# Cyber Sensor

**Worden er verouderde softwareversies in mijn bedrijf gebruikt? Hoe weet ik snel of mijn medewerkers op phishing berichten klikken? Welke apparaten zijn met mijn netwerk verbonden? Waar begin ik met cybercrime beveiliging? Hoe pak ik dit aan? Relevante vragen. Informatiebeveiliging en cyberweerbaarheid zijn vandaag de dag essentieel. Wij helpen u. De Cyber Sensor is, samen met onze Webscan, een belangrijk onderdeel in onze aanpak.**

## Cyber Sensor geeft 24x7 inzicht in de mogelijke kwetsbaarheden

Onze Cyber Sensor geeft u 24 x 7 inzicht in onveilig gebruik door uw medewerkers en in kwetsbaarheden in uw internetverkeer, uw netwerk en uw informatiesystemen. Om dit te kunnen doen plaatsen we onze Cyber Sensor in uw organisatie. Met Cyber Sensor sporen we onder andere geautomatiseerde aanvallen, fouten in configuraties, ontbrekende patches, aanvallen door hackers en ongewenst gedrag of uitbraken van malware (zoals ransomware) op. Ook brengen wij in kaart welke apparaten met uw netwerk verbonden zijn.

## Sygnius' visie

In onze visie moeten mensen en organisaties veilig kunnen werken in een digitale wereld en alle kansen benutten die technologie en digitalisering biedt. Deze digitale wereld raakt websites, app's, cloud, webapplicaties en webshops maar tevens fysiek het bedrijf, de kantooromgeving, maar ook thuiswerkplekken en onderweg.

Overal waar data over de organisatie en haar klanten beschikbaar en toegankelijk is, is passende digitale beveiliging belangrijk.

Het adequaat beveiligen van uw IT-omgeving is geen sinecure. Zeker als het uw bedrijfskritische applicaties en websites betreft. Een perfecte uitvoering door goed gebruik van de juiste tools, inzet van juiste methodieken en ervaring is daarbij essentieel. Kwetsbaarheden moeten worden door onze Sensor geïdentificeerd, terwijl tegelijkertijd bedrijfsgegevens zorgvuldig worden beschermd. Niet eenmalig maar doorlopend.

Technologie kan niet alle cyberrisico's oplossen. Daarom vertalen wij dreigingen naar de potentiële impact voor uw organisatie. Ook doen wij aanbevelingen om deze cybersecurityrisico's op te lossen. Tevens wordt de awereness van uw medewerkers vergroot.

## De juiste expertise

Met onze Cyber Sensor zoeken wij naar kwetsbaarheden in uw omgeving en geven wij advies welke basisbeveiligingsmaatregelen binnen uw organisatie kunnen worden verbeterd, om zo de cyberweerbaarheid te verhogen.

Wij doen dat binnen drie gebieden, waarvoor wij u losse modules aanbieden: internet, netwerk en systeembeveiliging.

Bij elke module krijgt u toegang tot de cybersecurity expertise van Sygnius.

Van inzicht naar bescherming

## Modules van de Sygnius Cyber Sensor

| **Internet beveiliging** | **Netwerk beveiliging** | **Systeem beveiliging** |
|---|---|---|
| - Simuleert een aanval op uw infrastructuur die via internet toegankelijk is. De Sensor zoekt de mogelijke ingangen tot uw interne netwerk via bijvoorbeeld configuratiefouten of verouderde software.<br><br>- analyseert al het in- en uitgaande verkeer tussen het interne netwerk en het Internet. Dat levert u inzicht in kwaadaardig verkeer en mogelijke aanvallen. | - zoekt in het netwerk naar kwetsbaarheden in de configuratie en verouderde software op systemen, zoals op computers, servers, printers, telefoons. Die kwetsbaarheden geven een aanvaller de kans om toegang te krijgen tot deze systemen of tot applicaties of gevoelige gegevens.<br><br>- brengt alle apparaten in kaart die met het netwerk verbonden zijn. Handig in het kader van device management maar ook essentieel voor adequate beveiliging. | - Verifiëren of gedetecteerde aanvallen een impact hebben op systemen. Daarnaast helpt device protection bij het beschermen tegen ransomware en andere vormen van malware.<br><br>- aanvallen detecteren en blokkeren, nog voordat een aanval een systeem of gebruiker bereikt.<br><br>- actief systemen beschermen wanneer apparaten onderweg worden gebruikt. Dus bijvoorbeeld tijdens een zakenreis of wanneer een publiek wifi-netwerk wordt gebruikt. |
| Als de Cyber sensor kwaadaardig verkeer signaleert rapporteert hij dit aan ons.<br>Wij onderzoeken de potentiële kwetsbaarheden en bepalen hun impact. Ook kijken wij naar mogelijke verbanden. | | |

## Aanpak en kosten

Onze aanpak is pragmatisch en kosteneffectief:

1. Wij plaatsen de Sensor in uw netwerk en stellen deze in. Daarna starten we met een proefperiode van 3 weken.

2. Daarna bespreken wij met u de eerste uitkomsten en lossen direct geconstateerde aandachtspunten op.

3. Op basis van onze bevindingen bepalen wij samen de voor uw organisatie relevante risico's en scenario's die vervolgens actief zullen worden bewaakt.

De kosten van de Sensor zijn afhankelijk van de grootte van het netwerk, het aantal gebruikers en de complexiteit, maar vanaf EUR 350 per maand kunt u al gebruiken maken van de Sensor.

Neem contact met ons op: info@sygnius.nl

## Wat levert het op?

- Actueel inzicht in de veiligheid van uw organisatie. Daarmee kunt u de cyber-weerbaarheid van uw organisatie verbeteren.

- Inzicht in de apparaten die zich op het netwerk bevinden: assetmanagement.

- 24 x 7 inzicht in kwetsbaarheden en aanvallen op uw netwerk, systemen en applicaties.

- Kwaadaardige aanvallen worden automatisch geblokkeerd.

- De Sensor wordt eenvoudig geïmplementeerd en het heeft geen impact op het netwerk. Ook niet op de snelheid van het netwerk.

- Uw organisatie kan met de hulp van Sensor aan de AVG-eisen voldoen.

# Van inzicht naar bescherming

SYGNIUS

www.sygnius.nl