TLP:GREEN

SOC STRATEGISCHE AANBEVELINGEN

Monitoring & Detectie – Readiness Assistance

Best Practice 1.2

Complexiteit document

Gemiddeld 

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

Monitoring- en detectiediensten zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om monitoring- en detectiediensten effectief in te kunnen zetten zijn er diverse onderwerpen die binnen een organisatie moeten zijn ingericht. Dit document "SOC Strategische Aanbevelingen" voorziet in tips en aanbevelingen op strategisch niveau en ondersteunt daarmee de organisaties die een Security Operations Center (SOC) willen realiseren.

Achtergrond

VSSR levert verschillende kennisproducten die aansluiten bij de SOC Readiness Quickscan. In dit document worden handvatten geboden die aansluiten bij de vragen op strategisch en tactisch niveau in de SOC Readiness Quickscan.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor Senior Management op strategisch niveau, functionarissen die zijn belast met inrichting van de SOC-functie, projectleiders, architecten en security officers.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
1.0	14-12-2023	Initiële versie
1.1	19-02-2024	Weergave document complexiteit opgenomen
1.2	11-9-2024	TLP Markering opgenomen

1.2 Referenties

Document	Link
VSSR Doelstellingen, v1.0 d.d. 16 november 2022	-
VSSR-kennisdocumenten	NCSC Producten en Diensten VSSR

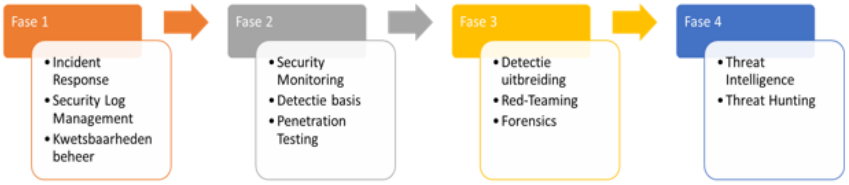
2 Management Samenvatting

Dit document is bedoeld voor een (Chief) Information Security Officer (CISO/ISO) of een Security Operations Center (SOC) Manager om een SOC-strategie uit te werken. In dit document wordt een SOC-strategie uitgewerkt met implementatie roadmap. Dit wordt gedaan op basis van de Baseline Informatiebeveiligingsbeleid Overheid (BIO) die als rode draad voor de opbouw en uitwerking van de strategie zal worden gebruikt.

Om tot een efficiënt functionerend SOC te komen, dienen er eerst een aantal basiselementen door de (C)ISO/SOC-manager te worden geformuleerd dan wel in kaart te worden gebracht. Deze basiselementen zijn: drivers, visie, missie, stakeholders, doelstellingen en strategie. Het beschrijven van deze onderdelen zijn belangrijke componenten om aan te werken voordat de roadmap wordt uitgewerkt.

Een voorbeelduitwerking van SOC-competenties met roadmap, voor implementatie op basis van de BIO, is hieronder weergegeven en in het document verder uitgewerkt. Hierbij worden drie hoofdcategorieën voor diensten gebruikt. Deze drie diensten worden ingevuld met verschillende competenties (teams/rollen) binnen het SOC. In de BIO worden verschillende (maar niet alle) competenties aangeraakt met bijbehorend Basis Beschermingsniveau (BBN-niveau). Op basis van de beschikbare BBN-niveaus en een gangbare ontwikkeling voor een SOC, is een fasering aangebracht. Deze fasering is gebruikt om op hoofdlijnen een implementatieplan uiteen te zetten.

Dienst	Competentie	BIO Thema	SOC Fase
Attack Services	Kwetsbaarhedenbeheer	Ja	1
	Threat Intelligence	Nee	4
	Penetratie Testen & Red-teaming	Ja / NVT	2 / 3
Detection Services	Security Log Management	Ja	1
	Detectie	Ja	2 / 3
	Security Monitoring	Ja	2
	Threat Hunting	Nee	4
Response Services	Incident Response	Ja	1
	Forensics	Nee	3



Figuur 1 Strategie samenvatting

De verdere uitwerking is stap voor stap, waarbij ook de BIO referenties zijn opgenomen. Daarnaast worden de verschillende competenties toegelicht, wordt een indicatie voor teamomvang gegeven en een basis set aan stuurmiddelen. Ook wordt per competentie op hoofdlijnen aangegeven welke technische ondersteuning in de vorm van tooling nodig zal zijn. Dit tezamen geeft een goed vertrekpunt en inzicht in de basismiddelen die nodig zijn om een SOC neer te zetten.

3 Inleiding

Het Security Operations Center (SOC) wordt meer en meer de spin in het web van cybersecuritystrategieën van organisaties. Veelal is risicobeheersing het vertrekpunt naar het op dagelijkse basis mitigeren van risico's. Het identificeren van kwetsbaarheden en eventueel ook het verder uitzetten binnen de organisatie kan bij een SOC worden belegd. Het detecteren, onderzoeken en opvolgen van mogelijke incidenten is doorgaans een SOC-taak. En zo zijn er nog meer operationele security taken die mogelijk bij een SOC zijn belegd. Hierbij is het vaststellen wat een SOC precies zou moeten doen binnen de organisatie vaak even uitdagend als het daadwerkelijk realiseren van het SOC.

Om een goed vertrekpunt te hebben voor het realiseren van een SOC (of het uitbreiden van een bestaand SOC), biedt dit document de nodige handvatten. Op basis van de BIO is een mogelijke strategie en implementatie roadmap uitgewerkt wat als leidraad kan dienen voor een willekeurige organisatie. De uitwerking is een voorbeeld en is niet voorschrijvend bedoeld. Iedere organisatie kan op basis van eigen inzichten de uitgewerkte roadmap aanpassen op basis van de eigen behoeften, strategie en volwassenheid.

In dit document worden de strategische uitgangspunten beschreven om het juiste vertrekpunt te hebben voor het bouwen van een eigen SOC of het inkopen van SOC-dienstverlening. Daarmee is dit document dan ook het meest geschikt voor een CISO/SOC-manager die de opdracht heeft gekregen om een SOC-strategie te ontwikkelen.

3.1 Leeswijzer

Strategie wordt in een aantal stappen ontwikkeld. De verschillende stappen in strategieontwikkeling worden in dit document gebruikt om tot een SOC-strategie te komen. In eerste instantie wordt de vraag in beeld gebracht (4.1). Hieruit wordt een Visie en Missie ontwikkeld (4.2). Stakeholders (4.3) worden in kaart gebracht waarna doelstellingen en strategie wordt bepaald (4.4). Als laatste wordt ingegaan op het Target Operating Model voor het SOC en hoe dit te realiseren (4.5).

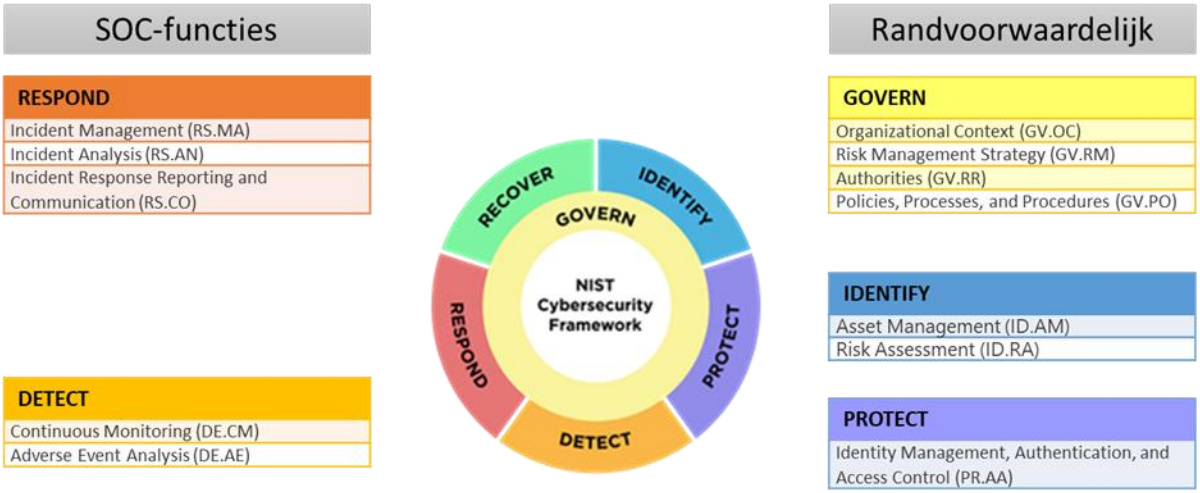
De uitwerking van de verschillende componenten wordt gedaan op basis van de Baseline Informatiebeveiliging Overheid (BIO) die als een rode draad voor de strategiebepaling zal fungeren. Om de rode draad te volgen, is het van belang om op voorhand de opbouw, structuur en begrippen van de BIO goed te begrijpen en het is raadzaam om de BIO als naslagwerk te gebruiken bij het doornemen van dit document.

3.2 Definities

Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities opgesteld in "Bijlage III – Definities" van dit document. Voor alle overige termen en begrippen verwijst dit document naar het online Woordenboek - Cyberveilig Nederland.

4 Security Operations Center strategie

In dit hoofdstuk worden handvatten geboden om stap voor stap een SOC-strategie op te bouwen. Een SOC-strategie dient onderdeel te zijn van een bredere cybersecuritystrategie die kan worden opgesteld op basis van bestaande frameworks. Een breed gedragen framework is het NIST CSF waarin vijf elementen worden onderkend, en in de nieuwe (draft) release nog een zesde element. De elementen zijn: Govern, Identify, Protect, Detect, Respond en Recover. Een SOC beslaat een aantal functies binnen deze zes elementen. Daarnaast zijn een aantal functies rand voorwaardelijke voor het goed functioneren van een SOC. Dit benadrukt direct het belang van de bredere cybersecurity context waarbinnen een SOC opereert.



Figuur 2 NIST CSF context voor een SOC

Binnen dit hoofdstuk wordt eerst het waarom voor de organisatie behandeld in de vorm van de business drivers om een SOC op te zetten of aan te besteden. Het doel hiervan is om vast te leggen wat de belangrijkste drijfveren zijn voor de organisatie om een SOC op te zetten en wat de toegevoegde waarde moet zijn.

Daarna wordt het wat voor de organisatie uitgewerkt door middel van het opstellen van een visie en missie en het in kaart brengen van de wensen van de verschillende belanghebbende binnen de organisatie.

Als laatste wordt ingegaan op het realisatie vraagstuk (hoe) door de doelstellingen, strategie en het target operating model (TOM) uit te werken.

4.1 Business Drivers voor een SOC

Vanuit de organisatie zullen verschillende drijfveren bepalen hoe en waarom een SOC moet worden opgebouwd. Het doel voor deze paragraaf is het beschrijven waarom een organisatie business drivers voor het SOC nodig heeft, wat het doel van deze business drivers is en hoe de organisatie specifieke business drivers kan vaststellen.

4.1.1 Waarom SOC-drivers vaststellen?

Het doel van het vaststellen van business drivers voor het SOC is om de beveiligingsstrategie en doelstellingen van de organisatie te ondersteunen door middel van het uiteenzetten en vastleggen van de belangrijkste drijfveren om een SOC op te zetten. De SOC-business drivers en de prioritering van deze drivers bepalen hoe de organisatie haar middelen en inspanningen moet inzetten om haar doelen te bereiken.

Managementkeuzes die zijn gebaseerd op de business drivers sluiten aan bij de doelstellingen en zijn daarom uitlegbaar aan de organisatie. Dit vergroot het draagvlak en daarmee ook de realiseerbaarheid van een keuze.

Het SOC heeft business drivers nodig om de beveiligingsstrategie van de organisatie te ondersteunen, zonder deze drivers is het SOC stuurloos en inefficiënt.

4.1.2 Vaststellen van SOC-drivers

SOC-drivers kunnen worden afgeleid van de business drivers die door de organisatie zijn opgesteld. Business/SOC drivers ontstaan door interne en externe invloeden (bijvoorbeeld wetgeving) en resulteren vaak in een koers, of koersveranderingen van de organisatie. Door de Business/SOC drivers vast te stellen heeft een organisatie handvatten om bepaalde keuzes tegen elkaar af te wegen. Door aan deze drivers een prioriteit toe te kennen kan een organisatie bepalen welke inspanningen en investeringen als eerste gedaan moeten worden. Met dit inzicht is een organisatie in staat om benodigde budgetten beschikbaar te stellen en potentiële risico's te identificeren.

Het opstellen van SOC-drivers vereist kennis van de organisatie en haar doelstellingen. Een aantal voorbeeld onderwerpen die kunnen helpen bij het opstellen van SOC-drivers worden hieronder beschreven.

- Identificeren van de strategische doelen

  Wat zijn de strategische doelen van de organisatie en hoe kan de beveiligingsstrategie van het SOC daaraan bijdragen.

- Uitvoeren Business Impact Analyse (BIA)

  Vaststellen van de belangrijkste bedrijfsprocessen en systemen (kroonjuwelen) die moeten worden beschermd door het SOC
  Vaststellen van de belangrijkste beveiligingsrisico's en wat de mogelijke impact daarvan is op de bedrijfsprocessen en systemen. Dit kan door het (laten) opstellen van een organisatie-specifiek dreigingsbeeld en/of het uitvoeren van risicoanalyses.

  Tip: Start met een beperkte scope voor het uitvoeren van een BIA. Op deze manier is de BIA-uitvoering behapbaar, scope uitbreiding kan in volgende iteraties.

- Identificeren compliance-eisen

  Welke compliance-eisen zijn van toepassing op de organisatie. Denk bijvoorbeeld aan AVG,

ISO27001 en BIO.

- Prioriteren van de beveiligingsrisico's

  Capaciteit en middelen zijn niet onbeperkt. Dit maakt het noodzakelijk om keuzes te maken in wat wel en niet mogelijk is. Het prioriteren van de belangrijkste beveiligingsrisico's op basis van bedreigingen en compliance-eisen helpt bij het maken van deze keuzes. Het opstellen van een dreigingslandschap kan helpen om deze beveiligingsrisico's in kaart te brengen.

- Vaststellen vereiste middelen en budgetten

  Welke vereiste middelen en budgetten zijn nodig om de geprioriteerde beveiligingsbehoeftes van de organisatie in te vullen. Geprioriteerde beveiligingsbehoeftes die (vanwege een beperkt budget) niet kunnen worden gerealiseerd moeten worden opgenomen in het Risicoregister en Risico Acceptatie Overeenkomst.

  De organisatie dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan. BIO paragraaf 4.2.

- Definiëren van meetbare doelstellingen

  Definieer meetbare doelstellingen die de voortgang en successen van het SOC meten. Hiermee wordt inzicht verkregen in de behaalde resultaten en doelstellingen die eventueel (nog) niet behaald zijn en is het mogelijk om hierop te sturen.

De business drivers van het SOC moeten periodiek worden geëvalueerd en indien nodig worden herzien en/of bijgewerkt. Dit als gevolg van veranderingen in bedrijfsprocessen, nieuwe certificeringseisen, beveiligingsrisico's, dreigingen, wet- en regelgeving en strategische doelen van de organisatie.

4.2 SOC Visie & Missie

Het doel voor deze paragraaf is beschrijven waarom een organisatie een visie en missie voor het SOC nodig heeft en wat hiervan het doel is.

4.2.1 Waarom een SOC-Visie & -Missie

Een SOC-visie beschrijft de gewenste toekomstige staat van het SOC en geeft een beeld van hoe het SOC er op de lange termijn uit gaat zien. Een visie helpt het SOC, en de organisatie, om een gemeenschappelijk beeld te creëren van de toekomst en geeft richting aan beslissingen en acties.

Een visie geeft het SOC strategische richting en doelstellingen, en het helpt om SOC-medewerkers gemotiveerd en gefocust te houden op de belangrijkste doelen en prioriteiten.

Een missie beschrijft het doel en bestaansrecht van het SOC. Het geeft aan wat het SOC voor de organisatie wil bereiken, beschrijft de kernactiviteiten en hoe deze bijdragen aan de visie. Een missie is meestal meer gericht op de korte termijn en beschrijft wat het SOC nu doet en waarom.

Een missie helpt het SOC om zich te concentreren op haar kerntaken, verantwoordelijkheden en geeft duidelijkheid over de rol van het SOC binnen de organisatie.

SOC-visie en missie in hoofdlijnen	
SOC Visie	Een visie geeft het SOC strategische richting en doelstellingen
SOC Missie	Een missie beschrijft de kernactiviteiten en hoe deze bijdragen aan de visie. Een missie is meestal meer gericht op de korte termijn en beschrijft wat het SOC nu doet en waarom

Tabel 1 – SOC-visie versus missie

4.2.2 Vaststellen van de SOC-Visie

Een visie voor het SOC moet gericht zijn op het creëren van een veilige digitale omgeving voor de organisatie.

Onderwerpen die kunnen worden opgenomen in de visie zijn:

- Risico of compliance gedreven beveiligingsstrategie;
- SOC Activiteiten;
- SOC Sourcing strategie;
- SOC Certificeringen;
- SOC Volwassenheidsniveau;
- Samenwerkingen.

4.2.3 Vaststellen van de SOC-Missie

Een missie voor het SOC moet gericht zijn op het beschermen van de organisatie tegen cyberbedreigingen en het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de kritische systemen en (privacy) gevoelige data.

Een aantal voorbeelden van onderwerpen die kunnen worden opgenomen in de missie zijn:

- Te beschermen belang (TBB)

  Het SOC draagt bij aan de bescherming van informatie en informatiesystemen tegen beveiligingsincidenten en dreigingen. Het SOC focust op de beschikbaarheid, integriteit en vertrouwelijkheid van deze informatie en de systemen waarin deze informatie wordt verwerkt.

- (Continue) Security Monitoring, detectie en response

  Het SOC heeft zicht op relevante dreigingen en is in staat om (pogingen tot) cyberaanvallen tijdig op te merken en hier tijdig en adequaat op te reageren. Dit alles om schade te minimaliseren en bij voorkeur te vermijden.
  Het SOC beschikt hiervoor over monitoringinfrastructuur, analisten en een incidentresponsproces dat hierop is ingericht. De beschikbaarheid van het SOC is hierop afgestemd.

- Proactieve houding

  Het SOC hanteert een proactieve houding om potentiële dreigingen te zoeken, te detecteren en opvolging te geven c.q. in gang te zetten zodanig dat deze schade wordt geminimaliseerd en bij voorkeur wordt vermeden.

- Samenwerking

  Het SOC werkt hiervoor samen met afdelingen binnen de eigen organisatie, (externe) leveranciers en organisaties en/of communities die zich inzetten voor de beveiliging van digitale systemen.

- Continue verbetering

  Cybercriminelen en statelijke actoren zijn in staat hun capaciteiten om cyberaanvallen uit te voeren snel te ontwikkelen. Dit vereist dat de verdedigende kant deze ontwikkelingen volgt en zich continu verbetert. Het effectief in stand houden van een SOC vereist daarom

dat het SOC zich continu ontwikkelt. Het SOC moet in staat zijn om continu en tijdig mee te bewegen met het voortdurend veranderende dreigingslandschap.

4.3 Stakeholdermanagement

Deze paragraaf beschrijft waarom een goed stakeholdermanagement essentieel is bij het opzetten van het SOC.

4.3.1 Waarom stakeholdermanagement

Voor het opzetten van een SOC is het belangrijk om eerst vast te stellen wie de stakeholders zijn en welke stakeholders bepalend zijn voor het succes van het SOC. Bij goed stakeholdermanagement is er transparante communicatie en worden de verschillende belangen gezamenlijk tegen elkaar afgewogen en geprioriteerd. Door de belangen gezamenlijk tegen elkaar af te wegen en te prioriteren ontstaat er een nauwe betrokkenheid van alle stakeholders. Deze nauwe betrokkenheid verkleint de kans op onvoorziene belangen die het opbouwen, of functioneren, van een SOC vertragen of in gevaar brengen.

4.3.2 Vaststellen SOC-stakeholders

De SOC-stakeholders zijn alle belanghebbenden en mogelijke tegenstanders. Invloedrijke tegenstanders vormen een groot risico voor het functioneren van een SOC. Door de belangen van deze stakeholders mee te nemen in de afwegingen en prioritering vergroot het de bewustwording en toegevoegde waarde van het SOC.

Potentiële SOC-stakeholders zijn:

- Het management of bestuur van de organisatie vanwege eindverantwoording beveiliging en financiering (Bijvoorbeeld de CEO, CFO, COO, CIO);
- Privacy Officer (PO) vanwege vereisten gegevensbescherming en privacy;
- Interne IT-afdelingen die verantwoordelijk zijn voor het beheer en onderhoud van de IT-infrastructuur. Dit vanwege de potentiële impact van het SOC op de team capaciteit en de samenwerking bij het oplossen van incidenten en kwetsbaarheden.
- Operationele securityteams die werken aan het ontwikkelen, implementeren en integreren van beveiligingsmaatregelen;
- Incident Response teams vanwege de potentiële impact van het SOC op de team capaciteit en afstemming van operationele processen bij incidentherstel;
- (Externe) Leveranciers van beveiligingsoplossingen die geïntegreerd moeten worden met het SOC;
- Ketenpartners waarmee (essentiële) integraties zijn gerealiseerd;
- Een vertegenwoordiger van de eindgebruikers en/of klanten die profiteren van een betere beveiliging en geraakt kunnen worden door beveiligingsmaatregelen.

4.4 Doelstellingen en Strategie

In een eerdere paragraaf is uiteengezet waarom een visie en een missie belangrijk zijn voor het opzetten van een SOC. In deze sectie wordt het uitwerken van doelstellingen en bijbehorende strategie verder uitgelegd.

4.4.1 Waarom doelstellingen en een strategie

Als de visie en missie duidelijk zijn geformuleerd, is de realisatie nog niet vanzelfsprekend. Hoe de visie en missie te realiseren, is afhankelijk van de doelstellingen en de strategiebepaling. De doelstellingen bepalen wat men op de middellange termijn wil bereiken. Hierbij wordt binnen de strategie uiteengezet met welke middelen, mensen en tijd de visie en missie gerealiseerd gaan worden. Een doelstelling kan verder worden opgedeeld in doelen om hiermee in kleinere brokken een planning te maken. De strategie en doelstellingen zijn op een redelijk hoog abstractieniveau

beschreven. In de volgende stap, het samenstellen van een target operating model, wordt in meer detail beschreven hoe het SOC gevormd zal worden. Pas als dat duidelijk is, kan een meer gedetailleerd plan worden gemaakt.

4.4.2 Hoe doelstellingen en strategie te bepalen

Voor het samenstellen van goede doelstellingen en een strategie zijn veel handvatten beschikbaar. Als een SOC nog in oprichting is, geniet het de voorkeur om eerst met de organisatie vast te stellen wie precies de verschillende stakeholders binnen de organisatie zijn en wat hun behoeften zijn. Op basis hiervan kan de scope voor het SOC worden vastgesteld.

Voor de bepaling van goede doelstellingen en een strategie kunnen bestaande tools zoals Business Model Canvas, een SWOT-analyse[1] (Strengths, Weaknesses, Opportunities en Threats) en beproefde methodes als OGSM[2] (Objective, Goals, Stategies and Measures) worden gebruikt. Een beschrijving van hoe deze tools te gebruiken, valt buiten de scope van dit document maar hier is voldoende literatuur over beschikbaar.

4.4.3 Strategie overwegingen

Bij de strategiebepaling is het van belang om een aantal zaken in overweging te nemen:

1. Reageren (Response) is het doel, detecteren is het middel (Detect)[3]
   Onafhankelijk van specifieke organisatiebehoeften is het verstandig om altijd te beginnen met het opzetten van een Incident Response competentie. Als dit onderdeel niet is opgezet, hebben andere competenties weinig ruimte om hun output te laten landen en zal de opvolging van incidenten in de organisatie een uitdaging zijn.
2. Reageren betekent afspraken maken
   Het SOC kan niet zelfstandig opereren, maar is afhankelijk van de rest van de organisatie. Met verschillende organisatieonderdelen dienen vooraf afspraken te worden gemaakt over verantwoordelijkheden bij incidenten en wie, wat wel en niet mag (denk bijvoorbeeld aan het stekkermandaat, of toegang tot systemen met gevoelige data). Ook voor het onderzoeken van eenvoudige (potentiële) incidenten is het van belang om goede afspraken te maken met eigenaren van data, applicaties en systemen. Bij outsourcing van diensten, is het verstandig om duidelijke afspraken te maken over de verantwoordelijkheden van opdrachtgever en leverancier.
3. Capaciteit en bekwaamheid
   Kleine, dagelijkse incidenten kunnen veelal opgevangen worden door eigen mensen. Bij grote en complexe incidenten is dit misschien anders. In specifieke gevallen kan het noodzakelijk zijn om qua capaciteit van het IR-team op te schalen (eventueel tijdelijk met extra externe mensen) of om niet alledaagse competenties in huis te halen die alleen bij gespecialiseerde partijen beschikbaar zijn (denk aan malware analisten, forensische specialisten die bevoegd zijn om politie van bewijslast te voorzien, etc.).
4. Doelstellingen
   Om een goed functionerend SOC neer te kunnen zetten (of te kunnen aanbesteden) is het van belang om na te denken over wat voor SOC de organisatie nodig heeft en waar de focus op moet liggen:
   - *Compliance*: Compliance met wet- en regelgeving is van belang voor elke organisatie dus hier dient altijd rekening mee gehouden te worden. Maar het zou kunnen dat dit ook het enige doel is voor het opzetten van SOC-diensten. Vanuit een cybersecurity perspectief heeft een compliance-gedreven SOC niet de voorkeur maar het kan voldoende zijn voor uw organisatie.
   - *Tactisch*: Is cyberweerbaarheid het doel, dan is een tactisch SOC het middel. Een tactisch SOC richt zich op het inrichten van detectie en response om op basis van actuele dreigingen aanvallen te kunnen detecteren om zo de organisatie te helpen.

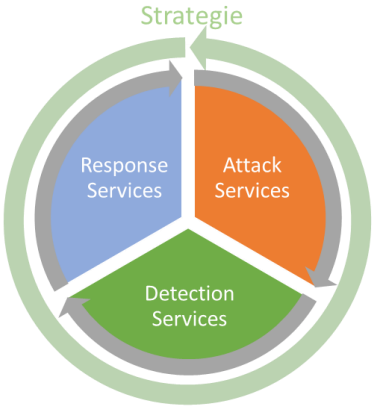
[1] Sterkte-zwakteanalyse - Wikipedia
[2] OGSM - Wikipedia
[3] In samenwerking met Defensie Cyber Security Centrum (DCSC)

- *Intelligence Driven*: Als uw organisatie nog een stap verder wilt, dan wordt het van belang om (een) eigen Threat Intelligence / Hunting team(s) in gaan te richten. Hiermee worden actuele dreigingen continu gemonitord zoals een security monitoring team continu naar detectie alerts kijkt. Daarnaast gaat het SOC actief opzoek naar gematerialiseerde dreigingen die niet door de detectiesystemen zijn opgepikt.
- *Cyber Defense Center (CDC)*: Gaat u nog een stap verder door een actieve component te introduceren, dan wordt het SOC een CDC. Een CDC kenmerkt zich door de mogelijkheid om actief in te grijpen zodra aanvallen of breaches worden geconstateerd. Hiervoor is dan vaak een ander mandaat nodig dat een meer passief SOC heeft.

Andere overwegingen kunnen zijn:

- Wat zijn de te beschermen belangen binnen de organisatie (eigendommen, gevoelige informatie, etc.) en in hoeverre bepaalt dit de benodigde competenties?
- Zijn bepaalde typische SOC-competenties al aanwezig binnen de organisatie en vallen deze mogelijk voor het SOC buiten scope of dienen ze juist expliciet bij het SOC ondergebracht te worden?
- Is het vanuit strategisch oogpunt van belang om bestaande competenties bij het SOC onder te gaan brengen, wat mogelijk een transformatie binnen de organisatie met zich meebrengt?
- Heeft de organisatie bestaande strategieën, bijvoorbeeld cloud strategie en (out)sourcingsstrategie, om rekening mee te houden en/of is het van belang dat bestaande strategieën wordt aangepast ter facilitering van het goede security monitoring?
- Is het SOC 24 uur per dag, 7 dagen per week, beschikbaar? Of volstaat een andere vorm van beschikbaarheid?
- In hoeverre wordt het SOC verantwoordelijk voor incidentopvolging en welk mandaat hoort hierbij (denk aan het stekkermandaat)?
- In hoeverre wordt het SOC, deels of geheel, verantwoordelijk voor compliance monitoring en -rapportages?
- Zijn er doelstellingen met betrekking tot volwassenheid[4] van het SOC vastgesteld?

Als deze overwegingen op de service categorieën worden gelegd, dan is de volgordelijkheid van implementeren tegengesteld aan de operationele volgordelijkheid. Operationeel gezien zal er eerst een aanval zijn, die wordt gedetecteerd en daarna start te opvolging van een incident. Om dit goed te kunnen doen, is het dus van strategisch belang om eerst opvolging (response) mogelijk te maken, dan detectie en security monitoring om dan als laatste te kijken naar de Attack Services.



[4] Voor het meten van SOC-volwassenheid kan gebruik worden gemaakt van het SOC-CMM: SOC-CMM - Improving security operations globally

In veel gevallen is het verstandig om een SOC gefaseerd op te bouwen. Op basis van praktijkervaringen zou een aanpak, zoals weergegeven in onderstaande Tabel 2 SOC-strategie fasering, kunnen worden gevolgd waarbij het voor elke fase is te overwegen om bij response te beginnen en bij attack te eindigen.

Dienst	Competentie	Fase 1	Fase 2	Fase 3
Attack Services	Kwetsbaarhedenbeheer	●	●	●
	Threat Intelligence			●
	Penetratie Testen & Red-teaming		●	●
Detection Services	Security Log Management	●	●	●
	Detectie		●	●
	Security Monitoring		●	●
	Threat Hunting			●
Response Services	Incident Response	●	●	●
	Forensics			●

Tabel 2 SOC-strategie fasering

Een laatste overweging betreft de financiering van een SOC. Een SOC is meer dan een samenstel van een set tools en een aantal analisten om alarmen te onderzoeken. Een goed opererend SOC draait op veel meer aspecten die mee dienen te worden gewogen binnen het bepalen van de Total Cost of Ownership (TCO). Voor de TCO zijn twee zaken van belang:

1. De organisatiecontext waarbij een kostentoename zal ontstaan door uit opbouwen van een SOC;
2. De kosten voor het SOC zelf.

- Context: Voordat een SOC opgezet kan worden, is het goed om te bepalen wat nodig is bij andere organisatie(onderdelen). Het is bijvoorbeeld verstandig om:
    - Verschillende security policies te beschrijven;
    - Afspraken te maken met IT-leveranciers en mogelijk zaken in contracten op te nemen;
    - Onderzoeken welke wijzigingen binnen de IT-infrastructuur nodig zijn om data bij het SOC te krijgen;
    - Afspraken te maken met verschillende organisatieonderdelen betreft incident opvolging.
- SOC-aanschaf versus operationele kosten: In eerste instantie zal voor de opbouw van een SOC-projectbudget nodig zijn. Daarna zal ook operationeel budget nodig zijn. Bij het vaststellen van het operationeel budget dient ook rekening gehouden te worden met ondersteunende IT-dienstverlening zoals server- en applicatiebeheer.

Binnen dit document is voor strategiebepaling gekozen om de Baseline Informatiebeveiliging Overheid (BIO) te gebruiken. De BIO geeft vanuit een risicobeheerperspectief, op basis van basisbeveiligingsniveaus, richting aan de verschillende aspecten van informatiebeveiliging waarbij onderdelen betrekking hebben op een Security Operations Center. Dit wordt gebruikt om richting te geven, keuzes te maken en te prioriteren binnen, bijvoorbeeld, het samenstellen van het Target Operating Model, de fasering hiervan en het maken van een lange termijnplanning. De BIO wordt binnen dit document gebruikt maar deze keuze is nadrukkelijk niet bedoeld om voorschrijvend te zijn. Elke organisatie heeft eigen drijfveren op basis waarvan strategie kan worden bepaald dus bekijk dit goed voor de eigen omgeving.

4.5 Target Operating Model

Deze paragraaf beschrijft met welke onderdelen rekening kan worden gehouden bij het opstellen van een Target Operating Model (TOM) voor een SOC. Hierbij is het voor de CISO/SOC-manager van belang om goed te kijken naar de visie, missie, doelstellingen, strategie en roadmap om te bepalen welke onderdelen van toepassing zijn op de eigen organisatie.

4.5.1 Waarom een Target Operating Model

Het Target Operating Model (TOM) beschrijft hoe een organisatie haar mensen, informatie, processen en technologie inzet om het SOC daadwerkelijk te realiseren. Hierbij zal vooral worden gekeken naar de verschillende diensten die door een SOC kunnen worden geleverd en de bijbehorende competenties die hiervoor nodig zijn. Om continu te kunnen evalueren of de verschillende competenties opereren en presteren in lijn met de vastgestelde strategische doelstellingen is het van belang om een aantal mogelijke meetinstrumenten en stuurmechanismen vast te stellen in de vorm van kritieke prestatie-indicatoren (KPI's)[5]. Het is aan de CISO en/of SOC-manager om te beoordelen welke competenties nodig zijn, welke KPI's men wil gebruiken en welke targets hierbij horen. De verdere uitwerking van de verschillende competenties volgt in 4.5.4 en een set voorbeeld KPI's zijn opgenomen in 4.5.8.

Rand voorwaardelijk voor een goed TOM zijn de strategische uitgangspunten voor het implementeren van een SOC en/of bijbehorende dienstverleningen. Zoals al aangegeven, is voor het bepalen van de SOC-strategie in dit document primair uitgegaan van de BBN-niveaus binnen de BIO. De keuzes binnen het TOM en de volgorde van implementatie zijn dan ook gebaseerd op het BBN zoals in de BIO weergegeven.

4.5.2 Besturing

Voordat de plaatsing van het SOC binnen de organisatie wordt beschouwd, is het van belang om eerst te kijken naar informatiebeveiliging in zijn geheel. Dit is een breder vraagstuk en betreft niet alleen het SOC, maar is wel van groot belang voor o.a. het goed functioneren van het stekkermandaat[6], maar ook voor de meer dagelijkse zaken als het opvolgen van kleinere incidenten en het (coördineren van) patchen van kwetsbaarheden in systemen. Binnen de overheid rapporteert de CISO direct aan de CIO[7].

Hoe past het SOC binnen de organisatie? In tegenstelling tot de CISO rol, is de positionering van een SOC binnen een overheidsinstantie niet nadrukkelijk vastgelegd. Van belang is dat een SOC relatief onafhankelijk van de beheerorganisatie is gepositioneerd. Daarom rapporteert in veel gevallen de SOC-manager direct aan de CISO. Afhankelijk van de rol van het SOC, kan worden overwogen om incident response binnen of buiten het SOC te positioneren. Als incident response verantwoordelijkheden niet onder het SOC vallen kan worden overwogen om deze functie direct aan de CISO te laten rapporteren. Een andere mogelijkheid is dat incident response breder wordt gezien dan alleen informatiebeveiliging-gerelateerd, in welk geval deze functie mogelijk elders in de organisatie wordt opgehangen en mogelijk direct aan de CIO rapporteert. Voor een goed functioneren van het SOC en een incident responsefunctie is het van belang dat het juiste mandaat wordt afgegeven. In geval van kritische incidenten zal risico-mitigatie soms boven beschikbaarheid gaan, waardoor een eigenaar of beheerder van een ICT-systeem soms niet het laatste woord heeft bij belangrijke beslissingen. Hierbij is het van belang om goed af te wegen welke functie onder welke omstandigheden gebruik mag maken van het stekkermandaat.

Ook bij het uitbesteden van SOC-diensten, heeft de eigen organisatie nog altijd enkele functies nodig om te zorgen dat de dienstverlening aansluiting heeft bij de behoefte van de organisatie:

- Regie: Bij uitbesteding zal er altijd een regieorganisatie aanwezig moeten zijn om de kwaliteit en continuïteit van de dienst te waarborgen en te sturen.

[5] Kritieke prestatie-indicator - Wikipedia
[6] Het stekkermandaat geeft het SOC de mogelijkheid om schadebeperkend op te kunnen treden bij kritische cyber-security incidenten door systemen en/of processen af te sluiten waardoor erger wordt voorkomen.
[7] wetten.nl - Regeling - Besluit CIO-stelsel Rijksdienst 2021 - BWBR0044613 (overheid.nl)

- Incident Response: In veel gevallen zullen uit een SOC-dienst incidenten voortkomen die binnen de eigen organisatie opgelost moeten worden (en soms bij of in samenwerking met een ICT-dienstverlener welke mogelijke een andere partij is dan de SOC-dienstverlener). Hier is een coördinerende functie nodig vanuit de organisatie zelf.

4.5.3 Service Categorieën en Competenties

Binnen een SOC kunnen verschillende competenties worden ondergebracht. De verschillende competenties kunnen worden geclusterd in een aantal categorieën. Het model dat binnen dit document wordt gehanteerd, verdeelt de verschillende competenties, zoals hieronder weergegeven in *Figuur 3: Type* SOC-Diensten.

Security operations maakt gebruik van veel platformen en gespecialiseerde tooling. Het inrichten en beheren van de ondersteunende tooling is een tijdrovende taak die ten koste gaat van de kerntaken. Om te voorkomen dat het technische beheer van platformen en applicaties door de securityspecialisten wordt gedaan kan een organisatie overwegen een engineer competentie toe te voegen aan het SOC.

Figuur 3: Type SOC-Diensten[8]

Binnen bovenstaand dienstverleningsmodel worden verschillende competenties per dienst ondergebracht. Voor de verschillende competenties kan uit de BIO worden afgeleid bij welk BBN ze van toepassing worden. Dit is opgenomen in *Tabel 3: BIO-referenties* en kan helpen bij het bepalen van prioriteiten.

BIO	BBN	BIO Eis	Competentie
6.2.1.1	2**	Toegangsbeveiligingsmechanismen op mobiele apparaten	Detectie (use case)
6.2.1.2	2**	Patchmanagement mobiele apparaten	Detectie (use case)
8.1.1	1	Inventarisatie bedrijfsmiddelen	Asset Management
8.2.1	1	Classificatie van informatie	Asset Management
9.1	1**	Toegang tot netwerken voor (on)geauthentiseerde componenten.	Security Log Management (use case)
9.2	1*/**	Beheer op toegangsrechten	Security Log Management (use case)
9.4	1**	Beperking toegang informatie en inlogprocedure	TBD
9.4.3	1**	Centrale policy voor wachtwoorden	Detectie (use case)
9.4.4.2	2	Logging gebruik systeemhulpmiddelen	Security Log Management

[8] Een veel gebruikt model is het NIST CSF (Cybersecurity Framework | CSRC (nist.gov)). Een goede mapping, vooral betreft Attack Services, is beperkt mogelijk omdat het NIST CSF een aantal operationele taken niet direct aanraakt. De verdere NIST CSF context is eerder in dit document toegelicht.

BIO	BBN	BIO Eis	Competentie
12.2	1**	Malware bescherming	Detectie
12.4.1	1	Gebeurtenisregistratie	Security Log Management
12.4.1.3	2	Monitoring door SIEM en/of SOC	Detectie
12.4.1.4	2	Centrale melding incidenten	Incident Response
12.4.1.5	2	Interne incidentregistratie en -melding	Security Monitoring
12.4.2.1/ 2	1	Vastlegging van gegenereerde logbestanden met bewaartermijn	Security Log Management
12.4.2.3	2	Wijzigingen op logbestanden	Detectie (use case)
12.4.3	1	Vastlegging activiteiten beheerders en operators	Security Log Management
12.5.1	1**	Software-installatie op operationele systemen**	Security Log Management
12.6	1	Beheer van technische kwetsbaarheden	Kwetsbaarhedenbeheer
13.1.2.1	2	Detectie op inkomend en uitgaand dataverkeer	Detectie
13.1.2.4	1	Detectie op koppelvlakken met externe of niet vertrouwde zones	Detectie
13.2.3.1	1**	Phishing en afluisteren	Detectie (use case)
14.2.8	1	Testen van systeembeveiliging	Penetratie testen
16.1	1	Beheer van informatiebeveiligingsincidenten	Incident response

Tabel 3: BIO-referenties

* Onderdelen in deze BIO sectie hebben BBN2 maar dit zijn voornamelijk procedurele zaken.
** Geen monitoring op gedefinieerd

Op basis van “Tabel 3: BIO-referenties” is in “Tabel 6: SOC Competentie fasering" per dienst competentie een mapping gemaakt naar de SOC-fasering fase.Tabel 6: SOC Competentie fasering

Naast de competenties die in de BIO al worden aangestipt, zijn een aantal gangbare additionele SOC-competenties in de tabel opgenomen.

Dienst	Competentie	BBN
Attack Services	Kwetsbaarhedenbeheer	1
	Threat Intelligence	NVT
	Penetratie Testen & Red-teaming	1/NVT
Detection Services	Security Log Management	1
	Detectie	1/2
	Security Monitoring	1
	Threat Hunting	NVT
Response Services	Incident Response	1
	Forensics	NVT

Tabel 4: SOC-Competenties mapping

Een verdere beschrijving en uitwerking van de verschillende competenties wordt in de volgende paragraaf gegeven.

4.5.4 Competenties

In deze paragraaf worden de verschillende competenties, zoals in dit document gebruikt, op hoofdlijnen beschreven. Dit is van belang om goed te kunnen begrijpen hoe de verschillende competenties, en later detectie en security monitoring, zijn opgebouwd om tot een volledig model te komen. Elke organisatie dient voor zichzelf te bepalen of deze omschrijvingen bruikbaar zijn voor het realiseren van haar doelstellingen. Daarnaast is het voor elke individuele organisatie van belang om goed te kijken naar de relevantie van de verschillende competenties binnen de organisatie. Verschillende competenties kunnen veelal ook bij gespecialiseerde partijen worden ingekocht. Dit is soms een goed alternatief als het opbouwen van de competentie binnen de organisatie te kostbaar is.

KWETSBAARHEDENBEHEER	
BESCHRIJVING	Binnen kwetsbaarhedenbeheer vallen alle werkzaamheden bedoeld om technische kwetsbaarheden in de IT-omgeving van de organisatie te onderkennen en mitigeren. Kwetsbaarhedenbeheer kan verder worden doorontwikkeld naar Attack Surface Management waarbinnen het aanvalsoppervlak van de organisatie verder in kaart wordt gebracht. Deze informatie kan verder worden gebruikt om security monitoring risico gestuurd in te richten.
TAKEN	• Scannen van de IT-omgeving op Netwerk- en Applicatie-kwetsbaarheden • Het verzamelen van de uitkomst van scans • Het rapporteren over de gevonden kwetsbaarheden naar systeem en applicatie eigenaren • Opzetten en beheren van een responsible disclosure proces
VERANTWOORDELIJKHEDEN	WEL • Verzamelen, aggregeren en distribueren van informatie betreft technische kwetsbaarheden binnen het IT-landschap NIET • Oplossen van de kwetsbaarheden. Dit ligt primair bij de eigenaar van het IT-component en/of eigenaar van de keten waar het component onderdeel van uitmaakt • Rapporteren over de oplosstatus en beheren van bijbehorend risico. Dit is primair een risicobeheersingsactiviteit
BEVOEGDHEDEN	• Non-intrusive scannen van IT-componenten • Intrusive scannen van IT-componenten • Beheren van gevoelige informatie betreft kwetsbaarheden in IT-componenten

THREAT INTELLIGENCE	
BESCHRIJVING	De Threat Intelligence-competentie is voornamelijk gericht op het plannen, verzamelen, verwerken, analyseren en verspreiden van dreigingsinformatie die specifiek van toepassing is op de informatiesystemen en applicaties binnen de organisatie. Dit kan, afhankelijk van de doelstellingen van de organisatie, resulteren in dreigingsinformatie op zowel strategisch, tactisch als operationeel niveau.
TAKEN	• Verzamelen, aggregeren, prioriteren en distribueren van dreigingsinformatie • Opstellen en onderhouden van dreigingsscenario's • Beschikbaar stellen van Indicator of Compromise (IoC)-informatie in gestandaardiseerd formaat voor consumptie in preventie- en detectiesystemen
VERANTWOORDELIJKHEDEN	WEL • Verschillende belanghebbenden binnen de organisatie tijdig en correct informeren over dreigingen • Bijdragen aan security- en detectiestrategie op basis van dreigingsbeelden • Voedend optreden om aanvalssimulaties gericht te doen en detectie te verbeteren • Registreren van security incidenten bij grote/belangrijke dreigingen NIET • Mitigeren en/of coördineren van het mitigeren van dreigingen
BEVOEGDHEDEN	• Heeft toegang tot dreigingsinformatie • Heeft toegang tot security log informatie, aanvalsoppervlak informatie en kwetsbaarheden informatie voor zover nodig voor het vormen van een goed dreigingsbeeld

PENETRATIE TESTING & RED-TEAMING	
BESCHRIJVING	Deze competentie is tweeledig waarbij veelal ongeveer dezelfde profielen nodig zijn. Penetratie Testing: Deze competentie houdt zich voornamelijk bezig met het evalueren van software, het vinden van kwetsbaarheden en het definiëren van bijbehorende risico's. Dit kan via DevSecOps[9] volledig in de SDLC[10] worden geïntegreerd. Red-Teaming: Het scenario gedreven testen van de defensie en detectielinies van de organisatie.
TAKEN	• Evalueren van software en vaststellen van lekken en misconfiguraties

[9] What is DevSecOps? | IBM
[10] Software/Systems Development Life Cycle: Systems development life cycle - Wikipedia

PENETRATIE TESTING & RED-TEAMING	
	• Testen van het totaal aan securitymaatregelen en detectie • Vaststellen en rapporteren over bevindingen
VERANTWOORDELIJKHEDEN	WEL • Constateren van technische risico's. • Rapporteren over technische risico' NIET • Opvolgen van de gevonden risico's: Dit is beter belegd bij een risicomanagement team • Oplossen van de gevonden risico's: Dit is de verantwoordelijkheid van de systeemeigenaar
BEVOEGDHEDEN	• Bevoegdheden zijn per pentest of red-team activiteit opnieuw vast te stellen, afhankelijk van de scope

SECURITY LOG MANAGEMENT	
BESCHRIJVING	Binnen een IT-organisatie kan onderscheid worden gemaakt tussen Log Management en Security Log Management. Hierbij is Log Management breder dan Security Log Management en is gericht op het verzamelen van alle loggegevens die van belang zijn voor de organisatie. Dit kan bijvoorbeeld betrekking hebben op het monitoren en optimaliseren van Supply Chain-processen. Met Security Log Management wordt het verzamelen van alle loggegevens die van belang zijn in het kader van security monitoring en Detectie bedoeld. Dit is dus een specifiek aandachtsgebied binnen log management en is qua scope beperkter dan log management in de bredere zin.
TAKEN	• Aansluiten van logbronnen op een centraal securitylogmanagementsysteem • Zorg dragen voor goede verwerking van de data • Implementeren van eenvoudige detectie en rapportages op aangeven van een systeemeigenaar of andere belanghebbenden
VERANTWOORDELIJKHEDEN	WEL • Koppelen en beheren van data • Ontwikkelen en beheren van functionele content • Aanleveren van detectie-alarmeringen en rapportages bij de juiste eigenaar NIET • Aanleveren van data: Dit ligt bij de eigenaar en dient afgedwongen te worden via security policies
BEVOEGDHEDEN	• Verzamelen en inzien van alle logdata binnen de organisatie rekening houdend met doelbinding

DETECTIE	
BESCHRIJVING	Detectie gaat voornamelijk over de technische mogelijkheden om aanvallen te detecteren. Hierbij hoort ook het technisch en functioneel beheer van de verschillende detectiecomponenten en de geïmplementeerde Use Cases (detectieregels)
TAKEN	• Installeren, configureren en beheren van detectietechnologie
VERANTWOORDELIJKHEDEN	WEL • Functionele kwaliteit van detectie • Use case-bouw • Use case-beheer NIET • Opvolging van alarmen uit de detectiesystemen
BEVOEGDHEDEN	• Toegang tot alle detectiemiddelen voor kwaliteitsbeheersing • De juiste toegang tot data op basis van doelbinding bepaling

SECURITY MONITORING	
BESCHRIJVING	Dit onderdeel betreft *eyes on screen* en opvolging van de alerts die uit de detectiecomponenten komen. In veel gevallen wordt security monitoring opgedeeld in twee of drie niveaus van expertise die doorwerkt in de rolbeschrijvingen: • Niveau 1: Initiële alarmopvolging en eerste triage waarbij vaak niet meer dan 15 tot 30 minuten per alert wordt gebruikt, om te bepalen of het een vals alarm of potentieel incident is • Niveau 2: Hier worden de alarmen opgevangen die als potentieel incident door niveau 1 zijn aangemerkt en verder onderzoek vereisen, om dit met zekerheid vast te stellen en om de eerste omvang en diepte vast te stellen • Niveau 3: Dit zijn veelal security-analisten met specialisaties op bepaalde onderwerpen analyse
TAKEN	• Reageren en onderzoeken van security-alarmen die uit de detectiesystemen komen • Potentiële incidenten communiceren naar Incident Response
VERANTWOORDELIJKHEDEN	WEL • Alarm triage • Alarm onderzoek • Rapportage over alarmonderzoek (kwantiteit en kwaliteit) • Potentiële security incidenten naar de juiste persoon of afdeling (Incident Response-team of systeem-eigenaar) doorzetten voor verder onderzoek NIET • Najagen van potentiële incidenten bij de eigenaar • Opvolgen van incidenten samen met, en op aangeven van, Incident Response-team
BEVOEGDHEDEN	• Heeft toegang tot alle logdata om onderzoek naar alarmen te kunnen doen

THREAT HUNTING	
BESCHRIJVING	Binnen het Threat Hunting-team wordt de verzamelde log data actief gebruikt om actief aanvallen op te sporen die door de automatische detectie niet zijn ontdekt
TAKEN	• Proactieve data-analyse om niet-gedetecteerde security breaches te vinden • Registreren van potentiële incidenten
VERANTWOORDELIJKHEDEN	WEL • Constateren van potentiële, niet eerder gevonden, security breaches • Vastleggen en communiceren van deze breaches • Geven van aanbevelingen om automatische detectie te verbeteren op basis van hunting activiteiten NIET • Opvolging van gevonden breaches
BEVOEGDHEDEN	• Heeft toegang tot relevante logdata om onderzoek naar alarmen te kunnen doen

INCIDENT RESPONSE	
BESCHRIJVING	Het Incident Response-team is verantwoordelijk voor het opvangen van de vastgestelde security-incidenten die uit het monitoringteam zijn gekomen. Dit team is verantwoordelijk voor de opvolging van incidenten tot het moment dat ze volledig zijn opgelost
TAKEN	• Opvolgen van potentiële security-incidenten • Bieden van handelingsperspectief voor applicatie- en systeemeigenaren bij incidenten • Bijdragen leveren aan het beheersen van crisissituaties betreft security-incidenten • Rapporteren over incidenten en inbraken naar management • Rapporteren naar detectie en security monitoring teams over de uitkomsten van onderzoeken om de kwaliteit van detectie te verbeteren
VERANTWOORDELIJKHEDEN	WEL • Onderzoeken van security aanvallen en -incidenten • Eindverantwoordelijk voor het uitlopen van security incidenten • Zoveel mogelijk schade beperkend handelen bij incidenten • Kennisdeling en communicatie naar interne en externe partijen over security-incidenten NIET • Detecteren of verbeteren van detectie
BEVOEGDHEDEN	• Heeft toegang tot systemen van systeemeigenaren om onderzoek te kunnen verrichten • Heeft toegang tot alle security log data om breed onderzoek te kunnen doen

INCIDENT RESPONSE	
	• Blokkeren van gebruikersaccounts of communicatiekanalen • In quarantaine brengen van systemen om te kunnen isoleren, verdere schade te voorkomen en om onderzoek te kunnen verrichten • Heeft stekkermandaat • Rapporteert direct aan de CISO of dienstdoende crisismanager

FORENSICS	
BESCHRIJVING	Forensisch onderzoek is een afzonderlijke specialisatie die wordt ingezet bij specifieke incidenten waarbij diepgaand technisch onderzoek is vereist, op gecompromitteerde systemen en waarbij, eventueel juridisch houdbare, bewijs verzamelen en vastleggen extreem belangrijk is
TAKEN	• Verrichten van diepgaand forensisch onderzoek bij incidenten
VERANTWOORDELIJKHEDEN	<u>WEL</u> • Verrichten van forensisch onderzoek • Vastleggen van bewijslast op een juridisch houdbare wijze • Rapporteren over bevindingen <u>NIET</u> • Constateren van incidenten en bepalen of/wanneer forensische expertise wordt ingezet
BEVOEGDHEDEN	• Heeft voor onderzoeksdoeleinden speciale toegang tot alle systemen, met goedkeuring van de eigenaar of verantwoordelijke anderszins

In Tabel 5: RACI-Verantwoordelijkhedenoverzicht is een overzicht opgenomen van een aantal belangrijke verantwoordelijkheden die door en voor het SOC dienen te zijn geregeld zodat het SOC goed zijn werk kan verrichten. Dit overzicht is indicatief en kan worden gebruikt als startpunt of leidraad voor het opstellen van een RACI[11] voor de eigen organisatie.

Rollen	Systeem/Applicatie Eigenaar	CIO	CISO	SOC Manager	Kwetsbaarhedenbeheer	Threat Intelligence	Penetratie Testen & Red teaming	Security Log Management	Detectie	Security Monitoring	Threat Hunting	Incident Response	Forensics
Toegang verlenen (tot systemen en data)	A,R	A	I	C	C	C	C	C	C	C	C	C	C
Logdata Aanleveren	A,R	I	I	I		R		C	C				
Kwetsbaarheden onderkennen en rapporteren	R,I	I	A	R	R	R	R		I			I	C
Kwetsbaarheden oplossen	R	A	C	C	C	I	I		I	I		C	
Security incidenten rapporteren	R	I	A	R	R	R	R	R	R	R	R	C	
Security incidenten oplossen	R	A	C	R,C	I			C	C	C		R	C
Stekkermandaat	R,C	A	C	R,C				I	I	I		R	

Tabel 5: RACI-Verantwoordelijkhedenoverzicht

[11] RACI-model - Wikipedia

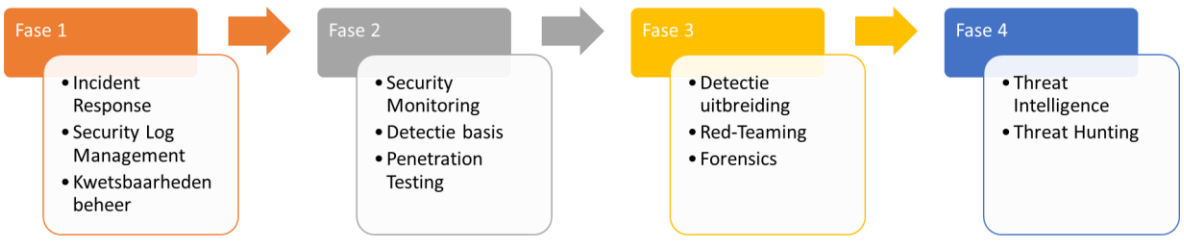
4.5.5 Roadmap

Zoals aangegeven in paragraaf 4.5.1, wordt in dit document de BIO gebruikt voor het bepalen van volgordelijkheid voor de roadmap. Het gebruik van de BIO is de keus die voor dit document is gemaakt voor strategiebepaling maar is zeker niet als voorschrijvend bedoeld voor het uiteenzetten van een strategie van de eigen organisatie. In 4.5.3 zijn bij de verschillende competenties de BIO BBN classificaties toegevoegd. In Tabel 6: SOC Competentie wordt hiermee een verdere fasering uitgewerkt.

Dienst	Competentie	BIO Thema	SOC Fase
Attack Services	Kwetsbaarhedenbeheer	Ja	1
	Threat Intelligence	Nee	4
	Penetratie Testen & Red-teaming	Ja/NVT	2/3
Detection Services	Security Log Management	Ja	1
	Detectie	Ja	2/3
	Security Monitoring	Ja	2
	Threat Hunting	Nee	4
Response Services	Incident Response	Ja	1
	Forensics	Nee	3

Tabel 6: SOC Competentie fasering

De onderdelen die overeenkomen met BBN 1 zijn veelal in fase 1 en 2 geplaatst maar mogelijk is de hier gemaakte keuze in volgordelijkheid voor de eigen organisatie onwenselijk en dient deze dus aangepast te worden. Asset Management komt niet direct terug in onderstaande tabel omdat dit eerder een rand voorwaardelijke functie binnen de organisatie dan een SOC-functie. Op basis van 1) BIO–BBN-definities en 2) een goed groeimodel voor een SOC, is bij de SOC-Competenties aangegeven wat een goede gefaseerde aanpak zou kunnen zijn voor implementatie. Een volgordelijk implementatieplan is verder uitgewerkt in Figuur 4: Gefaseerde aanpak.



Figuur 4: Gefaseerde aanpak

In de fasering is een opsplitsing gemaakt tussen *"Detectie basis"* en *"Detectie uitbreiding"*. Onder *"Detectie basis"* worden de detectie-componenten zoals voorgeschreven in de BIO voor BNN1 bedoeld. Dit betreft onder andere malwaredetectie en het monitoren van activiteiten van beheerders, maar ook security monitoring van netwerkkoppelingen naar nietertrouwde zones. Malwaredetectie kan worden gedaan met Antivirussoftware of Endpoint-Detectie en Response (EDR)-oplossingen.

Het monitoren van activiteiten van beheerders kan in de basis worden gedaan met behulp van Security Log Management-tools en -rapportages waarbij niet direct uitgebreidere detectie tooling

(zoals SIEM-software) nodig is. Onder *"Detectie uitbreiding"* wordt alle additionele security monitoring bedoeld. Dit is in eerste instantie een uitbreiding op de detectie zoals voorgeschreven vanuit de BIO met BBN2 (bijvoorbeeld het monitoren van inkomend en uitgaand netwerkverkeer) en in tweede instantie uitgebreidere security monitoring op andere datastromen op basis van organisatie specifieke behoefte (bijvoorbeeld ingegeven door een risicoanalyse).

4.5.6 Sourcing Strategie

Afhankelijke van de omvang van de organisatie, kan het verstandig zijn om diensten extern te beleggen in plaats van dit zelf op te bouwen. Voor het uitwerken van het beste model voor de eigen organisatie zijn er een aantal modellen om in overweging te nemen:

1. Self-sourcing: Volledig zelf opbouwen van de competentie waarbij de organisatie zelf mensen gaat aantrekken met de juiste vaardigheden.

2. In-sourcing: Opbouwen van een competentie binnen de organisatie waarbij de teams, teamaansturing en bemensing door een externe partij wordt gedaan. Hierbij blijft de strategische en tactische aansturing bij het eigen CISO-team.

3. Co-sourcing: Dit is een combinatiemodel van self- en in-sourcing met een deel eigen mensen en een deel uitbesteed aan een externe partij.

4. Outsourcing: Het outsourcingmodel is minder op mensen en teams gericht, maar meer op diensten. Bij dit model wordt een diensten afgenomen bij een leverancier, en wordt alleen de output van een dienst opgevangen binnen de eigen organisatie.
   Outsourcing kan op verschillende wijzen worden gedaan, bijvoorbeeld door een onshore, offshore of nearshore model. De verschillende modellen hebben allemaal voor- en nadelen en soms zelfs verschillende mogelijkheden en onmogelijkheden.

Bij het intern opbouwen van verschillende competenties is het in eerste instantie van belang om goed te kijken naar wat wel en wat niet te willen doen en in welke volgorde.
Tabel 7: Competentie–Sourcing kan handvatten bieden bij het uitwerken van de eigen strategie. Dit is een uitgangspunt voor een gemiddelde organisatie. Bekijk op basis van de behoefte van de eigen organisatie en de te beschermen belangen wat werkelijk nodig is.

Competentie	< 200	- 500	- 1.000	- 2.500	- 5.000	- 10.000	> 10.000
Kwetsbaarhedenbeheer	2	2	2	3	3	4	4
Threat Intelligence	1	1	1	2	2	2	3
Penetration Testing & Red-teaming	2	2	2	3	3	4	4
Security Log Management	2	2	2	3	3	4	4
Detectie	2	2	2	3	3	4	4
Security Monitoring	2	2	2/3	3	3	4	5
Threat Hunting	1	1	1	1	1	4	4
Incident Response	4	4	5	5	5	5	5
Forensics	1	2	2	2	2	2	3

Tabel 7: Competentie–Sourcing op basis van de het aantal medewerkers in een organisatie

1: Niet doen
2: Uitbesteden
3: Overweeg dit zelf te doen, maar uitbesteden is een goed alternatief.
4: Binnen de organisatie inrichten op basis van een 5x8 service window.

5: Binnen de organisatie inrichten op basis van een 24x7 service window via piket dienst.

De omvang van het SOC en Incident Response team hangt af van de servicetijden en de omvang van de organisatie. Een indicatie van omvang is hieronder opgenomen in *Tabel 8: Team* omvang. Bij het opstellen van de tabel zijn een aantal uitgangspunten genomen:

1) Elke organisatie heeft altijd een eigen Incident Response-team nodig (waarbij de naam niet van heel groot belang is, maar vaak is dit een variatie op een Computer Emergency Response Team of CERT). Als hierbij wordt besloten om op 24x7 service window over te gaan (bijvoorbeeld via piketdienst) dan is het verstandig om het team hierop mee te schalen zodat deze taak niet bij één persoon is belegd;

2) De omvang van het SOC-team gaat uit van *Tabel 7: Competentie*–Sourcing waarbij voor organisaties tot 500 medewerkers het de aanbeveling verdient om te outsourcen en waarbij tot 1000 FTE de omvang van het SOC alleen van toepassing is als de dienst niet wordt ingekocht en;

3) Om een 24x7-team in te richten is doorgaans een minimum van 8 à 10 FTE nodig. De werkelijke omvang dient vooraf goed te worden bekeken en kan sterk afhangen van CAO's en mogelijke kosten die een 24x7 operatie met zich meebrengt.

Team	< 200	- 500	- 1.000	- 2.500	- 5.000	- 10.000	> 10.000
SOC-team omvang	0	0	2	4	8	10	10+
Incident Response team omvang	1	1	2	2	3	3	4+

Tabel 8: Team omvang op basis van het aantal medewerkers in een organisatie

Binnen de verschillende teams worden de verschillende competenties ondergebracht door kennis eisen en wensen te stellen binnen de rollen en profielen voor het team.

4.5.7 Technologie

Voor het inrichten van de verschillende competenties is technologie nodig. Dit betreft zowel software, hardware als ook mensen. Het is verstandig om inrichting, onderhoud en wijzigingen op technische componenten bij technische en systeem/applicatiebeheerspecialisten neer te leggen zodat deze taken niet bij het SOC-analisten komen te liggen. Een valkuil is dat de Security-specialisten binnen het SOC-team een dagtaak kunnen hebben aan het onderhouden van alle tooling, een taak waar veelal helemaal geen specifieke security-kennis voor nodig is.

Ter ondersteuning van verschillende competenties in een SOC is een grote verscheidenheid aan technische componenten nodig. Hiervan is in "
Tabel 9: Technische ondersteuning voor *SOC*" een niet uitputtend overzicht weergegeven. In het licht van de eerdere paragraaf (4.5.6) over sourcing, is het goed om rekening te houden met deze diversiteit aan techniek en bijbehorende ondersteuning. Bij alle vormen van sourcing heeft de organisatie in ieder geval met een kostenaspect te maken, maar afhankelijk van de keuze is deze inrichting en ondersteuning dus intern of extern (of een combinatie hiervan) belegd. Een verdere overweging kan zijn om het SOC op te bouwen met voornamelijk SaaS-tools. Dit brengt beperkingen betreft flexibiliteit met zich mee, maar daarvoor krijg je terug dat het technisch (niet security) beheer van de applicatie niet intern ondersteund hoeft te worden. Houd hierbij wel rekening met het juridisch en dataprivacy aspect van SaaS-oplossingen.

Dienst	Competentie	Applicatie
Attack Services	Kwetsbaarhedenbeheer	Kwetsbaarheden-scan en -beheer tool en in een later stadium tooling ter ondersteuning van Attack Surface Management
	Threat Intelligence	Threat Intelligence Platform (TIP) en Indicator of Compromise (IOC) feeds
	Penetration Testing & Red-teaming	PT: Speciale PT-tools en een systeem om bevindingen/risico's vast te leggen (mogelijk een bestaande ISMS-tool) RT: Speciale RT software om missies uit te voeren
Detectie Services	Security Log Management	(Security) Log management tools en data-bus/management tools voor grotere organisaties waar grote hoeveelheden data naar SIEM systemen wordt gestuurd
	Detectie	Netwerk Detectie en Response (NDR) technologie, Endpoint/eXtented Detectie en Response (EDR/XDR) technologie, en Security information and event management (SIEM)- technologie. Afhankelijk van de organisatie mogelijk ook Cloud-SIEM oplossingen
	Security Monitoring	Security Orchestration, Automation and Response (SOAR) waarbij in veel gevallen, zeker in kleinere organisaties, SIEM tooling voldoende handvatten biedt voor onderzoek en opvolging
	Threat Hunting	Log Analytics-tooling (kan onderdeel uitmaken van SIEM en of Security Log Management (SLM) oplossingen) of gespecialiseerde Threat Hunting-tooling
Response Services	Incident Response	Ticketing-Systeem om alarmen en incidenten (en bijbehorend onderzoek) vast te leggen
	Forensics	Gespecialiseerde applicaties en hardware voor forensische onderzoek die o.a. de mogelijkheid biedt om een onderzoek forensisch correct vast te leggen Case managementsysteem om bewijsmateriaal te bewaren

Tabel 9: Technische ondersteuning voor SOC

4.5.8 Sturingsinformatie & Rapportage

Voor de verschillende onderdelen binnen een SOC dienen vooraf stuurmechanismen vastgesteld te worden. Deze sturingsmechanismen vallen uiteen in:

- Key Performance Indicators (KPI): Hoe effectief en efficiënt zijn de verschillende SOC-componenten.
- Key Risk Indicators (KRI): Wat is het risicoprofiel voor de organisatie.

Hierbij is het belangrijk om altijd te kiezen voor KPI's die goed zijn te meten en waarmee kan worden gestuurd. Om indicatoren te laten helpen bij het sturen van het SOC zijn een aantal zaken van belang:

- Breng de verschillende metrics samen in een Dashboard zodat in één oogopslag helder is of doelstellingen worden/zijn gehaald.
- Begin met een beperkte set die verder kan worden uitgebouwd naar gelang de volwassenheid en omvang van het SOC toeneemt.
- Meet op kwaliteit en minder op kwantiteit. Het is bijvoorbeeld verstandig om te kijken naar de alarm vs. false positive ratio om de efficiëntie van detectie te meten, maar minder interessant om te weten hoeveel alarmen er per analist worden afgehandeld in een korte tijd. Wel kan het interessant zijn om het gemiddeld aantal alarmen bij te houden om te zien wat de trend is en of het team voldoende groot is alles af te handelen.
- Meet de verschillende onderdelen binnen SOC-processen zodat sturen mogelijk wordt.
- Stel alleen metrics vast waarvoor het eenvoudig is om bruikbare data te verkrijgen zodat de het samenstellen van een Dashboard ook haalbaar is.

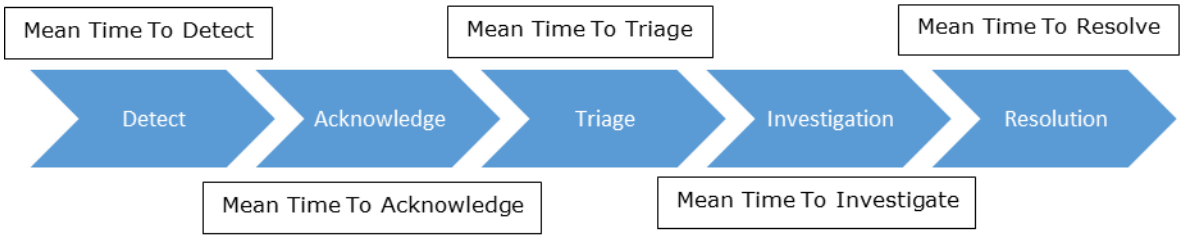
Voor verschillende onderdelen zijn in "
Tabel 10: KPI en " een aantal voorbeeld KPI's beschreven. Dit is geen uitputtende lijst en per organisatie zal de behoefte anders zijn. Welke KPI's met welke frequentie en voor wie te rapporteren zal ook per organisatie verschillen. Het is verstandig om de rapportage behoefte samen met de verschillende stakeholders vast te leggen.

Competentie	Type	Metric	Doel
Incident Response	KRI	Aantal kritisch en hoog risico incidenten	Weergeven van het bestaansbelang van Incident Response
	KPI	Afhandeltijd van de kritische en hoog risico incidenten	Meten van de efficiëntie van het Incident Response team
	KPI	Percentage relevante incidenten dat tijdig is gemeld bij het NCSC	Meten van compliance met wet- en regelgeving
	KPI	Mean Time To Resolve*	Meten van de doorlooptijd van het oplossen van incidenten
Kwetsbaar-hedenbeheer	KRI	Aantal nieuwe kritische en hoog risico kwetsbaarheden	Meten van de verandering in het risicoprofiel
	KRI	Aantal kwetsbaarheden op systemen met Internet exposure	Vaststellen van het risicoprofiel met betrekking tot het aanvalsoppervlak van de organisatie
	KPI	Verandering van het aantal kritische en hoog risico kwetsbaarheden	Meten van de voortgang van het oplossen van risico's

Competentie	Type	Metric	Doel
	KPI	Percentage kritische en hoog risico kwetsbaarheden dat volgens de policy tijdig/niet tijdig is verholpen	Meten van organisatie compliance met de eigen policy
Security Monitoring	KPI	Mean Time To Detect*	Detectie tot alarm
	KPI	Mean Time To Acknowledge*	Alarm tot start eerste triage
	KPI	Mean Time To Triage*	Start tot afronding eerste triage
	KPI	Mean Time To Investigate*	Tijd tussen afronding triage en afronding SOC-onderzoek (en overdracht Incident Response)
Detectie	KRI	Aantal alarmen per risico gebied (zoals: phishing, credential access, data leakage, etc.)	Weergeven van trendwijzigingen en het vaststellen van mogelijke aandachtsgebieden voor awareness campagnes
	KPI	Aantal alarmen over de afgelopen periode	Meten van de werkdruk op het SOC-personeel
	KPI	Percentage false positive alarmen	Meten van de kwaliteit van de huidige detectie

Tabel 10: KPI en KRI-voorbeelden

* Het detectie, security monitoring en responseproces valt in een aantal onderdelen uiteen waarbij op verschillende momenten gemeten kan worden.



Eerder is aangegeven dat het in mindere mate interessant is om te weten hoeveel alarmen per analist worden afgehandeld. Het meten van Acknowledgement en Triage tijden is nog zo'n metric die niet altijd interessant is, maar wel interessant kan zijn. Deze metrics zijn vooral van belang als hierover afspraken zijn gemaakt met leveranciers van securitymonitoringdiensten. Het maken van afspraken hierover kan wel een negatief gevolg hebben op de kwaliteit van de afhandeling. Onder tijdsdruk is de kans groter dan men shortcuts gaat nemen. Om kwaliteit te borgen is het van belang om strikte (en realistische) afspraken te maken over de triage draaiboeken en informatie die dient te worden geregistreerd in tickets.

Bijlage I – Checklist

Paragraaf	Onderwerp	Status	Opmerkingen
4.1	Vaststellen van SOC-drivers		
4.2	Vaststellen van de SOC-Visie		
	Vaststellen van de SOC-Missie		
4.3	Vaststellen SOC-stakeholders		
4.4	Bepalen SOC doelstellingen & Strategie		
4.4.3	Implementeren Incident Response team		
4.5	Opstellen Target Operating Model (TOM)		
4.5.2	Positionering SOC binnen organisatie		
	Vaststellen stekkermandaat		
	Implementeren stekkermandaat proces		
	Vaststellen SOC-mandaat		
	Vaststellen regietaken eigen organisatie *(Van toepassing bij uitbesteden)*		
4.5.3, 4.5.4	Vaststellen relevante competenties		
4.5.5	Opstellen roadmap		
4.5.6	Bepaal de relevante competenties		
4.5.6	Bepaal per relevante competentie de sourcing strategie (in- of out-sourcing)		
4.5.7	Bepaal per relevante competentie waar de beheer & ondersteuningstaken worden belegd voor technische componenten *(Ook van toepassing bij uitbesteden)*		
4.5.8	Vaststellen stuurmechanismen		

Bijlage II – Bron informatie

- Besluit CIO-stelsel Rijk: wetten.nl - Regeling - Besluit CIO-stelsel Rijksdienst 2021 - BWBR0044613 (overheid.nl)
- KPI: Kritieke prestatie-indicator - Wikipedia
- NIST Cyber Security Framework: Cybersecurity Framework | CSRC (nist.gov)
- RACI-Model: RACI-model - Wikipedia

Bijlage III – Definities

Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is in deze bijlage een verzameling van definities opgesteld. Voor alle overige termen en begrippen verwijst dit document naar het online Woordenboek - Cyberveilig Nederland.

Detectie

- Detectie is het (continu) zoeken naar specifieke patronen of afwijkende gedragingen die kunnen leiden tot (beveiligings-) incidenten. Detectie gebeurt mede op basis van door logging verzamelde informatie (logs). Detectie is daarmee een belangrijk onderdeel van (Security) Monitoring.

  Doel: Rapporteren van mogelijke (beveiligings-) incidenten.

Logging

- Logging is het verzamelen en opslaan van informatie over gebeurtenissen die plaatsvinden op een systeem, applicatie of netwerk.

  Doel: Logging maakt het mogelijk inzicht te krijgen in systeem- of netwerkactiviteit, problemen op te lossen, beveiligingsincidenten te onderzoeken, of achteraf te kunnen reconstrueren wat er bij een incident gebeurde. Verder is logging vaak een vereiste vanuit compliance.

Monitoring

- Monitoring is het continu bewaken van gebeurtenissen en veranderingen die mogelijk tot een incident kunnen leiden.

  Doel: Borgen van beschikbaarheid (continuïteit), prestaties en veiligheid van informatie en systemen door potentiële incidenten (proactief) te identificeren en daar, indien nodig, op te reageren.

Security Monitoring

- Security Monitoring is het continu controleren en analyseren van potentiële beveiligingsincidenten, welke door de detectie-activiteit zijn opgemerkt.

  Doel: Borgen van beschikbaarheid (continuïteit), integriteit (betrouwbaarheid) en vertrouwelijkheid (exclusiviteit) van informatie en systemen door potentiële beveiligingsincidenten (proactief) te identificeren en daar, indien nodig, op te reageren.

Target Operating Model (TOM)

- Het Target Operating Model (TOM) beschrijft hoe een organisatie haar mensen, informatie, processen en technologie inzet om het SOC daadwerkelijk te realiseren.

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://www.ncsc.nl/vssr

info@ncsc.nl

vssr.info@minjenv.nl (Rijksoverheid)

December 2023