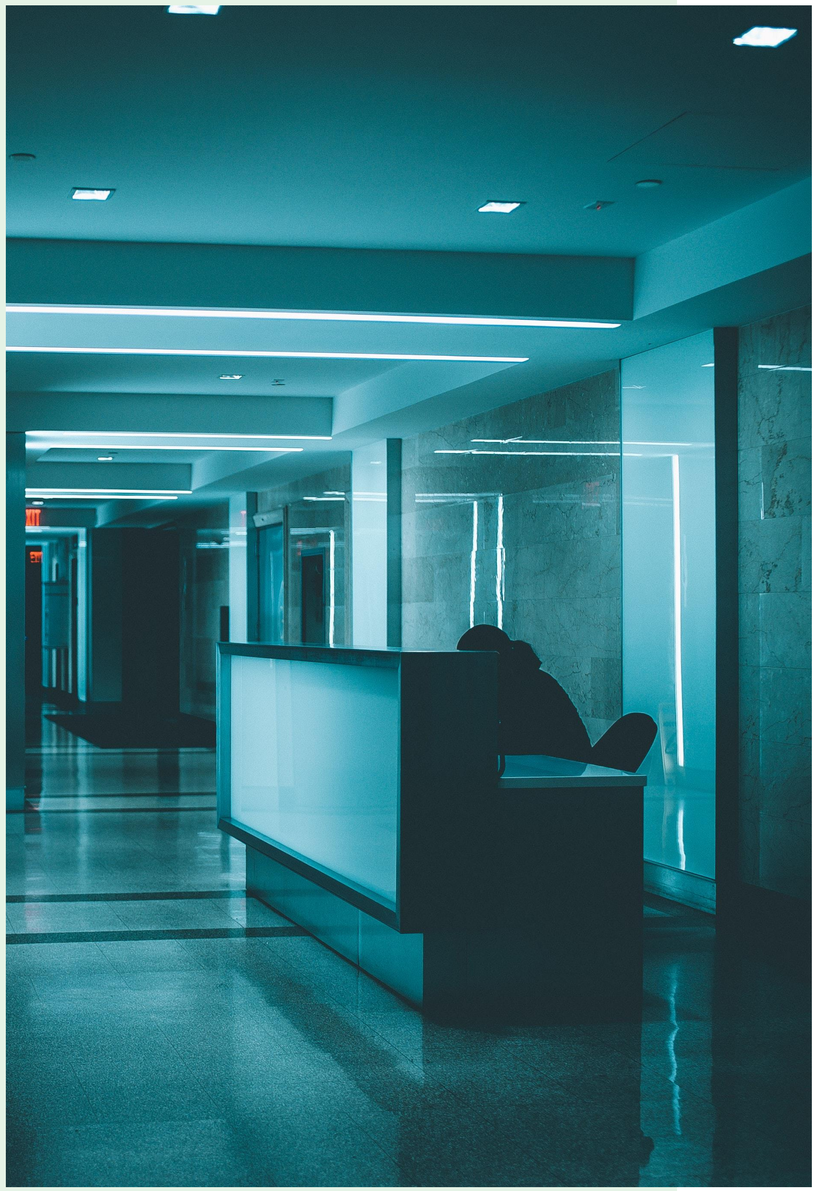
TLP:GREEN

Dienstverlening Z-CERT & Dreigingsbeeld voor de zorg 2024

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG



Onderwerpen

- Dienstverlening Z-CERT
- Dreigingsbeeld 2024
- Praktijk

Stichting Z-CERT

Over ons

1 juni 2017

Oprichting

60 Medewerkers

Care en cure, 1e lijn, GGD en acute zorg

350 Deelnemers

Private stichting

Geen winstoogmerk

Treden niet marktverstorend op

Financiering

Subsidie vanuit VWS

Deelnemersvergoedingen

Hét CERT voor de zorg

Wettelijk takenpakket NIS2

Groei naar 1500-2000 deelnemers en 70 collega's

Diensten Z-CERT

Informatieberichten en alarmering

Z-CERT ontvangt informatie van het NCSC, andere (inter-) nationale CERTS, leveranciers en eigen bronnen.

Kennisdeling

Z-CERT nodigt haar deelnemers uit om actief kennis te delen over hun aanpak van cybersecurity en waargenomen dreigingen. En maakt, samen met deelnemers, kennisproducten. Bijvoorbeeld rondom Opleiden Trainen en Oefenen!

Monitoring (en nu ook scannen) IP-adressen en domeinnamen

Z-CERT controleert elke dag of IP-adressen en domeinnamen van deelnemers op blocklists of in data breaches voorkomen.

Afhandeling en coördinatie incidenten

Wanneer een deelnemer te maken heeft met een incident, adviseert Z-CERT bij de aanpak en het oplossen van het incident. Tevens kan Z-CERT 24/7 ondersteuning bieden bij de communicatie en coördinatie

Aanvullende diensten

Zorg Detectie Netwerk (ZDN)

Deelnemers kunnen kiezen voor een aansluiting op het ZDN. Het ZDN deelt realtime ‘indicators of compromise’ met deelnemers. Deze informatie vormt een collectief geheugen voor digitale dreigingen met als doel een weerbare zorgsector.

15

Aantal aangesloten security partners

Het ZDN wordt door Z-CERT met actuele dreigingsinformatie gevoed vanuit haar nationale en internationale bronnen. Aansluiten is mogelijk via een virtuele appliance, een MISP-server of een SOC-leverancier.

Coordinated Vulnerability Disclosure (CVD)

Kwetsbaarheden in websites van deelnemers en in (medische) apparatuur of programmatuur, die door derden zijn ontdekt, kunnen bij Z-CERT worden gemeld.

TLP:GREEN

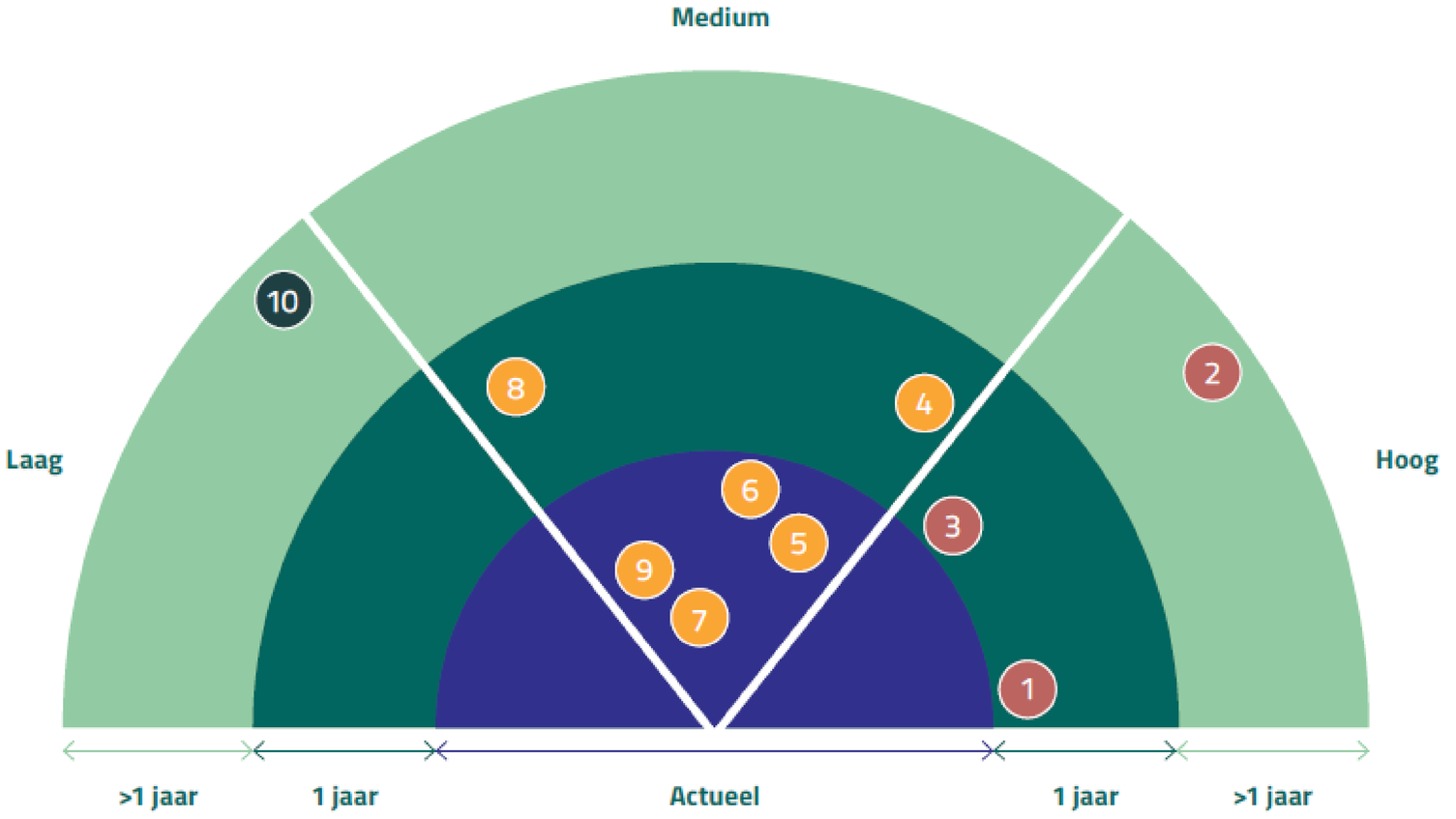
Dreigingsbeeld voor de zorg 2024

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

CERT

Hoe tot stand gekomen

- Incidenten
- Publieke bronnen
- Samenwerkingspartners
- Gesprekken met (C)ISO’s



1. Ransomware met afpersen en datalek
2. Spionage (onderzoek)
3. Ransomware bij leverancier
4. DDoS bij leverancier
5. Credential phishing
6. Malware
7. Insider threats
8. DDoS
9. Financiële fraude
10. Spionage (reguliere zorginstellingen)

Vragen?

Stichting Z-CERT
www.z-cert.nl