

# NETVÆRKS- ARKITEKTUR

PBA I CYBERSIKKERHED



APPLIKATION

PRÆSENTATION

SESSION

TRANSPORT

NETVÆRK

DATALINK

FYSISK

1	2	3	4	5	6	7
Virksomheds - forståelse	Kommunikation og rapportering	Cybersikkerheds - governance	Systemsikkerhed	Praktik	Valgfag 3	Lokalt fagelement Cybersikkerhed ; Metode og Formidling
Programmering	Automatisering og scripting	Lokale fagelementer: Industriel informationssikkerhed	Netværks - og kommunikationssikkerhed			Bachelor

Computerarkitektur	Computerarkitektur	Valgfag 1
Netværksarkitektur	Netværksarkitektur	Valgfag 2

### 3.4. Integreret Cybersikkerhed, 2. semester – 40 ECTS

#### Læringsmål for prøven

Læringsmål for prøven er identisk med læringsmålene for fagelementerne Computerarkitektur (10 ECTS), Netværksarkitektur (10 ECTS), Automatisering og Scripting (5 ECTS), Datasikkerhed (5 ECTS) samt Kommunikation og rapportering (10 ECTS), som fremgår af den nationale del af studieordningen.

#### Prøveform og tilrettelæggelse herunder evt. formkrav

Prøven er en mundtlig eksamen med afsæt i dels et projekt udarbejdet i grupper og dels en individuel synopsis pba. gruppeprojektet samt trækspørgsmål til eksamen.

Alle spørgsmål, der kan trækkes til eksamen, er udleveret til de studerende mindst 14 dage før eksamen, så de studerende har mulighed for at forberede sig på alle eksamensspørgsmål. Ud af de på forhånd udleverede spørgsmål, trækker den studerende ét spørgsmål inde til eksamen. Der er ingen forberedelse på selve eksamensdagen.

HUSK



## Forudsætninger for at gå til eksamen – deltagelsespligt og aflevering

*Forudsætning 1:* For at gå til prøven skal den studerende have min. 80% fremmøde i hvert af fagelementerne Computerarkitektur, Netværksarkitektur, Automatisering og Scripting, Datasikkerhed samt Kommunikation og rapportering, herefter blot benævnt fagelementerne. Den studerende kan følge sin fremmødeprocent i Attender.

# 3 mål for dagen

- Hvorfor netværk
- Hvad er min IP? (hvad er IP?)
- Første "mini netværk"

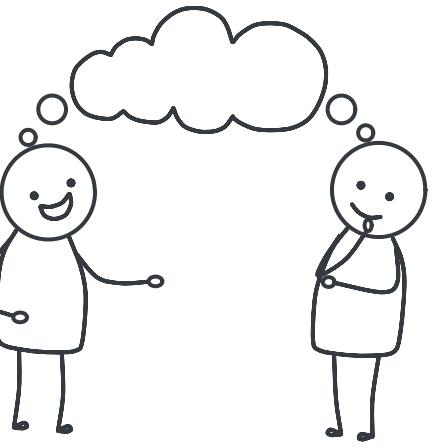
# Netværksarkitektur - CSIK



Fagelementet beskæftiger sig med netværksudstyr og komponenter og de forskellige udfordringer i netværk knyttet til cybersikkerhed

herunder specificering af relevante sikkerhedskrav til en netværksløsning i cloud- og hybridmiljø. Fagelementet beskæftiger sig med praktisk opsætning, drift og sikring af mindre netværk.

# Netværksarkitektur - CSIK



håndtere komplekse og udviklingsorienterede situationer i forhold til at designe, herunder opdele, simple netværk i segmenter ved brug af netværksudstyr

håndtere komplekse og udviklingsorienterede situationer i forbindelse med analyse af netværkstrafik med henblik på at forebygge eller afbøde angreb

# Hvorfor netværksviden er fundamental

Netværk er angrebsvejen: Næsten alle cyberangreb sker gennem netværk

grundlæggende forståelse af  
netværkstrafik er essentiel

"You can't defend what you don't understand"

Detektering og respons: Anomalier i netværkstrafik er ofte første tegn på kompromittering

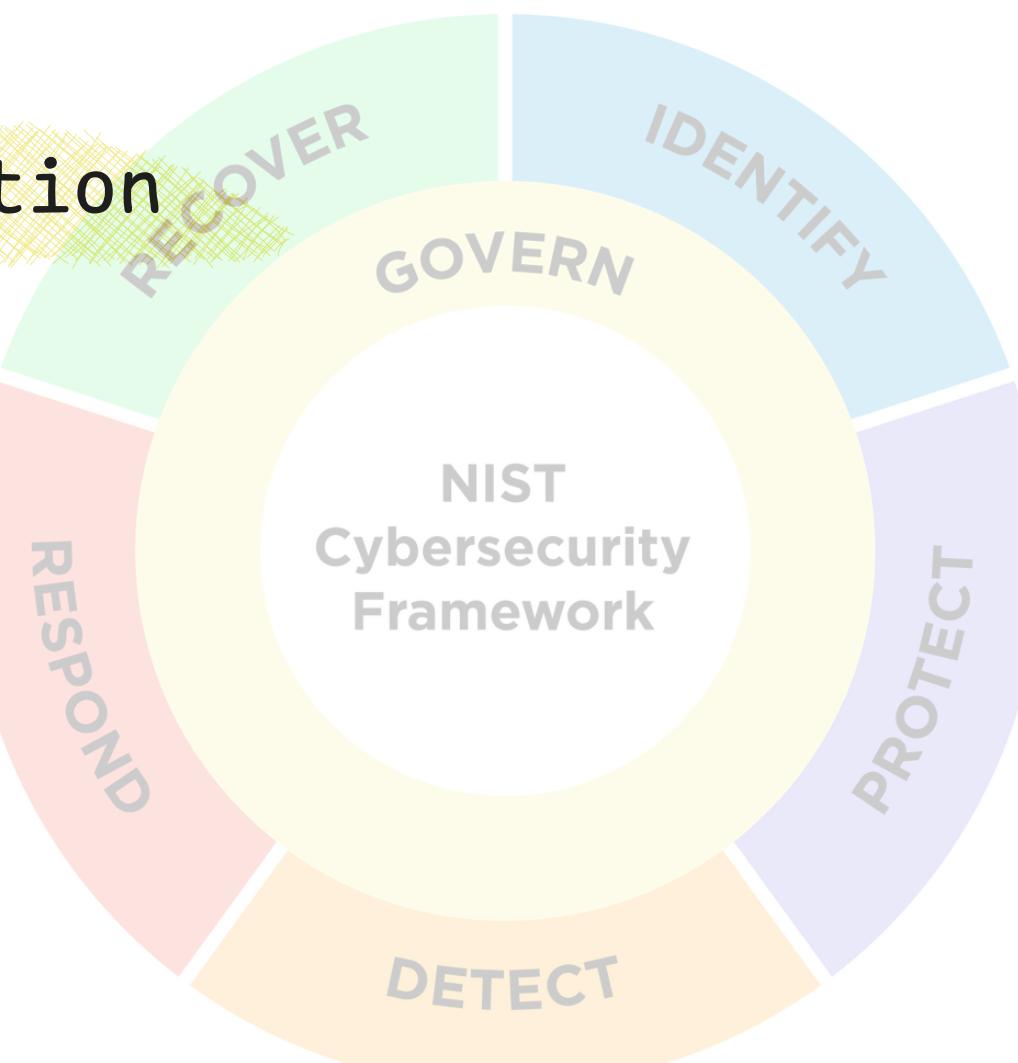
# Praktiske anvendelser

Incident Response: Sporing af lateral movement gennem netværket

Threat Hunting: Identificering af mistænkelig trafik og kommunikation

Forensic: Rekonstruktion af angrebsforløb gennem netværkslog

Beskyttelse: Konfiguration af firewalls, IDS/IPS og network segmentation



# Konkrete netværkskompetencer

Protokolforståelse: TCP/IP, HTTP/HTTPS, DNS, DHCP m.fl

Netværksanalyse: Wireshark, tcpdump, netstat

Log-analyse: Firewall logs, proxy logs, DNS logs

Netværkstopologi: Forståelse af subnets, VLANs, routing

# Konsekvenser af manglende netværksviden

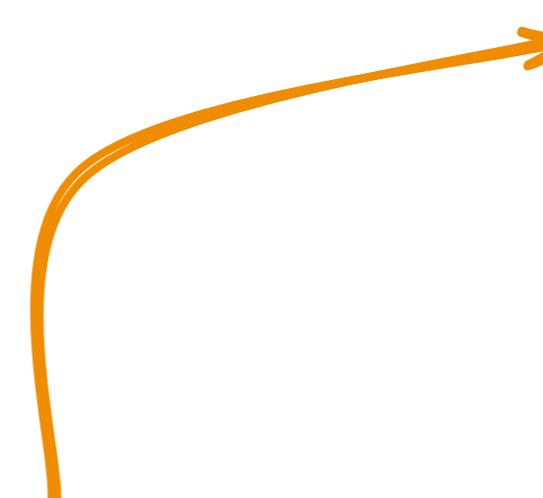
network literacy

Blind spots: Kan ikke identificere unormal trafik

Ineffektiv incident response: Langsom containment og kan ikke tracke lateral movement

Misconfigurations: Security gaps i firewall rules, network segmentation og access controls

Compliance issues: Manglende opfyldelse af regulatory requirements omkring network monitoring og logging



## 2. Håndtering af hændelser

*Det siger NIS 2-loven:*

### **§ 6, stk. 1, nr. 2**

### *Håndtering af hændelser*

*Det følger af det foreslæde nr. 2, at foranstaltningerne skal omfatte eller tage højde for håndtering af hændelser.*

*Dette indebærer bl.a., at enheder skal udarbejde procedurer for håndtering af hændelser. Enheder skal i fornødendt omfang implementere logning og monitorering af uregelmæssigheder i enhedens net- og informationssystemer med henblik på at kunne identificere hændelser. Logdata skal derudover sikres mod manipulation og beskyttes mod uautoriseret adgang.*



VEJLEDNING TIL NIS 2-LOVEN

# IMPLEMENTERING AF CYBERSIKKERHEDS- FORANSTALTNINGER

## B. LOGNING OG MONITORERING

### **Formål**

At enheden er i stand til at opdage hændelser, der kan bringe data i fare, og reagere passende og derved i videst mulige omfang afværge skadesvirkningen af hændelsen. Logs anvendes også til at undersøge hændelsen efterfølgende.

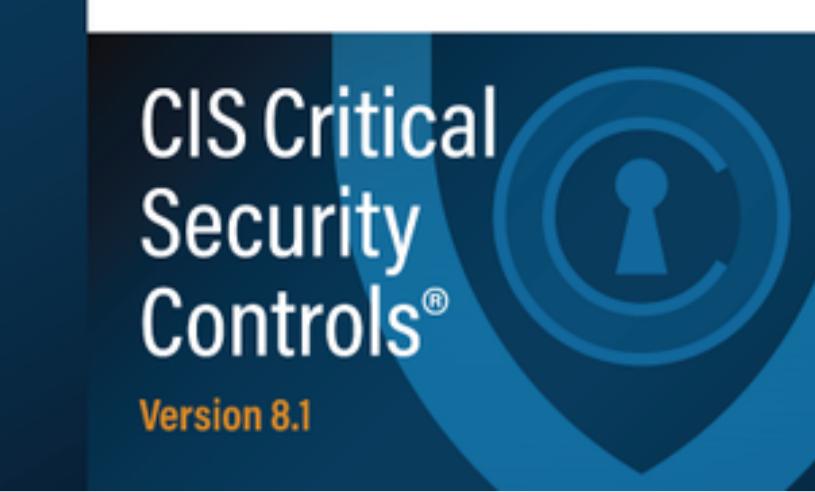
### **Foranstaltning**

Enheden skal i nødvendigt omfang have processer og bruge værktøjer til at monitorere og logge samt reagere på aktiviteter på deres netværk og i deres informationssystemer. Hermed bliver enheden i stand til at opdage eventuelle hændelser og reagere i overensstemmelse hermed for at afbøde virkningerne.

Monitorering bør så vidt muligt være automatiseret (f.eks. Intrusion Detection Systems) og kan udføres enten i realtid eller med regelmæssige intervaller, afhængigt af virksomhedens muligheder.

# CIS Critical Security Controls

## Version 8.1



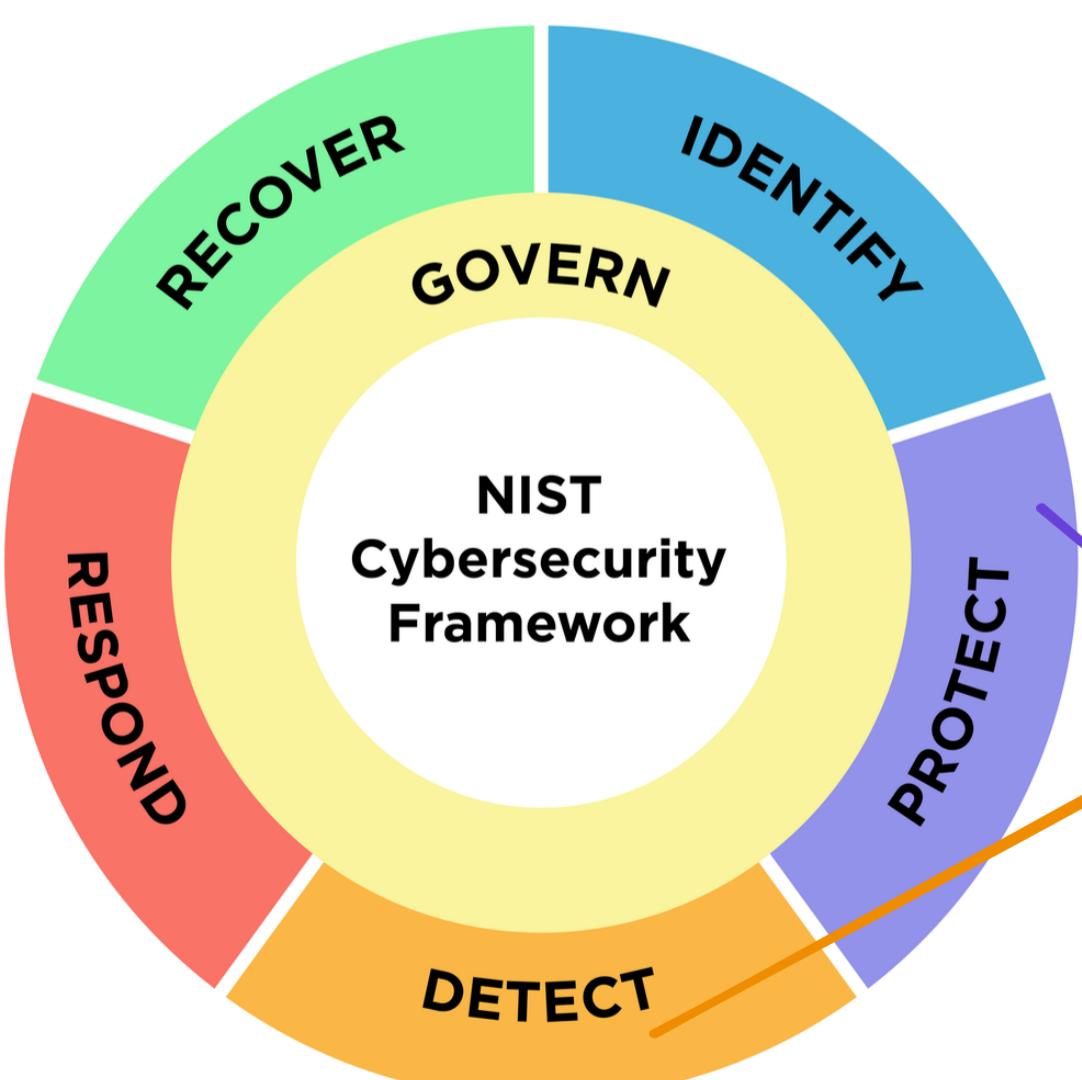
<https://learn.cisecurity.org/cis-controls-download>

### CONTROL 13 Network Monitoring and Defense

Safeguards: 11 | IG1: 0/11 | IG2: 6/11 | IG3: 11/11

#### Overview

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.



#### Why is this Control critical?

We cannot rely on network defenses to be perfect. Adversaries continue to evolve and mature, as they share, or sell, information among their community on exploits and bypasses to security controls. Even if security tools work "as advertised," it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective. Often, misconfigurations due to human error or lack of knowledge of tool capabilities give enterprises a false sense of security.

##### Safeguard 13.3: Deploy a Network Intrusion Detection Solution

Asset Type: Network | Security Function: Detect | IG2 | IG3

Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.

##### Safeguard 13.4: Perform Traffic Filtering Between Network Segments

Asset Type: Network | Security Function: Protect | IG2 | IG3

Perform traffic filtering between network segments, where appropriate.

# Øvelse

Find den også i Canvas

IP-adresser i virkeligheden

## Gruppeøvelse: "IP-adresser i virkeligheden - Research først"

Formål: Forstå hvad IP-adresser er og bruges til, før vi selv udforsker dem

Arbejd i grupper på 4 personer. Brug internettet til research:

### Del 1: Grundlæggende forståelse

1. Søg og find ud af: Hvad er en IP-adresse? Beskriv det med jeres egne ord
2. Find eksempler: Hvordan ser IP-adresser ud? Find 3 forskellige eksempler
3. Hvad kan man bruge dem til? Find mindst 3 konkrete anvendelser

### Del 2: Forskellige typer

4. Private vs public IP - Hvad betyder det? Hvorfor er der forskel?
5. Find ud af: Hvad betyder det når man siger "din IP-adresse"?

### Del 3: Real-world eksempler

7. Søg på "what is my IP" - Hvad viser forskellige hjemmesider jer?
8. Find ud af: Kan andre se jeres IP-adresse? Hvornår og hvordan?
9. Cybersecurity vinkel: Hvordan kan IP-adresser bruges i cyberangreb? Find et konkret eksempel

Afslutning: Hver gruppe præsenterer deres bedste fund og stiller 1 spørgsmål til klassen de gerne vil have besvaret

ourGOAL

### Præsentation

Format: Hver gruppe har 3-4 minutter

Hver gruppe skal:

1. Præsentere deres bedste fund (2 min)
  - Hvad var det mest interessante/overraskende I fandt?
  - Del jeres bedste eksempel eller indsigt
2. Stille 1 spørgsmål til klassen (1-2 min)
  - Test de andre gruppers viden med jeres spørgsmål (ikke for let, ikke for svært)

Fair