COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

# Bijlage 2 - Profielen zorgorganisaties

Behorende bij *Marktconsultatie Detectie en Response, 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

# Inleiding

Dit document is een bijlage voor de marktconsultatie *detectie en respons, security monitoring en incident respons voor de zorgsector*. In dit document staan de profielen die zijn opgesteld om verschillende typen zorgorganisaties te kunnen onderscheiden. Doel van het document is om meer inzicht te geven in de aan te sluiten partijen. U kunt dit document gebruiken om beter invulling te geven aan uw antwoorden op de vragen die gesteld zijn in de 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

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

# Profielen

Voor de realisatie van de SOC dienstverlening voor de zorgsector zijn verschillende profielen van toepassing. Deze profielen geven een vereenvoudigde beschrijving van zorgpartijen die gebruikt kunnen worden voor het vaststellen van een geschikte dienstverlening.

Voor de dienstaanbieder zijn de profielen van belang om een security monitoring aanbieding te kunnen doen die in verhouding staat met de klant. Een security dienstverlening die is ingericht op klanten met een volwassen security aanpak en interne kennis en kunde rondom de infrastructuur, zal niet effectief kunnen functioneren bij klanten die dit niet hebben. Dan is de mismatch tussen de aangeboden dienst en de eisen die deze stelt aan de afnemers te groot. Vice versa is dat ook zo: een hoog volwassen zorgpartij zoekt een security partnership op gelijkwaardig niveau.

In dit document worden 3 profielen uiteengezet. Deze profielen zijn deels geënt op volwassenheidsniveaus, maar nemen een iets andere invalshoek. De volgende profielen worden behandeld:

- **Profiel 1**: ad-hoc security
- **Profiel 2**: gedefinieerde security
- **Profiel 3**: aantoonbare security

Onderstaande figuur toont hoe deze profielen zich verhouden tot de CMMI volwassenheidsniveaus:


Voor elk van de profielen wordt hierna uiteengezet welke kenmerken ze hebben, welken dienstverlening in grote lijnen het meest passend is, welke relevante use cases er voor het profiel zijn en welke rol Z-CERT heeft ten aanzien van de security monitoring voor organisaties met het betreffende profiel.

**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

# Profiel 1: ad-hoc security

## Beschrijving

Een zorgpartij op niveau *ad-hoc security* kenmerkt zich doordat deze op een weinig gestructureerde en herhaalbare manier omgaat met (de security van) IT middelen. Er is een sterke afhankelijkheid van externe leveranciers voor het beveiligen en op orde houden van de IT middelen.

## Kenmerken

Kenmerken van dit profiel zijn de volgende:

- Met name gebruik van (public) cloud middelen, weinig diversiteit tussen deelnemers
- Relatief eenvoudig IT landschap, niet veel diversiteit. Zo min mogelijk apparatuur op locatie
- Weinig eigen IT capaciteit
- Ad-hoc security functie
- Grote afhankelijkheid van leveranciers, weinig regie
- Weinig kennis binnen de organisatie
- Relatief weinig  awareness binnen de organisatie
- Geen eigen security incident respons capability

## Passende dienstverlening

De meest passende dienstverlening is een standaard SOC dienstverlening gericht op het totaal ontzorgen van de klant. De dienstleverancier moet comfortabel zijn met het samenwerken met de IT partner van de organisatie voor het (laten) onderzoeken van security alarmen. Tijdens de onboarding van ad-hoc security zorgpartijen dient de SOC dienstleverancier het voortouw te nemen in de technische realisatie. Dat geldt zowel voor het aansluiten van logbronnen als het veilig versturen van de logging van de zorgpartij naar de leverancier.
Naast security monitoring moet de aanbiedende partij ook een incident respons dienst kunnen aanbieden die de klant kan ondersteunen bij incidenten.

## Relevante use cases

Relevante use cases voor dit profiel zijn:

- Ongeautoriseerde toegang tot cloud resources
- Fouten in de cloud configuratie
- Phishing
- Brute force aanvallen
- Malware in het algemeen, ransomware in het bijzonder

## 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. Zodoende ontvangt Z-CERT relevante informatie van de dienstverlener over een aantal geselecteerde use cases. Daarnaast wordt Z-CERT op de hoogte gesteld van grote incidenten.

**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

# Profiel 2: gedefinieerde security

## Beschrijving

Een zorgpartij op niveau '*gedefinieerde security*' kenmerkt zich door het gebruik van standaarden en een gestructureerde inrichting van security. Dit profiel heeft vaak een regievoerende rol in het informatiebeveiligingsproces. Daarbij zijn de verantwoordelijkheden voor security beschreven en belegd. Een security manager of CISO zorgt voor de regie op security en beleid voor informatiebeveiliging.

## Kenmerken

Kenmerken van deze organisatie zijn de volgende:

- Gebruik van public en private cloud middelen
- Hybride opzet van cloud middelen en IT apparatuur op locatie
- Eigen IT beheer
- IT ingericht conform standaarden en best practices
- Aantal vaste leveranciers, structureel management van leveranciers
- Beleid voor security aanwezig en actief uitgedragen
- Security awareness bij alle IT personeel
- Security verantwoordelijkheid belegd
- Security vaak als vaste extra taak binnen bestaande rollen
- Beperkte of geen eigen security incident respons capability

## Passende dienstverlening

De meest passende dienstverlening is een SOC dienstverlening die gericht is op de samenwerking met de zorgpartij, en het helpen van de zorgpartij om een hoger niveau van volwassenheid en standaardisatie te bereiken. Advies voor verbetering van de inrichting van de IT bij de zorgpartij is daarbij een belangrijke component.
Tot de diensten die passen bij dit profiel hoort security monitoring en incident response. Daarnaast kan de dienstenleverancier ook bijdragen door het actief delen van informatie over bekende kwetsbaarheden en het identificeren van mogelijk tekortkomingen in de IT inrichting op basis van informatie uit de security logging. Denk daarbij bijvoorbeeld aan openstaande netwerkpoorten, maar ook ontbrekende of onvoldoende sterke authenticatie en encryptie methoden.

## Relevante use cases

Relevante use cases voor dit profiel zijn:

- Ongeautoriseerde toegang tot cloud infrastructuur
- Ongeautoriseerde toegang tot de infrastructuur
- Misbruik accounts
- Phishing
- Brute force aanvallen
- Verkrijgen van verhoogde (domein) privileges
- Toegang tot kern systemen
- Malware in het algemeen, ransomware in het bijzonder

**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

# Profiel 3: aantoonbare security

## Beschrijving

Een zorgpartij op niveau '*aantoonbare security*' kenmerkt zich doordat er op een zeer gestructureerde en zorgvuldige wijze omgegaan wordt met security. De security awareness binnen de gehele organisatie is hoog en er is een team binnen de organisatie dat zich volledig richt op het continu verbeteren van security. Daarnaast is aandacht voor de meetbaarheid en aantoonbaarheid van security.

## Kenmerken

Kenmerken van dit profiel zijn de volgende:

- Eigen uitvoering IT
- Complex landschap met grote variëteit aan IT apparatuur
- Actief management van- en regie op IT leveranciers
- (Sterk) gesegmenteerd netwerk
- Security specialisten aanwezig, soms een multidisciplinair security team
- NEN gecertificeerd, of daar actief mee bezig
- Strategisch management en beleid voor security aanwezig, actieve sturing op naleving
- Security awareness bij alle personeel, zowel IT als zorg
- Eigen security incident respons capability
- Mogelijkheid tot verwerken van *indicators of compromise*
- Duidelijke wensen rondom security monitoring, in sommige gevallen ook behoefte aan gesegmenteerde security monitoring met meerdere dienstleveranciers

## Passende dienstverlening

De meest passende dienstverlening is een SOC dienstverlening waarbij veel oog is voor de individuele omgeving van de klant. Een breed palet aan diensten, met security monitoring, incident respons, threat intelligence en eventueel threat hunting is passend voor dit profiel.
Voor security monitoring geldt dat een grote diversiteit aan logbronnen aangesloten dient te worden, maar dat geldt evenzogoed voor de realisatie van organisatie-specifieke use cases. Wat betreft incident respons zal de focus met name liggen op het ondersteunen van- en samenwerken met het interne incident respons team bij grote incidenten waar bijzondere expertise nodig is, die binnen het interne team niet voorhanden is.
Organisaties met dit profiel verwachten van een dienstverlener meer dan alleen een partij die een security monitoring dienst levert, maar vooral een partij die proactief de samenwerking zoekt en als volwaardige security partner kan optreden, ook bij grote incidenten. Daarbij speelt de kwaliteit van de geleverde diensten, die regelmatig geëvalueerd wordt, een grote rol.

## Relevante use cases

Relevante use cases voor dit profiel zijn:

- Ongeautoriseerde toegang tot cloud infrastructuur
- Ongeautoriseerde toegang tot de infrastructuur
- Data exfiltratie

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

- Phishing
- Interne scanning
- Verkrijgen persistente toegang
- Opzetten command & control kanaal
- Laterale interne beweging
- Verkrijgen van verhoogde (domein) privileges
- Toegang tot kern systemen
- Malware in het algemeen, ransomware in het bijzonder
- NEN7510/7513 use cases
- Organisatie-specifieke use cases

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