COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

# Marktconsultatie Detectie en Respons

Security monitoring en incident respons voor de zorgsector

| | |
|---|---|
| Auteur | Rob van Os |
| Datum | 16.02.2023 |
| Versie | Definitief |
| TLP | CLEAR |

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Z-CERT

# Inhoud




**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09

info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

# Achtergrond

## Inleiding

Stichting Z-CERT is gestart met een traject om security monitoring voor de zorgsector vorm te geven. Daarbij is gekozen om deze dienstverlening op vrijwillge basis aan deelnemers van Z-CERT ter beschikking te stellen via managed security service providers, die de kennis en kunde aan boord hebben om kwalitatief goede diensten te kunnen leveren. Met dit document nodigen wij u uit om deel te nemen aan de marktconsultatie.

De marktconsultatie is voor Z-CERT en deelnemers uit de zorgsector een manier om te toetsen of de huidige ideeën over security monitoring dienstverlening kloppen en beter inzichtelijk te krijgen op welke manier de huidige markt voor security monitoring dienstverlening aansluit op de wensen en profielen binnen de zorg. Deze marktconsultatie is dan ook een uitnodiging om uw ideeën over de best passende dienstverlening met ons te delen. Dan kan zijn over de invulling van de dienst, maar ook over de vormgeving van het proces van aanbesteding.

De Request for Proposal (RfP) fase Is de volgende fase van dit traject. Momenteel is de planning om in het 2e kwartaal (april 2023) te starten met het RfP traject. Aan deze planning kunnen geen rechten ontleend worden. Afhankelijk van de uitkomsten van deze marktconsultatie kan de planning aangepast worden, of besloten worden om het vervolgtraject niet in te gaan.

## Doelstellingen

Met deze marktconsultatie wil Z-CERT het volgende bewerkstelligen:

1. Een beeld krijgen van de marktpartijen op het gebied van security monitoring en respons
2. Een beeld krijgen van hoe deze dienstverlening aansluit op de vraag vanuit de sector
3. De deelnemers informeren over het aanbod vanuit marktpartijen
4. Goed geïnformeerd een besluit kunnen nemen over het vervolgtraject
5. De kwaliteit voor een eventueel volgende Request for Proposal te verhogen
6. Een selectie te kunnen maken van partijen die het meest geschikt worden geacht voor de volgende fase van deze uitvraag.

## Over Z-CERT

Z-CERT is een afkorting van Computer Emergency Response Team voor de zorgsector. Met andere woorden: Bij Z-CERT werken cybersecurity-experts die helpen om zorginstellingen digitaal veilig te houden. Dagelijks speuren de eerstelijns security-specialisten van Z-CERT diverse bronnen af naar dreigingen voor de zorgsector. De zorgorganisaties zijn zelf verantwoordelijk voor de beveiliging van hun digitale systemen, maar als het misgaat kan Z-CERT te hulp schieten. Om die reden wordt Z-CERT ook wel de ‘digitale brandweer van de zorgsector’ genoemd.

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

## Zorgspecifieke kennis

De tweedelijns support bestaat uit security-specialisten die nauw samenwerken met het security-netwerk van Z-CERT. Zij analyseren binnengekomen dreigingsinformatie en vertalen dit naar de zorgsector. Deze specialisten hebben specifieke kennis van zorggerelateerde ICT-systemen.

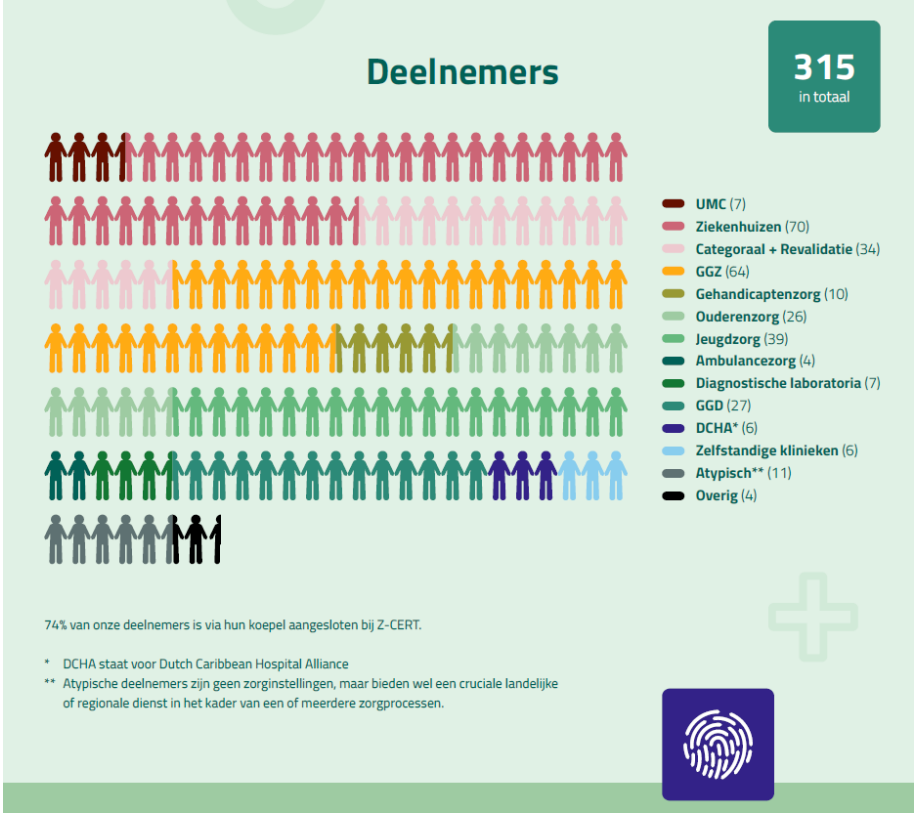
Het team van Z-CERT bestaat verder uit directeur Wim Hafkamp, business consultants, office management en een communicatieadviseur.

## Sinds 2017

Z-CERT is opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU), de Nederlandse GGZ (GGZ) en het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Z-CERT is een stichting zonder winstoogmerk. In januari 2020 is Z-CERT aangewezen als computer emergency response team voor de gehele zorgsector (Wet beveiliging netwerk- en informatiediensten).

## Deelnemers

Z-CERT heeft op moment van schrijven van deze marktconsultatie 315 deelnemers, als volgt verdeeld:




Z-CERT kan geen uitspraak doen over het percentage deelnemers wat nu of in de toekomst gebruik zal maken van de security monitoring dienstverlening.

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

## Voorgenomen scope

Voor deze marktconsultatie wordt security monitoring als primaire dienst gevraagd, met als doel het detecteren van security incidenten binnen zorgpartijen om deze adequaat op te kunnen volgen. Deze opvolging vindt plaats in de vorm van security incident respons. Aanbieders moeten in staat zijn om advies te leveren over adequate opvolging en daarin samen te werken met security incident respons teams binnen een zorgpartij. Ook de samenwerking met Z-CERT in incident response is een belangrijke component. Tenslotte verwachten veel partijen meer dan alleen een leverancier van monitoring en respons, maar een security partner die samen met hen optrekt om het niveau van beveiliging continu te verbeteren.

## Bijlagen

Dit document kent 2 bijlagen:

1. Antwoordformulier
2. Profielen zorgpartijen

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

# Procedure

## Procedure en spelregels

Deelname aan de marktconsultatie is geheel vrijblijvend. Wel geldt dat op basis van de marktconsultatie een aantal partners gekozen zal worden waarmee een volgende stap gezet wordt richting de volgende fase waarin concrete voorstellen en contractering zullen geschieden.

Er kunnen geen rechten aan deze marktconsultatie ontleend worden. Kosten die gemaakt worden door marktpartijen om een beantwoording in te sturen kunnen niet verhaald worden op Z-CERT. Ook inhoudelijk kunnen geen rechten ontleend worden aan de marktconsultatie in het verdere verloop van het traject.

Hierna volgen enkele bepalingen. Door deel te nemen aan de marktconsultatie gaat u akkoord met deze bepalingen. Indien een marktpartij zich niet houdt aan de hier gestelde bepalingen zal deze gediskwalificeerd worden van verdere deelname aan het traject.

## Contactpersonen en communicatie

Communicatie zal primair via email plaatsvinden. Voor vragen of ander contact betreffende deze marktconsultatie kunt u contact opnemen met robvanos@z-cert.nl. U krijgt binnen 3 werkdagen antwoord.

Ook zal er gelegenheid zijn om een sessie te boeken met Z-CERT over de inhoud van de marktconsultatie. Hiervoor zijn momenten beschikbaar op de volgende dagen:
- Donderdag 23 februari
- Maandag 27 februari
- Donderdag 2 maart
- Maandag 6 maart
- Donderdag 9 maart

Voor deze data worden momenten in de ochtend (10.00 - 12.00) en in de middag (14.00 - 16.00) ter beschikking gesteld. U kunt per email 2 werkdagen van te voren een moment reserveren. Per marktpartij wordt 1 uur beschikbaar gesteld voor een interactieve sessie.

## Werkwijze

De marktconsultatie wordt gepubliceerd op de site van Z-CERT. Aankondigingen van de marktpublicatie worden zo breed mogelijk in de markt gezet. De marktconsultatie bestaat uit een schriftelijke beantwoording van de vragen. Voor deze beantwoording is een template beschikbaar gesteld in Word formaat. Het template kan meegestuurd worden als bijlage bij de beantwoording.

Na afronding van de uitvraag kunnen partijen gevraagd worden om een mondelingen toelichting te geven op hun antwoorden. Deze mondelinge toelichting zal plaatsvinden in de week van 13 tot en met 19 maart. Marktpartijen wordt

gevraagd ruimte in hun agenda te houden op **maandag 13 maart** en **donderdag 16 maart** voor een eventuele mondelinge toelichting. Ook aan het participeren in een mondelinge toelichting kunnen geen rechten ontleend worden. Z-CERT bepaalt zelf met welke partijen een mondelinge toelichting aangegaan wordt.

## Eindrapport

Op basis van de Ingezonden informatie wordt een eindrapport opgesteld voor de marktconsultatie. Daarin zullen geaggregeerde antwoorden van de deelnemende marktpartijen terug te vinden zijn. Het document wordt door Z-CERT gebruikt om verder vorm te geven aan het RfP traject, in nauwe samenwerking met een aantal zorgpartijen.

## Tijdslijnen

De tijdslijnen voor de marktconsultatie zijn als volgt:

1. Publicatie marktconsultatie: 16 februari
2. Uiterlijke datum voor respons: 10 maart
3. Mondelinge toelichting beantwoording: of 16 maart
4. Publicatie samenvatting marktconsultatie: uiterlijk 27 maart
5. Go/No-go moment voor RfP fase: 30 maart
6. Start RfP fase: Q2 2023
7. Start contractering: Q3 2023

## Vertrouwelijkheid

Alle aan Z-CERT ingestuurde informatie ten behoeve van beantwoording van de marktconsultatie wordt vertrouwelijk behandeld. Indien na het 'Go/No-go' moment de RfP gestart wordt, wordt de informatie ingezonden door partijen die niet geselecteerd zijn om te participeren in de RfP vernietigd.

## Taal

De voertaal in deze marktconsultatie is Nederlands. Marktpartijen dienen dan ook in de Nederlandse taal de beantwoording in te sturen.

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

# Dienstbeschrijving

De informatie in dit document is nog onderhevig aan verdere besluit- en ideevorming. Wij nodigen u uit om uw ideeën over de beste invulling van de in deze marktconsultatie beschreven uitvraag met ons te delen. Daarmee kunnen we een zo goed mogelijk resultaat bereiken in de volgende fase.

## Gevraagde dienst

De dienstverlening die gevraagd wordt is een security monitoring en respons dienst, ondersteund door een Security Operations Center (SOC) waar analyse van informatie plaatsvindt en incidenten gedetecteerd, gecontextualiseerd en geprioriteerd worden om tot een effectieve opvolging te komen. De security monitoring en respons dienst dient monitoring op basis van logging te ondersteunen, alsmede logging op basis van componenten op werkstations en servers (endpoint detection & response, EDR). Tenslotte is monitoring van het netwerk een pre, maar geen vereiste.

## Scope

De volgende werkzaamheden behoren bij de dienstverlening:
- Het uitvoeren van security monitoring op basis van security informatie verkregen uit de IT infrastructuur en het applicatielandschap
- Het analyseren van afwijkende gebeurtenissen in de infrastructuur
- Het uitvoeren van initiële incident respons door het contextualiseren en prioriteren van events en het leveren van advies voor opvolging
- Het aansluiten van nieuwe logbronnen
- Het adviseren over welke logbronnen ontbreken in de monitoring
- Het monitoren van de status van logbronnen en verzorgen van alerts indien logbronnen niet langer informatie aanleveren
- Het rapporteren over de kwaliteit en performance van de dienst
- Het continu verbeteren van de security monitoring dienstverlening voor klanten
- Het ontwikkelen van nieuwe use cases die specifiek zijn voor de klant of sector
- Het delen van operationele informatie met Z-CERT en/of het ZDN
- Het monitoren van relevante kwetsbaarheden en dreigingen en deze te delen met dienstafnemers en Z-CERT
- Het, op basis van bevindingen uit de monitoring, doen van aanbevelingen ter verbetering van de beveiliging van dienstafnemers

## Criteria

De dienstverlening moet tenminste voldoen aan de volgende eisen:
- De data in dienstverlening moet verwerkt worden binnen de EU, conform AVG/GDPR
- De dienstverlener moet tenminste 2 jaar ervaring hebben met 24/7 security monitoring dienstverlening
- De dienstverlener moet bereid zijn om actief informatie te delen en samen te werken met Z-CERT

Deze criteria zijn knock-out criteria. In de RfP fase kunnen additionele knock-out criteria van toepassing zijn.

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

## Mantelovereenkomst

Omdat Z-CERT herkent dat niet alle zorgpartijen hetzelfde zijn, zal ook niet elke dienstverlener voldoende passend kunnen zijn. Om zorginstellingen te voorzien van de meeste flexibiliteit zal gewerkt gaan worden met een mantelcontract waarin een aantal partijen is opgenomen. Zorginstellingen kunnen vervolgens zelf een keuze maken uit de partijen. het aantal partijen in de mantelovereenkomst is nader te bepalen en mede afhankelijk van de uitkomst van de marktconsultatie. Om de balans tussen complexiteit en flexibiliteit voor de zorgpartijen te behouden is het de verwachting dat dit minimaal 3 en maximaal 5 partijen zullen zijn. Daaraan kunnen echter geen rechten ontleend worden.

## Rol van Z-CERT in de dienstverlening

Z-CERT wil als partij op de hoogte zijn van wat er in de sector en bij de aangesloten partijen gebeurt op het gebied van informatiebeveiliging. Z-CERT onderhoudt daarvoor een actieve relatie met zowel de zorgpartij als de dienstleverancier. Zorgpartijen zijn voor Z-CERT sparringpartners en daarmee zowel afnemer als bron van relevante dreigingsinformatie uit de sector. Z-CERT wil actief op de hoogte gehouden worden van observaties van dreigingen in geselecteerde use cases. Ook wil Z-CERT graag indicatoren van aanvallen ontvangen die voortgekomen zijn uit security analyse en/of security incident respons. Specifiek is daar aandacht voor Tools, Technieken en Procedures (TTPs) van de aanval en concrete indicators of compromise (IoC)s, zoals IP adressen, domeinen, emailadressen, etc. De TTPs worden gebruikt voor verdere analyse en berichtgeving richting de sector, de IoCs worden gebruikt voor delen in het zorg detectie netwerk (ZDN). Z-CERT voorziet ook een rol in incident management en (coördinatie van) incident response, met name wanneer aanvallen bij meerdere partijen in de sector gezien worden.

Tenslotte wil Z-CERT graag meedenken en technische kennis leveren voor het ontwikkelen van applicatie specifieke use cases gebaseerd op risico's die geconstateerd worden in de sector.

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

# Vragen over de dienstverlening

In deze marktconsultatie willen wij graag antwoord krijgen op de volgende onderwerpen:

- Wat is de meest passende dienstverlening voor de verschillende profielen?
- Wat is de visie van het bedrijf ten aanzien van monitoring?
- Op welke manier wordt vormgegeven aan detectie en respons (in mensen, processen en techniek)?
- Hoe wordt gezorgd voor een passende en kwalitatief hoogwaardige dienstverlening?

Voor de beantwoording van deze vragen is een aparte template beschikbaar gesteld (bijlage 1).

**1. Vragen over het bedrijf (bedrijfsprofiel)**

A. Hoe lang bestaat het bedrijf?

B. Is het bedrijf in Nederland gevestigd?

C. Worden klanten bediend in de Nederlandse voertaal?

D. Beschikt het bedrijf over relevante certificeringen (zoals ISO27001, ISO9001, NEN7510, enzovoorts)? Zo ja, welke certificeringen zijn dat?

E. Is er een bedrijfsprofiel beschikbaar? Zo ja, deze graag meesturen.

**2. Vragen of het SOC (SOC profiel)**

A. Hoe lang voert u al security monitoring en respons dienstverlening uit?

B.1 Hoeveel klanten heeft het SOC?
B.2 Welke sectoren bedient het SOC? Specificeer het aantal klanten per sector.
B.3 Hoe groot (aantal werkplekken) zijn de klanten?

C.1 Op welk volwassenheidsniveau acteert het SOC?
C.2 Op welke manier wordt deze volwassenheid vastgesteld?

D. Hoe zou u de gemiddeld klant van het SOC beschrijven?

E. Heeft u klanten (bij voorkeur uit de zorg) die als referentie kunnen optreden?

**3. Vragen over het SOC personeel**

A.1 Uit hoeveel FTE bestaat het SOC?
A.2 Hoe zijn de FTEs verdeeld over de verschillende functies (inclusief tiers) binnen het SOC?

B. Wat is het gemiddelde verloop van het personeel?

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972

C. Wat is uw strategie voor het aantrekken en behouden van security talent?

D.1 Hoe wordt vormgegeven aan kennismanagement binnen het SOC?
D.2 Hoe wordt kennis van de klanten en kennis van het cyber speelveld geborgd en gedeeld binnen het SOC?

E. Welke trainingen dient het SOC personeel te volgen, en/of welke certificeringen dienen behaald te zijn / worden?

F. Welke screening wordt toegepast op SOC personeel?

**4. Vragen over de dienstverlening**

A. Heeft u reeds ervaring met het uitvoeren van security monitoring in de zorg? Zo ja: om hoeveel klanten gaat het, welke profielen en hoe lang?

B. Voert u 24/7 dienstverlening? Zo ja: op welke manier wordt vormgegeven aan de 24/7 dienstverlening?

C. Welke rol speelt threat intelligence in de dienstverlening?

D. Welke rol speelt automatisering in de dienstverlening?

E. Wat zijn volgens u de meest relevante cyber risico's voor de zorgsector?

F. Wat zijn de aansluiteisen om succesvol aan te kunnen sluiten op de dienstverlening?

G.1 Hoe ziet het onboarding proces er uit voor nieuwe klanten?
G.2 Welke informatie is nodig om de onboarding efficiënt en effectief te laten verlopen?
G.3 Hoe veel tijd neemt het onboarden in beslag? En waar is dat afhankelijk van?
G.4 Is er een wachtrij voor onboarding? Zo ja: hoe lang is deze wachtrij?

H. Is de dienstverlening voldoende schaalbaar om de instroom vanuit de zorgsector goed te kunnen bedienen?

I.1 Op welke manier wordt invulling gegeven aan incident respons proces binnen de dienstverlening?
I.2 Wat is volgens u nodig (in proces en technologie) om incident escalatie effectief en efficiënt te laten verlopen? En wat wordt daarbij verwacht van de dienstafnemer (kennis, kunde, beschikbaarheid, etc.)?

J. Hoe faciliteert u de overgang naar een andere monitoring dienstleverancier of een intern SOC?

K. Welke voertaal wordt gebruikt in de communicatie naar de klanten? Dit betreft zowel operationele communicatie (events en incidenten) als tactisch / strategische communicatie (gesprekken over de dienstverlening tussen leverancier en afnemer).

**5. Vragen over de detectiestrategie en visie**

A. Op welke manier wordt vorm gegeven aan gelaagde detectie voor de dienstafnemers?

B.1 Welke technologieën worden gebruikt om security monitoring mee uit te voeren?
B.2 Wordt de detectie-technologie als cloud-native oplossing aangeboden?
B.3 Worden dezelfde technologieën gebruikt voor alle profielen, of wordt daar onderscheid in gemaakt (bijvoorbeeld uit oogpunt van kostenefficiënte monitoring)? Zo ja, op welke manier wordt dit onderscheid gemaakt?
B.4 Hoe wordt detectie uitgevoerd in omgevingen waar overwegend Microsoft gebruikt wordt?

C.1 Welke technieken worden gebruikt om de benodigde security informatie te verzamelen in de infrastructuur en van applicaties?
C.2 Bent u in staat om uw security monitoring processen aan te sluiten op bestaande security monitoring technologie (zoals een SIEM systeem) die binnen een organisatie al uitgerold is?

D.1 Op welke manier wordt actief gevalideerd dat detecties werken zoals bedoeld?
D.2 Op welke manier wordt zorg gedragen dat het aantal false-positive meldingen naar dienstafnemers beperkt blijft?

E.1 Op welke manier wordt de coverage van detecties ten opzicht van bekende aanvalstechnieken vastgesteld?
E.2 Hoe wordt zorggedragen voor verbetering van deze coverage?
E.3 Welke rol spelen bestaande (preventieve) security maatregelen hierin?

F.1 Welke ontwikkelingen ziet u in de markt of het gebied van (de detectie van) cyber aanvallen?
F.2 Op welke manier zal detectie volgens u gaan ontwikkelen om in te spelen op de veranderende markt?

**6. Vragen over SOC processen**

A.1 Op welke manier wordt continue verbetering toegepast binnen het SOC?
A.2 Is er gereserveerde capaciteit voor het doorontwikkelen van de detectie dienstverlening? Zo ja, licht toe.

B.1 Op welke manier wordt de kwaliteit van de dienstverlening geborgd?
B.2 Welke rol wordt daarin verwacht van de partij waar de dienstverlening aan geboden wordt?

C. Op welke manier wordt gezorgd dat de dienstverlening aansluit bij de wensen, risico's en IT inrichting van de klant?

D. Wat is uw invulling van security partnerschap in een detectie en respons dienstverlening?

E.1 Op welke manier wordt over de dienst gerapporteerd?
E.2 Kunt u een voorbeeld meesturen van een SOC rapportage?
E.3 Op welke manier wordt interactie met de klant over de dienst vormgegeven?

**7. Vragen of het samenspel tussen dienstleveranciers, dienstafnemer en Z-CERT**

A. Op welke manier kan Z-CERT het beste op de hoogte gehouden worden van de belangrijkste informatie uit de security monitoring zodat Z-CERT haar functie richting de sector goed kan uitvoeren?

B. Op welke manier kan Z-CERT betrokken worden in het incident respons proces richting de dienstafnemers?

C. Bent u in staat om (geautomatiseerd) indicatoren van aanvallen te delen binnen het zorg detectie netwerk (ZDN)?

**8. Vragen over de prijsstelling**

A.1 Welk kostenmodel gebruikt u voor het berekenen van de kosten voor de dienstverleningen?
A.2 Welke vaste en variabele componenten zitten in dit model?
A.3 Is het model van toepassing op alle profielen organisaties of wordt daar onderscheid in gemaakt? Zo ja, welk onderscheid is dat?

B. Zijn er additionele kosten binnen de dienst van toepassing? Bijvoorbeeld voor het aansluiten van niet-standaard componenten en het realiseren van niet-standaard use cases.

C. Op welke manier wordt zorg gedragen voor een kosteneffectieve en risico-gedreven security monitoring en respons?

**9. Vragen over privacy en dataopslag**

A.1 Werkt u met een standaard verwerkersovereenkomst?
A.2 Bent u bereid om de verwerkersovereenkomst van de dienstafnemer te tekenen?

B. Waar wordt de data voor de dienstverlening opgeslagen?

C. Hoe wordt veilige toegang tot data voor de dienstverlening geborgd?

D. Hoe lang wordt de data bewaard?

**10. Vragen over de mantelovereenkomst**

A. Bent u bereid om uw diensten in een mantelovereenkomst met meerdere andere partijen aan te bieden?

B. In de mantelovereenkomst worden de volgende zaken contractueel vastgelegd:
- dienstenniveaus
- bewerkersovereenkomst
- inkoopvoorwaarden
- algemene voorwaarden
- prijsstelling / prijsmodel
- duur van de overeenkomst
- opzegging en gevolgen van vroegtijdige opzegging
- toekenning opdrachten

- uitvoering opdrachten
- intellectueel eigendom
- aansprakelijkheid

1. Welke hierboven niet genoemde zaken horen volgens u ook nog in de mantelovereenkomst?
2. Welke van hierboven genoemde zaken horen volgens u niet in de mantelovereenkomst? Licht toe

**11. Toelichting**

A. Bent u bereid uw antwoorden mondeling toe te lichten als daar behoefte aan is?

B. Op welke manier wenst u op de hoogte gehouden te worden van de uitkomst van deze marktconsultatie?

**12. Ten slotte**

A. Heeft nu nog aanvullende opmerkingen aangaande deze marktconsultatie?

**Stichting Z-CERT**
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
**KvK** 67374972