Datum
10 augustus 2020

Ons kenmerk
(10)(2g)

Contactpersoon
(10)(2e)

Telefoon
+31 (10)(2e)

E-mail
(10)(2e)@kpn.com

Ministerie van Volksgezondheid, Welzijn en Sport
(10)(2e)
Parnassusplein 5,
2511 VX 's Gravenhage

KPN aanbod: SOC / SIEM CoronaMelder Security omgeving

Geachte (10)(2e),

Hierbij ontvangt u naar aanleiding van uw aanvraag voor de SOC/SIEM dienstverlening van de applicatie CoronaMelder van KPN B.V. het aanbod voor de SOC / SIEM CoronaMelder Security.

Deze offerte hangt onlosmakelijk samen met de offerte van de extra servers in de hostingomgeving CoronaMelder van KPN BV t.b.v. de SOC/SIEM dienstverlening met referentienummer (10)(2g) (10)(2g)

Hebt u vragen met betrekking tot dit aanbod, belt u dan met uw (10)(2e), (10)(2e) (10)(2e), bereikbaar op (10)(2e), of met uw (10)(2e) (10)(2e), bereikbaar op (10)(2e).

Wij vertrouwen erop u hiermee een passende oplossing aan te bieden en zien met veel belangstelling uit naar uw reactie.

Met vriendelijke groet,

(10)(2e)

(10)(2e)
(10)(2e)
KPN B.V.

Aanbod: SOC / SIEM CoronaMelder

Security omgeving

Aanbod voor	:	Ministerie van Volksgezondheid, Welzijn en Sport, (10)(2e)
Uitgebracht door	:	(10)(2e) KPN B.V.
Bereikbaar op	:	(10)(2e) , (10)(2e) @kpn.com
Plaats en datum	:	Houten, 10 augustus 2020
Referentienummer	:	(10)(2g)
Referentienummer VWS	:	Geen

Inhoudsopgave

1.	**Uw vraag**	**4**
1.1	Scope	4
2.	**Onze oplossing**	**6**
2.1	Aanpak voorlopige planning	6
2.2	Uitgangspunten dienstverlening KPN	13
3.	**Onze werkwijze**	**13**
3.1	Samenvatting werkzaamheden	13
3.1.1	Activiteiten KPN	13
3.1.2	Activiteiten VWS	14
3.2	Deliverables	14
3.3	Planning	14
4.	**Uw investering**	**15**
4.1	Eenmalige investering	15
4.2	Toekomstige maandelijkse kosten	15
4.3	Financiële uitgangspunten	15
5.	**Voorwaarden**	**16**
5.1	Algemene voorwaarden	16
6.	**Bedrijfsinformatie opdrachtgever**	**17**
7.	**Bevestiging van de opdracht**	**18**

1. Uw vraag

Dit document beschrijft het voorstel voor de security dienstverlening ten behoeve van de managed hosting van de CoronaMelder App voor het ministerie van VWS - CIBG (vanaf nu: VWS).
Voor de Corona Melder App zijn een aantal onderdelen van belang:

- De backend
- De App
- De CDN
- De security en compliancy conform BIO
- De SOC-dienstverlening

Dit document focust op het voorstel voor de security SOC / SIEM dienstverlening – Fase 1.

1.1 Scope

1. Schaalbaarheid en snelheid, om de gevraagde oplossing goed en op afspraak te kunnen leveren aan de klant VWS is het van belang dat KPN van te voren een duidelijk beeld krijgt van wat er geleverd dient te worden.
2. Beschikbaarheid van de logging. Nog niet alle logging zal aanwezig zijn op het moment van opstarten van het project. KPN kan op dit moment nog niet voorzien wanneer alle logging beschikbaar zal zijn en hoe deze bruikbaar zullen zijn.
3. Overvloed aan informatie bij opleveren SIEM systemen. Door gefaseerd in te voeren kan KPN samen met de klant steeds de aanwezige informatie delen en bespreken. Uitvoering is als volgt: We leveren de rapportages en IOC's geautomatiseerd aan naar een portal waar de klant/Cloud.NL deze zelf kan inzien, en halen deze realtime informatie op en verwerken deze vervolgens in een dashboard voor de klant/Cloud.NL. Op deze manier is er geen information overflow.

De omgeving zal voor de klant VWS bestaan uit een drietal niveaus en componenten als het gaat om logging, deze componenten staan voor een deel in de Cloud.NL omgeving (Platform & Back-end) en voor een deel bij KPN Broadcast (CDN).

1. Platform met daarin de servers onder de back-end en de dedicated firewall. Totaal 57 logbronnen bestaande uit 45 windows machines, 10 Linux Machines en een Cisco Firewall met IDS functionaliteit. Deze bronnen / logging zal aangesloten worden in Fase1.
2. De logging van de back-end zelf. Dit wordt beschouwd als een applicatie logging en daarvan heeft KPN een sample nodig. Op basis van de inhoud van de logging zal de inzetbaarheid bepaald worden en zal er mogelijk een of meerdere parsers moeten worden geschreven. Deze bronnen / logging aangesloten worden in Fase 2.
3. Het CDN platform zal zijn eigen logging aan moeten leveren aan KPN Security. Op het moment van schrijven van dit document is er contact tussen de betreffende afdelingen om te kijken welke logging er geleverd kan en mag worden. (Privacy vs Security). Deze bronnen / logging zal in Fase 3 aangesloten worden.

De correlatie van deze gegevens vind plaats in de centrale monitoring omgeving van KPN Security dat specifiek wordt ingericht op het binnenhalen van events, deze correleren naar verdachte zaken en worden aangeleverd aan een klant specifieke portal en dashboard. De drie belangrijkste componenten staan hieronder kort beschreven.

Naast de technische inrichting van de dienst dient tevens in elke fase de service en Governance ingericht te worden. Onderdelen hiervan zijn onder andere het inrichten van het portaal, inrichting van ServiceNOW dat binnen KPN gebruikt wordt voor het proces met oplosgroepen, klantenteam en de Enterprise Service Desk, inrichting van kennis artikelen, het opstellen van een communicatie matrix en de inrichting service management organisatie.

2. Onze oplossing

2.1 Aanpak voorlopige planning

Planning fase1

KPN heeft een detail overleg gehad met Cloud.NL over wat er gezamenlijk gebouwd dient te worden en ziet er als volgt uit:

- 28 & 29 juli 2020 – HLD & LLD overleg met Cloud.NL, geen blocking issues in het design.
- 30 juli 2020 – LLD (detail design) gemaakt door KPN Security (15 uur bespreking met Cloud.NL, daarna Resources claimen binnen Cloud.NL. Indien akkoord start bouwen omgeving).
- 7 augustus 2020 – Opleveren omgeving door Cloud.NL (Cloud.NL).
- 21 augustus 2020 – Opleveren Security omgeving inclusief VSED (KPN Security).
- 28 augustus 2020 – Opleveren SIEM en Use Cases fase 1 (KPN Security).

Nog onder voorbehoud planning fase2 en in overleg met VWS.

- September 2020 – Detail planning na analyse back-end logs en vaststellen extra use cases met CISO en klant.

Nog onder voorbehoud planning fase3 en in overleg met VWS.

- Oktober 2020 – Detail planning na analyse CDN logs en vaststellen extra use cases met CISO en klant.

De Logcollector (VSED) in de Cloud.NL Omgeving

Het Virtuele Security Edge Device ((V)SED) is een unit die geplaatst zal worden in de Cloud.NL omgeving. Het is feitelijk een virtuele server met daarin een virtualisatie laag die op een efficiënte manier Log Collectie en Log Managment faciliteert. Hierop worden de logbronnen aangesloten zoals die in de uitvraag **Fase 1** zijn beschreven. Het betreft hier de volgende bronnen:

- De Cisco Firepower Firewall met IDS
- Windows Servers 45 stuks
- Linux Servers 10 stuks

Bovenstaande logbronnen worden bij levering van **Fase 1** bij het plaatsen van de VSED aangesloten op deze VSED. De loggegevens worden vervolgens doorgestuurd naar het centrale platform en daar opgeslagen op basis van een ElasticSearch stack. De ElasticSearch stack zorgt voor een snelle en betrouwbare dataopslag en de mogelijkheid deze te doorzoeken. De Events off Interest die nodig zijn voor het laten afgaan van de "Use Cases" worden voor verdere verwerking getagd en doorgestuurd voor correlatie in de SIEM omgeving. De SIEM omgeving is op basis van IBM QRadar on Cloud (Qrock) uitgevoerd en wordt gehost in Frankfurt binnen de EER. De data opslag bevind zich in een KPN datacenter binnen NL.

SIEM & Use Cases

Binnen de SIEM omgeving worden de verderop in deze paragraaf genoemde "Use Cases" actief gemaakt als onderdeel van de oplevering van **Fase 1**. Voor de keuze van dit pakket is de volgende analyse en onderbouwing meegenomen in dit document.

Het netwerk heeft een omgeving per OTAP straat. Voor **Fase 1** is het advies van KPN Security om ons te focussen op alleen de productie omgeving. Dit omdat er geen productie data aanwezig is in de OTA omgevingen. Zou één van de OTA omgevingen gecompromitteerd worden dan heeft dit minder risico dan wanneer de productie gecompromitteerd wordt.

Voor het advies is er gekeken van buiten naar binnen van zowel de omgeving alsmede de infrastructuur. Op basis daarvan weten we welke Use Cases er nu aangeboden kunnen worden vanuit onze 80 best practice Use Cases set die qua doorlooptijd het snelst ingeregeld kan worden.

KPN heeft voor deze specifieke case de volgende zaken beschouwd:

Perimeter

- Distributie server naar CDN (controle op data verkeer naar niet toegestane adressen vanuit de distributie server).
- Verkeer vanuit WWW (mobiele app & browser) kan gemonitord worden op misdragingen (scan gedrag).
- De IDS module monitort al op de inhoud van de netwerk stromingen. We kunnen alerting doorzetten via SIEM/SOC voor actievere opvolging wanneer er een bepaalde signaturen gevonden is. (bijvoorbeeld alle criticals).

Interne netwerk

- Verkeer monitoren tussen API & Database server. (er zouden geen directe verzoeken op de Database server gedaan mogen worden).
- Verkeer monitoren tussen beheer server en de omgeving. Alle authenticaties bijvoorbeeld op het netwerk moeten afkomstig zijn van de beheer omgeving.
- Eventuele nog andere communicatie patronen die vast staan en niet mogen afwijken (navraag hiervan kan gedaan worden bij netwerk beheerders).

Hosts

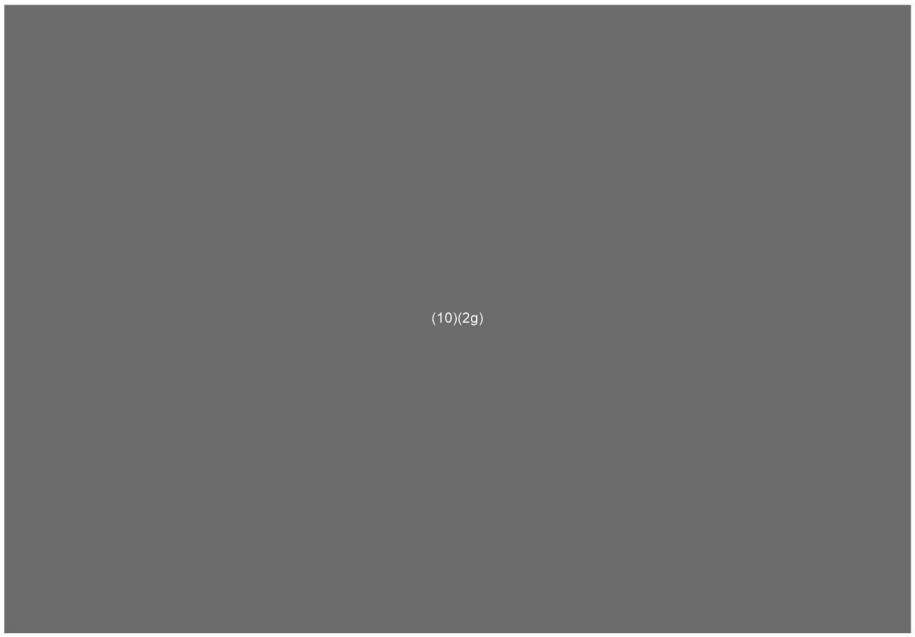
- Het monitoren van inlogpogingen vanaf de beheer server in het algemeen op alle servers. Zo om te constateren op misdragingen van een account. (Scope hiervan is wel alleen de authenticatie op de OS).

Eventuele verbeteringen

Kijken naar de SQL logging (errors) om onder andere HTML verzoeken op niet bestaande pagina's te constateren.

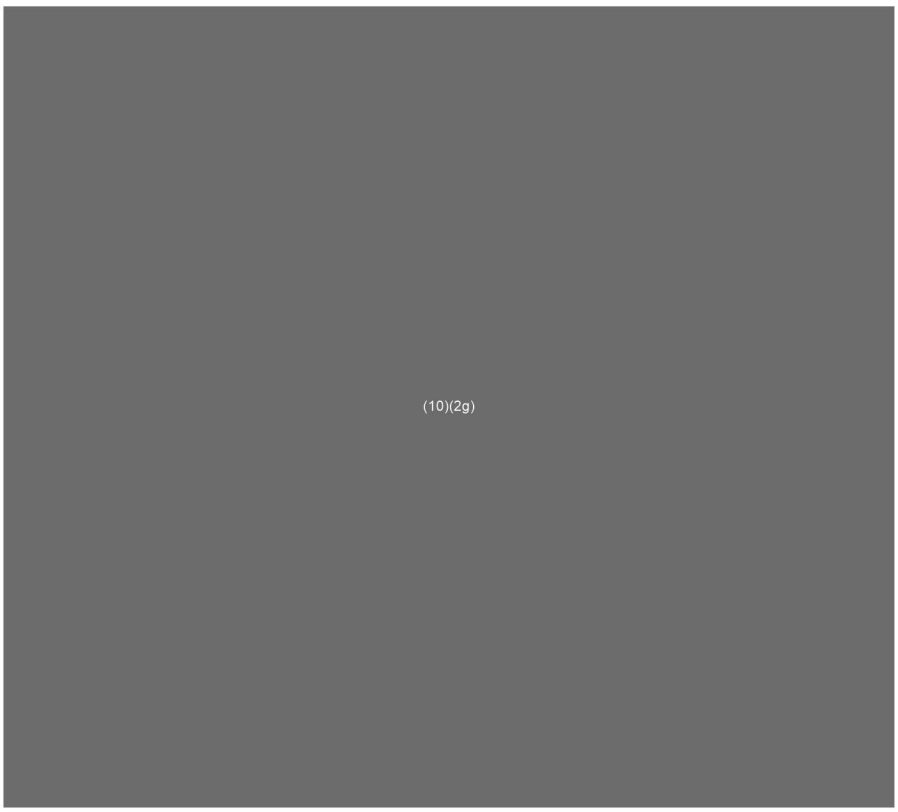
Overig advies

De dienst is Monitoring & Alerting. De klant/oplosgroep dient opvolging te doen als er iets geconstateerd is.


(10)(2g)

Voorgestelde use cases

Op basis van de analyse van de logbronnen en de omgeving stelt KPN security voor om fase 1 op te leveren met de onderstaande use cases:

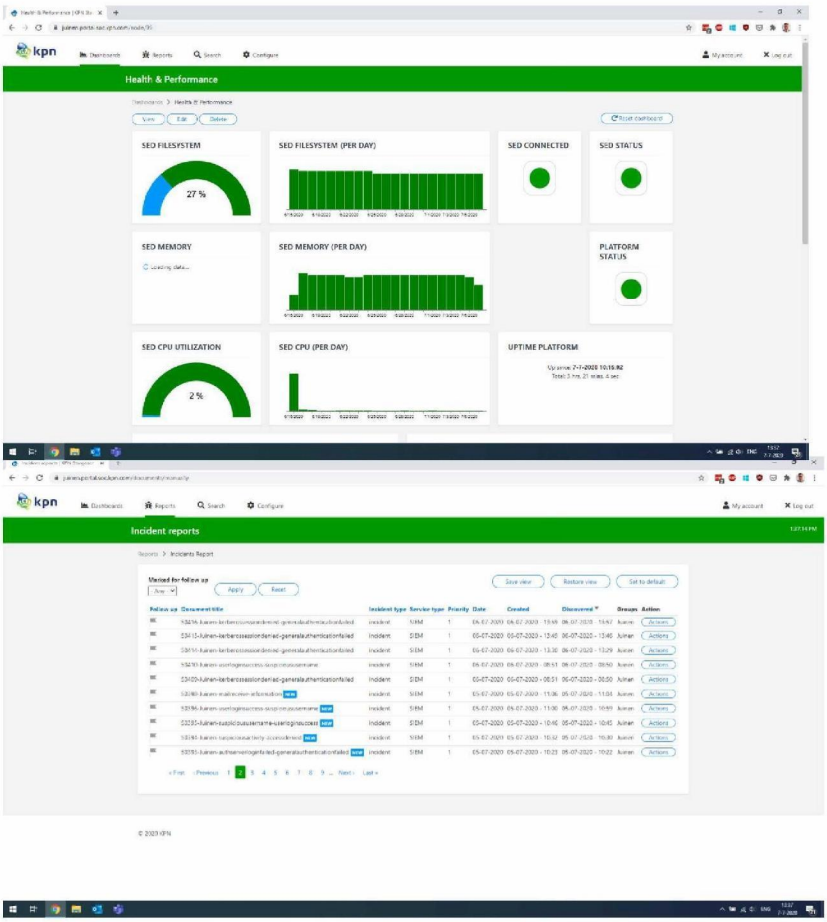


Op basis van deze use cases genereert het systeem drie zaken:

- Data om de Dashboards te vullen en een Realtime beeld de geven van de security status van de klant.
- Rapportages waarin de output van de use cases op een duidelijke en overzichtelijke wijze wordt weergegeven en Security Incidenten.
  De rapportages worden direct op de portal van de klant geplaatst, de incidenten gaan volautomatisch door naar het Incident Response Platform (IBM Resilient) waarin er een check plaats vind of het geen false positive is. Hierna wordt het incident verrijkt op basis van Threat Intell en indien nodig ge-upgrade naar een Indicator of Compromise (IOC).
- Deze IOC wordt dan op de portal van de klant geplaatst en kan er desgewenst actie worden ondernomen en/of een oplosgroep worden aangestuurd.

De klant portaal

Communicatie met de klant en/of oplosgroep vindt plaats via een portaal. Hier worden alle relevante zaken gepost zodat de communicatie op een goede en veilige manier kan plats vinden. De portal is voor elke klant afgeschermd met behulp van two factor authenticatie. Onderstaand als voorbeeld een twee tal screenshots:



2.2 Uitgangspunten dienstverlening KPN

Uitgangspunten waarmee KPN rekening houdt in deze offerte:

De volgende aannames zijn gemaakt en ook afgestemd met VWS:

- Er zijn geen specifieke certificeringseisen.
- In de eerste twee weken van augustus 2020 dient de hostingomgeving en bijbehorende dienstverlening opgeleverd te worden. De security dienstverlening dient hierop aan te sluiten en zo snel mogelijk hierna te worden ingericht.

Projectmanagement:

- Beschikbaarheid van resources van VWS voor het project moet zijn geborgd.
- De opdrachtgever stelt een contactpersoon aan voor de interne aansturing bij VWS en communicatie binnen VWS.
- VWS is verantwoordelijk voor het voeren van de overall project governance.
- VWS stelt een testplan op waarmee acceptatie testen worden uitgevoerd ter acceptatie van de (deel)oplevering.
- VWS voert de acceptatietesten binnen een week na (deel)oplevering uit en tekent deze daarna af.

3. Onze werkwijze

3.1 Samenvatting werkzaamheden

3.1.1 Activiteiten KPN

KPN verricht de volgende werkzaamheden:

- Projectmanagement.
- Resourcemanagement.
- Opzetten van de projectadministratie.
- Afstemmen van de projectactiviteiten met VWS.
- Protocol van Oplevering en facturatievoorbereiding.
- Dagelijkse aansturing.
- Projectvergaderingen voorbereiden en bijwonen.
- Aanbieden Acceptatie testen ter goedkeuring VWS.

3.1.2 Activiteiten VWS

VWS verricht de volgende werkzaamheden:

- Voeren van de overall project governance.
- Opstellen testplan.

3.2 Deliverables

Tijdens de uitvoering worden navolgende deliverables opgeleverd:

- Security dienstverlening, zoals gespecificeerd.

3.3 Planning

Voorlopige oplevering: 28 augustus 2020

4. Uw investering

4.1 Eenmalige investering

Onderstaand vindt u een overzicht van de door u te maken investering.

(10)(1c)

4.2 Toekomstige maandelijkse kosten

Onderstaand treft u de maandelijkse tarieven aan voor de CoronaMelder hostingomgeving.

(10)(1c)

4.3 Financiële uitgangspunten

- De kosten vallen onder hostingomgeving CoronaMelder maar zijn excl. de Hostingomgeving uitbreiding. Zie offerte KPN met referentie (10)(2g)
- De prijzen zijn conform de DFA met uitzondering van specifieke dedicated security dienstverlening.
- De contractduur van de NOK bedraagt 12 maanden, met optie tot verlenging. Gezien de investeringen in dedicated security die door KPN worden gedaan, is het niet mogelijk voor VWS om dit contract tussentijds te beëindigen.

5. Voorwaarden

5.1 Algemene voorwaarden

Op deze offerte is de overeenkomst betreffende de uitbesteding van Managed Hosting & Storage Services met kenmerk-201700274.068 welke op 16 mei 2017 is afgesloten tussen Ministerie van Volksgezondheid, Welzijn en Sport - CIBG, IGZ en ESTT en KPN BV (ARBIT-2016) van toepassing. De contractduur van de NOK bedraagt 12 maanden, met optie tot verlenging. Gezien de investeringen in dedicated security die door KPN worden gedaan, is het niet mogelijk voor VWS om dit contract tussentijds te beëindigen.

Deze offerte hangt onlosmakelijk samen met de offerte van de extra servers in de hostingomgeving CoronaMelder van KPN BV t.b.v. de SOC/SIEM dienstverlening met referentienummer (10)(2g)

(10)(2g)

Betaling
Netto, binnen 30 dagen na factuurdatum.

Geldigheid
De geldigheidsduur van deze offerte is zestig (60) dagen, en onder voorbehoud van typefouten.

Tarieven
Exclusief BTW.

Facturatiemomenten eenmalige kosten
100% per type omgeving (O, T, A, P) bij oplevering van dit type omgeving. De eenmalige kosten worden op basis van de werkelijk bestede uren gefactureerd.

Facturatie maandelijkse kosten
De maandelijkse kosten van de nieuwe hostingomgeving worden gefactureerd vanaf technische acceptatie door VWS van de geleverde dienstverlening.

6. Bedrijfsinformatie opdrachtgever

Opdrachtgever (bedrijfsnaam)	: Ministerie VWS
Straat en huisnummer	: Parnassusplein 5
Postcode / Plaats	: 2511 VX 's Gravenhage
KvK- nummer	: 50000535

7. Bevestiging van de opdracht

Plaats en datum:
Namens VWS, gevestigd te 's-Gravenhage,
met KvK-nummer 50000535

Naam:

Functie:

Plaats en datum: Houten 10 augustus 2020
Namens KPN B.V., gevestigd te Rotterdam
met KvK-nummer 27124701

(10)(2e)

(10)(2e)