COB Quickscan cybersecurity

Erik Versteegt – Siemens Mobility BV

Team: Rene Valstar – FoxIT / Ico Jacobs – RWS / Robbert Ross - RWS

SIEMENS

Doel / uitgangspunten Quickscan cybersecurity

Doel:
Leveren van handvat voor gesprek over cybersecurity

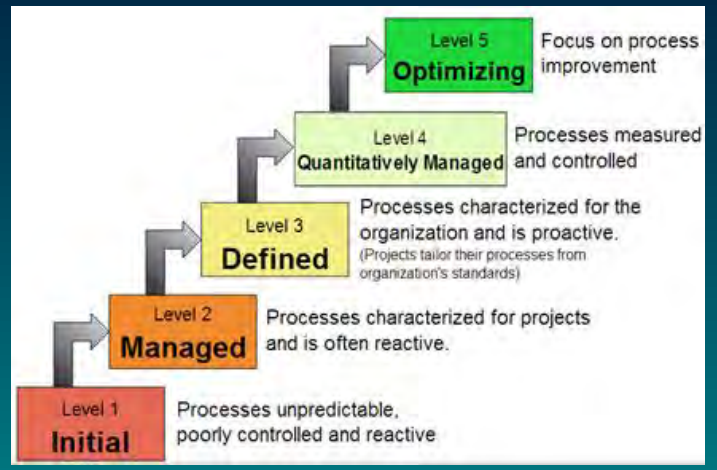
Uitgangspunten:
- Het moet aanleiding bieden tot gesprek
- Toegankelijk / begrijpelijk voor niet-deskundigen
- Het moet wel iets zeggen
- Geen volwaardige volwassenheidsanalyse
- Gemakkelijk bruikbaar

Opzet quickscan

- 21 vragen verdeeld over 4 categorieën
  - Governance en compliance (hoe organiseer je)
  - Preventie (hoe voorkom je)
  - Detectie (hoe ontdek je)
  - Response (hoe reageer je)

- Bij elke vraag scoren volwassenheid op 5 niveaus (CMMI maturity levels)

- Uitkomsten visueel weergegeven



De quickscan

- https://www.cob.nl/document/quickscan-cybersecurity-tunnels

Quickscan cybersecurity tunnels

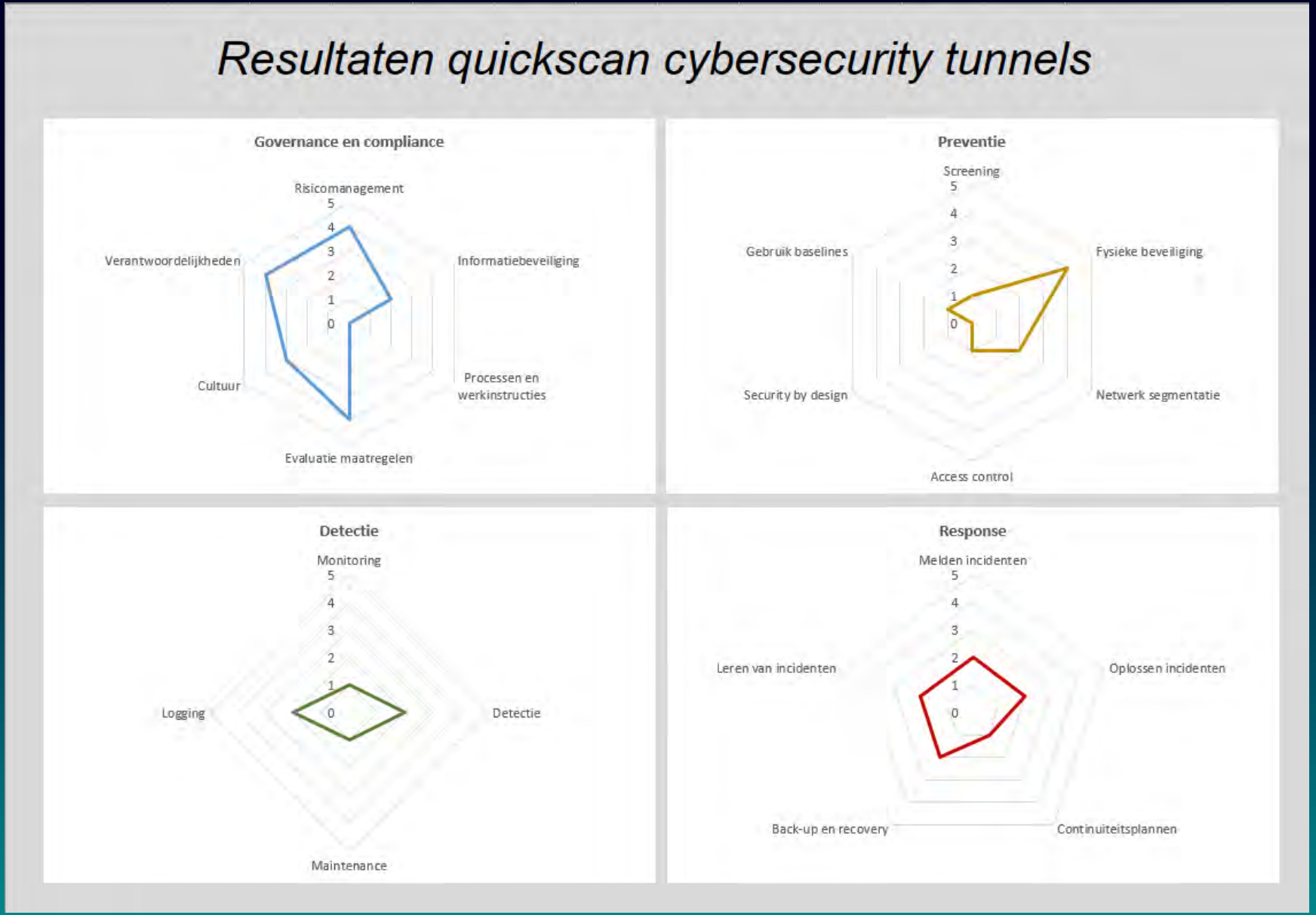
Instructies

De quickscan maakt gebruik van vier categorieën: (1) Governance & compliance, (2) Preventie, (3) Detectie en (4) Response.
1. Vul in de kolom 'Score' voor elke vraag/maatregel de juiste score in door te kijken naar de criteria die aan de rechterzijde gegeven wordt. Kies hierbij het niveau waaraan nog volledig voldaan wordt.
2. Op het werkblad 'Resultaten' is vervolgens per categorie grafisch de score te zien.

			Een organisatie bevindt zich op NIVEAU 1 als nog onbekend is hoe een proces in elkaar zit en hoeveel hulpmiddelen er nodig zijn om een resultaat te bereiken. Procesverbetering is niet systematisch.	Als het proces onder normale omstandigheden voorspelbaar is in termen van tijd en geld, bevindt de organisatie zich op NIVEAU 2. Bij invoering van nieuwe technologieën of methoden valt men nog terug op niveau 1.	Op NIVEAU 3 is het proces gedefinieerd en onder controle. Ook bij afwijking van de normale omstandigheden kan goed worden gereageerd. Procesverbetering vindt plaats op basis van een kwalitatieve analyse.	Er is sprake van NIVEAU 4 als er systematisch aan het proces wordt gemeten om afwijkingen vroegtijdig te constateren en te verbeteren. Procesverbetering vindt plaats op basis van kwantitatieve analyse.	Op NIVEAU 5 is systematische procesverbetering op basis van metingen een geïntegreerd onderdeel geworden van de bedrijfsvoering. Nieuwe technologieën kunnen beheerst worden ingevoerd.	
Categorie	**Vraag/maatregel**	**Score**	**Initieel**	**Herhaalbaar**	**Gedefinieerd**	**Beheerst**	**Geoptimaliseerd**	**Ruimte voor opmerkingen**
Governance & compliance *Maatregelen op het niveau van de organisatie*	Er is risicomanagement geïmplementeerd en er worden periodiek risicoanalyses uitgevoerd.	4	Er wordt aan risicomanagement gedaan.	Risicomanagement is meerdere keren uitgevoerd.	Het proces van risicomanagement is gedetailleerd beschreven.	Het risicomanagement wordt gecontroleerd en er zijn KPI's voor vastgesteld.	De kwaliteit van het proces van risicomanagement wordt gemeten en op basis hiervan verbeterd.	
Governance & compliance	Er is een informatiebeveiligingsbeleid (IB-beleid) opgesteld en gedeeld binnen de organisatie, en naar onderaannemers doorgeleid.	2	Er is een IB-beleid.	Het opstellen van het IB-beleid heeft meerdere keren plaatsgevonden.	Het proces van het opstellen van het IB-beleid is vastgelegd.	De kwaliteit van het IB-beleid wordt gemeten.	Er vindt verbetering van het IB-beleid plaats en van het proces om dit vast te stellen.	
Governance & compliance	Geformuleerd beleid is vertaald naar bijbehorende processen en werkinstructies.	0	Er zijn vastgelegde processen.	Voor al het vastgestelde beleid zijn processen.	Processen zijn op gelijke wijze beschreven en gedocumenteerd.	De processen worden periodiek geaudit en beoordeeld.	Processen worden aangepast op basis van tests en uitkomsten van geleerde lessen.	
Governance & compliance	Genomen securitymaatregelen worden gemonitord, getest en geëvalueerd en eventuele bijstelling vindt plaats aan de hand van uitkomsten.	4	Maatregelen wordt getest.	Testuitkomsten worden gestructureerd beoordeeld en verwerkt.	Processen om maatregelen te monitoren zijn vastgelegd.	Er vinden audits plaats op het proces van continu verbeteren van de genomen maatregelen.	Er wordt actief gezocht naar nieuwe dreigingen en mogelijke verbeteringen.	
Governance & compliance	Er is een cybersecuritycultuur geïmplementeerd binnen de organisatie.	3	Er vinden initiatieven plaats om de awareness te vergroten.	Het vergroten van de awareness vindt plaats op basis van een vooraf vastgesteld plan. Er worden trainingen aangeboden.	De cultuurverandering vindt plaats met daarbinnen aandacht voor verschillende groepen medewerkers. Ook trainingen worden gedifferentieerd aangeboden.	De cultuurverandering wordt gemeten en beoordeeld.	Er worden verbeteringen voorgesteld aan de hand van de meting van de cultuurverandering.	
Governance & compliance	Verantwoordelijkheden voor de beveiliging van de netwerk- en informatiesystemen zijn belegd.	4	De beveiliging van netwerk- en informatiesystemen wordt ad-hoc uitgevoerd.	De verantwoordelijkheid voor de beveiliging van netwerk- en informatiesystemen is vastgelegd.	Er is een RACI-matrix (omschrijving van rollen van medewerkers in een proces) of toegang tot systemen is gebaseerd op role-based access.	Organisatorische onafhankelijkheid is gewaarborgd voor informatiebeveiliging.	De verantwoordelijkheid voor informatiebeveiliging wordt aangepast op basis van onderzochte resultaten.	
Preventie *Maatregelen ter voorkoming van cybersecurity-incidenten.*	Er vindt screening plaats van medewerkers, toeleveranciers, aannemers en onderaannemers die op het object werken.	1	Personeel en toeleveranciers worden ad-hoc gescreend.	Personeel moet een VOG overleggen bij indiensttreding. Toeleveranciers moeten zich legitimeren bij aankomst.	Medewerkers en toeleveranciers worden volgens een gedefinieerd proces gecontroleerd (bv. vooraf VOG overleggen, legitimeren bij aankomst).	Medewerkers en (vaste) toeleveranciers worden met regelmaat (bv. elke 2 jaar) gecontroleerd (bv. nieuw VOG overleggen).	Alle medewerkers en toeleveranciers worden gescreend op basis van een risico-gebaseerd profiel van hun werkzaamheden.	
Preventie	Er is fysieke beveiliging ingericht.	4	De fysieke beveiliging van de automatiseringssystemen (toegang tot technische ruimtes en kasten) gebeurt ad-hoc en op basis van eigen initiatief.	De fysieke beveiliging van de automatiseringssystemen verloopt volgens een redelijk vast stramien (bv. via een sleutelverantwoordelijke). Technische	De fysieke beveiliging van de automatiseringssystemen is vastgelegd in een beveiligingsplan, dat ook nageleefd wordt. Toegang wordt vastgelegd in een	Het beveiligingsplan wordt met regelmaat herzien. Er vinden controles plaats of toegang (bv. sleutels) op de juiste wijze wordt verleend en vastgelegd, of ruimtes en	De fysieke beveiliging van de automatiseringssystemen is gebaseerd op een risico-gebaseerd proces dat periodiek herzien wordt.	

SIEMENS

De uitkomsten



Quickscan cybersecurity tunnels

*De quickscan cybersecurity voor tunnels (en andere infra objecten) biedt op een **toegankelijke** en **praktische** wijze **handvatten** voor een **eerste inzicht** in en een **gesprek** over de volwassenheid van uw object.*

Voor vervolgacties, een meer diepgravende analyse, en plannen om de volwassenheid te verbeteren, zijn experts nodig.

Contact

info@cob.nl
085 4862 410