

Pass 10: Följ upp arbetet

Praktisk incidenthantering i industriella informations- och styrsystem

Foto: iStockPhoto

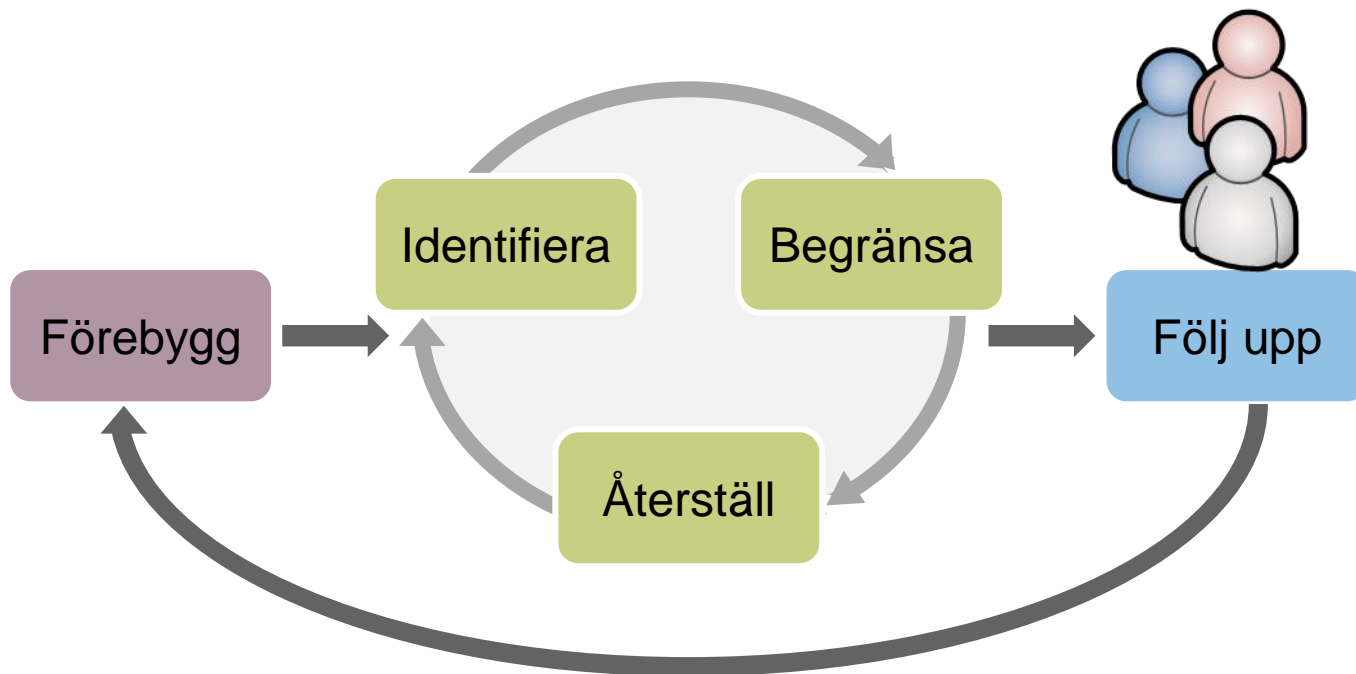
MSBFS 2018:8, 11 §

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?

	COMMENT	DATE
○	CREATED MAIN LOOP & TIMING CONTROL	14 HOURS AGO
○	ENABLED CONFIG FILE PARSING	9 HOURS AGO
○	MISC BUGFIXES	5 HOURS AGO
○	CODE ADDITIONS/EDITS	4 HOURS AGO
○	MORE CODE	4 HOURS AGO
○	HERE HAVE CODE	4 HOURS AGO
○	AAAAA	3 HOURS AGO
○	ADKFJSLKDFJSDKLFJ	3 HOURS AGO
○	MY HANDS ARE TYPING WORDS	2 HOURS AGO
○	HAAAAAAAAAANDS	2 HOURS AGO

AS A PROJECT DRAGS ON, MY GIT COMMIT MESSAGES GET LESS AND LESS INFORMATIVE.

Bild från XKCD.com

Hur bör man dokumentera?

davli at White *submitted a* Observation on Aug 3, 2021 10:41

Obs_name

Något gick fel i näten.

Obs_affected

Det är fixat nu.

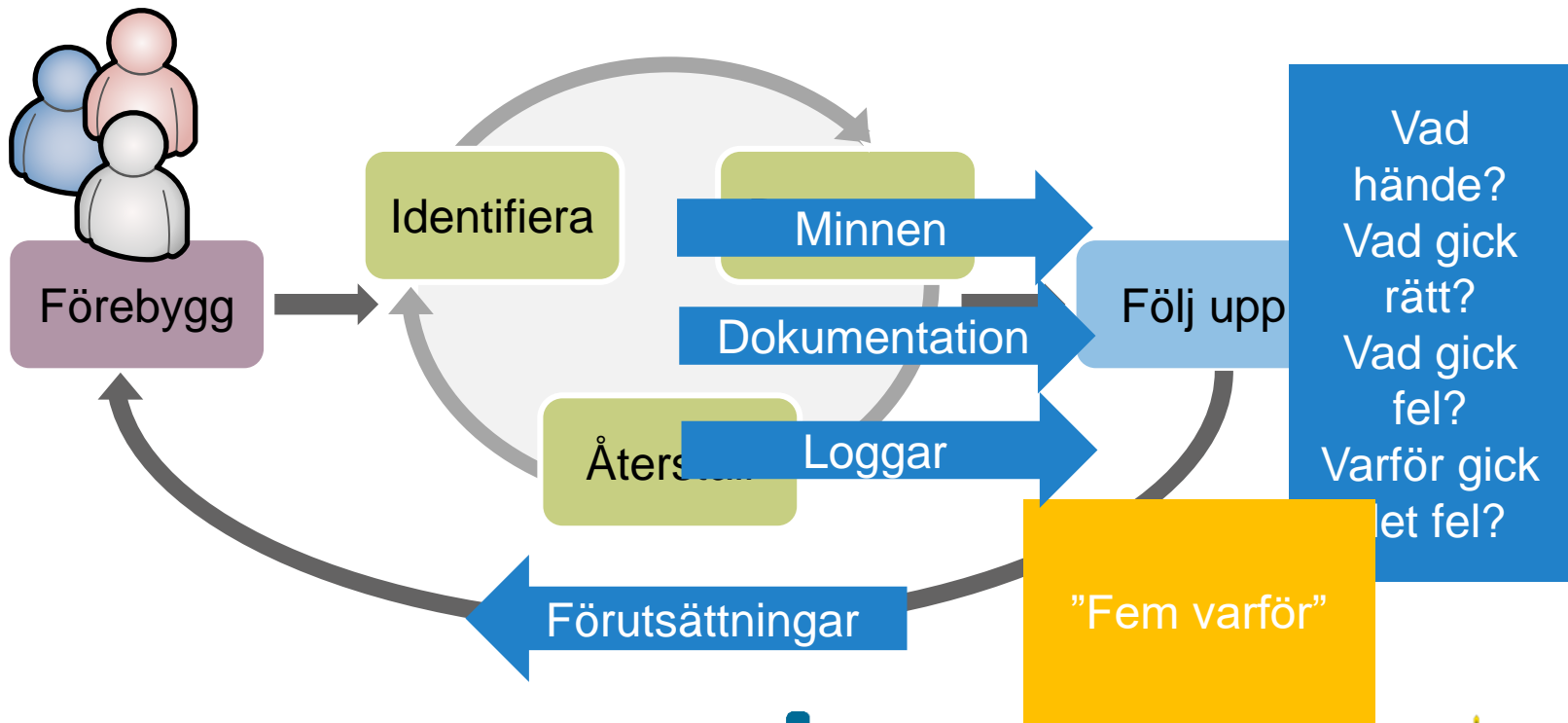
MSBFS 2018:8, 11 §

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

	Prevention	Detection	Triage	Analysis	Incident response	Incident closure	Post-analysis
ENISA (2010)	(1) Prevention management	(2) Detection	(3) Triage	(4) Analysis	(5) Incident response	(6) Incident closure	(7) Post-analysis
CERT SE (2013)	(1) Förbyggande	(2) Identifiera	(3) Begripna	(4) Analysera	(5) Återställa	(6) Erfarenheter	(7) Lärdomar
ISO (2021)	(1) Plan and Policy	(2) Detection and Reporting	(3) Assessment and Decision	(4) Response and Recovery	(5) Post-incident Activity	(6) Lessons learned	(7) Improvement
NIST (2017)	(1) Preparation	(2) Detection & Analysis	(3) Containment, Eradication & Recovery	(4) Post-incident Activity	(5) Reporting	(6) Lessons learned	(7) Improvement
NCS3 (2019)	(1) Prepare for incidents	(2) Identify and categorize	(3) Resolve the incident	(4) Report incident to stakeholders	(5) Learn from the incident	(6) Follow up	(7) Improve
ANSI (2020)	(1) Prevention	(2) Monitor & Identify	(3) Respond	(4) Recover	(5) Report	(6) Learn from the incident	(7) Improve
SANS (2020)	(1) Preparation	(2) Identification	(3) Containment	(4) Eradication	(5) Recovery	(6) Lessons learned	(7) Improvement
Kursumodell	Förberedelser	Upptäckt	Hantering		Efterarbete		



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

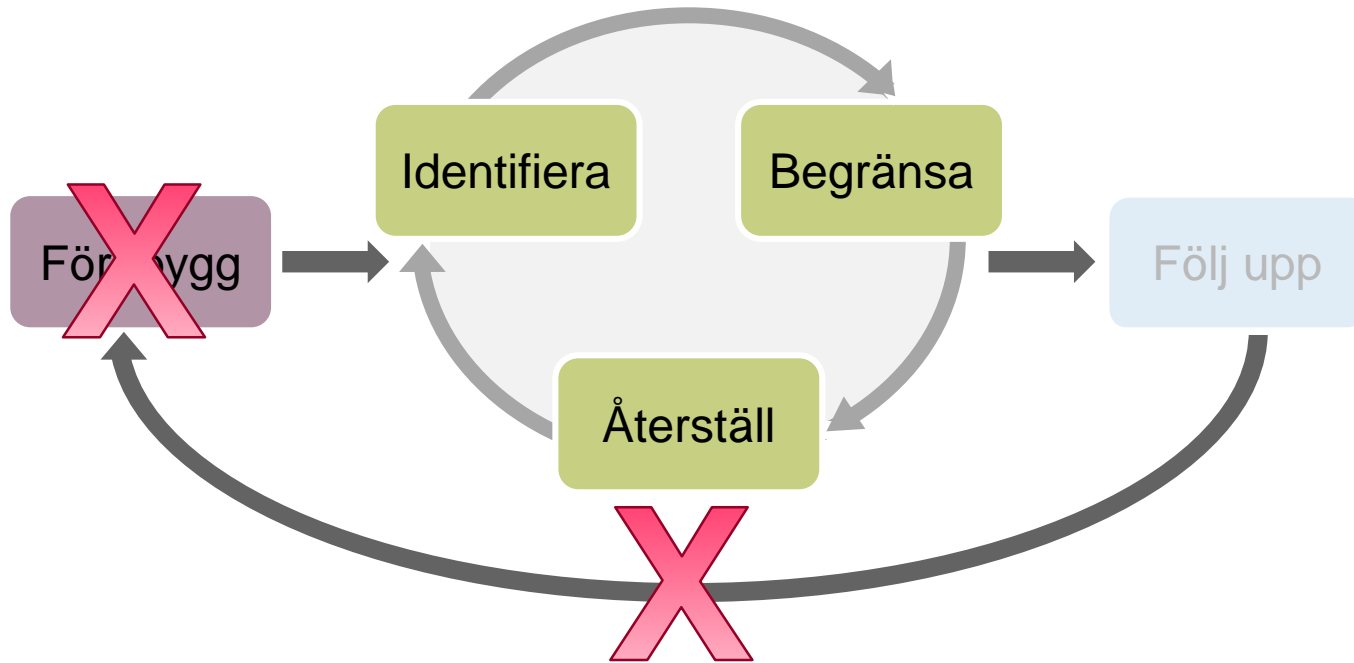
Övningsinformation

- 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



NCS3 

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 lagstiftning dokumenteras
- Incidenthanteringslogg
 - Dokumentera vad som sker
 - Primär bedömning från vår sida
 - Sker via "Messages" i CEC

Vad ska dokumenteras?

Vem sköter denna?

Med vilka data?



The screenshot shows a web form with a title bar containing a close button (x). Below the title bar is a text input field. Underneath the input field is a label "message" and a larger text area for the message content. At the bottom right of the form are two buttons: a "Close" button and a red "Submit" button.






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"

New Note

Title

Body

← → Paragraph **B** *I*      ...

0 WORDS POWERED BY TINY

File Input

No files selected.

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.



The image shows a screenshot of a web form titled "Add Message". The form has a close button (X) in the top right corner. It contains two main input fields: "Thread title" and "Message". The "Thread title" field is a single-line text input with a vertical cursor. The "Message" field is a larger, multi-line text area with a diagonal cursor icon in the bottom right corner. At the bottom right of the form, there are two buttons: a white "Close" button and a red "Submit" button.

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

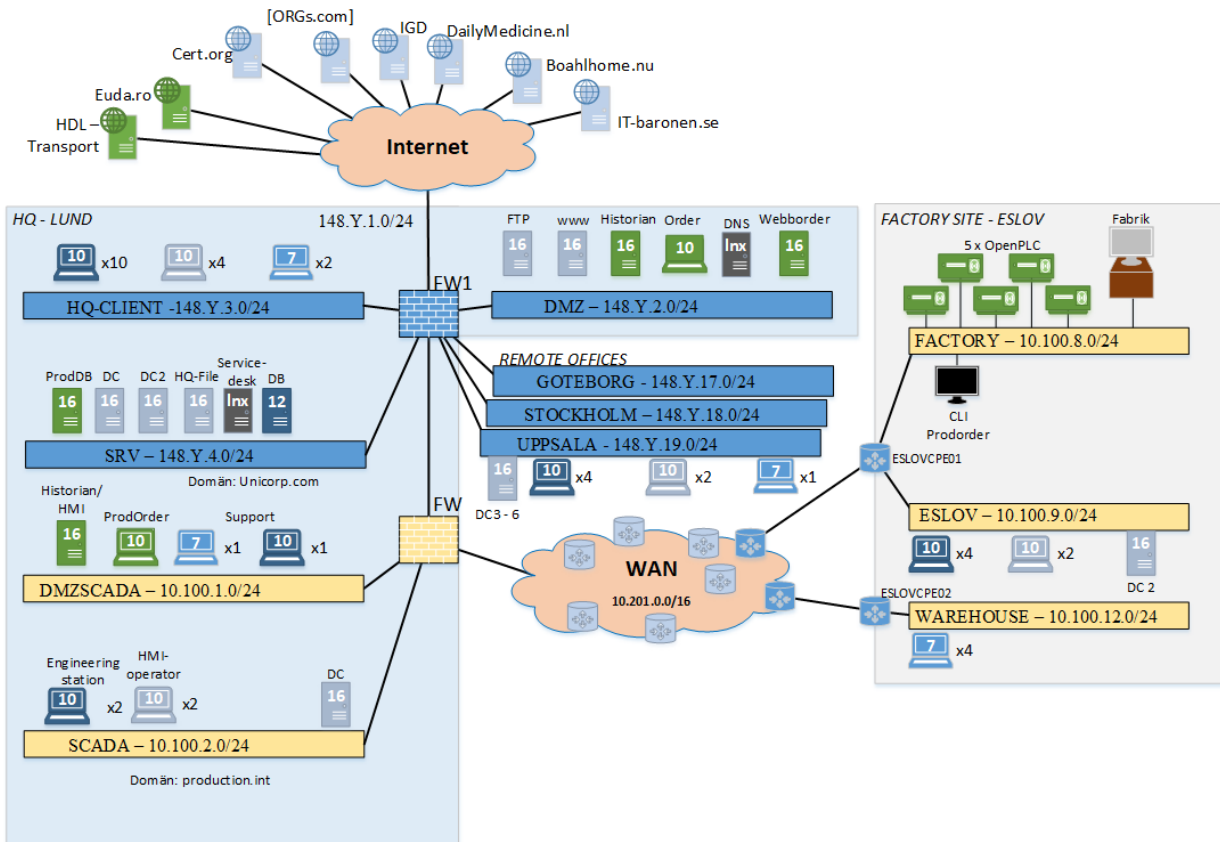
Övningar – Kontaktvägar

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

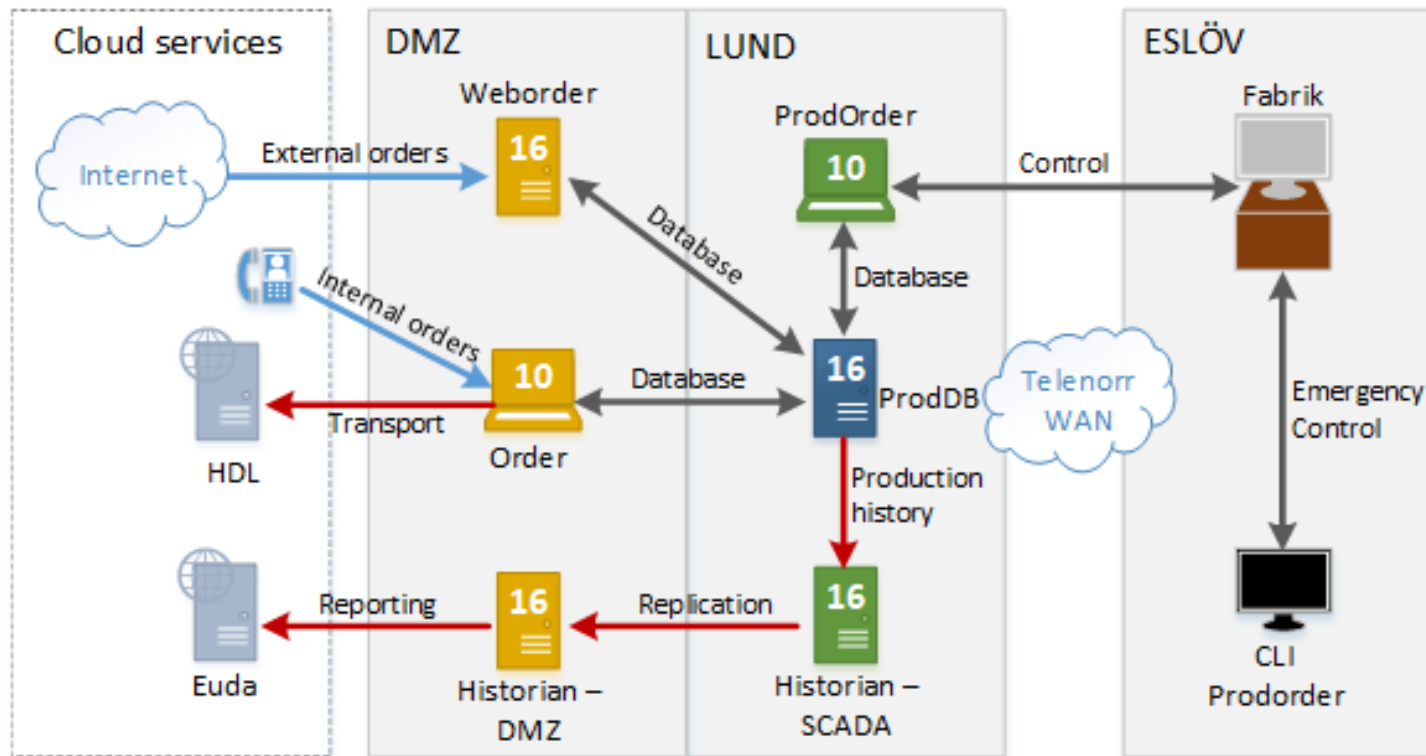
Övningar – Bevakning

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

Övningsmiljön – Unicorp/Pharmenta



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 utskrivnen

BP-Documnt
Internat
2021-10-13

PHARMERTA
Author: Bo Alm

BP-Documnt
Internat
2021-10-13

Pharmerta Medical process
Manual version 1.02

1. Forgetmenot (Product 1)
EU MED ID: 980345-423-2012
Ingredients:
15 % Aurum Flavus
40 % Triticum Aloe
45% Hordeum Vitae
Active Component: Hordeum Vitae

2. Nobrainer (Product 2)
EU MED ID: 982095-425-2010
Ingredients:
15 % Argentum Flavus
30 % Triticum Aloe
55% Malandica Vitae X
Active Component: Triticum Aloe

3. Vivareck (Product 3)
EU MED ID: 232095-427-2014
Ingredients:
5 % Pythoussa Argentum
20 % Triticum Striga VII
75% Malandica Vitae IX
Active Component: Triticum Striga VII

PHARMERTA
Author: Bo Alm

BP-Documnt
Instruktion IT
Security clearance: INTERNAL
Date: 2021-10-13
Department: IT-Dept
Version/nummernummer: 6492-67

Instruktion – Autonom Drift
Denna instruktion beskriver hur ni vid behov kan ställa om produktionen till autonom drift. Notera att så länge ProdOrder har lämnats till fabriken och det finns order i databasen så kommer fabriken att skicka sig själv.

För att övergå i autonom drift gör ni följande:

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

För att koppla bort noder i WAN, kontakta ISP:n Telcelor via CEC och ange vad ni vill koppla bort.

```
StartProduction :  
Start production of current product  
  
AbortProduction :  
Aborts current batch  
  
Start: NewProduct Forgetmenot  
Product: 1 Forgetmenot: Aurum Flavus 15  
Requested value 'Aurum' was not found.  
Product: 1 Forgetmenot: Add Aurum Flavus 15  
Product: 1 Forgetmenot: Add Triticum Aloe 40  
Product: 1 Forgetmenot: Add Hordeum Vitae 45  
Product: 1 Forgetmenot: StartProduction  
Product sent to factory  
Start> Running Batch step
```

Göm inte knappen när den lyser!

Cloud services | DMZ | Weborder | LUND | ESLOV | Fabriks
Internet | External orders | ProdOrder | Control | Emergency Control
HMI | Order | Database | Production Energy | Historian SCADA | Historian | SCA
Code | Historian-DMZ | Historian-SCADA | CLI | Prodorder

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