IRISnet paradigm Powered by Orange

Micro-SOC Werkstation

Mijn werkstations en servers beschermen tegen cyberaanvallen

Werkstations en servers, favoriete doelwitten van aanvallers

Bedrijven worden geconfronteerd met een toename van cyberaanvallen, met steeds geavanceerdere bedreigingen. Werkstations en servers vormen strategische toegangspunten tot het volledige informatiesysteem van het bedrijf.

Het wordt daarom noodzakelijk om oplossingen te implementeren om aanvallen te anticiperen, uw digitale activa te beveiligen en uw gegevens te beschermen door middel van continue monitoring van uw werkstations en servers.

Waarom moet ik cyberaanvallen voorkomen?

Deze aanvallen kunnen ernstige gevolgen hebben voor uw bedrijfsactiviteiten en uw merkimago. Ze kunnen deze verstoren of zelfs onderbreken en leiden tot materiële schade en financiële verliezen.

Door afwijkingen zo vroeg mogelijk op te sporen, is het mogelijk om ze tegen te gaan voordat ze zich op grotere schaal verspreiden.

330.000 kleine en middelgrote ondernemingen werden in 2022 in Frankrijk aangevallen. Dit zijn de bedrijven die het zwaarst getroffen zijn.
Bron: Cabinet Asterès, 2023

55% van de activa die door een incident worden getroffen, zijn werkstations en servers.
Bron: Security Navigator 2024

30% van de omzet
Dat is de gemiddelde kostprijs van een cyberaanval voor een bedrijf, bovenop het verlies aan vertrouwen van klanten en partners.
Bron: Cabinet Asterès, 2023

70 dagen
Dit is de gemiddelde tijd die nodig is om een herstelstrategie te implementeren en de bedrijfsactiviteiten weer op gang te brengen na een cyberaanval.
Bron: ANSSI, 2023

Onze oplossing: Micro-SOC-werkstations

Proactieve detectie van bedreigingen

Preventieve bescherming en bewaking van uw servers en werkstations. Analyse van incidenten en correlatie van informatie op basis van de dreigingssituatie en de nieuwste cybercriminele technieken.

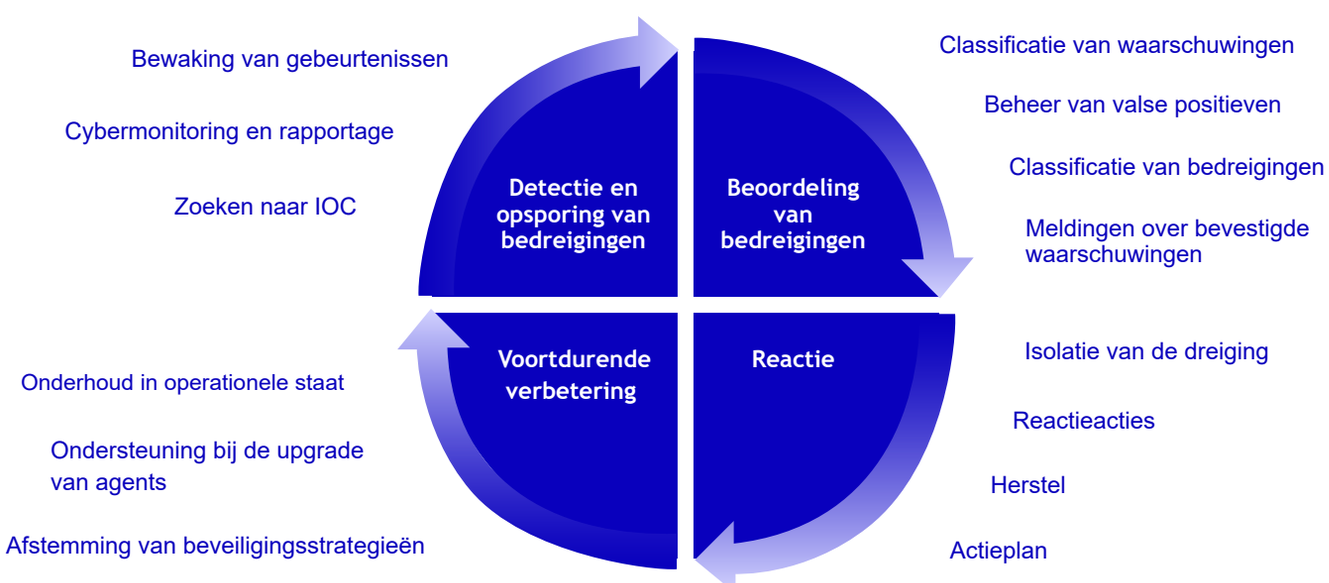
Versterking van de beveiligingspositie

Grondig onderzoek voor een diepgaande oplossing van het incident. Continue evaluatie van uw kwetsbaarheidsniveau en identificatie van uw cyberrisico's.

Gerichte respons

Automatische neutralisatie van de meest voorkomende inbreuken en toepassing van gerichte inperkingsmaatregelen voor de systemen die door de aanval zijn getroffen, afgestemd op uw zakelijke uitdagingen.

De diensten die in ons aanbod zijn inbegrepen



Uw voordelen

- Monitoring van uw apparatuurpark 8 uur per dag, 5 dagen per week. Optioneel uitbreidbaar naar 24 uur per dag, 7 dagen per week.
- Speciaal portaal waarmee u uw situatie en de te nemen corrigerende maatregelen kunt bekijken, als aanvulling op onze aanbevelingen.
- Prijzen per licentie om de oplossing aan uw ontwikkelingen.

Waarom Orange Cyberdefense?

- Alles wat we doen is gebaseerd op onze kennis van de dreigingen.
- Meer dan 280 experts verspreid over 13 CyberSOC's om u te beschermen tegen de meest geavanceerde bedreigingen.
- Meer dan 1500 klanten vertrouwen op de Micro-SOC-dienst.

IRISnet paradigm Powered by Orange

Meer weten ?

Contacteer uw accountmanager
sales.admin@irisnet.brussels
02 563 12 10 - irisnet.brussels/nl/services