COMBITECH

Skydd mot informationspåverkan

Försämrat säkerhetsläge och förhöjt terrorhot medför ett ökat behov för alla, verksamheter, att kunna upptäcka, hantera och möta påverkanskampanjer och desinformation.

Informationsmiljön

INFORMATIONSMILJÖN (ENG. INFORMATION ENVIRONMENT, IE) ÄR ETT SÄTT ATT FÖRSTÅ HUR MÄNNISKOR OCH ORGANISATIONER KOMMUNICERAR OCH PÅVERKAR VARANDRA. DEN HJÄLPER OSS ATT SE HUR VI UPPFATTAR VÄRLDEN OCH FATTAR BESLUT BASERAT PÅ DEN INFORMATION VI FÅR.
Informationsmiljön består av tre delar:

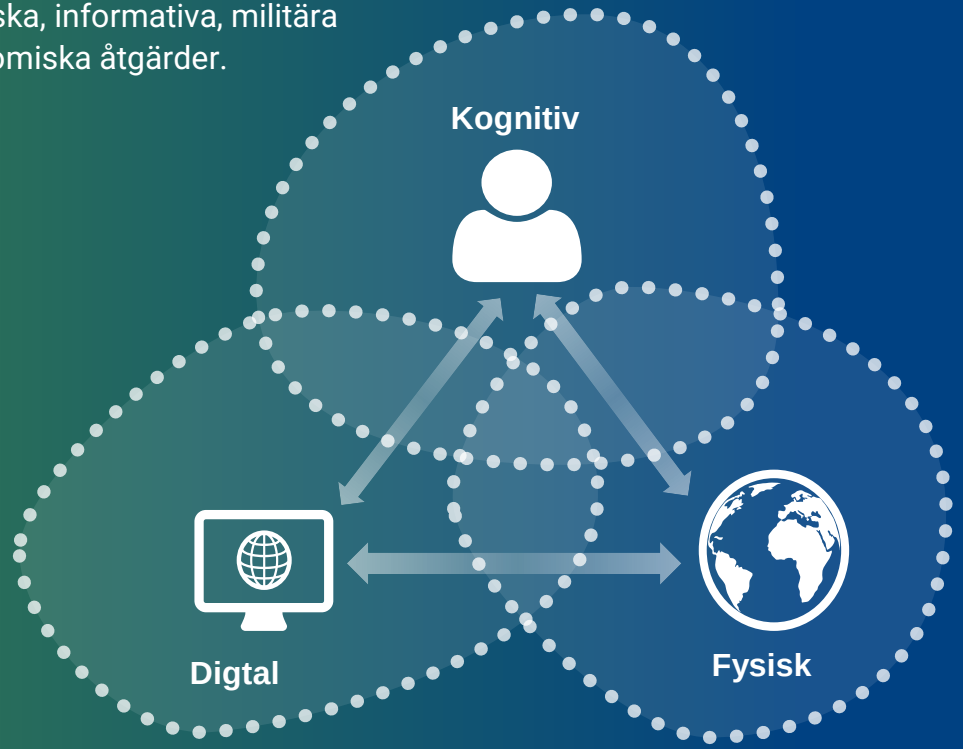
- Kognitiv dimension: Det handlar om hur vi tänker, förstår saker och tar beslut.
- Fysisk dimension: Den omfattar människor, organisationer och den fysiska infrastrukturen som vi använder.
- Digital dimension: Den består av all slags information som vi använder, som fakta, kunskap och data.

Även om informationsmiljön ofta kopplas till mediavärlden, är den mycket bredare. Den tar upp allt från militära ställningstaganden till byggandet av stora projekt som gasledningar. Genom att använda informationsmiljön kan vi förstå hur olika handlingar och händelser kommunicerar meddelanden till människor. Det handlar alltså om mer än bara nyheter och media; det är ett sätt att se på kommunikation och påverkan i stort.

⇒ Analys av informationsmiljön kan hjälpa till att förstå hur hybrida hot utnyttjar sårbarheter, såsom kulturella skillnader eller missnöjen, för att underminera den målinriktade nationen samtidigt som det gynnar den ansvariga aktörens strategiska intressen. Att ta itu med inhemska frågor och bygga samhällelig motståndskraft är en nyckelkomponent i bekämpningen av hybrida hot.

⇒ Alla aktiviteter som en aktör genomför påverkar informationsmiljön och påverkar beslutsfattandet i den kognitiva dimensionen. Samtidigt som information kan vara en möjliggörare för nationell makt, kommer förmågan att påverka publik från samverkan av nationella instrument, inklusive diplomatiska, informativa, militära och ekonomiska åtgärder.

SAMVERKAN AV OLIKA FIENTLIGA ÅTGÄRDER KAN UTNYTTJA SÅRBARHETER ÖVER HELA SPEKTRUMET AV EN MÅLINRIKTAD NATIONS STATSSYSTEM – POLITISKA, MILITÄRA, EKONOMISKA, SOCIALA, INFORMATIVA OCH INFRASTRUKTURELLA (KÄNDA SOM PMESII-SPEKTRUMET). HYBRIDA HOT.



Spelplanen

COMBITECH

Främmande makt

Konspirations-teorier …

Terrorism

Organiserad brottslighet

Vem som helst?

Företag

Bedragare

Pengar

”Frontrunning”

Geopolitik

Underminera

Störa

Övertyga

Skada

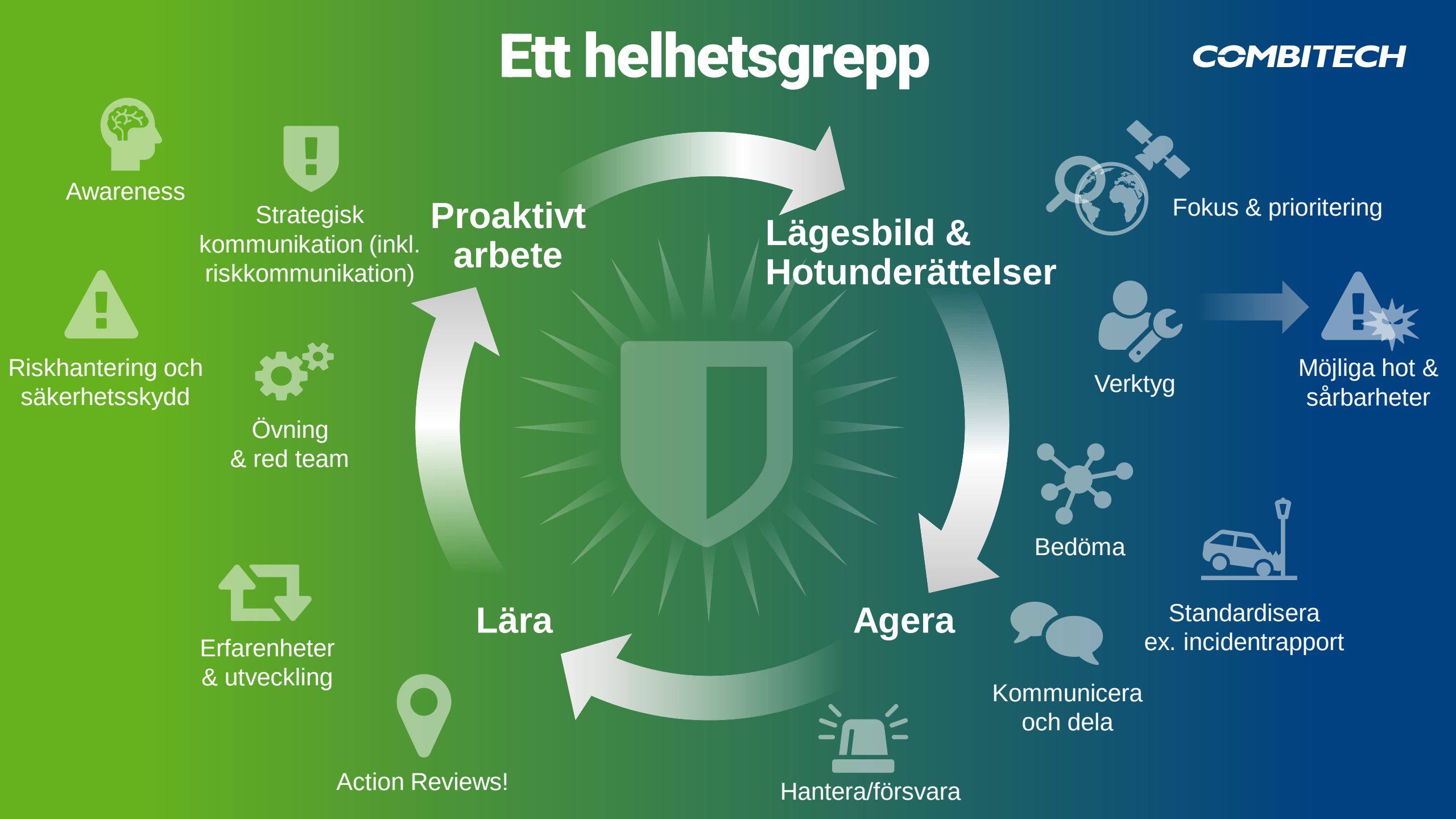
En global industri

COMBITECH

Skydd mot informationspåverkan - verktyg för er!

Ett helhetsgrepp

COMBITECH



Följ kriget med säkrare källor

COMBITECH

KARTOR/GRAFIK

- Follow the Russia-Ukraine Monitor Map – Bellingcat
- Ukraine Interactive map - Ukraine Latest news on live map - liveuamap.com
- Eyes on Russia: The Russia-Ukraine Monitor Map by Cen4infoRes · MapHub

FACT CHECKERS

- #UkraineFacts: fact-checking disinformation about Ukraine's invasion by the IFCN Signatories
- War in Ukraine: the fact-checked disinformation detected in the EU – EDMO - EU
- Reality Check - BBC News - UK
- Kallkritikbyran – Sverige
- Reuters Fact Check – Internationell
- Ukraine Conflict Resource Hub - EU DisinfoLab - EU

Våra favoriter:

Ukraine: Intelligence-Driven Insights (recordedfuture.com)

Våra favoriter:

www.krisinformation.se

Våra favoriter:

#UkraineFacts: fact-checking disinformation about Ukraine's invasion by the IFCN Signatories

ANDRA KÄLLOR/AKTÖRER

- Institute for the Study of War (understandingwar.org) - US
- Oryx (oryxspioenkop.com)
- UI.se | Utrikespolitiska institutet – Sverige
- Läs mer om Ryssland - Totalförsvarets forskningsinstitut – FOI - Sverige
- Tema: Rysk krigföring - Försvarshögskolan (fhs.se) - Sverige
- Homepage | Royal United Services Institute (rusi.org) UK
- EU vs DISINFORMATION – EU
- StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia (stratcomcoe.org)

FOKUS PÅ BARNEN

- Lilla Aktuellt | SVT Barn
- Vår psykolog: Så pratar du med barnen om Ukraina - Rädda Barnen (raddabarnen.se)
- Att prata med barn och unga om krig och kriser - Skolverket

Verktyg för ER

COMBITECH

GRATISUTBILDNINGAR

- Webbutbildning informationspåverkan, MSB
- Training & Vaccine Insights hub, First Draft (Allmän mot olika risker)
- MIK Kunskapsbank
- Fojo Faktajouren
- Bli inte lurad, MPF

Våra favoriter:
Threat Intelligence Blog | Recorded Future

HANDBÖCKER & RAPPORTER

- Att möta informationspåverkan (mpf.se)
- Vägledning för kommunikation under kriser MSB
- Handbok debunking 2020
- The Conspiracy Theory Handbook
- Sveriges Radio Sociala medier
- MSB Faktablad (ABCDE modellen mm.)
- Rättsligt ramverk för bemötande av informationspåverkan (foi.se)
- CORE_comprehensive_resilience_ecosystem.pdf (hybridcoe.fi)

Våra favoriter:
DISARM - Framwork countering disinformation

Våra favoriter:
RESIST Counter Disinformation Toolkit, GCS

OMVÄRLDSBEVAKNING & OSINT

- BBC Monitoring Essential Media Insight
- Samtalet om Sverige , Svenska institutet
- DisinfoDocket
- OSINT Toolkit | Links To Digital Tools Used By Researchers (comskills-ukraine.co.uk)
- Online investigation Toolkit, Bellingcat
- Social Media Monitoring: A Primer, Stratcom
- Social Media Monitoring Tools: An In-Depth Look, Stratcom

SPELA ETT SPEL

- Spot the Deepfake
- Bad News
- Troll Factory
- Go Viral
- Nyhetsvärderaren (nyhetsvarderaren.se)

Prenumerera på Anton Lif nyhetsbrev!

MITT digitala fotavtryck

Roller och intressen

Privat och på jobbet. Vilka behörigheter och tillstånd har jag? Digitala och fysiska. Vilka behörigheter och tillstånd har jag delat ut till andra?

Intressen, hobbys – djur, idrott, kultur, resa, friluftsliv osv.

Medlemskap

Medlemskap, lojalitets-program, abonnemang, streamingtjänster, familjemedlemmars abonnemang.

”Spela djävulen”

– hur kan denna info användas för att påverka dig?

Min egen berättelse

Vad delar jag i olika nätverk. Vilka beteenden har jag? Profil på Facebook, Instagram, LinkedIn mm. status-uppdateringar, incheckningar.

”goggla” dig själv

INFORMATIONSLÄCKAGE

[Är min mejladress säker? (sakerhetskollen.se)]

Andras berättelse

Vad delar vänner och familj om mig? Vad delar din kollega, dotter, granne …
I vilka sammanhang och miljöer dyker jag upp? Bilder, album, inlägg, status-uppdateringar, incheckningar …

”Osynliga spår”

Positionsdata – karttjänster, appar. Stänger jag av Wifi, Bluetooth? Mobildata, Smarta prylar.

Rapportera – 8 frågor

COMBITECH

Kort beskrivning av händelse och informationen

1) **Hur upptäcktes händelsen?**
   I vilket forum/media?
2) **Varför misstänker ni att det har koppling till en antagonist?**
3) **Går det att identifiera ett syfte bakom informationen?**
4) **Går det att se några tydliga effekter redan nu av informationen?**
5) **Hur stor är spridningen?**
6) **Hur påverkar händelsen organisationens förmåga att utföra ert uppdrag?**
7) **Hur påverkar händelsen aktörer som är beroende av ert uppdrag, och/eller den generella allmänheten?**
8) **Har åtgärder vidtagits? Hur och varför?**

CYBERSÄKERHET - tips för att säkra upp

COMBITECH

- Inventera din verksamhets tillgångar. **Identifiera ”guldäggen”.**
- Kartlägg **möjliga hot och hotaktörer**.
- Få en överblick av informationsflödena.
- Ta reda på vilka tjänster som exponeras mot internet.
- Säkra upp IT-miljön genom att uppdatera systemen och göra sårbarhetsscanners. **Skapa möjlighet att snabbt kunna stänga ned system**.
- Var uppmärksam på **förändringar och avvikande trafikmönster i IT-miljön**. Undersök det som avviker och ta reda på vad som är orsaken.
- Etablera en **förmåga att upptäcka och hantera incidenter och avvikelser.**
- Följ standarder och de regelverk som finns för din verksamhet, för att få en stabil grund.
- Utbilda medarbetare inom cybersäkerhet. Det är ett effektivt sätt att höja riskmedvetenheten.
- Informera alla medarbetare om hur de **rapporterar** något misstänkt.
- Till dig som person; ha **ett långt och komplext lösenord**. Använd aldrig samma lösenord på mer än ett ställe. Ha alltid olika lösenord, både i arbetet och privat. Använd tvåfaktorsautentisering. **Byt lösenord om något händer**.
- Använd inte din arbetsmail för privata tjänster och sociala medier.
- Tänk på vilken information du exponerar och för vem. Likaså vad du delar i olika kanaler. För en verksamhet gäller samma sak. **Det handlar om att minimera risken för exponering.**

COMBITECH

Skydd mot informationspåverkan - Combitech

Exempel på tjänster

Föreläsning och rådgivning

Utbildningar (ex. allmän, syntetisk media, risk-kommunikation eller OSINT)

Övning, spel och **workshop**

Analys och **utredning,** (ex. exponeringsanalys, hotbildsanalys).

RSA- och **säkerhetsskyddsarbete** (ex. Red Team Testing)

Omvärldsbevakning, scenarioanalys och framsyn

Strategiarbete (ex. varumärke, försvarsvilja, säkerhetskultur).

Utvärdering (ex. Gapanalys, mognadsbedömning)

Operativt stöd,
(ex. incidenthantering & kriskommunikation)

Verksamhetsanpassade filmer

Table-top och simuleringsövningar

Utredningar och omvärldsbevakning

MED UTGÅNGSPUNKT I ER VERKSAMHET

Framsyn – ett proaktivt helhetsgrepp

COMBITECH

”Seven step forecasting funnel”

1-3) Analys

4) Scenario

5) Spel

6) Planering

7) Åtgärder

Innehåll/ambition

Hotbilds/omvärldsanalys

Utgångspunkt i verksamheten. Inkl. ex exponeringsanalys.

Rapport

Scenarioanalys

Innehåll: baserade på hotbilds/omvärldsanalys

Spel

Table-top,
Målgruppsanpassat

Webinar

Exempelvis Introduktion, fördjupning

Strategisk rådgivning

Stöd med ex mognadsgrad, implementering i RSA eller säkerhetsskyddsplan. Övning/utbildningsplan. Kommunikationsplan

Uppföljning

Återkoppling och kompletterande träning

Mål

Stärkt förmåga

- Ökad förståelse för hotbilden
- Planerings/ övningsunderlag
- Gap-analys
- Åtgärder

Aktivitetsplan + Syntes

COMBITECH

Shaping a smart and resilient society