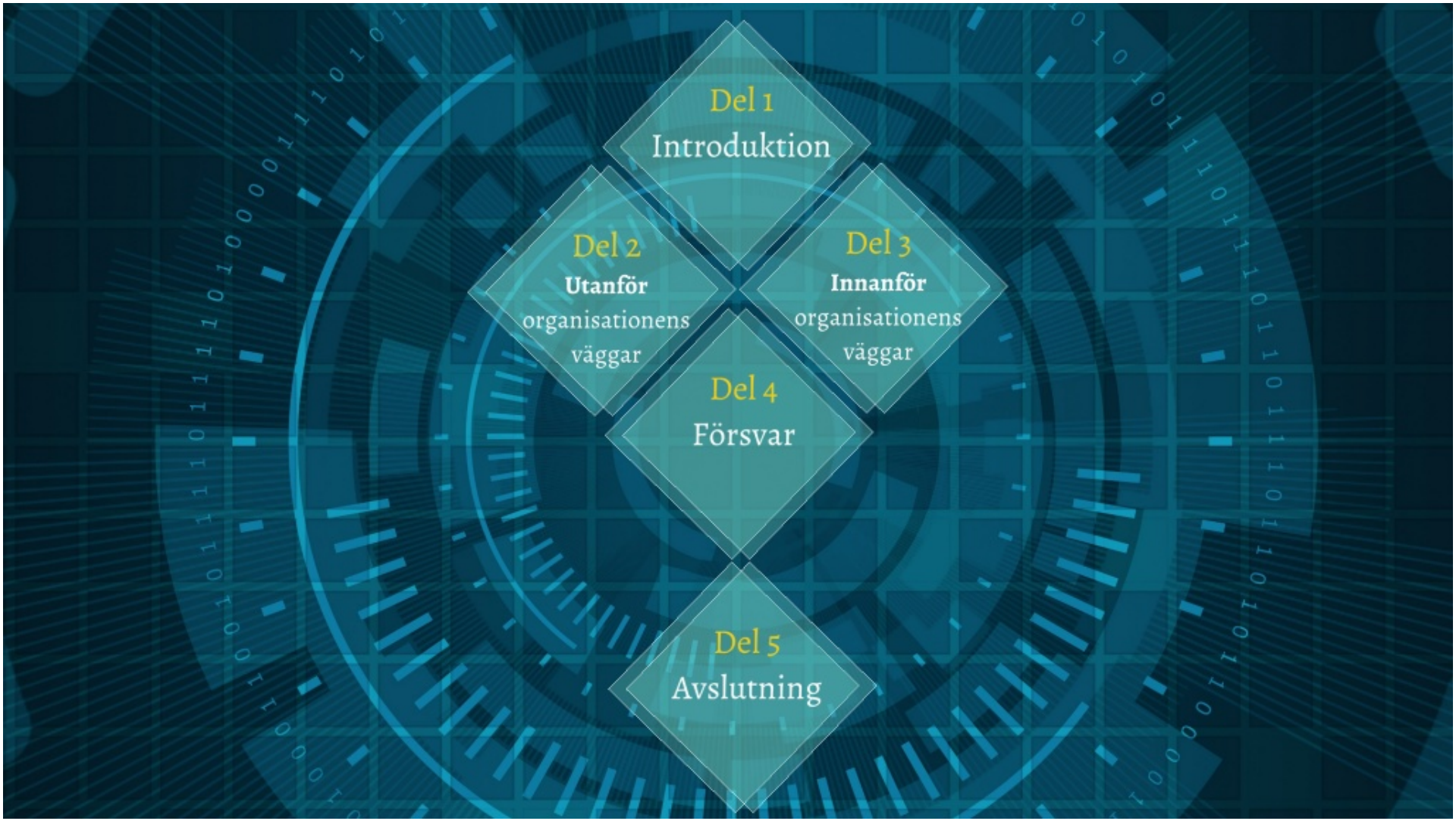
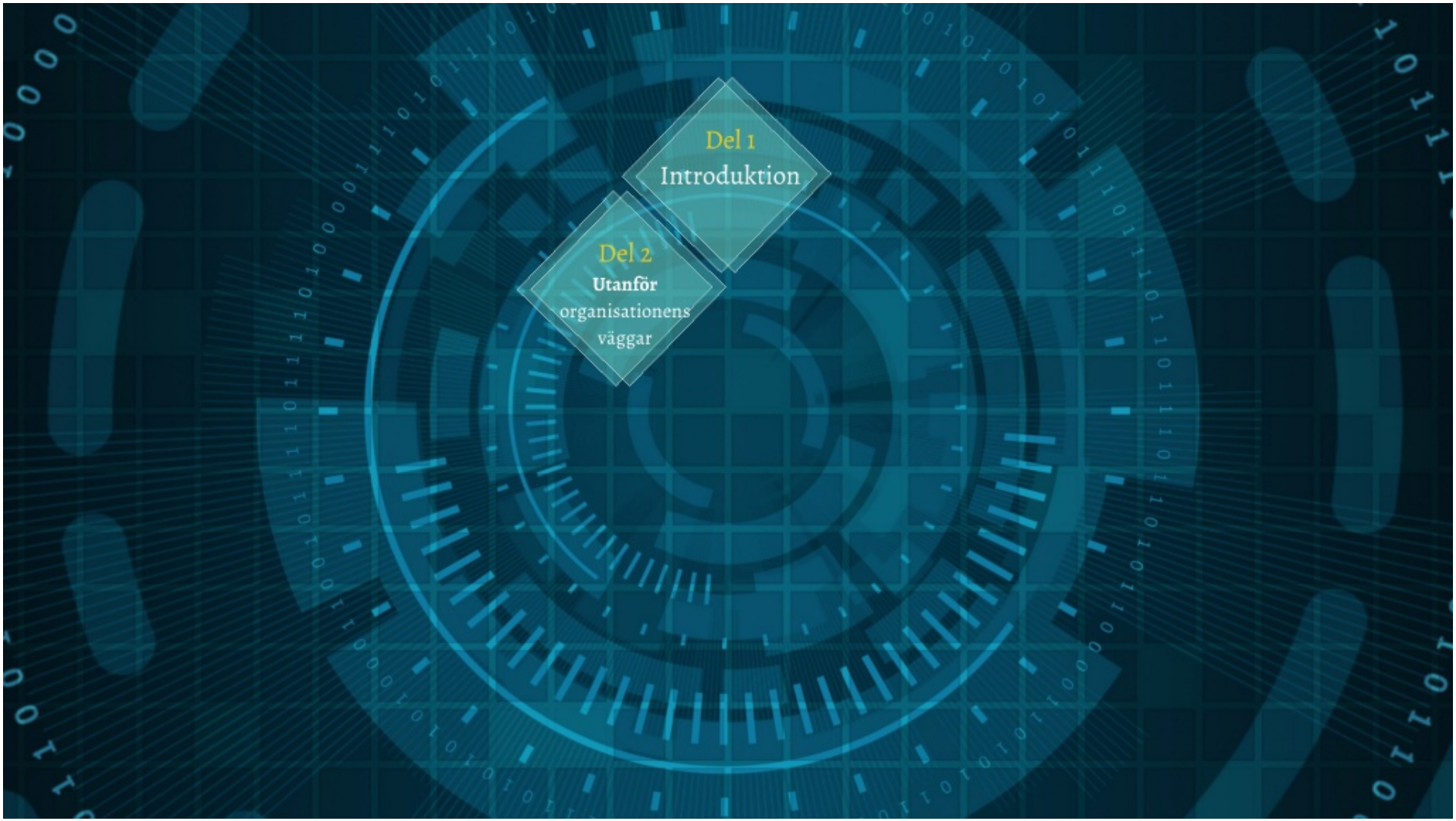

En resa genom
Cyberangreppet
från angriparens perspektiv
av
Christoffer Strömblad
Polismyndigheten


Del 1
Introduktion
Del 2
Utanför
organisationens
väggar
Del 3
Innanför
organisationens
väggar
Del 4
Försvar
Del 5
Avslutning


Del 1
Introduktion

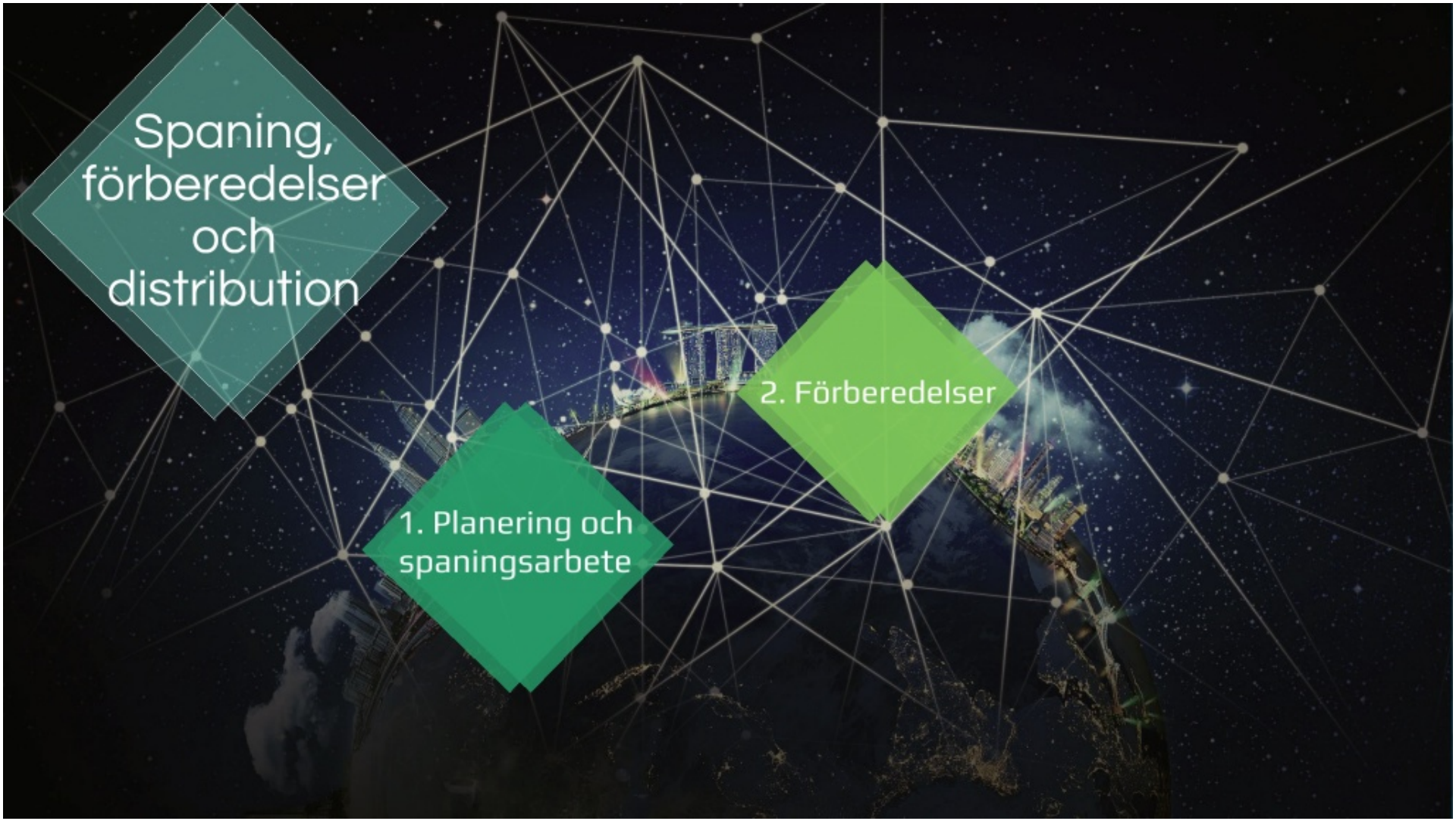

Introduktion
Om föreläsningen
1. Följa ett cyberangrepp
Fiktivt angrepp
2. Förstå förloppet
Faserna och aktiviteterna
3. Skyddsåtgärder
Neka, lura, fördröja...

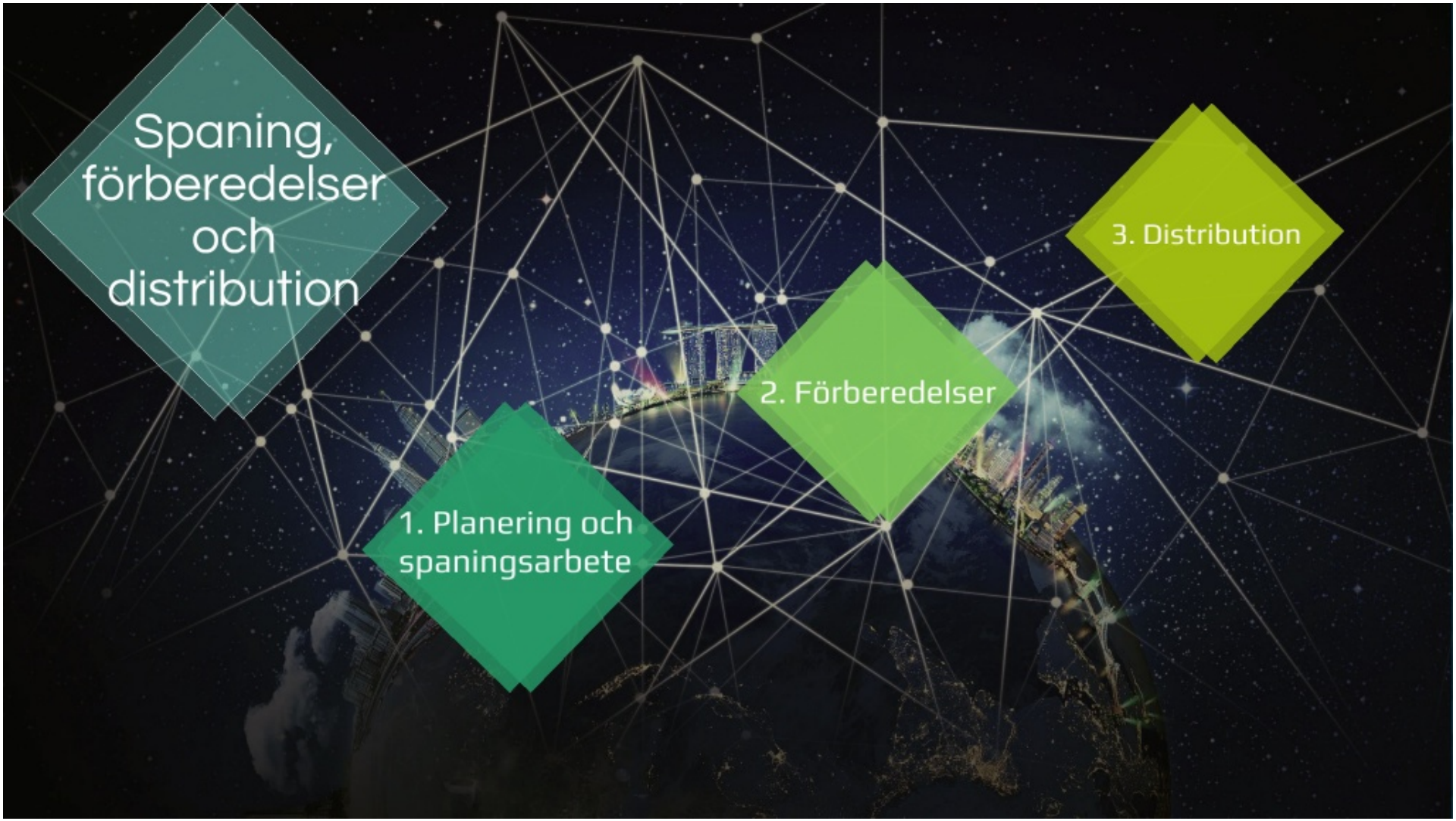

Del 1
Introduktion


Del 1
Introduktion
Del 2
Utanför
organisationens
väggar

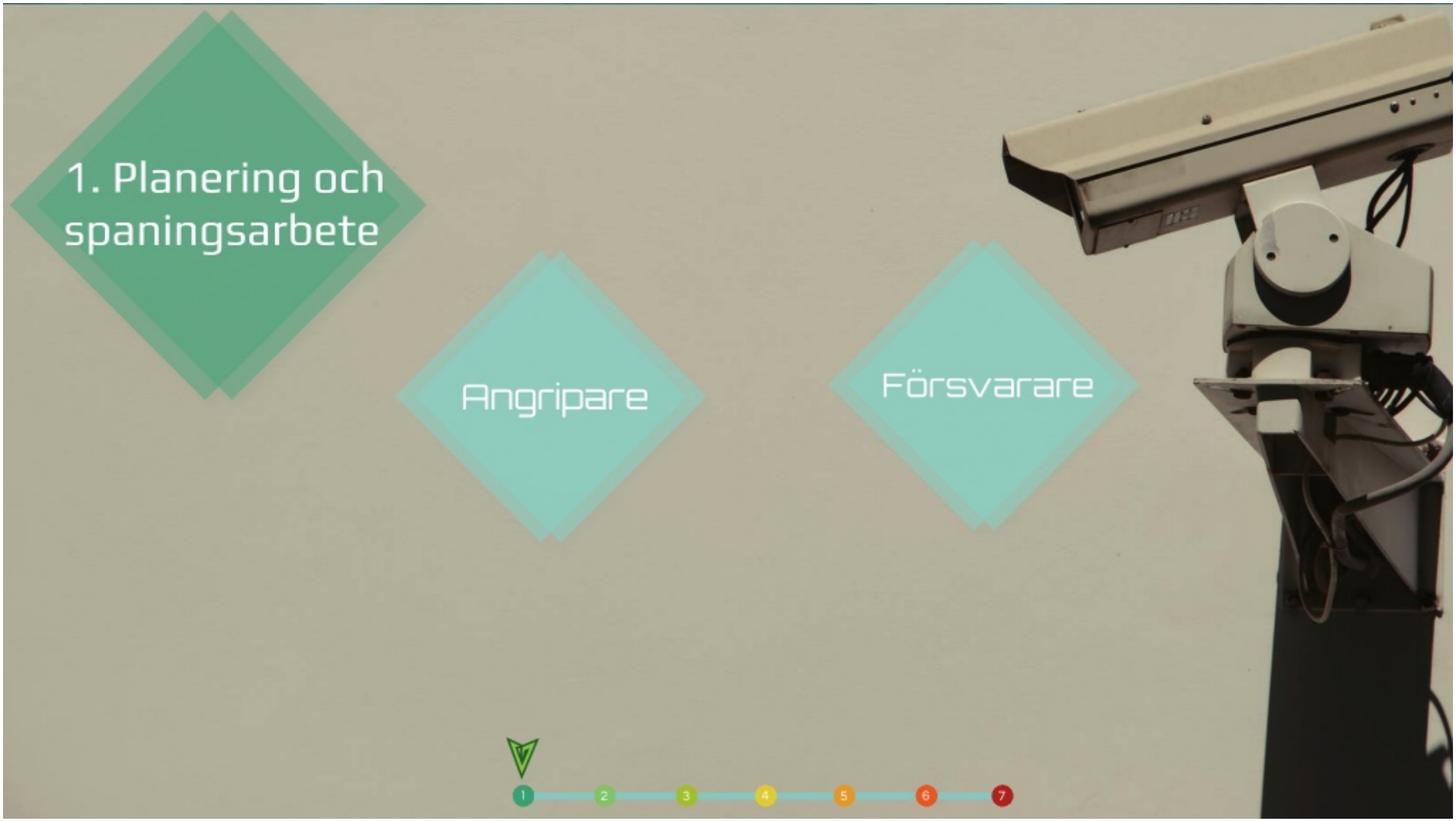

Spaning,
förberedelser
och
distribution

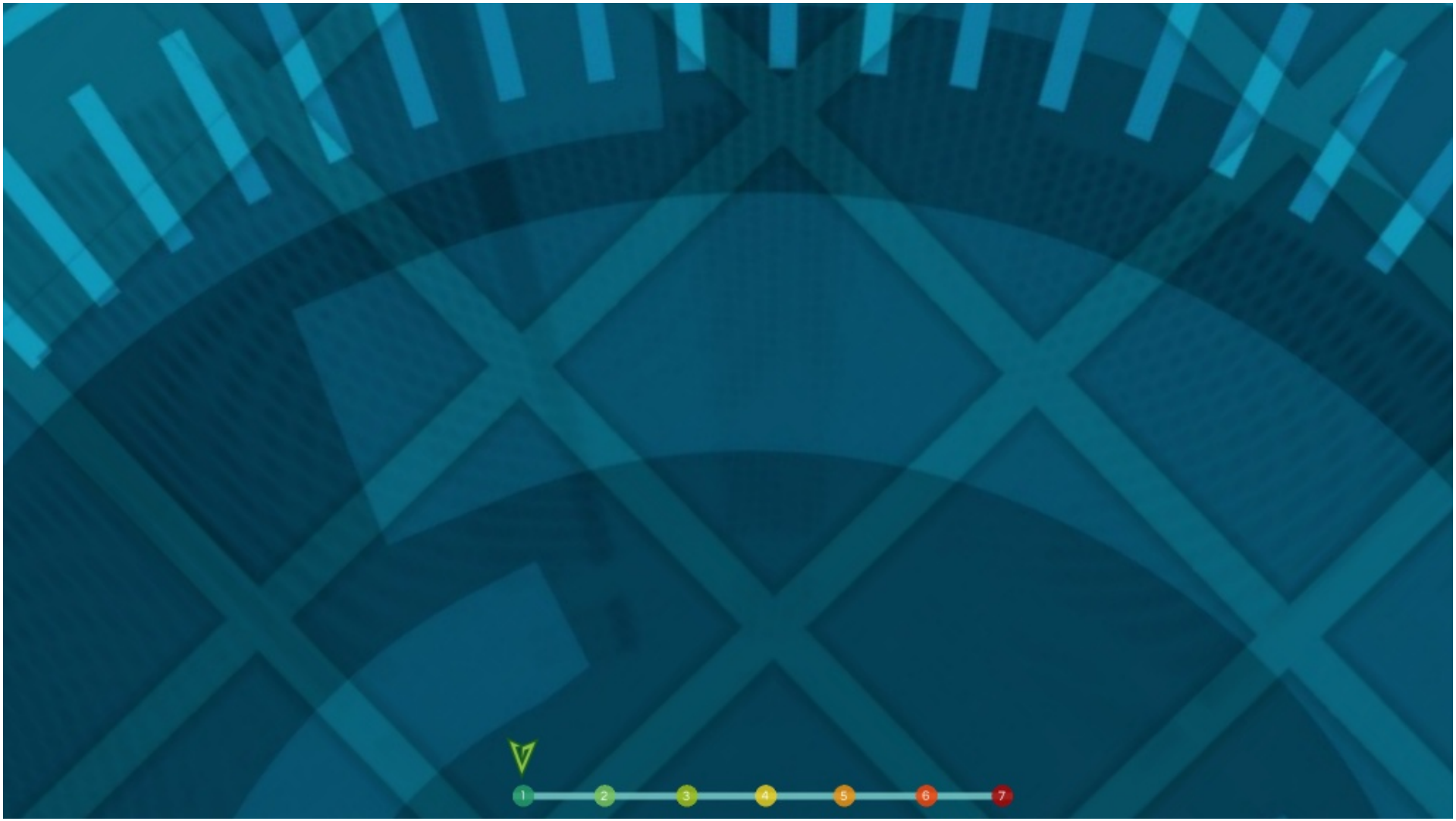

Spaning, förberedelser och distribution
1. Planering och spaningsarbete

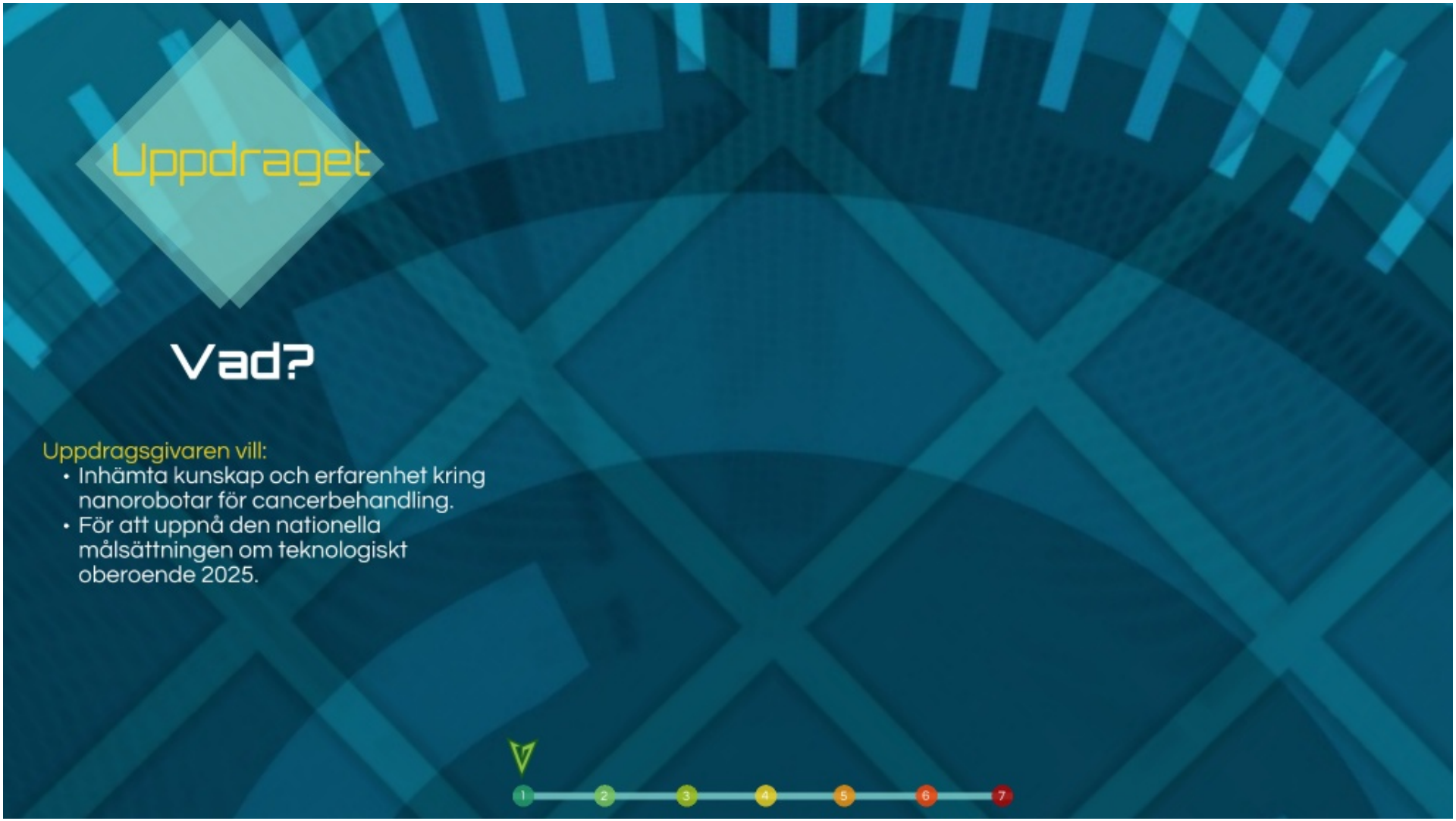

Spaning, förberedelser och distribution
2. Förberedelser
1. Planering och spaningsarbete

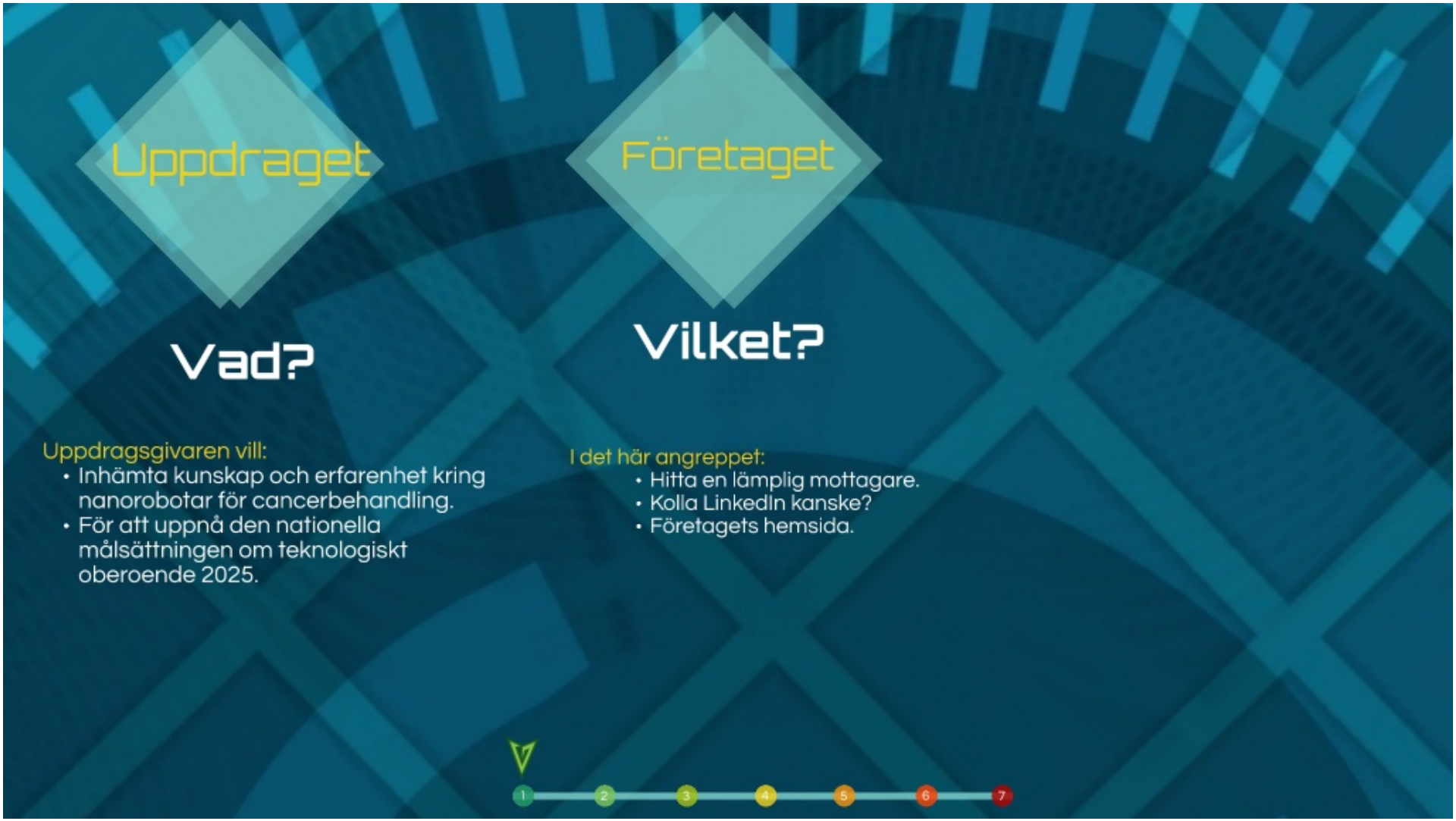

Spaning, förberedelser och distribution
1. Planering och spaningsarbete
2. Förberedelser
3. Distribution

1. Planering och spaningsarbete


1. Planering och spaningsarbete
Angripare
Försvarare
1
2
3
4
5
6
7


1
2
3
4
5
6
7


Uppdraget
Vad?
Uppdragsgivaren vill:
• Inhämta kunskap och erfarenhet kring nanorobotar för cancerbehandling.
• För att uppnå den nationella målsättningen om teknologiskt oberoende 2025.
1
2
3
4
5
6
7


Uppdraget
Företaget
Vad?
Vilket?
Uppdragsgivaren vill:
• Inhämta kunskap och erfarenhet kring nanorobotar för cancerbehandling.
• För att uppnå den nationella målsättningen om teknologiskt oberoende 2025.
I det här angreppet:
• Hitta en lämplig mottagare.
• Kolla LinkedIn kanske?
• Företagets hemsida.
1
2
3
4
5
6
7

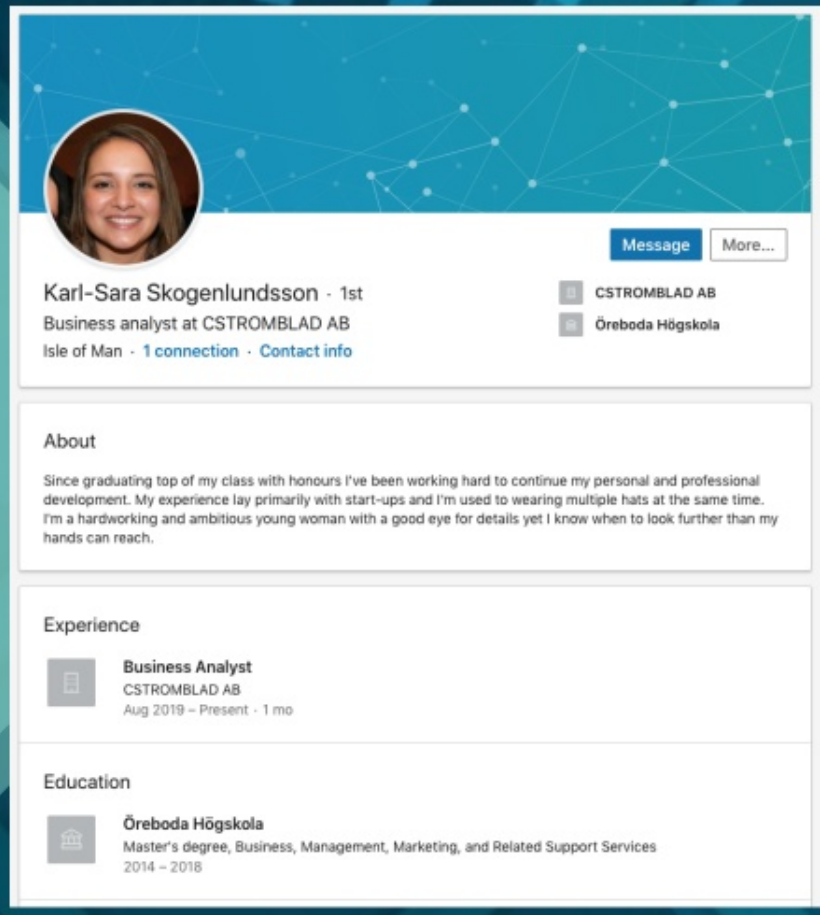

Uppdraget
Företaget
Offret
Vad?
Vilket?
Vem?
Uppdragsgivaren vill:
• Inhämta kunskap och erfarenhet kring nanorobotar för cancerbehandling.
• För att uppnå den nationella målsättningen om teknologiskt oberoende 2025.
I det här angreppet:
• Hitta en lämplig mottagare.
• Kolla LinkedIn kanske?
• Företagets hemsida.
Angriparen behöver ett fotfäste, en patient zero.
I vårt fall är det Karl-Sara, affärsanalytiker på Kirurgiskt AB och vi vänder oss till LinkedIn för mer info.
1
2
3
4
5
6
7

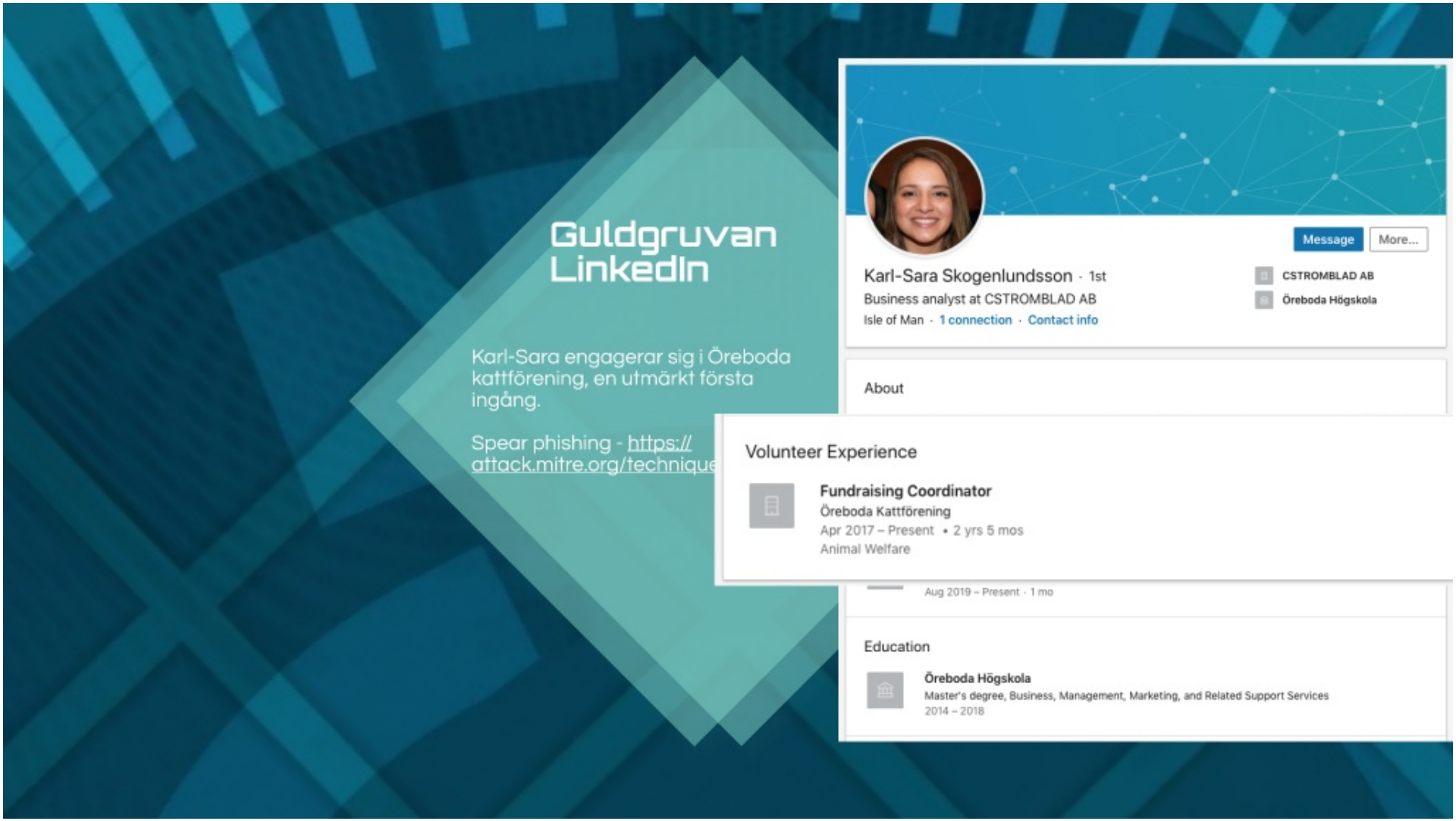

Uppdraget
Företaget
Offret
Vad?
Vilket?
Vem?
Uppdragsgivaren vill:
• Inhämta kunskap och erfarenhet kring nanorobotar för cancerbehandling.
• För att uppnå den nationella målsättningen om teknologiskt oberoende 2025.
I det här angreppet:
• Hitta en lämplig mottagare.
• Kolla LinkedIn kanske?
• Företagets hemsida.
Angriparen behöver ett fotfäste, en patient zero.
I vårt fall är det Karl-Sara, affärsanalytiker på Kirurgiskt AB och vi vänder oss till LinkedIn för mer info.
LinkedIn
1
2
3
4
5
6
7

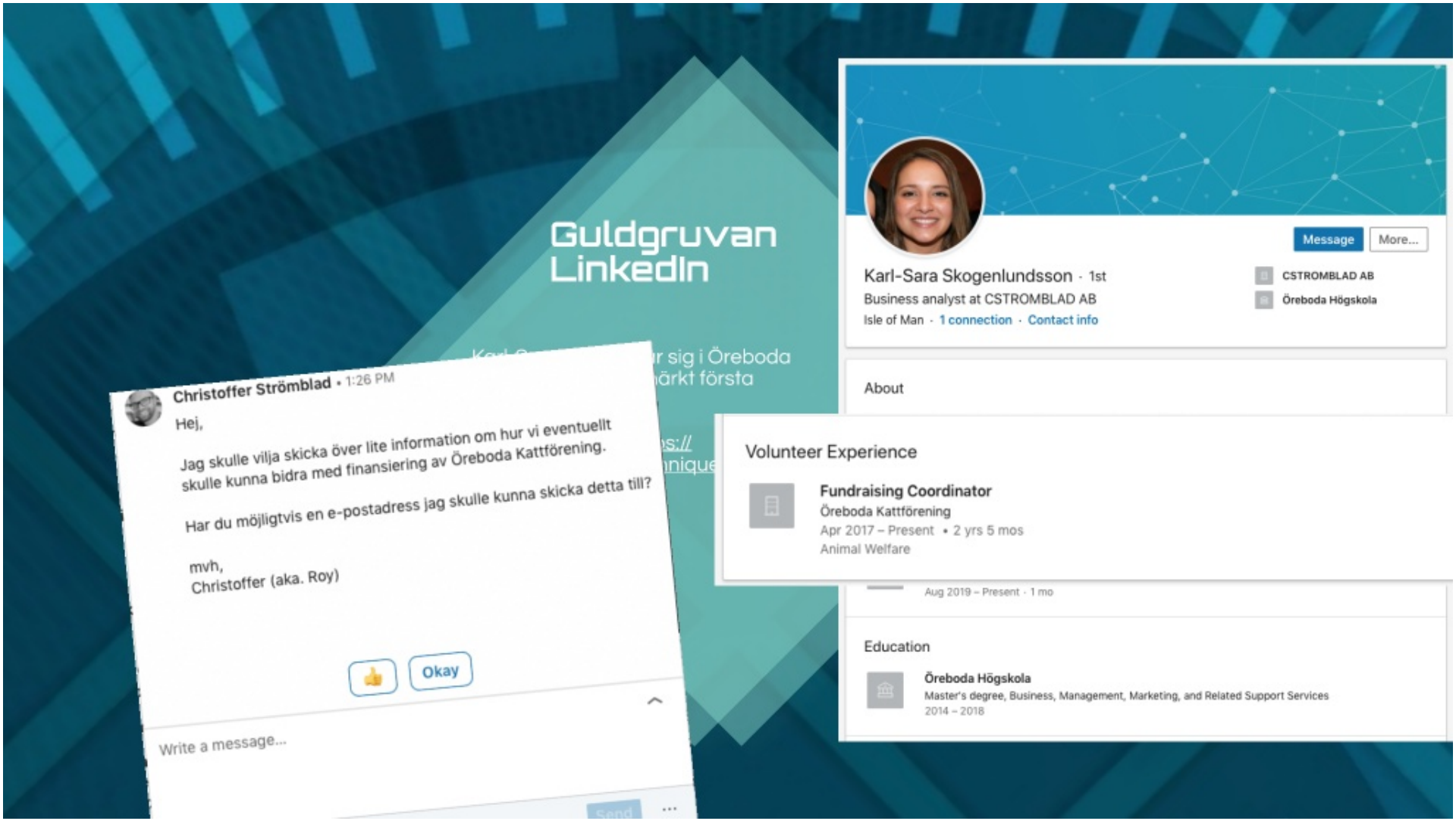
Guldgruvan LinkedIn

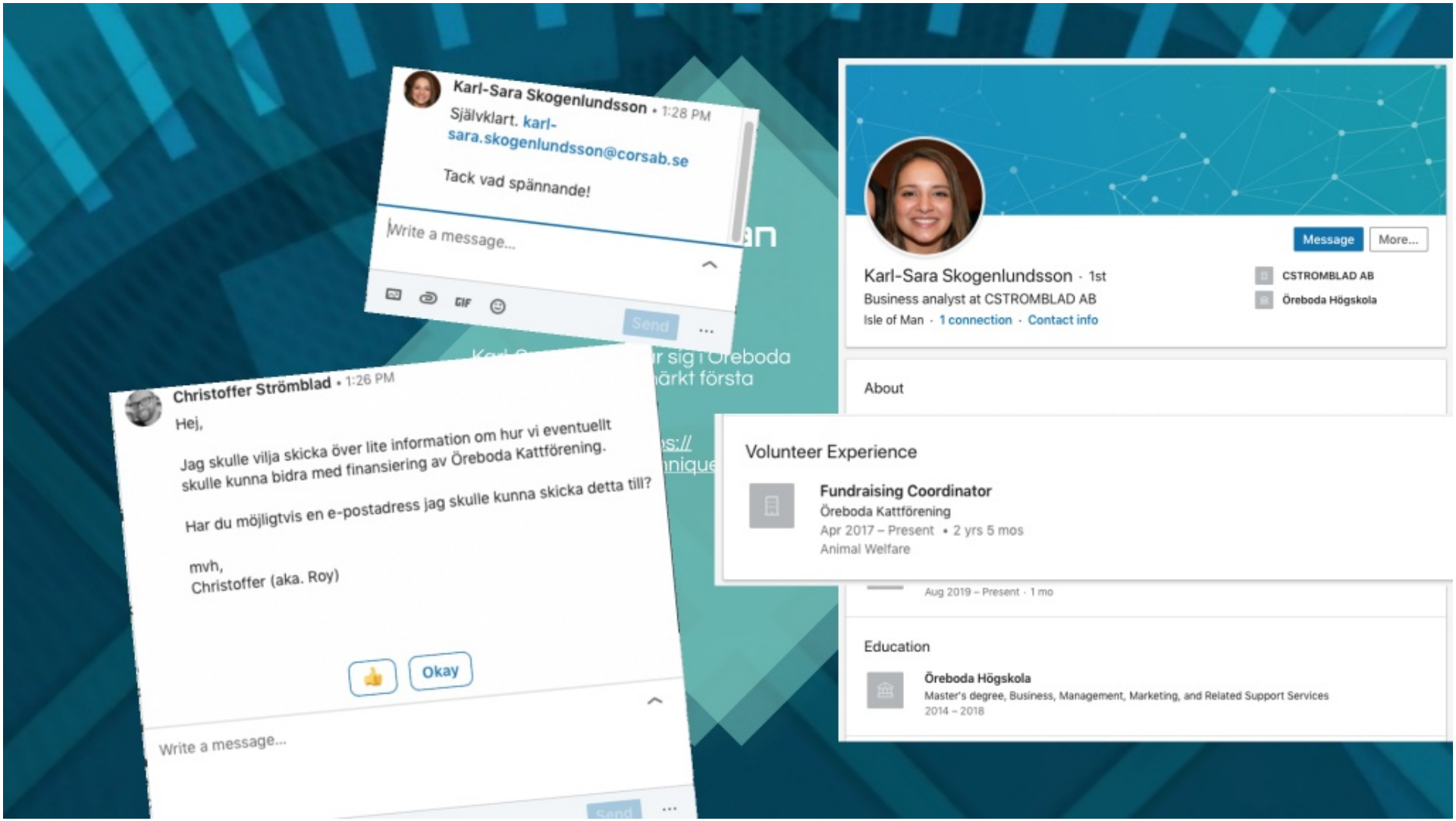
Karl-Sara engagerar sig i Öreboda kattförening, en utmärkt första ingång.

Spear phishing - https://attack.mitre.org/techniques/T1193/



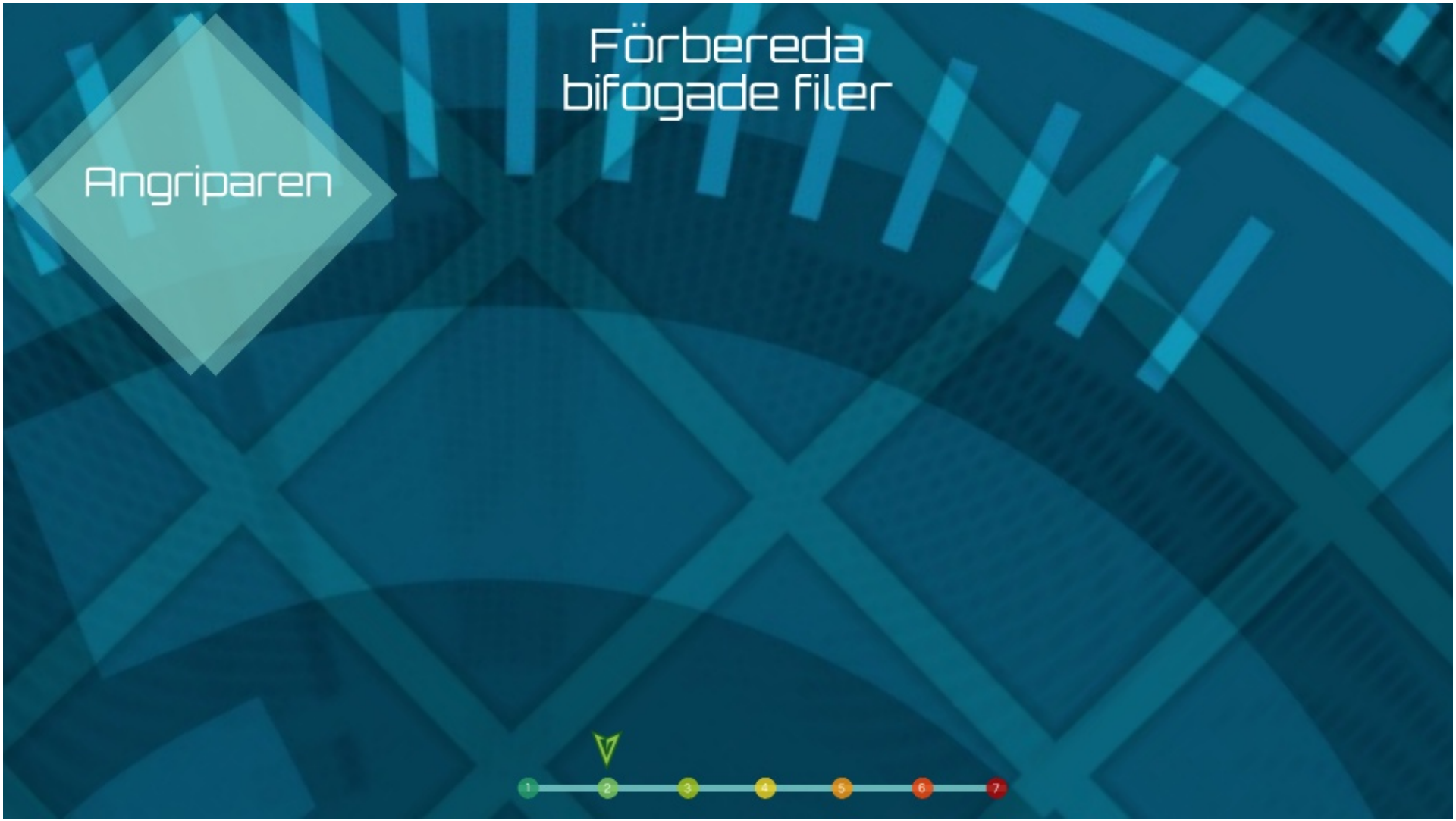

Guldgruvan
LinkedIn
Karl-Sara engagerar sig i Öreboda kattförening, en utmärkt första ingång.
Spear phishing - https://attack.mitre.org/technique
Message
More...
Karl-Sara Skogenlundsson · 1st
Business analyst at CSTROMBLAD AB
Isle of Man · 1 connection · Contact info
CSTROMBLAD AB
Öreboda Högskola
About
Volunteer Experience
Fundraising Coordinator
Öreboda Kattförening
Apr 2017 – Present • 2 yrs 5 mos
Animal Welfare
Aug 2019 – Present · 1 mo
Education
Öreboda Högskola
Master's degree, Business, Management, Marketing, and Related Support Services
2014 – 2018


Guldgruvan
LinkedIn
Christoffer Strömblad • 1:26 PM
Hej,
Jag skulle vilja skicka över lite information om hur vi eventuellt skulle kunna bidra med finansiering av Öreboda Kattförening.
Har du möjligtvis en e-postadress jag skulle kunna skicka detta till?
mvh,
Christoffer (aka. Roy)
Okay
Write a message...
Send
Message
More...
Karl-Sara Skogenlundsson · 1st
Business analyst at CSTROMBLAD AB
Isle of Man · 1 connection · Contact info
CSTROMBLAD AB
Öreboda Högskola
About
Volunteer Experience
Fundraising Coordinator
Öreboda Kattförening
Apr 2017 – Present • 2 yrs 5 mos
Animal Welfare
Aug 2019 – Present · 1 mo
Education
Öreboda Högskola
Master's degree, Business, Management, Marketing, and Related Support Services
2014 – 2018


Karl-Sara Skogenlundsson • 1:28 PM
Självklart. karl-sara.skogenlundsson@corsab.se
Tack vad spännande!
Write a message...
GIF
Send
Christoffer Strömblad • 1:26 PM
Hej,
Jag skulle vilja skicka över lite information om hur vi eventuellt skulle kunna bidra med finansiering av Öreboda Kattförening.
Har du möjligtvis en e-postadress jag skulle kunna skicka detta till?
mvh,
Christoffer (aka. Roy)
Okay
Write a message...
Send
Karl-Sara Skogenlundsson · 1st
Business analyst at CSTROMBLAD AB
Isle of Man · 1 connection · Contact info
Message
More...
CSTROMBLAD AB
Öreboda Högskola
About
Volunteer Experience
Fundraising Coordinator
Öreboda Kattförening
Apr 2017 – Present • 2 yrs 5 mos
Animal Welfare
Aug 2019 – Present · 1 mo
Education
Öreboda Högskola
Master's degree, Business, Management, Marketing, and Related Support Services
2014 – 2018


Försvarare
Vad gör vi?
Försvarstrategi:
• Lura och förvränga.
• Målsättning:
• Förmedla en alternativ verklighet.
• Skapa osäkehet.
Åtgärder:
• Falska profiler på LinkedIn
• "Felaktig" information i DNS
• "Öppna" portar (HoneyPots)
• Honung över hela stället...
1
2
3
4
5
6
7

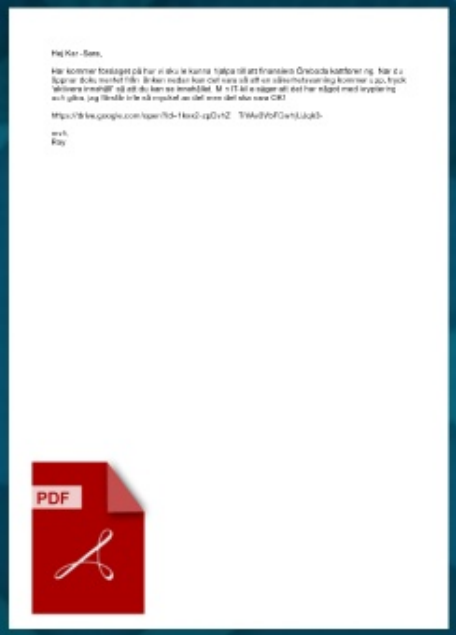

2. Förberedelser
Angripare
Försvarare
1
2
3
4
5
6
7


Förbereda
bifogade filer
Angriparen
1
2
3
4
5
6
7

Förbereda bifogade filer

Angriparen

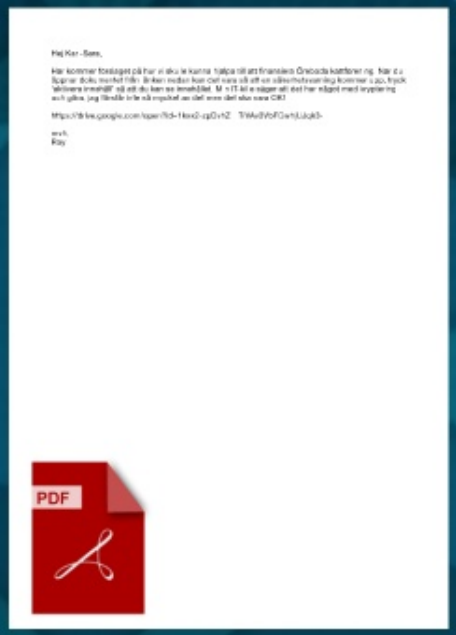
Stage 1 - PDF med länk till Google Drive



Förbereda bifogade filer

Angriparen

Stage 1 - PDF med länk till Google Drive



Stage 2 - Word-dokument med Makron.

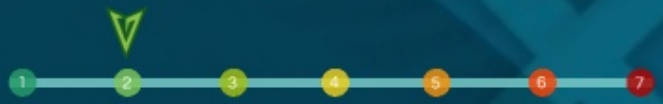
Försvarare
Vad gör vi?

Försvarstrategi:

- Neka och begränsa.
- *Målsättning*
  - Tidigt avväpna.
  - Öka angriparens insatser och resursanvändning.

Åtgärder:

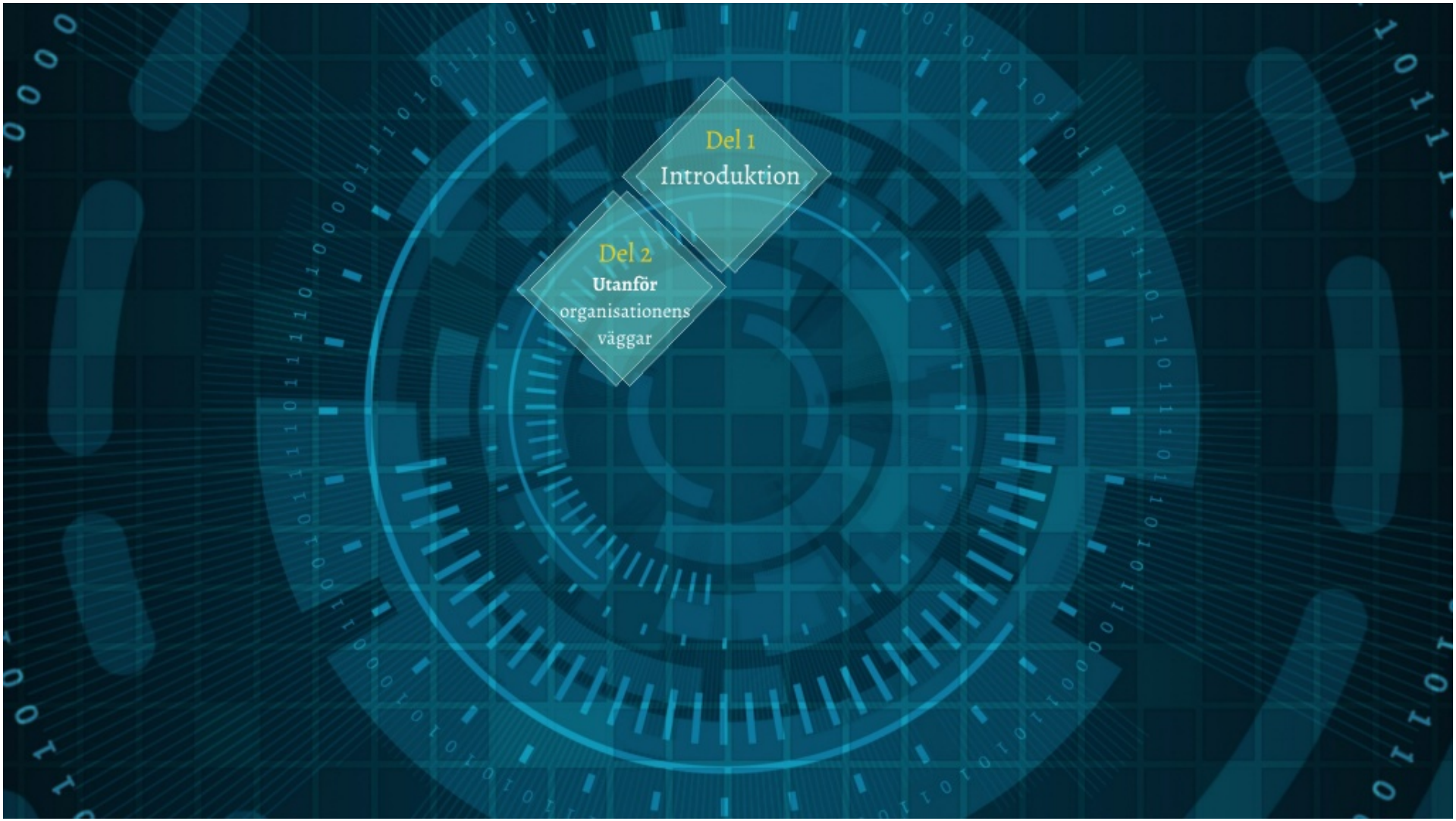
- Blockera bifogade filer med uppenbart suspekt innehåll; Makron, PowerShell, Python osv.
- "Detonera" bifogade filer.

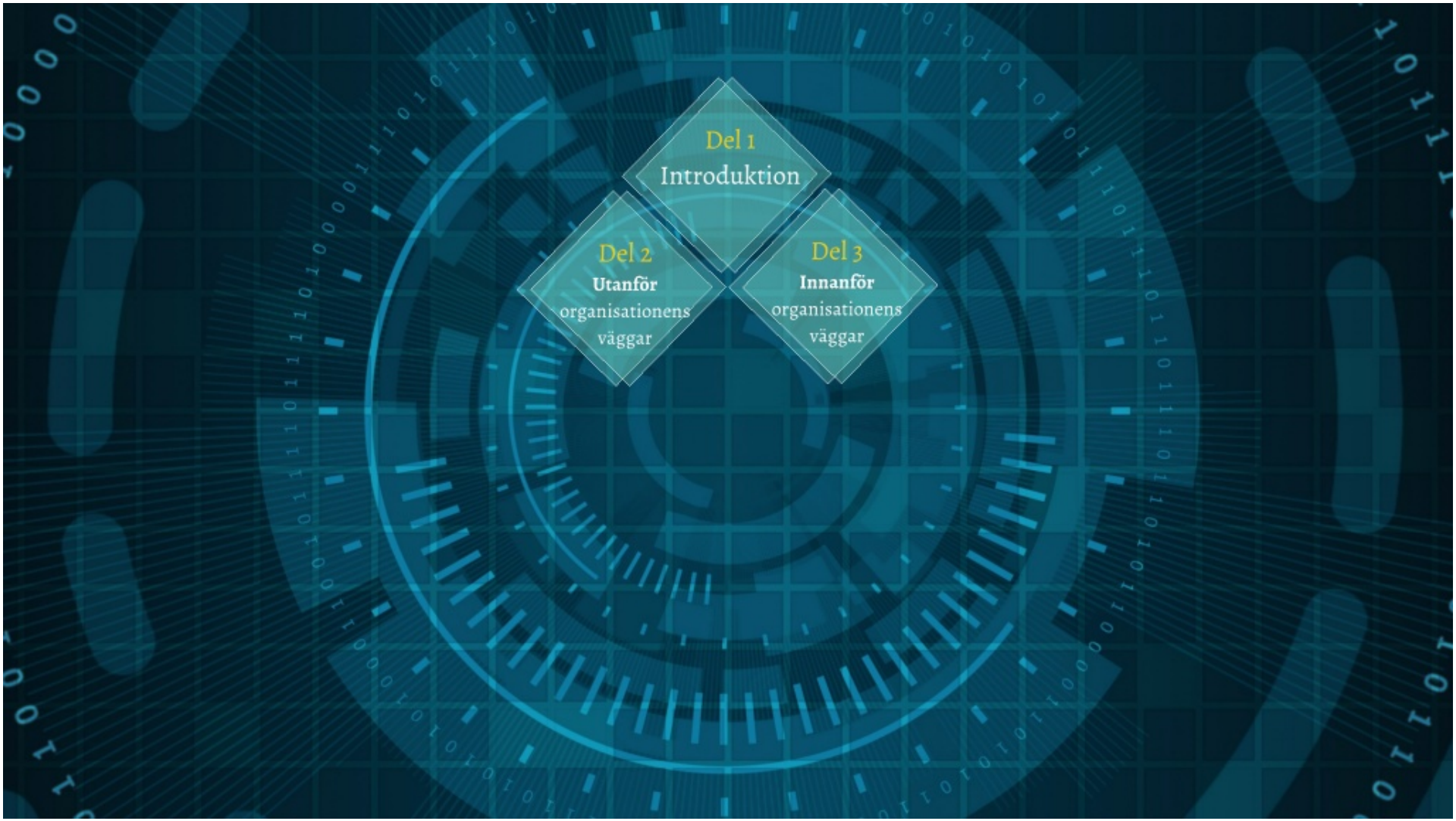


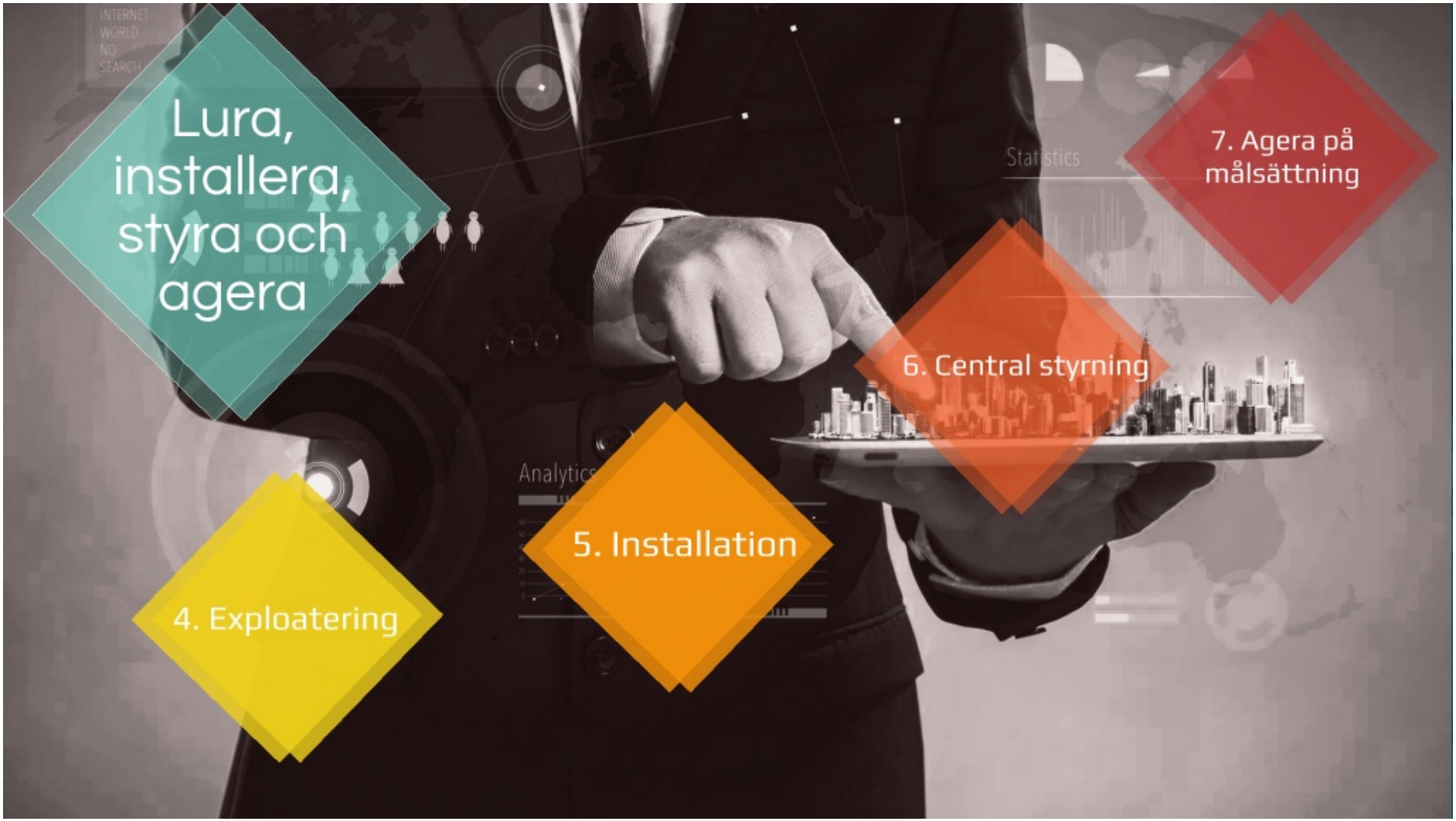

3. Distribution
Angriparen
Försvarare
1
2
3
4
5
6
7


Angriparen
Skicka e-post (spear phishing)
• Målet är att leverera den skadliga koden.
• Först ett epost-meddelande utan bifogad fil.
• Efter första "felskicket", skicka den bifogade filen...
• ... bifogar stage 1-dokumentet, PDF med länk till Google Drive där det skadliga Word-dokument finns (innehåller makro-kod).
1
2
3
4
5
6
7


Försvarare
Vad gör vi?
Försvarstrategi:
• Neka och begränsa.
• Målsättning
• Tidigt avväpna.
• Försvåra angrpepet.
• Öka resursanvändning och nödvändiga insatser.
Åtgärder:
• Använda SPF, DMARC och DKIM.
• Varna mottagare om följande villkor uppfylls:
• Relativt ny avsändare
• Bifogad fil (pdf, docx et al.)
• Bifogad fil innehåller länk till Dropbox, Google Drive, SharePoint et al.)
1
2
3
4
5
6
7


Del 1
Introduktion
Del 2
Utanför
organisationens
väggar


Del 1
Introduktion
Del 2
Utanför
organisationens
väggar
Del 3
Innanför
organisationens
väggar

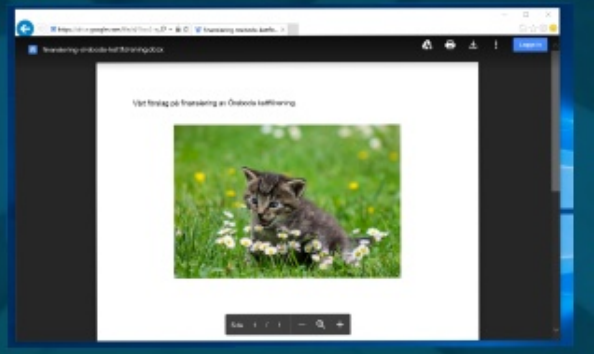

Lura, installera, styra och agera
7. Agera på målsättning
6. Central styrning
5. Installation
4. Exploatering


4. Exploatering
Angriparen
Försvarare
1
2
3
4
5
6
7

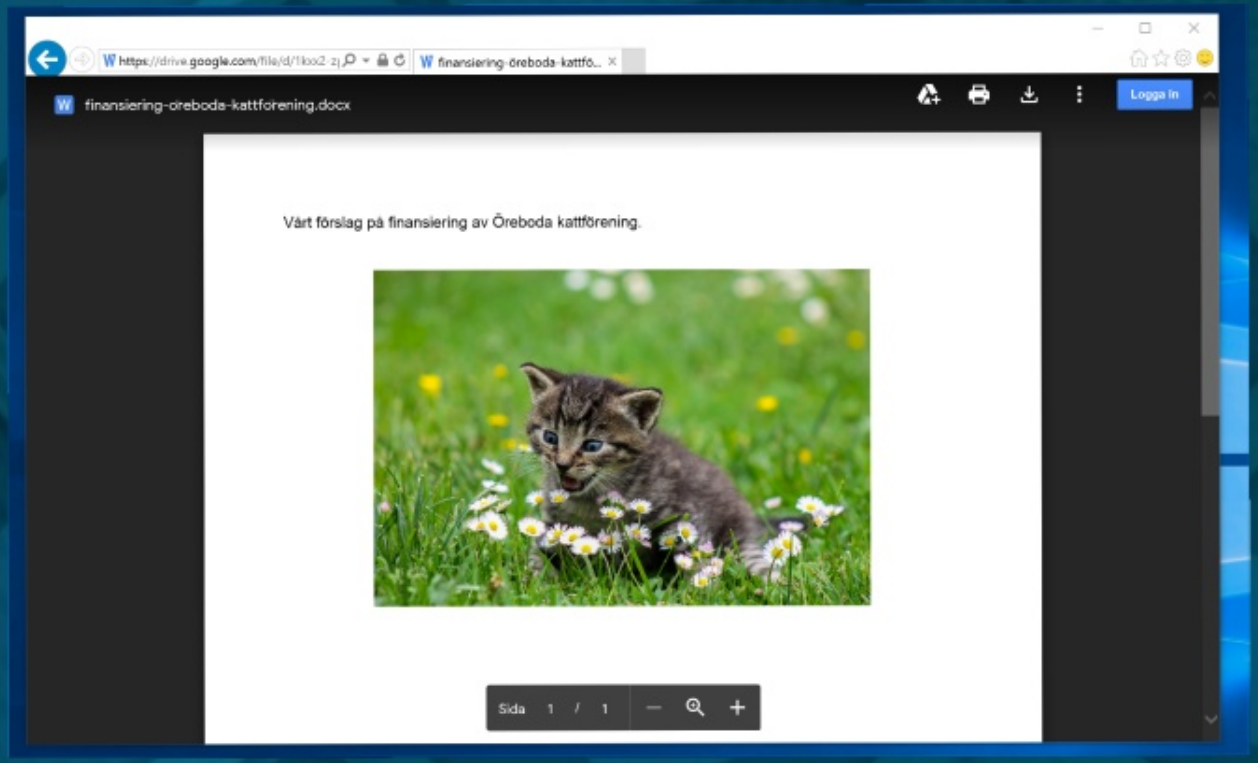
Lurar användaren

Angriparen
Gör...

- Användaren ser det som en självklarhet att öppna den bifogade filen...
- ... och som givetvis även laddar ner dokumentet från den inkluderade länken till Google Drive.
- Men... varför? Därför att användaren förväntade sig dokumenten. Hen var "preppad".



umenten. Hen var

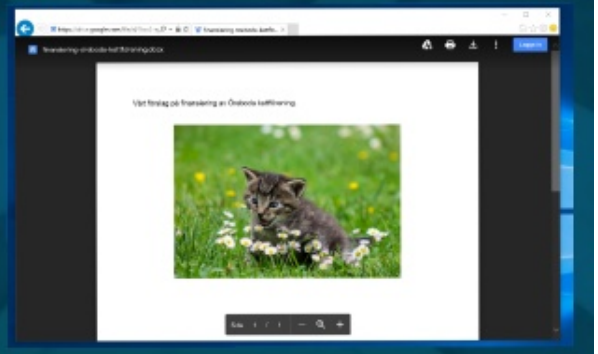


6 7

Lurar användaren

Angriparen
Gör...

- Användaren ser det som en självklarhet att öppna den bifogade filen...
- ... och som givetvis även laddar ner dokumentet från den inkluderade länken till Google Drive.
- Men... varför? Därför att användaren förväntade sig dokumenten. Hen var "preppad".

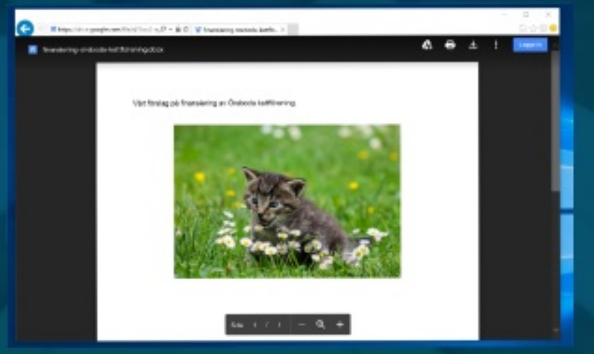


Lurar användaren

Angriparen
Gör...

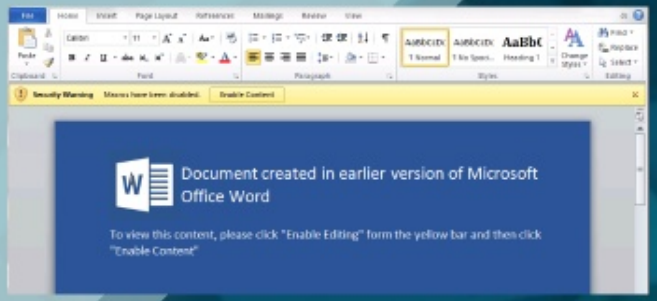
- Användaren ser det som en självklarhet att öppna den bifogade filen...
- ... och som givetvis även laddar ner dokumentet från den inkluderade länken till Google Drive.
- Men... varför? Därför att användaren förväntade sig dokumenten. Hen var "preppad".

Aktivera makron

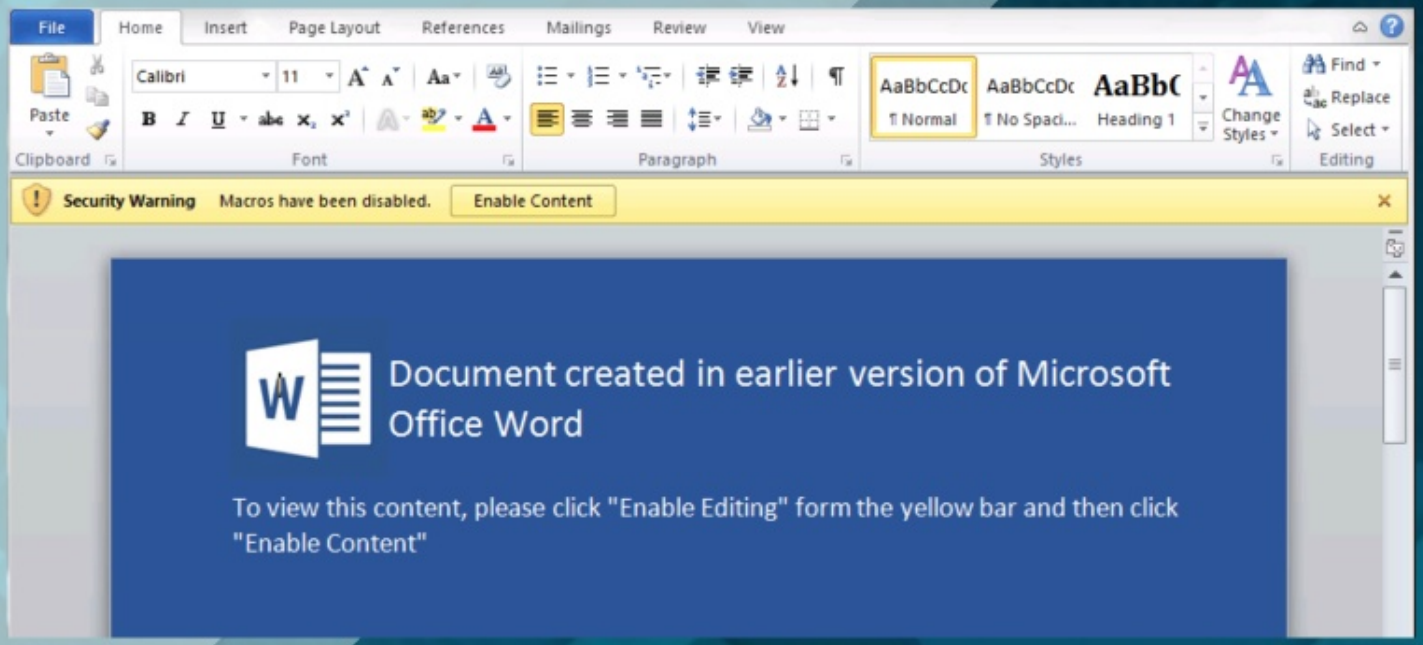


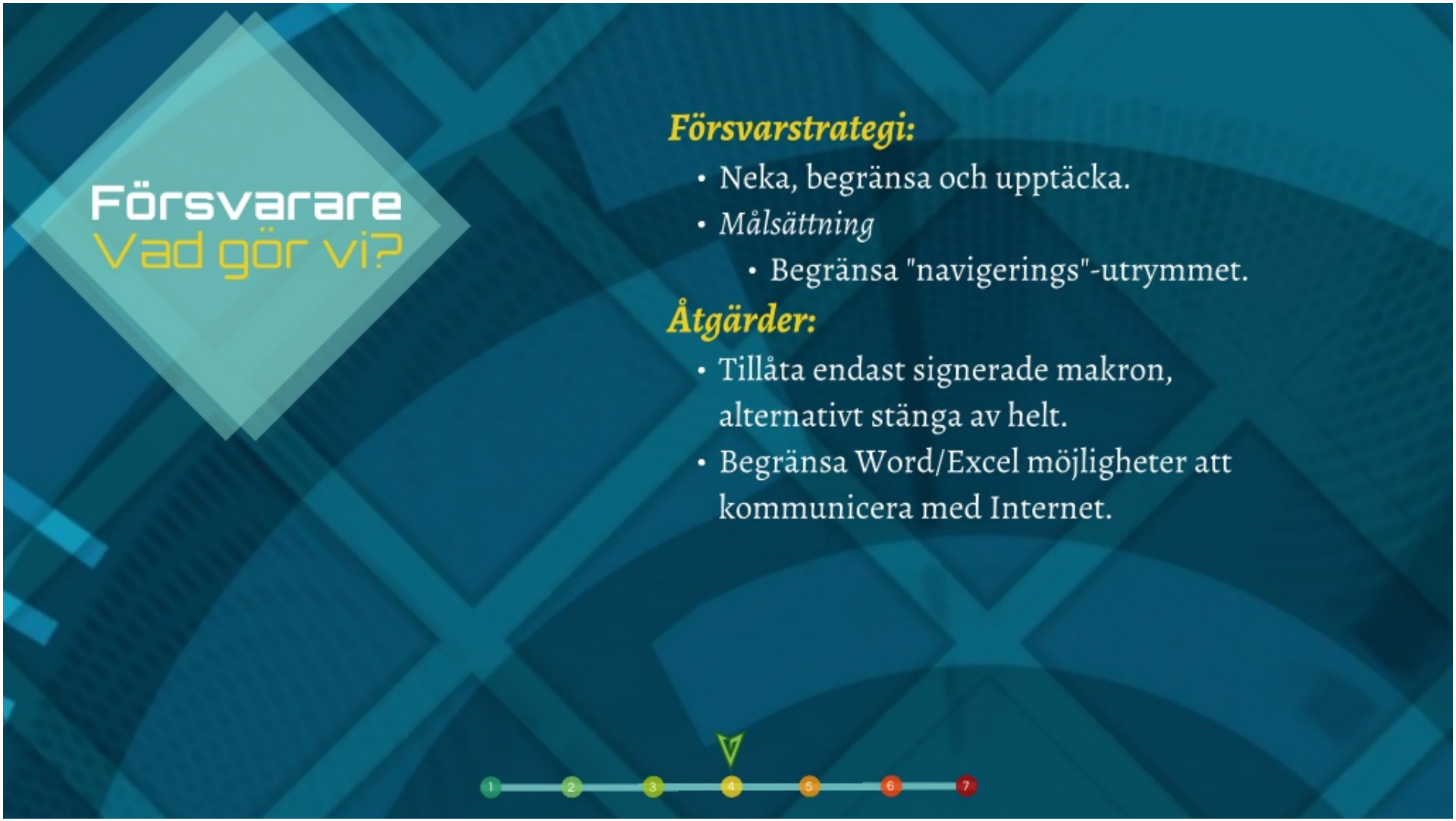
Word - Aktivera makron

- Användaren aktiverar makron
- Makro-koden laddar ner den första payloaden från angriparens infrastruktur.

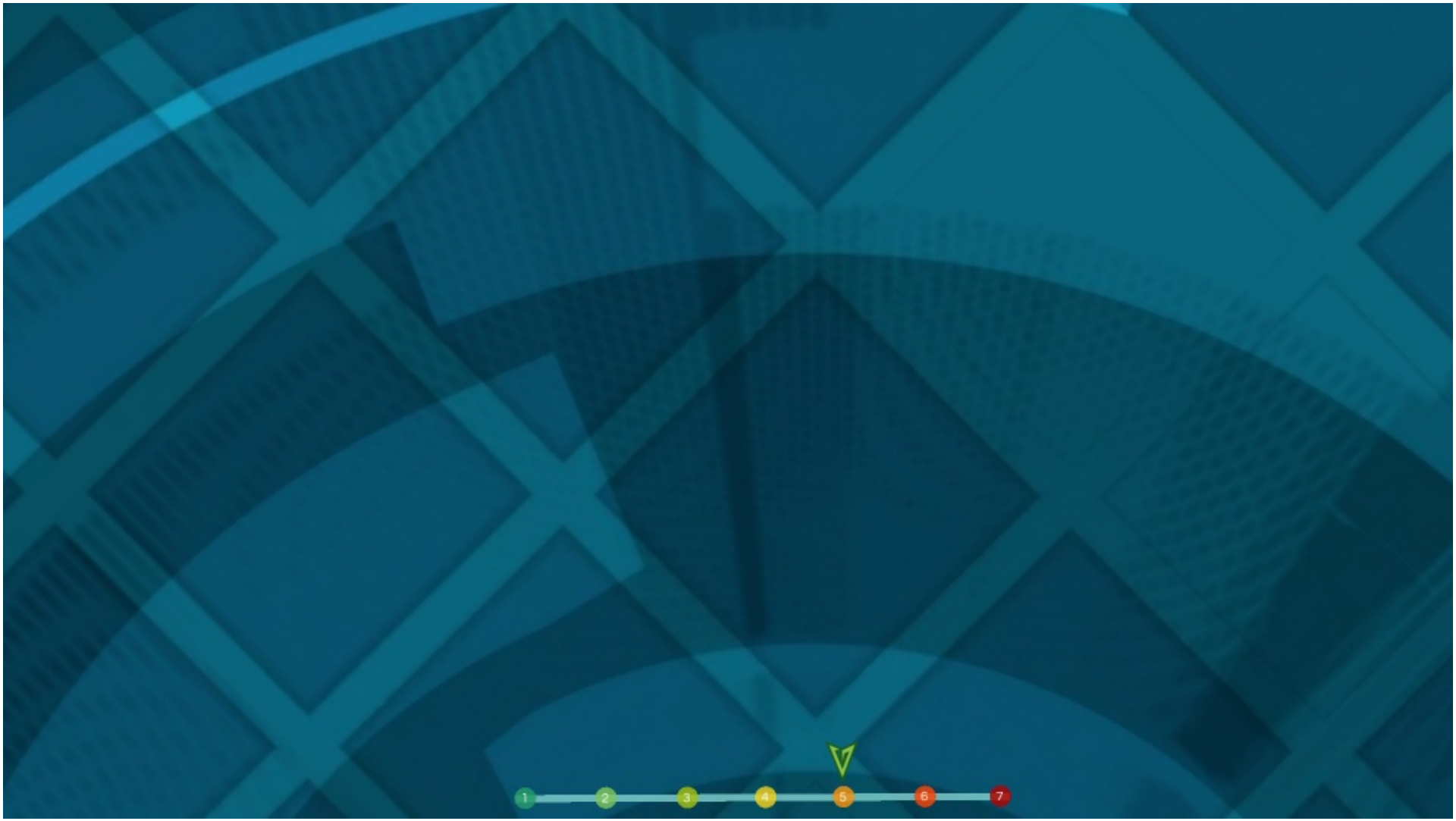


arens infrastruktur.




Försvarare
Vad gör vi?
Försvarstrategi:
• Neka, begränsa och upptäcka.
• Målsättning
• Begränsa "navigerings"-utrymmet.
Åtgärder:
• Tillåta endast signerade makron, alternativt stänga av helt.
• Begränsa Word/Excel möjligheter att kommunicera med Internet.
1
2
3
4
5
6
7


5. Installation
Angriparen
Försvarare
1
2
3
4
5
6
7

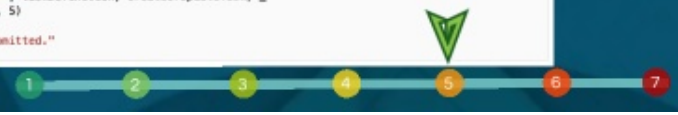

1
2
3
4
5
6
7

Persistens

Schemalagt jobb - T1053

- Varje gång användaren loggar in ska ett av angriparen kontrollerat program starta.
- Beskrivs i MITRE ATT&CK T1053 - https://attack.mitre.org/techniques/T1053/

```
'*************************************************************
' Create a boot trigger.
Dim triggers
Set triggers = taskDefinition.Triggers

Dim trigger
Set trigger = triggers.Create(TriggerTypeBoot)

' Trigger variables that define when the trigger is active.
Dim startTime, endTime
startTime = "2006-05-02T10:49:02"
endTime = "2006-05-02T10:52:02"

WScript.Echo "startTime :" & startTime
WScript.Echo "endTime :" & endTime

trigger.StartBoundary = startTime
trigger.EndBoundary = endTime
trigger.ExecutionTimeLimit = "PT5M"    ' Five minutes
trigger.Id = "BootTriggerId"
trigger.Delay = "PT30S"                ' 30 Seconds

'*************************************************************
' Create the action for the task to execute.

' Add an action to the task. The action executes notepad.
Dim Action
Set Action = taskDefinition.Actions.Create( ActionTypeExecutable )
Action.Path = "C:\Windows\System32\notepad.exe"

WScript.Echo "Task definition created. About to submit the task..."

'*************************************************************
' Register (create) the task.
const createOrUpdateTask = 6
call rootFolder.RegisterTaskDefinition( _
    "Test Boot Trigger", taskDefinition, createOrUpdateTask, _
    "Local Service", , 5)

WScript.Echo "Task submitted."
```



Persistens

Schemalagt jobb - T1053

- Varje gång användaren loggar in ska ett av angriparen kontrollerat program starta.
- Beskrivs i MITRE ATT&CK T1053 - https://attack.mitre.org/techniques/T1053/

```
'************************************************************
' Create a boot trigger.
Dim triggers
Set triggers = taskDefinition.Triggers

Dim trigger
Set trigger = triggers.Create(TriggerTypeBoot)

' Trigger variables that define when the trigger is active.
Dim startTime, endTime
startTime = "2006-05-02T10:49:02"
endTime = "2006-05-02T10:52:02"

WScript.Echo "startTime :" & startTime
WScript.Echo "endTime :" & endTime

trigger.StartBoundary = startTime
trigger.EndBoundary = endTime
trigger.ExecutionTimeLimit = "PT5M"     ' Five minutes
trigger.Id = "BootTriggerId"
trigger.Delay = "PT30S"                 ' 30 Seconds

'************************************************************
' Create the action for the task to execute.

' Add an action to the task. The action executes notepad.
Dim Action
Set Action = taskDefinition.Actions.Create( ActionTypeExecutable )
Action.Path = "C:\Windows\System32\notepad.exe"

WScript.Echo "Task definition created. About to submit the task..."

'************************************************************
' Register (create) the task.
const createOrUpdateTask = 6
call rootFolder.RegisterTaskDefinition( _
    "Test Boot Trigger", taskDefinition, createOrUpdateTask, _
    "Local Service", , 5)

WScript.Echo "Task submitted."
```

Övriga aktiviteter

- Registrera "mutex" för att inte infektera flera gånger
- Extrahera datornamn, användare, IP-adresser, subnät osv. En enklare lokal datoranalys.
- ... plus ungefär tusen andra saker.

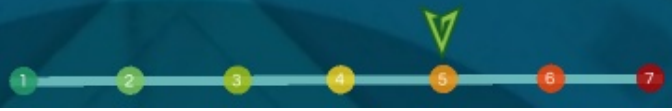
Försvarare
Vad gör vi?

Försvarstrategi:

- Upptäcka och begränsa
- *Målsättning*
  - Identifiera oegentligheter.
  - Upptäcka angreppet.
  - Begränsa skadlig kods nätverksåtkomst.

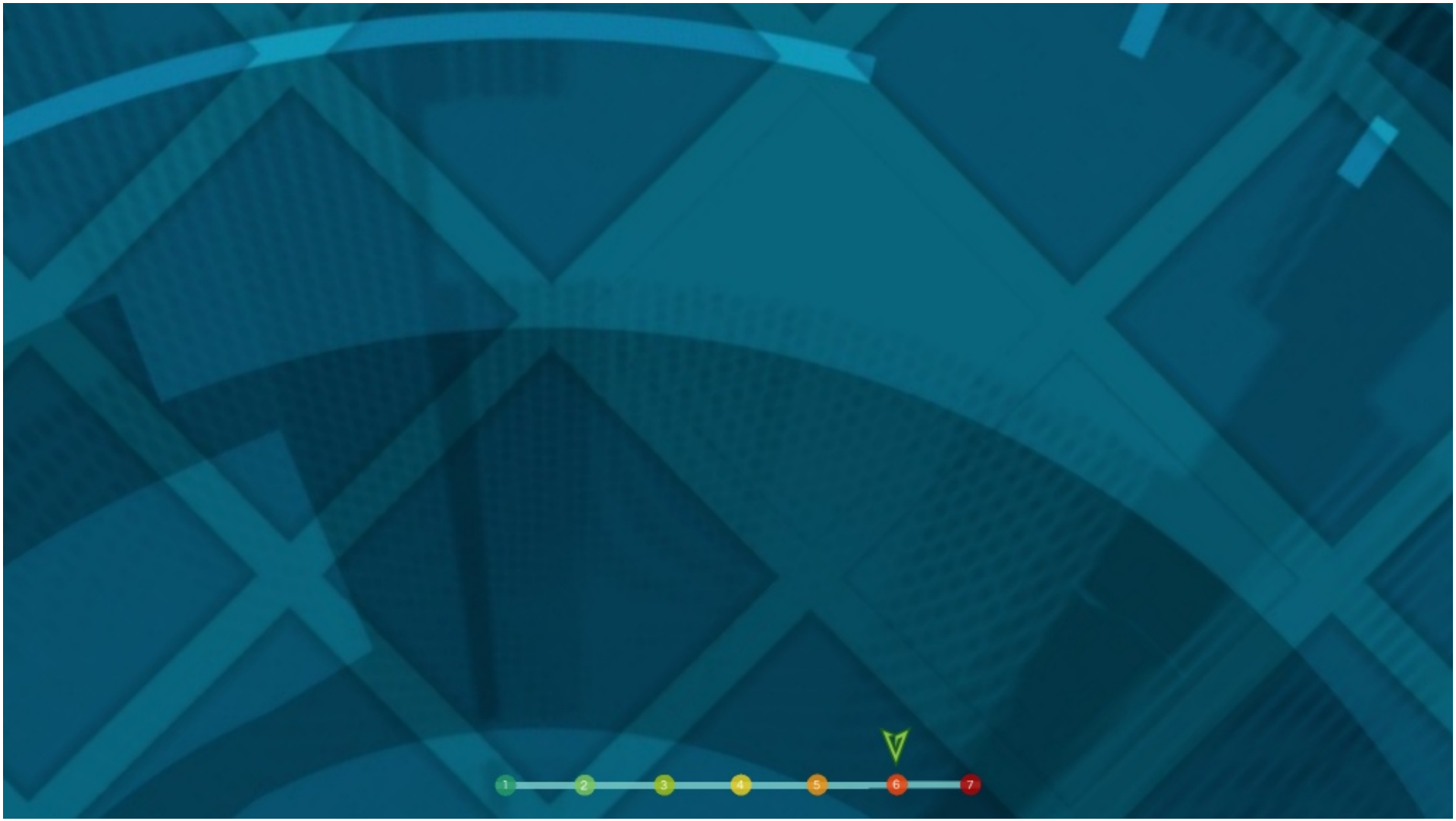
Åtgärder:

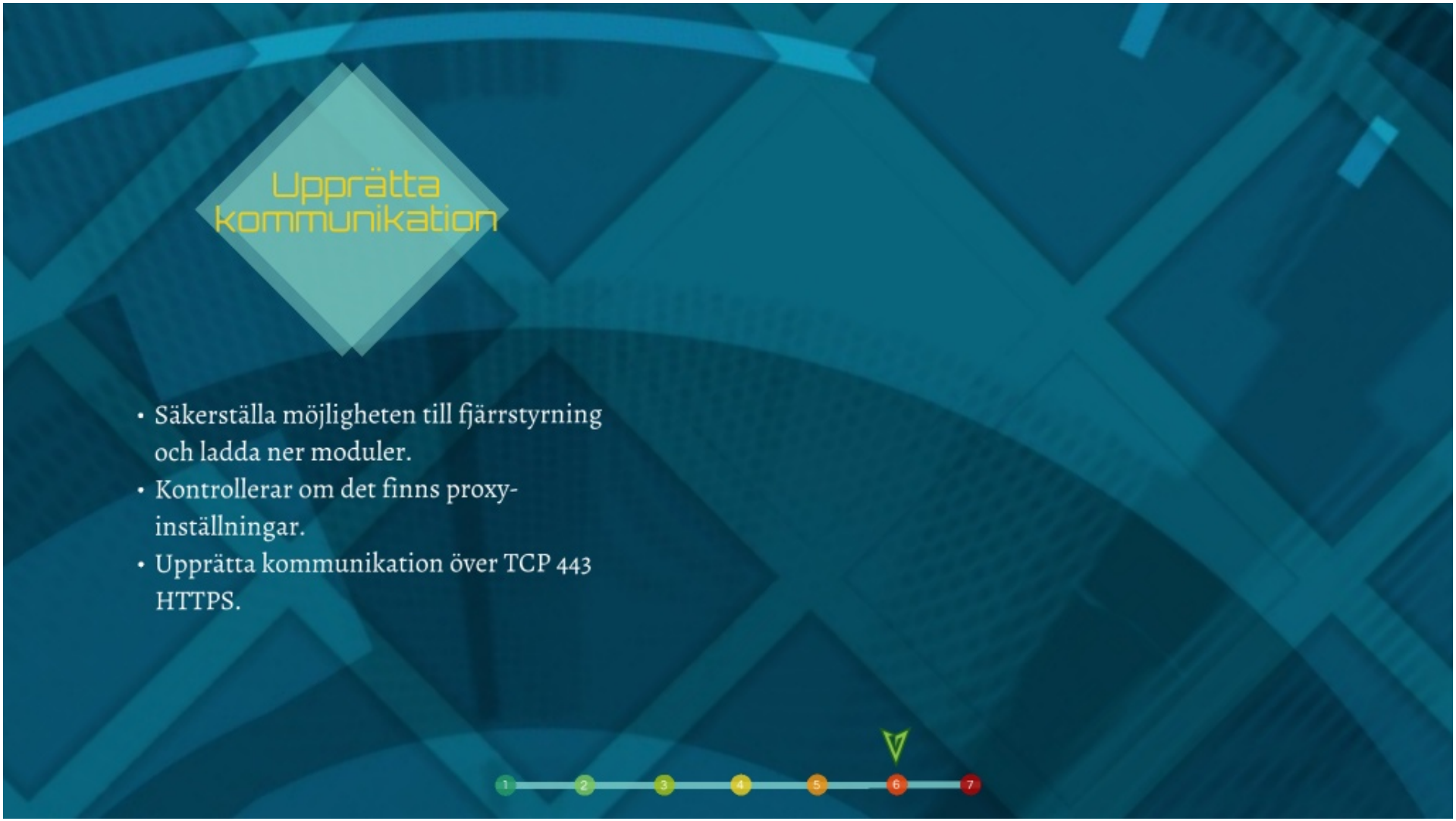
- Loggar händelser som rör nya schemalagada jobb.
- Begränsar Word från att prata med Internet.




6. Central styrning


6. Central styrning
Angriparen
Försvarare
1
2
3
4
5
6
7


1
2
3
4
5
6
7

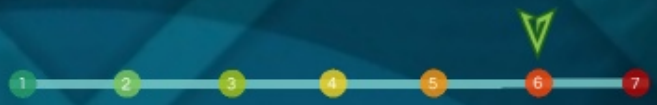

Upprätta kommunikation
• Säkerställa möjligheten till fjärrstyrning och ladda ner moduler.
• Kontrollerar om det finns proxy-inställningar.
• Upprätta kommunikation över TCP 443 HTTPS.
1
2
3
4
5
6
7

Upprätta kommunikation

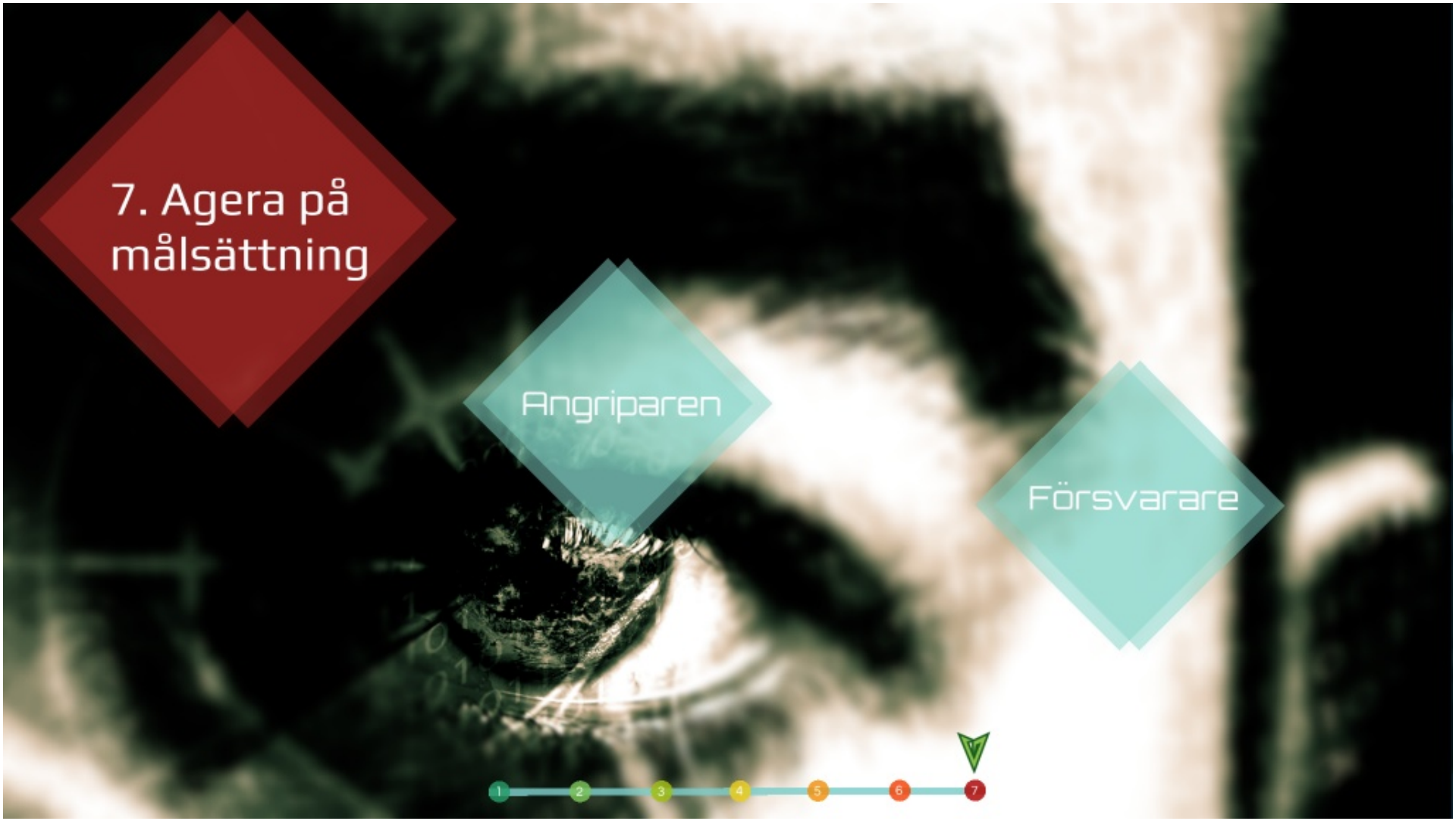
- Säkerställa möjligheten till fjärrstyrning och ladda ner moduler.
- Kontrollerar om det finns proxy-inställningar.
- Upprätta kommunikation över TCP 443 HTTPS.

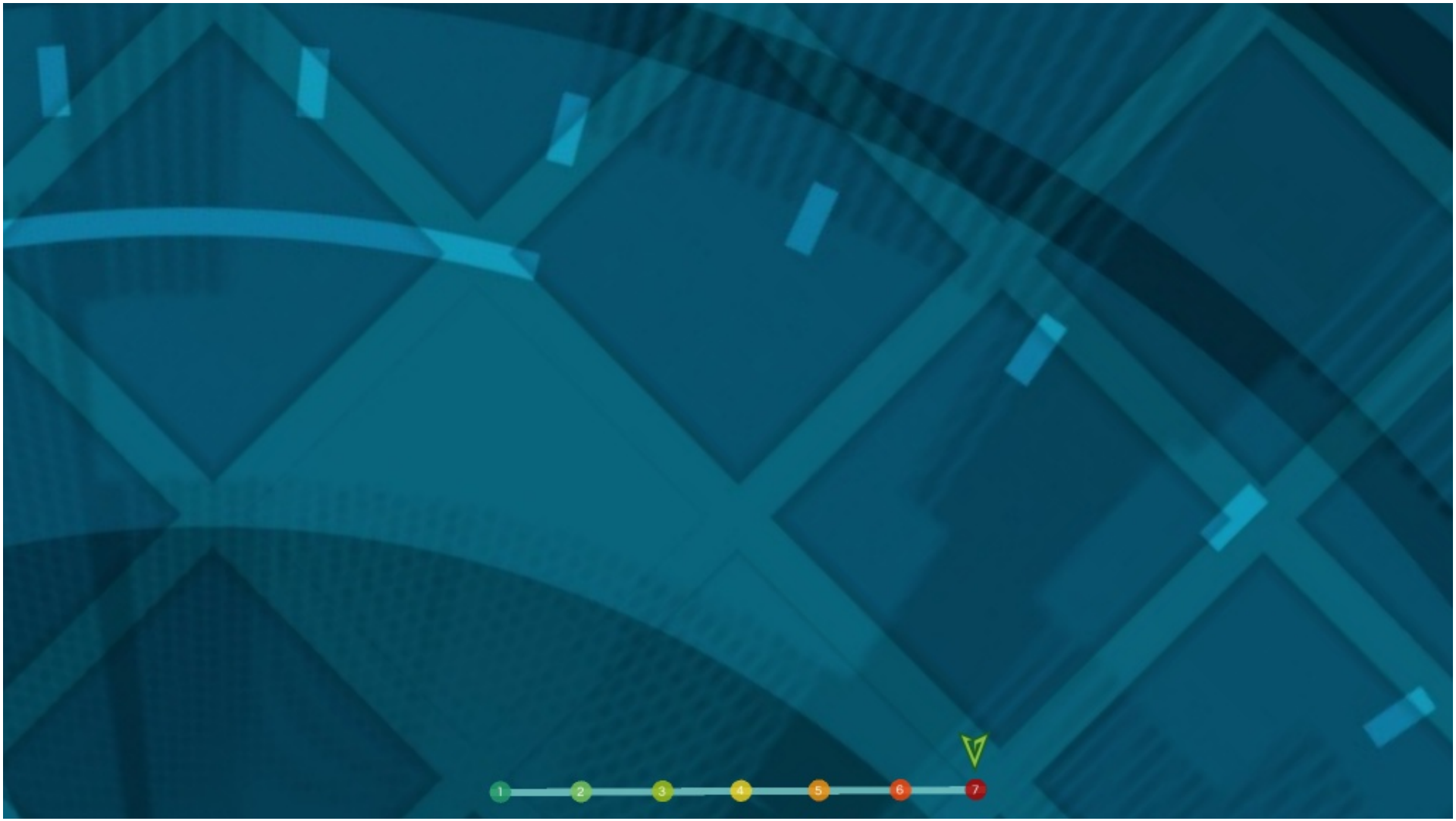
Vänta på instruktioner

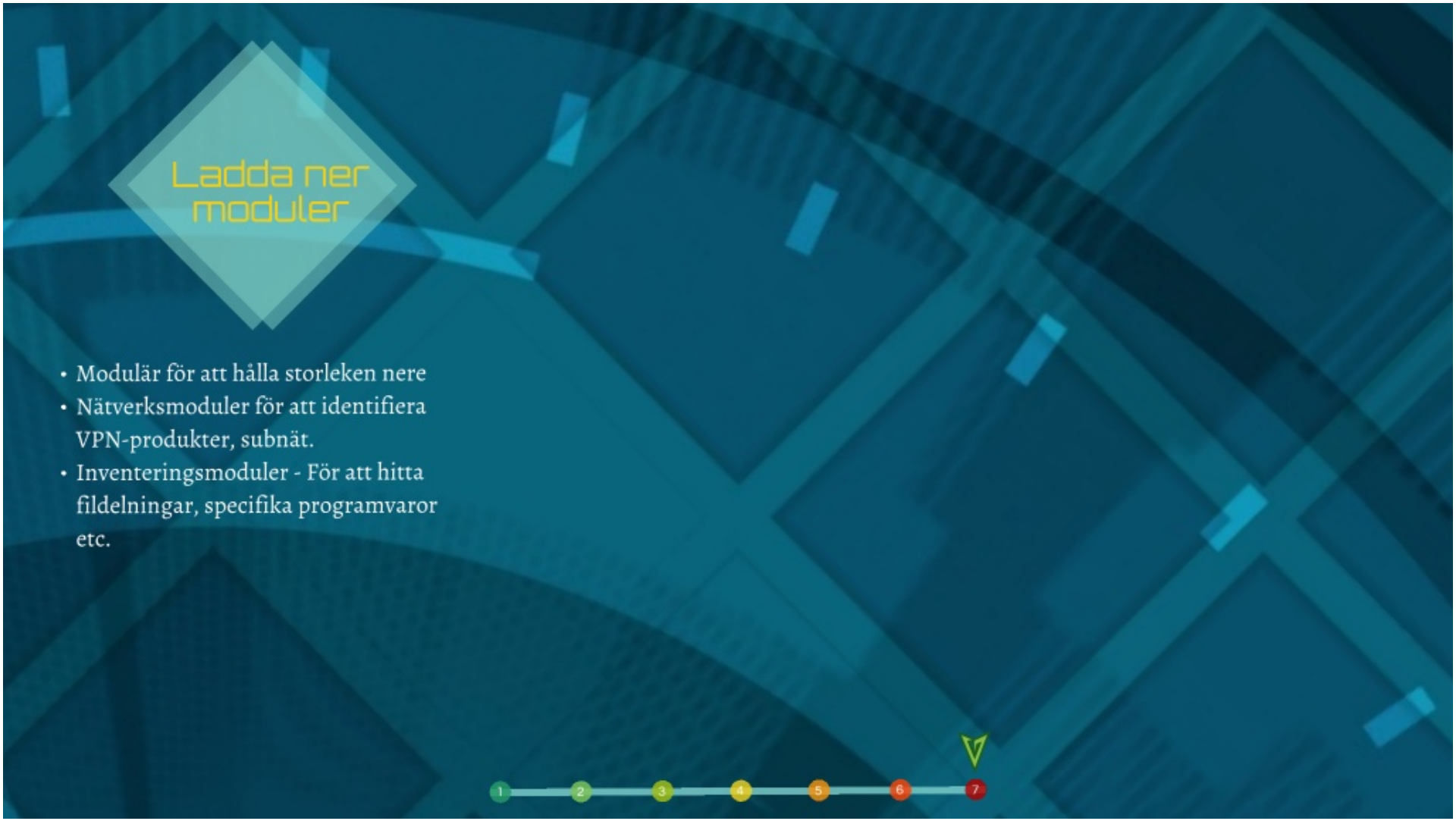
- För avancerade statsaktörer tar detta mellan 20 minuter och 4h.
- ... och efter 20 minuter påbörjas angreppet på riktigt...




Försvarare
Vad gör vi?
Försvarstrategi:
• Neka och begränsa
• Målsättning
• Neka skadlig kod från att slutföra sin exekvering.
Åtgärder:
• Vitlistar godkända applikationer från att prata med Internet med hjälp av lokal klientbrandvägg.
1
2
3
4
5
6
7


7. Agera på målsättning
Angriparen
Försvarare
1
2
3
4
5
6
7


1
2
3
4
5
6
7

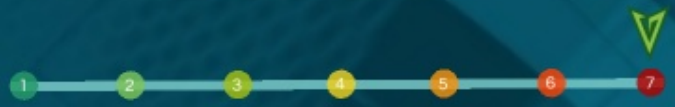

Ladda ner moduler
• Modulär för att hålla storleken nere
• Nätverksmoduler för att identifiera VPN-produkter, subnät.
• Inventeringsmoduler - För att hitta fildelningar, specifika programvaror etc.
1
2
3
4
5
6
7

Ladda ner moduler

- Modulär för att hålla storleken nere
- Nätverksmoduler för att identifiera VPN-produkter, subnät.
- Inventeringsmoduler - För att hitta fildelningar, specifika programvaror etc.

Lateral förflyttning

- Navigera nätverket, hitta "rätt" datorer eller användare.
- Förflytta sig från en dator till en annan.
- Inte alltid nödvändigt att höja privilegier.
- Lagen om minsta motstånd.



Ladda ner moduler

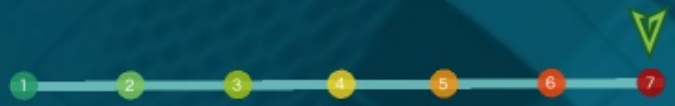
- Modulär för att hålla storleken nere
- Nätverksmoduler för att identifiera VPN-produkter, subnät.
- Inventeringsmoduler - För att hitta fildelningar, specifika programvaror etc.

Lateral förflyttning

- Navigera nätverket, hitta "rätt" datorer eller användare.
- Förflytta sig från en dator till en annan.
- Inte alltid nödvändigt att höja privilegier.
- Lagen om minsta motstånd.

Hitta rätt åtkomst

- *Hitta konton (hitta rätt användare)*
  - (T1087) https://attack.mitre.org/techniques/T1087
- *Hitta intressanta file-shares*
  - (T1120) https://attack.mitre.org/techniques/T1120
- *Process discovery*
  - (T1057) https://attack.mitre.org/techniques/T1057



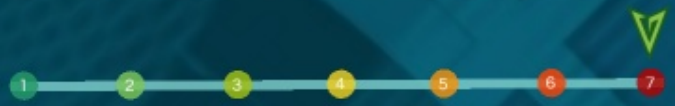
Försvarare
Vad gör vi?

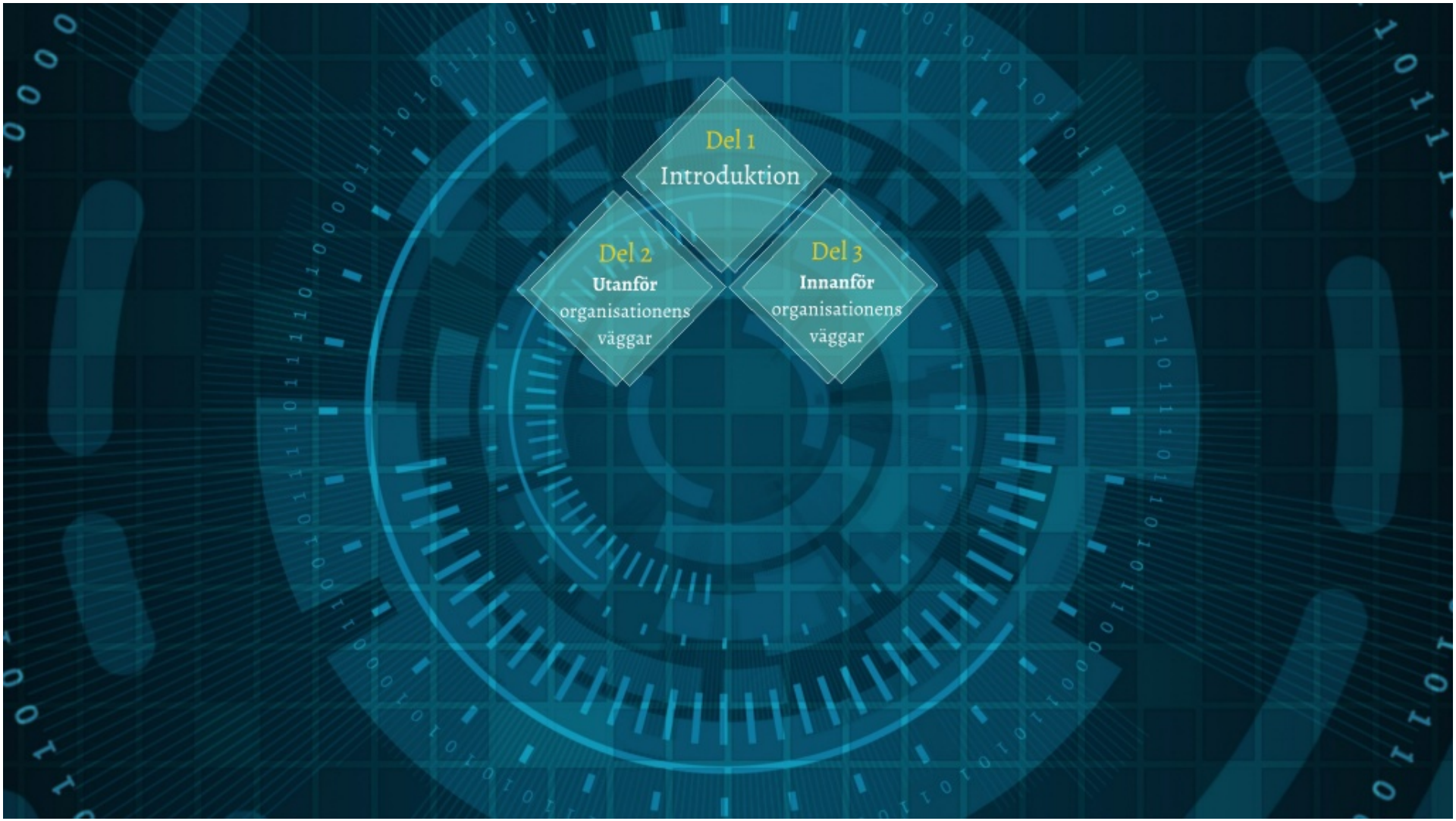
Försvarstrategi:

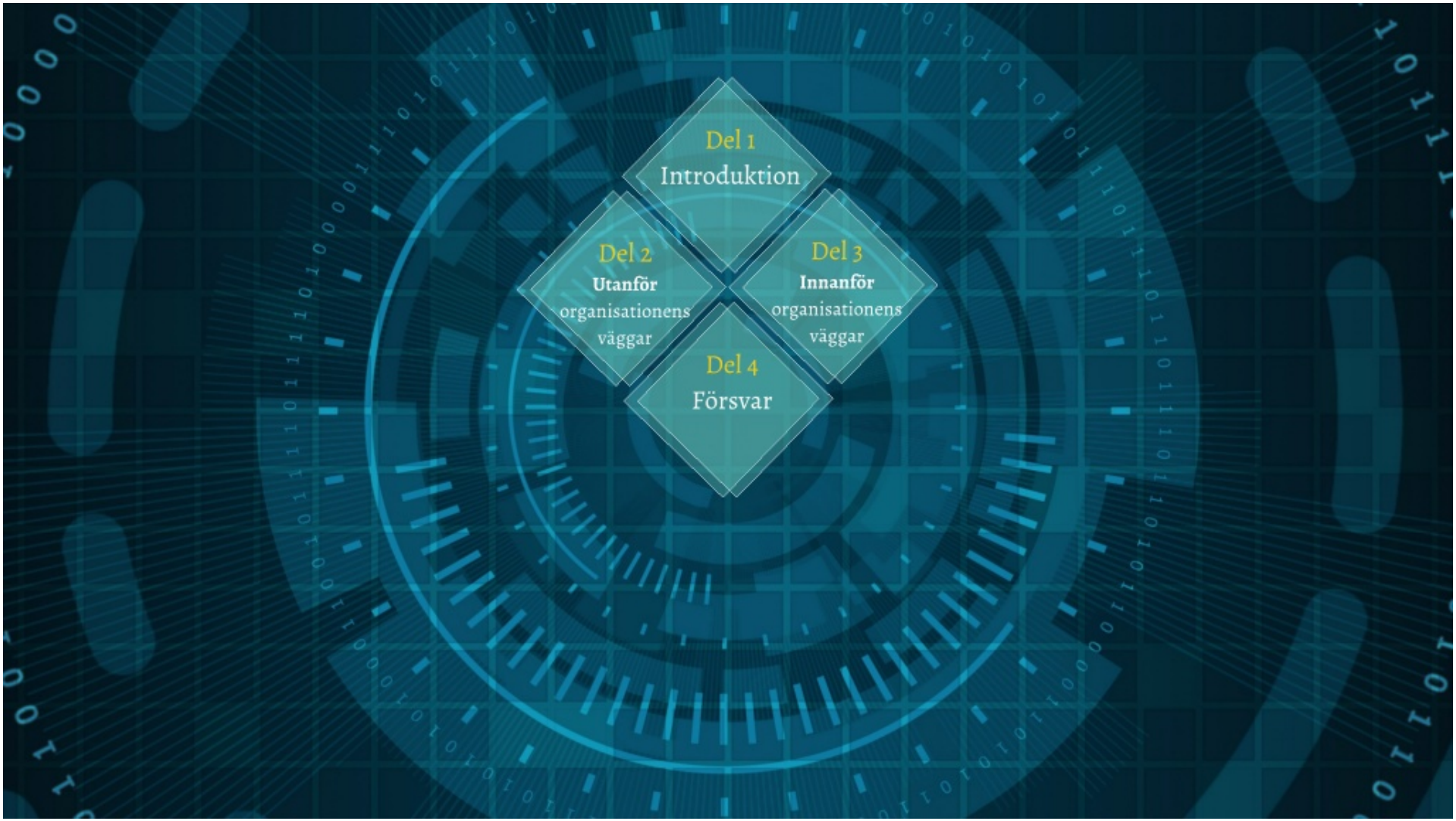
- Upptäcka, begränsa, lura
- *Målsättning*
  - Göra "tyst" förflyttning svår.
  - Få angriparen att snubbla på åtminstone en av många snubbeltrådar.

Åtgärder:

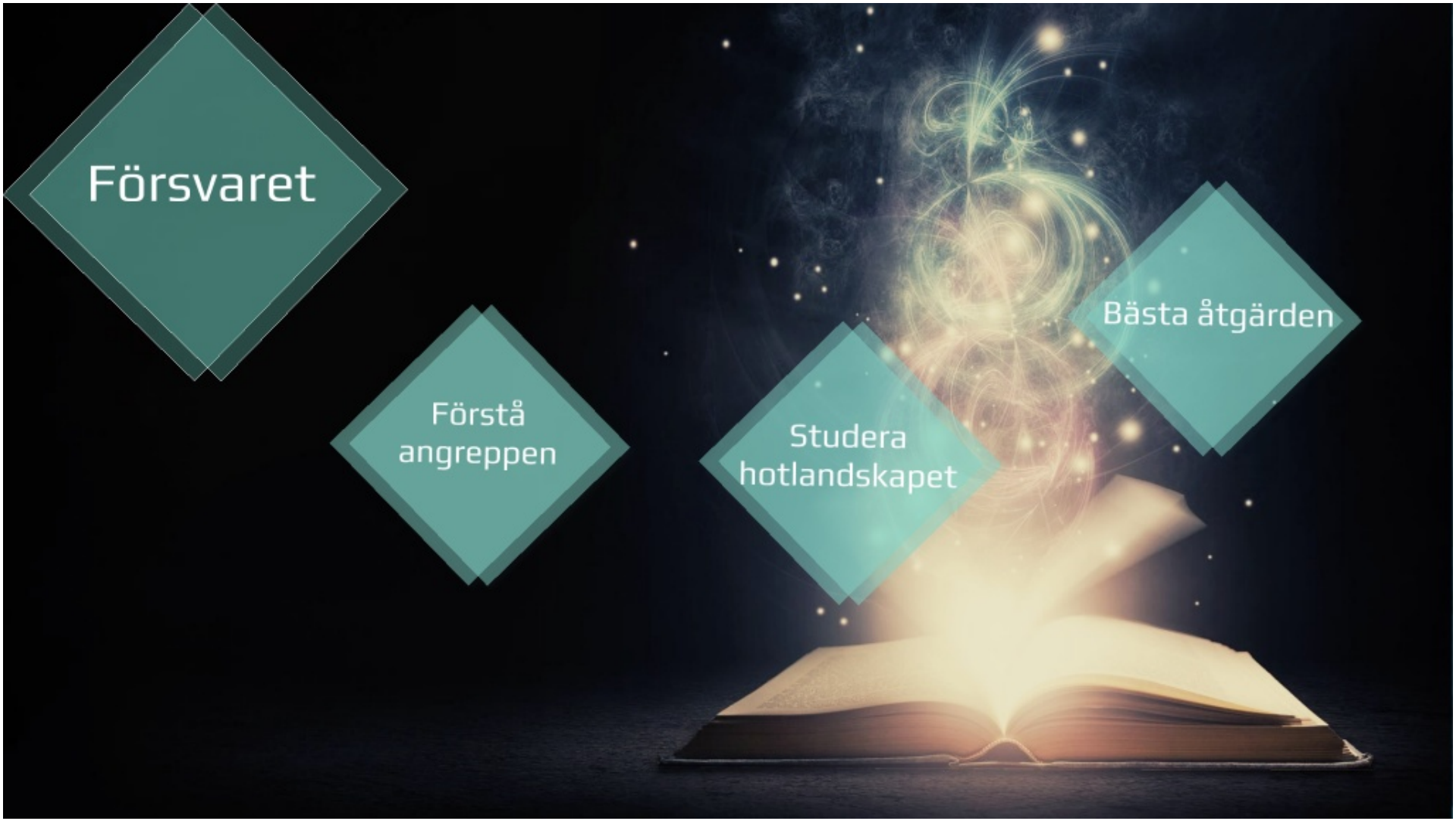
- Plantera "honungs-[allt-du-kan-komma-på]", men för guds skull... kom ihåg vilka!
- Logga händelser kopplade till fildelnings-enumerering.
- ... plus ett skepp-kommer-lastat med betydligt fler åtgärder.




Del 1
Introduktion
Del 2
Utanför
organisationens
väggar
Del 3
Innanför
organisationens
väggar


Del 1
Introduktion
Del 2
Utanför
organisationens
väggar
Del 3
Innanför
organisationens
väggar
Del 4
Försvar

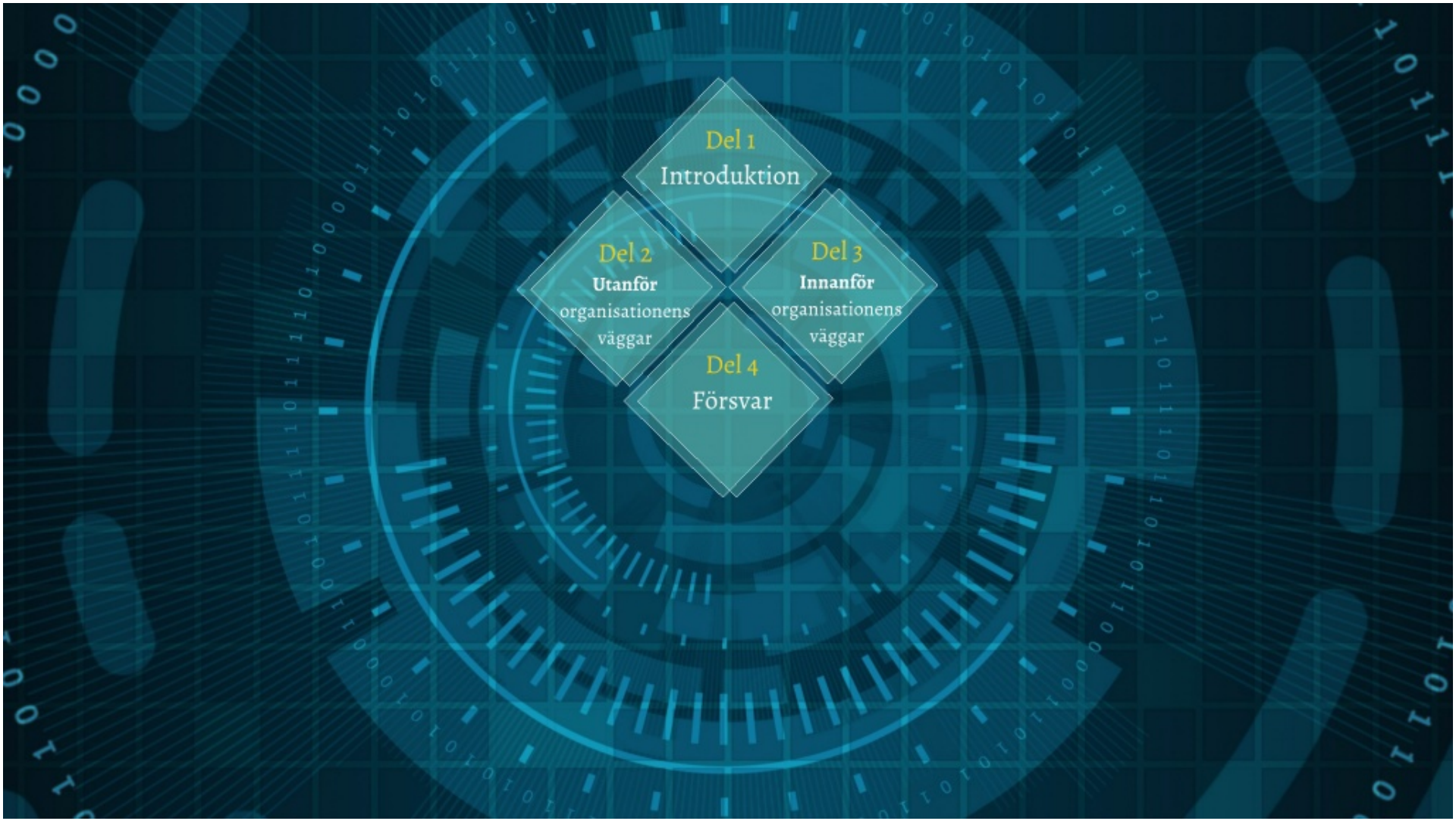

Försvaret

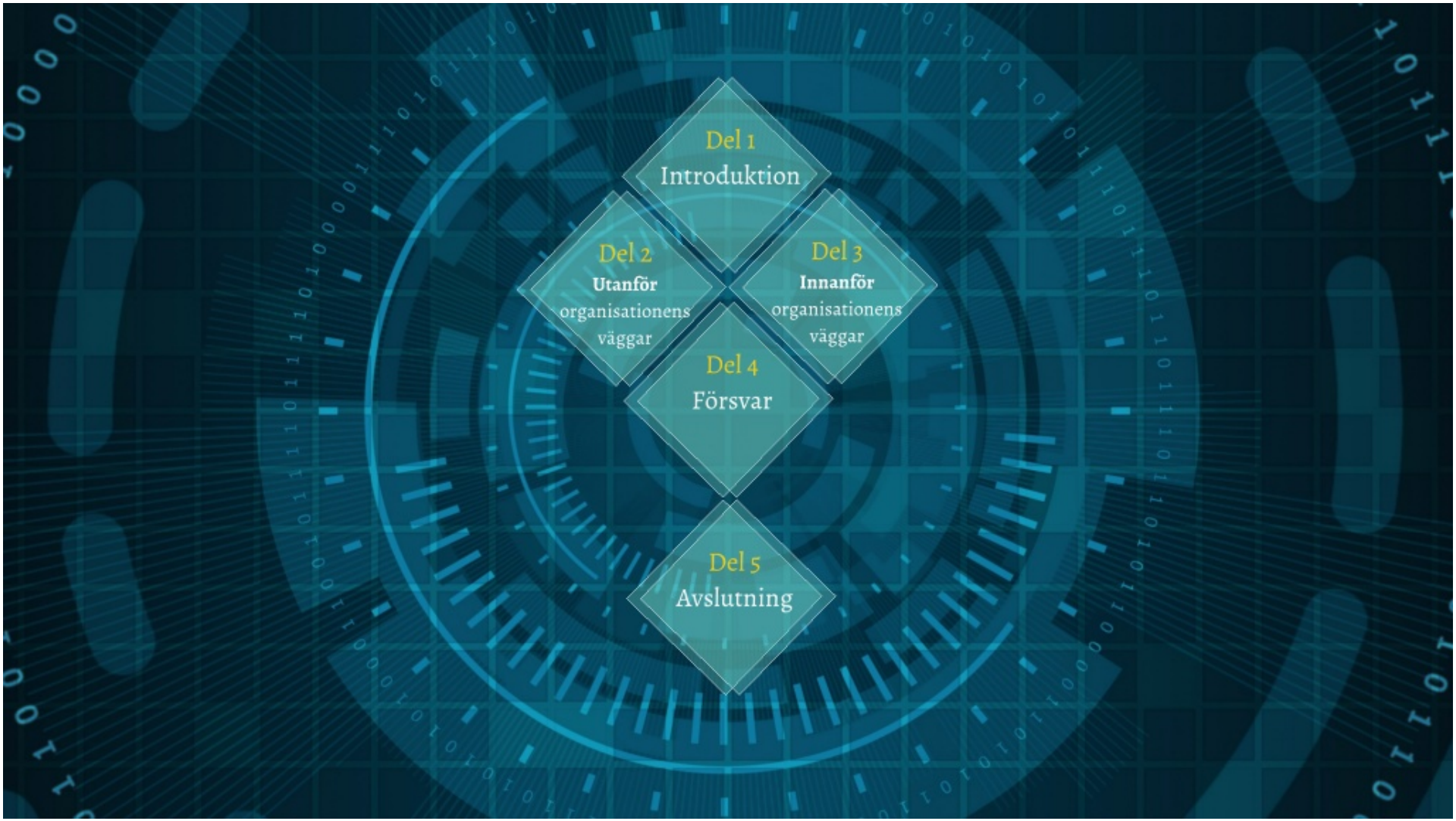

Försvaret
Förstå angreppen
Studera hotlandskapet
Bästa åtgärden


Förstå
angreppen
• Cyber Kill Chain
• MITRE ATT&CK

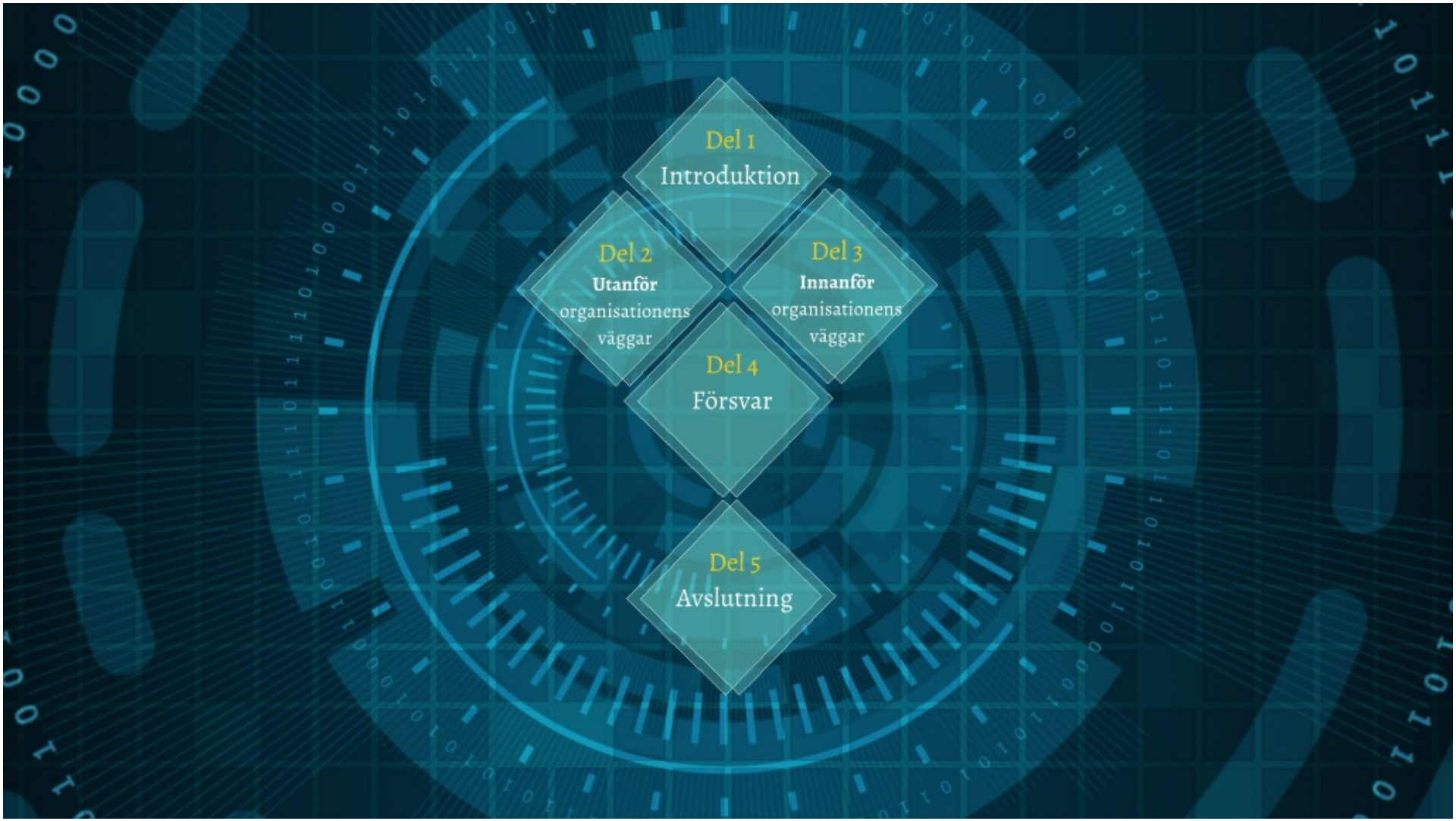

Studera hotlandskapet
• Läs rapporter och sammanställningar
• Förstå vad angriparna gör på riktigt
• Förstå ert sammanhang i det här:
• Hoten mot er bransch
• Vilka tillgångar har ni som angriparna faktiskt vill ha?


Bästa åtgärden
• Vitlista nätverkstrafik på klientnivå
• Se till att endast godkända applikationer kan kommunicera med Internet.
• Hindrar upprättande av C2, hindrar nedladdning av stage-moduler.
• Hindrar inte fullständigt autonoma programvaror (ovanliga)


Del 1
Introduktion
Del 2
Utanför
organisationens
väggar
Del 3
Innanför
organisationens
väggar
Del 4
Försvar


Del 1
Introduktion
Del 2
Utanför
organisationens
väggar
Del 3
Innanför
organisationens
väggar
Del 4
Försvar
Del 5
Avslutning


Avslutning
Christoffer Strömblad (Jedi Cybersäkerhet)
Polismyndigheten
Mejl: christoffer@cstromblad.com
Jobb: christoffer.stromblad@polisen.se
Tel: 073-374 50 86
Twitter: https://twitter.com/cstromblad
Blog: https://www.cstromblad.com/


Del 1
Introduktion
Del 2
Utanför
organisationens
väggar
Del 3
Innanför
organisationens
väggar
Del 4
Försvar
Del 5
Avslutning