

# Cybersecurity-innovatie: Geavanceerde Phishing Kit-detectie

## Context en bestaande oplossing

Als onderdeel van zijn Advanced DNS Security-dienst implementeert Belnet de Secure DNS-oplossing ontwikkeld door Secutec. Deze geavanceerde technologie bewaakt en analyseert voortdurend internetdomeinen en creëert een beschermende barrière tegen kwaadaardige sites die de netwerkindegriteit en vertrouwelijkheid van gebruikersgegevens kunnen compromitteren.

## Visie en uitbreidingsdoelstellingen

De dienst werd onlangs uitgebreid dankzij een strategische samenwerking met het Centrum voor Cybersecurity België (CCB), gericht op het aanzienlijk versterken van de bescherming van openbare diensten. Deze nieuwe functionaliteit maakt ultrasnelle detectie van kwaadaardige links in inkomende elektronische communicatie mogelijk, waarmee wordt voldaan aan een cruciale beveiligingsuitdaging.

Met 25.000 dagelijkse e-mails die het CCB ontvangt, implementeert het systeem geavanceerde geautomatiseerde analyse die onmiddellijk de aanwezigheid van phishing-kits in gerapporteerde links en websites kan identificeren. Deze vroege detectie blijkt bijzonder kritisch tegen cybercriminelen die deze kits gebruiken om massale phishing-campagnes op te zetten, waarbij ze gelijktijdig duizenden frauduleuze berichten verspreiden.

## Architectuur van de uitbreiding

De uitbreiding is gebaseerd op een drieledige synergie tussen Secutec, CCB en de Gerechtelijke Politie, waarbij een collaboratief ecosysteem voor informatie- en expertise-uitwisseling wordt opgezet. Deze samenwerking krijgt vorm via vier hoofdassen:

1. Proactief delen door Secutec van zijn expertise over de evolutie van aanvalspatronen en geïdentificeerde phishing-kits.
2. Continue onderhoud van het detectiesysteem, verrijkt door de collectieve intelligentie van de drie partners, met broncode beschikbaar gesteld aan autoriteiten.
3. Implementatie van toegewijde infrastructuur via een webservice, waardoor CCB en de Gerechtelijke Politie toegang krijgen tot Secutec's detectiebronnen.
4. Dynamische integratie van gedetecteerde dreigingen in Belnet's Advanced DNS Security-oplossing, waardoor de bescherming voor alle netwerkgebruikers wordt versterkt.

Deze geïntegreerde aanpak maakt een effectievere en gecoördineerde respons op opkomende cyberdreigingen mogelijk.