ved bruk av **skytenester**



Tilgjengelighet



Sikkerhet



Compliance



Lock-in



Kontraktrisiko\*

## Største **kontraktsrisikoer**



Databehandling



Immaterielle-  
rettigheter



Ansvar og erstatnings-  
begrensinger



Regulatoriske  
krav



Uklare bestemmelser  
som kan lede til tvister

# De viktigste «praktiske» **risikoene** vi kan og må håndtere



Sikkerhet



Compliance



Databehandling

# Klassifiser

## leveransen/leverandøren

- Skille mellom «viktige» og «mindre viktige»  
— hvordan sette kriterier?
- Kategorisering på tvers av  
regelverk/hensyn/verdier

# Praktisk oppfølging

Må tilpasses egen virksomhet og risikoer

- Type virksomhet
- Internasjonal overføring
- Antall underleverandører
- Type behandling

## A. Spesielle kategorier av personopplysninger?

- ☐ Under 1000: (1 poeng)
- ☐ 1000 - 10 000: (2 poeng)
- ☐ Over 10 000: (3 poeng)

POENG

## B. Spesielle kategorier av personopplysninger?

- ☐ Ja (3 poeng)

POENG

## C. Andre beskyttelsesverdige personopplysninger?

- ☐ Ja (2 poeng)

POENG

## D. Spesielle behandlinger?

- ☐ Ja (2 poeng)

POENG

## Samlet antall poeng

A + B + C + D:

POENG

# Konsepter

1

—

2

POENG

Du kan velge mellom konsept 1 - 6

3

—

4

POENG

Du kan velge mellom konsept 2 - 6

5

—

6

POENG

Du kan velge mellom konsept 3 - 6

7

—

10

POENG

Du kan velge mellom konsept 5 - 6

## Konsept 1

- Du skal ikke gjøre noe, med mindre du blir oppmerksom på at det er noe galt hos databehandleren

## Konsept 2

- Databehandler bekrefter - helst skriftlig - overfor deg at alle krav i databehandleravtalen fortsatt overholdes

## Konsept 3

- Databehandleren gir deg årlig - enten direkte eller via sin nettside - en skriftlig status på forhold som omfattes av databehandleravtalen og andre relevante områder (f.eks. organisasjons- eller produktendringer)

## Konsept 4

- Databehandleren har en relevant og oppdatert sertifisering eller følger en såkalt atferdskodeks som er relevant for din behandlingsvirksomhet

## Konsept 5

- En uavhengig tredjepart har gjennomført en dokumentert tilsyn med databehandleren i et område som også dekker dine behandlingsaktiviteter

## Konsept 6

- Du selv - eller sammen med andre - gjennomfører et dokumentert tilsyn med databehandleren

# Hva gjør du? — Konkretisering

- Spørreskjemaer og undersøkelser tilpasses egen virksomhet
- Sertifiseringer
  - Kun et øyeblikksbilde
- Revisjonsrapporter/Sertifisering?
  - ISAE 3402
  - Type 1 eller type 2?
  - ISO sertifisering?
- Frekvens?
  - Avhengig av type/kategorisering
  - Tilpasses risikoprofil og virksomhet

## Konsept 1

- Du skal ikke gjøre noe, med mindre du blir oppmerksom på at det er noe galt hos databehandleren

## Konsept 2

- Databehandler bekrefter - helst skriftlig - overfor deg at alle krav i databehandleravtalen fortsatt overholdes

## Konsept 3

- Databehandleren gir deg årlig - enten direkte eller via sin nettside - en skriftlig status på forhold som omfattes av databehandleravtalen og andre relevante områder (f.eks. organisasjons- eller produktendringer)

## Konsept 4

- Databehandleren har en relevant og oppdatert sertifisering eller følger en såkalt atferdskodeks som er relevant for din behandlingsvirksomhet

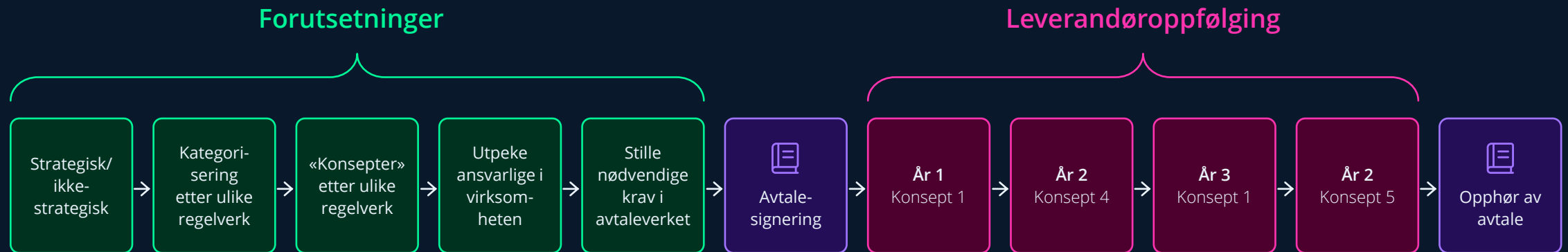
## Konsept 5

- En uavhengig tredjepart har gjennomført en dokumentert tilsyn med databehandleren i et område som også dekker dine behandlingsaktiviteter

## Konsept 6

- Du selv - eller sammen med andre - gjennomfører et dokumentert tilsyn med databehandleren

# Leverandøroppfølging





# Audit assurance and transparency

## ISAE 3402 Type II Audit Report

Rapporten uttaler seg om Intilitys informasjonssikkerhetstiltak

Rapporten gir revisjonssikkerhet for at Intilitys informasjonssikkerhetskontroller har fungert gjennom hele revisjonsperioden på 1 år



## ISAE 3000 Type II Audit Report

Kontroller og aktiviteter knyttet til Intilitys rolle som databehandler.

Rapporten gir revisjonssikkerhet for at Intility ivaretar sine plikter som databehandler etter GDPR



## ISO 27001 sertifisering

Sertifiseringen dekker alle tjenesteleveranser fra Intility, og gir revisjonssikkerhet for at et styresystem for informasjonssikkerhet er implementert ihht ISO kravene i standarden





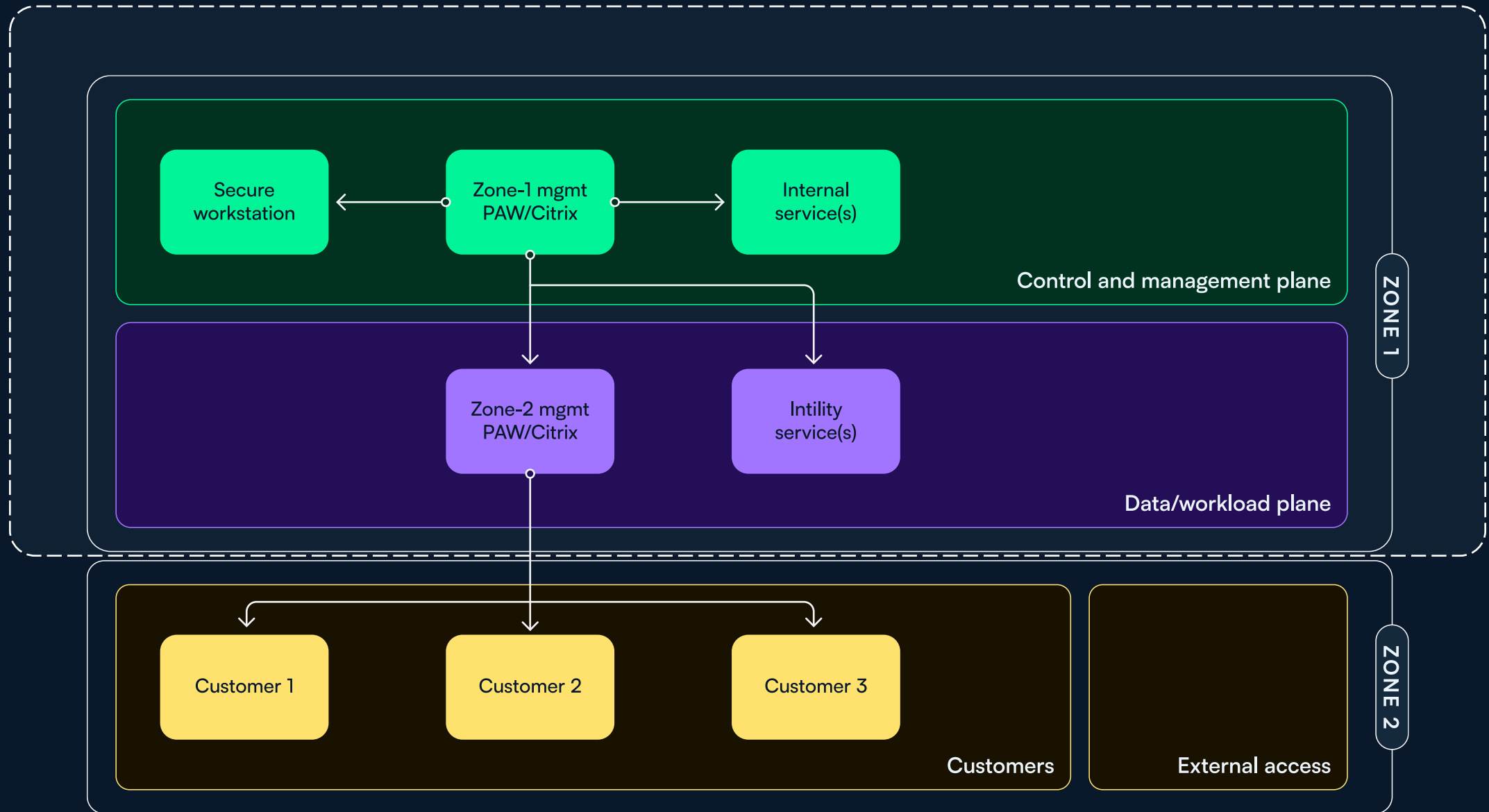
# CrowdStrike Falcon

## Endpoint Detection & Response

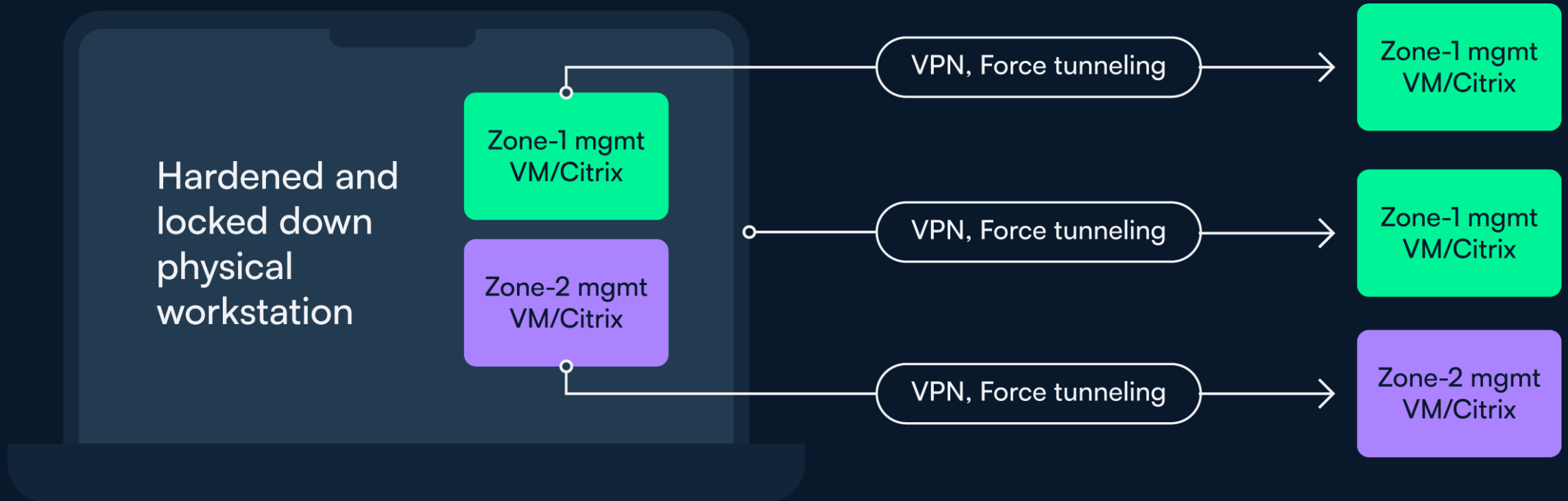
Avansert deteksjon av mulige angrep på alle endepunkter

Verktøy for å respondere hurtig på endepunktet fra et sentralisert grensesnitt

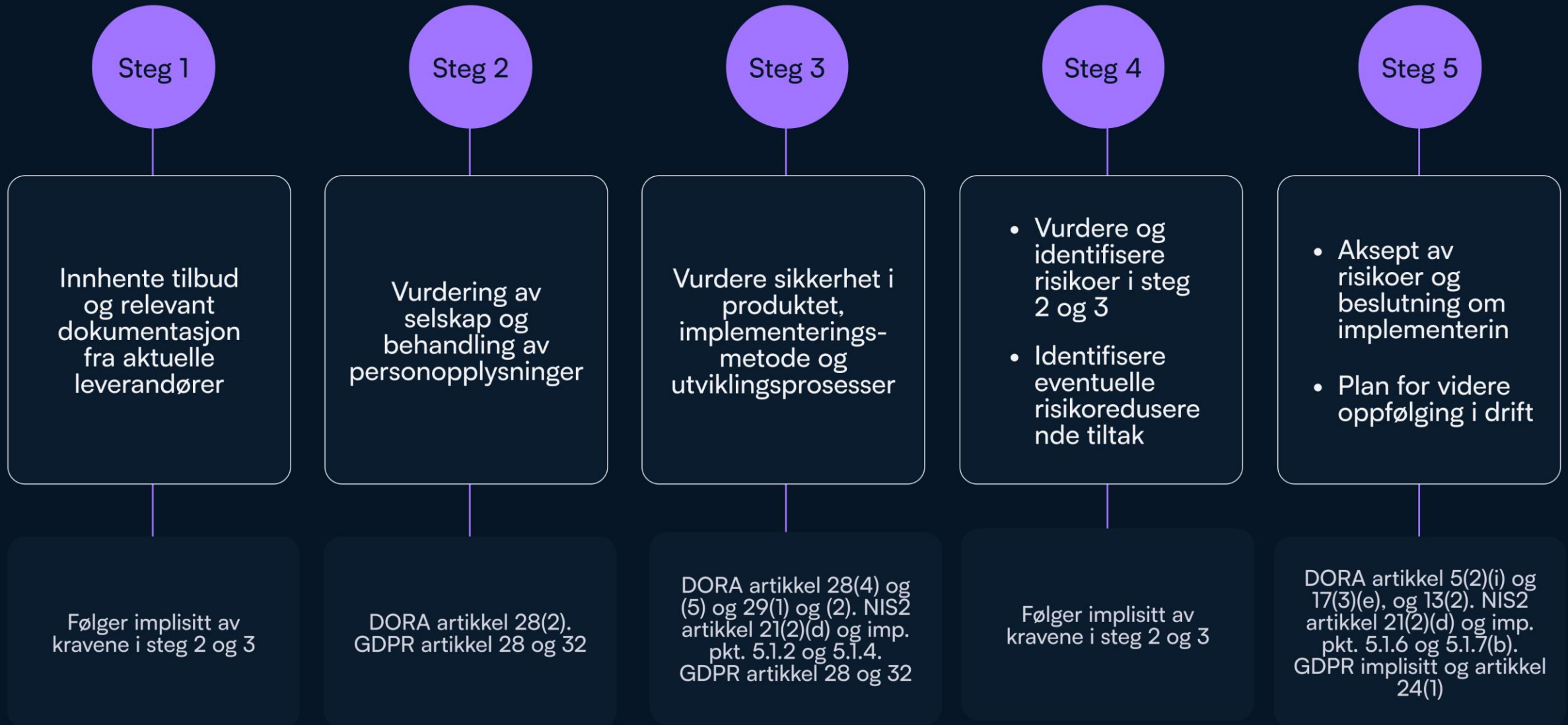




# Secure Admin Workstations



# Risiko og leverandørvurderingsprosess



# Risiko og leverandørvurderingsprosess

Steg 1

SOC 2 rapportert  
SOA for ISO 27001  
sertifisering,  
privacy-  
dokumentasjon mv.

Steg 2

Privacy-package  
1-GDPR  
Privacy Transfer  
Fact Sheet

Steg 3

Kartlegge kontroll  
knyttet til sikkerhet  
og utvikling i SOC  
2 rapporter og ISO  
— sertifisering  
Møter med  
sikkerhets og  
løsningsarkitekter  
Review av  
løsningsarkitektur

Steg 4

Overføring og  
behandling av  
data — begrenset  
til EU og kryptert  
Tilgangskontroll  
og sikkerhet —  
gode rutiner  
Endringer i  
konfigurasjon for  
avinnstallering og  
utrulling av  
oppdateringer for  
agentent

Steg 5

Overføring og  
behandling av  
data — begrenset  
til EU og kryptert  
Tilgangskontroll  
og sikkerhet —  
gode rutiner  
Endringer i  
konfigurasjon for  
avinnstallering og  
utrulling av  
oppdateringer for  
agentent

# Crowdstrike — Identifisere risikoer og implementerte tiltak

Utrulling av  
oppdateringer

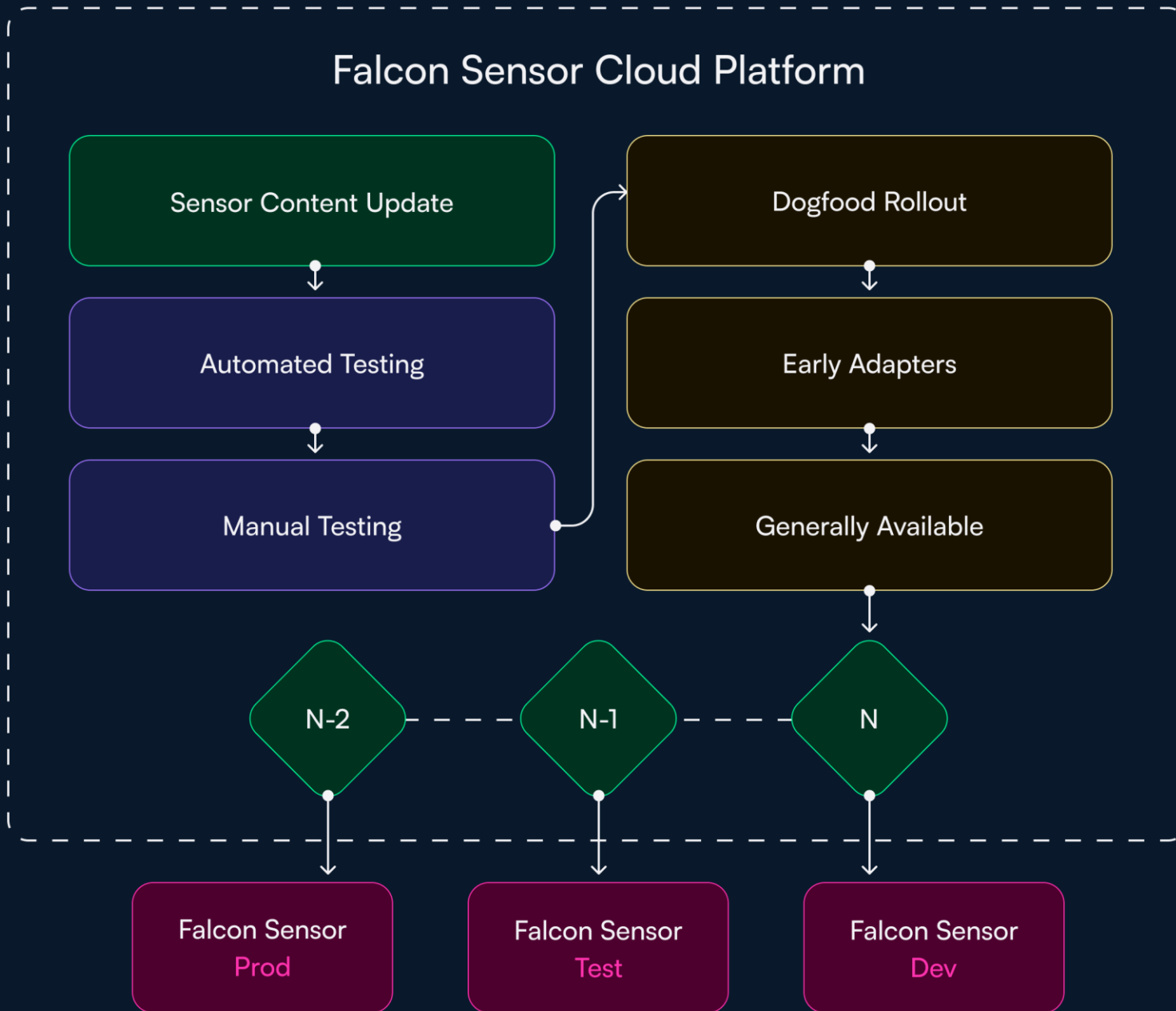
Adgang til avinstallasjon  
ved feilhendelser

Risikovurdert i henhold  
til våre rutiner

Dataprosessering og lagring  
i EU — all data er kryptert

An aerial, high-angle view of a dense urban landscape, likely New York City, showing a variety of skyscrapers and mid-rise buildings. The image is heavily stylized with a dark blue, almost black, color palette and a grainy, textured appearance. The text "CrowdStrike — Hva gikk galt?" is centered in the middle of the image.

CrowdStrike — Hva gikk galt?

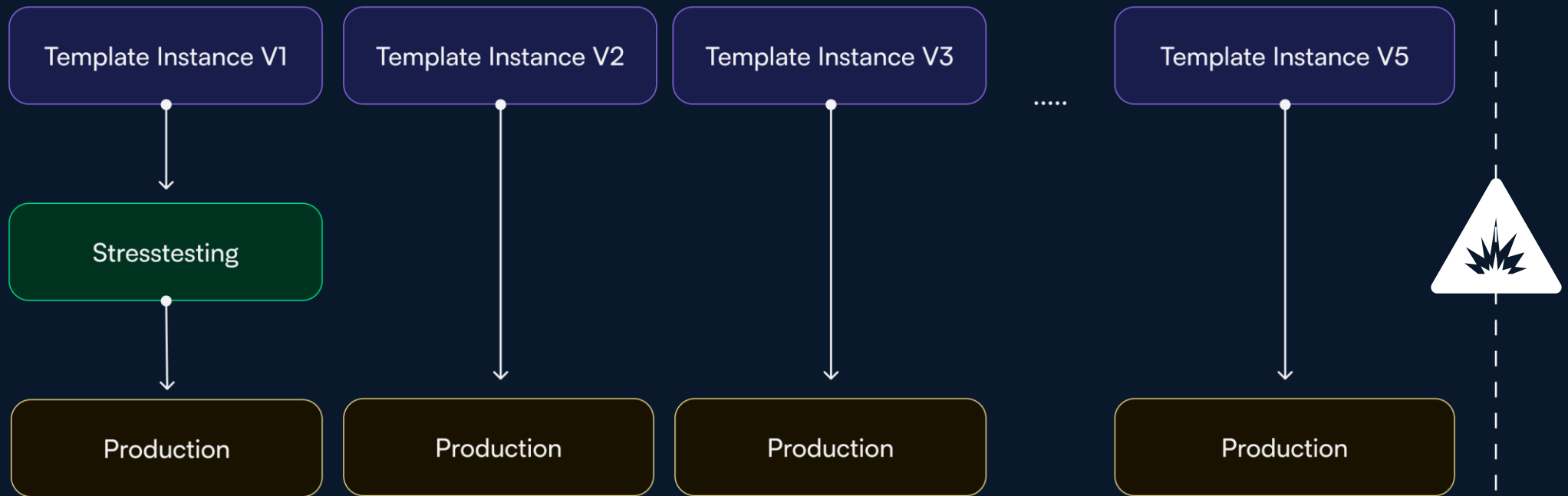


→ Holde tilbake versjonsoppdatering

→ Gradvis utrulling/oppdatering

→ Avinstallere sensor på endepunktet

## Rapid Response Content Deployment Proses





# Crowdstrike

## Hva er gjort?

Flere tester knyttet  
til konfigurasjon

Test av alle  
innholdsoppdateringer

Gradvis utrulling og  
tilgjengeliggjøring av  
innholdsoppdateringer

Intility får kontroll over utrulling  
av innholdsoppdateringer

# Takk for meg!



**Daniel Henriksen**

Vice President,  
Security Management

[daniel.henriksen@intility.no](mailto:daniel.henriksen@intility.no)