Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

SOC inrichten: begin klein

Start vanuit eenvoud, groei vanuit behoefte

Factsheet FS-2017-04 | versie 1.1 | 2 mei 2023

Een Security Operations Center (SOC) is een goed middel om zicht te houden op de beveiliging van bedrijfsinformatie en digitale dreigingen, maar het inrichten ervan kost tijd, geld en moeite. Om een SOC tot een succes te maken is het van belang dat het SOC op een gecontroleerde wijze meegroeit met de behoefte aan zicht en grip op informatiebeveiliging vanuit de organisatie. Begin klein, maak de resultaten inzichtelijk voor de organisatie en gebruik een positieve ontvangst van deze resultaten als mogelijkheid voor een volgende stap in het groeiproces. Wees reëel in de planning, het groeipad en de invulling van een in te richten SOC. Besef daarbij: een SOC is een middel, geen doel.

Achtergrond

Om beschermd en weerbaar te zijn tegen digitale aanvallen, is het nodig om zicht en grip te hebben op de digitale infrastructuur binnen uw organisatie en op wat daarbinnen allemaal gebeurt. Een steeds meer gebruikte aanpak om daartoe te komen is het in gebruik nemen van een Security Operations Center (SOC).

Doelgroep

Deze factsheet richt zich op de Information Security Officers van organisaties die een start willen maken met het monitoren van de beveiliging van bedrijfsinformatie.

Samenwerkingspartners-blok

AlertTeam, Belastingdienst, Ministerie van Veiligheid en Justitie, Rijkswaterstaat, SSC-ICT en de Volksbank.

Wat zijn de uitdagingen?

Om een SOC effectief te laten zijn, zal de samenwerking aangegaan moeten worden met een groot deel van de organisatie. Informatieverwerking gebeurt namelijk door de gehele organisatie. Dit maakt het inrichten van een SOC een uitdagende opgave. Bij het inrichten van een SOC komen vele zaken kijken.[1] Omdat een SOC een relatief nieuw fenomeen is, zijn echter weinig experts te vinden die daarbij kunnen helpen. Daarnaast kost het inrichten van een SOC veel tijd en geld, waardoor het lastig kan zijn om een directie te overtuigen van het nut en de noodzaak. Deze factsheet helpt bij het om kunnen gaan met deze uitdagingen.

> Hoewel bij een Security Operations Center een hoop techniek komt kijken, is het inrichten ervan vooral een organisatorische uitdaging.

Wat is een SOC?

Hoewel geen harde definitie bestaat van een SOC, laat de praktijk zien dat security monitoring de meest ingevulde taak is van een SOC. Daarbij wordt log-informatie van relevante applicaties en apparaten in het netwerk centraal verzameld en gecorreleerd om te zien of afwijkende zaken hebben plaatsgevonden. Het soort applicaties en apparaten waar log-informatie van verzameld wordt, kan zeer uiteenlopend zijn: van IDS, firewalls, webapplicaties, Active Directory servers en antivirus-software tot aan industriële controle systemen. Alle systemen die relevante informatie kunnen aanleveren om zicht te krijgen op de beveiliging of de status van het netwerk en de daarop aangesloten systemen, kunnen daarbij worden gebruikt. Bij de vraag welk soort informatie verzameld moet worden, vanaf welke systemen en op welke wijze deze moet worden gecorreleerd, gaat het niet om wat 'hoort', maar puur om wat voor de organisatie van belang is.

Een hulpmiddel dat onlosmakkelijk verbonden is met een SOC is een Security Information & Event Management (SIEM) systeem. Het betreft software die in staat is om log-informatie vanuit verschillende bronnen te interpreteren en te correleren naar wat zich binnen en rondom het netwerk afspeelt op gebied van cyberaanvallen en andere beveiligingsincidenten.

Naast informatie over systemen en het netwerk, gebruikt een SOC ook 'threat intelligence'. Dit is informatie uit derde bronnen over kwetsbaarheden en dreigingsinformatie op het gebied van cybersecurity. Deze informatie kan gebruikt worden bij het beoordelen van gebeurtenissen op systemen en binnen het netwerk.

Begin met eenvoudige monitoring

Vanuit het niets een volwaardig SOC opzetten is een uitdagende opgave. Een eenvoudigere aanpak is door klein te beginnen en langzaam en gecontroleerd door te groeien naar een volwaardig SOC. Begin, om daartoe te komen, bij de ICT-beheerorganisatie met het monitoren van log-informatie van een paar belangrijke infrastructurele of middelwarecomponenten, bijvoorbeeld de firewall, een webserver of de anti-

[1] Voor een overzicht van aandachtspunten bij inrichting van een SOC, zie http://rafeeqrehman.com/wp-content/uploads/2014/12/Building_SOC.pdf

virusoplossing. Hanteer bij het monitoren in eerste instantie een technische insteek, zodat alleen geschakeld hoeft te worden met de ICT-beheerorganisatie. Zoek daarbij naar meldingen die een concreet probleem aangeven of indicatoren van mogelijke komende problemen. Maak van gevonden zaken melding bij de ICT-servicedesk.

Voor het monitoren van logbestanden zijn tal van software-pakketten beschikbaar. Met behulp van een zoekmachine of eigen onderzoek kunt u daar een keuze in maken.

Doe ervaring op met monitoren en het detecteren, registreren en afhandelen van incidenten. Wees niet gehaast met het toevoegen van extra systemen waarop gemonitord wordt. Ervaring opdoen met het hele proces van monitoren is in eerste instantie belangrijker dan het monitoren zelf. Zorg voor de juiste middelen voor het registeren van incidenten, het periodiek kunnen rapporteren daarover en het vastleggen van opgedane kennis. Zorg dat de medewerkers die zich bezighouden met de monitoring, deelnemen aan de juiste overleggen binnen de ICT-beheerorganisatie en rondom change management. Op die manier zijn zij goed voorbereid op wijzigingen in het netwerk.

Richt uw aandacht in het begin niet te veel op het per se willen inrichten van een SOC. Begin met het verkrijgen van zicht op de beveiliging op basis van behoeften vanuit de organisatie. Het is niet verkeerd om later tot de conclusie te komen dat wat u ingericht hebt, onder de noemer SOC valt.

Wat is nodig om te kunnen monitoren op beveiligingsincidenten?

Gedegen monitoring op informatiebeveiliging vraagt meer van een organisatie dan het monitoren van de logbestanden van bijvoorbeeld de anti-virusoplossing of de firewall. Voordat vanuit de monitoringsopzet binnen de ICT-beheerorganisatie doorgegroeid kan worden naar een SOC, dient daarom eerst een aantal zaken binnen de organisatie ingericht en georganiseerd te worden.[2]

Informatiebeveiligingsincidenten

Een door de directie goedgekeurd informatiebeveiligingsbeleid is een belangrijk hulpmiddel bij het inrichten van een SOC. In een informatiebeveiligingsbeleid staan de doelstellingen van informatiebeveiliging voor de organisatie en hoe informatie-beveiliging binnen de organisatie is georganiseerd (wie welke verantwoordelijkheid heeft). De doelstellingen uit het informatiebeveiligingsbeleid kunnen gebruikt worden bij het bepalen waar het SOC zich op gaat richten. Uit de wijze waarop informatiebeveiliging is georganiseerd, is op te maken wie de belangrijke stakeholders zijn.

Overzicht van het applicatielandschap

Een overzicht van het applicatielandschap geeft zicht op welke informatie een organisatie in huis heeft en de wijze waarop deze informatie verwerkt wordt. Dit overzicht is nodig bij het goed en effectief inrichten van de monitoring. Tevens is deze informatie noodzakelijk om een goede risicoanalyse te kunnen uitvoeren.

Resultaten van een recente risicoanalyse

Met behulp van een risicoanalyse wordt in kaart gebracht wat de gevolgen zijn voor de organisatie in het geval van problemen met de

[2] Voor aanvullende informatie, zie https://www.cip-overheid.nl/media/1125/7-kritische-succesfactoren-voor-een-soc.pdf

beschikbaarheid, integriteit en vertrouwelijkheid van bepaalde informatie. Daarnaast wordt in kaart gebracht welke dreigingen bij de verwerking van informatie een onacceptabel risico vormen. Deze informatie geeft goed zicht op waar een SOC zich primair op moet richten.

De resultaten en uitkomsten vanuit risicomanagement zijn belangrijk voor een SOC. De afdeling risicomanagement is bij uitstek de afdeling die antwoord geeft op de vraag waar een SOC op moet monitoren. Dat hoeft dus niet alleen om kantoorautomatisering te gaan. Ieder systeem en iedere informatieverwerking waarvan het risico door de afdeling risicomanagement als voldoende hoog wordt geclassificeerd, komt in aanmerking om door het SOC te worden gemonitord.

ICT-beheerorganisatie

Een SOC gaat ongetwijfeld aanvallen detecteren en zwakheden in het netwerk aan het licht brengen. Van daaruit zullen voorstellen komen voor het afwenden van een aanval of ter verbetering van de beveiliging. Deze voorstellen dienen niet door het SOC te worden opgepakt, maar door de ICT-beheerorganisatie. Een volwassen incidentafhandelingsproces, een goed ingerichte ICT-servicedesk, goede afspraken met de ICT-beheerorganisatie over de prioritering van meldingen vanuit het SOC en het juiste mandaat van het SOC zijn daarbij van belang.

Eigenaarschap van informatiesystemen

Veel problemen die door een SOC geïdentificeerd worden, kunnen waarschijnlijk door inzet van de ICT-beheerorganisatie aangepakt worden. Echter, er kunnen zich incidenten voordoen waarbij beslissingen op tactisch niveau genomen moeten worden. Ieder informatiesysteem moet daarom een manager als systeemeigenaar hebben, die dit soort beslissingen kan nemen. Het gaat dan om beslissingen die genomen moeten worden bij het inwerkingtreden van een noodplan, zoals het wel of niet offline halen van een informatiesysteem en wat gedaan moet worden om een offline-tijd goed door te komen.

Doorgroeien naar een SOC

Het uitgaan van techniek is een goede aanpak om een begin te maken met monitoren. Om een SOC echt effectief te maken, moet aansluiting gevonden worden bij de bedrijfsprocessen. Wat zijn de vitale processen binnen de organisatie, welke informatievoorziening is daarbij noodzakelijk en op welke wijze kan die informatievoorziening verstoord worden? Door te denken en te praten in termen van processen is het makkelijker om aansluiting te vinden bij de verschillende afdelingen en hun medewerkers. Om die aansluiting te kunnen vinden, is een juiste aanpak in de groei van het SOC noodzakelijk.

Kennis en vaardigheden van SOC-medewerkers

Begrijpen wat voor de business belangrijk is en het monitoren op dreigingen die deze business bedreigen, gaat verder dan het zoeken naar technische problemen in logbestanden. Of een systeem een bepaalde fout genereert, is iets waar een concrete controle voor ingericht kan worden. Maar wanneer is een login valide? Wanneer hoort het raadplegen, wijzigen of verwijderen van informatie tot de gebruikelijke werkzaamheden en wanneer is een kwaadwillende aan het werk? Het controleren of de beveiliging doorbroken is, vraagt om een geheel andere aanpak. Dit vraagt dus om een andere insteek en met name een ander soort denken van de medewerker. Omdat een SOC een relatief nieuw fenomeen is, zijn goede en vooral ervaren SOC-medewerkers lastig te vinden. Start een SOC daarom met medewerkers met de juiste motivatie en mentaliteit en investeer voldoende in opleidingen.

Zelf doen of uitbesteden?

Een belangrijke keuze bij het ingebruiknemen van een SOC, is of de verschillende onderelen van een SOC zelf worden opgebouwd en beheerd, worden uitbesteed of dat er voor een mix tussen deze twee vormen woordt gekozen, waarin bepaalde onderdelen wel worden uitbesteed en andere onderdelen niet.

Iedere organisatie heeft zijn eigen specifieke wensen, eisen en uitdagingen ten aanzien van een SOC. Deze zijn dan ook leidend voor het soort SOC dat uiteindelijk gekozen wordt. Voorbeelden van factoren waartussen een afweging wordt gemaakt zijn flexibiliteit, kosten, beschikbaarheid van kennis en personeel, etc. Een juiste keuze is noodzakelijk om vanuit een SOC te kunnen voldoen aan deze specifieke wensen en eisen.

Voor het afnemen van SOC-diensten en -producten zijn tal van leveranciers beschikbaar. Praat met meerdere van hen over de diensten die zij kunnen leveren, om zo een beter beeld te vormen over wat er te krijgen is en wat er komt kijken bij het hebben van een SOC. Houd bij het buiten de deur plaatsen van informatie die door een SOC verwerkt wordt, rekening met de geldende wet- en regelgeving.

Processen

Een van de belangrijkste zaken om te organiseren zijn de processen voor het afhandelen van een incident, zodat iedereen weet wat van hem of haar verwacht wordt. Definieer typen incidenten, waarbij onderscheid gemaakt wordt in grootte van de impact, en bepaal de te volgen stappen voor de SOC-medewerkers. Bepaal welke mensen in geval van een incident benaderd moeten worden. Kies daarvoor mensen met de juiste verantwoordelijkheden en het juiste mandaat. Spreek met hen door dat zij in zo'n geval benaderd kunnen worden en welke beslissingen van hen verwacht worden. Bepaal welke opschaling- en escalatiemogelijkheden wenselijk zijn en stem dit af met de juiste verantwoordelijken. Zorg dus voor goed verwachtingsmanagement binnen de organisatie. Organiseer dat de reguliere monitoringswerkzaamheden binnen het SOC tijdens een incident door kunnen gaan. Zorg voor een communicatieplan en richt de processen zodanig in dat de inzet en de meerwaarde van het SOC meetbaar zijn.

Contact met de business

Om zicht te hebben wat belangrijk is voor de business, dient het SOC contact te hebben met de business. Zorg voor contact met de juiste managers en systeemeigenaren. Betrek de afdeling risicomanagement bij deze gesprekken. Het informatie-beveiligingsbeleid en de resultaten van de risicoanalyse kunnen helpen bij het inzichtelijk maken van de dreigingen en de juiste prioritering daarbij.

Maak concrete en duidelijke afspraken met de business over de wijze waarop en het formaat waarin informatie ten behoeve van het SIEM-systeem wordt aangeleverd. Betrek de organisatie bij de resultaten van het SOC door middel van periodieke rapportages.

Keuze voor een SIEM-systeem

Hoewel de grootste uitdagingen bij het inrichten van een SOC van organisatorische aard zijn, dient ook een belangrijke technische keuze gemaakt te worden. Dit betreft de keuze voor de SIEM-systeem. Veel van deze pakketten hebben vergelijkbare functionaliteiten. De belangrijkste verschillen zitten in de details, wat het kiezen van het juiste pakket lastig maakt. Daar kan pas een goede beslissing over genomen worden als voldoende duidelijk is of een pakket voorziet in alle behoeften vanuit de organisatie. Ga, nadat alle behoeften vanuit de organisatie in kaart zijn gebracht, daarom praten met leveranciers, bezoek beurzen en ga, indien mogelijk, kijken bij organisaties die reeds een SIEM-systeem hebben ingericht. Maak een weloverwogen keuze, want is eenmaal een pakket gekozen, dan kost het veel geld en moeite om op een later moment te migreren naar een ander pakket.

Let naast de mogelijkheden van de SIEM-syssteem ook op wat nodig is om dit systeem te installeren en te onderhouden en welke kennis dit vraagt van de SOC-medewerkers.

Threat intelligence

Een SIEM-systeem gaat een heleboel zaken aan het licht brengen. Om deze zaken goed te kunnen beoordelen is het noodzakelijk dat zowel het SIEM-systeem als de SOC-medewerkers voorzien worden van de juiste informatie en kennis. Investeer in het verkrijgen van dreigingsinformatie voor het voeden van het SIEM-systeem en geef SOC-medewerkers voldoende tijd om op de hoogte te blijven van de ontwikkelingen op het gebied van digitale dreigingen.

Impact op de privacy

Bij het verwerken van informatie ten behoeve van monitoring, bestaat de kans dat daar privacygevoelige informatie bij zit. Voer voor iedere vorm van informatieverzamelen waar mogelijk privacygevoelige informatie bij zit, samen met de privacy officer een Privacy Impact Assessment (PIA) uit. Bekijk de mogelijkheden die de SIEM-systemen hebben op het gebied van privacybescherming.

Extra taken voor een SOC

Verschillende partijen benoemen, naast monitoring, andere mogelijke taken van een SOC.[3,4] Uiteraard is het mogelijk om de werkzaamheden van verschillende medewerkers, zoals het uitvoeren van penetratietesten en forensisch IT-onderzoek, onder dezelfde organisatorische noemer te plaatsen, maar pas op met het toekennen van extra taken voor de medewerkers die met monitoring belast zijn. Gebruik rustige momenten niet als excuus om hen meer taken toe te kennen. Het gevaar daarbij is dat deze extra taken onvoldoende tijd krijgen in de drukke perioden of tijdens incidenten. Gebruik de rustige moment om kritisch naar de eigen securitymonitoringinrichting te kijken, nieuwe kennis op te doen, te oefenen en de actualiteit bij te houden. Internetcriminelen zijn namelijk voortdurend op zoek naar nieuwe manieren om hun aanvallen uit te voeren. Laat SOC-medewerkers daar continu hun aandacht op richten.

Verdere groei van het SOC

Een gevaar bij het te snel laten groeien van een SOC is dat meer informatie verzameld wordt dan het SOC verwerken kan.[5] Ook de ICT-servicedesk moet ingesteld zijn op het aantal meldingen dat een SOC bij hen indient. Stel, gebaseerd op de verwerkings-capaciteit van het SOC en de ICT-servicedesk, een grens aan wat precies verzameld wordt. Communiceer dit op een heldere manier richting de organisatie, zodat alle verwachtingen helder zijn. Ga met de directie in gesprek over het op een gecontroleerde manier laten groeien van het SOC en de ICT-servicedesk.

Een groter SOC betekent waarschijnlijk ook meer zaken waarop gemonitord wordt. In andere woorden: meer correlatieregels waarmee bepaald wordt of een ongewenste of afwijkende situatie zich heeft voorgedaan. Meer regels betekent meer onderhoud aan deze regels. Immers, iedere aangebrachte wijziging in een systeem of het netwerk, vereist mogelijk een wijziging in een of

[3] Zie hoofdstuk 8 uit https://www.jbisa.nl/download/?id=17700082

[4] Zie hoofdstuk 'Soorten SOC' uit https://www.pvib.nl/kenniscentrum/documenten/expert brief-security-operations-center-een-inrichtingsadvies

[5] https://www.computable.nl/artikel/nieuws/security/5901142/250449/security-operations-centers-worden-overspoeld.html

meerdere regels. Zorg dat het SOC daarop voorbereid is.

Een SIEM-systeem kan grote hoeveelheden informatie verwerken en daar met behulp van slimme en op maat gemaakte regels de juiste zaken uit halen. Bij een volwassen SOC zijn dat, naast de gebruikelijke technische controles, ook controles en zaken die dicht tegen de dagelijkse processen van de afdelingen aanzitten. Een valkuil hierbij is dat een SOC controles uitvoert die goed zijn voor een afdeling, maar weinig met informatiebeveiliging te maken hebben. Een SOC moet ervoor waken dat het bij al die controles bij zijn oorspronkelijke doel blijft en zich niet laat verleiden om een veredelde big-data-afdeling te worden voor de gehele organisatie.

Indien de organisatie beschikt over een Computer Security Incident Response Team (CSIRT), laat het SOC daar dan deel aan nemen. Vanuit het SOC kunnen de nodige technische gegevens geleverd worden die helpen bij het bepalen van de oorzaak van een incident en waar de eventuele aanval vandaan komt.

Om te zien hoe volwassen een SOC is, kan gebruik gemaakt worden van SOC-CMM[6]: het SOC Capability & Maturity Model. De ideeën uit dit model kunnen tevens gebruikt worden om een groeipad uit te stippelen of als checklist voor het inrichten van een SOC.

Tot slot

Een SOC is een goed middel om zicht te houden op de beveiliging van bedrijfsinformatie en digitale dreigingen, maar het inrichten ervan kost tijd, geld en moeite. Om een SOC tot een succes te maken, is het van belang dat het SOC op een gecontroleerde wijze meegroeit met de behoefte aan zicht en grip op informatiebeveiliging vanuit de organisatie.[7] Begin klein, maak de resultaten inzichtelijk voor de organisatie en gebruik een positieve ontvangst van deze resultaten als mogelijkheid voor een volgende stap in het groeiproces. Wees reëel in de planning, het groeipad en de invulling van een in te richten SOC. Besef daarbij: een SOC is een middel, geen doel

[6] https://www.soc-cmm.com/

[7] Voor aanvullende informatie, zie https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Mei 2023