

# Cybersecurity Innovation: Advanced Phishing Kit Detection

## Context and existing solution

As part of its Advanced DNS Security service, Belnet deploys the Secure DNS solution developed by Secutec. This sophisticated technology continuously monitors and analyzes Internet domains, creating a protective barrier against malicious sites that could compromise network integrity and user data confidentiality.

## Vision and extension objectives

The service evolution revolves around a strategic collaboration with the Belgian Center for Cybersecurity (CCB), aiming to significantly strengthen public service protection. This new functionality enables ultra-rapid detection of malicious links in incoming electronic communications, thus addressing a crucial security challenge.

Facing 25,000 daily emails received by the CCB, the system deploys sophisticated automated analysis, capable of instantly identifying the presence of phishing kits in reported links and websites. This early detection proves particularly critical against cybercriminals who exploit these kits to orchestrate massive phishing campaigns, simultaneously distributing thousands of fraudulent messages.

## Extension architecture

The extension is based on a tripartite synergy between Secutec, CCB, and the Judicial Police, establishing a collaborative ecosystem for information and expertise exchange. This collaboration materializes through four main axes:

1. Proactive sharing by Secutec of its expertise on the evolution of attack patterns and identified phishing kits.
2. Continuous maintenance of the detection system, enriched by the collective intelligence of the three partners, with source code made available to authorities.
3. Deployment of dedicated infrastructure via a web service, allowing CCB and Judicial Police to access Secutec's detection resources.
4. Dynamic integration of detected threats into Belnet's Advanced DNS Security solution, thus strengthening protection for all network users.

This integrated approach enables a more effective and coordinated response to emerging cyber threats.