METRICS VOOR SOC-DIENSTEN

Monitoring & Detectie – HAVIK

Handreiking versie 1.1

Complexiteit document

Eenvoudig

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inleiding

Deze handreiking is opgesteld voor organisaties die voornemens zijn om Security Operations Center (SOC)-diensten extern in te kopen. Dit document maakt onderdeel uit van een bredere set document (HAVIK) opgesteld door VSSR om partijen te ondersteunen bij het aanbesteden van externe SOC-diensten. HAVIK staat voor Handige Aanpak Voor Inkoop van Kwalitatieve SOC-diensten. De volledige set van HAVIK documenten zijn beschikbaar op de VSSR-portal[1].

In overeenkomsten met de externe partij worden veelal prestatie-indicatoren opgenomen om de kwaliteit van de dienstverlening te kunnen meten. Dit document bevat een basis set kritische prestatie-indicatoren met de aanbeveling om (een subset van) deze indicatoren op te nemen in contractuele overeenkomsten, er over te laten rapporteren en de rapportages frequent te bespreken. Op deze wijze kunt u samen met uw leverancier op continue serviceverbetering sturen.

De beschreven indicatoren zijn niet willekeurig gekozen. Met als uitgangspunt een aantal kernprocessen binnen een SOC, zijn de genoemde indicatoren belangrijke punten om het verloop van deze processen te kunnen meten. Dit document bevat dan ook een beknopte uiteenzetting van de kernprocessen binnen een (beginnend) SOC en geeft bij deze processen een basis set kritische prestatie-indicatoren. Voor de indicatoren die hier zijn opgenomen, ligt de nadruk op het kunnen sturen van extern gecontracteerde dienstverlening. Dit laat onverlet dat de zelfde indicatoren een goed vertrekpunt zijn bij het opzetten van een eigen SOC.

Naast prestatie-indicatoren om de overeenkomst tussen opdrachtgever en -nemer op kwaliteit te kunnen sturen, worden binnen een SOC vaak ook verschillende risico-indicatoren samengesteld. Deze risico-indicatoren zijn van belang voor de opdrachtgever maar in mindere maten voor opdrachtnemer en ze zijn ook niet bruikbaar om de overeenkomst te sturen. In dit document zijn een aantal van deze risico-indicatoren opgenomen zodat u, als opdrachtgever, de mogelijkheid heeft om in de overeenkomst met uw opdrachtnemer een degelijke set rapportages op te nemen om zelf inzicht te houden in het risicoprofiel van uw organisatie op basis van operationele data. Voor de sturing van de overeenkomst is het niet direct van belang om deze indicatoren op te nemen.

SOC-Kernprocessen en Metrics

Security Operations is een bewegend concept en door de jaren heen zijn de activiteiten van een SOC telkens aangepast. Daarnaast verschilt het per organisatie wat een SOC wel en niet doet waarbij bepaalde processen bij de ene organisatie binnen de SOC-verantwoordelijkheden vallen en elders erbuiten. Ondanks dit dynamisch speelveld en een breed scala aan mogelijke verantwoordelijkheden, zal elk SOC een aantal kern-processen onderscheiden die veelal aan de basis van het SOC en gerelateerde werkzaamheden liggen. Deze kernprocessen worden hier kort uiteengezet waarna per proces de bijbehorende indicatoren worden toegelicht.

SOC-Kernprocessen

De belangrijkste taken die bij een (beginnend) SOC liggen, zijn: Kwetsbaarhedenbeheer en Monitoring & Detectie. Om deze taken goed uit te kunnen voeren, is logdata van essentieel belang. Dit heeft als gevolg dat vrijwel elk SOC ook, bedoeld of onbedoeld, een stevige competentie op het beheer van logdata opbouwt. De vier kernprocessen om de twee hoofdtaken goed te ondersteunen, vallen hiermee uiteen in: Kwetsbaarhedenbeheer, Databeheer, Detectie en Monitoring.

Deze vier kernprocessen zijn verder op te delen in een aantal processtappen. Deze stappen zijn in *Tabel 1:* SOC-kernprocessen weergegeven. De weergave is beknopt en vooral bedoeld om de indicatoren te ondersteunen. Voor een verdere uiteenzetting van deze processen kunt u goede houvast vinden in verschillende andere publicaties, deze zijn opgenomen bij de referenties.

[1] VSSR (ncsc.nl)

Proces	Processtap	Beschrijving
Kwetsbaarheden-beheer[2]	Identificeren	Identificeren van ICT-assets en kwetsbaarheden met behulp van gespecialiseerde software voor kwetsbaarhedenbeheer.
	Evalueren	Evalueren van gevonden kwetsbaarheden, deze voorzien van duiding en handelsperspectief en deze communiceren naar de juiste eigenaar/oplosgroep.
	Oplossen	Verhelpen van gevonden kwetsbaarheden (veelal een taak die buiten het SOC ligt).
	Rapporteren	Het opstellen en verspreiden van periodieke statusrapportages om de procesinzicht te bieden en de risico-status te communiceren.
Databeheer[3]	Extract	Security gerelateerde logdata ophalen bij de logbron.
	Transform	Transformeren van de verschillende formaten logdata naar het formaat van de centrale logging en monitoring oplossing.
	Load	Het laden van de getransformeerde data in de centrale logging en monitoring oplossing.
Detectie[3]	Definiëren	Vaststellen van de detectie use cases die betrekking hebben op het risicoprofiel van de organisatie en bijbehorende aanvalsscenario's.
	Bouwen	Bouwen van detectietechnologie en use cases om het risico voor de organisatie te verminderen.
	Testen	Periodiek testen van de afzonderlijke detectie elementen en de competentie als geheel om onvolkomenheden aan het licht te brengen.
	Verbeteren	Continu verbeteren van bestaande detectie op basis van testresultaten en nieuwe trends in de markt.
Monitoring[3]	Detecteren	Detecteren van gebeurtenissen met een mogelijke informatiebeveiligingsimpact.
	Bevestigen	Onderkennen van een gebeurtenis door een SOC-analist, en het bevestigen en eventueel door te zetten voor eerste onderzoek.
	Triage	Uitvoeren van een eerste onderzoek om te bepalen of de melding voldoende relevant is om serieus verder te onderzoeken en/of de use case aangepast moet worden.
	Onderzoeken	Uitvoeren van een diepgaand onderzoek op bevindingen om te bepalen wat een incident is en welke opvolging is vereist.

Tabel 1: SOC-kernprocessen

[2] VSSR (ncsc.nl)
[3] CSIRT Services Framework Version 2.1 (first.org)

Key Performance Indicators (KPI)

Onderstaande indicatoren zijn bedoeld ter ondersteuning van de contractuele afspraken die zijn gemaakt tussen opdrachtgever (OG) en opdrachtnemer (ON). De nadruk van onderstaande indicatoren ligt op kwaliteit van de inhoudelijke processen. Het zwaartepunt van de indicatoren ligt niet op de tijdigheid van afhandeling van potentiële incidenten. Het meten van deze tijdigheid is wel heel gebruikelijk, echter, de ervaring leert dat afspraken over tijdigheid veelal resulteren in tijdsdruk op de afhandeling van meldingen. Tijsdruk komt de kwaliteit niet altijd ten goede waarmee dit dus ook niet het middel van eerste keuze is om de overeenkomst te sturen. Uiteraard staat het iedereen vrij om tijdigheidsindicatoren op te nemen in de eigen overeenkomst.

Proces	Metric	Doel
Kwetsbaar-hedenbeheer	Percentage tijdig gescande assets.	Controleren van scan-frequentie die is afgesproken tussen OG en ON.
	Percentage geëvalueerde kritische en hoog risico kwetsbaarheden.	Controleren of ON de juiste kwetsbaarheden volgens afspraak heeft onderzocht.
	Percentage kritische en hoog risico kwetsbaarheden die tijdig zijn gerapporteerd voor opvolging uitgesplitst naar leveranciers/ beheerorganisaties.	Controleren of ON de gevonden kwetsbaarheden tijdig heeft onderzocht en gerapporteerd aan OG.
Databeheer	Percentage log bronnen waarvan log data wordt ontvangen.	Controleren of alle afgesproken logbronnen zijn aangesloten op de detectiesystemen van ON en daadwerkelijk logdata aanleveren.
	Percentage incorrecte data parsing die tijdig is gecorrigeerd.	Controleren of alle door ON ontvangen incorrect verwerkte data tijdig volgens afspraak is gecorrigeerd.
	Percentage incorrecte data filtering die tijdig is opgelost.	Controleren of data filtering volgens afspraak is geïmplementeerd of gecorrigeerd waar van toepassing.
	Percentage log data verwijderd conform afgesproken retentietijden.	Controleren of de afspraken voor data retentietijden worden nageleefd.
Detectie	Percentage geïmplementeerde use cases t.o.v. de gedefinieerde use cases.	Controleren of de afgesproken detectie ook is geïmplementeerd.
	Aantal gedetecteerde aanvallen bij testen van use cases.	Controleren of de afgesproken use cases correct zijn geïmplementeerd en correct werken.
	Percentage onderzochte CTI-sightings.	Controleren of CTI-sightings volgens afspraak zijn onderzocht.
	Percentage false positive alarmen.	Controleren of de kwaliteit van de detectie use cases voldoende is en/of bijgesteld moet worden.
Monitoring	Percentage tijdig afgeronde en overgedragen alarmonderzoeken.	Controleren of alarmen tijdig zijn onderzocht door ON en gecommuniceerd naar OG volgens contractuele afspraken.
	Aantal gemiste incidenten tijdens de alarm onderzoeksfase.	Controleren of het onderzoekswerk van ON kwalitatief goed is[4].
	Percentage true/false positive incidenten per prioriteitsniveau.	Controleren van de kwaliteit van de huidige detectie.
	Aantal alarm events correct gedocumenteerd.	Controleren van de kwaliteit en compleetheid van onderzochte en overgedragen incidenten.

Tabel 2: Prestatie-indicatoren

[4] Deze KPI is niet bedoeld om ON af te rekenen op gemiste incidenten. Bij onderzoek worden altijd incidenten over het hoofd gezien waarvoor de verantwoordelijkheid niet perse altijd en alleen bij ON ligt. Het doel is om gezamenlijk verbeterpunten vast te stellen om zo de dienstverlening te verbeteren.

Key Risk Indicators (KRI)

Naast een aantal relevante prestatie-indicatoren kunt u ook risico-indicatoren opnemen in de overeenkomst tussen OG en ON. Zoals gezegd zijn deze indicatoren niet bedoeld om contractuele afspraken te ondersteunen maar meer voor de eigen organisatie om inzicht te hebben in het risicoprofiel op basis van de informatie die in het SOC (bij ON) beschikbaar is.

Proces	Metric	Doel
Kwetsbaar-hedenbeheer	Aantal via scanning geïdentificeerde assets die niet in de CMDB voorkomen.	Vaststellen van de compleetheid en volledigheid van het aanvalsoppervlak zoals vastgelegd in de asset database.
	Aantal kwetsbaarheden ingedeeld naar risico niveau op systemen met Internet exposure.	Vaststellen van het risicoprofiel met betrekking tot het aanvalsoppervlak van de organisatie op het internet.
	Trend (13 maanden) van het totaal aantal, opgeloste, en openstaande kritische en hoog risico kwetsbaarheden.	Lange termijn analyse van het risicoprofiel van de organisatie.
	Percentage systemen dat niet volgens de voorgeschreven standaard is ingericht.	Vaststellen van het aantal systemen dat niet volgens afspraak is ingericht en wat hieruit voorvloeiende risico's zijn.
Databeheer	*Binnen dit proces zijn de KPI's veelal ook maatgevend voor de daaruit voortvloeiende risico's: In afwezigheid van correcte en volledige data werkt detectie niet goed. Op dit proces zijn dan ook geen afzonderlijke KRI's gedefinieerd.*	
Detectie	Percentage geïmplementeerde use cases (per aanvalsscenario[5]).	Vaststellen in hoeverre de belangrijkste dreigingen kunnen worden gedetecteerd.
	Percentage aanwezige log bronnen noodzakelijk voor het ontwikkelen van de use cases.	Vaststellen van de beschikbaarheid en gaps in de datavoorziening om dreigingen te kunnen detecteren.
	Aantal alarmen per aanvalstechniekcategorie (bijvoorbeeld: phishing, credential access, data leakage, etc.)	Weergeven van trendwijzigingen en het vaststellen van mogelijke aandachtsgebieden voor monitoring.
Monitoring	Aantal kritische incidenten.	Weergeven van het bestaansbelang en werkdruk voor Incident Response.
	Aantal hoog risico incidenten.	Weergeven van het bestaansbelang en werkdruk voor Incident Response.
	Trend (13 maanden) van true/false positive kritische en hoog risico incidenten per maand.	Vaststellen hoeveel kritische/hoog-risico incidenten zich hebben voorgedaan en wat de impact was.

Tabel 3: Risico-indicatoren

[5] Per aanvalsscenario is alleen van toepassing als de use cases zijn opgesteld vanuit een risico-gestuurde aanpak met een dreigingsanalyse zoal beschreven in "VSSR Risicogestuurde SOC-planning".

Tot Slot

De set met indicatoren die hier zijn gepresenteerd is een beperkte set die van toepassing is op de meest voorkomende kernprocessen van een SOC. Voor elke omgeving zijn de kernprocessen mogelijk anders waarvoor andere meetinstrumenten nodig zijn. Ook voor het risicoprofiel zijn mogelijk andere instrumenten nodig. Bepaal dit voor uw eigen organisatie en kijk wat nodig is. Voor een uitgebreidere set prestatie- en risico-indicatoren kunt u terecht op het https://www.ncsc.nl/vssr.

Referenties

Incident Response processen raamwerk - CSIRT Services Framework Version 2.1 (first.org)

VSSR Best Practice Kwetsbaarhedenbeheer - VSSR (ncsc.nl)

VSSR Risicogestuurde SOC-planning – VSSR SOC Readiness Assistance (ncsc.nl)

VSSR Prestatie- en risico-indicatoren voor een SOC – VSSR (ncsc.nl)

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