INLEIDING TOT HET NIST CYBERSECURITY FRAMEWORK

- **Wat is het NIST Cybersecurity Framework?**
- **Een set richtlijnen ontwikkeld door het National Institute of Standards and Technology (NIST).**
- **Bedoeld om organisaties te helpen bij het beheren en verminderen van cybersecurity-risico's.**

DE VIJF KERNFUNCTIES VAN HET NIST-MODEL

IDENTIFY (IDENTIFICEER)

Doel:

- Begrijp de risico's en middelen binnen de organisatie.

Voorbeelden:

- Asset Management
- Risicobeoordelingen
- Beveiligingsbeleid en governance

PROTECT (BESCHERM)

Doel:

- Implementeren van maatregelen om systemen te beschermen.

Voorbeelden:

- Encryptie en toegangscontrole
- Bewustwordings- en trainingsprogramma's
- Netwerkbeveiliging

DETECT (DETECTEER)

Doel:

- Cybersecurity-incidenten snel identificeren.

Voorbeelden:

- Monitoring
- Anomaliedetectie
- Incidentdetectieprocessen

RESPOND (REAGEER)

Doel:

- De schade minimaliseren door snel te reageren op incidenten.

Voorbeelden:

- Incident Response Planning
- Communicatie tijdens incidenten
- Analyse en herstelacties

RECOVER (HERSTEL)

Doel:

- Zo snel mogelijk herstellen en leren van incidenten.

Voorbeelden:

- Herstelprocessen
- Verbeteringsplannen
- Communicatie met stakeholders

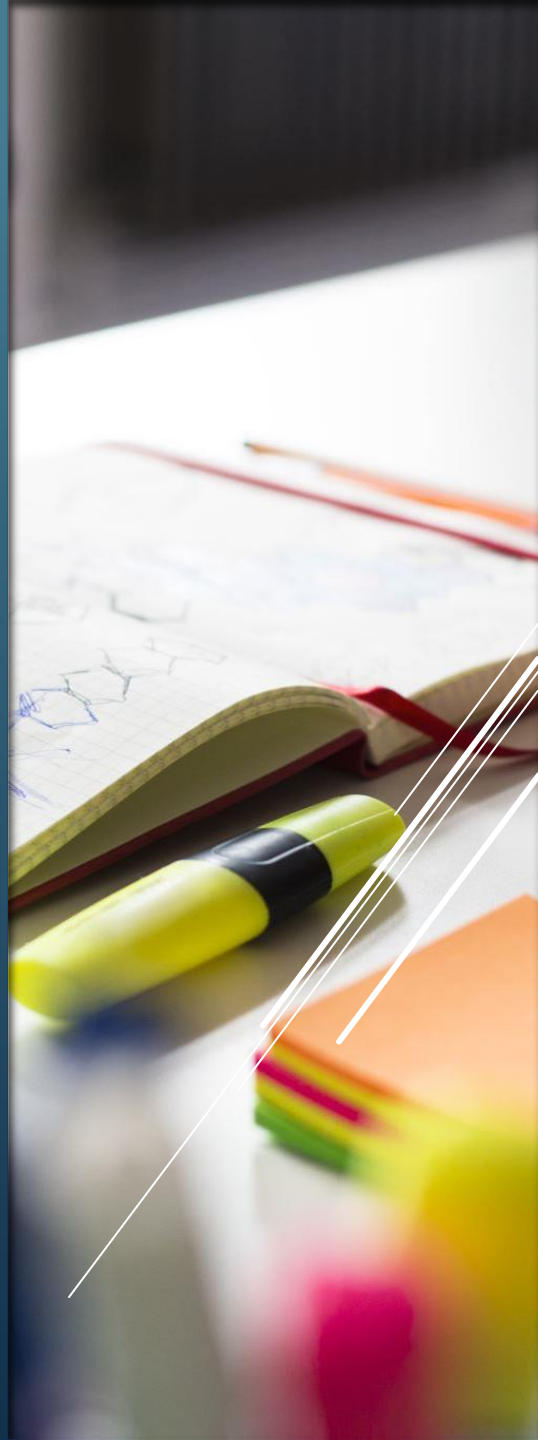
BELANG VAN HET NIST FRAMEWORK

Waarom het NIST Framework?

- Universeel toepasbaar
- Geschikt voor zowel grote als kleine organisaties
- Flexibel en schaalbaar

VOORBEELDEN UIT DE PRAKTIJK

- Case study 1: Implementatie van het NIST Framework bij een gezondheidsorganisatie.
- Case study 2: NIST-gebaseerde strategie voor een overheidsinstantie.



CONCLUSIE

- Het NIST Framework biedt een uitgebreide en flexibele aanpak voor cybersecurity-risico's.
- Elke organisatie kan het model aanpassen aan hun behoeften.

- Bedankt voor je aandacht!
  Zijn er nog vragen?