TLP:GREEN

BESCHRIJVENDE TEKSTEN SOC-DIENSTEN

Monitoring & Detectie – HAVIK

Handreiking 1.1

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 supply-chain, 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. Vervolgens kan op basis van deze alarmen opvolging gegeven worden om mitigerende maatregelen te nemen. Dit soort diensten brengen organisaties veelal onder in een Security Operations Center (SOC).

Het is niet altijd opportuun om een Security Operations Center binnen de eigen organisatie in te richten. Als alternatief kan via een aanbestedingsprocedure een geschikte externe partij worden gezocht die dergelijke diensten voor uw organisatie verzorgt.

Met deze handreiking geeft VSSR u de beschikking over beschrijvende teksten van SOC-diensten. Deze teksten kunnen gebruikt worden in aanbestedingen die gericht zijn op het inkopen van SOC-diensten. De teksten uit dit document kunt u naar eigen inzicht hergebruiken en aanpassen om deze optimaal aan te laten sluiten op de behoeften van uw organisatie. Dit document dekt een breed spectrum aan SOC-diensten af. Niet elke organisatie zal alle diensten die in dit document beschreven zijn nodig hebben. Maak voorafgaand aan een aanbesteding inzichtelijk wat de specifieke behoeftes van uw organisatie zijn en richt uw aanbesteding alleen op die betreffende onderdelen.

Achtergrond

VSSR levert verschillende kennisproducten die gezamenlijk HAVIK vormen. HAVIK staat voor Handige Aanpak Voor Inkoop van Kwalitatieve SOC-diensten. Dit document is een onderdeel van HAVIK en biedt handvatten voor het beschrijven van monitoring- en detectiediensten in een aanbesteding.

Doelgroep

Senior management, operationeel management, 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	29-01-2025	Initiële versie
1.1	09-07-2026	Referenties geactualiseerd

1.2 Referenties

Document	Link
VSSR-kennisdocumenten	VSSR (ncsc.nl)

2 Inleiding

Het Security Operations Center (SOC) krijgt in toenemende mate een prominente rol in de digitale weerbaarheid 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 vaak bij een SOC zijn belegd. Het vaststellen wat een SOC precies zou moeten doen binnen de organisatie vaak een behoorlijke uitdaging.

Na het vaststellen van een goede definitie van wat een SOC voor uw organisatie moet gaan betekenen, is het noodzakelijk een keuze te maken in de wijze waarop u een SOC gaat inrichten. Een mogelijkheid is het met eigen mensen en systemen intern opbouwen van SOC. In het geval dat dit niet goed mogelijk of wenselijk is, kunt u (delen van) SOC-taken bij een externe partij onderbrengen. Overheidspartijen zijn verplicht om opdrachten waarvan de waarde een bepaalde drempel overstijgt volgens Europese aan te besteden. SOC-diensten zullen in vrijwel alle gevallen deze drempelwaarde overschrijven. Wij adviseren een expert op het gebied van aanbesteden te betrekken bij het inkopen van SOC-diensten. Deze kan u begeleiden bij het correct toepassen van wet- en regelgeving.

Om SOC-diensten goed aan te besteden, is het noodzakelijk om de gewenste dienstverlening goed te beschrijven. Dit document bevat concept dienstbeschrijvingen die u kunt gebruiken bij het opstellen van een aanbesteding. De dienstbeschrijvingen uit dit document kunt u als basis gebruiken waarbij u de beschrijvingen kan aanpassen aan uw specifieke situatie en behoefte.

De verschillende paragrafen in dit document geven beschrijvingen van dienstverlening die u mogelijk wilt afnemen bij een externe partij. Hierbij zullen onderdelen wel of niet van toepassing zijn. Maak een juiste selectie uit de beschikbare beschrijvingen en pas de teksten indien nodig aan zodat ze optimaal aansluiten op de behoefte van uw organisatie. Gebruik de andere producten van HAVIK om de uitvraag compleet te maken.

3 Beschrijving van de dienstverlening

3.1 Security Log Management

Security Log Management is een dienst die organisaties helpt bij het verzamelen, beheren en analyseren van informatiebeveiliging gerelateerde loggegevens. Het biedt gecentraliseerde mogelijkheden voor logboekbeheer en is ontworpen om organisaties te helpen voldoen aan wettelijke vereisten en hun beveiligingspropositie te verbeteren.

Security Log Management verzamelt loggegevens uit verschillende bronnen, waaronder netwerkapparaten, servers, toepassingen en clouddiensten. Vervolgens normaliseert en aggregeert het de gegevens en biedt het één uniforme weergave van de beveiligingslogs van een organisatie.

Als onderdeel van de aanbesteding is een assetoverzicht gepubliceerd. Dit Assetoverzicht omvat de aan te sluiten logbronnen. Na gunning zal Opdrachtnemer in samenspraak met Opdrachtgever afstemmen welke informatie uit deze logbronnen nodig is en hoe deze logbronnen worden aangesloten worden op de monitoringsystemen.

3.1.1 Koppeling

Opdrachtnemer verzameld de benodigde en relevante logdata bij Opdrachtgever via een centraal verzamelpunt dat bij Opdrachtgever is ingericht. Het centrale verzamelpunt verzorgt de koppeling naar de logbronnen van de te bewaken systemen en de verbinding naar de opslag en monitoringsystemen bij opdrachtnemer. Logdata wordt in eerste instantie altijd aangeleverd op basis van (één van de) standaard methoden die door de log bron wordt ondersteund. Het staat opdrachtnemer vrij om de logdata te converteren naar het formaat dat de log- en/of detectiesystemen nodig hebben voor een goede dienstverlening met inachtneming van de gestelde eis dat de oorspronkelijke data beschikbaar en overdraagbaar moet zijn (zie paragraaf “Data opslag”).

Opdrachtnemer realiseert de benodigde koppelingen met en verzamelpunt(en) in de ICT-infrastructuur van Opdrachtgever. Opdrachtnemer hanteert een aanpak waarbij de overlast voor Opdrachtgever tot een minimum beperkt blijft en de performance, continuïteit en veiligheid van de ICT-infrastructuur niet nadelig wordt beïnvloed.

Opdrachtnemer informeert Opdrachtgever op welke wijze de infrastructuur wordt opgezet en waar eventueel log agents nodig zijn. Dit gebeurt in overleg met Opdrachtgever zodat gezamenlijk kan worden bepaald of, waar en wanneer de installatie van log agents kan geschieden.

3.1.2 Data opslag

Opdrachtgever blijft te allen tijden eigenaar van de logdata. Logdata wordt minimaal in het oorspronkelijk formaat opgeslagen en wordt bij beëindiging van de overeenkomst aan opdrachtgever overgedragen. De dataretentie-eisen zijn in een bijlage door opdrachtgever gespecifieerd op basis van wet- en regelgeving en behoefte van de opdrachtgever. Opdrachtnemer hanteert deze normen en maakt melding indien er afwijkingen op de retentie eisen ontstaan. Bij het implementeren van de voorschriften voor dataretentie houdt opdrachtnemer rekening met het verwijderen van data. Opdrachtnemer zal op basis van de gestelde eisen data tijdig verwijderen. Opdrachtnemer wordt in staat gesteld om ook zelf de logdata te doorzoeken.

3.2 Managed Detection and Response

Managed Detection and Response (MDR) is de dienst waarmee Opdrachtnemer voorziet in het detecteren, onderzoeken en melden van verdachte situaties in de ICT-infrastructuur van Opdrachtgever en hiermee Opdrachtgever in staat te stellen hierop te reageren. Om aanwijzingen van een mogelijke aanval te identificeren, worden met MDR activiteiten op het ICT-landschap van Opdrachtgever gemonitord en geanalyseerd,. Als er iets verdachts wordt gedetecteerd, wordt direct actie ondernomen om de eventuele schade zoveel mogelijk te beperken. Opdrachtnemer draagt zorg voor de bewaking van het netwerk, triage van meldingen, het notificeren van de opdrachtgever en het bieden van duiding en handelsperspectief.

MDR valt in twee hoofdcomponenten uiteen: detecteren en reageren. Om MDR goed uit te kunnen voeren, maakt Opdrachtnemer gebruik van een aantal onderliggende diensten zoals in de bijbehorende sub-paragrafen is beschreven.

3.2.1 Detecteren

Monitoring betreft het continu observeren van het ICT-landschap (gebruikers, netwerk, infrastructuur, applicaties en data) met als doel het vaststellen van afwijkende en verdachte gedragingen. Dit gebeurt op basis van logdata uit het ICT-landschap en gespecialiseerde detectietechnologie. Bij vaststelling van verdachte gedragingen of patronen registreren de monitoringsystemen meldingen die opvolging ondervinden via de gespecificeerde diensten zoals beschreven in de sectie “Reageren”.

3.2.1.1 Netwerkdetectie

Network Detection and Response (NDR) is een dienst waarmee wordt voorzien in het detecteren van verdachte netwerkactiviteiten en het onderzoeken en melden van (mogelijke) hieruit voortkomende beveiligingsincidenten. Detectie wordt hier verder uitgewerkt, Response wordt verder behandeld in de Respond-sectie.

Netwerkdetectie omvat inspectie van het netwerkverkeer op verdachte gedragingen. Deze inspectie kan op verschillende plaatsen in het netwerk plaatsvinden. In ieder geval dient het netwerkverkeer geïnspecteerd worden tussen het netwerk van Opdrachtgever en het Internet. De detectie kan gebeuren op basis van probes/agents/sensoren die direct naar het netwerkverkeer kijken of op basis van logdata afkomstig van bestaande netwerkcomponenten zoals Intrusion Detection Systems, Firewalls, Proxy servers, etc. Een combinatie van deze toepassingen is ook mogelijk.

3.2.1.2 Endpoint-detectie

Een Endpoint Detection & Response (EDR) oplossing voorziet in continue bewaking en bescherming van componenten op het netwerk en het onderzoek, en melden van (mogelijke) hieruit voortkomende beveiligingsincidenten. Waar netwerkdetectie verkeerstromen in een netwerk bewaakt, bewaakt Endpoint-detectie de componenten die op een netwerk aangesloten zijn zelf. Elk apparaat dat verbinding maakt met het netwerk van Opdrachtgever is een EndPoint.

Detectie wordt hier verder uitgewerkt, response wordt verder behandeld in de Reageren-paragraaf. Tekenen van bedreigingen resulteren in acties om deze te verhelpen om verdere schade te beperken. Naast detecteren en voorkomen zorgt de EDR-oplossing ook voor het centraal registreren van de bevindingen zodat (mogelijke) incidenten worden opgemerkt en kunnen worden onderzocht. De EDR-oplossing biedt ook de mogelijkheid om op de te beschermen componenten handmatig en diepgaand incidentonderzoek uit te voeren.

3.2.1.3 User and Entity Behaviour Analytics

Op basis van informatie uit verschillende logbronnen bouwt de User and Entity Behaviour Analytics (UEBA) oplossing basisprofielen op van de entiteiten binnen de organisatie. Dit betreft gebruikers, end-points, IP-adressen en toepassingen. De oplossing zal verdachte activiteiten identificeren en dit registreren. Bevindingen worden centraal geadministreerd en waarbij verdachte situaties worden onderzocht en gemeld voor incidentafhandeling.

3.2.1.4 CTI-integratie

Voor een optimale werking van de verschillende detectiecomponenten wordt gebruik gemaakt van Cyber Threat Intelligence data integratie. Het gaat hierbij specifiek om de integratie van Indicator of Compromise (IOC) informatie zoals IP-adressen, domeinnamen, bestandhashes, url's, email adressen, etc. Voor CTI-integratie dient u minstens gebruik te maken van de IOC-feed die door het NCSC beschikbaar wordt gesteld. De hieruit voortkomende sightings (matches op IOC's) dienen te worden onderzocht waarbij het resultaat wordt vastgelegd. De vastgelegde resultaten dienen geautomatiseerd teruggekoppeld te worden aan het NCSC. Elders in deze aanbestedingsstukken zijn de technische/functionele eigenschappen van dit koppelvlak beschreven. Het staat u vrij om naast de aangeleverde data vanuit het NCSC ook eigen data te gebruiken als de kwaliteit van de dienstverlening hiermee is gebaat.

3.2.2 Reageren

Reageren betreft het direct opvolgen van security-meldingen die voortkomen uit detectiesystemen op basis van security-informatie verkregen uit de IT-infrastructuur, -assets en het applicatielandschap. Detectie geeft waarschuwingen zodra er verdachte gedragingen of patronen gesignaleerd worden. Reageren voorziet in de opvolging van de detectiemeldingen. Dit onderdeel valt uiteen in verschillende componenten zoals in de volgende paragrafen beschreven.

3.2.2.1 Registreren

Meldingen vanuit de detectiesystemen worden centraal vastgelegd zodat opvolging plaats kan vinden. Deze registratie gebeurt in een ticketsysteem van Opdrachtnemer. Het ticketsysteem is zodanig georganiseerd dat er een integraal overzicht is van tickets. Dit overzicht is ook voor Opdrachtgever beschikbaar en geeft inzicht in alle relevante informatie van het ticket, zowel met betrekking tot inhoud als proces (tijdstip, status, etc). Het ticketsysteem is zodanig ingericht dat indien gewenst Opdrachtgever en Opdrachtnemer gezamenlijk kunnen werken aan openstaande tickets. Vanuit het ticketsysteem wordt de status en voortgang geregistreerd, de opvolging bewaakt en zo nodig bijgestuurd. Daarnaast wordt het centrale registratiesysteem gebruikt voor reguliere evaluatie van de kwaliteit van opvolging en het voldoen aan de afspraken die betrekking hebben op afgesproken doorlooptijden van activiteiten.

De registratie wordt, binnen de gemaakte afspraken over service windows, continu gemonitord. Nieuwe meldingen worden op basis van gemaakte afspraken tijdig onderkend/vastgesteld (acknowledged) en toegewezen voor eerste analyse (triage). Zo wordt dus o.a. continue werkverdeling gedaan.

Opmerking: Als opdrachtgever een eigen ticketsysteem heeft, kan worden overwogen om integratie van de twee systemen op te nemen in de beschrijvingen en eisen.

3.2.2.2 Triage (1e-lijn analyse)

Direct nadat verdachte gedragingen, patronen of afwijkingen zijn opgemerkt, wordt een eerste analyse opgestart. Deze analyse gebeurt op een gestandaardiseerde manier. Doel van deze analyse is het bepalen of de detectie valide is en of er verder onderzoek nodig is. Zogenaamde "false positives" worden als zodanig gemarkeerd en gefilterd. Er wordt een eerste inschatting gemaakt van de ernst en het risico dat de melding mogelijk oplevert. Op basis van deze analyse wordt een prioriteit toegekend en bepaald of de melding verder onderzoek nodig heeft door Opdrachtnemer of direct kan worden gemeld bij Opdrachtgever. Meldingen bij Opdrachtgever vinden op een eenduidige en consistentie manier. Meldingen bevatten alle informatie en elementen die Opdrachtgever nodig heeft om adequaat verdere opvolging te geven.

3.2.2.3 Opvolging en melden (2e-lijn analyse)

Gedurende de triage is bepaalde welke meldingen verdere opvolging behoeven en welke niet. Voor meldingen die verdere opvolging behoeven start de Opdrachtnemer een opvolgingsonderzoek. Het opvolgingsonderzoek resulteert in duiding en handelingsperspectief voor Opdrachtnemer.

Na afronden van het opvolgingsonderzoek zal Opdrachtnemer melding doen bij Opdrachtgever en, voor zover van toepassing, bij instanties die door Opdrachtgever zijn aangewezen. De uitkomst van een onderzoek wordt op een gestandaardiseerde wijze vastgelegd en inclusief

handelingsperspectief gemeld aan Opdrachtgever. De procedure om meldingen te doen, wordt in de DAP vastgelegd en de snelheid waarmee melding plaats moeten vinden, ligt vast in het Service Level Agreement.

Opdrachtgever heeft een inspanningsverplichting om meldingen op te volgen en Opdrachtnemer terugkoppeling te verstrekken over de status en het oplossen/sluiten van meldingen. Indien opvolging door Opdrachtgever uitblijft, zal Opdrachtnemer enkele malen conform overeengekomen procedure rappelleren.

Indien opvolging uitblijft nadat Opdrachtnemer volgens de overeengekomen procedures en normen heeft gerappelleerd, mag Opdrachtnemer de melding uit het operationele proces halen (sluiten). Gesloten meldingen dienen met afhandelstatus in de periodieke rapportages terug te komen zodat het inzichtelijk is of en wanneer correcte opvolging is uitgebleven, het aantal meldingen waarvoor dit het geval is en de ernst van deze meldingen. Indien Opdrachtgever op een later moment alsnog opvolging geeft, worden de betreffende meldingen alsnog uit deze categorie weggehaald.

3.3 Kwetsbaarheden- en configuratiebeheer

Een kwetsbaarheid (volgens de NIS2 richtlijn) is een zwakheid, vatbaarheid of gebrek van ICT-producten of ICT-diensten die door een cyberdreiging kan worden uitgebuit. Rijksoverheidsorganisaties zijn via de BIO en de NIS2 gehouden aan het inrichten van beheer rondom kwetsbaarheden. Kwetsbaarhedenbeheer is het volledige proces dat resulteert in het identificeren, beoordelen, oplossen, verifiëren en rapporteren van kwetsbaarheden. De diensten zoals in deze sectie beschreven, hebben betrekking op een subset van het volledige proces gericht op identificeren, beoordelen, verifiëren en rapporteren van kwetsbaarheden.

Binnen de dienstverlening van deze opdracht maken we onderscheid in verschillende aandachtsgebieden te weten: External Attack Surface Management (EASM), kwetsbaarhedenbeheer met betrekking tot end user computing en kwetsbaarhedenbeheer op het interne netwerk. Voor deze aandachtsgebieden spitst de dienst zich toe op vier procesonderdelen uit de hierboven genoemde proces: identificeren, beoordelen, verifiëren en rapporteren.

Kwetsbaarheden kunnen ook ontstaan door configuratiefouten in applicaties, besturingssystemen, etc. Om configuratiefouten zoveel mogelijk te voorkomen, is het gebruikelijk om inrichtingsstandaarden te hanteren en daarbij regelmatig te controleren of omgevingen conform standaard zijn ingericht. Dit wordt in de regel Security Configuration Assessment genoemd. Dit onderdeel is hieronder als een afzonderlijke dienst benoemd.

3.3.1 External Attack Surface Management (EASM)

Het externe aanvalsoppervlak omvat alle ICT-componenten van een organisatie die aangevallen kunnen worden vanaf buiten de organisatie (veelal via het internet). Het aanvalsoppervlak van een organisatie bestaat uit alle toegangspunten die een aanvaller zou kunnen gebruiken om ICT-toepassingen binnen te dringen. Hoe groter het aanvalsoppervlak, des te meer inspanningen nodig zijn om dit te beschermen. En alles wat niet in beeld is, kan ook niet worden beschermd.

De dienstverlening in deze opdracht omvat het in kaart brengen van alle toegangspunten tot ICT-bedrijfsmiddelen met bijbehorende kwetsbaarheden en configuratiefouten (identificeren). De bevindingen worden geëvalueerd en geprioriteerd (beoordelen). De uitkomsten worden met Opdrachtgever gedeeld (rapporteren) zodat deze in staat is om deze op te volgen en op te lossen. Opdrachtgever zal aan Opdrachtnemer melden welke mitigerende maatregelen genomen zijn en op basis van deze terugkoppeling wordt van Opdrachtnemer verwacht controle uit te voeren op het resultaat van deze opvolging en hierover te rapporteren.

Opdrachtgever heeft een inspanningsverplichting om meldingen op te volgen en Opdrachtnemer terugkoppeling te verstrekken over de status en het mitigeren van de kwetsbaarheid. Indien opvolging door Opdrachtgever uitblijft, zal Opdrachtnemer enkele malen conform overeengekomen procedure en normen rappelleren.

Indien opvolging uitblijft nadat Opdrachtnemer volgens de overeengekomen procedures en normen heeft gerappelleerd, mag Opdrachtnemer de melding uit het operationele proces halen (sluiten). Dergelijke niet opgevolgde meldingen worden geregistreerd en in de periodieke rapportages inzichtelijk gemaakt.

3.3.2 Kwetsbaarhedenbeheer End-user Computing

Het verminderen van cyberrisico's vereist een uitgebreid, op risico's gebaseerd, beheer van beveiligingsproblemen op alle ICT-assets binnen een organisatie. Hierbij is het van belang zowel de ICT-assets zelf als ook kwetsbaarheden in ICT-assets te identificeren. Vervolgens is het noodzakelijk om gevonden kwetsbaarheden te evalueren en op te lossen.

Via deze dienst verzorgt Opdrachtnemer het periodiek in kaart brengen van assets en kwetsbaarheden, het evalueren van bevindingen, en het rapporteren hierover. Rapportages worden inclusief duiding en handelsperspectief voor kwetsbare assets opgeleverd. Opdrachtnemer adviseert Opdrachtgever bij het verhelpen van de bevindingen en bewaakt en rapporteert u over de opvolging (is de kwetsbaarheid opgelost?).

De scope van dit onderdeel betreft alleen End-user computing omgevingen waarbij het volstaat om een ICT-asset met een lokale agent uit te lezen.

3.3.3 Kwetsbaarhedenbeheer Intern Netwerk

Het verminderen van cyberrisico's vereist een uitgebreid, op risico's gebaseerd, beheer van beveiligingsproblemen om alle ICT-assets binnen een organisatie. Hierbij is het van belang zowel de ICT-assets zelf als ook kwetsbaarheden in ICT-assets te identificeren. Vervolgens is het noodzakelijk om gevonden kwetsbaarheden te evalueren en op te lossen.

Via deze dienst verzorgt Opdrachtnemer het periodiek in kaart brengen van assets en kwetsbaarheden, het evalueren van bevindingen, en het rapporteren hierover. Rapportages worden inclusief duiding en handelsperspectief voor kwetsbare assets opgeleverd. Daarnaast adviseert u de organisatie bij het verhelpen van de bevindingen en bewaakt en rapporteert u over de opvolging (is de kwetsbaarheid opgelost?).

De scope van dit onderdeel betreft alles behalve End-user computing waarbij het aandachtsgebied in de meeste gevallen voornamelijk datacentrum omgevingen zal betreffen. Voor deze dienstverlening is het van belang de ICT-assets zowel vanaf de buitenkant (communicatiepoorten en interfaces) onder de loep te nemen alsook lokaal te evalueren (bijvoorbeeld door het inloggen op een component met voldoende privileges om een volledige inventarisatie te doen, of met behulp van een lokaal geïnstalleerde agent die het component kan uitlezen).

3.3.4 Configuratiebeheer

Configuratiebeheer, of Security Configuration Assessment (SCA) kan worden afgenomen als dienst waarbij Opdrachtnemer periodiek een scan op de gehele ICT-infrastructuur uitvoert. Met het resultaat van deze periodieke scan krijgt Opdrachtgever inzicht in eventuele configuratiefouten en wordt in staat gesteld maatregelen te nemen om deze configuratiefouten weg te nemen. Voor deze dienst kan, indien gewenst en geschikt, gebruik worden gemaakt van software die voor kwetsbaarhedenbeheer wordt ingezet.

Naast de hiervoor bedoelde periodieke scans, kan Opdrachtnemer op verzoek ook gerichte scans uitvoeren. Dergelijke gerichte scans zullen vaak in het kader van hardening en compliancetesten gevraagd worden en gericht zijn op specifieke ICT-assets of delen van de ICT-Infrastructuur.

Voor het invullen van de dienstverlening scant Opdrachtnemer platformen op basis van security inrichtingsstandaarden en levert op basis hiervan gewenste rapportages aan Opdrachtgever. Uitgangspunt voor het scannen zijn gangbare marktstandaarden voor het inrichten van de beveiliging van platformen. Opdrachtgever kan minimaal scannen en rapporteren op basis van:

- CIS-controls: De meest recente en de op één na meest recente versie en op aanvraag op elke eerdere versie niet ouder dan vijf jaar.
- PCI-DSS: De meest recente versie en alle eerdere versies die resulteren in PCI-DSS compliance. Deze standaard is van toepassing indien Opdrachtgever betalingen met betaalkaarten verwerkt.
- NIST SP 800-53: De meest recente versie en op aanvraag oudere versies.

Opmerking: Naast deze gangbare standaarden kan door Opdrachtgever worden gevraagd om te scannen en rapporteren op basis van een eigen standaard van de Opdrachtgever.

3.4 Incident Response

Onder Incident Response (IR) wordt verstaan: het proces waarmee een organisatie omgaat met incidenten en de gevolgen van incidenten. Hierbij wordt op basis van een IR-plan op een gecoördineerde en gestructureerde wijze op incidenten gereageerd. Hierdoor wordt de impact van beveiligings-incidenten zoveel mogelijk beperkt door ze snel en efficiënt het hoofd te kunnen bieden.

Incident Response wordt veelal gedaan door gespecialiseerde teams zoals CSIRT en/of CERT teams. De benodigde expertise is niet altijd binnen elke organisatie (in voldoende mate) voorhanden. Om de juiste expertise op het juiste moment beschikbaar te hebben, stelt opdrachtnemer deze beschikbaar conform afspraken in het DAP, SLA en prijzenblad.

Om incidenten op de juiste wijze gevolg te geven, beschikt opdrachtnemer over kennis, processen en expertise om volgens internationale standaarden en best practices (bijv. NIST SP 800-61) het hoofd te kunnen bieden bij voorkomende situaties. Opdrachtnemer kan hierbij op voorhand aangeven aan welke randvoorwaarden opdrachtnemer moet voldoen om goed voorbereid te zijn voor incident- en crisissituaties als startpunt van een melding.

3.4.1 Incident Response op afstand

Om onverwachte situaties ten alle tijden op te kunnen vangen, stelt Opdrachtnemer een 24x7 dienst beschikbaar waarbij Opdrachtgever via een noodhulplijn altijd contact op kan nemen voor eerste hulp bij incidenten. Van Opdrachtgever wordt verwacht dat een eerste triage wordt uitgevoerd om snel en efficiënt vast te stellen wat de omvang en potentiële impact van het incident is. Op basis hiervan wordt in overleg vastgesteld wat de beste vervolgstappen zijn. Waar nodig kan Opdrachtnemer ondersteuning op afstand blijven bieden gedurende de looptijd van het incident.

3.4.2 Incident Response op locatie

Op basis van de eerste triage kan worden vastgesteld dat Opdrachtnemer ondersteuning op locatie wenst. Opdrachtgever faciliteert incident response op locatie en kan hierbij binnen drie (3) uur op locatie binnen Nederland aanwezig zijn. Op locatie geeft Opdrachtnemer op basis van de wens van Opdrachtgever ondersteuning of leiding aan het onderzoeken en oplossen van incidenten. Waar nodig is opdrachtnemer 24x7 beschikbaar tot het eind van het incident.

3.4.3 Forensisch onderzoek

In specifieke gevallen kan het nodig zijn diepgaand digitaal sporenonderzoek uit te voeren met als doel het verzamelen van juridisch houdbaar bewijsmateriaal. Opdrachtnemer is in staat om op forensische wijze digitale sporen en gegevens te verzamelen. Op basis van deze informatie kunnen gebeurtenissen worden gereconstrueerd. Digitale sporen worden op correcte forensische wijze veiliggesteld en geanalyseerd. De bevindingen worden in een heldere rapportage vastgelegd waarbij de rapportage geschikt is voor gebruiken als bewijsmateriaal in de rechtbank mocht opdrachtgever over willen gaan tot rechtsgang. De rapportage is daarnaast ook geschikt voor het

maken van melding bij andere officiële instantie zoals de Autoriteit Persoonsgegevens. Om deze dienstverlening goed te faciliteren, beschikt opdrachtnemer over alle noodzakelijke apparatuur en technische hulpmiddelen voor forensisch onderzoek.

3.5 Detectie use case-beheer en -ontwikkeling

Om de verschillende monitoring en detectie-diensten goed in te richten, beschikt Opdrachtnemer over een eigen set detectie use cases die is ontwikkeld op basis van de eigen kennis en ervaring van de Opdrachtnemer. Deze set is niet statisch en wordt op basis van een veranderend dreigingslandschap continu bijgewerkt en verbeterd. Twee maal per jaar wordt Opdrachtgever bijgepraat over de ontwikkeling van de detectie use case-bibliotheek met daarbij een vooruitblik op de voorziene ontwikkelingen op basis van een veranderend dreigingslandschap.

Naast de use cases van de Opdrachtnemer kan Opdrachtgever desgewenst eigen use cases op ad-hoc basis inbrengen voor ontwikkeling. Deze use cases kunnen op verschillende zaken betrekking hebben maar zullen veelal gerelateerd zijn aan organisatie specifieke risico-inschattingen die door Opdrachtgever worden gedaan. Bronnen hiervoor kunnen zijn:

- Overheid specifieke dreigingen die door instanties als NCSC worden gevoed;
- Red-team of pentest resultaten die in acute dreigingen resulteren;
- Dreigingsanalyses die resulteren in use cases die specifiek op Opdrachtgever van toepassing zijn.

Met uitzondering van de hiervoor bedoelde specifieke use cases, zal Opdrachtgever niet voorschrijvend optreden betreft de implementatie van de verschillende use cases. Opdrachtgever eist wel dat de use cases dekkend zullen zijn op een aantal relevante categorieën, te weten:

- Malware en ongewenste software detectie;
- Ransomware-detectie;
- Endpoint breach detectie;
- Identiteit-gerelateerd misbruik detectie inclusief authenticatie en autorisatie misbruik;
- Detectie van phishing-aanvallen;
- Detectie van dreiging die ontstaan uit internet browsing;
- Detectie op het misbruik maken van externe toegang of VPN-toegang;
- Detectie op het verkrijgen van oneigenlijke toegang tot web-diensten;
- Detectie op het misbruik maken van andersoortige generieke diensten zoals DNS (door opdrachtgever gespecificeerd in de bijlagen);
- Perimeter netwerkverkeer monitoring;
- Data(base) misbruik en ongeautoriseerde toegang detectie;
- Detectie op afwijkend interne netwerkcommunicatie;
- IoC-analyse op basis van de door Opdrachtgever geleverde IoC-data via NCSC.

Naast deze categorieën dient monitoring plaats te vinden op basis van normen en richtlijnen die voor Opdrachtgever van toepassing zijn zoals de BIO en NIS2/Cyberbeveiligingswet. Opdrachtgever anticipeert erop dat het dreigingslandschap continu veranderend.

Intellectueel eigendom van ad-hoc use cases op basis van input van de Opdrachtgever, blijft blij de Opdrachtgever. Daarbij dient de bijbehorende content aan Opdrachtgever overgedragen te worden.

3.6 Maatwerk

Opdrachtgever kan onder deze overeenkomst optioneel maatwerk afnemen bij Opdrachtnemer.

Het af te nemen maatwerk heeft altijd betrekking op SOC-dienstverlening en zal naar verwachting vooral van toepassing zijn bij security monitoring op niet-standaard applicaties, cloud-toepassingen, workloads en database.

Indien opdrachtgever maatwerk wenst af te nemen, dan zal Opdrachtgever voor aanvang van de werkzaamheden een offerteaanvraag bij Opdrachtnemer indienen. Op basis van deze aanvraag brengt Opdrachtnemer een offerte uit en specificeert hierin tenminste:

- De aangeboden producten en diensten;
- het aantal uren dat benodigd is om het maatwerk uit te voeren;
- het uurtarief gespecificeerde kosten van de aangeboden producten en diensten;
- de totaalprijs excl. BTW en;
- de voor realisatie benodigde doorlooptijd gerekend vanaf opdrachtverstrekking.

Opdrachtgever kan in de offerteaanvraag om aanvullende of meer specifieke informatie vragen. Opdrachtnemer zal trachten om deze aanvullende of meer specifieke informatie zo goed mogelijk te beantwoorden.

Voor personele inzet bij maatwerk hanteert Opdrachtgever altijd de van toepassing zijnde uurtarieven die in het prijzenblad van zijn Inschrijving zijn vermeld.

De doorlooptijd voor het uitbrengen van een offerte hangt sterk samen met de complexiteit van de vraag. Om die reden is in dit document geen eis opgenomen met betrekking tot de doorlooptijd om offertes uit te brengen. Richtinggevend hanteert Opdrachtgever een termijn van vijftien werkdagen voor het uitbrengen van een offerte na aanvraag.

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