

En resa genom Cyberangreppet

från angriparens perspektiv

av
Christoffer Strömblad
Polismyndigheten









A central diamond-shaped frame contains the text "Del 1" in yellow and "Introduktion" in white. The background features a complex, abstract design in shades of blue and black. It includes several concentric circles, a grid pattern, and binary code (0s and 1s) displayed in various orientations across the slide.

Del 1

Introduktion

Introduktion

Om föreläsningen

1. Följa ett
cyberangrepp

Fiktivt angrepp

2. Förstå förloppet

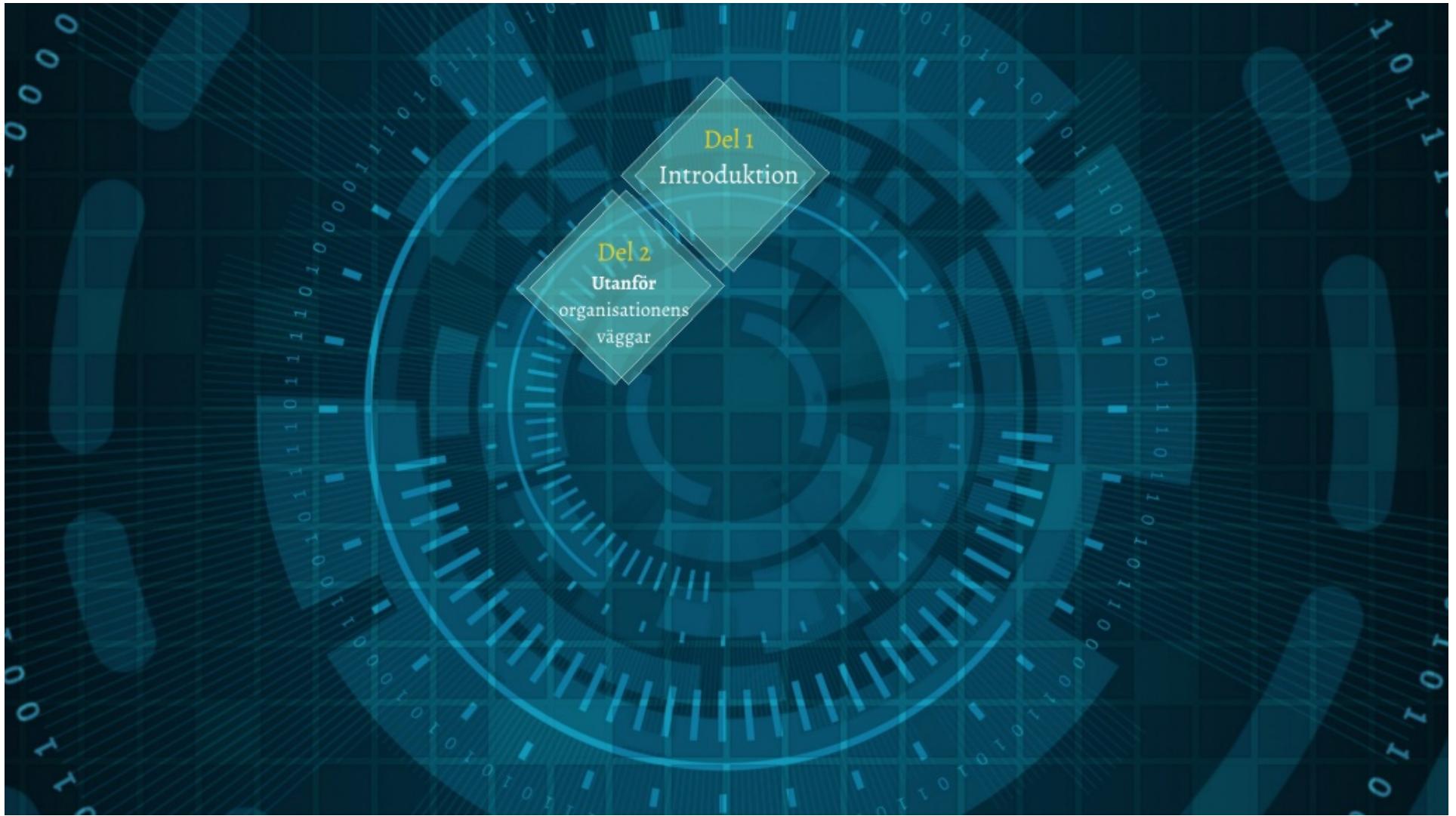
Faserna och
aktiviteterna

3. Skyddsåtgärder

Neka, lura,
fördröja...



Del 1
Introduktion





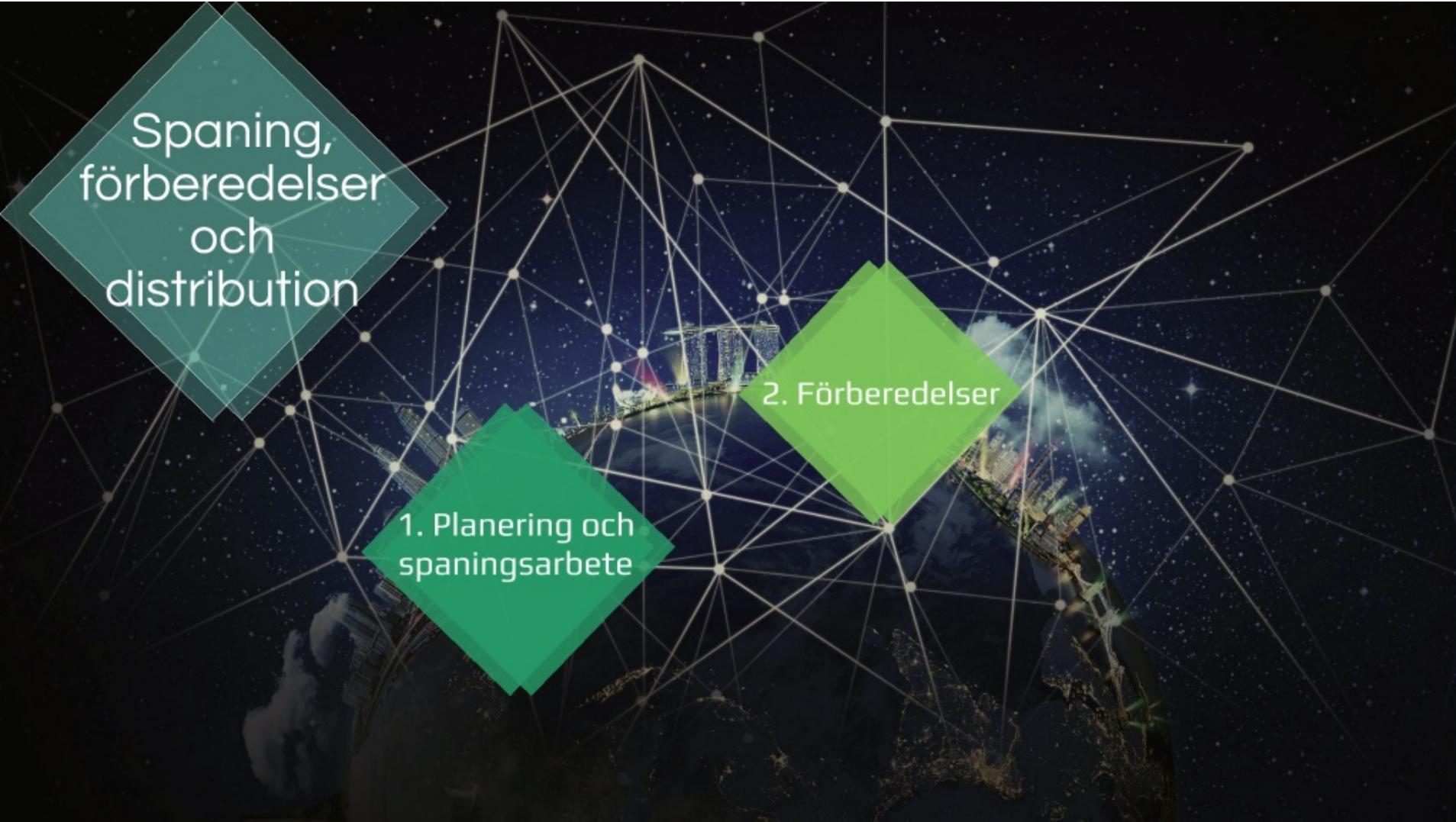
A large, semi-transparent teal diamond shape is positioned in the upper-left corner of the slide. Inside this diamond, the text "Spaning,
förberedelser
och
distribution" is written in white, sans-serif font.

Spaning,
förberedelser
och
distribution



Spaning,
förberedelser
och
distribution

1. Planering och
spaningsarbete



Spaning,
förberedelser
och
distribution

1. Planering och
spaningsarbete

2. Förberedelser

Spaning,
förberedelser
och
distribution

1. Planering och
spaningsarbete

2. Förberedelser

3. Distribution

1. Planering och spaningsarbete



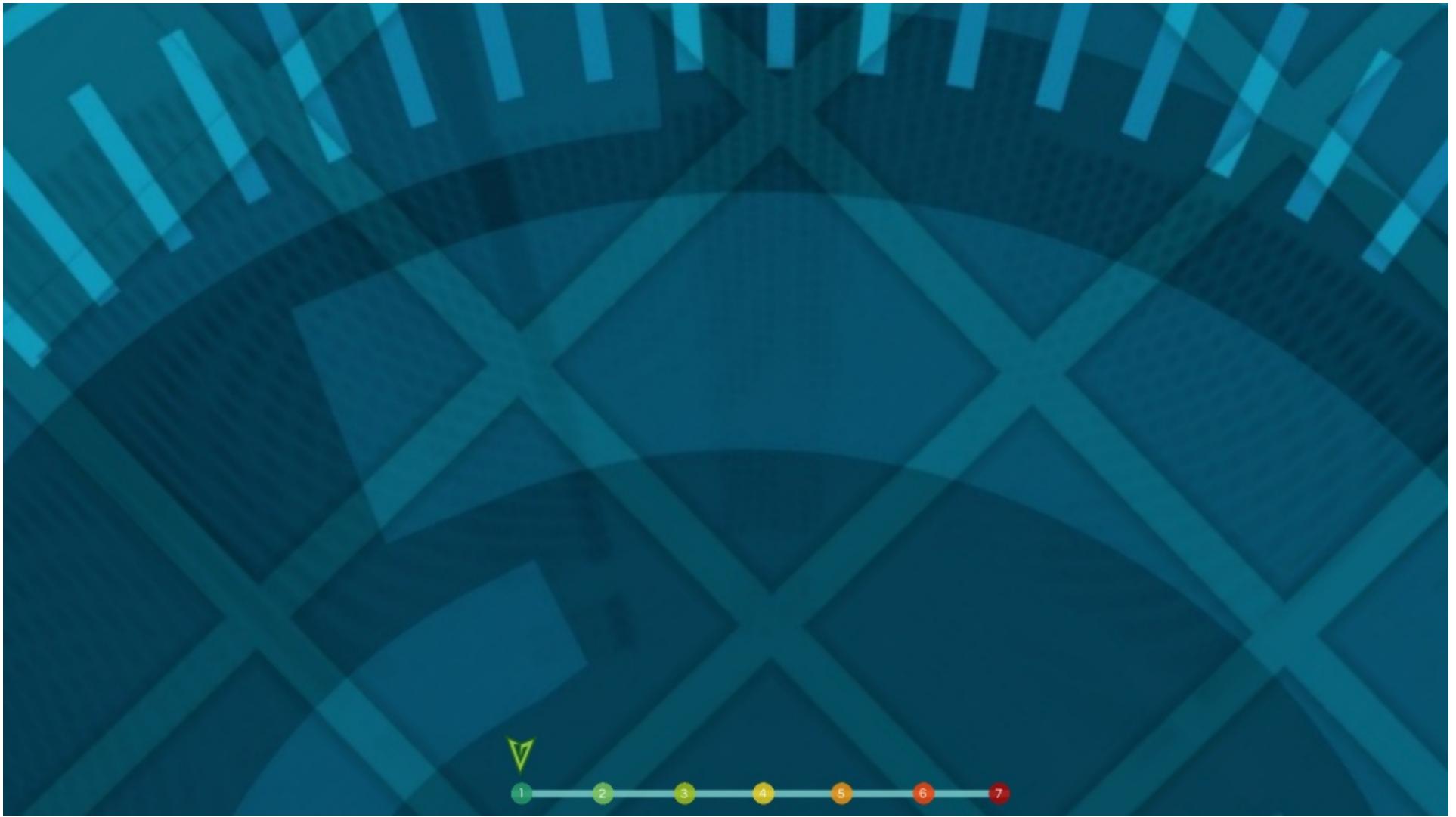


1. Planering och spaningsarbete

Angripare

Försvarare





Uppdraget

Vad?

Uppdragsgivaren vill:

- Inhämta kunskap och erfarenhet kring nanorobotar för cancerbehandling.
- För att uppnå den nationella målsättningen om teknologiskt oberoende 2025.



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.



Uppdraget

Vad?

Uppdragsgivaren vill:

- Inhämta kunskap och erfarenhet kring nanorobotar för cancerbehandling.
- För att uppnå den nationella målsättningen om teknologiskt oberoende 2025.

Företaget

Vilket?

I det här angreppet:

- Hitta en lämplig mottagare.
- Kolla LinkedIn kanske?
- Företagets hemsida.

Offret

Vem?

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.



Uppdraget

Vad?

Uppdragsgivaren vill:

- Inhämta kunskap och erfarenhet kring nanorobotar för cancerbehandling.
- För att uppnå den nationella målsättningen om teknologiskt oberoende 2025.

Företaget

Vilket?

I det här angreppet:

- Hitta en lämplig mottagare.
- Kolla LinkedIn kanske?
- Företagets hemsida.

Offret

Vem?

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.

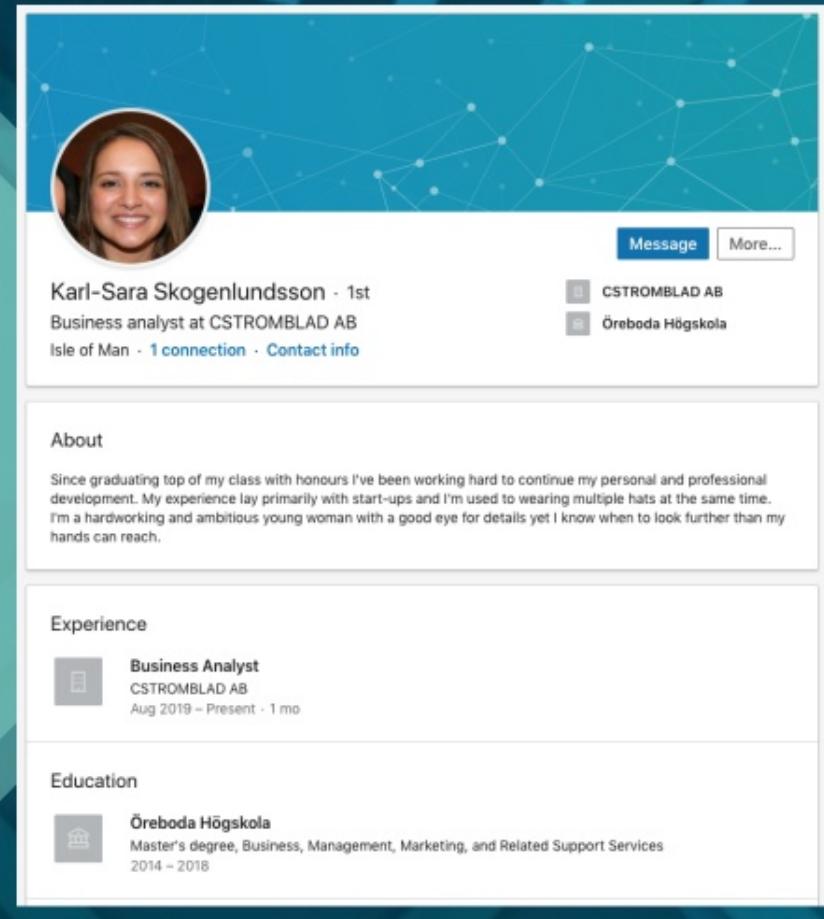
LinkedIn



Guldgruvan LinkedIn

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

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

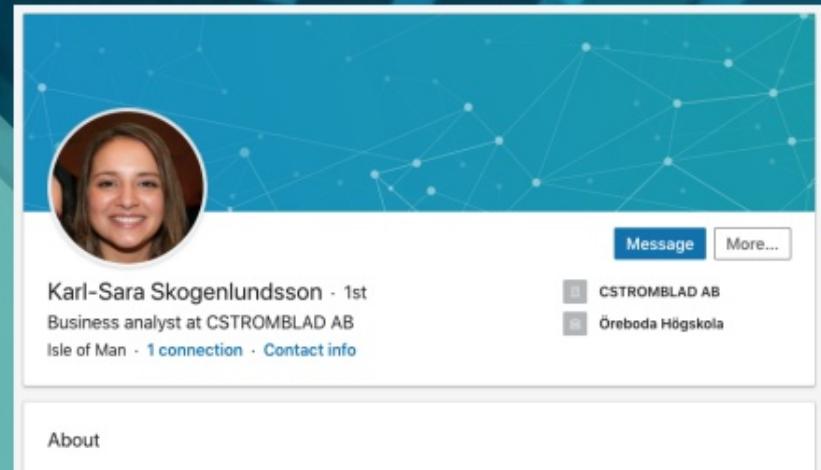


A screenshot of a LinkedIn profile page for Karl-Sara Skogenlundsson. The profile features a circular photo of a smiling woman with brown hair. The background of the page is a blue gradient with a network of white dots and lines, suggesting a digital or professional theme. At the top right, there are two buttons: "Message" and "More...". Below the photo, her name is listed as "Karl-Sara Skogenlundsson · 1st" and her title is "Business analyst at CSTROMBLAD AB". It also mentions "Isle of Man" and "1 connection · Contact info". On the far right, there are two small profile icons with the names "CSTROMBLAD AB" and "Öreboda Högskola". The main content area is divided into sections: "About", "Experience", and "Education". The "About" section contains a short bio: "Since graduating top of my class with honours I've been working hard to continue my personal and professional development. My experience lay primarily with start-ups and I'm used to wearing multiple hats at the same time. I'm a hardworking and ambitious young woman with a good eye for details yet I know when to look further than my hands can reach." The "Experience" section lists her role as "Business Analyst" at CSTROMBLAD AB from Aug 2019 to Present. The "Education" section shows she has a Master's degree in Business, Management, Marketing, and Related Support Services from Öreboda Högskola between 2014 and 2018.

Guldgruvan LinkedIn

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

Spear phishing - <https://attack.mitre.org/techniques>



A LinkedIn profile page for Karl-Sara Skogenlundsson. The profile picture shows a woman with brown hair smiling. The background of the page features a blue gradient with a network of white dots and lines, representing connectivity. At the top right, there are buttons for "Message" and "More...". Below the profile picture, her name is listed as "Karl-Sara Skogenlundsson · 1st" and her title is "Business analyst at CSTROMBLAD AB". It also mentions "Isle of Man" and "1 connection · Contact info". On the far right, there are two small profile icons with the names "CSTROMBLAD AB" and "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

The image consists of two main parts. On the left, a screenshot of a LinkedIn messaging interface. A message from 'Christoffer Strömlad' at 1:26 PM is shown, reading:

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)

Below the message are 'Like' and 'Okay' buttons. At the bottom, there's a 'Write a message...' input field and a 'Send' button. On the right, a LinkedIn profile page for 'Karl-Sara Skogenlundsson' is displayed. The profile picture shows a woman smiling. The bio reads:

Karl-Sara Skogenlundsson · 1st
Business analyst at CSTROMBLAD AB
Isle of Man · 1 connection · Contact info

Below the bio are sections for 'About' and 'Volunteer Experience'. The 'Volunteer Experience' section lists:

Fundraising Coordinator
Öreboda Kattförening
Apr 2017 – Present · 2 yrs 5 mos
Animal Welfare

Below that is a section for 'Education' listing:

Öreboda Högskola
Master's degree, Business, Management, Marketing, and Related Support Services
2014 – 2018

The image displays a composite view of digital communication and professional networking.

Messaging Interface:

- Message from Karl-Sara Skogenlundsson:** "Tack vad spännande!" (Thank you for the interesting information!).
- Message from Christoffer Strömlad:** "Hej,
Jag skulle vilja skicka över lite information om hur vi eventuellt
skulle kunna bidra med finansiering av Öreboda Kattförening.
Har du möjligheten att skicka detta till? Har du möjligheten att skicka detta till?
mvh,
Christoffer (aka. Roy)"

LinkedIn Profile (Karl-Sara Skogenlundsson):

- Profile Picture:** A circular photo of a smiling woman with brown hair.
- Basic Info:** Karl-Sara Skogenlundsson, 1st connection at CSTROMBLAD AB, Isle of Man.
- Buttons:** "Message" and "More..."
- Background:** A blue network graph pattern.

Volunteer Experience:

- Role:** Fundraising Coordinator
- Organization:** Öreboda Kattförening
- Duration:** Apr 2017 – Present • 2 yrs 5 mos
- Description:** Animal Welfare

Education:

- Institution:** Öreboda Högskola
- Degree:** Master's degree, Business, Management, Marketing, and Related Support Services
- Years:** 2014 – 2018

Försvarare Vad gör vi?

Försvarstrategi:

- Lura och förvränga.
- Målsättning:
 - Förmedla en alternativ verklighet.
 - Skapa osäkerhet.

Åtgärder:

- Falska profiler på LinkedIn
- "Felaktig" information i DNS
- "Öppna" portar (HoneyPots)
- Honung över hela stället...



2. Förberedelser

Angripare

Försvarare



Angriparen

Förbereda
bifogade filer



Angriparen

Förbereda bifogade filer

Stage 1 - PDF med länk till Google Drive



Angriparen

Förbereda bifogade filer

Stage 1 - PDF med länk till Google Drive



Hej Kar - Sven,
Kärkommen hälsningar från den svenska hälften till den franska Ördbotskambrén ing. Kar & Sven.
Skriftet detta innehåller flera linjer som inte ska vara siktade av en skrivmaskin, men som är lätt att se för en mänsklig ögon. Detta är en teknik som heter "Watermark".
Vad kan du göra om du hittar denna teknik i ett dokument? Ta ut ett foto av det och skicka det till mig så kan jag hjälpa dig att få bort tekniken.

<https://docs.google.com/open?id=1HxG-1pGzH2-TWAvdVorGwhtLjuk3>

mvn,
Ray

Stage 2 - Word-dokument med Makron.



Vänligen se till att fylla i följande ord i ditt dokument:



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



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).



Försvarare

Vad gör vi?

Försvarstrategi:

- Neka och begränsa.
- *Målsättning*
 - Tidigt avväpna.
 - Försvara angräpset.
 - Öka resursanvändning och nödvändiga insatser.

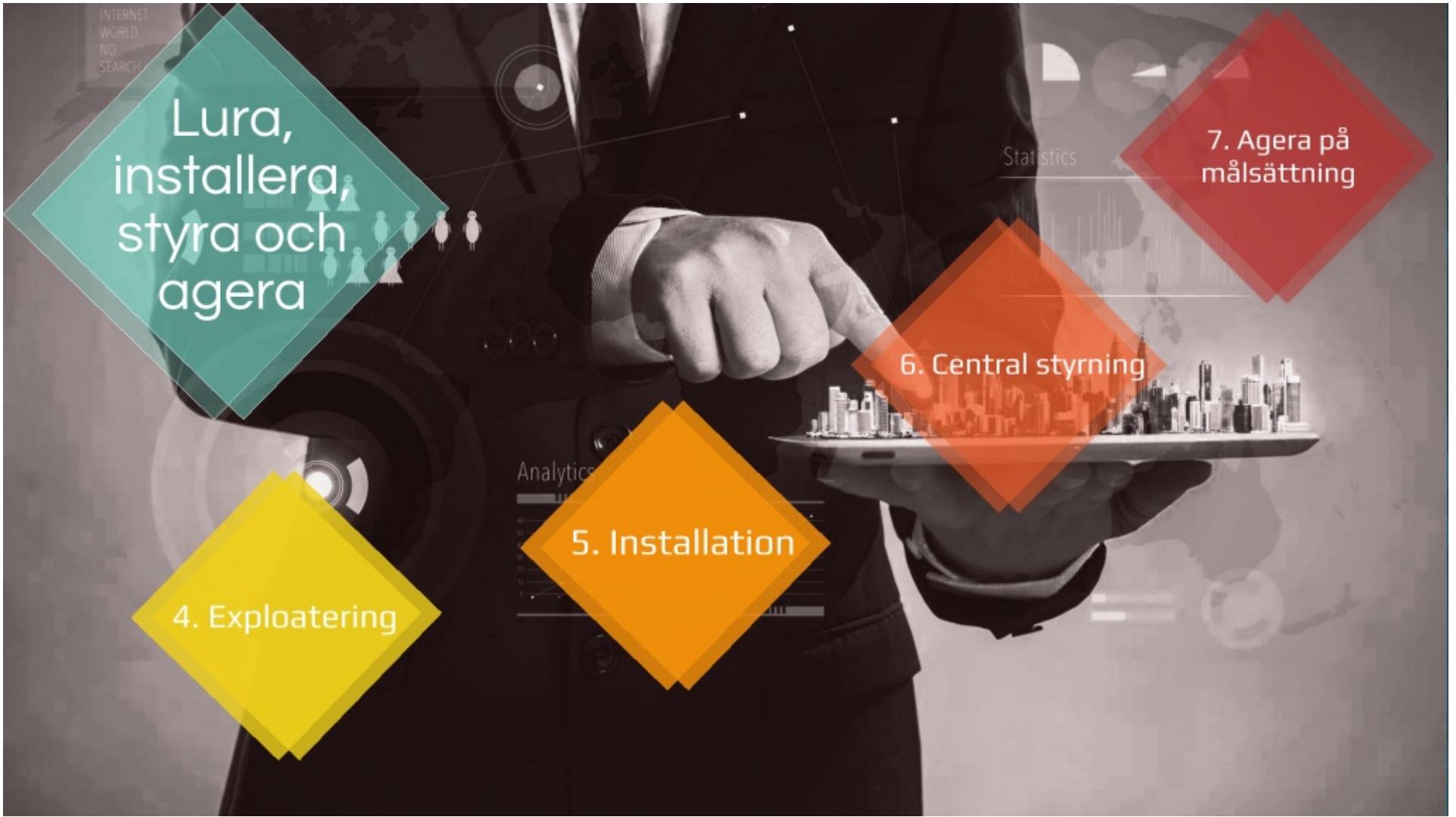
Åtgärder:

- 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.)









4. Exploatering

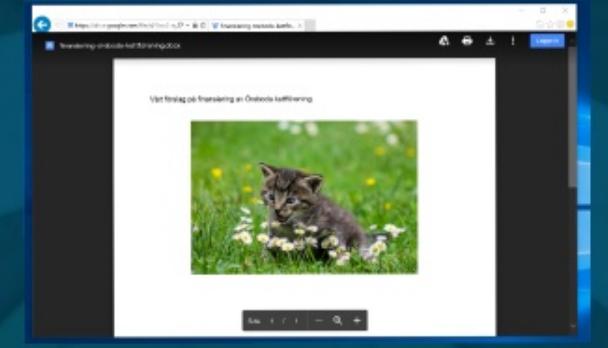
Angriparen

Försvarare

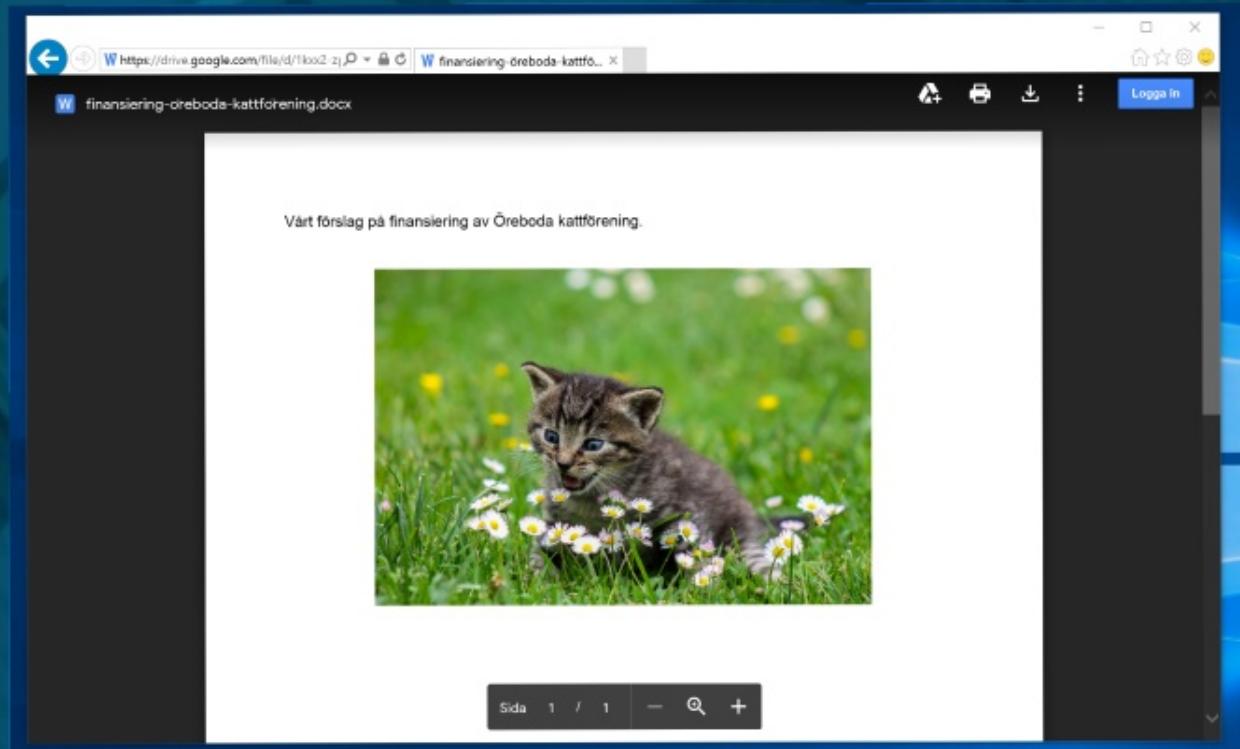
Lurar användaren

Angruppen
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



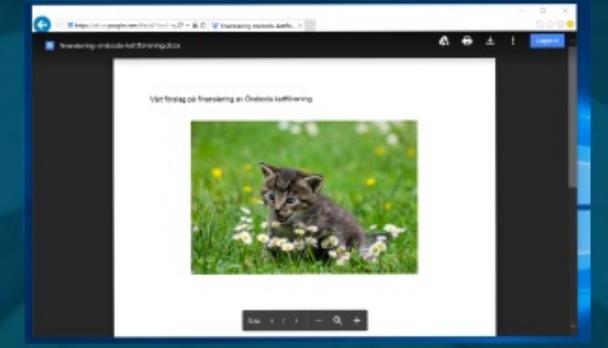
6

7

Lurar användaren

Angruppen
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".

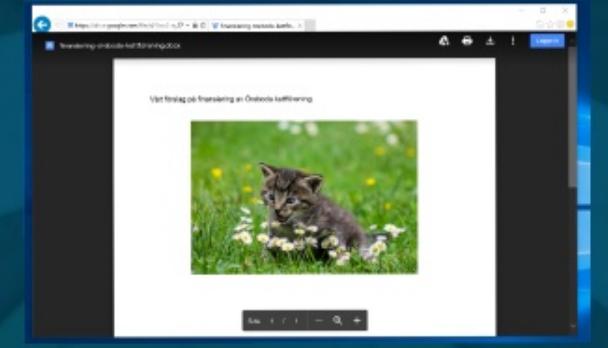


Lurar användaren

Angruppen
Gör...

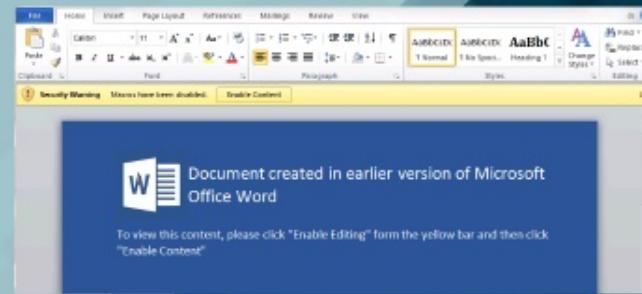
Aktivera
makron

- 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".

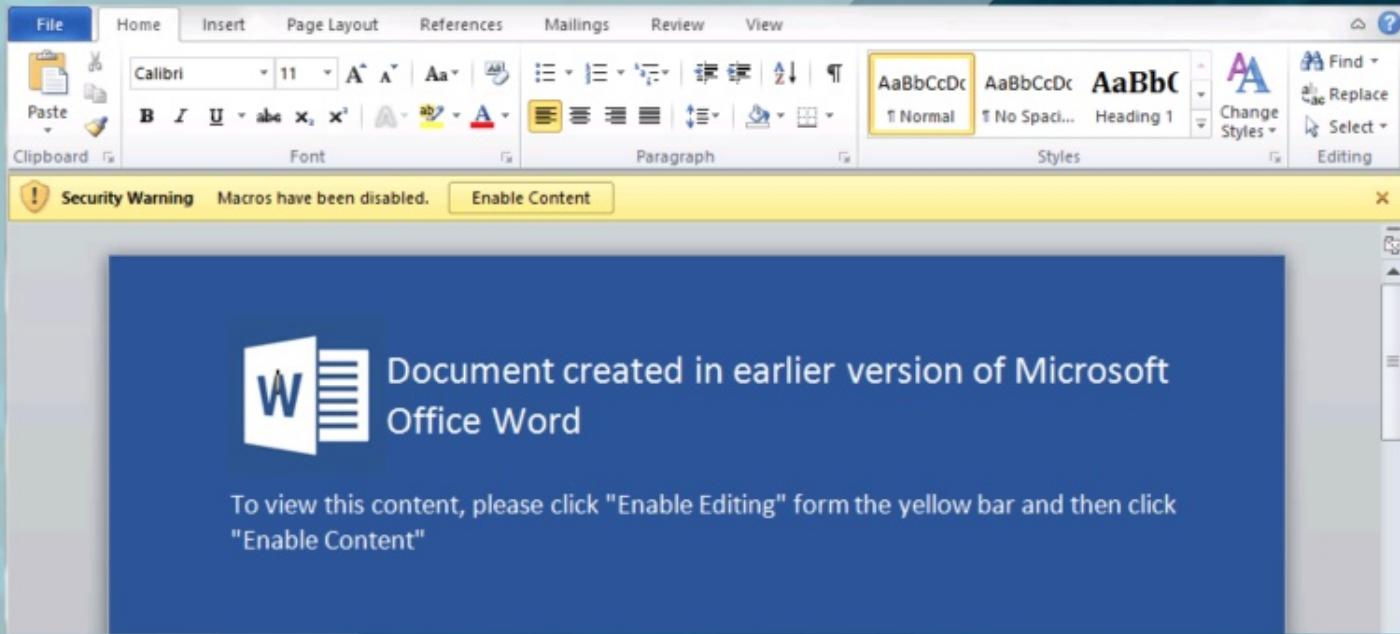


Word - Aktivera makron

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



Polytechnikum arens infrastruktur.



Försvarare

Vad gör vi?

Försvarstrategi:

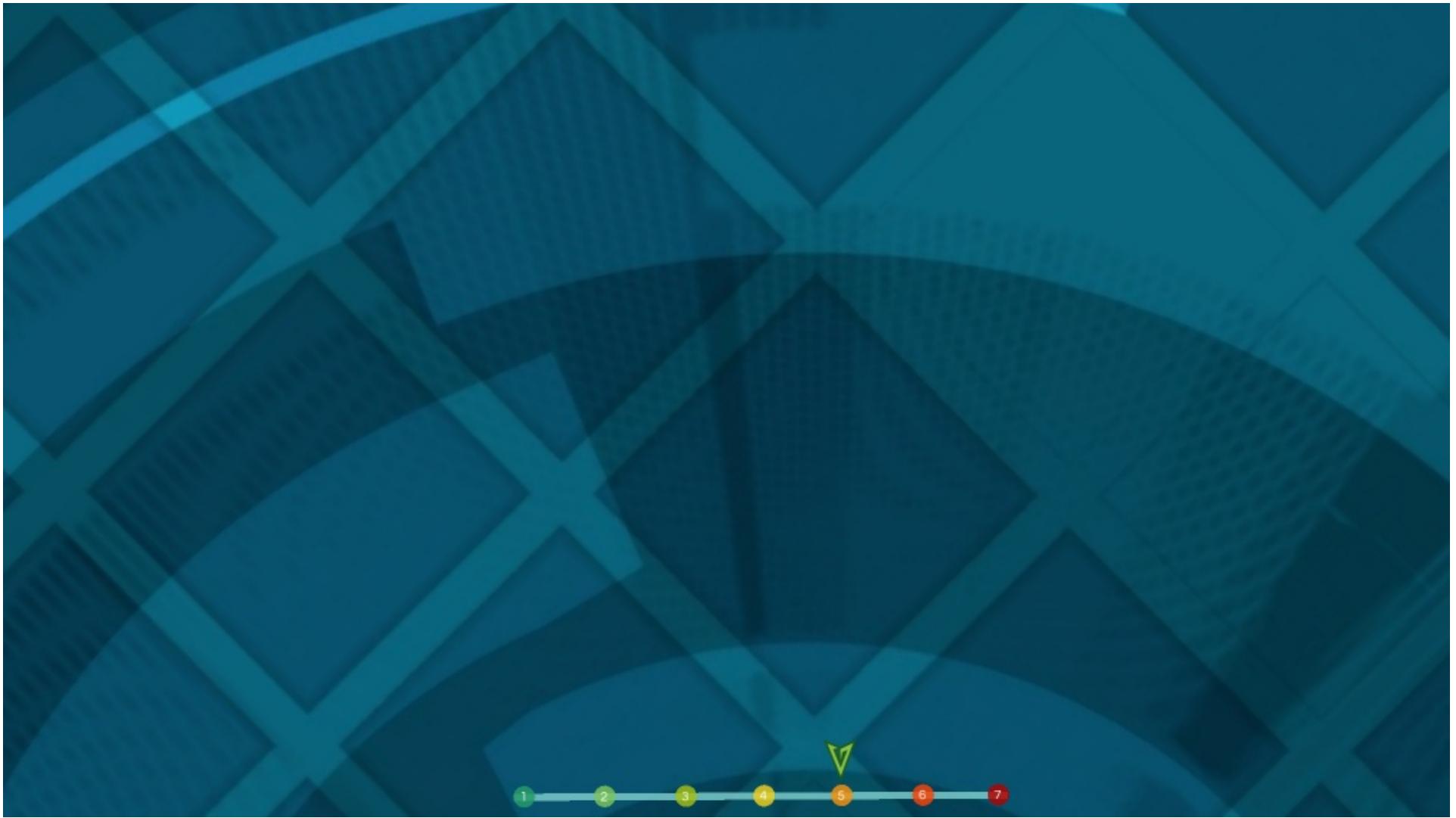
- Neka, begränsa och upptäcka.
- *Målsättning*
 - Begränsa "navigerings"-utrymmet.

Åtgärder:

- Tillåta endast signerade makron, alternativt stänga av helt.
- Begränsa Word/Excel möjligheter att kommunicera med Internet.







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"                  ' 3B Seconds  
trigger.Delay = "PT30S"  
  
'*****  
' 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"                  ' 3B Seconds  
trigger.Delay = "PT30S"  
  
'*****  
' 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 schemalagda jobb.
- Begränsar Word från att prata med Internet.



6. Central styrning



6. Central styrning





Upprätta kommunikation

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



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.



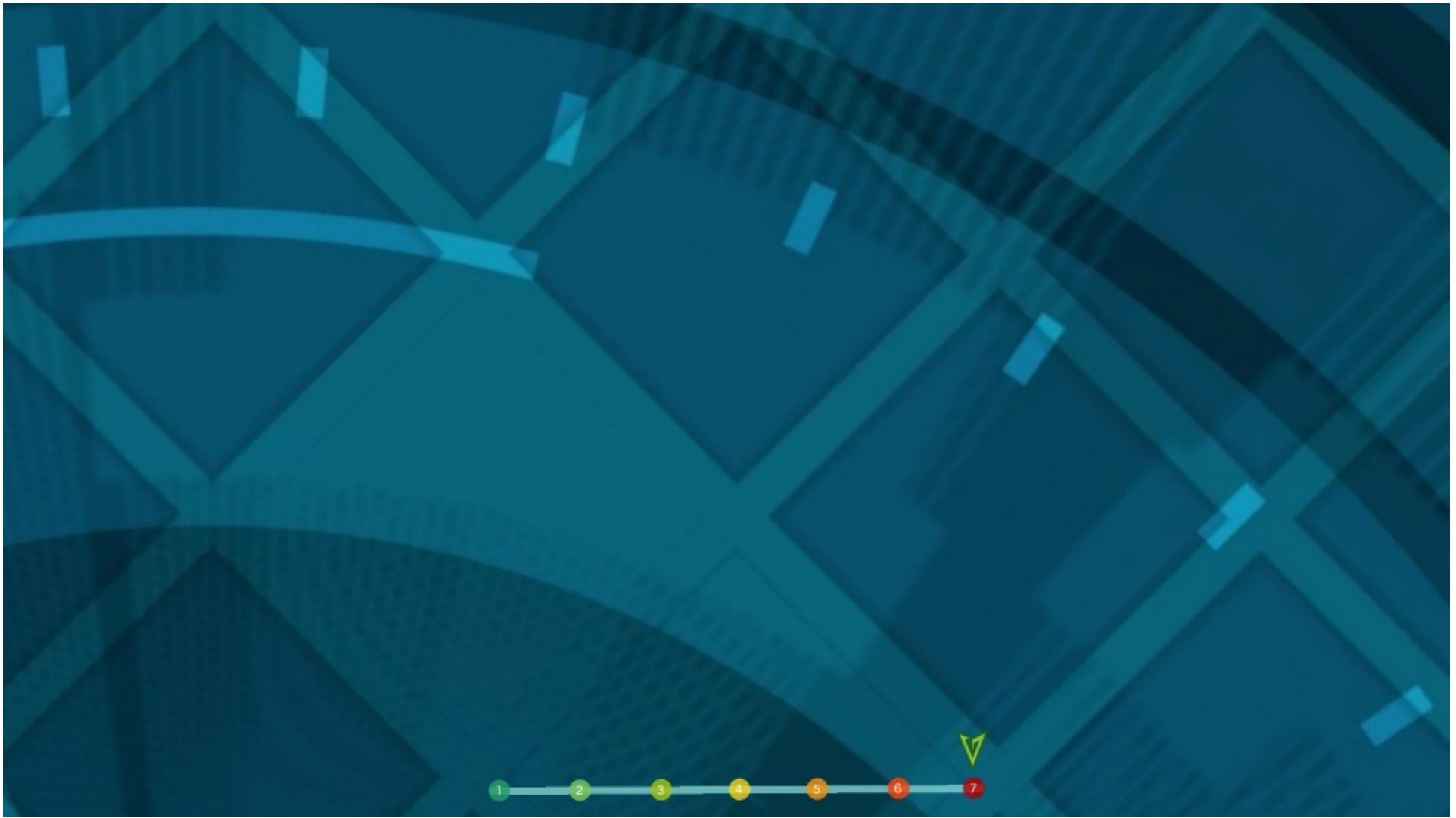


7. Agera på målsättning

Angriparen

Försvarare





Ladda ner moduler

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



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:

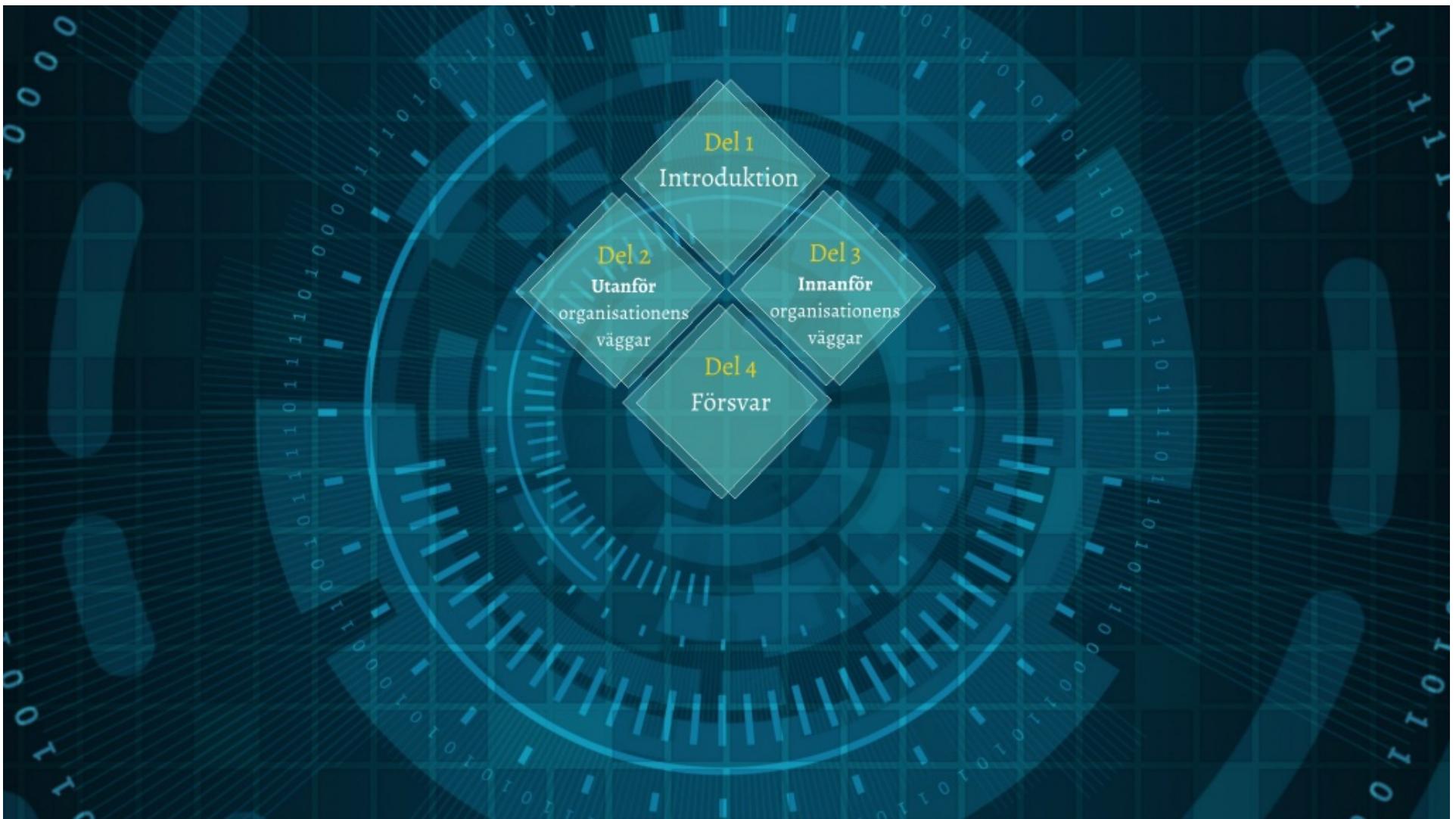
- Upptäcka, begränsa, lura
- Målsättning
 - Göra "tyst" förflyttning svår.
 - Få angriparen att snubbla på åtminstone en av många snubbeltrådar.

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.

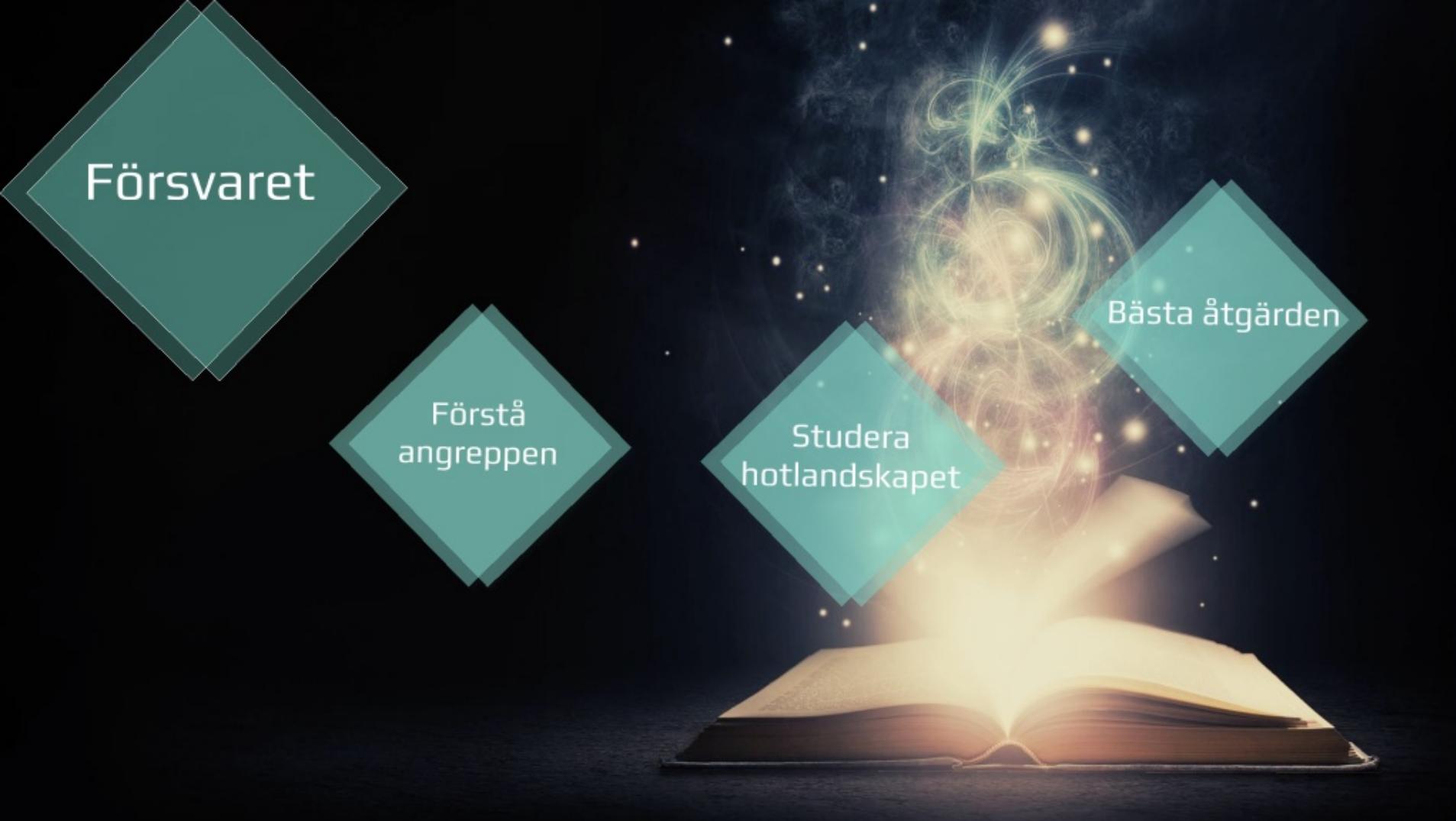






Försvaret





Försvaret

Förstå
angreppen

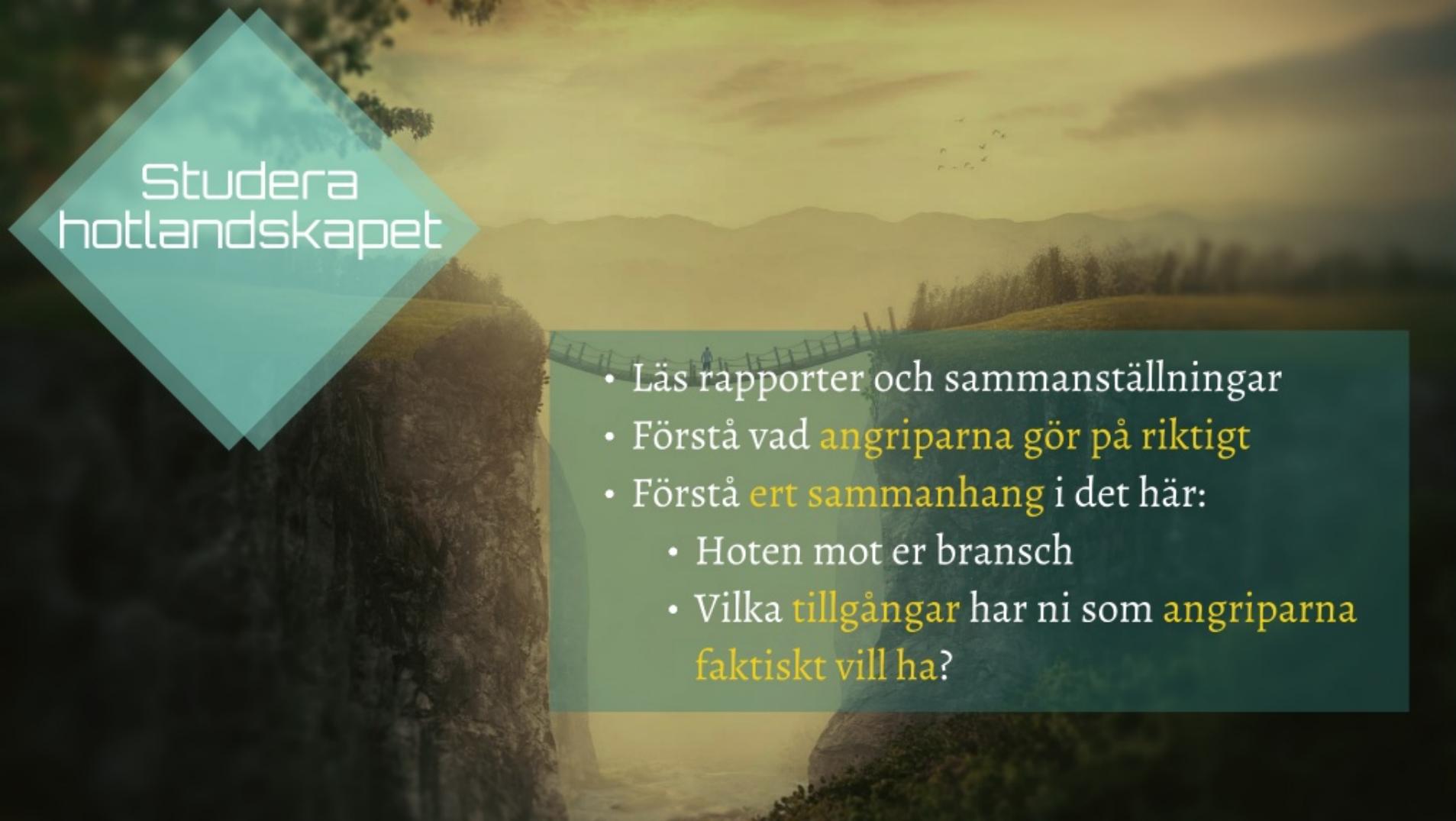
Studera
hotlandskapet

Bästa åtgärden



Förstå angreppen

- Cyber Kill Chain
- MITRE ATT&CK



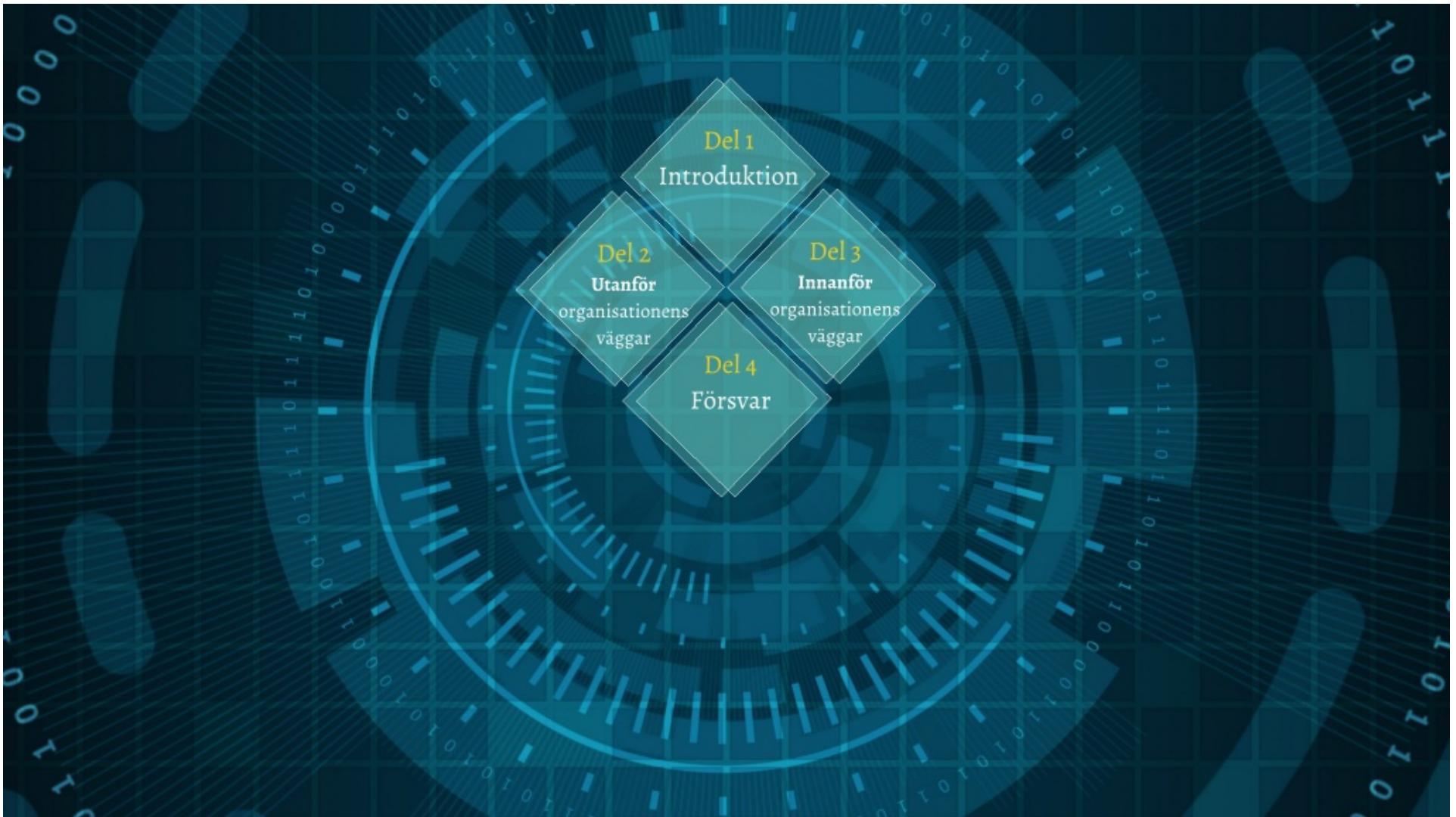
Studera hotlandskapet

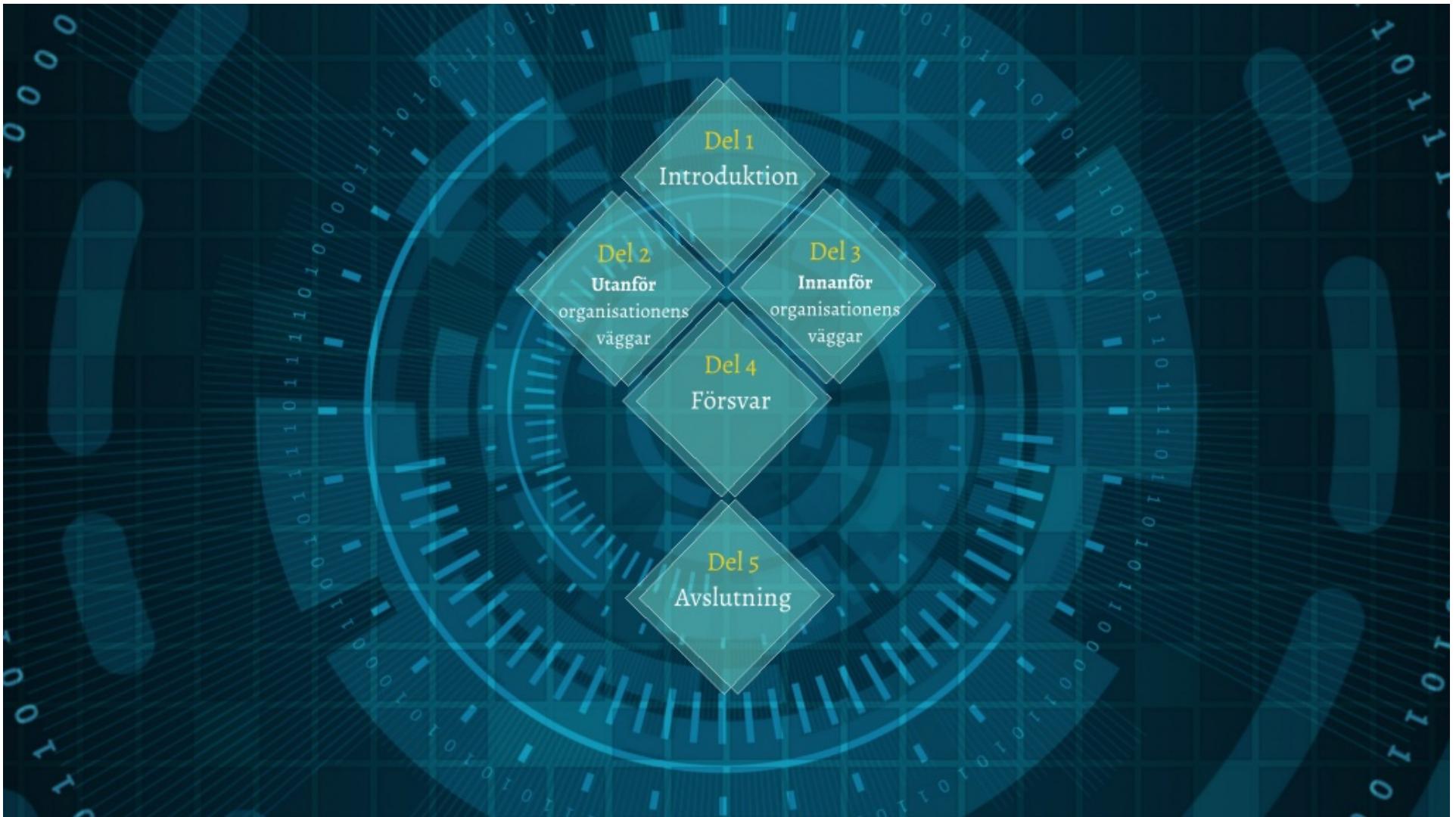
- Läs rapporter och sammanställningar
- Förstå vad **angriparna gör på riktigt**
- Förstå **ett sammanhang i det här:**
 - Hoten mot er bransch
 - Vilka **tillgångar** har ni som **angriparna faktiskt vill ha?**



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)





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/>

