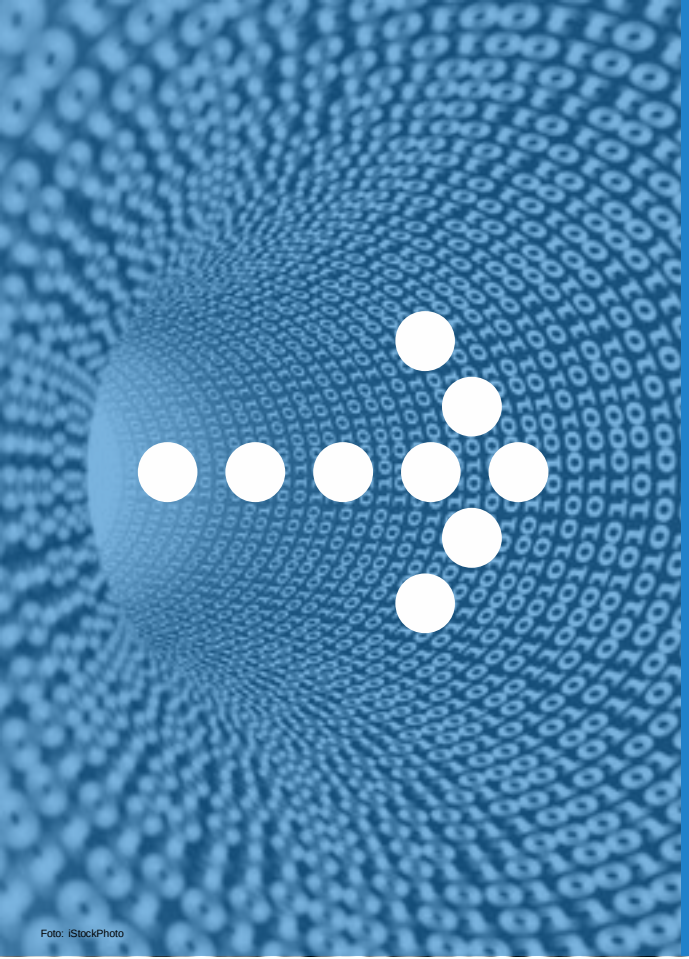


Foto: iStockPhoto

Pass 10:
Följ upp arbetet

Praktisk incidenthantering i industriella informations- och styrsystem

Myndigheten för samhällsskydd och beredskap

NCS3

FOI

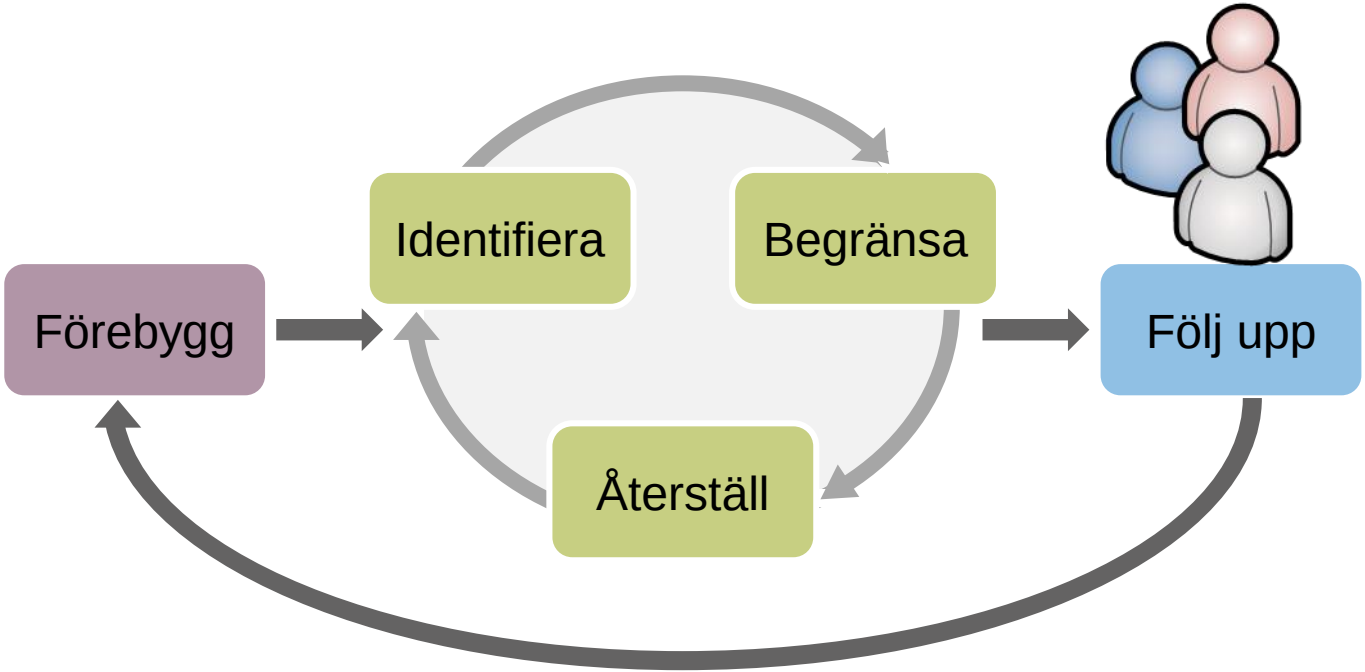
MSBFS 2018:8, 11 §

En leverantör ska ha interna regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser avseende informationshanteringen i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster.

Efter avslutad incidenthantering ska leverantören identifiera grundorsaker till att incidenter och avvikelser inträffat samt vidta åtgärder för att förhindra att liknande incidenter och avvikelser inträffar på nytt.

Arbetet ska dokumenteras.

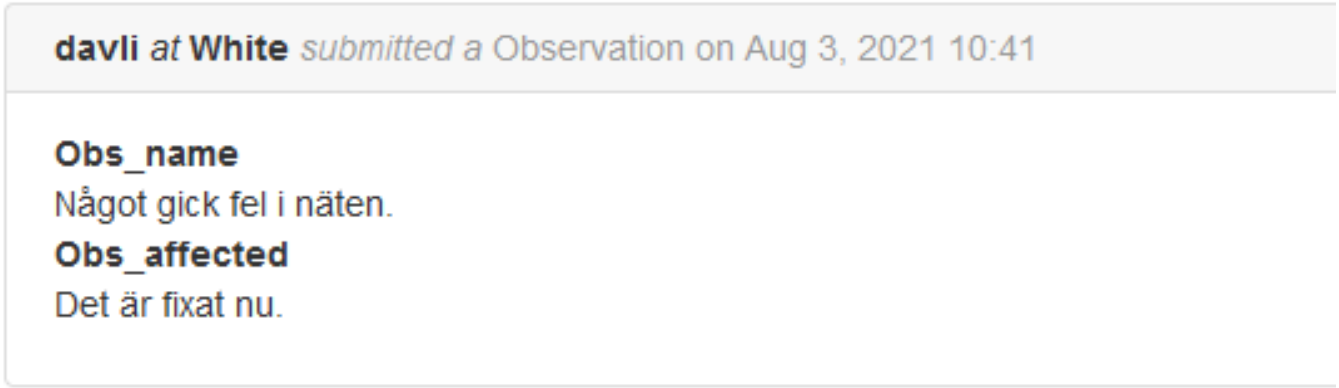
Incidenthanteringsprocessen



Varför organiserad uppföljning?

Bild från XKCD.com

Hur bör man dokumentera?



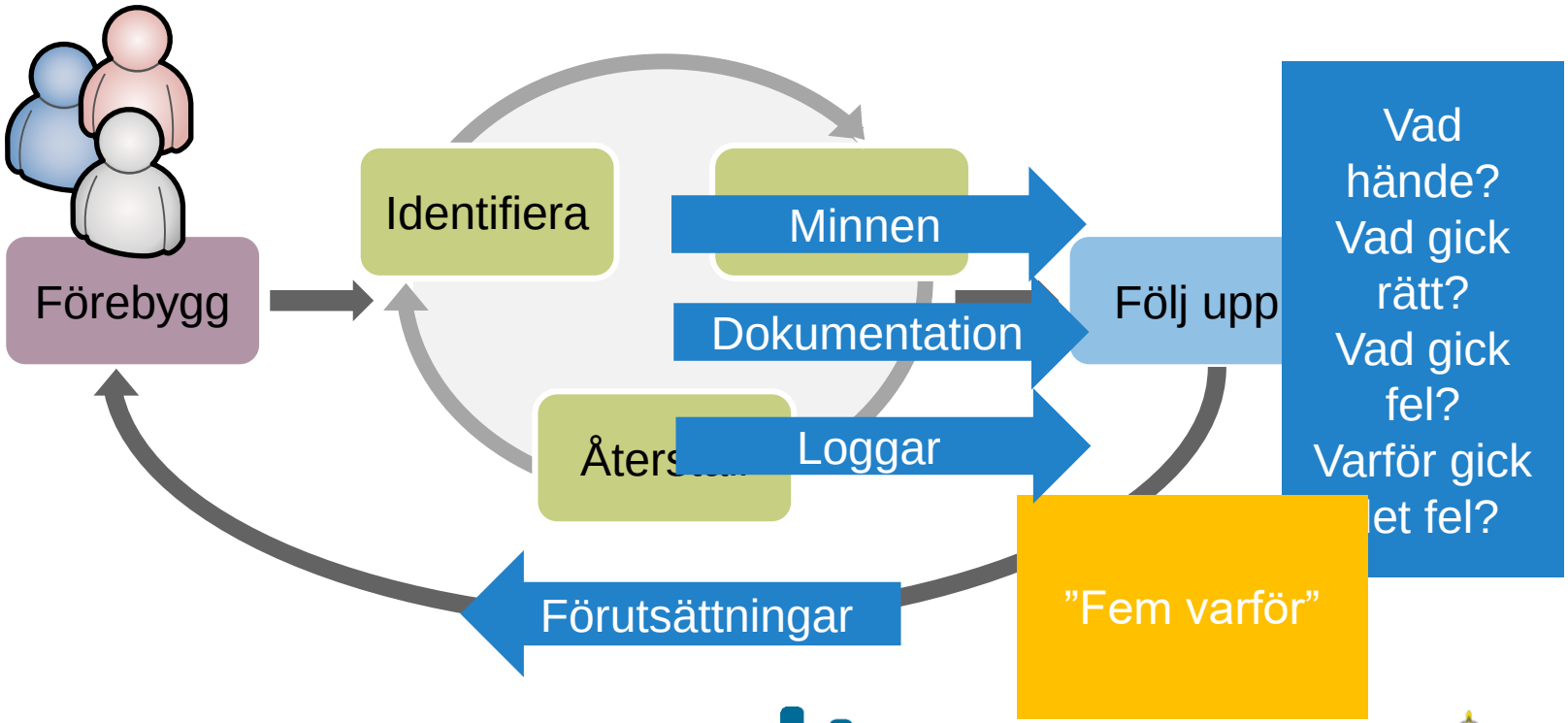
MSBFS 2018:8, 11 §

En leverantör ska ha interna regler och arbetssätt för att upptäcka och vidta åtgärder för att minimera konsekvenserna av incidenter och avvikelser avseende informationshanteringen i nätverk och informationssystem som används för att tillhandahålla samhällsviktiga tjänster.

Efter avslutad incidenthantering ska leverantören **identifiera grundorsaker till att incidenter och avvikelser inträffat samt vidta åtgärder för att förhindra att liknande incidenter och avvikelser inträffar på nytt.**

Arbetet ska dokumenteras.

Uppföljningen



Efterarbete

- Dokumentera händelseförlopp
- Bedöm incidentens omfattning
  - Hur påverkades verksamheten
- Identifiera lärdomar och erfarenheter
- Förbättra system, rutiner och arbetsmetoder
  - Enligt ordinarie rutiner
- Kommunicera ut lärdomar

Simulerade incidenter

- Använd praktiska exempel och gör dry-run incidenthantering
- Övning och simulering är sämre än riktiga incidenter, men bättre än överraskning.

Sammanfattning

- Uppföljning ska
  - Visa vad som hände
  - Visa VARFÖR det hände
  - Identifiera förutsättningar för att hindra att det hände igen

Övningarna

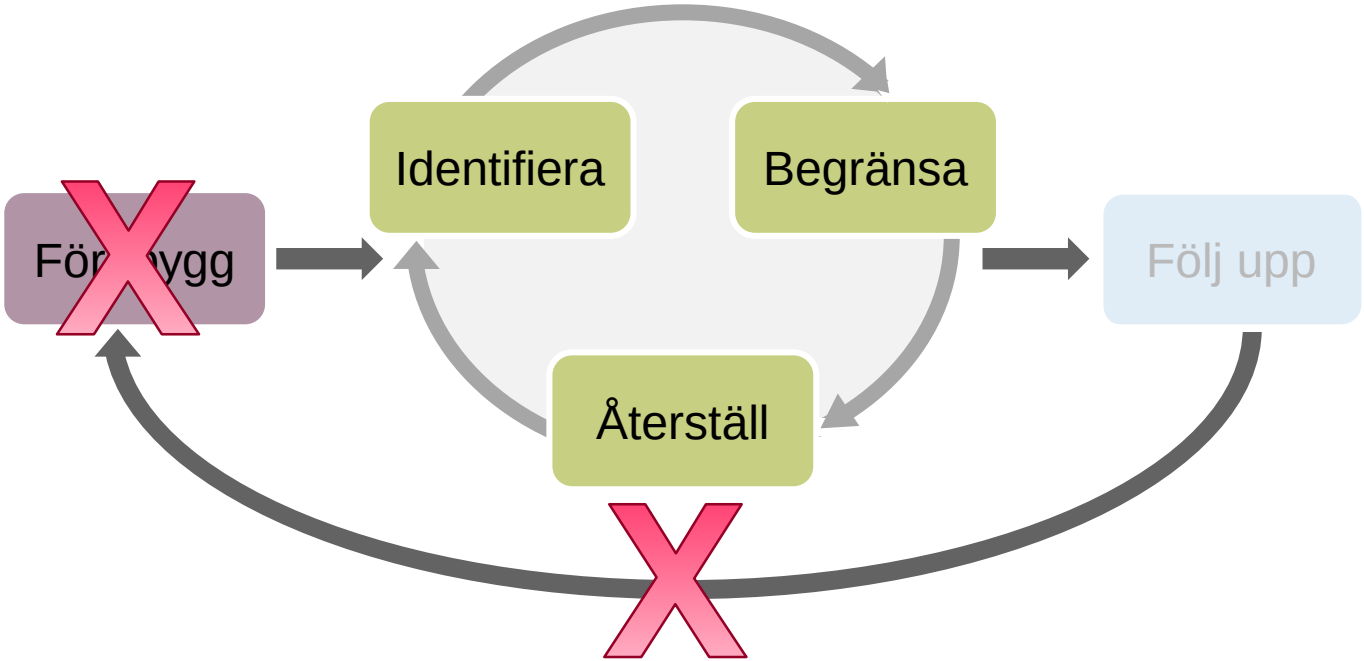
Övningsinformation

- Gäster från FA
  - Observerar övningsupplägget
  - Inte er

Övningarna – Övergripande info

- Övergripande scenario
  - Ni har nyligen fått en plats i Pharmentas incidenthanterings-team. Grattis!
- HANTERA INCIDENTERNA
  - Förbättra inte miljön utan anledning!
  - Ni får INTE aktivera lokal FW på klienterna!
- Håll produktionen igång!

Övningsinformation



Myndigheten för samhällsskydd och beredskap

NCS3

FOI

Instruktion – Hantera incidenterna

- Identifiera
  - Bevaka IGD, Dailymedicin, Mail, Chat och CEC
  - Analysera konsekvenser för produktion
  - Prioritera!
- Begränsa
  - Förhindra påverkan på prod
- Återställ
  - Enligt instruktioner som tillhandahålls

Dokumentationskrav i loopen

- ”Krigsdagbok”
  - Enligt lag[illegible]ård
- Incidenth[illegible]ingslogg
  - Dokumentera vad som sker
  - Primär bedömning från vår sida
  - Sker via ”Messages” i CEC

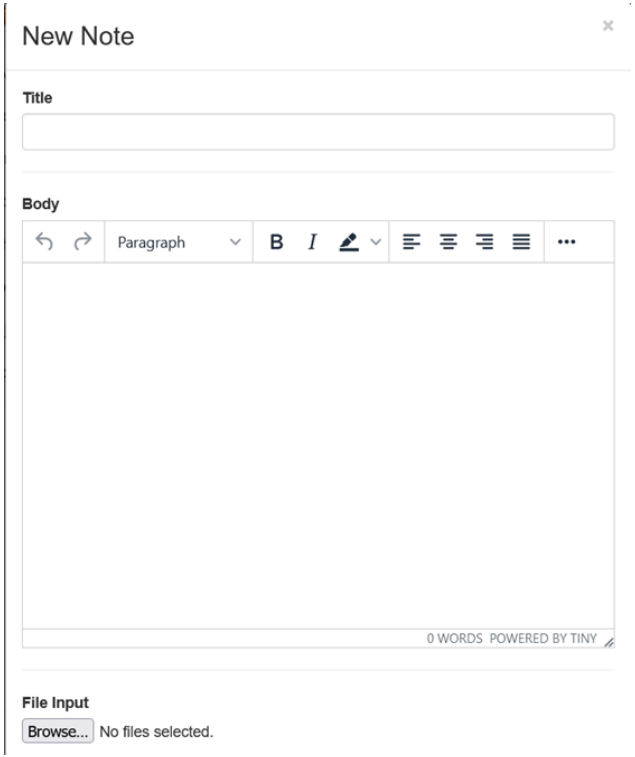
Vad ska dokumenteras?

Vem sköter denna?

Med vilka data?

Uppföljningsfasen (25 minuter)

- Dragning för ledningen
  - Fem minuter
    - Vad hände när? Vad vidtog ni för åtgärder?
    - Konsekvenser/möjliga konsekvenser?
    - Framtida åtgärder?
    - Görs i ”Notes”
- Egen utvärdering
    - Hur gick övningen?
    - Vad vill ni ändra på till nästa övning?
    - Också ”Notes”



Av övningstekniska skäl

- Svar på inspel ska läggas i CEC som ”Messages”
  - E-post, videomeddelanden, tfnsamtal -> Svar i ”Message”
  - Skriv mottagare och ärende i titeln.
  - Svaret i meddelanderutan.

Övningsmiljön

Övningar – praktiskt genomförande

- Arbeta genom CEC
  - Rapportering och meddelanden
  - Fjärrstyr Unicorp och Pharmenta via RDP
    - Använd HQIT01-04 samt Kali
    - Endast en användare per maskin
    - WT kommer att ansluta till HQIT05 och 06 samt på Weborder

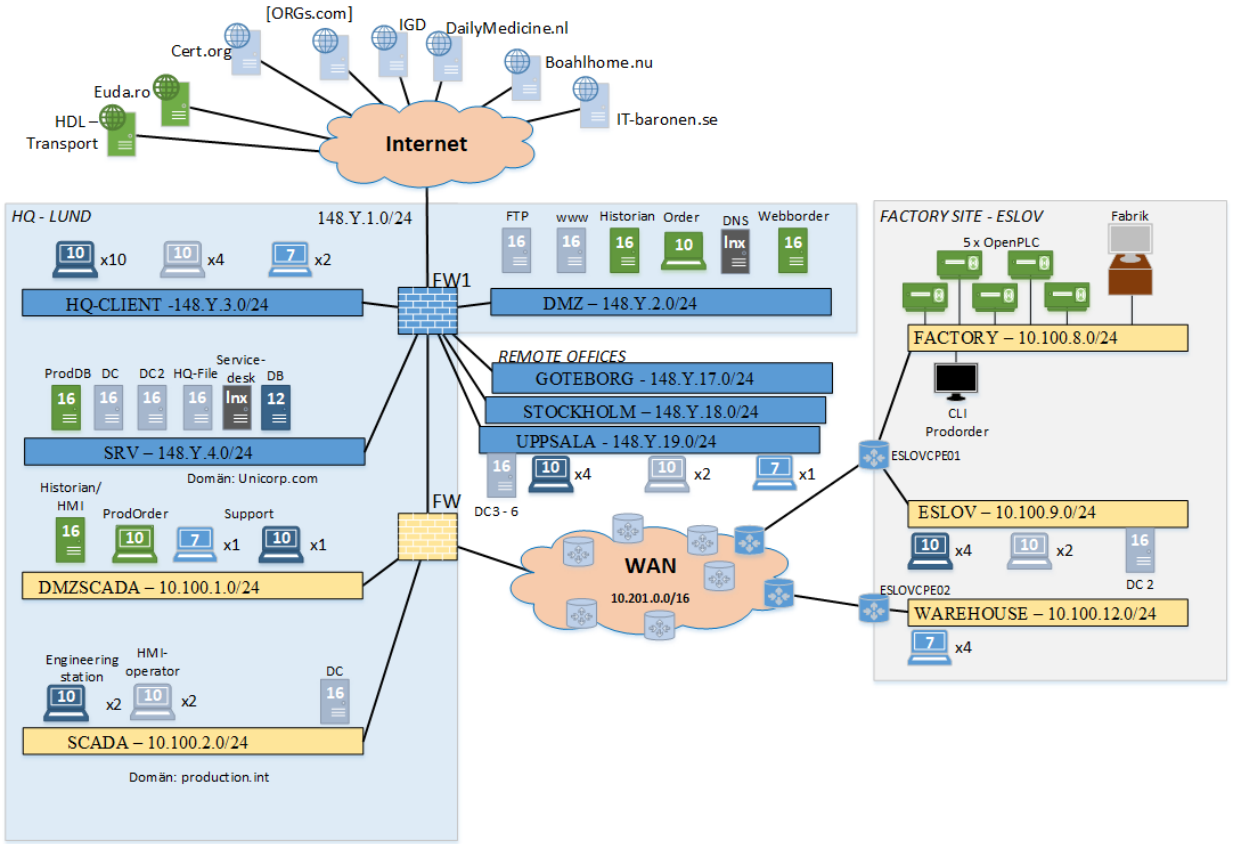
Övningar – Kontaktvägar

- Green och white team finns tillgängliga
  - Övningsledning/White team – via CEC
  - Support/Green Team – via CDXChat

Övningar – Bevakning

- Indata
  - Mail
  - IGD.se och Dailymedicine.nl
  - CDXChat (för samtal) samt reserv för mail
    - Endast från silvrig dator

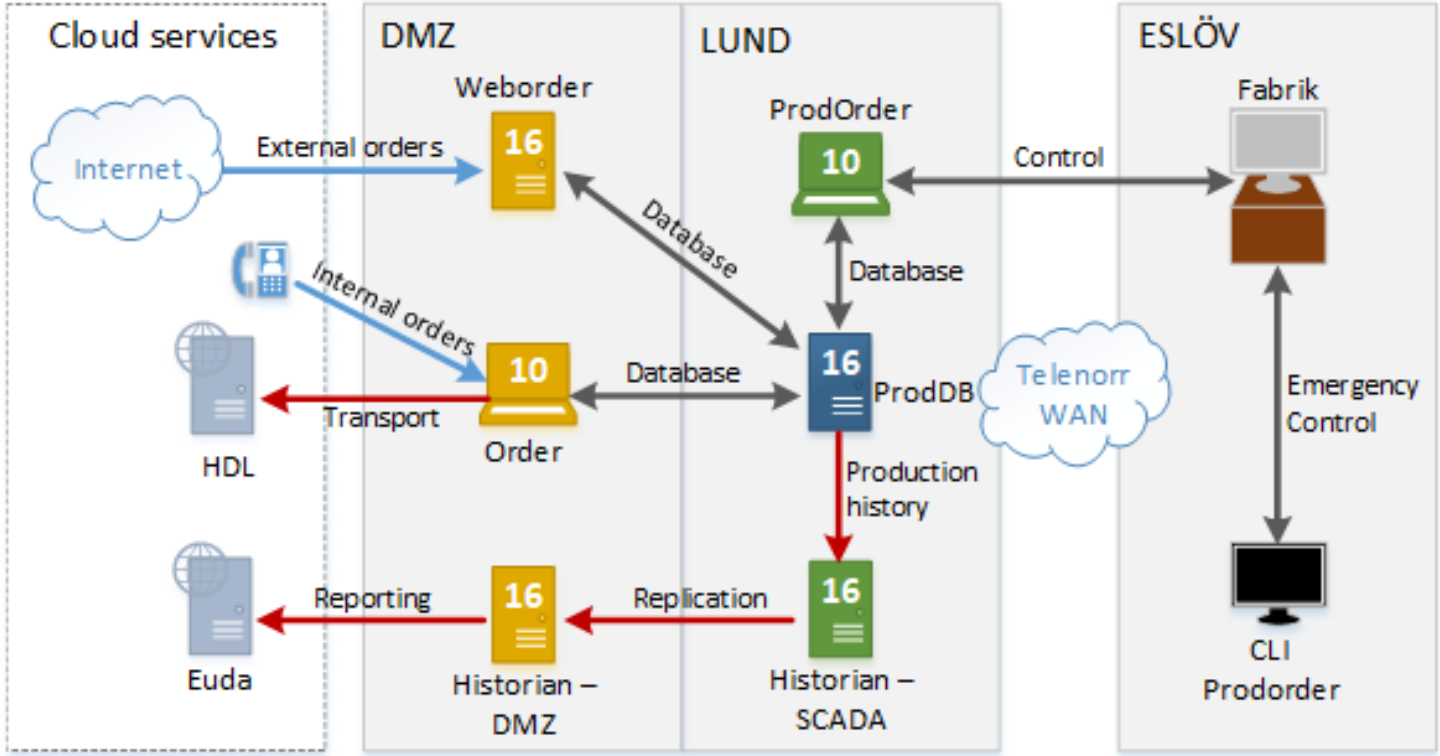
Övningsmiljön – Unicorp/Pharmenta



Myndigheten för samhällsskydd och beredskap

FOI

Produktionssystem



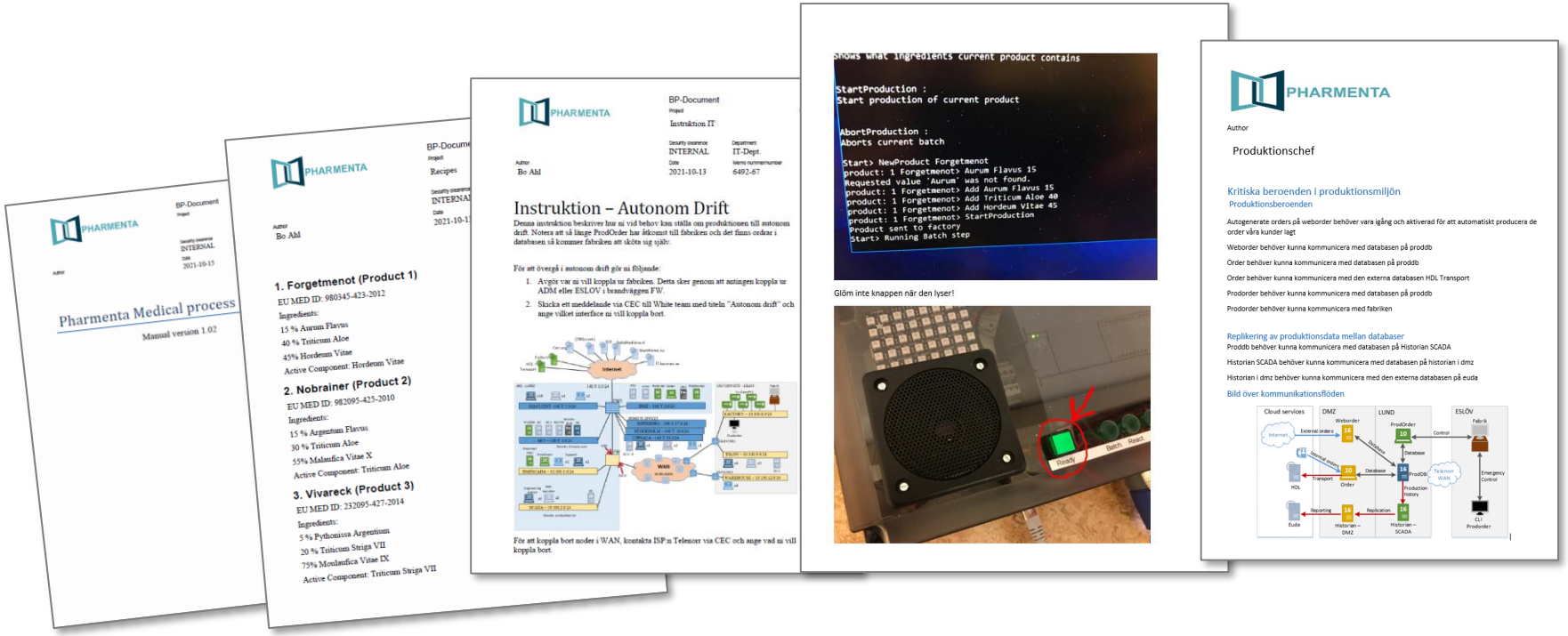
Autonom drift

För att övergå i autonom drift gör ni följande:

1. Avgör var ni vill koppla ur fabriken. Detta sker genom att antingen koppla ur ADM eller ESLOV i brandväggen FW.
2. Skicka ett meddelande via CEC till White team med titeln ”Autonom drift” och ange vilket interface ni vill koppla bort.

Denna instruktion beskriver hur ni vid behov kan ställa om produktionen till autonom drift. Notera att så länge ProdOrder har åtkomst till fabriken och det finns ordrar i databasen så kommer fabriken att sköta sig själv.

Driftdokumentation – Finns utskriven



Avgränsningar. Ni får ej:

- Aktivera lokal brandvägg på datorerna
- Använda HQIT05 eller 06
- Ta bort användaren FOIWhite i brandväggarna
- Ändra i miljön innan övningen börjat

Adresser – Fysisk plattform

- CEC
  - https://i4sv43.cec.crate.foi.se/
- Chat (via silvrig dator)
  - https://cdxchat.crate.foi.se/
- Inloggningar
  - UCXU1 till UCXU6 enligt utdelad lapp.

Adresser - Övningsmiljön

- Ingame Mail
  - Webmail.unicorpX.se
  - Inloggning Servicedesk, pwd: CorpService
- Snort
  - snart-fw1.unicorpX.se
  - snart-int.int.pharmentaX.se
  - Inloggning admin@unicorpX.se, pwd: rootroot
- Brandväggar
  - fw1.unicorpX.se
  - fw.int.pharmentaX.se
  - Inloggning admin, pwd: Random77