

KEUZEMODULE CYBERSECURITY **WEERBAAR TEGEN CYBERCRIME**

Module 1, Wat is cybersecurity en cybercrime?

Workshop 5, Beveiligingsmaatregelen

LEERUITKOMST MODULE 1

Je hebt een fundamenteel begrip van cybersecurity en bent met een risico-bewuste mentaliteit in staat om wet- en regelgeving, risicomanagement en het beheer van cybersecurity toe te passen in een organisatie, zodanig dat daarmee effectief wordt bijgedragen aan het beveiligingsbeleid en risicobeheer binnen organisaties.

Overzicht

Week 1: Risicodenken

- Workshop 1: De wereld van cybercrime
- Workshop 2: Risicodenken en -management
- Workshop 3: Governance van cybersecurity

Week 2: Risicoanalyse

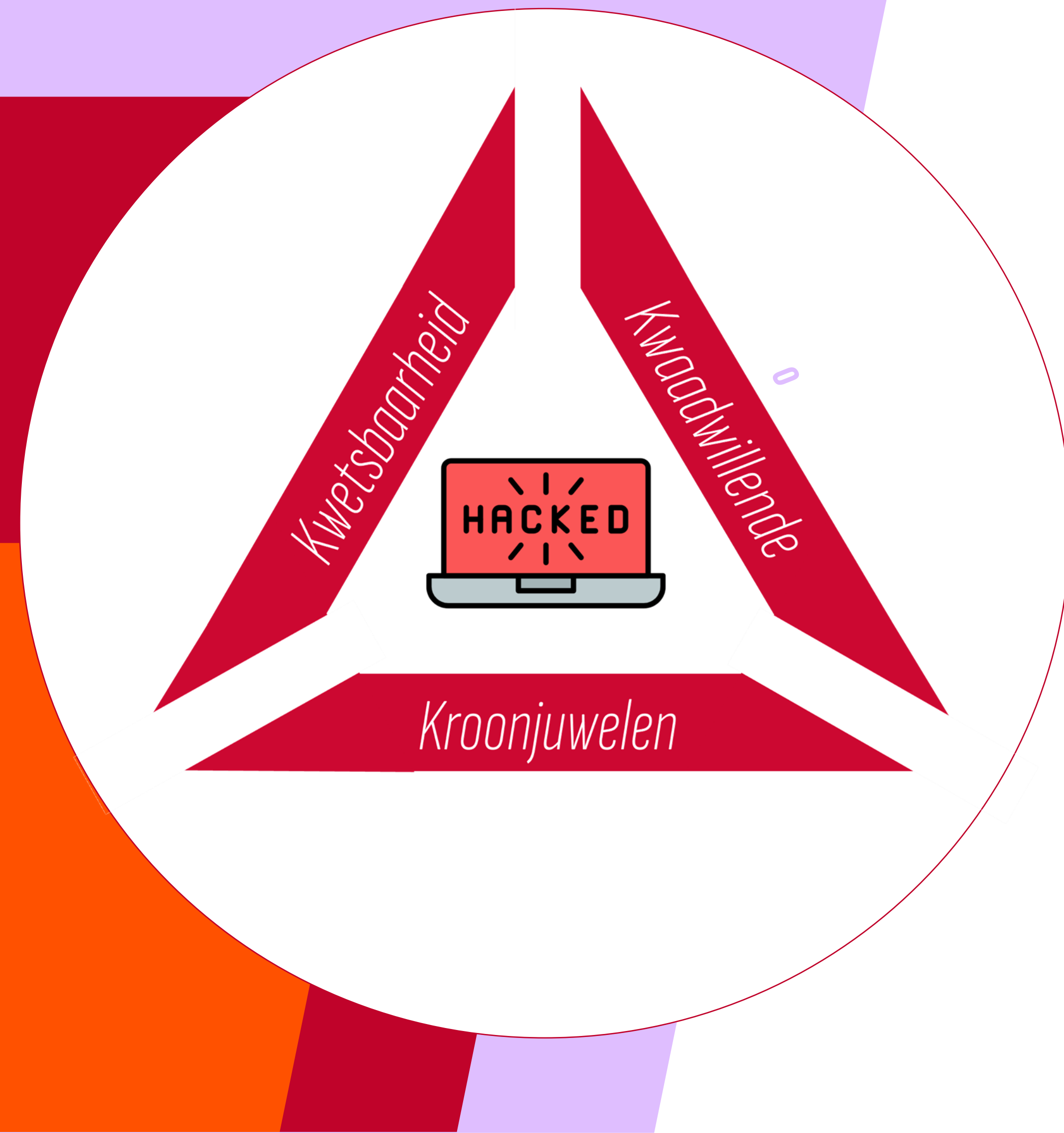
- Workshop 4: Risicoanalyse en -assessment
- Workshop 5: Beveiligingsmaatregelen

Week 3: Challenge en afronding

WAT HEBBEN WE TOT NU TOE GEDAAN?

Risicoanalyse en -assessment

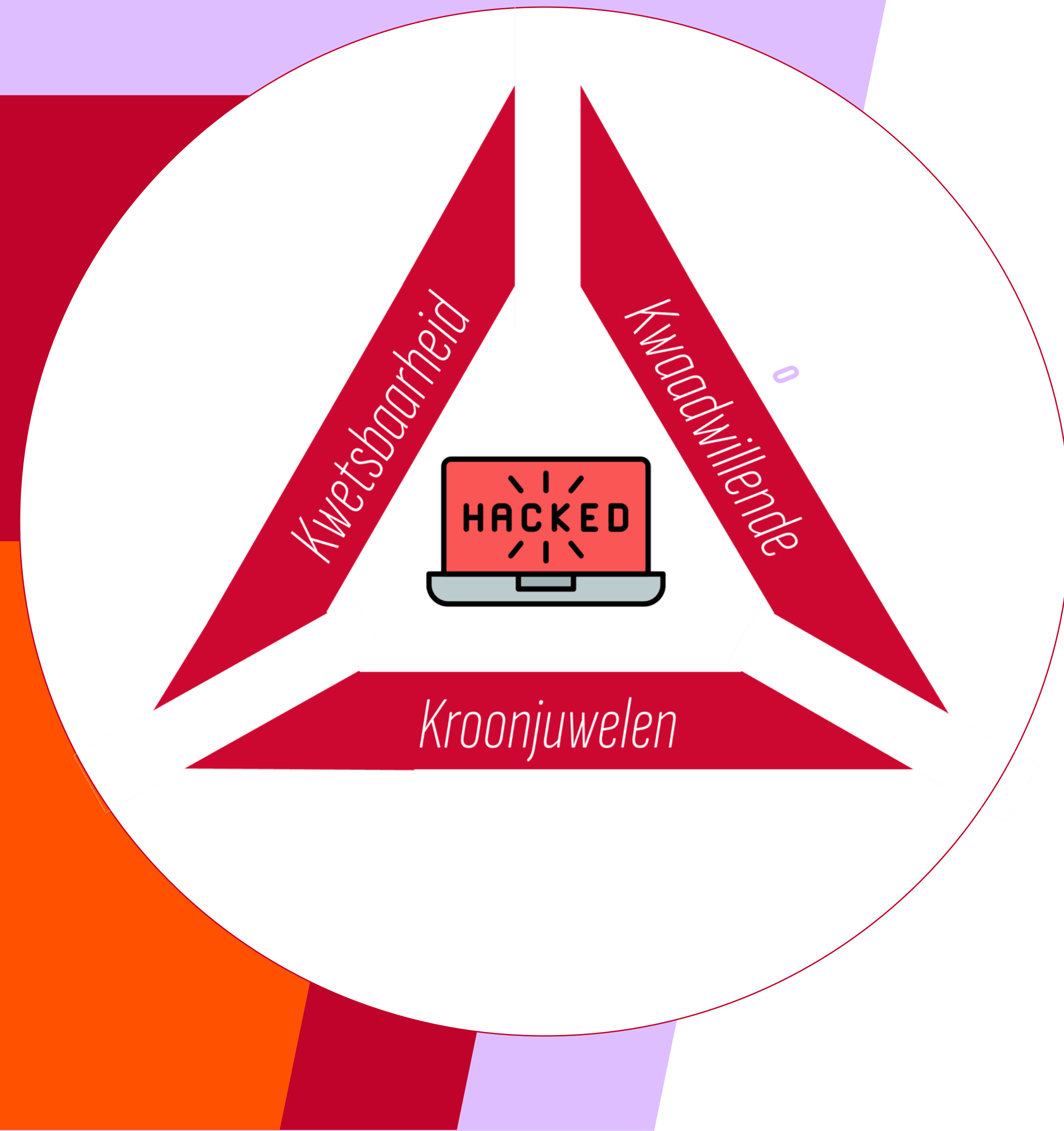
- Hack-driehoek: Kwetsbaarheid, Kwaadwillende en Kroonjuwelen
- Typen kwaadwillende
- Risicoanalyse
- Risicobron
- Risicomatrix
- Risicoassessment



WAT HEBBEN WE TOT NU TOE GEDAAN?

Presenteren resultaten opdracht

- Risicomatrix
- Risicoanalyse
- Risicoregister



WAARMEE GA JE VANDAAG AAN DE SLAG?

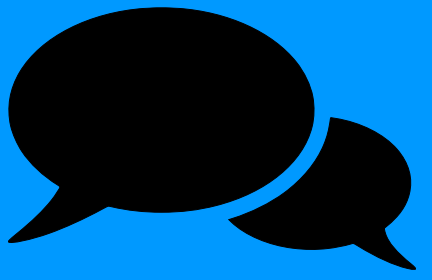
Leeruitkomst workshop

- Je bedenkt en beschrijft maatregelen om de kans en impact van de risico's te verminderen, zodanig dat een goed risk treatment plan gerealiseerd kan worden.
- Je presenteert de resultaten op een gestructureerde wijze, zodanig dat de (cyber)aanpak van maatregelen goed worden gecommuniceerd aan het management.

RISICOANALYSE STAPPENPLAN

1. Bepaal wat je wil beschermen
2. Identificeer de risico's
3. Analyseer de gevonden risico's
4. Besluit wat je gaat doen: accepteren, oplossen (of mitigeren), overdragen of stoppen.

WANNEER DOE JE WAT?

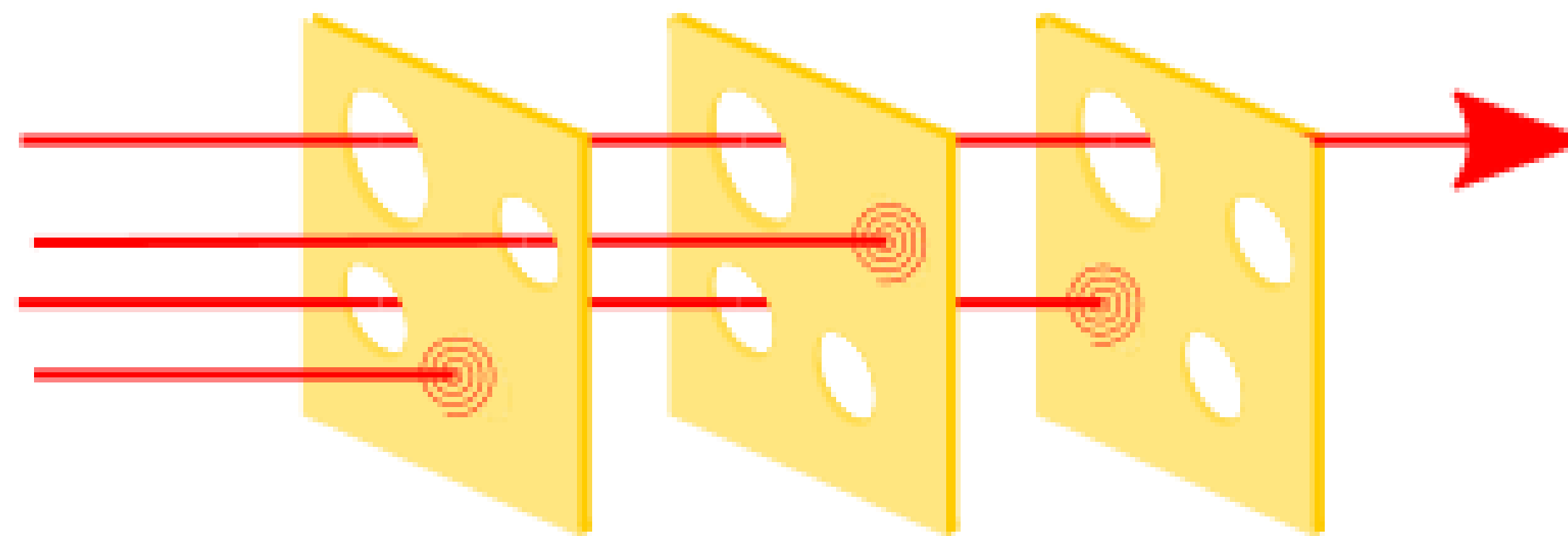


- Accepteren - *accept*
- Oplossen (of mitigeren) - *mitigate*
- Overdragen - *transfer*
- Stoppen - *avoid*

Impact	Kans				
	Zeer onwaarschijnlijk	onwaarschijnlijk	Mogelijk	Waarschijnlijk	Zeer waarschijnlijk
Onbelangrijk					
Minder ernstig					
Serieus					
Zeer serieus					
Catastrofaal					

DEFENSE IN DEPTH MODEL (1/3)

- Defense in Depth (DiD) is een cybersecuritystrategie die meerdere lagen van bescherming gebruikt om systemen en data te beveiligen.
- Het idee is dat als één beveiligingslaag faalt, de andere lagen nog steeds bescherming bieden.

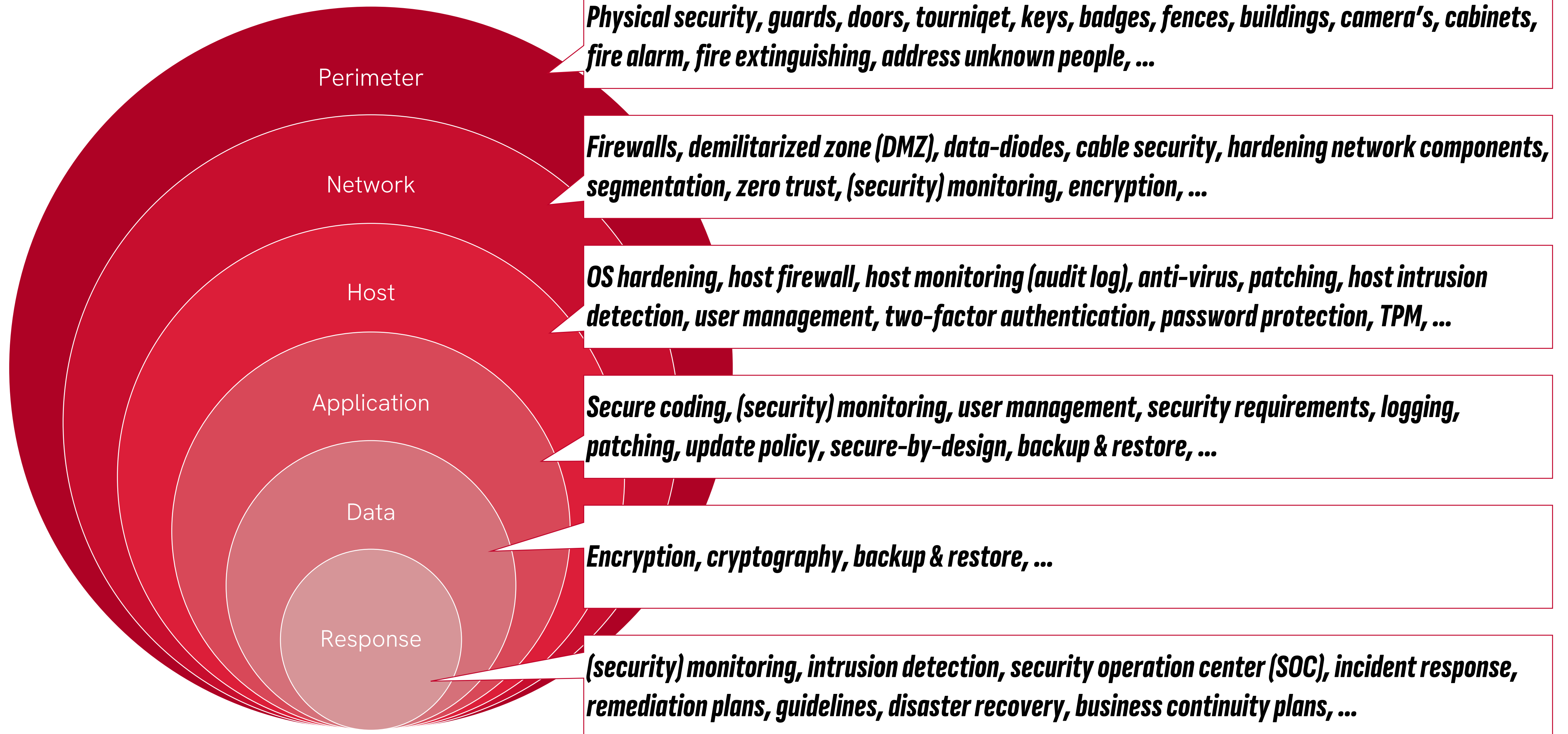


Swiss Cheese Model

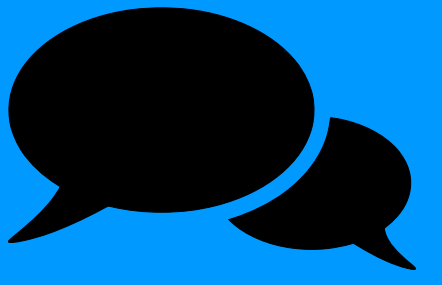
DEFENSE IN DEPTH MODEL (2/3)

- Het gebruik van meerdere lagen zorgt ervoor dat als een aanvaller één beveiligingsmaatregel weet te omzeilen, er nog andere barrières zijn die de aanval kunnen stoppen of vertragen. Dit verhoogt de kans dat een aanval wordt gedetecteerd en afgeslagen voordat er schade wordt aangericht.
- Door het combineren van verschillende beveiligingsmaatregelen, creëert Defense in Depth een robuuster beveiligingsmodel dat beter bestand is tegen de diverse en complexe bedreigingen van vandaag.

DEFENSE IN DEPTH MODEL (3/3)



WELKE MAATREGELEN?



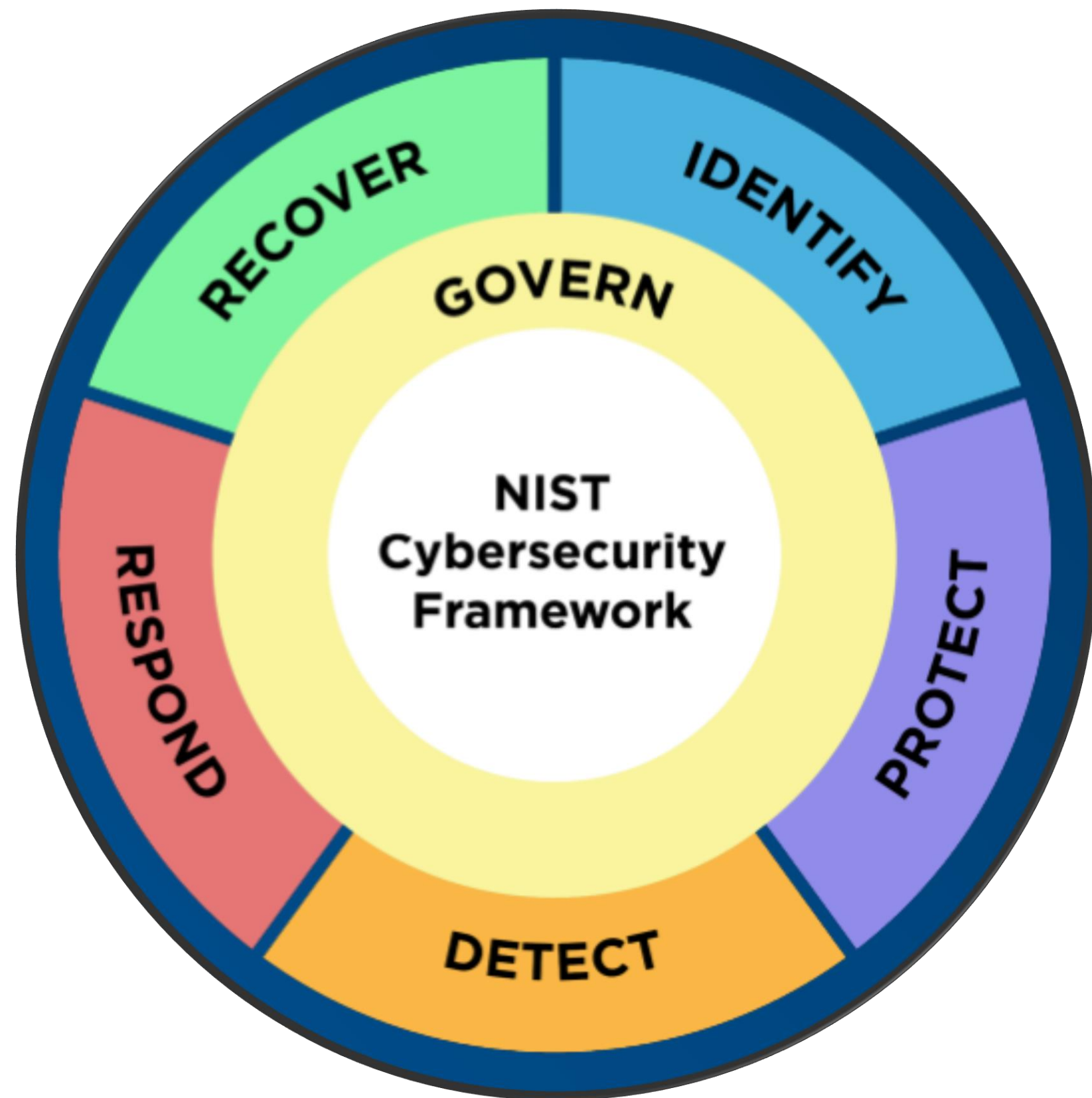
- Op basis van de bow-tie “jouw laptop” van de vorige workshop gaan we kijken naar een pakket van maatregelen.
- *Probeer zo goed mogelijk het DiD model toe te passen bij het nemen van deze maatregelen.*

SECURITY STANDAARDEN

Wat vertellen de standaarden
op het gebied van
maatregelen?



NIST CYBERSECURITY FRAMEWORK 2.0



<https://www.nist.gov/cyberframework>

- Het NIST Cybersecurity Framework 2.0 biedt een gestructureerde aanpak voor het beheren en verbeteren van cybersecurity-risico's.
- Weerbaarheid zit met name in impact verlagende maatregelen én in de onderdelen detect, respond en recover.
- Maatregelen worden op al deze onderwerpen genomen.

ISO27002:2022

- 5.2 Information security roles and responsibilities
- 5.3 Segregation of duties
- 5.15 Access control
- 5.26 Response to information security incidents
- 5.37 Documented operating procedures
- 6.3 Information security awareness, education and training
- 7.3 Securing offices, rooms and facilities
- 8.8 Management of technical vulnerabilities
- 8.16 Monitoring activities
- 8.26 Application security requirements
- 8.32 Change management



NCSC – BASISMAATREGELEN

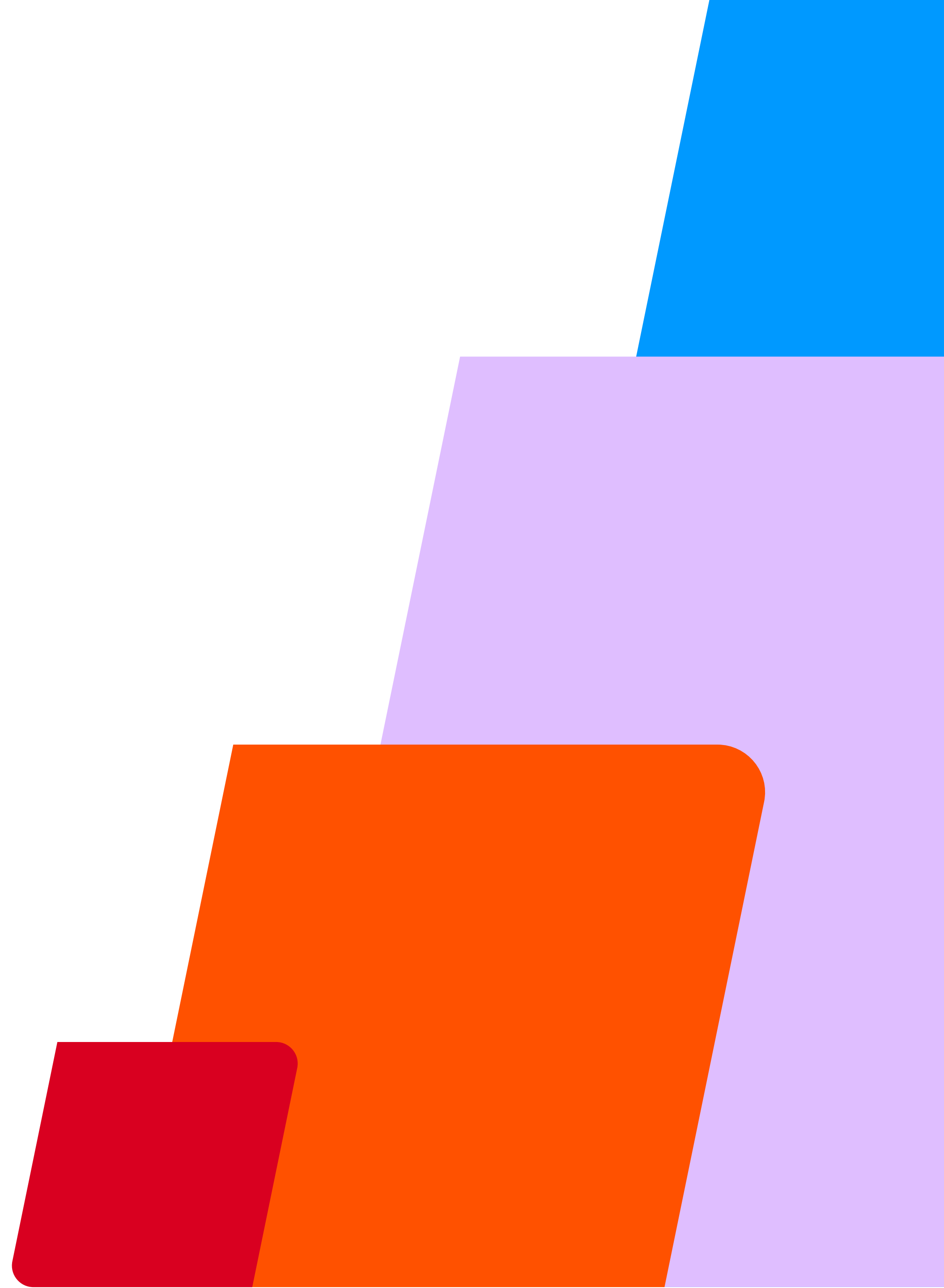


EU CYBERSECURITY ACT ANNEX 1 – EISEN

- Producten met digitale elementen worden zodanig ontworpen, ontwikkeld en geproduceerd dat zij een passend cyberbeveiligingsniveau op basis van de risico's waarborgen
- Producten met digitale elementen worden geleverd zonder bekende kwetsbaarheden die kunnen worden uitgebuit
- Producten worden ontworpen, ontwikkeld en geproduceerd om de gevolgen van een incident te beperken met behulp van passende mechanismen en technieken om uitbuiting te beperken;

HARDENING

Hardening in cybersecurity verwijst naar het proces van het beveiligen van een systeem of applicatie door het verminderen van zijn kwetsbaarheden. Het doel is om de aanvalsvectoren (mogelijkheden voor aanvallers om binnen te dringen) zo veel mogelijk te verkleinen.



SECURITY CONCEPTEN

- Secure-by-design
- Secure-by-default
- Privacy-by-design
- Privacy-by-default

MAATREGELEN

Neem maatregelen waar mogelijk bij de bron van het risico.

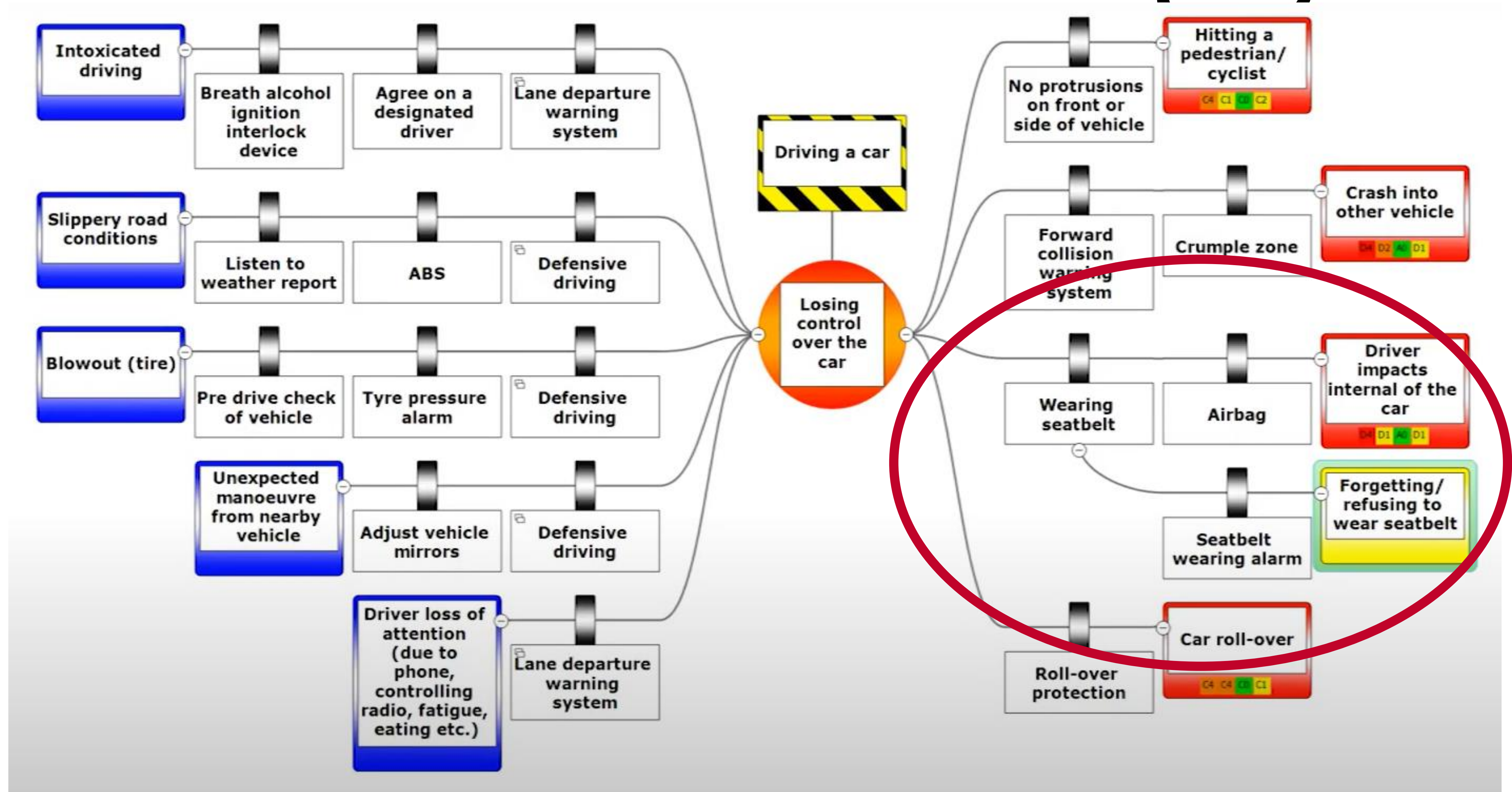
Neem passende maatregelen die passen bij de organisatie, cultuur en het risico.



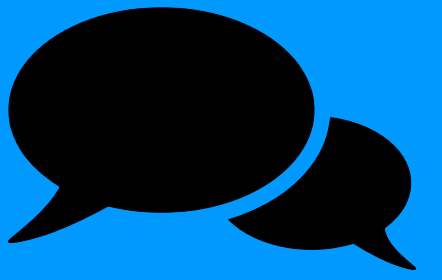
EFFECTIVITEIT VAN MAATREGELEN (1/2)

- Het is belangrijk dat de effectiviteit van maatregelen worden geëvalueerd.
- Denk ook na om maatregelen te nemen om de effectiviteit van maatregelen te borgen.
- Voorbeeld is het vervelende geluid dat je in je auto hoort op het moment dat je de gordel niet aan doet.

EFFECTIVITEIT VAN MAATREGELEN (2/2)



EFFECTIVITEIT



Kan jij nog meer maatregelen bedenken die de effectiviteit van cybersecurity maatregelen verhoogt of borgt?

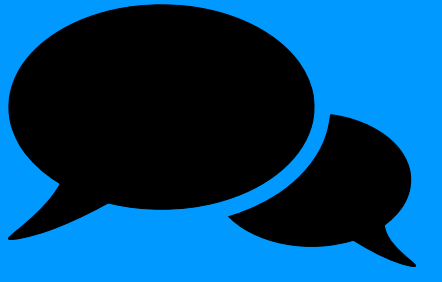
ANDERE VOORBEELDEN M.B.T EFFECTIVITEIT

- Training medewerkers
- Stickers met herinnering om de deur op slot te doen
- Cybersecurityvideo basismaatregelen voor leveranciers
- (Interne) audit
- Automatisch locken van je laptop
- Blokkeren van USB poorten
- Regelmatig incident response plannen oefenen
- ...

WANNEER HEB JE VOLDOENDE MAATREGELEN GETROFFEN?

- Hackers zijn zeer creatief en hebben één kwetsbaarheid nodig!
- Een goede risico-analyse
- Goed inzicht in je digitale middelen
- Goed inzicht in de hackers
- Kijken naar best-practices en pakket van maatregelen
- Kijken naar securitystandaarden en -richtlijnen
- Gezond verstand
- ...

RISICO'S

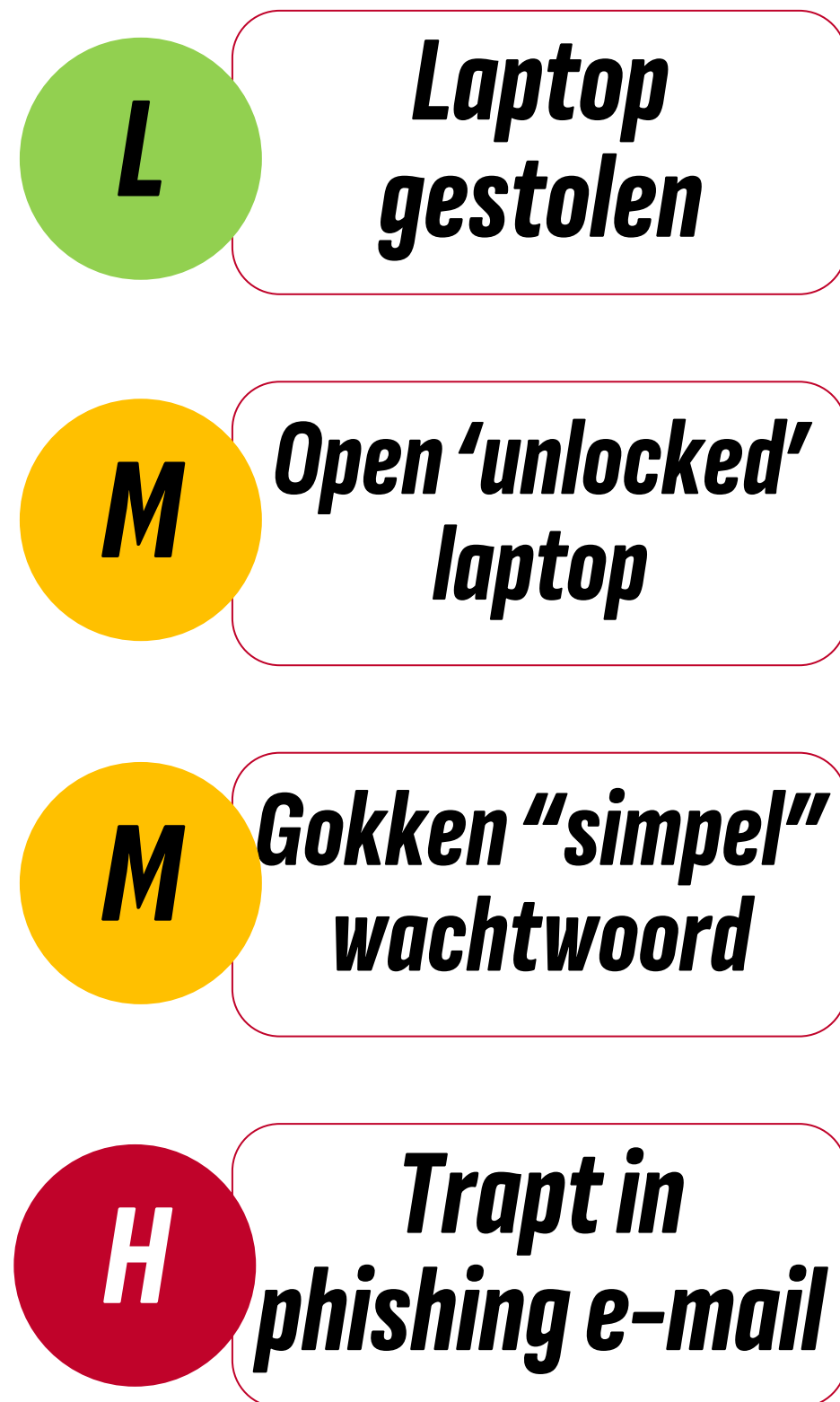


Verzin een pakket van maatregelen voor de volgende risico's:

- 1. Een medewerker klikt op een malafide link in een e-mail, waardoor zijn laptop geïnfecteerd wordt met malware.*
- 2. Een opensource tekenapplicatie (GIMP) wordt gedownload en bevat ransomware en verspreidt door het netwerk.*
- 3. Een medewerker heeft een fout gemaakt in configuratie van de remote toegang applicatie, waardoor een kwaadwillende met een standaard wachtwoord toegang krijgt tot het systeem.*

BOW-TIE EXAMPLE – YOUR LAPTOP

UNAUTHORIZED ACCESS - MAATREGELEN



LAPTOP

**Unauthorized
Access**

Loss of integrity, availability and confidentiality

**Wachtwoorden
gelekt**

H

**Overnemen
webapplicaties**

H

**Laptop door-
verkopen**

L

**Malware
infectie**

H

**Identiteit
overnemen (mail)**

H

**Lekken
vertrouwelijke
documenten**

H

CYBERSECURITY VERZEKERING

Wat is een cybersecurity
verzekering?

Wanneer sluit je een
cybersecurity verzekering af?

Welk probleem los je op?



WAT IS EEN CYBERSECURITY VERZEKERING?

- **Een cyberverzekering vergoedt kosten als je slachtoffer bent van een cyberincident.**
 - Directe kosten van een cyberincident: o.a. het repareren of vervangen van hard en software, het herstellen van data, terugvinden van informatie en opnieuw opbouwen van de administratie. Onder directe kosten kan het inhuren van specialisten voor het herstel, verlies van (productie)uren of omzet;
 - Indirecte kosten: o.a. reputatieschade, boetes van toezichthouders (bijvoorbeeld AVG boetes), schadevergoedingen aan gedupeerden.
- **Een cyberverzekering is meestal opgebouwd uit drie onderdelen:**
 - Voorkomen: met de verzekeraar kijk je naar de risico's die je nu loopt. Je neemt als het nodig is maatregelen om ze te voorkomen.
 - Herstellen: als je slachtoffer bent van cybercrime, herstellen experts de schade zo snel mogelijk.
 - Vergoeden van schade: je verliest bijvoorbeeld omzet doordat een virus je computer of server onbruikbaar maakt. Of doordat je webwinkel tijdelijk onbereikbaar is na een ransomware-aanval. Je bent verzekerd tot een maximumbedrag.

EXTRA MOGELIJKE DIENSTEN

- Bewustwording, kennis en kunde van de ondernemer of personeel (bijvoorbeeld ondersteund met online trainingen)
- Incidentondersteuning (bijvoorbeeld een 24/7 alarmcentrale en technische ondersteuning)
- Juridische ondersteuning (bijvoorbeeld bij datalekken in het kader van de AVG)
- Forensische diensten (het uitzoeken wie er achter een aanval zit)

WANNEER SLUIT JE DEZE AF?

- Wanneer je zelf niet de schade van een cyberincident kan betalen
- Extra stok achter de deur
- Directe hulp vanuit verzekering bij cyberincident

SAMENVATTING

- Defense in depth model
- NIST cybersecurity framework
- ISO27002
- Cybersecurity ACT
- Effectiviteit van maatregelen
- Cyberverszekering

OPDRACHT

Je gaat met je projectgroep aan de slag met deze opdracht. Later geven een aantal projectgroepen een presentatie van het resultaat aan de klas. Je neemt het werk op in je portfolio.





OPDRACHT A

Werk de volgende vragen uit met de projectgroep. Verdiep je in het onderwerp door bronnen te raadplegen. Je mag het werk verdelen, maar zorg dat je de kennis met elkaar deelt en discussies voert over het resultaat. Maak een plan van aanpak, want de tijd is beperkt!

1. Neem de ISO27002:2022 / IEC62443 security maatregelen door en werk voor één maatregel van iedere categorie uit hoe je dat binnen een organisatie zou kunnen implementeren.
2. Neem het NIST cybersecurity framework door en reflecteer op hoe dit bijdraagt aan het verbeteren van de cybersecurity van een organisatie.
3. Doe online onderzoek naar hardening van Windows 11 (of wat je op je laptop hebt staan). Evaluer hoe het staat met jouw laptop én wat je hier van meeneemt. (technisch)
4. Bedenk een pakket van maatregelen voor het risico dat een interne medewerker van een organisatie kwaadwillend wordt of omgekocht wordt en data steelt of systemen verwoest. Lees je eerst in op het onderwerp “insider threat”.

OPDRACHT B

Vrijdag bij de challenge uitleg starten we eerst met een aantal presentaties



Werk de volgende vragen uit met de projectgroep. Zorg dat je de kennis met elkaar deelt en discussies voert over het resultaat.

1. Eerder heb je een bow-tie diagram gerealiseerd op basis van een casus. Hiervoor heb je nog geen maatregelen bedacht (als het goed is). Maatregelen bedenken kan lastig zijn, omdat je simpelweg nog niet alle kennis hebt. Ga dus eerst op onderzoek uit voor iedere consequentie én bedreiging wat voor soort maatregelen hier genomen kan worden. Zorg ervoor dat je de gevonden maatregelen indeelt in het DiD-model.
2. Stel een pakket van maatregelen voor alle bedreigingen en consequenties samen en zet deze in de bow-tie. Challenge elkaar en beargumenteer waarom dit het juiste pakket is. Welke maatregelen pakken de bedreiging/consequentie/risico bij de bron aan en waarom?
3. Bepaal de nieuwe kans en impact als alle maatregelen zijn toegepast en noteer je argumentatie. Maak een nieuw risico-register.
4. Bekijk de maatregelen en bespreek met elkaar de effectiviteit hiervan. Wat kunnen redenen zijn waarom de effectiviteit afneemt? Zijn er mogelijkheden om de effectiviteit te borgen met andere maatregelen?
5. Maak een presentatie, zodat je deze aan het management zou kunnen presenteren.



BRONNEN

1. Zie Bibliotheek op Brightspace
2. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf
3. <https://www.informatiebeveiligingsdienst.nl/product/handreiking-diepgaande-risicoanalyse-methode-gemeenten/>
4. https://www.bio-overheid.nl/media/13kduqsi/bio-versie-104zv_def.pdf