TLP:GREEN

STANDAARD CONTENTEN DEPLOYMENT GUIDE

Monitoring & Detectie – **Security Information & Event Management** (SIEM)

Best Practice versie 1.0

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 supply-chain, 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.

Een Security Information & Event Management (SIEM) systeem is een typische toepassing om binnen een SOC de monitoring- en detectiediensten in te richten. Een SIEM-systeem is in principe een prachtig stuk software dat helemaal niets doet totdat het gevoed wordt met de juiste data waarbij de juiste detectieregels geconfigureerd en afgestemd op de organisatie moeten worden. Veel SIEM-systemen zijn voorzien van standaard detectieregels die het proces van ingebruikname kunnen versnellen mits dit procesmatig goed wordt aangevlogen. Deze Best Practice helpt startende organisaties om de juiste stappen te zetten bij ingebruikname van een (nieuw) SIEM-systeem en zorgt dat een aantal standaard valkuilen vermeden kunnen worden.

Achtergrond

VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set van producten die rijksorganisaties helpt om een (nieuwe) SIEM-deployment snel en efficient in te richten.

Doelgroep

Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor SOC-Managers, -Leads, en -Analysten en kan handvatten bieden voor projectmanager bij een stapsgewijze SIEM-implementatie.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	3-02-2026	Initiële versie

1.2 Referenties

Document	Link
Logmanagement en SIEM Design Guide (VSSR)	Logmanagement en SIEM design guide
VSSR-kennisdocumenten	VSSR (rijksapplicaties.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 Inleiding

Een kerntaak van een Security Operations Center (SOC) is monitoring en detectie. Vooral de detectie is soms best een uitdaging. Wat moet er worden gedetecteerd? Waarom dan? Waar beginnen we mee? Hoe doen we dat dan? Werkt het goed? Om maar enkele van de vragen en uitdagingen te noemen.

In dit document worden de meeste van deze vragen niet beantwoord omdat ze veelal strategisch en tactisch van aard zijn. De vraag die wel wordt beantwoord is “Waar beginnen we mee?”, of eigenlijk, dit document biedt een handvat voor een eerste stappen voor SIEM-content implementatie. Het is niet noodzakelijk de beste-mogelijke eerste stap, maar het is een mogelijke eerste stap om snel van de kant te komen.

De eerste stap die wordt gezet, is op basis van middelen die veelal voorhanden zijn zodra een SIEM-systeem is aangekocht. Vrijwel alle SIEM-systemen komen met standaard sets detectie regels of bieden de mogelijkheid om pakketten met gestandaardiseerde regels vanuit een marktplaats te downloaden en installeren. Deze functionaliteit biedt voordelen, waarvan snel van de kant komen er één van is. Maar met het uitrollen van standaard content komen ook overwegingen en uitdagingen.

Standaard content heeft als voordeel dat het een goed vertrekpunt biedt bij ingebruikname van een nieuwe SIEM-oplossing of voor een startend Security Operations team waar nog kennis en ervaring opgebouwd moet worden. Vaak wordt standaard content vanuit leveranciers regelmatig bijgewerkt en vernieuwd wat werkdruk binnen het team kan verminderen.

Tegelijkertijd zijn een aantal van de uitdagingen dat het niet altijd duidelijk is hoe de content precies werkt (vaak door beperkte of ontbrekende documentatie) en het lastig kan zijn om dit snel te doorgronden. Hierdoor is het inschatten van de impact op het team bij ingebruikname lastig in te schatten. Zaken om rekening mee te houden:

- Is het duidelijk welke systemen, volgens de SOC-opdracht, in monitoring moeten worden opgenomen;
- Zijn de regels in voldoende maten van toepassing op de organisatie (past het bij de SOC-opdracht) en welk deel is onbruikbaar;
- Beschikt het SOC over de juiste log data om de detectieregels goed te laten werken;
- Zijn de detectieregels voldoende afgestemd op de organisatiecontext (zijn de drempelwaarden voor alarmering wel passend bij de organisatie);
- Wat is de performance impact op het SIEM-systeem van de afzonderlijke detectieregels en is het in sommige gevallen – ook al lijkt de detectie zelf relevant – beter bepaalde om regels niet aan te zetten;
- In hoeverre is de false-positive ratio vooraf in te schatten om het team niet te overladen met werk.

In deze Best Practice komen de belangrijke aandachtspunten aan bod zodat een SOC-team dit als leidraad kan gebruiken bij het implementeren van een nieuw SIEM-systeem of de standaard content sets van een bestaand systeem. Daarnaast worden een aantal belangrijk onderwerpen voor onderhoud aangeraakt om te zorgen dat bestaande content optimaal blijft werken en het SIEM-systeem goed blijft functioneren.

3 Standaard Content – Deployment Guide

Deze deployment guide is in eerste instantie toegespitst op standaard content aangeleverd bij een SIEM-systeem maar kan eenvoudig worden toegepast op bestaande implementaties. Er wordt ingegaan op een aantal generieke uitgangspunten waarna implementatie en beheer uiteen worden gezet. Als laatste wordt ingegaan op minder standaard SIEM-functionaliteit die, afhankelijk van het systeem, wel of niet aanwezig kan zijn. Voor een startende implementatie is het verstandig om eerst de aandacht te richten op uitgangspunten, implementatie en beheer. Als deze fasen achter de rug zijn dan is het een goed moment om de additionele functionaliteit verder te onderzoeken.

3.1 Uitgangspunt

Deze algemene uitgangspunten zijn in principe van toepassing voor elke SIEM-deployment, dit omdat de meeste SIEM-systemen ongeveer op dezelfde manier werken.

- **SOC-missie:** Vooraf is bepaald door de organisatie wat de missie is voor het SOC. Wat wil de organisatie bereiken, wat zijn de doelstellingen en hoe wordt succes gemeten.
- **Monitoring scope:** Op basis van de SOC-missie is bepaald wat wel en niet in scope is voor logging, monitoring en detectie (let op: de logging scope kan prima afwijken van de monitoring en detectie scope).
- **Log policy:** Logging en monitoring is in de Security Policy vastgelegd zodat het duidelijk is wat de plichten en verantwoordelijkheden zijn van proces, applicatie, systeem en data-eigenaren met betrekking tot het aanleveren van log data.
- **Log scope:** Het is duidelijk welke data op welk systeem moet worden opgeslagen waarbij een SIEM veelal een dure oplossing is voor log management. Zorg dus dat het SIEM alleen de data ontvangt die nodig is voor geautomatiseerde detectie.
- **Endpoint agent policy:** Er zijn duidelijke afspraken over het ophalen van log data via lokaal-geïnstalleerde log agents of via het netwerk opgestuurd door endpoints.

3.2 Implementatie

Een SOC doet vaak veel meer dan monitoring en detectie van inbraakpogingen op de digitale footprint van de organisatie. Vooral actieve componenten als EDR-agents maken de rol van het SOC vaak diffuus. Met zulke agents op endpoints wordt eigenlijk impliciet een stuk bescherming (protect), detectie (detect) en reactie (respond) geboden en gaat het dus niet alleen om monitoring en detectie. Met dit in het achterhoofd, komen zowel protect, detect als ook respond aan bod bij de implementatievraagstukken.

3.2.1 Protect

In veel gevallen maakt een SOC gebruik van EDR-agents. Dit is software geïnstalleerd op endpoints die een complex aan taken kan uitvoeren. Bedenk wel heel goed dat een software agent op een endpoint een impact heeft op de performance van het endpoint. Afhankelijk van de configuratie en de gebruikte componenten, kan deze impact nogal verschillen. Bedenk vooraf en overleg met ICT-beheerders en architecten:

- **EDR-gebruik:** Of agents überhaupt geïnstalleerd kunnen/mogen worden en eventueel waar wel en niet (misschien dat op een aantal belangrijke systemen voor ondersteuning van kritische processen het niet acceptabel is dat er (nog meer) agents op draaien.
- **EDR-scope:** Welke functionaliteit nodig is: 1) log-only; 2) uitbreiding met anti-virus (als beschikbaar); 2) full-scale detectie; 3) automatisch ingrijpen om gedetecteerde inbraakpoging te blokkeren (met als risico dat ook gewone processen die zich onverwacht gedragen, geblokkeerd worden); en, 3) mag forensisch-onderzoek op afstand plaatsvinden (met alle mogelijke implicaties van dien).
- **EDR-inrichtingstandaard:** Hoe de EDR-toepassing geconfigureerd moet worden om de juiste functionaliteit in detail correct te implementeren.

- **EDR-detectie testen:** Hoe de configuratie kan worden getest. Dit om te zien of de voorziene configuratie ook het gewenste resultaat heeft. Bekijk ook voor kritische systemen of de configuratie in praktijk geen ongewenste bijeffecten geeft.
- **EDR-beheer eigenaarschap:** Wie eigenaar is en/of beheer op zich neemt. Het beheer van dit soort componenten kan bij een SOC worden ondergebracht, maar daarmee maakt het SOC ook direct onderdeel uit van de ICT-beheerorganisatie. Een andere mogelijkheid kan zijn om de ICT-afdeling het beheer te laten doen wat een stuk flexibiliteit voor het SOC uit handen geeft.

3.2.2 Detect

Voordat detectieregels (regels) worden geïmplementeerd, is het verstandig om een aantal zaken op een rij te krijgen:

- **Detectie scope:** Welke regels zijn (eventueel "waar") van toepassing. De pre-built regels sets zijn vaak behoorlijk uitgebreid, maar als er bijvoorbeeld regels zijn voor Cloud omgevingen maar AWS of GCP is niet in gebruik door de organisatie dan zijn de bijbehorende detectieregels ook niet van toepassing.
- **Databronnen:** Als is bepaald welke regels wel van toepassing kunnen zijn, is de ondersteunende data het volgende aandachtspunt. Zorg dat het duidelijk is welke databronnen en event types per regel nodig zijn zodat de regels ook hun werk kunnen doen. Zonder data gebruiken de regels alleen maar onnodig resources door regelmatig naar niet beschikbare data te zoeken.
- **Audit policy configuratie:** Als het duidelijk is welke regels in gebruik genomen kunnen worden en welke data hiervoor nodig is, dient vervolgens gekeken te worden naar de benodigde configuratie op endpoints. Welke audit policy moet worden geconfigureerd en welke lokale tools zijn er eventueel nodig (gebruik van Sysmon op Windows, wel/geen noodzaak voor auditd op Linux, etc.)
- **Datakwaliteit aanlevering:** Bekijk goed welke datavelden nodig zijn in de logregels om de regels goed te laten werken. Kijk bijvoorbeeld naar het W3C logformaat en bepaal of de Webserver goed is geconfigureerd om de juiste velde te loggen die nodig zijn voor de regels.
- **Log-integraties en configuraties:** Welke zaken zijn nodig om data van de verschillende benodigde databronnen aan te sluiten op het SIEM-systeem. Deze vereisen implementatie, updates en onderhoud.
- **Datakwaliteit verwerking:** Als de logintegratie is gerealiseerd, controleer dan of de velden in de logregels ook goed worden verwerkt naar het datamodel van het SIEM. Als dit maar deels of niet van toepassing is, breng dan de juiste configuratie aan om te zorgen dat de data juist wordt verwerkt. Zorg dat er een intern proces is om dit (automatisch) regelmatig te valideren en corrigeren waar nodig. Software op endpoints veranderen dus wat vandaag werkt, is misschien morgen stuk.
- **Tuning:** Standaard detectieregels hebben een standaard configuratie die zeer waarschijnlijk niet aansluit bij de context van de organisatie. Een simpel voorbeeld is een detectieregel die afgaat bij een X-aantal foutieve login pogingen; De Security Policy kan per organisatie afwijken met een andere X die in de regel moet staan. Maar mogelijk is dit ook afwijkend voor bijvoorbeeld laptops voor eindgebruikers ten opzichte van applicaties met kritische data. Deze fijn afstelling zal bijna altijd gerealiseerd moeten worden en hier dient dus op voorhand rekening mee te worden gehouden.
- **Alerting:** Bekijk op voorhand heel goed naar welke regels ook echt in een alert mogen resulteren. Elk alert betekent dat een Analist aan het werk moet om uit te zoeken of het een mogelijk incident betreft. Daarbij komt dat een te veel aan alerts (en bijkomende hoge werkdruk) ervoor zorgen dat analisten hun werk met minder aandacht uitvoeren. Het komt vaak voor dat een teveel aan detectieregels vrijwel automatisch resulteert in meer false-positives. Analisten die de hele dag false-positives moeten onderzoeken, gaan steeds meer op de automatische piloot werken en dingen over het hoofd zien (en uiteraard is het ook gewoon tijdsverspilling). Zodra je zaken gaat implementeren, zorg dan ook dat er

rapportages draaien om alert-trends te monitoren en eventuele slecht-functionerende regels er snel uit te filteren.

- **Deployment:** De hoeveelheid standaard regels is vaak best veel. Het is verstandig om eerst de agents gecontroleerd uit te rollen in batches (test-lab), kleine test batch (25 endpoints o.i.d.), middelgrote batch (250), full coverage deployment in batches van ongeveer 1000 endpoints per keer. Bepaal de batchgrootte op basis van de hoeveelheid support die kan worden verleend als er dingen verkeerd gaan (en dit gaat gebeuren). Als de eerste agents draaien, evalueer dan de eerste set regels. Doe dit ook in batches van ongeveer 25 per keer zodat de alert-stroom niet opblaast. Bij voorkeur worden regels eerst aangezet, geëvalueerd door senior analisten en vervolgens in kleine stappen naar productie gebracht met bijbehorende uitleg en ondersteuning voor de analisten.

3.2.3 Respond

Voor het reageren op incidenten zijn twee onderdelen van belang: 1) EDR-oplossingen kunnen aanvallen **automatisch blokkeren** als ze gebeuren; en, 2) met EDR-oplossingen is het veelal mogelijk om diepgaand **forensisch onderzoek** op afstand uit te voeren. Bij het blokkeren van aanvallen is het van belang om goed naar de configuratiemogelijkheden te kijken om te zien wat wel en niet wenselijk is en voor welke omgeving. Mogelijk is het acceptabel dat op werkplekken alles wordt geblokkeerd maar is dit op servers met kritische processen te risicovol. Voor incident response en forensisch onderzoek op afstand moet goed worden gekeken naar de mogelijkheden van de software. Wat mag volgens de security policy en HR-policy wel of niet en wat is op welke omgeving acceptabel. Neem hierbij ook het mandaat van het SOC in ogenschouw en andere mandaten, zoals het stekkermandaat, om te zien wie wat wel en niet mag doen vanuit een bedrijfsvoering perspectief.

3.3 Beheren

Zoals bij alles heeft ook een SIEM, en de detectieregels, onderhoud nodig. Op vrijwel alle bovengenoemde onderdelen is regelmatige aandacht vereist om alles blijvend goed te laten werken. Geautomatiseerde dashboards of regelmatige rapportages kunnen hierbij heel veel helpen.

Zaken die regelmatige aandacht vragen en eigenlijk als terugkerende taak in de agenda van Senior analisten en/of SOC-leads terug moeten komen, zijn o.a. het volgend:

- **Datakwaliteit aanlevering:** komt alle benodigde data, voor de werking van de detectie, nog binnen. Het ontbreken van data kan duiden op connectiviteitsissues (meestal valt dan een hele stroom uit), of wijzigingen in de audit configuratie op systemen/applicaties (hierdoor vallen vaak specifieke kleine onderdelen weg uit de verder intacte datastroom).
- **Datakwaliteit verwerking:** Wordt de ontvangen data goed ingelezen in het systeem en komt alles op een bruikbare wijze in de SIEM-database? Is dit niet het geval dan dient er naar de log-parsers te worden gekeken.
- **Detectieregels:** Werken alle detectieregels naar behoren? “Naar behoren” is een lastig concept en valt in verschillende onderdelen uiteen:
    - Zijn de thresholds voor alarmering nog correct? Data verandert over tijd en gedrag van mensen en applicaties veranderen over tijd.
    - Gaan de regels ook af? Test regelmatig of alle content onder de juiste omstandigheden nog correct werkt. Dit kan eventueel worden gesimuleerd met test-data.
    - Hoe hoog zijn de false-positive ratio’s en hoe verandert dit over tijd? Bekijk continu of regels nog wel goed functioneren en aansluiten bij de detectiebehoefte. Zo niet, zet regels uit.
    - Worden de juiste dingen gedetecteerd? Als bepaalde detectieregels veel afgaan en altijd false-positives genereren en misschien altijd afgaan als bijvoorbeeld mensen aan het werk zijn (en nauwelijks buiten kantoortijden), dan wordt er misschien

vooral "normaal" gedrag gedetecteerd. Soms kan dit een doel zijn, maar in de meeste gevallen genereerd het vooral veel ruis en werk. Misschien is het verstandig om bepaalde regels dan uit te zetten.

- **Black/white-lists:** Dit onderwerp is nog niet eerder aangeraakt, maar veel detectie maakt gebruik van uitzonderingen of heel specifieke targets om op te detecteren. Na verloop van tijd is uiteraard altijd de vraag of de targets nog goed zijn en of de lijst met uitzonderingen misschien niet te lang is geworden. Beide gevallen resulteren in blinde vlekken wat zoveel mogelijk voorkomen moet worden.
- **Resourcegebruik:** SIEM-systemen werken allemaal op hun eigen manier, allemaal met specifieke sterke en zwakke eigenschappen en hun eigenaardigheden. Bekijk regelmatig en goed of en hoe bepaalde detectielogica invloed heeft op het resourcegebruik van het systeem. Als bepaalde regels teveel impact hebben, is het misschien een idee om naar een andere oplossing te zoeken.

3.4 Additionele Functionaliteit

De markt voor SIEM-producten is enorm gegroeid en de diversiteit aan product features is daarmee ook sterk gegroeid. Het ene product is het andere niet en alle producten hebben hun eigen specifiek aandachtsgebied met hun eigen sterke en zwakke punten. Hieronder zijn een aantal additionele features op een rij gezet die mogelijk aanwezig kunnen zijn boven op de standaard detectie mogelijkheden:

- **User and Entity Behaviour Analytics:** Het monitoren van gedrag van gebruikers op basis van organisatiebreed en gebruikers(groep)specifiek gedrag en afwijking hierop.
- **Privileged User Monitoring:** Specifieke monitoring gericht op een subset van accounts met vaak hogere privileges dan gemiddeld of belangrijke personen binnen de organisatie.
- **AI/ML based detection** of **Alert recommender system:** Artificial Intelligence en Machine Learning zijn heel brede begrippen waar veel verschillende algoritmen en mogelijkheden onder vallen. De mogelijkheden zijn heel breed en kunnen worden ingezet voor zowel detectie (vaak anomaly detection) alsook voor het automatisch analyseren van alerts om analisten te ondersteunen bij het uitvoeren van triage op alarm-events.
- **Network Anomaly Detection / Lateral Movement Detection:** Bewegingen op het intern netwerk is een ander toepassingsgebied om detectie op toe te passen. Hiervoor kunnen ook weer anomaly detection algoritmen worden ingezet, maar andere oplossingen zijn ook goed mogelijk. Sommige SIEM-systemen maken gebruik van log data van bijv. Firewalls, andere systemen kijken liever naar raw packet data die op basis van sensoren direct van het netwerk wordt gehaald.
- **Anomaly Detection:** Voor het detecteren van afwijkend gedrag kan Machine Learning worden gebruikt, maar er afwijkend gedrag kan ook anders worden gedetecteerd. De mogelijkheden hiervoor zijn behoorlijk breed en veel SIEM-oplossing hebben hier wel iets aan functionaliteit voor beschikbaar die voor verschillende doeleinden kan worden ingezet.

Deze lijst is niet uitputtend en wijzigt met de tijd. Wat, echter, niet zal veranderen, is dat elke oplossing, hoe mooi hij ook klinkt, altijd vrij complex van aard zal zijn. In de aanloop naar een zal de nodige tijd nodig zijn om zaken goed te configureren en er is structureel onderhoud nodig. Het goed begrijpen van complexere oplossingen vergt vaak meer jaren ervaring als security analist en een goed inzicht in de data en bijbehorende context om de oplossing goed te laten functioneren. Daarbij komt dat oplossingen met specialistisch toepassingen als AI en ML vaak ook de bijbehorende specialisten nodig hebben om alles goed te laten functioneren. Naast de juiste technische oplossing heeft de organisatie dus ook de juiste mensen nodig om de techniek goed te laten functioneren. Bekijk vooraf dus goed wat de voor- en nadelen zijn en of alle kennis, data en tijd beschikbaar is om de functionaliteit goed te implementeren en onderhouden.

Bijlage I – Checklist

Uitgangspunten			Alerting	
SOC-missie			Deployment	
Monitoring scope				
Log policy			**Reageren**	
Log scope			Automatisch blokkeren	
Endpoint agent policy			Forensisch onderzoek	
Beschermen			**Beheren**	
EDR-gebruik			Datakwaliteit aanlevering	
EDR-scope (log, detectie, voorkomen)			Datakwaliteit verwerking	
EDR-inrichtingstandaard			Detectieregels	
EDR-detectie testen			Black/white-lists	
EDR-beheer eigenaarschap			Resourcegebruik	
Detecteren			**Additionele Functionaliteit**	
Detectie scope			User & Entity Behaviour Analytics	
Databronnen			Privileged User Monitoring	
Audit policy configuratie			AI/ML gebaseerde detectie	
Datakwaliteit aanlevering			Alert recommender system	
Log-integraties en configuraties			Network Anomaly Detection	
Datakwaliteit verwerking			Lateral Movement Detection	
Tuning			Anomaly Detection	

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://vssr.rijksapplicaties.nl/

vssr.info@minjenv.nl

Februari 2026