Projektnummer/Project no
A740039
Uppdragsgivare/Client
Regeringskansliet
FoT-område
Inget FoT-område

Författare/Author
Tommy Gustafsson

Datum/Date
2022-07-06
Memo nummer/Number
FOI Memo 7913

Kursutbud i den nationella cyberanläggningen Crate - 2022

1 Bakgrund

FOI använder sedan 2009 den nationella cyberanläggningen Crate[1] för att tillhandahålla träning i cybersäkerhet till relevanta aktörer inom totalförsvaret. I detta memo beskrivs de kurser som använder cyberanläggningen för ett eller flera kursmoment. Syftet med memot är att ge läsaren en samlad bild av det kursutbud som finns tillgängligt under 2022.

Notera att detta memo inte beskriver de större övningarna såsom MSB:s *Nationell teknisk övning* eller Försvarsmaktens *SAFE Cyber* som regelbundet genomförs i Crate då dessa justeras för varje genomförande

[1] FOI-2021-2086:1, Strategi för Crate 2021

2 Kurs i elektronisk säkerhet

Kurs i elektronisk säkerhet (HKES) är en kurs som FOI ger i egen regi sedan 2012. Kursen är framtagen för att ge en bred genomgång av dagens elektroniska system, både vad gäller normal funktion och säkerhetsproblematik. Syftet är att deltagaren ska kunna hantera och bedöma frågor som rör säkerhet i elektroniska system vilket kräver en omfattande kunskap om systemen och de hot de är utsatta för.

För att göra kursen så givande som möjligt blandas personer från olika organisationer vid samma kurstillfällen. På detta sätt kan deltagarna lära sig av varandra och få en så bred syn som möjligt på säkerhetsområdet. Stor vikt läggs vid att knyta an till den verksamhet och verklighet som deltagarna kommer från.

Kursen genomförs under fem dagar i enlighet med Figur 1.

Schema - Kurs i elektronisk säkerhet

Dag 1	Dag 2	Dag 3	Dag 4	Dag 5
	Datanät	Trådlös teknik Grunder och säkerhet	Krypto/datanät laboration	Telekonflikt
	Enkel säkerhetsvärdering Genomgång	Trådlös teknik Grunder och säkerhet	Intrång föreläsning förberedelse	Telekonflikt
	Enkel säkerhetsvärdering Laboration	Mobiltelefoni	Intrång laboration	Case: Scenarier och diskussion
	Skadlig kod	Mobiltelefoni	Intrång laboration	Avslutning
	Lunch	Lunch	Lunch	Lunch
Inledning	It-säkerhet	Mobiltelefoni	Satellitnavigeringssystem	
It-säkerhetsarbete	It-krigföring	Pejling och störning av radiosystem	Satellitnavigeringssystem	Färgkodning:
				Föreläsningspass
Krypto	Demonstrationer	Pejling och störning av radiosystem	Diskussion/Scenario	Laborationspass
Krypto	Demonstrationer	Inbyggda system	Satellitnavigeringsystem, militärspecifik del	Övningspass
	Visningar av FOI:s verksamhet			

Figur 1: Schema för kurs i elektronisk säkerhet. Notera att kursen även inkluderar en förevisning av FOI:s verksamhet eftersom kursen ofta har många deltagare från totalförsvaret.

2.1 Målgrupp

Elektronisk säkerhet riktar sig till personer som har säkerhet inom sitt ansvarsområde men som inte nödvändigtvis själva är tekniskt verksamma, till exempel chefer, beslutsfattare, projektledare och tjänstemän.

2.2 Förkunskapskrav

Kursen kräver inga tekniska förkunskaper annat än att ha kommit i kontakt med säkerhetsfrågor, vara tekniskt intresserad och tycka att elektronisk säkerhet är viktigt.

2.3 Lärandemål

Kursen ska ge deltagaren kunskap så att denne kan förstå den omgivning som olika elektroniska system finns i och hur olika typer av system kan påverkas av hot och attacker. Deltagaren ska också få kunskap om förebyggande metoder inom säkerhet.

2.4 Ingående pass

Kursen består huvudsakligen av föreläsningar men demonstrationer, laborationer och fall-diskussioner används för att åstadkomma ett mer aktivt lärande. Föreläsningspassen omfattar trådbundna och trådlösa datornätverk, grundläggande radioteknik, signalspaning och störning av radio, mobiltelefoni, GPS, it-säkerhetstekniker, dataintrång och skadlig kod. I kursen genomförs också en demonstration av sårbarheter i it-system samt laborationer i säkerhetsvärdering, kryptoanvändning och datorintrång.

2.5 Övningsmiljö i Crate

Under kursens intrångslaboration används den så kallade trafikljusmiljön (se **Fel! Hittar inte referenskälla.**) som innehåller ett nätverk kopplat till en fysisk PLC som kontrollerar ett ”trafikljus”. Varje deltagare har en egen instans av trafikljusmiljön och använder Metasploit och Armitage för att kartlägga och angripa trafikljusen.

Figur 2: Trafikljusmiljön används under grundkursens laborationer där varje deltagare har en egen instans av övningsmiljön och ett eget ”trafikljus” som styrs av en PLC. Figuren visar också gränssnittet i Armitage som används under laborationen.

3 It-säkerhet i driftmiljö

It-säkerhet i driftmiljö (ID) är en kurs som har tagits fram och givits på direkt beställning av Försvarsmakten. Övergripande syfte med kursen är att förbättra deltagarnas förmåga att detektera, hantera och avrapportera it-säkerhetsincidenter samt dra erfarenheter av dessa, för att möjliggöra förbättringar i säkerhetsarbetet.

Kursen fokuserar på tekniska aspekter av it-system snarare än på juridiska, organisatoriska eller användarbaserade aspekter. Under kursen poängteras vikten av rapportering, dokumentation och uppföljning. Förvärvade kunskaper i kursen sätts in i ramen av hur it-säkerhetsarbete planeras, genomförs och förvaltas på olika nivåer inom Försvarsmakten.

Kursen genomförs under fyra dagar i enlighet med Figur 3 och består till större del av föreläsningspass.

Schema - It-säkerhet i driftmiljö

Dag 1	Dag 2	Dag 3	Dag 4
	Krypto	Mobiltelefoni - it-relaterade säkerhetshot	Inbyggda system
	Krypto	Mobiltelefoni - it-relaterade säkerhetshot	Tillit
	Aktörer, mål och förmåga	It-osäkerhetsdemo	It-säkerhet i FM
	Aktörer, mål och förmåga	It-osäkerhetsdemo	Utvärdering
	Lunch	Lunch	
Inledning	Attacker och försvar, översikt	It-forensisk metodik	
It-säkerhet, grundläggande begrepp och hot	Attacker och försvar, översikt	Hantering av intrång, laboration	
It-säkerhet, grundläggande begrepp och hot	Attacker och försvar, översikt	Hantering av intrång, laboration	
Skadlig kod	Attacker och försvar, översikt	Hantering av intrång, laboration	

Färgkodning:
Föreläsningspass
Laborationspass

Figur 3: Schema för kursen It-säkerhet i driftmiljö.

3.1 Målgrupp

Primär målgrupp är drift- och övervakningspersonal inom Försvarsmaktens centrala informations- och ledningssystemsinfrastruktur. Sekundär målgrupp är personal i incidenthanterande eller direkt arbetsledande roller i samverkan med den primära målgruppen, samt personal som utför teknisk produktion, utbyggnad eller förändring av Försvarsmaktens informations- och ledningssystemsinfrastruktur.

3.2 Förkunskapskrav

Kursen har en teknisk inriktning och kräver därför goda förkunskaper inom ett eller flera av områdena *nätverk och nätverksutrustning*, *servrar och datorer* eller *IP och operativsystem*.

Utbildningsmässigt förutsätts teknisk utbildning på åtminstone gymnasienivå.

3.3 Lärandemål

Målet med kursen är att deltagarna efter genomförd utbildning besitter en ökad kunskap, förståelse och beredskap för att detektera och rapportera anomalier och it-säkerhetsincidenter, samt kunskaper för att förbättra it-säkerhetsskyddet genom konkreta förslag eller direkta åtgärder.

3.4 Ingående pass

Kursen består huvudsakligen av föreläsningar men demonstrationer och laborationer används för att åstadkomma ett mer aktivt lärande. Föreläsningspassen tar upp: grundläggande begrepp inom it-säkerhet; skadlig kod; kryptering; aktörer, mål och förmåga; it-attacker och försvar; it-säkerhet inom Försvarsmakten, mobiltelefoni och inbyggda system; hantering av datorintrång samt vikten av tillit inom säkerhet.

Demonstrations- och laborationspassen tar upp sårbarheter i it-system samt hantering av intrång.

3.5 Övningsmiljö i Crate

ID-kursens laborationspass använder samma övningsmiljö som tidigare beskrivits under avsnitt 2.

4 Kurser inom NCS3

Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett samarbete mellan *Myndigheten för samhällsskydd och beredskap* (MSB) och *Totalförsvarets forskningsinstitut* (FOI) i syfte att stärka säkerheten i cyberfysiska system inom samhällsviktig verksamhet. En betydande del av verksamheten inom NCS3 är att utveckla och ge kurser baserade på de studier som bedrivs inom centrumet och inom övriga uppdrag som FOI utför med fokus på cybersäkerhet. Kurserna riktar sig primärt till aktörer inom samhällsviktig verksamhet som inkluderar industriella informations- och styrsystem.

4.1 Chefskurs – Säkerhet i industriella informations- och styrsystem

Chefskurs – Säkerhet i industriella informations- och styrsystem (CK-SI3S) togs fram under 2020. Beslutet att ta fram kursen baserades på återkommande efterfrågan från deltagarna på övriga NCS3-kurser. Kursen består huvudsakligen av föreläsningar med inslag av demonstrationer och interaktiva frågor för att åstadkomma ett mer aktivt lärande. Syftet med kursen är att deltagarna ska få en aktuell problembild för it-hot mot samhällsviktig verksamhet, en inblick i teknik, risker och sårbarheter som kan finnas i de industriella informations- och styrsystemen samt hur ett systematiskt it-säkerhetsarbete kan bedrivas inom en organisation.

CK-SI3S är tre timmar lång och det är möjligt att anpassa schemat baserat på kringarrangemang i enlighet med Figur 4. Tillexempel kan längre raster läggas till för att möjliggöra mer dialog mellan deltagarna. Kursen lämpar sig för både små och stora grupper och det är egentligen bara lokalens storlek som begränsar antalet deltagare. Mindre grupper möjliggör en mer aktiv dialog mellan deltagarna och föreläsaren och kan även kombineras med någon form av diskussionsbaserad övning.

Schema Förmiddag/Eftermiddag	
30 min	Problembild
15 min	Rast
90 min	Strukturerat säkerhetsarbete
15 min	Rast
30 min	Systemkunskap

Schema runt lunch	
30 min	Problembild
45 min	Strukturerat säkerhetsarbete
90 min	Lunch
45 min	Strukturerat säkerhetsarbete, forts.
30 min	Systemkunskap

Figur 4: Kursen är schemamässigt flexibel, pauser eller uppehåll kan till stor del läggas in efter önskemål och för att till exempel ge utrymme för mer utbyte mellan deltagarna. I figuren visas två förslag på hur chefskursen kan genomföras.

4.1.1 Målgrupp

Kursen riktar sig till beslutsfattare i organisationer inom både offentlig och privat sektor, som arbetar med samhällsviktig verksamhet som är beroende av industriella informations- och styrsystem.

4.1.2 Förkunskapskrav

Kursen kräver inga förkunskaper.

4.1.3 Lärandemål

Efter genomgången kurs ska deltagarna:

- ha kunskap om problembilden rörande cyberhot riktade mot industriella informations- och styrsystem inom samhällsviktig verksamhet
- förstå vilka cybersäkerhetsutmaningar som industriella informations- och styrsystem medför
- ha kunskap om hur en cybersäkerhetsincident kan påverka verksamheten och organisationen
- ha kunskap om hur ett systematiskt informationssäkerhetsarbete kan bedrivas.

Kursen syftar också till att ge deltagarna utrymme för kunskaps- och erfarenhetsutbyte samt nätverksbyggande.

4.1.4 Ingående pass

CK-SI3S innehåller tre pass som presenterar problembilden inom cybersäkerhetsområdet, systematiskt informationssäkerhetsarbete och systemkunskap med fokus på industriella informations- och styrsystem inom samhällsviktig verksamhet.

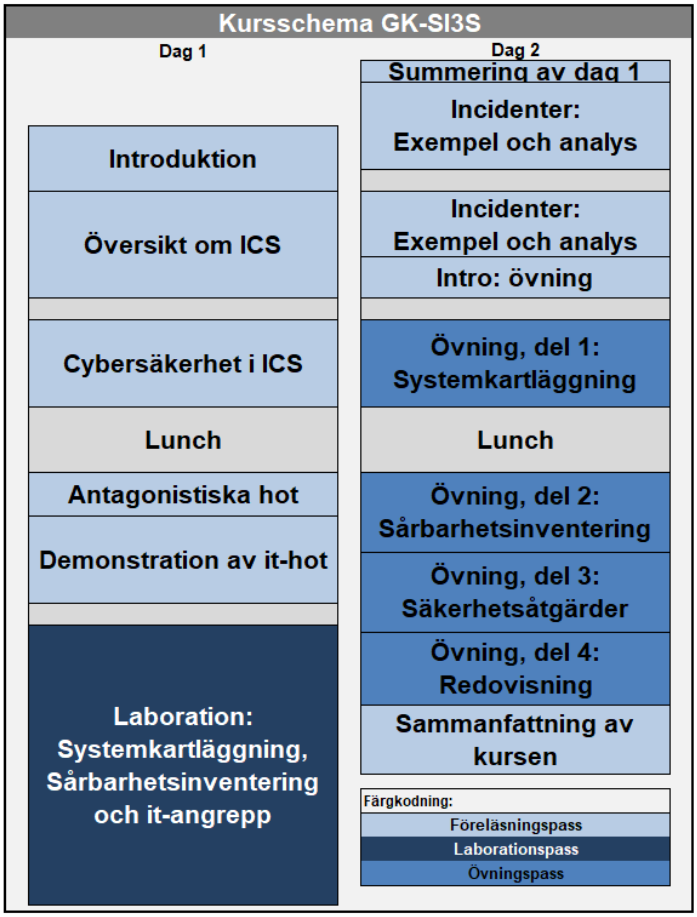
Problembilden förmedlas genom en beskrivning och analys av aktuella cybersäkerhetsincidenter som drabbat samhällsviktiga system. Systematiskt informationssäkerhetsarbete presenteras och ger deltagarna en introduktion till cybersäkerhet, dess förutsättningar och exempel på hur säkerhetsåtgärder kan användas för att minska exponering och förbättra säkerhetsskyddet av känsliga system. Vidare beskrivs hur beslutsfattare kan driva ett systematiskt informationssäkerhetsarbete i organisationen. Kursen avslutas med en genomgång av specifika utmaningar med industriella informations- och styrsystem inom samhällsviktig verksamhet. I detta pass ges också en beskrivning av utmaningar med distansarbete och molntjänster.

De demonstrationer som används i kursen kan köras oberoende av Crate för att göra det möjligt att genomföra kursen utan internetanslutning.

4.2 Grundkurs – Säkerhet i industriella informations- och styrsystem

Grundkurs – Säkerhet i industriella informations- och styrsystem (GK-SI3S) är den äldsta kursen och gavs första gången 2009. Kursen kallades då SIK (Säkerhet i kontrollsystem) och har sedan dess genomgått regelbundna uppdateringar för att fortsätta vara relevant. Under 2022 kommer en helt ny version av grundkursen att tas fram inom ramen för NCS3. Kursen består av föreläsningar, ett demonstrationspass , laborationer och ett längre övningspass. GK-SI3S syftar till att höja medvetenheten om vikten av att arbeta systematiskt med cybersäkerhetsfrågor inom informations- och styrsystem samt en introduktion till verktyg och metoder som kan användas för att åstadkomma detta.

Kursen tar två dagar i enlighet med Figur 5 och lämpar sig för mellan 12 och 16 deltagare.



Figur 5: Kursschema för grundkursen.

4.2.1 Målgrupp

Kursen riktar sig till de som arbetar med industriella informations- och styrsystem inom samhällsviktig verksamhet, till exempel som operatör, utvecklingsingenjör eller som ansvarig för sådan verksamhet.

4.2.2 Förkunskapskrav

För att tillgodogöra sig kursen behöver deltagaren ha en grundläggande praktisk kunskap om it-system.

4.2.3 Lärandemål

Efter genomgången kurs ska deltagarna:

- ha förståelse för betydelsen av och fördelarna med att arbeta aktivt och systematiskt med cybersäkerhetsfrågor i industriella informations- och styrsystem
- känna till lämpliga verktyg och metoder för att identifiera cyber-sårbarheter i industriella informations- och styrsystem
- kunna delta i arbetet med att förbättra och utveckla cybersäkerheten i en organisations industriella informations- och styrsystem.

Kursen ska också ge deltagarna möjlighet till kunskaps- och erfarenhetsutbyte samt nätverksbyggande.

4.2.4 Ingående pass

Kursen inleds med föreläsningar som ger en introduktion till cybersäkerhet i industriella informations- och styrsystem samt hur den skiljer sig från cybersäkerheten i it-system. Därefter följer en föreläsning om antagonistiska hot med fokus på hur de kan tänkas påverka samhällsviktiga system och en demonstration av sårbarheter som förekommer i datoriserade system. Den första dagen avslutas med en laboration där deltagarna får genomföra en kartläggning, sårbarhetsskanning och ett intrång i ett industriellt informations- och styrsystem.

Dag två inleds med en föreläsning om cybersäkerhetsincidenter som har skett inom samhällsviktig verksamhet samt en föreläsning som visar hur dylika incidenter kan utnyttjas som kunskapskällor för att förbättra säkerheten i egna system. Kursen avslutas med ett längre övningspass där deltagarna ska genomföra en säkerhetsanalys av både den fysiska och it-baserade miljön hos ett fiktivt företag. Deltagarna arbetar i grupper, vilket också ger en utökad möjlighet till kunskaps- och erfarenhetsutbyte samt nätverksbyggande.

4.2.5 Övningsmiljö i Crate

Grundkursens laborationspass använder samma övningsmiljö som tidigare beskrivits under avsnitt 2. Under kursens övningspass används en övningsmiljö som kallas Angmaskin. Övningsmiljön Angmaskin kompletteras med kartor och skisser som beskriver det fiktiva företaget och det scenario som deltagarna ska hantera.

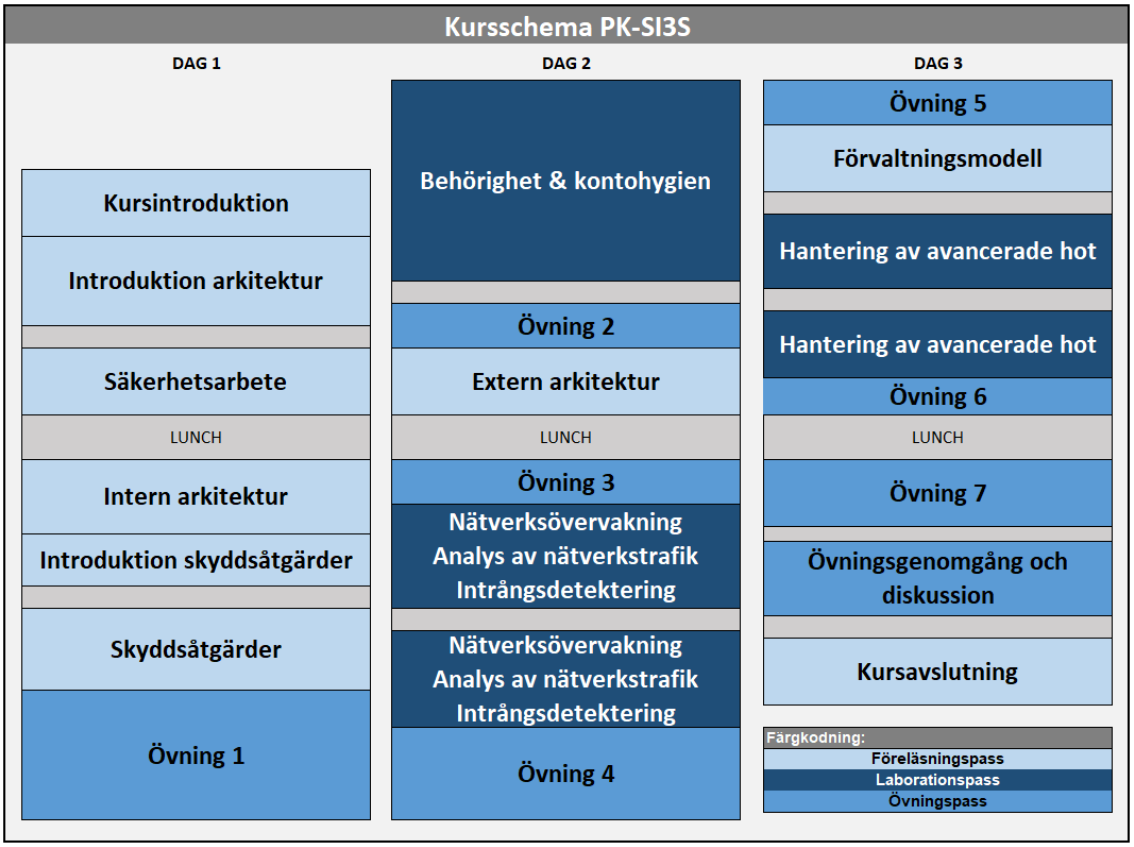
4.3 Påbyggnadskurs – Säkerhet i industriella informations- och styrsystem

Påbyggnadskurs – Säkerhet i industriella informations- och styrsystem (PK-SI3S) utvecklades 2018. Under kursen används föreläsningar och laborationer för att höja deltagarnas kunskaper om olika säkerhetsåtgärder och hur de kan användas för att skydda system. För att ge möjlighet till värdering av olika säkerhetsåtgärder och erfarenhetsutbyte mellan deltagarna används som ett moment i kursen ett brädspel utvecklat vid FOI där deltagarna i samarbete med varandra ska säkra upp en nätverksmiljö mot angrepp.

Påbyggnadskursen baseras på de säkerhetsåtgärder som presenteras i MSB:s *Vägledning för säkerhet i industriella informations- och styrsystem*[2] och de så kallade CIS-kontrollerna som sammanställs av organisationen *Center for Internet Security*[3]. Kursen lämpar sig för 12 till 20 deltagare och ges under tre dagar i enlighet med schemat i Figur 6.

[2] MSB718, Vägledning till ökad säkerhet i industriella informations- och styrsystem.

[3] https://www.cisecurity.org



Figur 6: Schema för påbyggnadskursen. Notera att övningspassen avser de pass där deltagarna använder brädspelet.

4.3.1 Målgrupp

Kursen riktar sig till tekniker som arbetar med underhåll och övervakning, leder verksamhet eller på annat sätt påverkar utformningen av industriella informations- och styrsystem inom samhällsviktig verksamhet.

4.3.2 Förkunskapskrav

Deltagaren bör ha erfarenhet av industriella informations- och styrsystem samt god förståelse för it-system, datornätverk och cybersäkerhetsproblematiken inom industriella informations- och styrsystem. Vidare rekommenderas att deltagaren har gått *Grundkurs – Säkerhet i industriella informations- och styrsystem.*

4.3.3 Lärandemål

Efter genomgången kurs ska deltagarna:

- ha en ökad kunskap om säkerhetsåtgärder i cyberfysiska och it-miljöer
- förstå hur tekniska, administrativa och organisatoriska säkerhetsåtgärder kan användas för att stärka skyddet av ett system
- ha en ökad förmåga att prioritera olika säkerhetsåtgärder
- förstå hur exponering av kritiska funktioner kan reduceras

- ha kunskap om hur cyberhot kan upptäckas och identifieras.

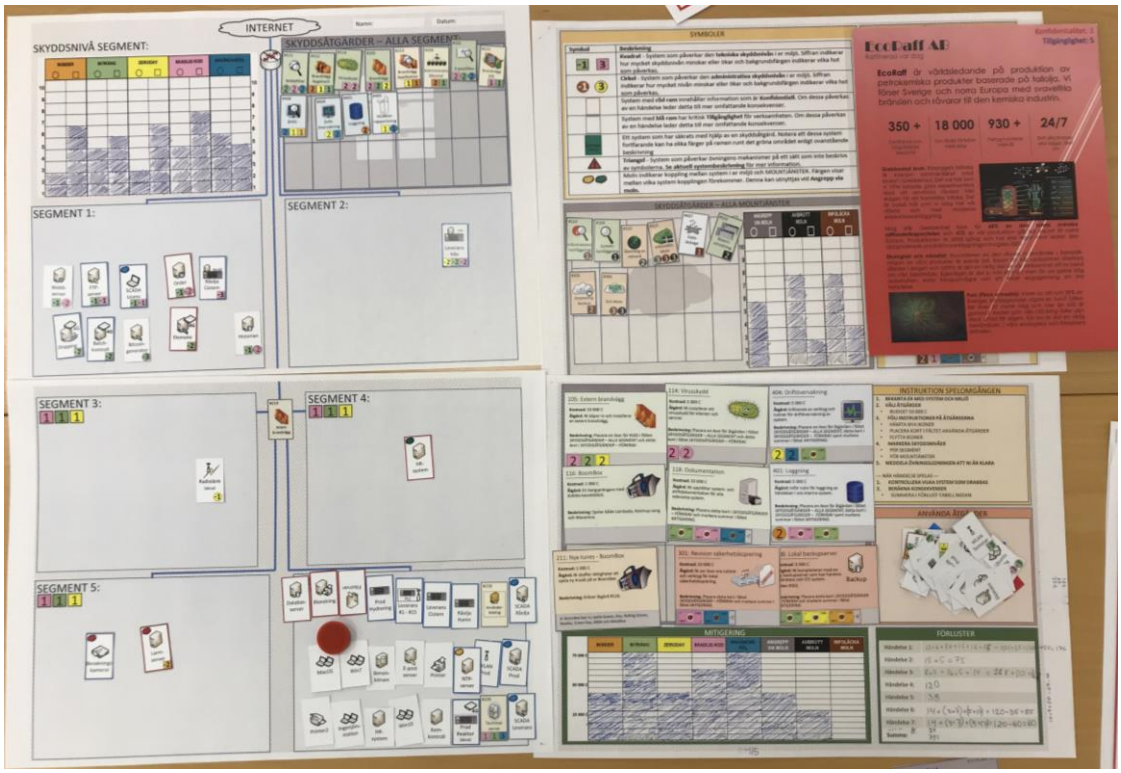
Kursen syftar också till att ge deltagarna möjlighet till kunskaps- och erfarenhetsutbyte samt nätverksbyggande.

4.3.4 Ingående pass

Påbyggnadskursen inkluderar föreläsningar som ska ge deltagaren en förståelse kring hur den övergripande infrastrukturarkitekturen påverkar exponeringen av system och hur en bra grunddesign kan användas för att mitigera kända och okända sårbarheter i systemen. Föreläsningar används också för att ge deltagarna kunskap om säkerhetsåtgärder, extern arkitektur och hur cybersäkerheten kan förvaltas under systemets hela livslängd.

Under kursen genomförs tre laborationer med fokus på behörighetskontroll och kontohygien, intrångsdetektering samt hantering av avancerade hot. Den senare laborationen utnyttjar den pedagogiska principen *productive failure*[4] för att påvisa vikten av att bedriva ett proaktivt säkerhetsarbete.

Brädspelet (se Figur 7) används under sju övningspass fördelade över hela kursen för att ge deltagarna möjlighet att successivt diskutera och värdera de säkerhetsåtgärder som har presenterats i tidigare pass. Deltagarna arbetar i grupp och ska tillsammans använda arkitekturmodifieringar och säkerhetsåtgärder för att höja skyddsnivån hos ett fiktivt företag. I spelets design ingår att deltagarna måste ta hänsyn till huruvida företagets verksamhet ställer högst krav på konfidentialitet eller tillgänglighet. För att ge deltagarna återkoppling på om de har åstadkommit en tillräcklig skyddsnivå utsätts de fiktiva företagen för simulerade cyberangrepp under spelets gång.

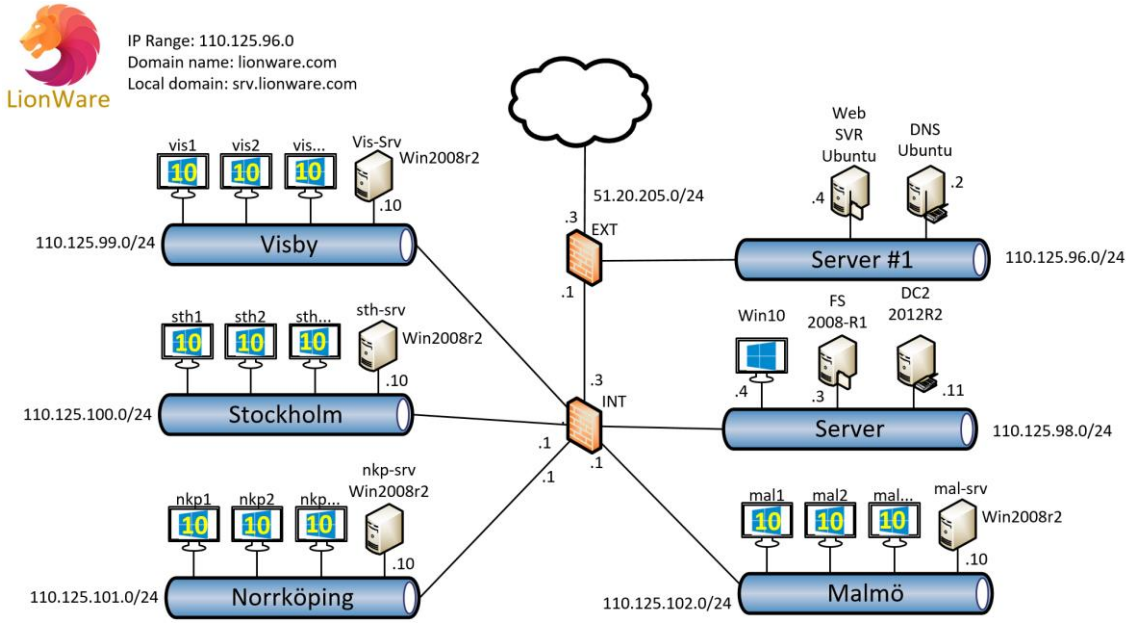


Figur 7: En av brädspelets spelplaner där deltagarna har infört säkerhetsåtgärder och använt arkitekturmodifieringar för att höja skyddsnivån hos det fiktiva företagets system.

[4] Kapur, M. & Bielaczyc, K. (2012). Designing for Productive Failure. Journal of the Learning Sciences

4.3.5 Övningsmiljö i Crate

Under laborationerna i påbyggnadskursen används en övningsmiljö som kallas Lionware (se Figur 8) som simulerar en Microsoft Windows-miljö hos ett fiktivt företag. Övningsmiljön innehåller också grundläggande säkerhetssystem i form av brandväggar och ett intrångsdetekteringssystem som användarna kan nyttja under laborationerna.



Figur 8: Övningsmiljön Lionware som används under påbyggnadskursen.

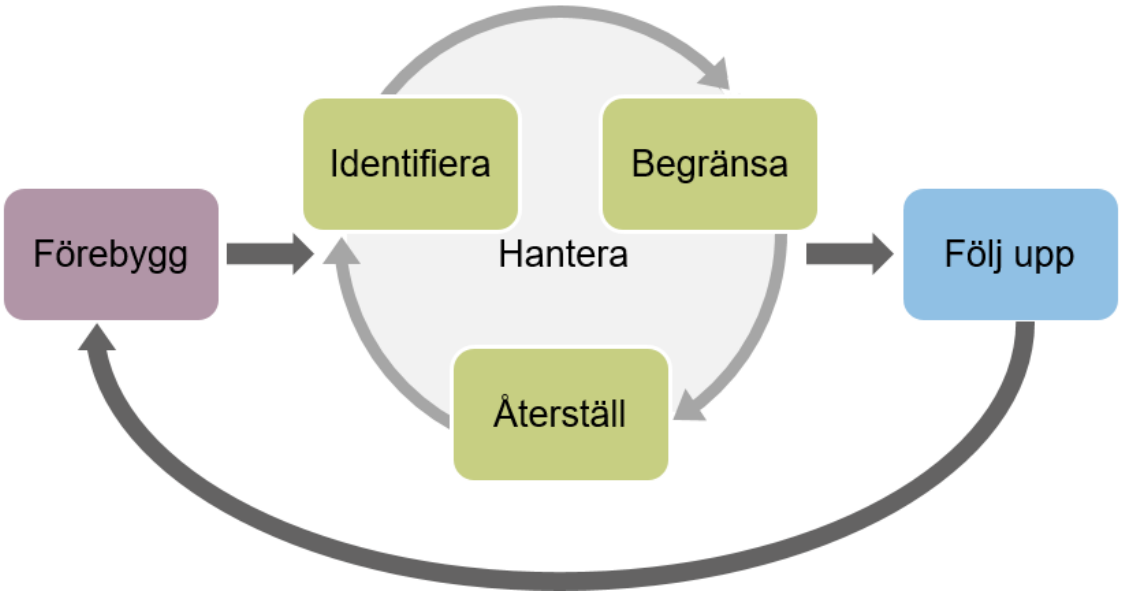
Under laborationerna *behörighetskontroll* och *hantering av avancerade hot* arbetar deltagarna i samma miljöinstans men under laborationen *intrångsdetektering* har de tillgång till varsin, mindre version av övningsmiljön. Anledningen till detta är att de då inte kan påverka varandras system av misstag.

4.4 Praktisk incidenthantering i industriella informations- och styrsystem

Praktisk incidenthantering i industriella informations- och styrsystem (I4S) syftar till att utveckla deltagarnas förmåga att upptäcka och hantera cybersäkerhetsincidenter och utvecklades ursprungligen 2013. Under 2020 och 2021 genomfördes en nyutveckling av incidenthanteringskursen där kursen moderniserades och fick en förstärkt pedagogik baserad på modellen 4C/ID[5] där deltagarnas förmåga förbättras genom att de löser svårare och svårare uppgifter i samma grundmiljö.

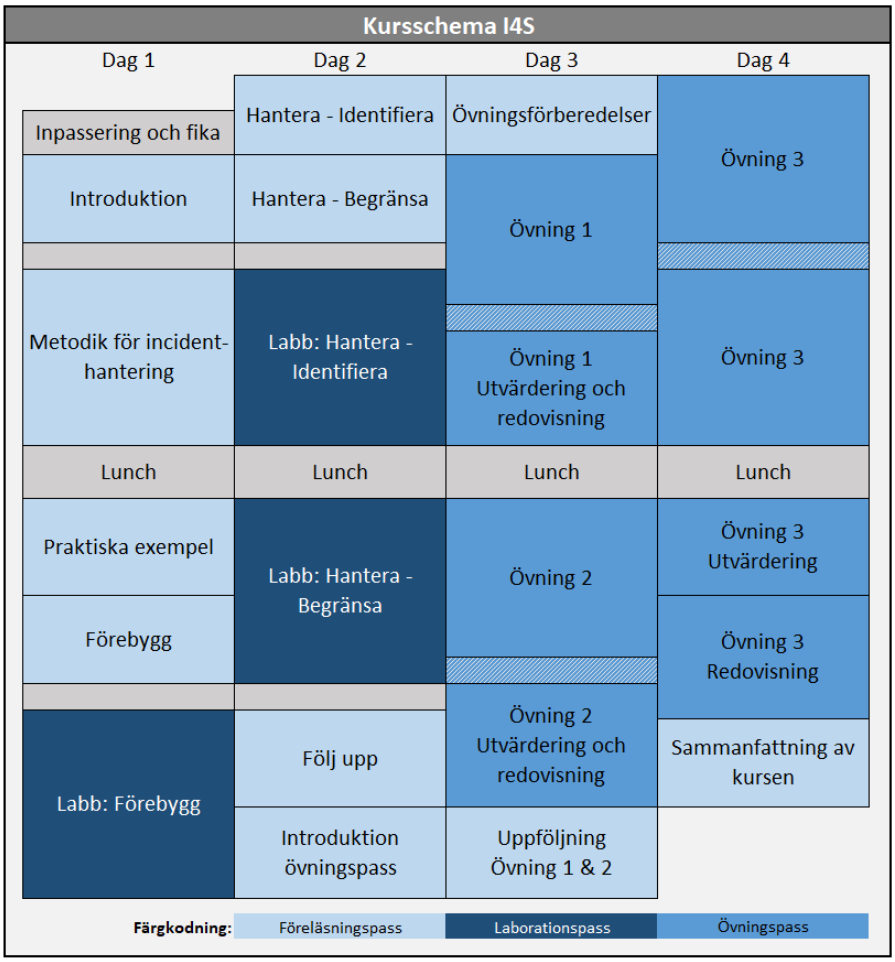
Figur 9 visar en generisk metod för incidenthantering som FOI har tagit fram för kursen. Den generiska metoden baseras på ett antal befintliga metoder för incidenthantering från bland andra MSB, ENISA, NIST och ISO. Anledningen till att en generisk metod används är att den är enkel att översätta till övriga metoder och att deltagarna på så sätt kan applicera kunskaperna från kursen oavsett vilken incidenthanteringsmetod den egna organisationen använder.

[5] Van Merriënboer, J. J. G., Jelsma, O., & Paas, F. G. W. C. (1992). Training for reflective expertise: A four-component instructional design model for complex cognitive skills. Educational Technology Research and Development



Figur 9: Den generiska incidenthanteringsmetod som FOI har tagit fram för kursen.

Incidenthanteringskursen lämpar sig för 10 till 20 personer och genomförs under fyra dagar i enlighet med Figur 10. Under kursen används föreläsningar för att introducera incidenthantering och ge deltagarna en fördjupad kunskap om olika åtgärder som kan användas i varje steg. Laborationer utnyttjas för att ge deltagarna en möjlighet att bekanta sig med övningsmiljön, dess process och de verktyg som de ska använda under övningspassen. Under kursens två avslutande dagar genomförs tre övningspass där deltagarna ska hantera ett antal incidenter i övningsmiljön.



Figur 10: Kursschema för incidenthanteringskursen.

4.4.1 Målgrupp

Kursen riktar sig till systemadministratörer i organisationer inom både offentlig och privat sektor, som arbetar med samhällsviktig verksamhet. Inom denna grupp prioriteras deltagare som redan har eller kan komma att få en roll i sin organisations it-incidenthantering.

4.4.2 Förkunskapskrav

För att tillgodogöra sig kursen behöver deltagaren ha erfarenhet av industriella informations- och styrsystem samt god kunskap om it-system, datornätverk och cybersäkerhetsproblematiken inom industriella informations- och styrsystem.

4.4.3 Lärandemål

Efter genomgången kurs ska deltagarna:

- ha en ökad förmåga att hantera incidenter i it-system i styrsystemsmiljöer
- ha förståelse för hur industriella informations- och styrsystem påverkar incidenthanteringsprocessen
- ha kunskap om metoder för incidenthantering

- ha kunskap om verktyg som kan användas för att förebygga, hantera och följa upp incidenter.

Vidare ska kursen ge deltagaren kunskaper som kan tillämpas i den normala arbetsmiljön. Kursens upplägg ger även deltagarna utrymme för kunskaps- och erfarenhetsutbyte samt nätverksbyggande.

4.4.4 Ingående pass

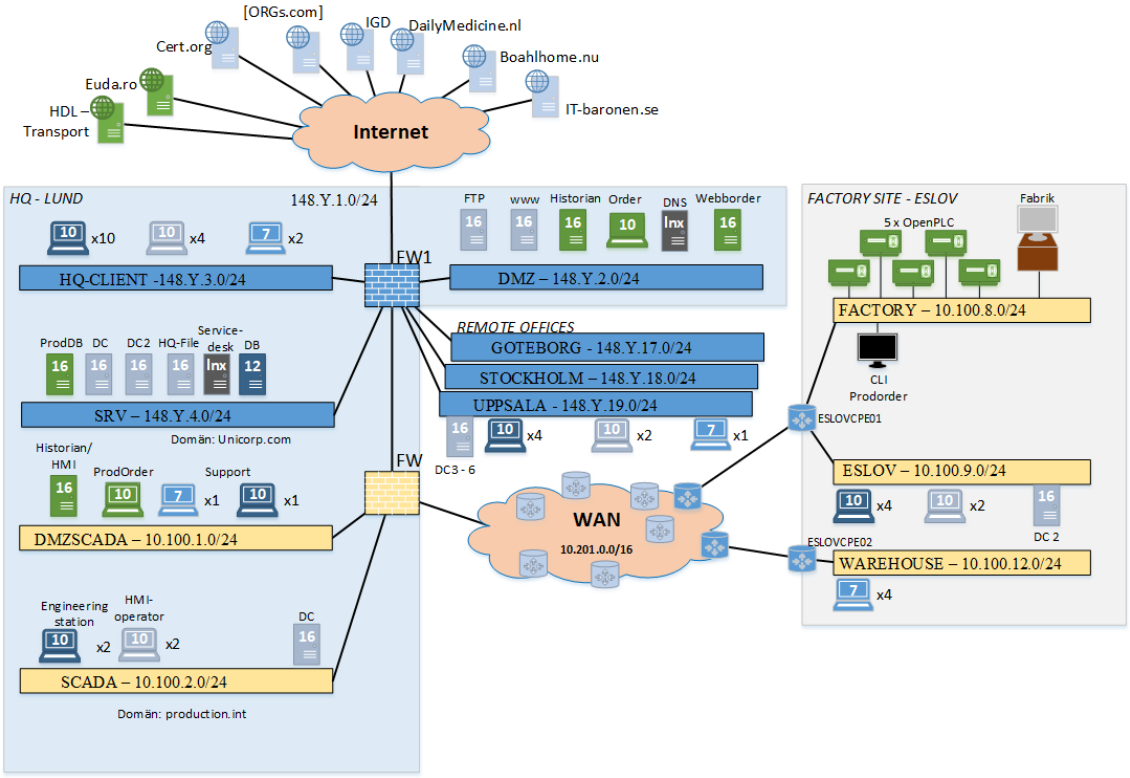
Incidenthanteringskursen innehåller föreläsningspass som introducerar den generiska modellen för incidenthantering samt fördjupningar med fokus på faserna *Förebygga, Hantera* och *Följa upp.* Kursen innehåller också ett föreläsningspass som presenterar exempel på incidenthantering hämtade från riktiga fall.

Under de två första dagarna genomförs tre laborationer med fokus på *kartläggning av nätverk och system, analys av nätverkstrafik och händelser* samt *hantering av brandväggar*. Laborationerna genomförs i samma övningsmiljö och använder samma verktyg som deltagarna kommer att utnyttja under övningspassen.

De tre övningspassen är framtagna för att deltagarna ska ges en möjlighet att praktisera incidenthantering i en miljö med en simulerad samhällsviktig process som inkluderar industriella informations- och styrsystem. Utöver att upptäcka, analysera, hantera och rapportera de incidenter som sker i miljön ska deltagarna säkerställa att incidenterna inte påverkar den simulerade industriprocessen. Detta för att skapa en rimligt realistisk övning där deltagarna utöver teknisk hantering också måste prioritera aktiviteter och fatta beslut om huruvida industriprocessen ska isoleras eller ej. De incidenter som sker under övningspassen är att miljön utsätts för ett botnet, ett utbrott av ett ransomware samt ett avancerat hot som varierar med temat på övningen. För att styra övningsdeltagarnas fokus och aktiviteter används administrativa inspel via simulerade nyhetssajter, e-post, videosamtal och telefonsamtal.

4.4.5 Övningsmiljö i Crate

Under 2022 finns två olika övningsmiljöer med olika processer som kan användas under kursen beroende på vilken sektor deltagarna kommer från. Övningsmiljön Pharmenta som visas i Figur 11, innehåller en produktionsprocess som inkluderar beställningssystem, SCADA-system, en hårdvarubaserad fabrik med en PLC samt system för rapportering och utleverans. Pharmenta inkluderar styrsystemsprotokollet Modbus och används som en generell övningsmiljö.



Figur 11: Övningsmiljön Pharmenta inkluderar en produktionsprocess med tillhörande it-system markerade i grönt i figuren. Övningsmiljön ska efterlikna en miljö hos en tillverkande industri och inkluderar många beroenden mellan system.

Övningsmiljön Energo innehåller en process där el produceras och distribueras, inklusive SCADA-system, emulerade RTU:er samt system för rapportering. Energo inkluderar styrsystemsprotokollen IEC-60870-5-104 samt IEC-61850 och används som en övningsmiljö för kurser riktade mot deltagare från energisektorn. Båda miljöerna använder samma grundstruktur och de scenarier som utspelar sig under övningspassen är automatiserade med hjälp av verktyget SVED[6].

[6] Holm, H. & Sommestad, T. (2016). SVED: Scanning, Vulnerabilities, Exploits and Detection. MILCOM 2016 - 2016 IEEE Military Communications Conference