TLP:GREEN

OR-1 NETWERKPLAN HANDLEIDING

Monitoring & Detectie – SOC Operational Readiness - Netwerkmanagement

Best Practice versie 1.3

Complexiteit document

Eenvoudig

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.

De wereld van cyberdreigingen verandert snel en vraagt om gezamenlijke inspanning om weerbaar te zijn. Dit vraagt om samen te werken aan breder toegepaste én verbeterde SOC-dienstverlening. Het programma Versterken SOC Stelsel Rijk (VSSR) is opgezet om hieraan bij te dragen.

Een belangrijk onderdeel van SOC-diensten zijn de monitoring- en detectiediensten. Deze 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 een SOC effectief en doelmatig in te zetten is het noodzakelijk dat er een aantal onderwerpen binnen een organisatie zijn ingericht. VSSR levert diverse producten die rijksorganisaties ondersteunen bij het inrichten van een SOC en de daarvoor benodigde randvoorwaarden.

Achtergrond

VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set van miniproducten die rijksorganisaties helpt om een aantal SOC operationele randvoorwaarden in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor IT-architecten, IT-beheerders, Security vertegenwoordigers en functionarissen betrokken bij informatiebeveiliging.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	28-01-2025	Initiële versie
V1.1	05-02-2025	Aanpassingen document opmaak
V1.2	19-02-2025	Toevoeging document context
V1.3	6-7-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
Netwerkplan overzicht	Zie "OR-1, Netwerkplan Overzicht" onder SOC Operational Readiness - Producten
IP Nummerplan	Zie "OR-1, IP Nummerplan" onder SOC Operational Readiness - Producten
VSSR-kennisdocumenten	VSSR (ncsc.nl)

1.3 Definities

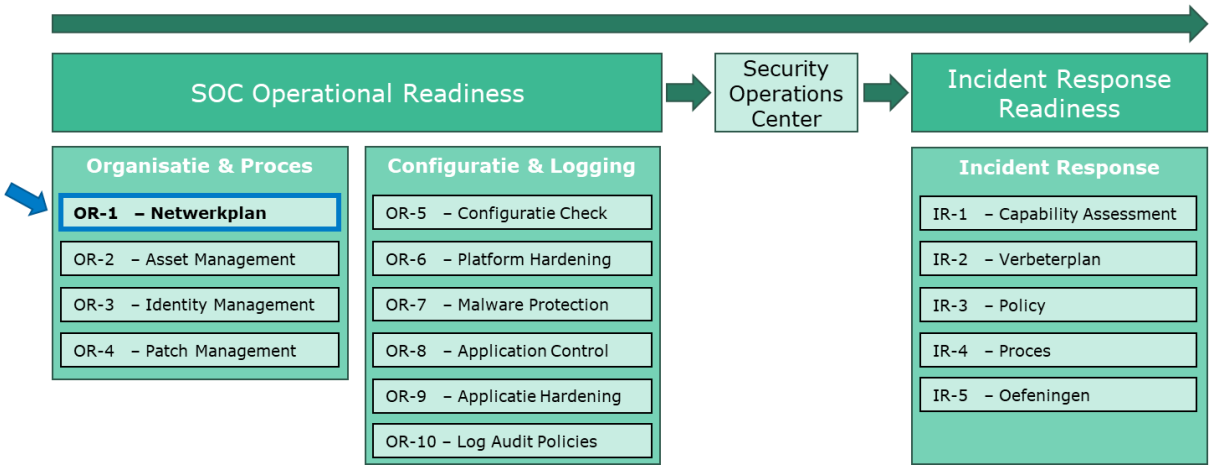
Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

2 Context miniproducten

Dit document maakt onderdeel uit van de SOC Readiness Assistance **miniproducten**. De SOC Readiness Assistance miniproducten ondersteunen uw organisatie bij de voorbereidingen die nodig zijn voor het optimaal benutten van een SOC(-dienst). Deze producten hebben een samenhangende opbouw maar kunnen ook los van elkaar worden gebruikt. De producten zijn in drie groepen te verdelen:

1) **Organisatie & Proces:** Helpt bij het inrichten van processen met als doel het SOC van de juiste informatie te voorzien om goed te kunnen monitoren.
2) **Configuratie & Logging:** Helpt bij het inrichten van basisbeveiliging met als doel om beter beschermd te zijn en de juiste logdata bij een SOC aan te kunnen leveren.
3) **Incident Response:** Met behulp van monitoring & Detectie zal een SOC security melding genereren. De Incident Response producten helpen bij het inrichten van de opvolging van deze meldingen binnen uw organisatie.

Onderstaande weergave toont dit document als onderdeel van **Organisatie & Proces** in het VSSR-Minipoducten raamwerk.



Figuur 1: Dit document als onderdeel van het VSSR-Miniproducten raamwerk

De twee productgroepen behorende bij *SOC Operational Readiness* bestaan telkens uit een vergelijkbare set document die in figuur 1 per groep zijn weergegeven. Niet elk product bestaat uit exact de zelfde componenten maar veelal wordt de zelfde structuur gebruikt waarbij dit document het **Netwerkplan** (OR-1), binnen **Organisatie & Proces**, behandelt.

3 Handleiding

Een goed gestructureerd netwerkplan is cruciaal voor de operationele effectiviteit van organisaties. Het netwerkplan behandelt belangrijke elementen zoals IT-infrastructuur, systemen en beveiligingsmaatregelen, zodat organisaties ervoor kunnen zorgen dat hun netwerken efficiënt in kaart worden gebracht en het inzichtelijk maakt voor een SOC. Door gebruik van de onderstaande bestanden is het mogelijk om een kort en bondig overzicht op hoog niveau te hebben voor SOC- en Incident Managementdoeleinden.

Het netwerkplan bestaat uit twee onderdelen: 1) "***Netwerkplan overzicht"***; en, 2) "***IP-nummerplan"***. Deze documenten dienen samen gebruikt te worden. Zorg dat eerst de visuele representatie van het netwerk wordt afgerond en laat hierbij de IP-details zoveel mogelijk achterwegen. Als de eerste stap is afgerond, ga dan in het ***"IP-nummerplan***" verder om de detailinformatie voor het netwerk in te vullen

3.1 Doel

Het doel van dit document is om een helder en gestructureerd netwerkplan in kaart te brengen, waarbij gebruik wordt gemaakt van de presentatie "***Netwerkplan overzicht.pptx***". Dit netwerkplan zal dienen als fundament voor het invullen van het document "***IP Nummerplan.xlsx***". Door deze aanpak te hanteren, kunnen we een samenhangend en effectief IP-nummerplan opstellen dat aansluit bij een kort en bondig inzicht in de kwetsbare segmenten en de manieren waarop deze kunnen worden beveiligd en gemonitord door een SOC.

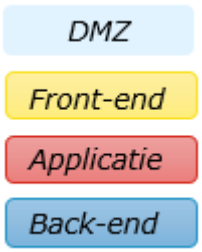
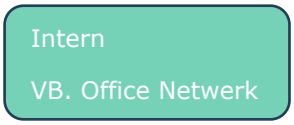
3.2 Gebruik van een netwerkplan

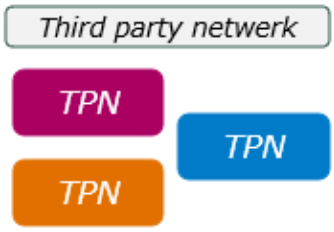
Het maken van een goed en compleet netwerkplan is essentieel voor het visualiseren van de structuur van je netwerk, het vergemakkelijken van de communicatie tussen belanghebbenden en het ondersteunen van de implementatie- en probleemoplossingsprocessen. Dit hulpmiddel bied je de bouwstenen en richtlijnen om duidelijke en effectieve netwerkdiagrammen te creëren.

Hieronder volgt eerst een overzicht van de componenten die worden gebruikt voor de opbouw van het netwerkdiagram. Daarna volgt een kort stappenplan aan de hand waarvan een kan worden opgebouwd.

3.2.1 Legenda: Netwerksegmenten en basiscomponenten

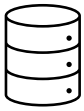
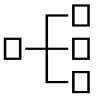
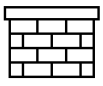
De hier weergegeven legenda bevat de verschillende elementen waarmee het visuele netwerkoverzicht in ***"Netwerkplan overzicht.pptx"*** kan worden opgebouwd en geeft bij de verschillende componenten een korte uitleg over de functie.

Zones	*Functie*	*Icoon*
DMZ	Host openbare diensten en fungeert als een buffer tussen het internet en het interne netwerk. Front-end, Applicatie, Back-end	
Intern Netwerk	Verbindt apparaten binnen een lokaal gebied, zoals een kantoor of een reeks van gebouwen. Voorbeelden: Kantoornetwerk en Datacenter netwerk.	

Zones	*Functie*	*Icoon*
LAN	Verbindt apparaten binnen een lokaal gebied, zoals een kantoor of gebouw.	
WAN (Wide Area Netwerk)	Verbindt meerdere LAN's over grote geografische gebieden.	
Cloud	Een virtueel netwerk dat verbindingen, gegevensoverdracht en communicatie binnen en tussen cloudomgevingen mogelijk maakt	
Extern (beheer) toegang (Virtual Private Network/Leased line)	Uitbreiding van een computernetwerk over een openbaar netwerk. De veilige verbinding valt te omschrijven als een tunnel en wordt afgekort VPN genoemd.	
Third party netwerk **(Haagse ring/Diginetwerk/ Justitienet)**	Netwerk van ketenpartners en derden die toegang bieden tot diensten of resources buiten de controle van de primaire organisatie.	

Tabel 1 Legenda

In de onderstaande tabel is een korte beschrijving gegeven van de verschillende componenten en de bijbehorende functies. In de laatste kolom is het bijbehorende pictogram weergegeven.

Component	*Functie*	*Icoon*
Server	Biedt middelen, gegevens, diensten of programma's aan andere apparaten (clients) via een netwerk.	
Werkstation	Eindgebruikersapparaten die worden gebruikt om toegang te krijgen tot netwerkbronnen.	
Werkstation (Remote gebruiker)	Eindgebruikersapparaten die worden gebruikt om via VPN-toegang te krijgen tot netwerkbronnen.	
Load balancer	Verdeelt netwerk- of applicatieverkeer over meerdere servers om ervoor te zorgen dat geen enkele server een bottleneck wordt.	
Firewall	Handhaaft beveiligingsbeleid door netwerkverkeer te monitoren en te controleren.	

Component	*Functie*	*Icoon*
Forward/Reverse Proxy server	Een forward proxy server stuurt clientverzoeken naar het internet, terwijl een reverse proxyserver internetverkeer naar back-end servers doorstuurt.	
Active Directory (AD)	Een directory service van Microsoft die wordt gebruikt voor het beheren van gebruikers, computers en andere netwerkbronnen binnen een netwerk, en het bieden van centrale authenticatie en autorisatie.	
IDS/IPS	Een IDS monitort het netwerkverkeer op verdachte activiteiten. Een IPS onderneemt actie om inbreuken te voorkomen.	
Cloud Service	Het toegankelijk maken van IT-diensten, zoals bijvoorbeeld hardware en software via een netwerk, meestal het Internet.	
M365	Cloud gebaseerde productiviteitsdienst van Microsoft die toegang biedt tot een suite van applicaties zoals Word, Excel en Teams, samen met cloudopslag en samenwerkingsmogelijkheden.	
Kantoor	Fysieke locaties waar men werkt.	
User	Een gebruiker van een informatiesysteem	
Externe Rijksdiensten	Rijksadresgids, RijksDNS, Rijksportaal, Pdirect, Overige centrale dienst, DWR active director	**Bijvoorbeeld**: ▪ Rijksadresgids

Tabel 2 Componentbeschrijving

3.2.2 Stapsgewijze uitleg voor gebruik in PowerPoint

Volg onderstaande stappen om op basis van de componenten uit de legenda op een gestructureerd manier het netwerkdiagram op te bouwen.

Stap 1: Gebruik het "***Netwerkplan overzicht"*** als leidend voorbeeld

- Gebruik PowerPoint voor het ontwerp van een netwerkplan.
- Open het voorbeeld dat zichtbaar is in het PowerPoint bestand, "***Netwerkplan overzicht"***.
- Zorg ervoor dat er geen andere zones of iconen worden toegevoegd dan die hierin beschreven staan.

Stap 2: Voeg vormen toe

- Kies beschikbare vormen en iconen die opgenomen zijn om netwerkzones en componenten in kaart te brengen. Beperk je tot de voorgeschreven iconen met als doel standaardisatie en simpelheid:
    - De voorgeschreven iconen staan uitgelegd in 2.2.1

Stap 3: Rangschik componenten

- Organiseer logisch van boven naar beneden bijvoorbeeld, het icoon internet en naar beneden een intern netwerk.
- Bekijk het voorbeeld wat is gemaakt in het "***Netwerkplan overzicht"***.

Stap 4: Verbind componenten aan elkaar

- Gebruik Lijnen of verbinders om vormen te koppelen.
- Dit geeft op een overzichtelijke manier weer welke verschillende componenten en zones aan elkaar gekoppeld zijn.

Stap 5: Label alles

- Voeg tekstvakken toe om verdere uitleg weer te geven.
- Vermeld Apparaat namen.
- Verdere toelichten of vermeldingen van IP-adressen is niet nodig, dit wordt vermeld in "***IP Nummerplan Excel"***.

Stap 6: Voeg een uitleg toe

- Maak een klein vakje of gebruik notities waarin, indien nodig, wijzigingen of uitzonderingen worden uitgelegd. Dit helpt anderen om het netwerk diagram snel te begrijpen.

Nadat alle stappen zijn doorlopen en het netwerkdiagram is opgebouwd, kunt u in de "***IP-nummerplan excelsheet***" de verdere details opnemen betreft de indeling van het netwerk.

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)

januari 2025