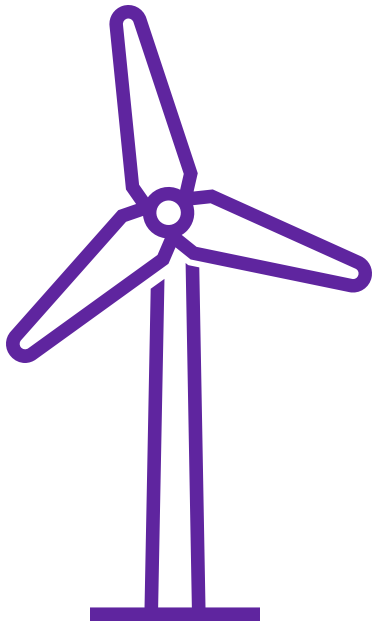
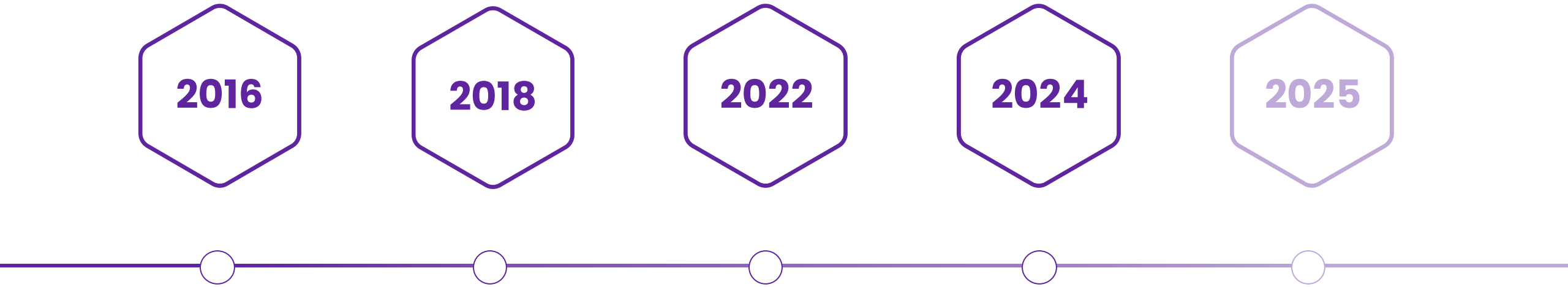


NIS2

VAD ÄR NIS?

EN GEMENSAM GRUNDFÖRSTÅELSE



NIS

Europaparlamentet och rådet antar direktivet för en hög gemensam nivå på säkerhet i nätverks- och informations-system

SVENSK LAG

NIS blir en svensk lag (2018:1174)

NIS 2

NIS upplevdes tandlöst. NIS2 antogs 14 dec 2022 och omfattar fler sektorer, hårdare krav och man inför tuffare påföljder.

TILLÄMPANDE

NIS2-direktivet börjar tillämpas i alla medlemsstater den 18 okt 2024

SVENSK LAG

”Cybersäkerhetslagen” föreslås börja tillämpas senare under 2025.

itm8

DEFINITIONER

OMFATTAS

En verkamhet som faller direkt under de stadgade kategorierna och kriterierna.

PÅVERKAS

En verkamhet påverkas indirekt genom exempelvis affärsmässiga krav.

VIKTIGA ENTITETER

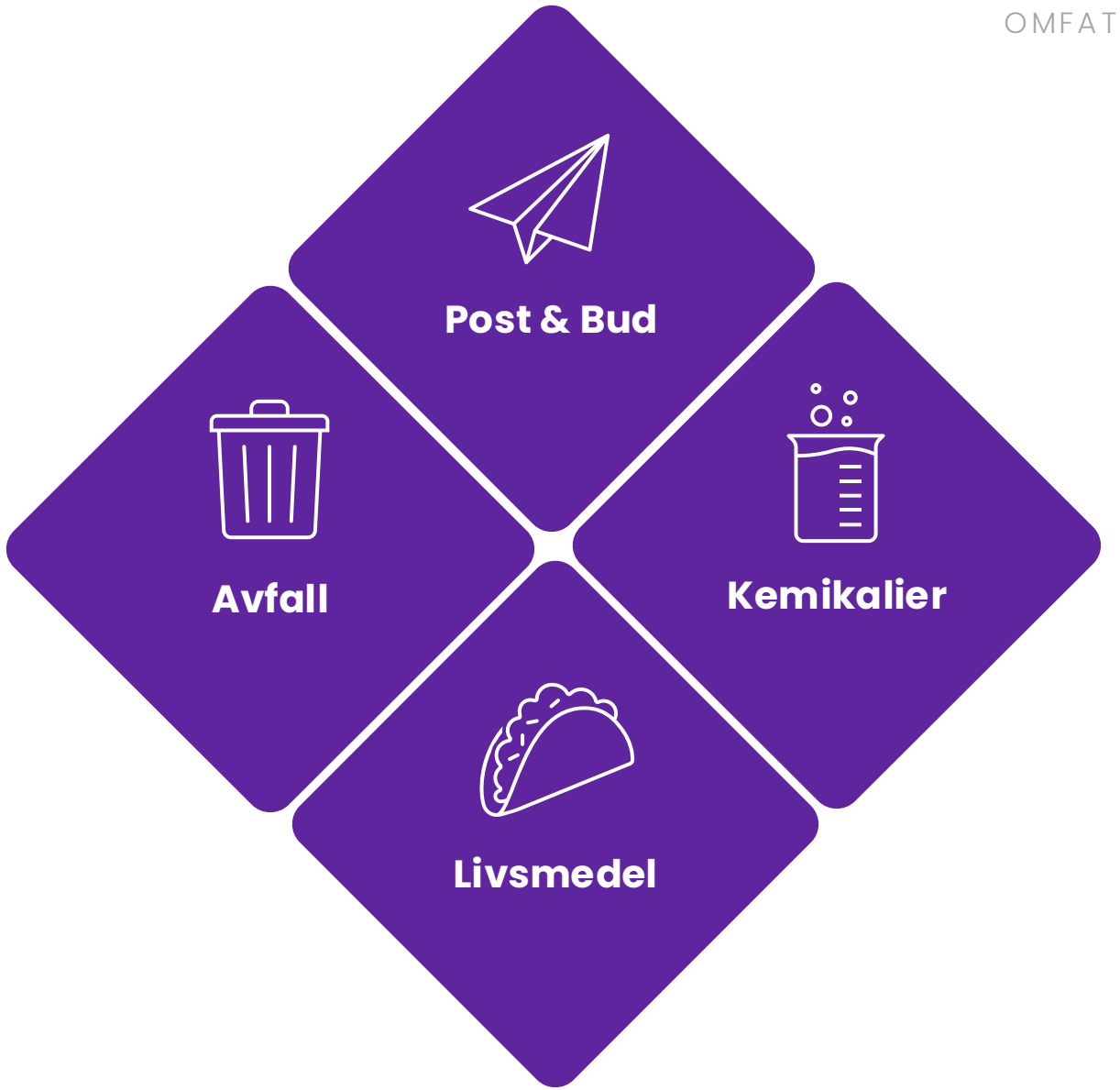
1. Lägre ekonomiska påföljder
2. Föremål för reaktiv tillsyn.

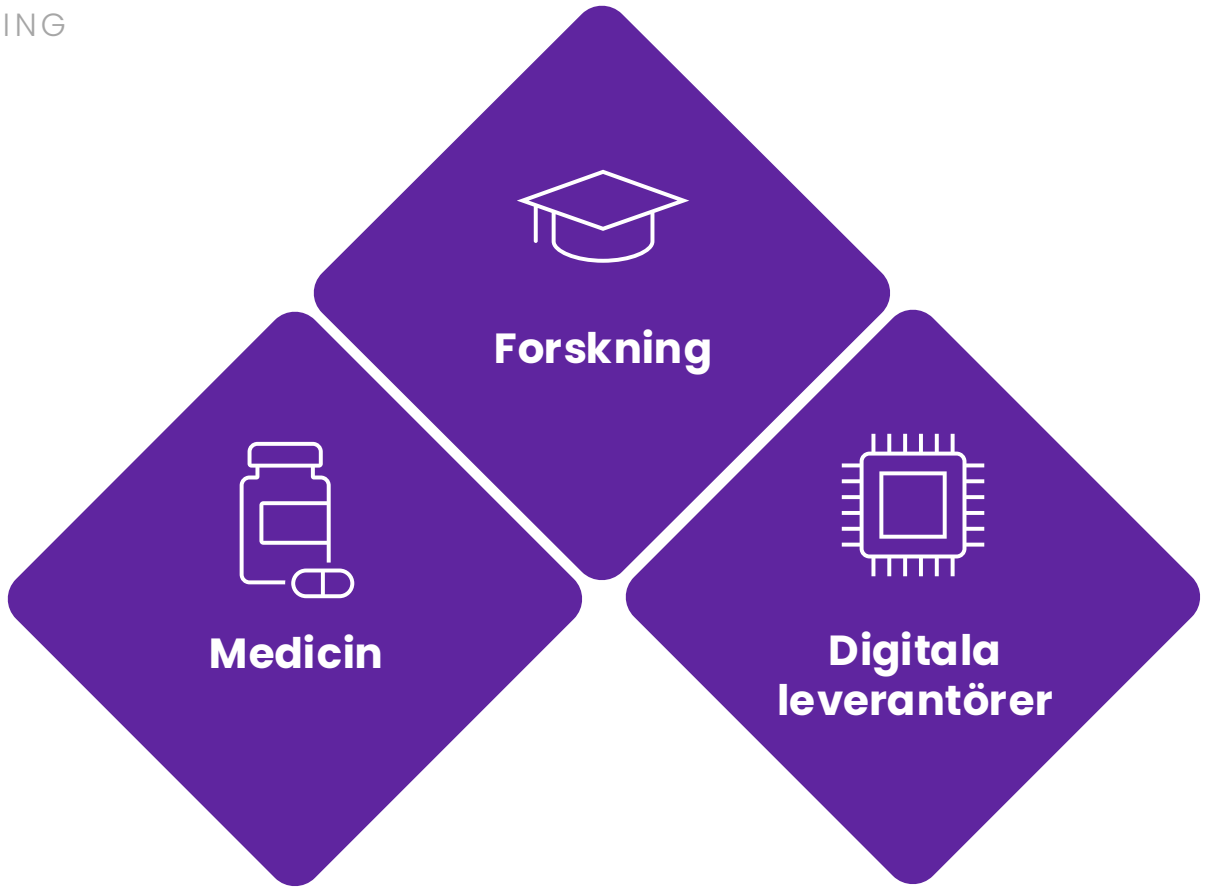
VÄSENTLIGA ENTITETER

1. Högre ekonomiska påföljder
2. Föremål för proaktiv tillsyn.

VIKTIGA ENTITETER

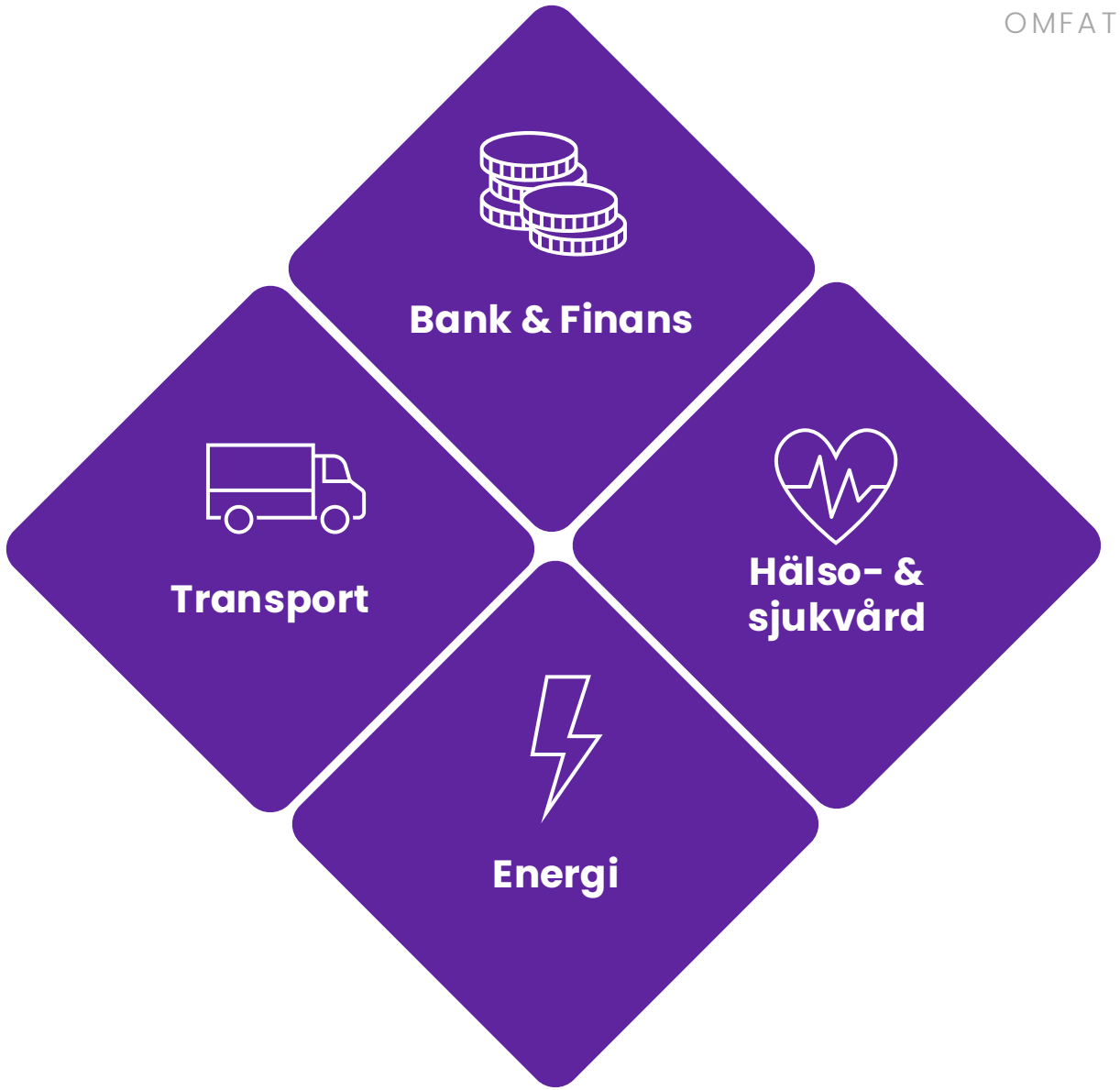
OMFATTNING

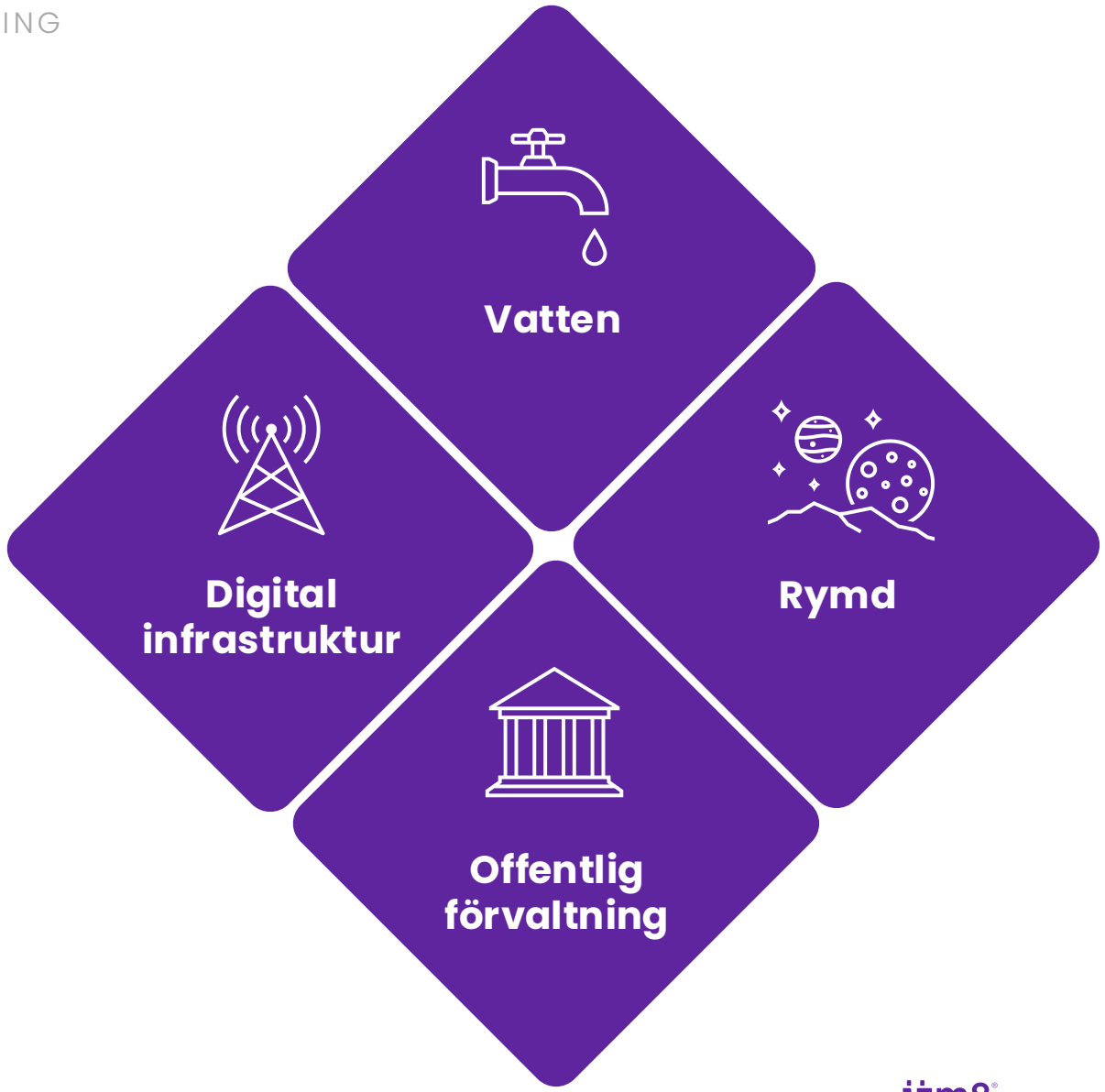




VÄSENTLIGA ENTITETER

OMFATTNING





itm8

VAD ÄR SKILLNADEN MOT NIS1?

1

Utökad omfattning

Fler sektorer omfattas nu. Under NIS1 fanns fokus på ett färre antal kritiska sektorer (ex. energi, transport m.m.). Med NIS2 täcks även verksamheter inom t.ex. avfallshantering, rymd, livsmedel, digital infrastruktur och mer.

2

Krav och sanktioner

Myndigheter får större befogenheter att utkräva ansvar. Företagsledningar kan hållas ansvariga och sanktionerna är kännbara.

3

Styrning och ansvar

Det räcker inte bara att ha en IT-avdelning som ”fixar säkerheten”. Ledningen måste aktivt äga frågan och visa att man investerar rätt resurser.

4

Rapporteringskrav

Incidenter ska rapporteras snabbare och mer detaljerat än tidigare.

SÅ DET PÅVERKAR OT MENAR DU?

1

Incidentrapportering

OT-operatörer måste ha tydliga processer för hur man rapporterar cyberincidenter. Detta innebär mer dokumentation och tydligare rutiner.

2

Samverkan

NIS2 uppmuntrar samarbete mellan olika aktörer och myndigheter. I en OT-miljö kan det innebära samverkan mellan drift, IT, säkerhetsteam och externa partners.

3

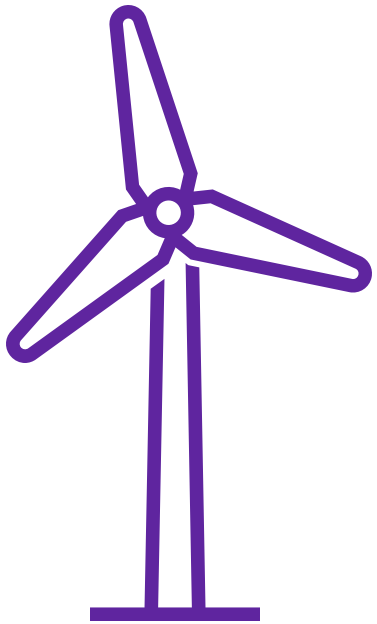
Riskhantering

Ledningsnivån måste förstå att OT inte är isolerat från IT-hot. Segmentering, uppdateringar och kontinuerlig övervakning blir kritiska.

4

Affärs- och säkerhetsrisk

Under NIS2 är det inte bara ett tekniskt problem. Om en produktion står still eller en samhällsfunktion slås ut, kan det bli fråga om stora ekonomiska och juridiska konsekvenser och tom risk för fara för liv.



OT

VARFÖR ÄR OT-SÄKERHET VIKTIGT?

1. Fysiska konsekvenser

Inom OT är riskerna ofta påtagliga för människor, utrustning och miljö. En felaktigt konfigurerad robotarm kan skada medarbetare eller förstöra maskiner. I en kemisk processindustri kan felaktiga inställningar leda till allvarliga utsläpp eller till och med explosioner.

2. Tillgänglighet och kontroll

Även små störningar kan stoppa produktionen eller äventyra säkerheten. Därför är fokus ofta på att systemet ska fungera och styras korrekt, snarare än att informationen i sig ska hållas hemlig (vilket ofta är prioritet i IT-säkerhet).

IT vs. OT

Gränsen mellan IT och OT är inte alltid helt tydlig. Inom exempelvis läkemedelsindustrin eller avancerad tillverkning kan man hantera både känslig information (IT-perspektiv) och kritisk processkontroll (OT-perspektiv) i samma system. Där uppstår ibland konflikt mellan kraven på dataskydd (t.ex. kryptering, åtkomstkontroller) och behovet av kontinuerlig drift och snabb åtkomst till styrsystemen.

Exempel

Om vi behöver patcha ett SCADA-system med en säkerhetsuppdatering, men det kräver omstart av en produktionslina – hur balanserar vi risken för ett eventuellt intrång mot risken för kostsam nedtid i verksamheten?

ANDRA TYPER AV RISKANALYSER

Inom traditionell IT-säkerhet brukar man resonera kring ”C-I-A” (Confidentiality, Integrity, Availability) – hemlighet, riktighet och tillgänglighet. Det är tre viktiga perspektiv, men i en OT-miljö kan man behöva titta på helt andra parametrar, som t.ex.:

S-R-P

Safety, *Resilience*, *Performance* – här handlar det om att ingen ska skadas, att processen tål störningar och att produktionen är effektiv.

C-O-O

Controlability, *Observability*, *Operability* – hur väl vi kan styra processen, övervaka den och påverka den i realtid.

VARFÖR SÄKERHET ÄR HÖGAKTUELLT INOM NIS2

NIS2 handlar inte bara om informationsläckor, utan lika mycket om avbrott i kritiska tjänster. För många OT-miljöer – som energiförsörjning, transport, vatten/avlopp eller tillverkningsindustri – kan ett angrepp orsaka samhällsstörningar och fysiska skador. Därför hamnar OT-frågor i skarpt fokus, och organisationer förväntas:

Ha koll på sina system och risker

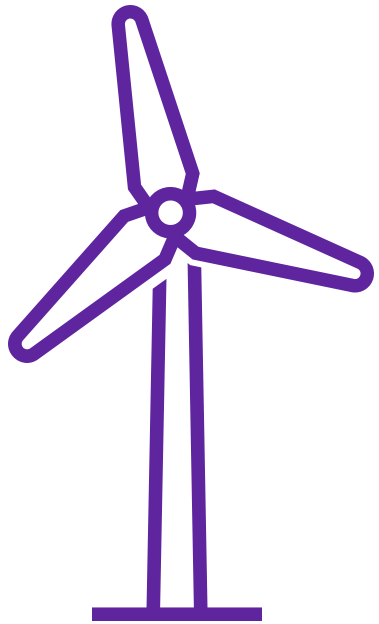
genomföra riskanalyser som täcker både IT- och OT-perspektiv.

Implementera rätt tekniska och organisatoriska åtgärder

t.ex. nätverkssegmentering, säkra uppdateringsrutiner och robusta nödlösningar.

Ha en incidenthanteringsplan anpassad för OT

inklusive processer för snabb rapportering till ansvariga myndigheter.



INCIDENTHANTERING

INCIDENTHANTERING

1. Identifiera problemet snabbt

Du märker ovanlig aktivitet i SCADA-systemet klockan 03.00 en fredagsnatt. Under NIS2 krävs att du inte väntar tills måndag morgon. Du måste direkt aktivera er incidenthanteringsplan.

Det krävs 24/7-övervakning – antingen med automatiska larm eller en SOC-tjänst som håller koll. Personalen måste veta vilken kontaktlista som gäller, och vem som beslutar om produktionen ska stoppas.

INCIDENTHANTERING

2. Inhämta data för rapport

När en misstänkt incident sker kan du behöva samla loggfiler från brandväggar, SCADA-system, operatörspaneler och även eventuella videoövervakningar.

Ni behöver tydliga rutiner för hur dessa loggar samlas in, struktureras och förvaras. Om de är utspridda i olika system blir det svårt att snabbt lämna en formell rapport. NIS2 kräver att rapporteringen görs inom en snäv tidsram, så du måste kunna agera fort.

INCIDENTHANTERING

3. Åtgärda problemet

Vid en pågående attack kan ni bli tvungna att ta ned en del av produktionslinan. Under NIS2 är det viktigt att kunna visa att ni inte bara rapporterat incidenten, utan också aktivt minimerat skadan.

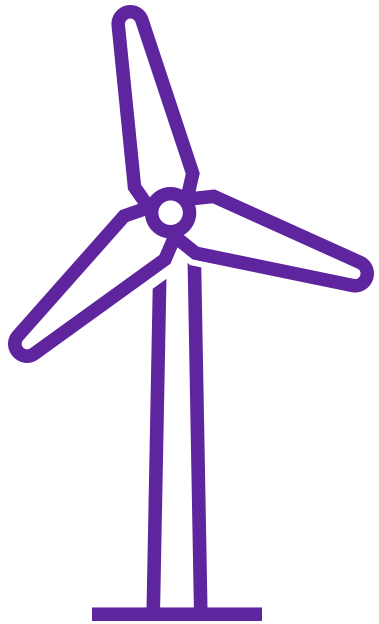
Personalen måste veta hur man säkert stänger av eller isolerar en maskin utan att orsaka farliga situationer eller större produktionsbortfall än nödvändigt. Samarbete med IT/SOC för att stoppa angriparen i nätverket, samtidigt som man upprätthåller säkerheten på golvet.

INCIDENTHANTERING

4. Efterrapportering och lärdomar

När incidenten är under kontroll kräver NIS2 att ni lämnar en mer detaljerad rapport om vad som hände, varför, och vad ni gör för att det inte ska upprepas.

1. Dokumentera incidentförloppet
2. Identifiera rotorsak (Root Cause Analysis)
3. Uppdatera policys och tekniska lösningar utifrån lärdomarna
4. Kommunicera eventuella förändringar till personal och leverantörer



FÖRBERED ER

FÖRBERED ER

1. Gör en GAP-analys

- Lista era kritiska system.
- Identifiera var ni brister i både teknik (t.ex. brist på loggning) och organisation (t.ex. otydliga mandat för incidenthantering).

FÖRBERED ER

2. Upprätta rutiner och roller

- Vem ansvarar för att stänga av utrustning vid ett hot?
- Vem kontaktar extern incidentresurs och vem gör den formella rapporten till myndighet?

FÖRBERED ER

3. Öva regelbundet

- Kör en table top-övning där ni spelar upp ett scenario: ”En angripare har fått in en skadlig kod i systemet. Vad gör ni första timmen? Hur rapporterar ni? Vem tar besluten?”

FÖRBERED ER

4. Säkerställ ledningsförankring

- Ledningen måste vara med på noterna. De behöver förstå att detta inte bara är ett IT-problem. Om du måste stänga ned produktionen i en timme för att hindra spridning av skadlig kod, måste ledningen backa upp det beslutet.

ROADMAP

Förberedelse

Gå igenom existerande dokumentation och krav.

Nuvarande status

Analysera hur företaget ligger till redan idag.

GAP

Identifiera de avvikelser från dagens status till krav och mål.

Risker

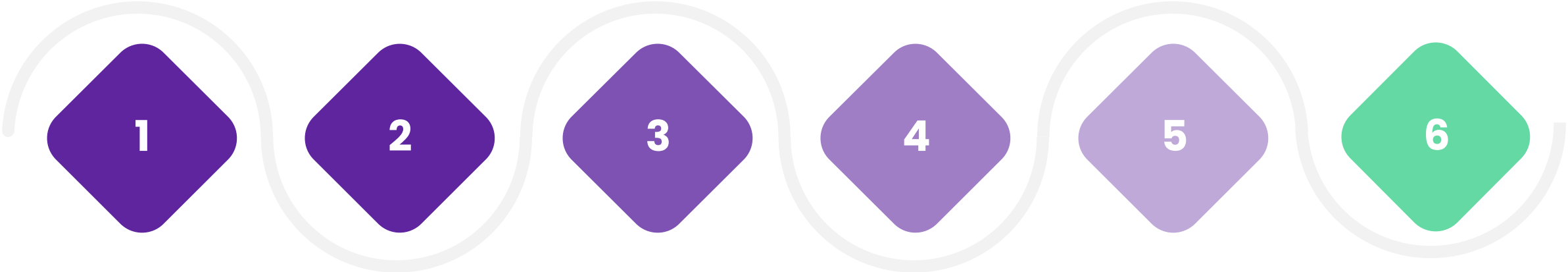
Bedöma och prioritera riskerna utifrån vad som är affärskritiskt.

Åtgärder

Rekommendationer och realistisk åtgärdsplan.

Resultat

Presentera resultat samt nästa steg i processen.



itm8

1

FÖRBEREDELSE OCH PLANERING

Vi skapar en tydlig struktur för analysen och säkerställa att alla krav från NIS2 adresseras. Målet är att identifiera relevanta NIS2-krav och samla nödvändig information om organisationens verksamhet.

MOMENT

- Kartläggning av krav
- Identifiering av omfattning
- Insamling av dokumentation

2

GRANSKNING AV NUVARANDE STATUS

Vi dokumenterar organisationens nuvarande säkerhetsåtgärder och styrprocesser. Målet är att få en tydlig bild av hur organisationen hanterar säkerhet i nuläget.

MOMENT

- Granskning av styrdokument
- Granskning av processer och rutiner
- Intervjuer med nyckelpersoner

3

GAP: IDENTIFIERA AVVIKELSER

Vi kartlägger skillnaderna mellan nuvarande status och de ställda kraven i NIS2. Målet är att dokumentera alla områden där organisationen inte uppfyller direktivets krav.

MOMENT

- Kartläggning mot krav
- Kategorisering av GAP:
    - Hög prioritet (kritiska brister)
    - Mellanprioritet (långsiktig påverkan)
    - Låg prioritet (kan åtgärdas på sikt)

4

RISKBEDÖMNINGAR

Med kunden bedömer vi riskerna som varje GAP innebär för organisationen. Målet är att prioritera åtgärder utifrån vad som är affärskritiskt och efterlevnad.

MOMENT

- Kvalificera risker
- Bedöma påverkan och sannolikhet

5

REKOMMENDATIONER & ÅTGÄRDSPLAN

Syftet är att ge tydliga och prioriterade rekommendationer för att åtgärda GAP:ar. Målet är att presentera en realistisk plan för att uppfylla direktivets krav på verksamheten.

MOMENT

- Specificera åtgärder
- Definiera tidsramar och ansvar

6

PRESENTATION AV RESULTAT

Vi hjälper er med att säkerställa att organisationen förstår avvikelserna samt vilka åtgärder som krävs för att åtgärda dessa samt varför.

MOMENT

- Sammanfatta GAP-analys
- Visualisera resultat
- Diskutera nästa steg