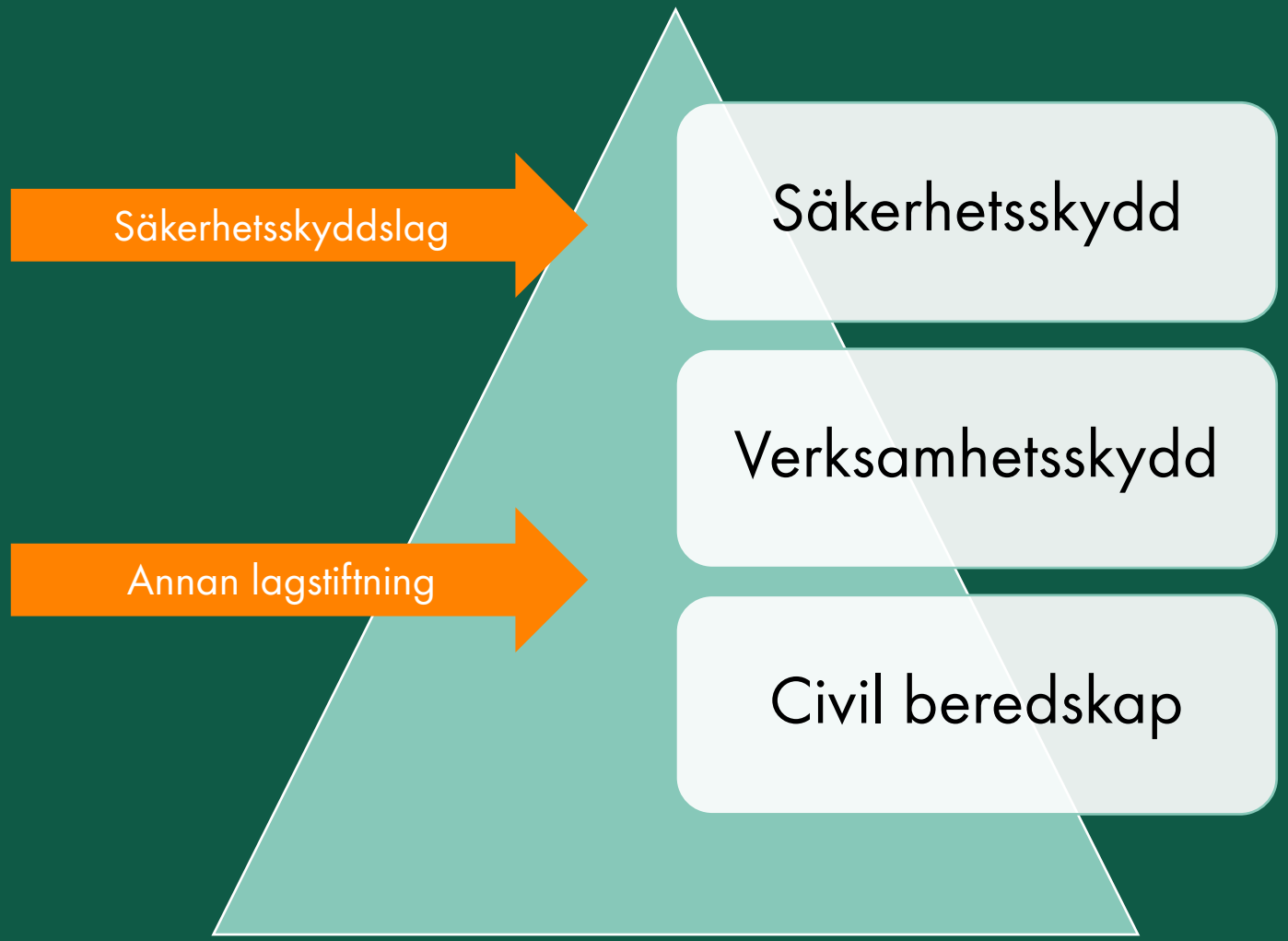
Security – ett lagspel

Terje Steisjö

ELLEVIO

Ellevios säkerhetsorganisation



Säkerhetskänslig verksamhet
Betydelse för Sveriges säkerhet

Verksamhet som inte är säkerhetskänslig men som behöver ett skydd från delvis andra utgångspunkter och krav i annan lagstiftning.

Ellevio säkerhetsorganisation

Funktionsområden och personal

- Säkerhetsskydd
  - Säkerhetsskyddssamordnare
  - Säkerhetsskyddsspecialister
  - Säkerhetsskyddsadministratör
- Verksamhetsskydd
  - Fysisk säkerhetsspecialist
- Civil beredskap
  - Beredskapssamordnare
  - Säkerhetssamordnare

- Personalsäkerhet
- Säkerhetsskydds-avtal
- Säkerhetsskydds-bedömningar
- Utredningar
- Kontroll av säkerhetsskydd

- Fysisk säkerhet
- Personsäkerhet
- Driftsäkerhet
- Utredningar
- Kontroll av verksamhetsskydd

- Krisberedskap
- Beredskaps-åtgärder
- Utbildning

Vad är säkerhetsskydd?

”Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spioneri, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskydds-klassificerade uppgifter.”

1 kap. 2 § första stycket
säkerhetsskyddslagen (2018:585)

ELLEVIO

Ett förändrat omvärldsläge

ELLEVIO

”Vi befinner oss i ett allvarligt omvärldsläge där Sveriges interna säkerhet påverkas av skeenden utanför våra gränser”

Magnus Krumlinde,
biträdande säkerhetspolischef

ELLEVIO

Säkerhetshot mot Sverige och utpekade sektorer

Energisektorn

- Cyberhot
- Skadegörelse och sabotage
- Informationsinsamling
- Uppköp av fastigheter
- Utkontraktering och osäkra leverantörskedjor
- Gråzonsproblematik och väpnat angrepp

Transportsektorn

- Intrång och störningar kan drabba anläggningar och system
- Säkerhetsrisker vid upphandling
- Infiltration och rekrytering av insiders
- Underrättelseinhämtning

Telekominfrastruktur

- Cyberhot
- Driftstörning/bortfall på grund av elavbrott
- Underrättelseinhämtning
- Skadegörelse och sabotage mot infrastruktur

ELLEVIO

Ryssland

- Ryssland använder sig i princip av alla inhämtningsdiscipliner
  - Personbaserad inhämtning
  - Signalspaning
  - Bildunderrättelse
  - Öppna källor
- Krigsförberedelser
- Strategiska uppköp
- Värvning av källor och insiders
- Cyberangrepp

ELLEVIO

Hotbild för elförsörjningen

- Cyberhot
  - Riktade cyberattacker mot energisektorn och kritisk infrastruktur
- Fysisk skadegörelse och sabotage
  - Förstörelse av fysiska delar i elnätet
  - Stölder och inbrott
- Informationsinsamling
  - Personbaserad informationsinhämtning
  - Teknisk inhämtning
- Uppköp av fastigheter och mark
  - Mark eller sjöområden
  - Fastigheter nära viktiga elanläggningar
  - Avlyssning och störa kommunikationstrafik för elsystemet
- Utkontraktering och osäkra leverantörskedjor
  - Stort beroende av entreprenörer och leverantörer
  - Tillhandahåller verksamhetskritiska tjänster/komponenter
- Gråzonsproblematik och väpnat angrepp
  - Varken krig eller fred = gråzon
  - Väpnat angrepp = militära våldsmedel
  - Elförsörjningen måltavla vid väpnat angrepp

ELLEVIO

Frågor?

ELLEVIO

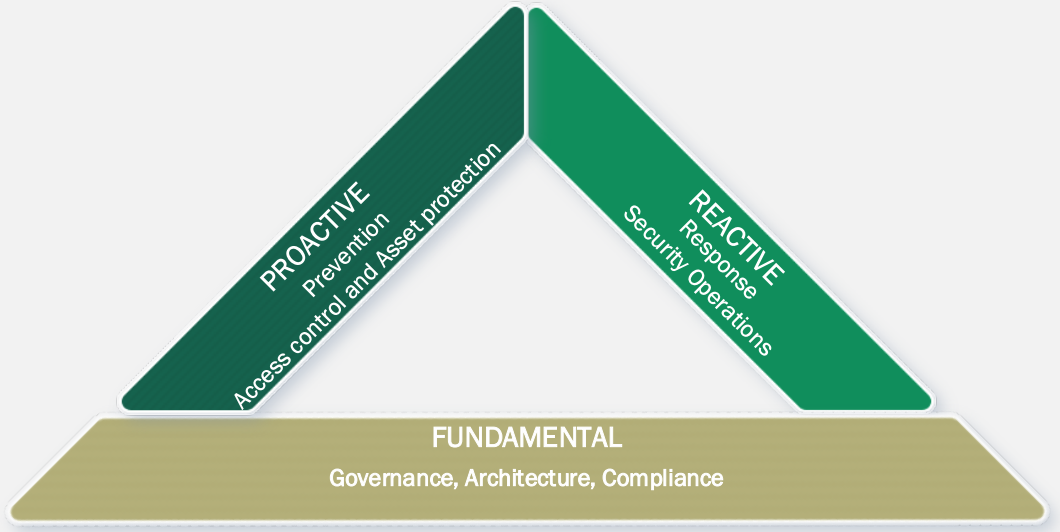
Information & Cyber Security

Thomas Widén

ELLEVIO

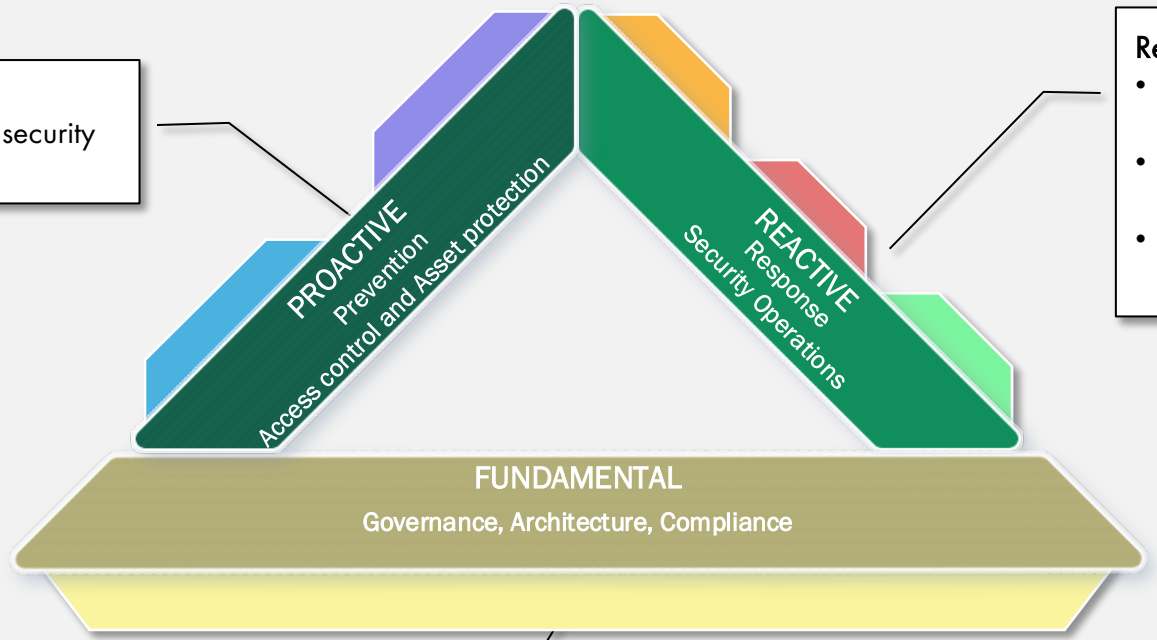
Objective – Information & Cyber Security

Säkerställ att Ellevios ramverk för säkerhet innehåller och upprätthåller proaktiva principer för cybermotståndskraft, prioriterar snabb cyberincidentrespons och upprätthåller strikta standarder för efterlevnad av lagar och förordningar.



Arbetsmodell

Proactive Cyber Security
- Continuously report on and improve the security posture of the organization

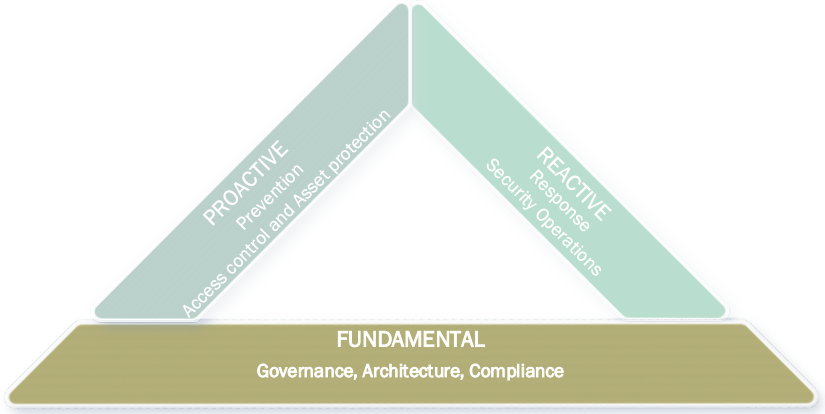


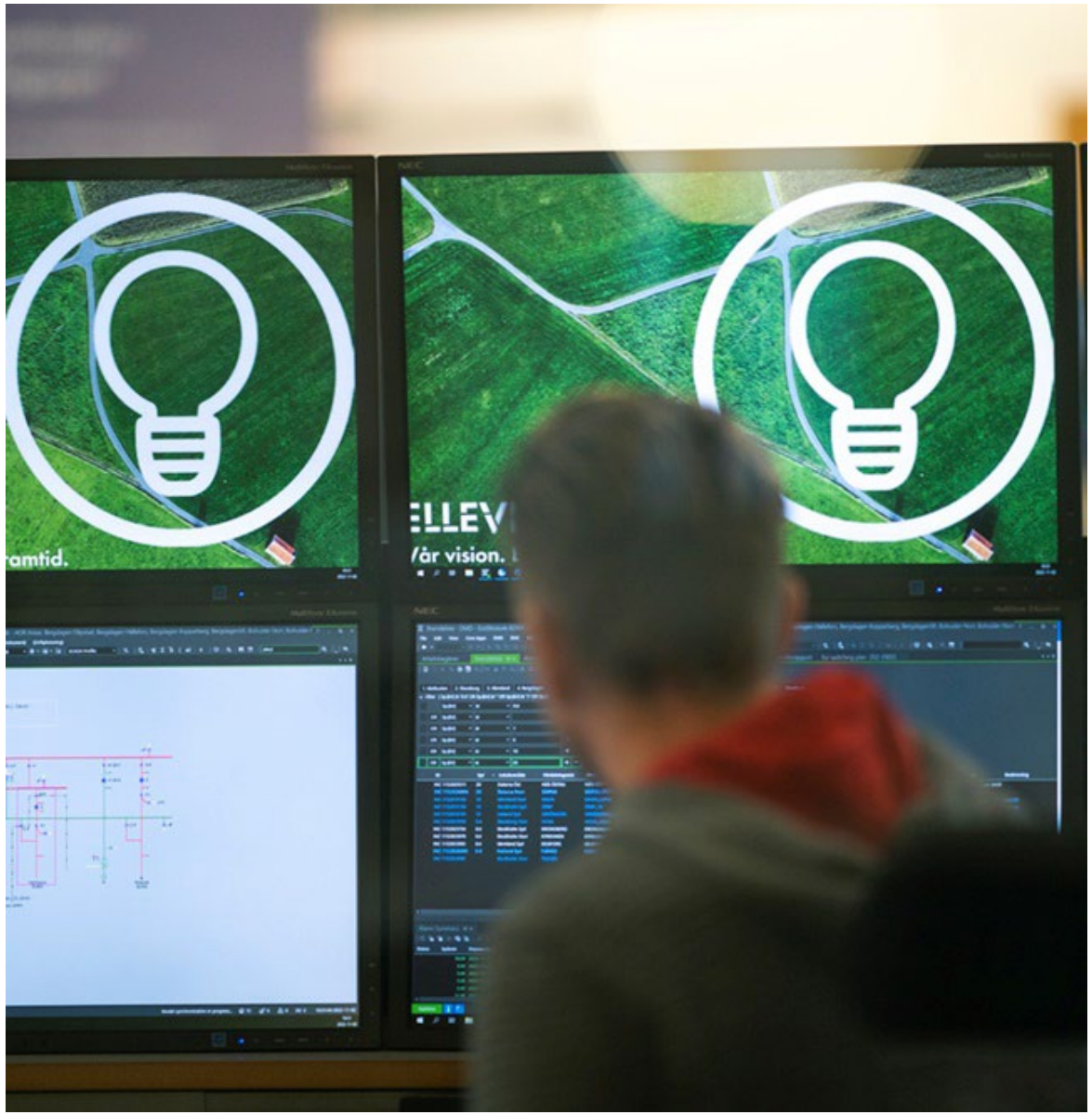
Reactive Cyber Security
- Detect, responding and recover from active attacks on enterprise assets.
- Build process maturity and muscle memory in a security perspective
- Provide context and actionable insights on active attacks and potential threats

Fundamental Cyber Security
- Evolve governing structure such as policies, security strategy, instructions, guidelines and requirements
- Translate business and assurance goals into guidelines for technical security decisions.
- Measure compliance and evolve the compliance framework

Fundamental

- Ramverk för Information och cybersäkerhet
- Systemklassificering
- Säkerhetsarkitektur
- IT-risk and Regulatorisk efterlevnad

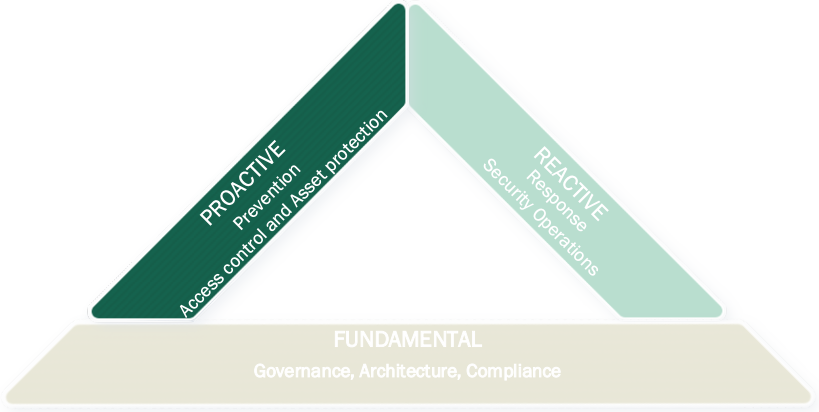


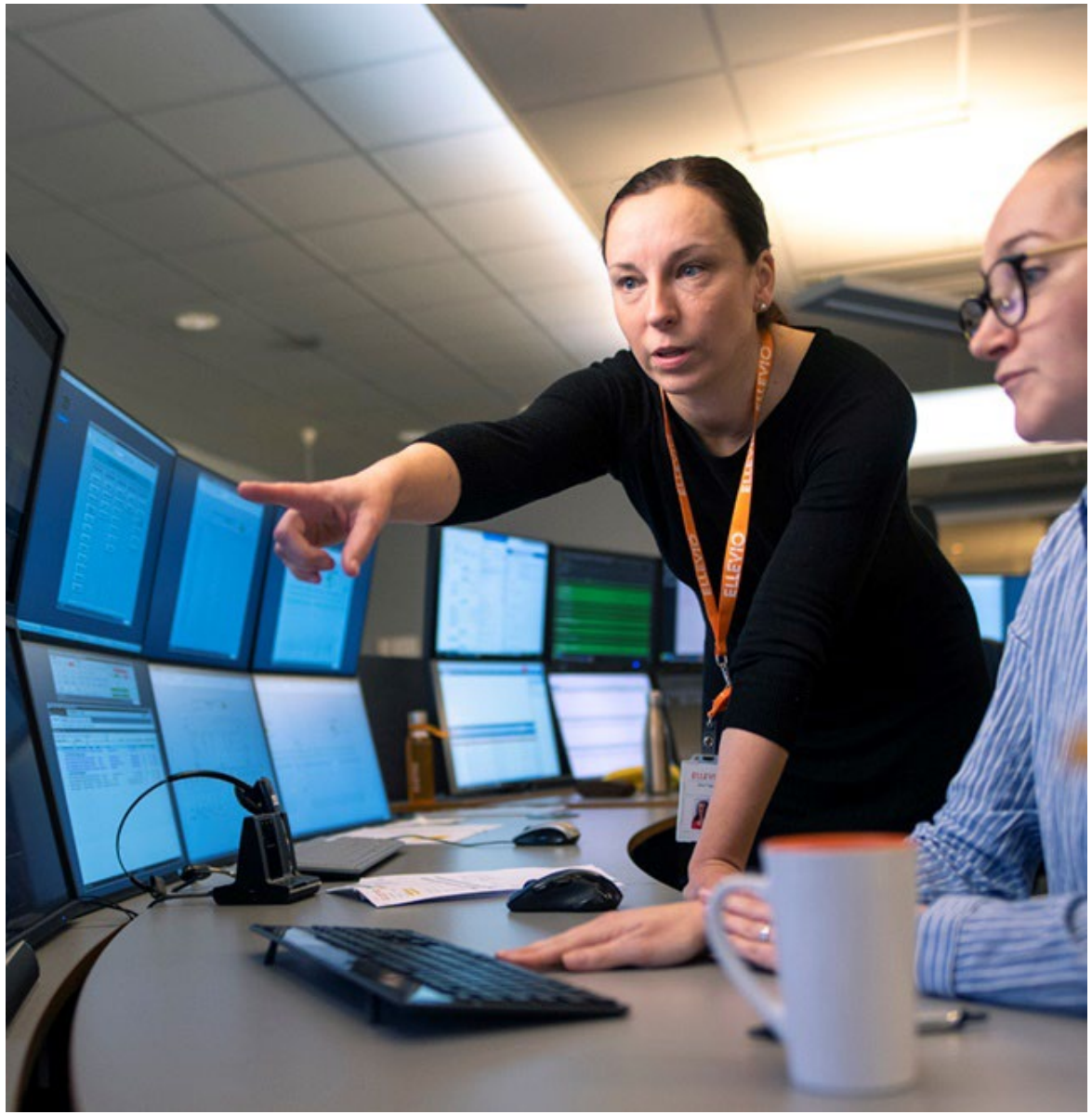


ELLEVIO

Proactive

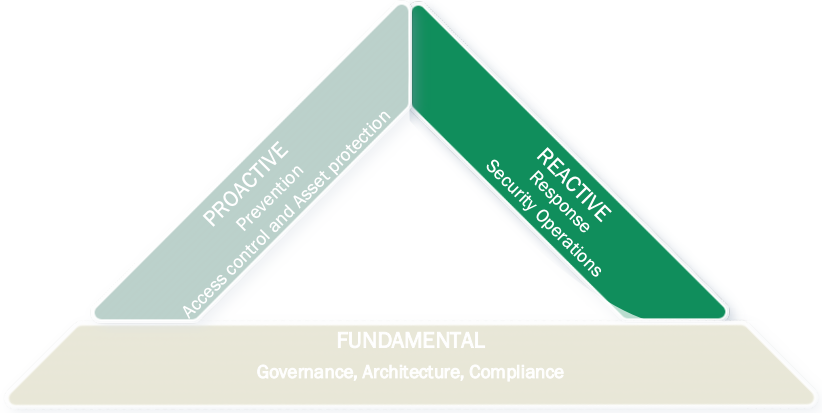
- Förstärkning av cybermotståndskraft
- Träning och utbildning
- Inköpsstöd
- Rekommendation och Sårbarhetshantering
- Säkerhetshandledning
- Mätning av säkerhetsmognadsgrad

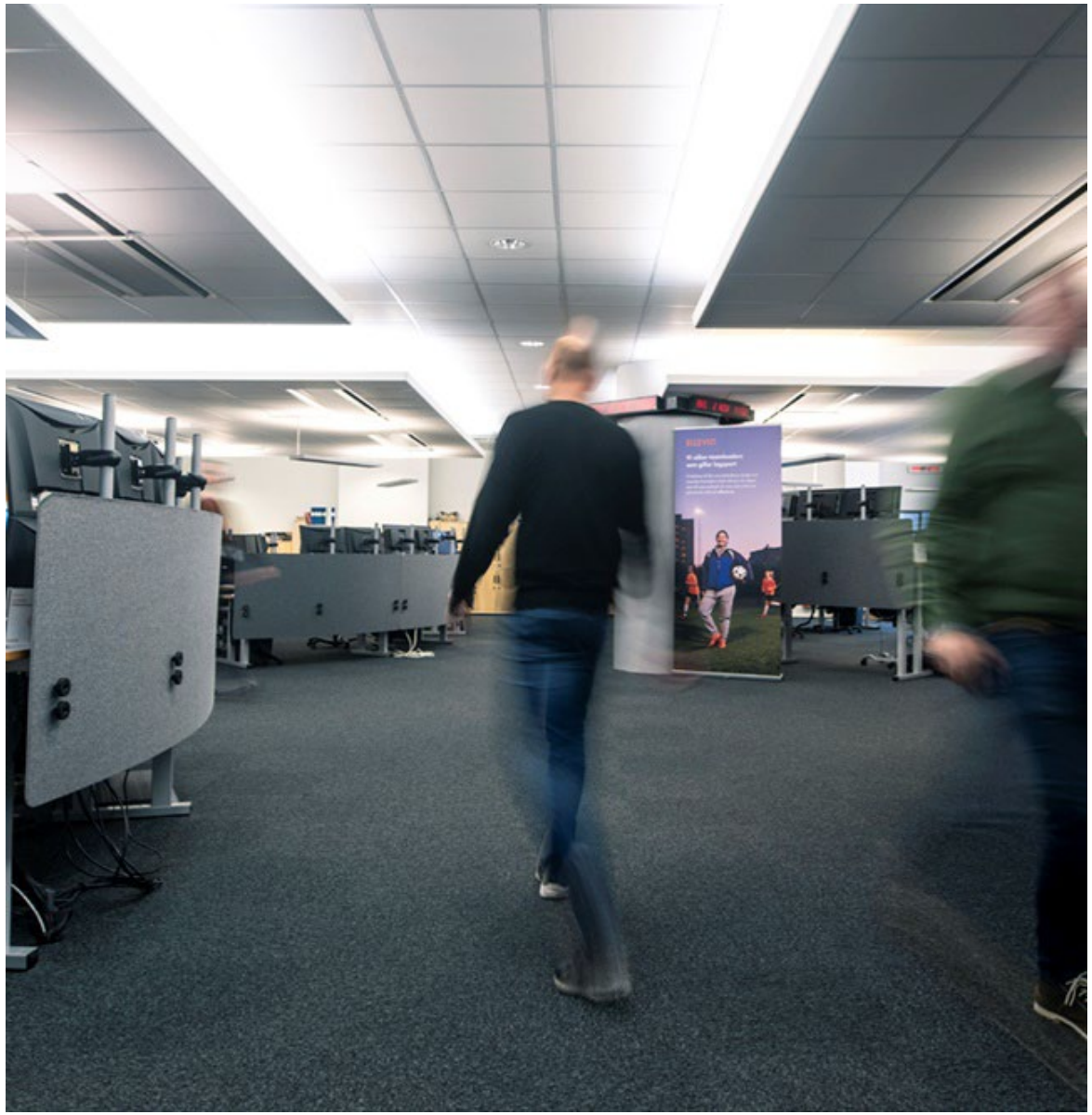




Reactive

- Upptäck och reagera på cyberattacker
- Omvärldsbevakning
- Hotsökning
- Forensisk analys
- Övningar och tester





ELLEVIO

Säkerhet är en lagsport

Exempel på gemensamma områden

- Omvärldsbevakning
- Hot och risk modellering
- Delning av angrepps information (MISP)
- Informationsdelning and analys
- Principer för automatisk respons
- Automatisk rapportering

ELLEVIO

Gruppdiskussioner:
Säkerhetsskydd vid deltagande inom säkerhetskänslig verksamhet

Bakgrund: Som verksamhetsutövare bedriver vi på Ellevio en säkerhetskänslig verksamhet och anlitar er som entreprenörer för att delta i denna verksamhet.

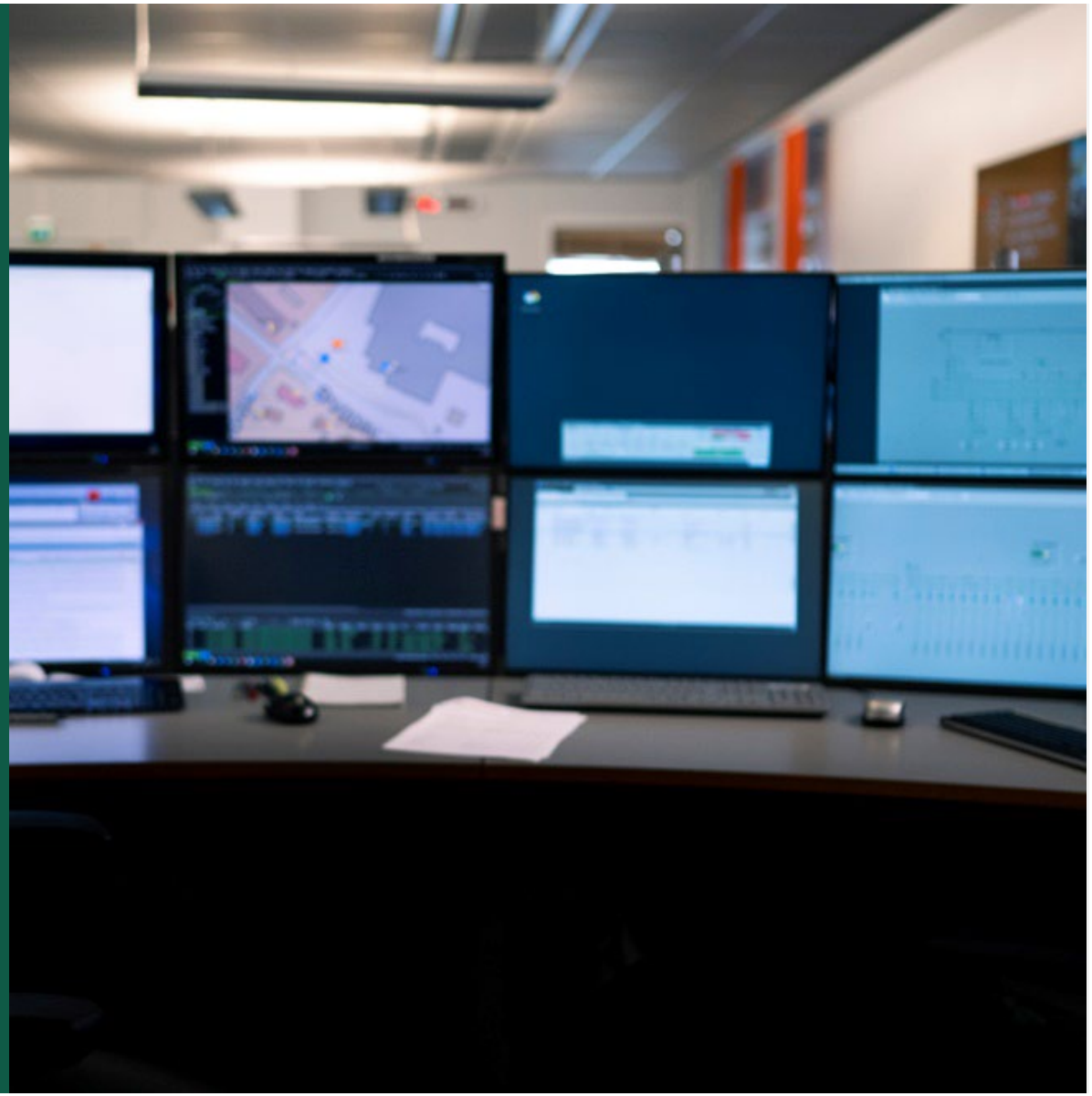
Det är av yttersta vikt att vi säkerställer att all känslig information hanteras på ett säkert sätt och att endast behöriga personer har tillgång till denna information samt tillträde till säkerhetskänslig verksamhet.

Detta inkluderar att genomföra säkerhetsprövningar av personal, implementera tekniska skyddsåtgärder och utbilda anställda i säkerhetsskydd.

ELLEVIO

Gruppdiskussion:
Frågeställningar

- Vilka steg bör vi som verksamhetsutövare och ni som entreprenörer ta för att säkerställa att vi uppfyller kraven enligt säkerhetsskyddslagen?
- Hur kan vi tillsammans genomföra effektiva säkerhetsprövningar av personalen som deltar i den säkerhetskänsliga verksamheten?
- Vilka tekniska skyddsåtgärder bör vi implementera för att skydda den känsliga informationen?
- Hur kan vi skapa en säkerhetsmedveten kultur bland alla anställda och entreprenörer som deltar i verksamheten?
- Vilka är de potentiella riskerna om vi misslyckas med att implementera tillräckliga säkerhetsskyddsåtgärder?

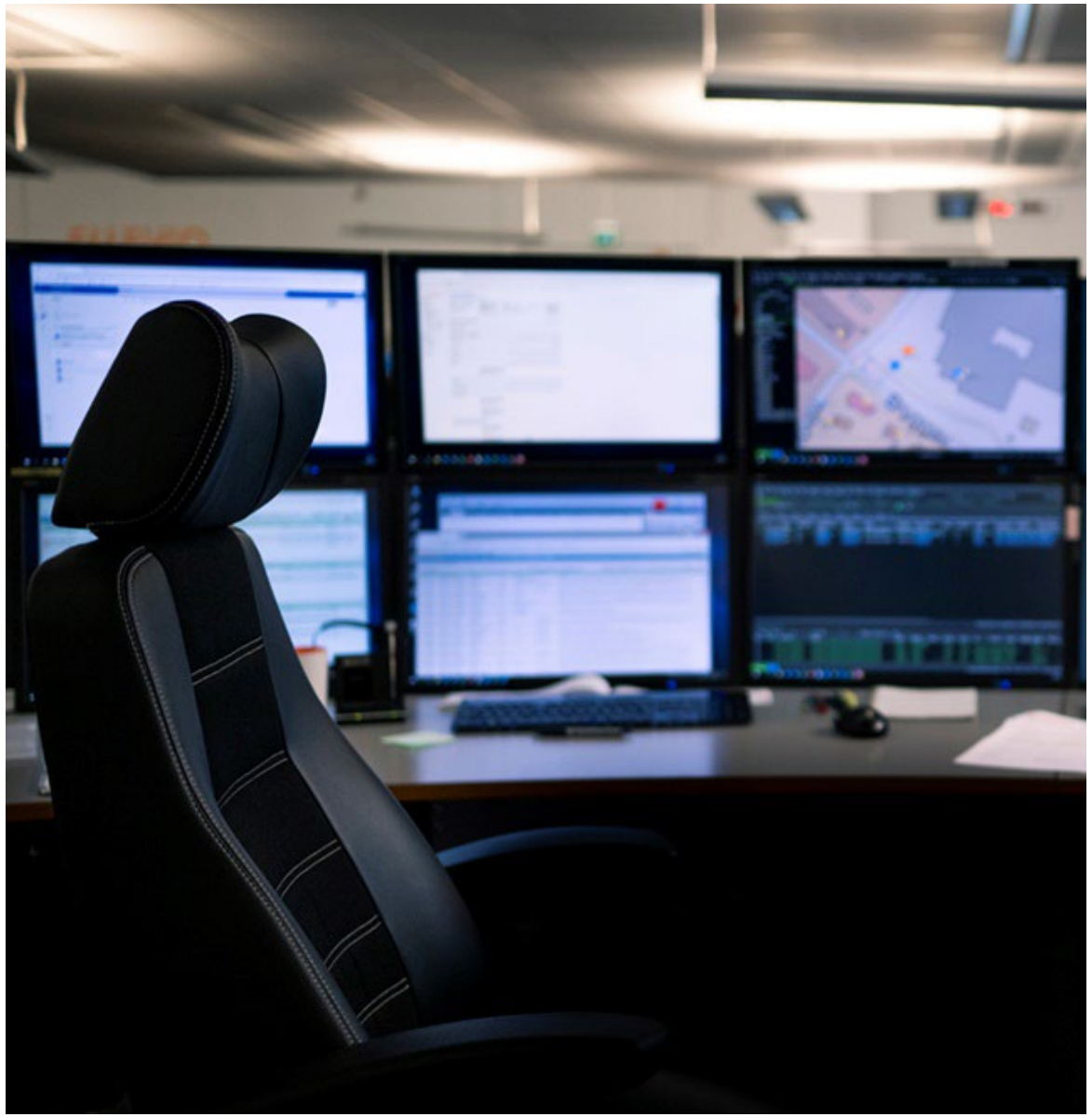


Case

Supplychain-attack

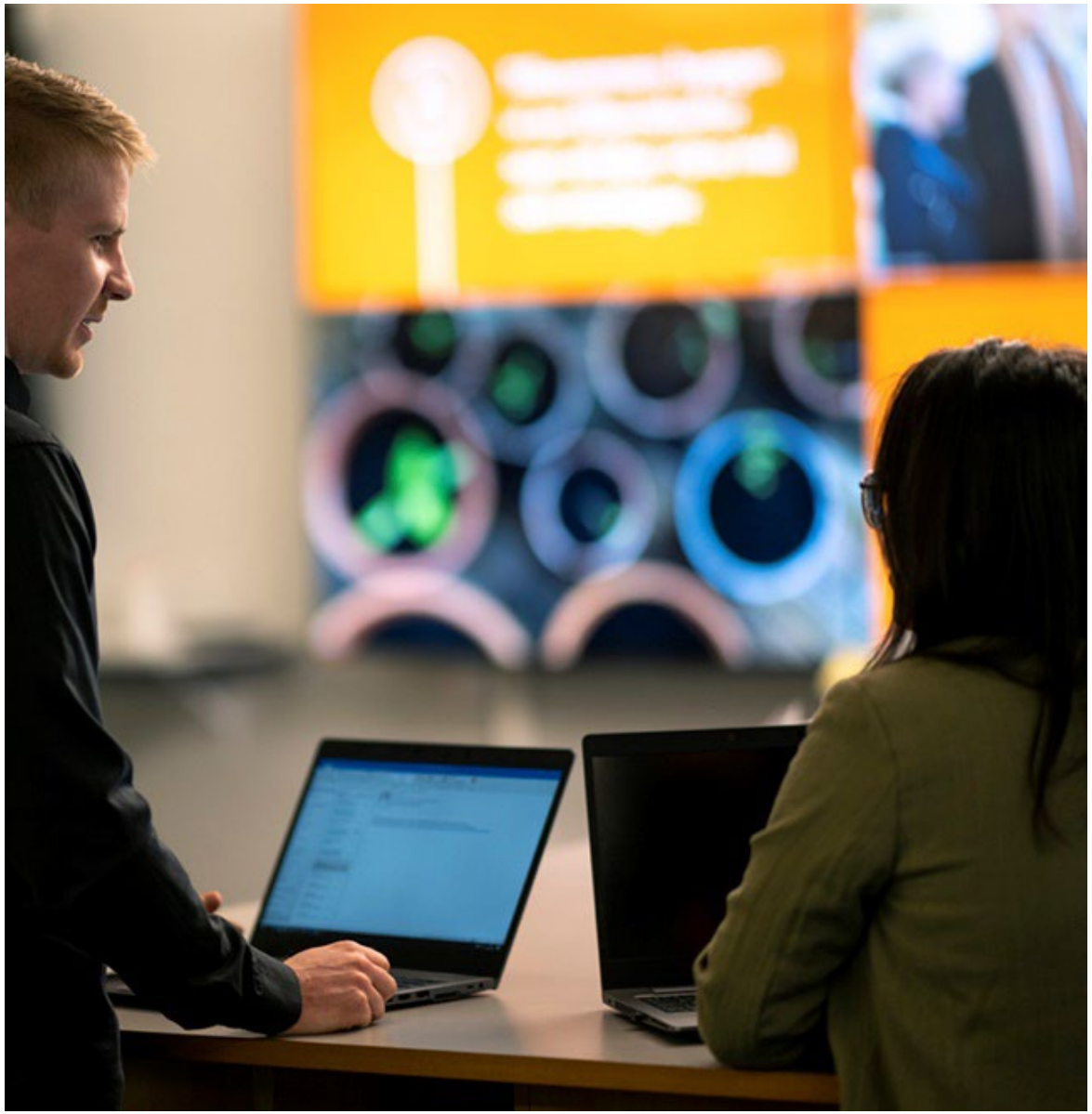
En angripare använder underleverantör till entreprenör för att angripa Ellevio:

- Exempel: Attacken 2024 mot TietoEvry där en IT-leverantör blev övertagen.



Frågor att diskutera

- Hur jobbar vi bättre ihop i händelse av ett angrepp?
- Hur och när ska vi informera varandra?
- Vilken information avseende incidenter förväntar ni er av oss?
- Vilken typ av information kan vi dela fritt mellan oss i händelse av en incident?



Utvärdering menti.com 1527 5027

Svara om du vill – klicka på ”skicka” för att komma vidare.

Tre frågor:
Var tar du med dig?
Förbättringsförslag?
Utvärdering

ELLEVIO