



Co-funded by
the European Union



ECCCC 
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

SOC4HEALTH

19/11/2024

CHARLES SALA – RESTRICTED EU – TLP AMBER

HCL
HOSPICES CIVILS
DE LYON

SOC4Health

www.chu-lyon.fr

SOC4HEALTH BY HCL

CO-FINANCÉ PAR DIGITAL-ECCE-2022-CYBER-03



Co-funded by
the European Union

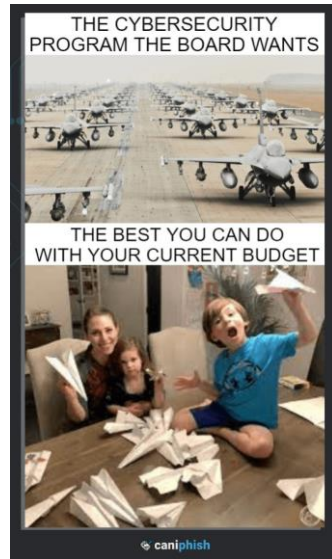
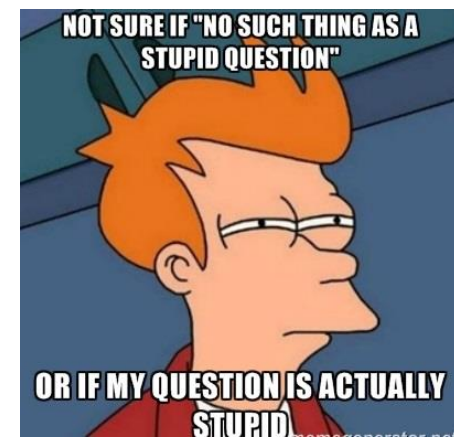
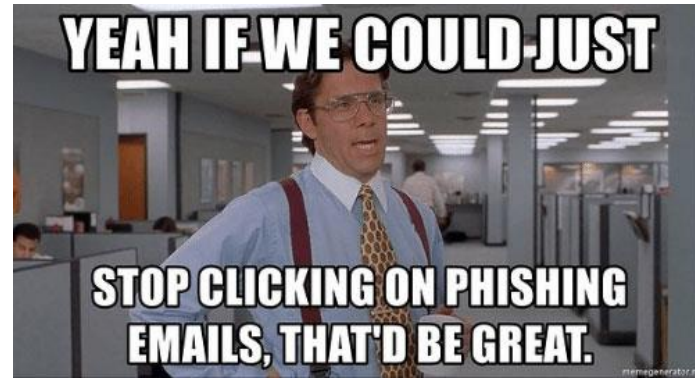


EC3
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

- Projet sur 3 ans / 1.2 M€ de fonds UE (50% total)
- Deux initiatives séparées mais complémentaires:
 - Un kit de développement d'un Security Operation Center (SOC) pour les hôpitaux
 - Une infrastructure permettant la contextualisation, l'enrichissement et le partage de CTI entre hôpitaux (MISP-based avec AI/ML)
- La phase 1 vient de se terminer: Amélioration et consolidation du SOC des HCL
- Début de la phase 2: Rédaction du kit. Première version mi-2025
- MISP déjà disponible: misp.chu-lyon.fr
- L'ensemble des livrables sera mis à disposition GRATUITEMENT aux Hôpitaux publics et CERT SANTE de l'UE

POURQUOI ?

EN 7 MEMES



STRUCTURE

DU KIT

- Le guide de creation d'un SOC sera composé de 2 niveaux de complexité:
 - Créer une équipe cybersécurité opérationnelle dans un hôpital (Part 1)
 - Internaliser un SOC dans un hôpital (Part 2)
- 7 sujets
 - CTI
 - Use cases / Détection
 - Partage de données
 - Forensics
 - Data Collection / Enrichissement
 - Automatisation
 - Documentation, procédures and checklists
- Format modulaire – chaque ES pourra utiliser les (morceaux de) chapitres qu'il souhaite et au niveau où il le souhaite

ADVISORY BOARD

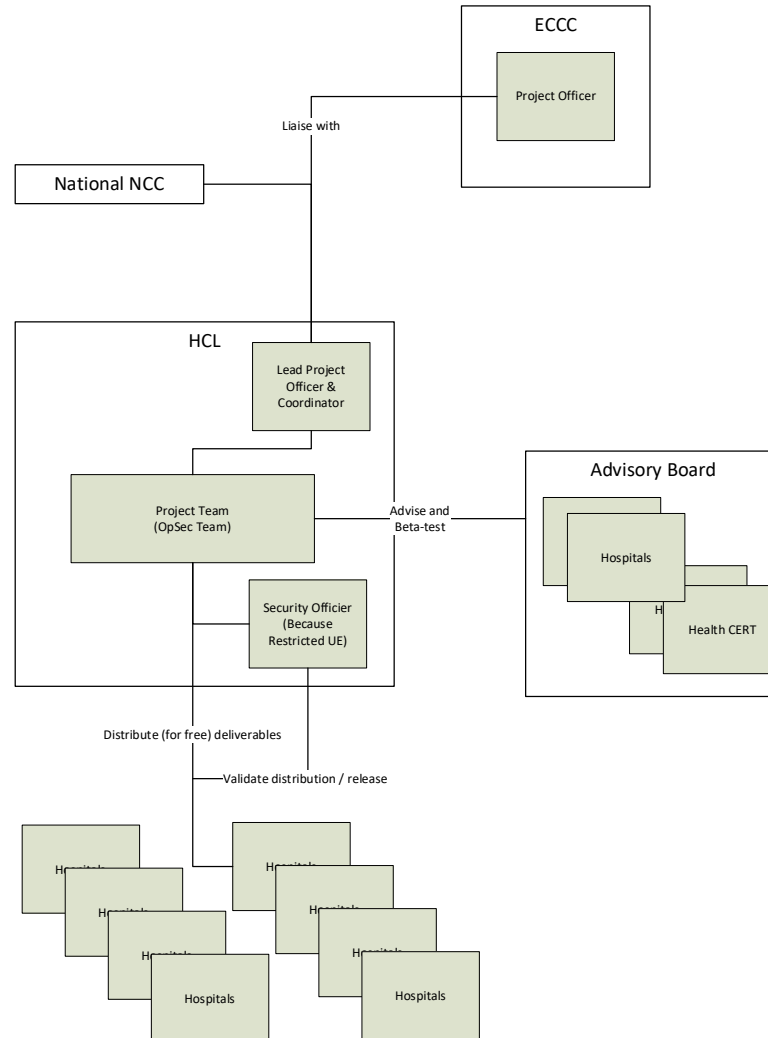
SOC4HEALTH



Co-funded by
the European Union



ECCE
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

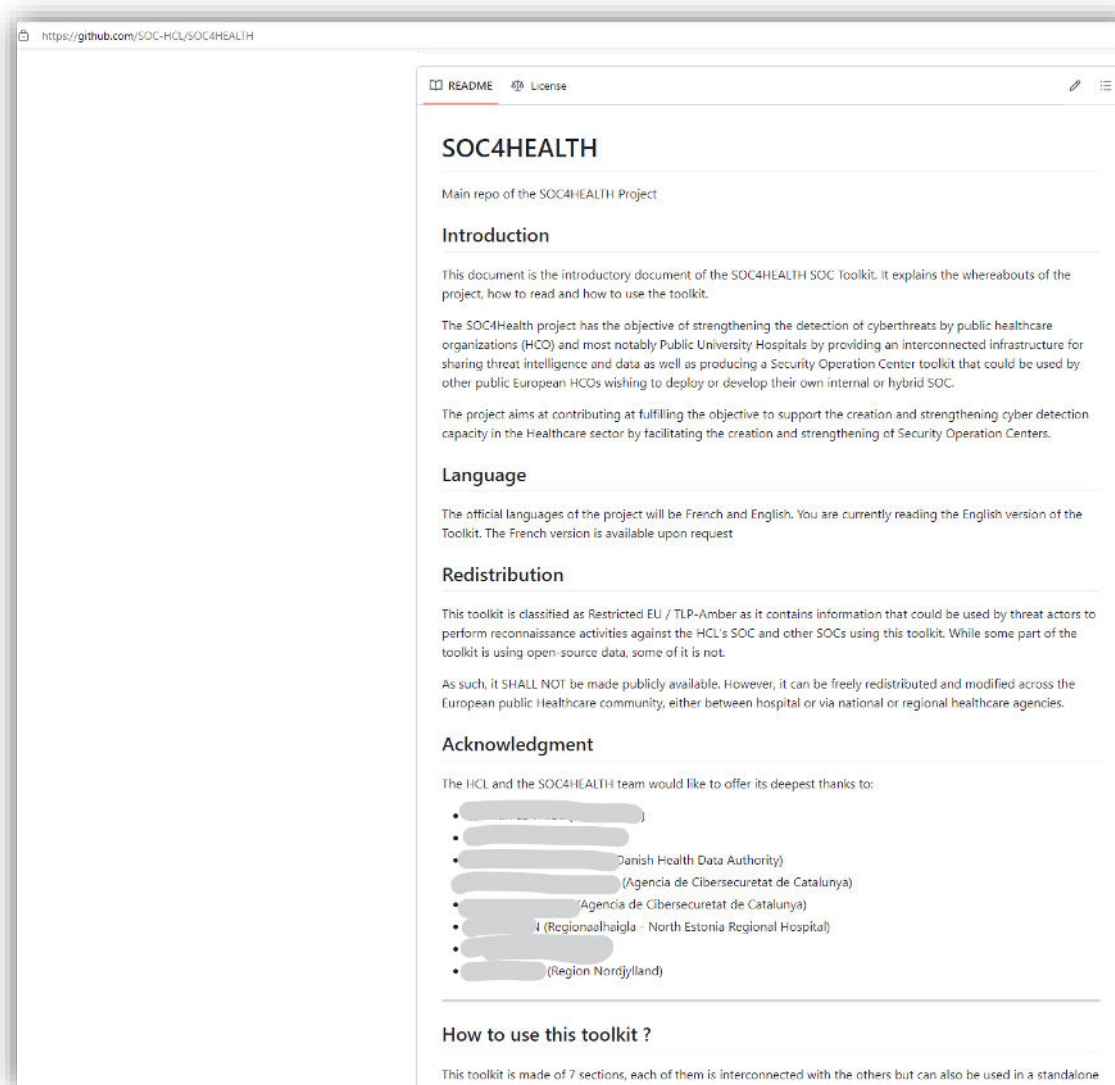


- Un advisory board composé de 2 CERT Santé (FR & DK), 1 Agence Régionale de Cybersécurité (Catalogne) et plusieurs hôpitaux (FR, DK, NL, IT et Estonie)

QUELQUES EXTRAITS DU KIT

TLP-AMBER STRICT – A NE PAS PUBLIER

- Démo ;)



The screenshot shows the GitHub README for the SOC4HEALTH project. The page is titled "SOC4HEALTH" and is the main repository for the project. It includes an introduction, a language section, a redistribution section, and an acknowledgment section. The acknowledgment section lists several organizations that have supported the project, including the Danish Health Data Authority, the Agencia de Ciberseguretat de Catalunya, and the Region Nordjylland.

https://github.com/SOC-HCL/SOC4HEALTH

README License

SOC4HEALTH

Main repo of the SOC4HEALTH Project

Introduction

This document is the introductory document of the SOC4HEALTH SOC Toolkit. It explains the whereabouts of the project, how to read and how to use the toolkit.

The SOC4Health project has the objective of strengthening the detection of cyberthreats by public healthcare organizations (HCO) and most notably Public University Hospitals by providing an interconnected infrastructure for sharing threat intelligence and data as well as producing a Security Operation Center toolkit that could be used by other public European HCOs wishing to deploy or develop their own internal or hybrid SOC.

The project aims at contributing at fulfilling the objective to support the creation and strengthening cyber detection capacity in the Healthcare sector by facilitating the creation and strengthening of Security Operation Centers.

Language

The official languages of the project will be French and English. You are currently reading the English version of the Toolkit. The French version is available upon request

Redistribution

This toolkit is classified as Restricted EU / TLP-Amber as it contains information that could be used by threat actors to perform reconnaissance activities against the HCL's SOC and other SOC's using this toolkit. While some part of the toolkit is using open-source data, some of it is not.

As such, it SHALL NOT be made publicly available. However, it can be freely redistributed and modified across the European public Healthcare community, either between hospital or via national or regional healthcare agencies.

Acknowledgment

The HCL and the SOC4HEALTH team would like to offer its deepest thanks to:

- [Redacted]
- [Redacted]
- [Redacted] (Danish Health Data Authority)
- [Redacted] (Agencia de Ciberseguretat de Catalunya)
- [Redacted] (Agencia de Ciberseguretat de Catalunya)
- [Redacted] (Regionaalhaigla - North Estonia Regional Hospital)
- [Redacted] (Region Nordjylland)

How to use this toolkit ?

This toolkit is made of 7 sections, each of them is interconnected with the others but can also be used in a standalone

COMMENT PARTICIPER

- Si vous êtes un hôpital universitaire et à l'aise en anglais => Vous pouvez rejoindre l'Advisory Board
 - Accès en alpha testing au kit et aux outils
 - Capacité à apporter votre expertise et contribuer à rendre le projet le plus utile possible
- Si vous êtes un hôpital public (ou privé non lucratif) => Vous pouvez demander à faire partie des beta-tester
 - Accès à la première version du kit à partir de mi-2025



MERCI

www.chu-lyon.fr



HCL
HOSPICES CIVILS
DE LYON