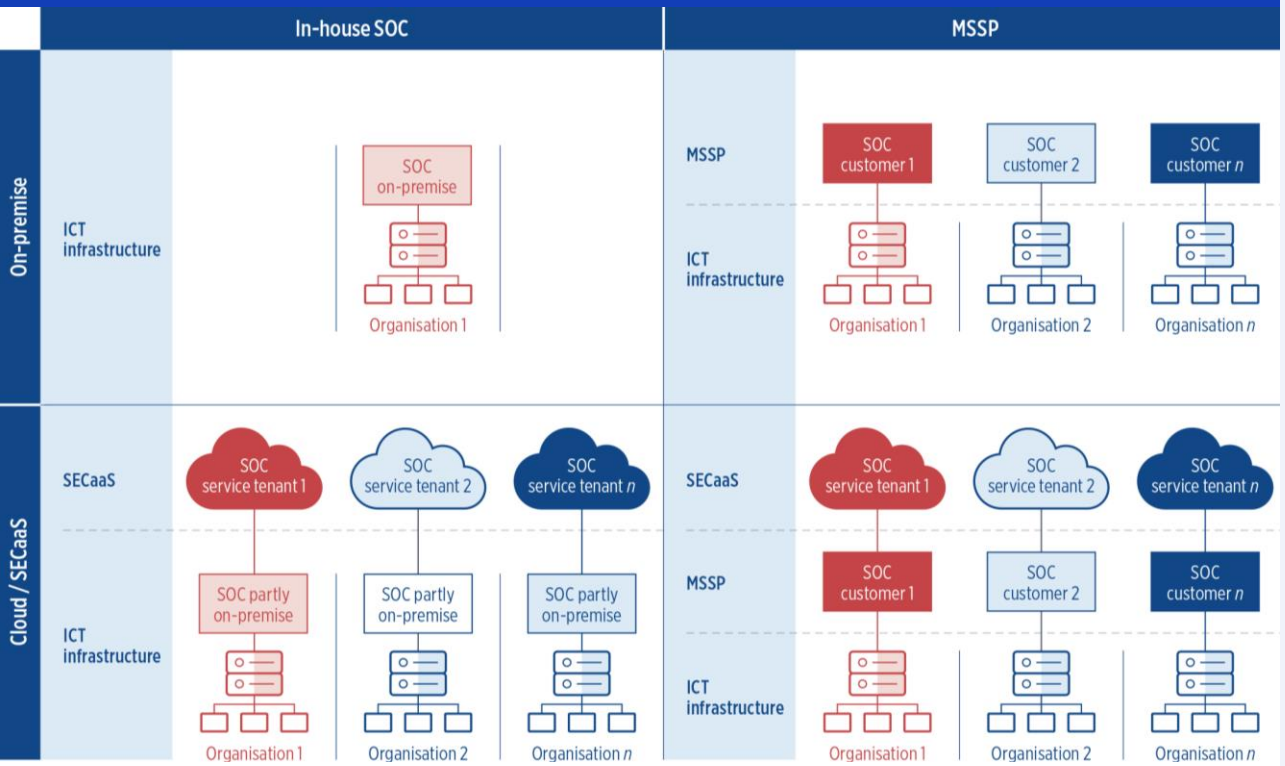
SOC of the Future

Blauwdruk voor een Security Operations Center in 2030

Reinder Wolthuis

PvIB event over security Innovatie

Agenda



1. Introductie
2. SOC blauwdruk voor 2030
3. Takeaways
4. Discussie

Introductie

Afkortingen

- SOC = Security Operations Center
- CSIRT = Computer Security Incident Response Team
- CERT = Computer Emergency Response Team
- MSP = Managed Service Provider
- MSSP = Managed Security Service Provider
- NIS = Network and Information Security Directive

Definitie van een SOC/CSIRT voor de blauwdruk

Een SOC/CSIRT kan deze diensten bieden:

- Information Security Event Management
- Information Security Incident Management
- Vulnerability management
- Situational Awareness
- Cyber Threat Intelligence, Hunting, and Analytics
- SOC Tools, Architecture, and Engineering.

Introductie

Wat is het SOC of the Future?

Een Blauwdruk die het SOC in 2030 beschrijft vanuit twee perspectieven:

1. **SOC-landschap**
2. **SOC en interactie met de omgeving**

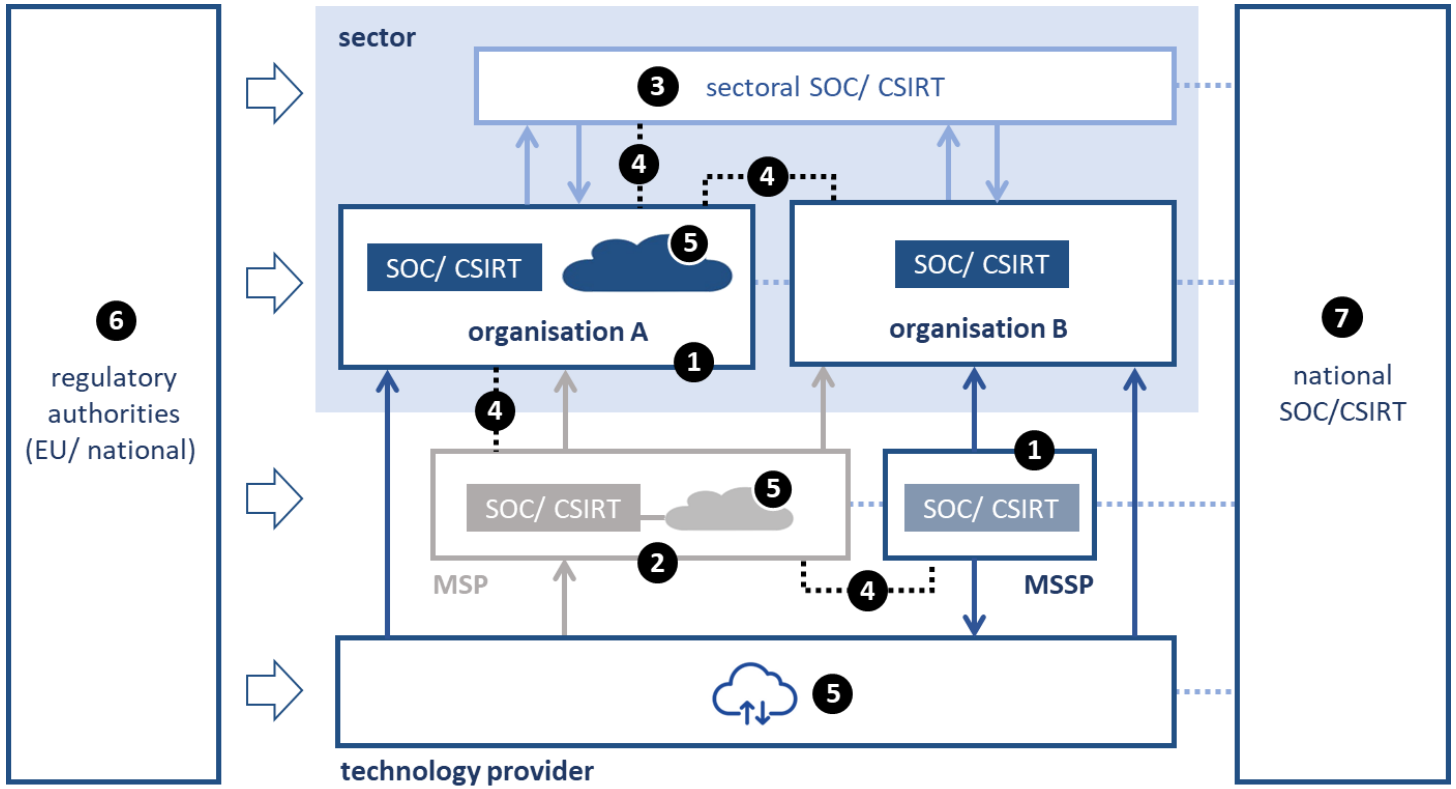
Let wel, het resultaat is bedoeld als **discussiestuk,** het is geen “glazen bol”.

Hoe hebben we dit resultaat bereikt?

- **Literatuurstudie** (academic papers, European R&D projects, etc.)
- **Interviews** met experts in NL (SOC managers, SOC innovatie partners, experts uit industrie en overheid)

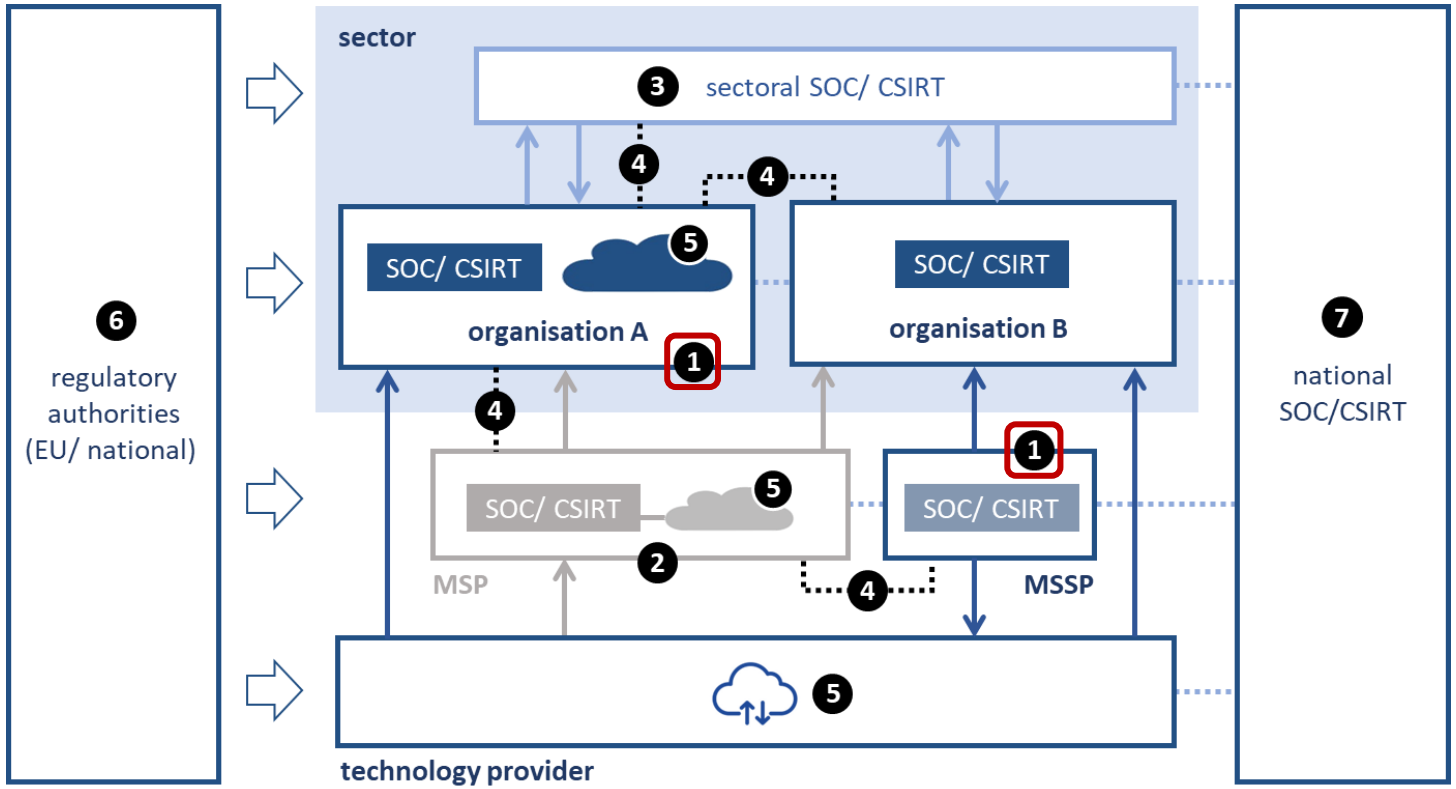
In opdracht van het NCSC

SOC-landschap



1. reduction of SOCs and MSSPs
2. MSPs absorb MSSP market
3. increase of sectoral SOCs
4. intensified SOC collaboration
5. evolved threat landscape
6. strong regulatory influence
7. repositioned NCSC

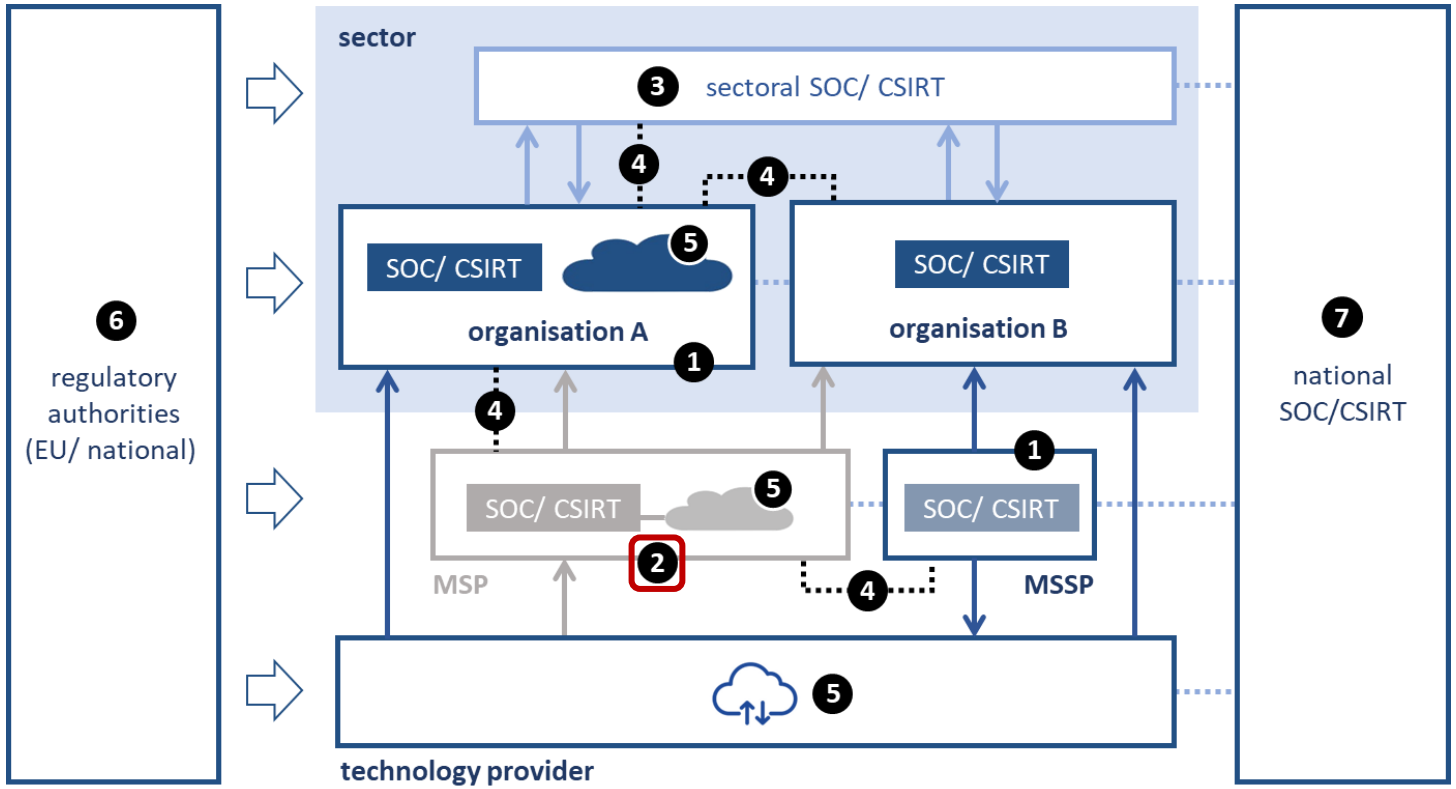
SOC-landschap



2030: Kleiner aantal SOC's in bedrijf.

- Factoren:
  - Stijgende kosten
  - Schaarse expertise
  - Prijs/kwaliteit-verhouding aanbod MSSP's, MSP's en tech leveranciers
- Aggregatie and integratie

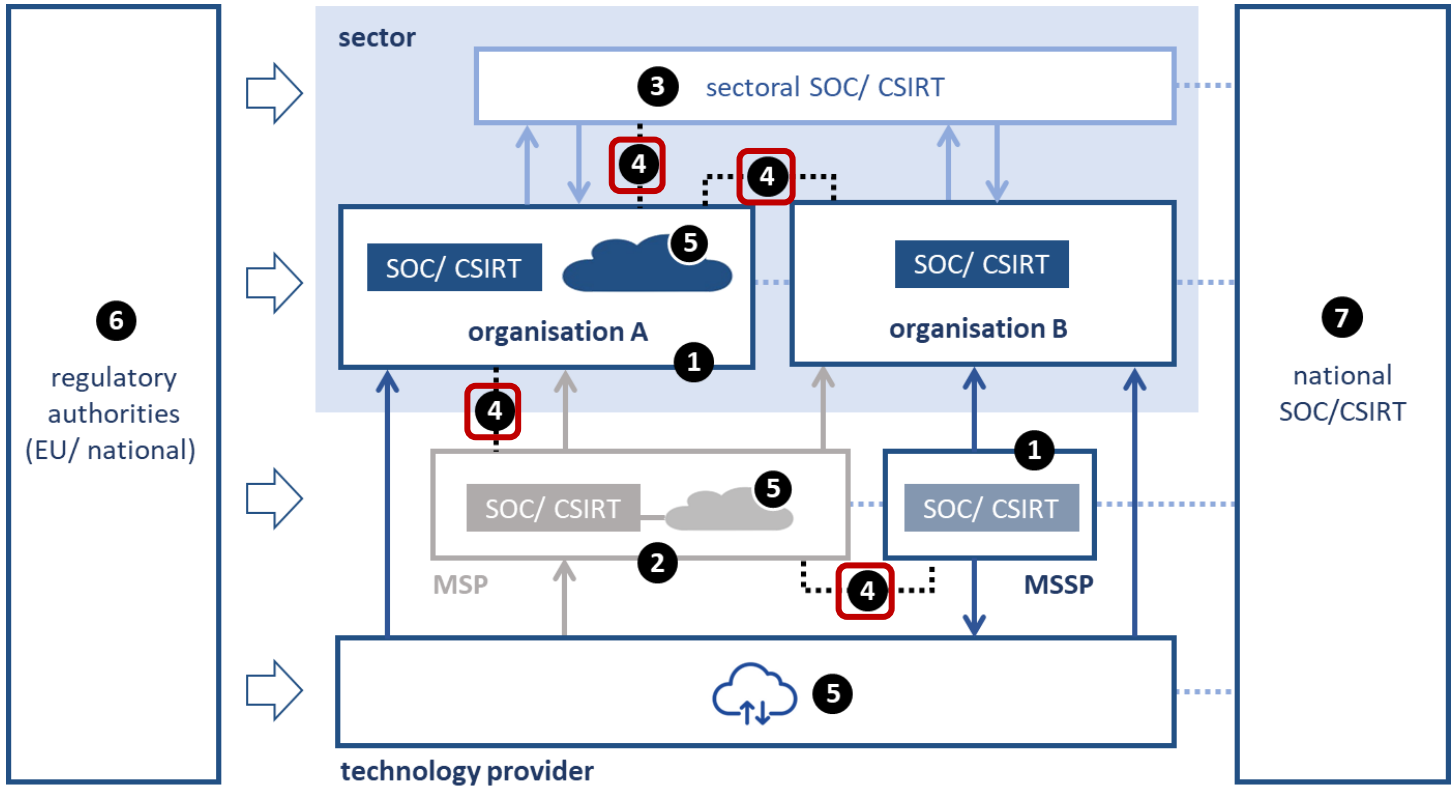
SOC-landschap



2030: MSP's hebben een deel van de MSSP-markt overgenomen

- Resultaat van het verder uitbreiden van dienstverlening van MSP's
- Integratie van configuratie en onderhoud met monitoring en response (vb. cloud infra)
- Samenwerking tussen MSP's en MSSP's (infra- vs security services)

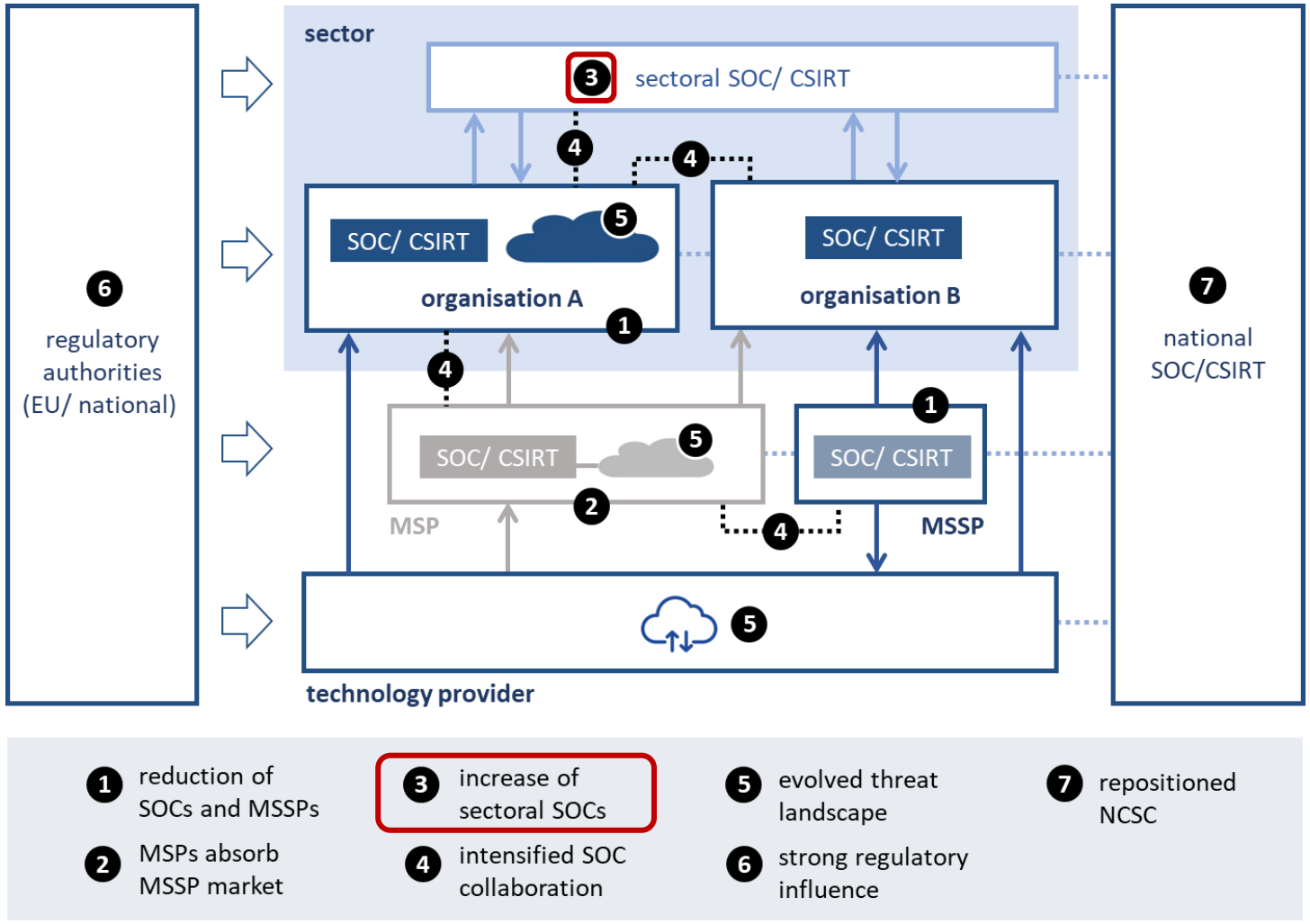
SOC-landschap



2030: Samenwerken en delen van informatie is de norm

- Groeiende belang van “situational awareness” en een goede informatiepositie voor de effectiviteit van het SOC
- Deze wordt vergroot door samenwerken en delen van informatie (e.g. “sightings”)
- Centrale rol voor nationaal SOC/ CSIRT, sectorale SOC/ CSIRTs

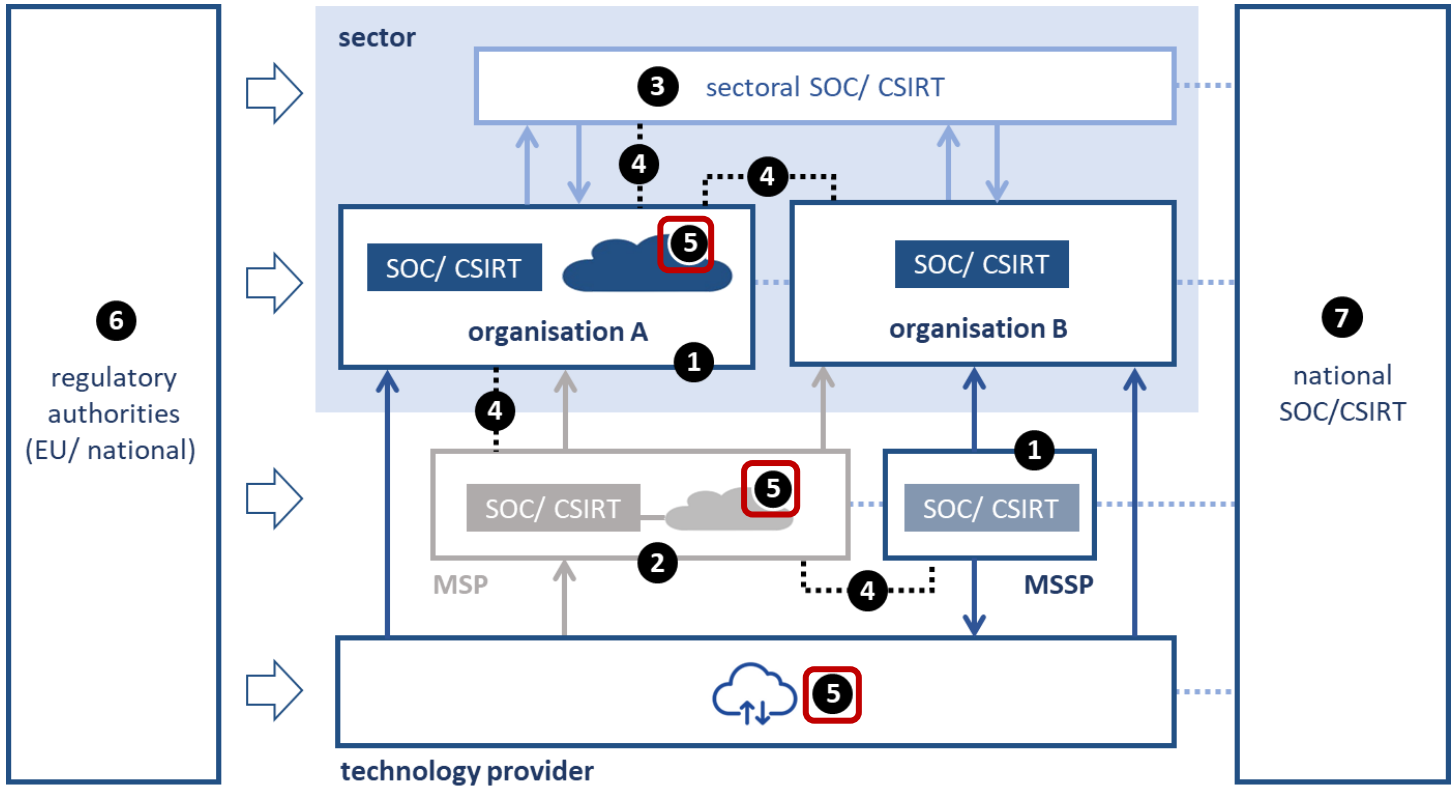
SOC-landschap



2030: Sectorale SOC/ CSIRTs voor veel sectoren (energie, water, …)

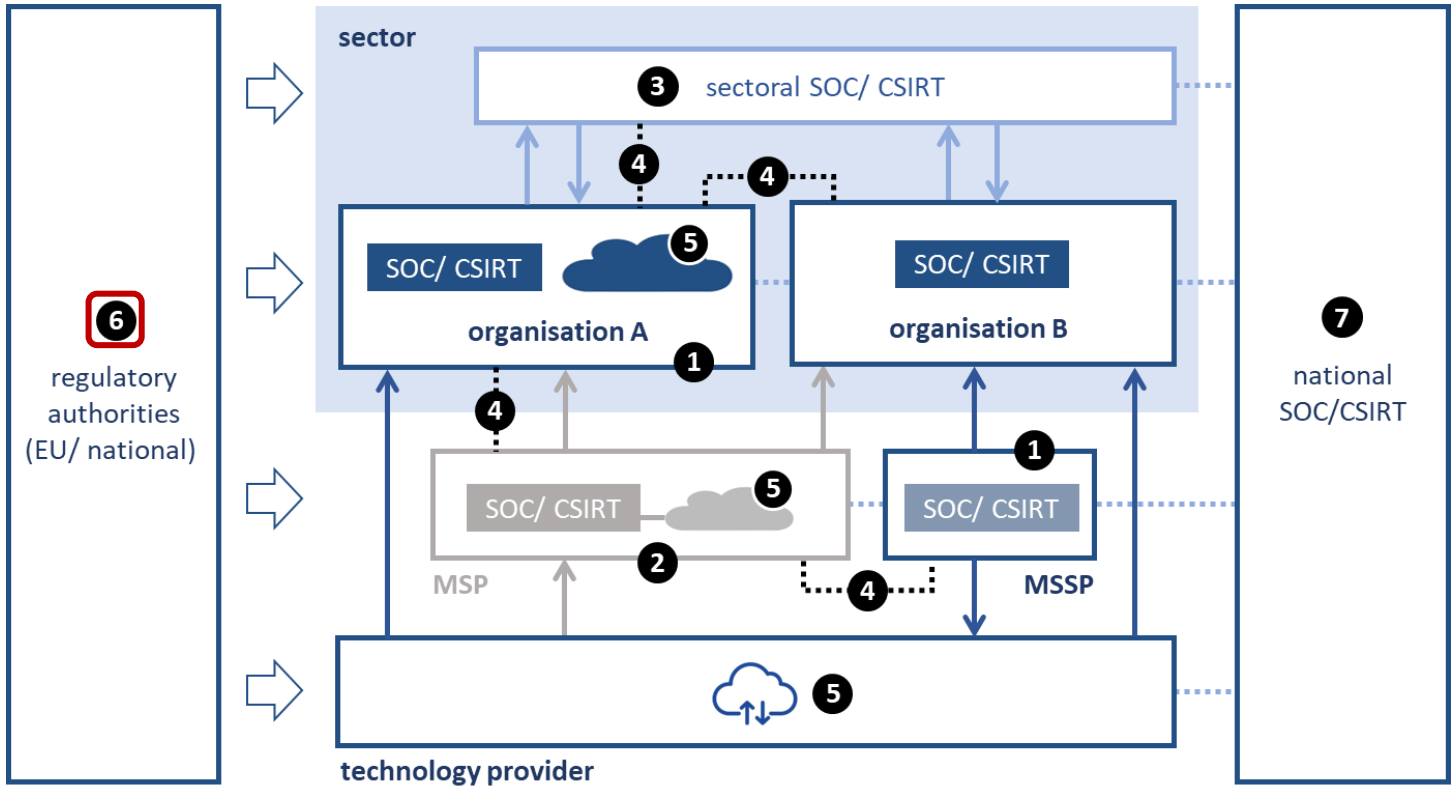
- Sectorale samenwerking natuurlijk en effectief:
  - Veel overeenkomsten tussen organisaties
  - Bestaande samenwerkingsverbanden
  - Campagnebenadering door actoren
- Huidige samenwerkingsverbanden (bijv. ISACs) evolueren naar meer operationele samenwerkingsvormen

SOC-landschap



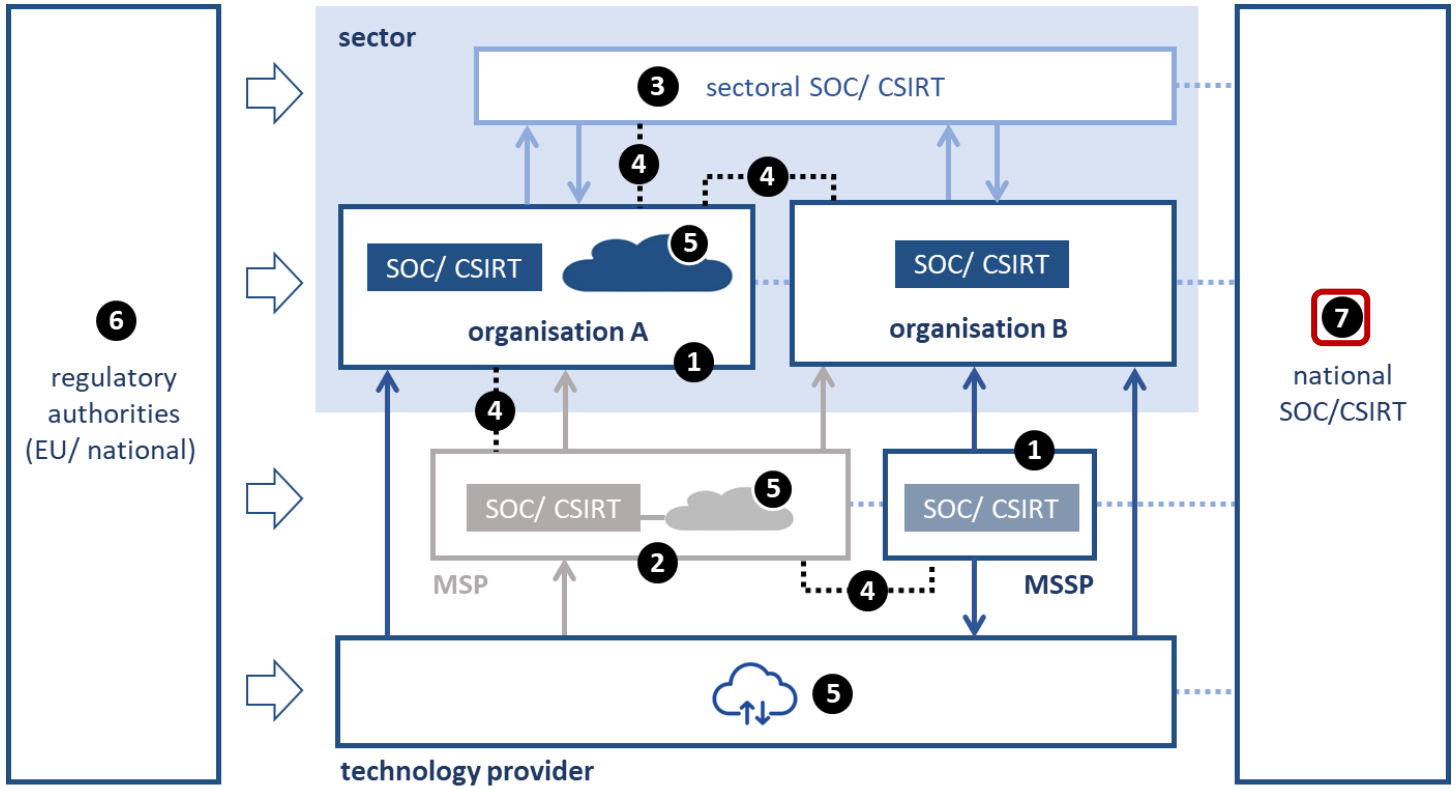
- **2030: Verder ontwikkeld dreigingslandschap**, waarin
  - Impact van kleine actoren verminderd is
  - Dreiging van cybercriminele organisaties hoog blijft
  - Dreiging van statelijke actoren is toegenomen
- Toegenomen gemiddelde complexiteit

SOC-landschap



- **2030: Invloed van wet- en regelgeving**
- NIS3 als opvolger van NIS2
- Nationale regelgeving inzake het gebruik van SOC-services
- Certificering van minimum maturity levels
- Geaccrediteerde SOC-services

SOC-landschap



- **2030: Herpositionering NCSC** met een grotere operationele rol
- Nationaal SOC/ CSIRT (“Cyberhub”)
- Coördinatie tussen (sectorale) SOC’s, MSSP’s e.a.
- Regierol bij grotere (nationale) incidenten

SOC en interactie met de omgeving

1. mainly proactive role
2. highly automated SOC
3. supports business processes
4. high degree of standardization
5. infra mostly cloud-based
6. staffing changes
7. Internal organisation changes

SOC en interactie met de omgeving

1 mainly proactive role
2 highly automated SOC
3 supports business processes
4 high degree of standardization
5 infra mostly cloud-based
6 staffing changes
7 Internal organisation changes

Focus is **proactief**

- Handelen op dreigingen in plaats van incidenten
- Predictive analysis en preventieve maatregelen

SOC en interactie met de omgeving

1 mainly proactive role
2 highly automated SOC
3 supports business processes
4 high degree of standardization
5 infra mostly cloud-based
6 staffing changes
7 Internal organisation changes

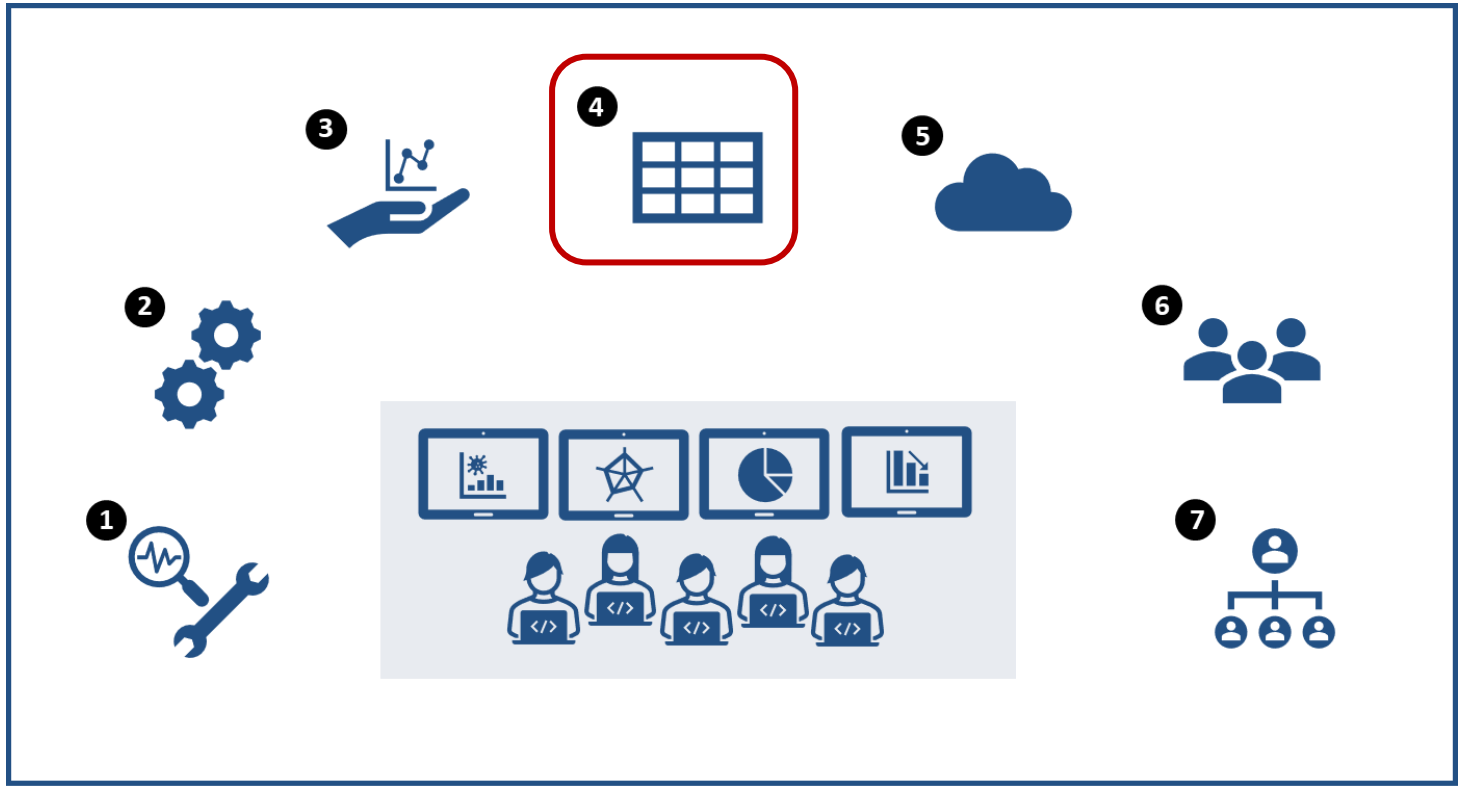
- Eerste lijn en grootste deel tweede lijn zijn vervangen door **geautomatiseerde oplossingen**
- AI (met beperkingen), SOAR en andere technologie
- Automatisering heeft andere ontwikkelingen in gang gezet

SOC en interactie met de omgeving

1 mainly proactive role
2 highly automated SOC
3 supports business processes
4 high degree of standardization
5 infra mostly cloud-based
6 staffing changes
7 Internal organisation changes

- SOC's verzamelen een grote hoeveelheid data van hoge kwaliteit in het kader van Situational Awareness
- Andere **bedrijfsprocessen profiteren** van de beschikbaarheid van deze data (continuous decision making in Zero Trust)

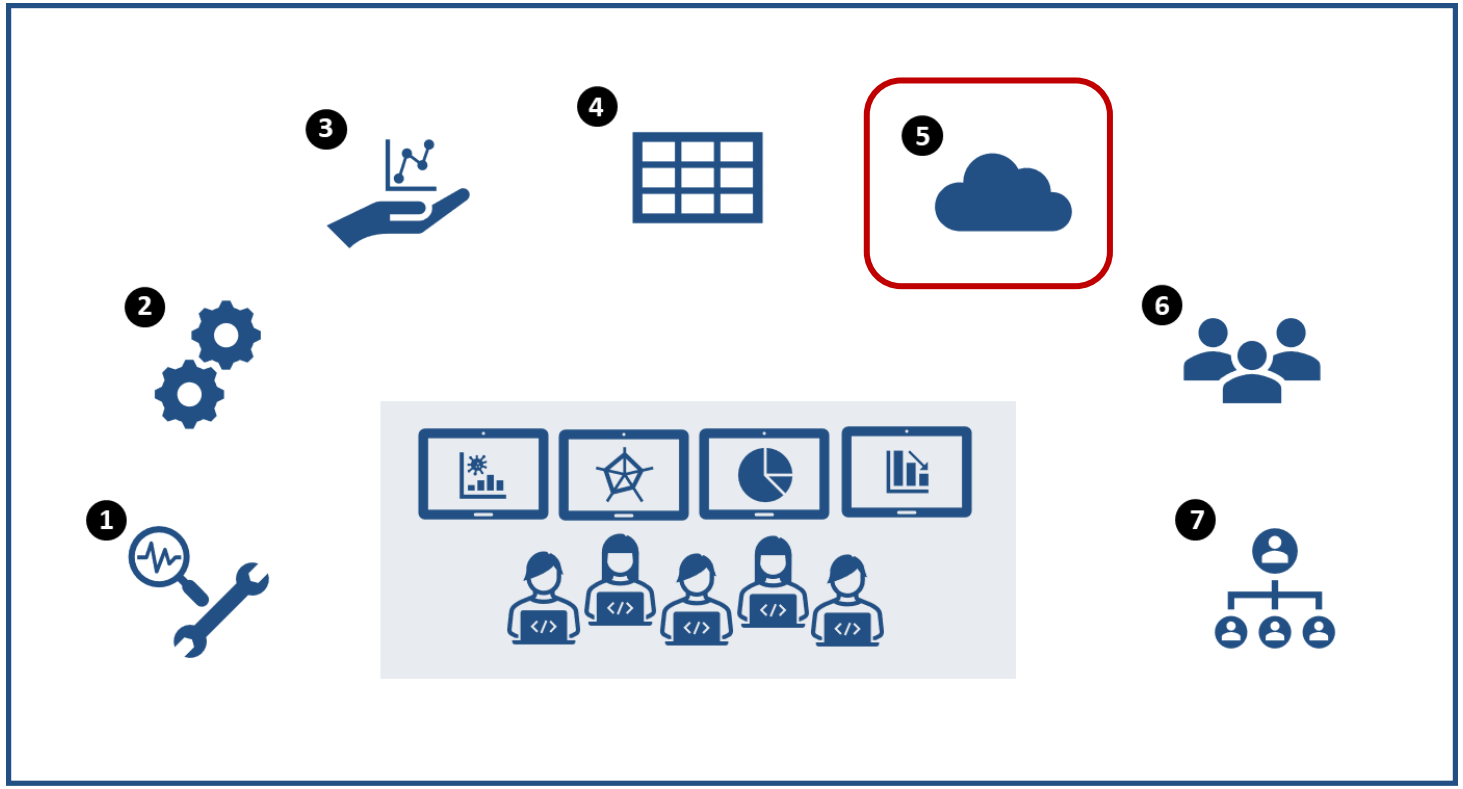
SOC en interactie met de omgeving



1 mainly proactive role
2 highly automated SOC
3 supports business processes
4 high degree of standardization
5 infra mostly cloud-based
6 staffing changes
7 Internal organisation changes

- Hoge mate van **standaardisatie**
- Gedreven door de noodzaak van samenwerking en hoge mate van automatisering
- Beter gebruik van:
  - Cyber security standaarden
  - Data exchange formats
  - Maturity models
  - …

SOC en interactie met de omgeving



1 mainly proactive role
2 highly automated SOC
3 supports business processes
4 high degree of standardization
5 infra mostly cloud-based
6 staffing changes
7 Internal organisation changes

Cloud security strategieën zijn de belangrijkste focus van SOC medewerkers

- Gebruik van gestandaardiseerde oplossingen van cloud tech providers
- IT services industrie heeft transitie naar “cloud tenzij” benadering achter de rug
- Uitzonderingen:
  - Gerubriceerde systemen
  - Zeer gevoelige IP
  - OT

SOC en interactie met de omgeving

1 mainly proactive role
2 highly automated SOC
3 supports business processes
4 high degree of standardization
5 infra mostly cloud-based
6 staffing changes
7 Internal organisation changes

Bemensing bestaat uit:

- CTI-analisten
- (business) risicoanalisten
- data analisten
- security engineers

Activiteiten bestaan uit:

- Verzamelen/ verwerken TI-data
- Situational Awareness verzorgen
- Predictive analysis
- Risk assessment
- Bepalen CoA

SOC en interactie met de omgeving

1 mainly proactive role
2 highly automated SOC
3 supports business processes
4 high degree of standardization
5 infra mostly cloud-based
6 staffing changes
7 Internal organisation changes

Interne organisatie is veranderd

- Tier-based model vervangen
- Georganiseerd op een skill- of role-based wijze, interdisciplinary teams
- Mandaat voor het doorvoeren van preventieve wijzigingen
- Business impact drempel voor additionele autorisatie

Takeaways

- De Blauwdruk kan overheden, organisaties met inhouse SOC, MSSP’s en MSSP-klanten helpen om plannen te ontwikkelen voor de toekomst

- De Blauwdruk is een discussie stuk en geen glazen bol

- We hebben al van verschillende kanten gehoord dat deze Blauwdruk nuttig is gebruikt

Discussie

Het volledige rapport kan hier worden gedownload:
https://publications.tno.nl/publication/34642162/x0DJXn/TNO-2023-R11803.pdf

Voor vragen en/of opmerkingen over het onderzoek:

reinder.wolthuis@tno.nl

gert.vanderlee@tno.nl

richard.kerkdijk@tno.nl

Thank you for your attention