Profil de l’association H-CSC

État : février 2026

1 Introduction

Le «Healthcare Cyber Security Center (H-CSC)» est une organisation nationale de cybersécurité. Il sert au partage des connaissances et à la collaboration entre les établissements de santé. Son objectif est de développer les capacités existantes et de créer des synergies afin de renforcer durablement la prévention, la détection et la gestion des incidents cybernétiques.

La participation active et la collaboration étroite des membres sont au cœur des activités du H-CSC. Il en résulte une communauté de spécialistes de la sécurité de l’information, fondée sur la confiance mutuelle, au sein de laquelle les spécialistes apprennent les uns des autres et s’engagent ensemble pour la résilience du système de santé suisse.

2 L’association

L’association à but non lucratif H-CSC a été fondée le 28 août 2025 par 18 hôpitaux suisses qui se sont fixé pour objectif de construire une base commune de cybersécurité pour l’ensemble du secteur de la santé.

Figure 1 : Logos des membres fondateurs

Le H-CSC a été fondé sur recommandation de l’Office fédéral de la cybersécurité (OFCS) et contribue directement à la mise en œuvre de la Cyberstratégie nationale (CSN) de l’OFCS. L’objectif stratégique principal est de garantir des services et infrastructures numériques sûrs, au sens global de la confidentialité, de la disponibilité et de l’intégrité.

Les statuts de l’association H-CSC peuvent être téléchargés sur le site www.h-csc.ch.

2.1 Objectifs de l'association H-CSC

Le H-CSC poursuit les objectifs suivants :

- Promouvoir la collaboration entre les équipes de cybersécurité des établissements de santé suisses
- Fournir des solutions de cybersécurité spécifiques au secteur répondant aux besoins des établissements de santé suisses, y compris dans le domaine des technologies médicales
- Réduire la dépendance à l'égard de fournisseurs externes de solutions de sécurité en développant une expertise sectorielle spécifique
- Mettre en place des structures organisationnelles pour l'échange continu d'informations sur les menaces et des bonnes pratiques
- Permettre des achats communs afin de renforcer le pouvoir de négociation et de réduire les coûts et les charges
- Renforcer la cybersécurité dans les établissements de santé de taille moyenne et petite
- Mettre à disposition des documents et partager les expériences avec d'autres établissements de santé afin d'accroître les compétences en matière de cybersécurité

2.2 Organes de l'association

L'association H-CSC repose sur un modèle de gouvernance transparent et participatif favorisant l'orientation stratégique, l'efficacité opérationnelle et la participation active des membres.

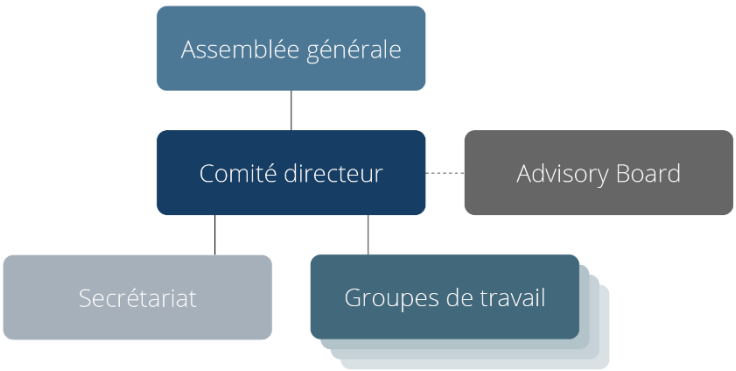

Figure 2 : Organes de l'association H-CSC

L'assemblée générale se compose de délégué·e·s de tous les établissements de santé membres. Elle élit le comité, approuve les résultats et décide de questions telles que l'extension des prestations.

Le comité directeur assure la direction stratégique. Composé de sept membres élus, il définit l'évolution de l'association, supervise le secrétariat et coordonne les travaux des groupes d'experts.

Le secrétariat est responsable de la gestion opérationnelle quotidienne et agit comme organe de coordination entre les membres, les partenaires et les autorités. Il soutient les groupes de travail et veille au bon déroulement de toutes les activités organisationnelles.

Le Advisory Board garantit un échange régulier entre l'association H-CSC et ses membres. Il permet de discuter des retours sur les prestations et la performance du H-CSC, ainsi que de recueillir les préoccupations, souhaits et questions concrètes des membres.

Les groupes de travail sont composés de spécialistes en cybersécurité issus des organisations membres. L'équipe technique assure le développement et la mise à disposition des services tech-niques de l'association et soutient les membres dans leur utilisation.

2.3 Partenaires

Afin de tirer parti des synergies et d'éviter les doublons, l'association H-CSC collabore avec plusieurs partenaires importants issus du secteur de la santé et de la cybersécurité. Les partenaires actuels comprennent la Vereinigung Gesundheitsinformatik Schweiz (VGI.ch), l'Office fédéral de la cybersécurité (OFCS) et l'Infrastructure Hôpital Suisse (IHS). Des discussions sont en cours avec d'autres partenaires potentiels.

2.4 Membres

L'adhésion est actuellement ouverte aux hôpitaux et cliniques suisses disposant d'un mandat de prestations publiques. Cela inclut les hôpitaux de soins aigus, les cliniques psychiatriques et les cliniques de réadaptation, tels que définis par l'Office fédéral de la santé publique (OFSP) et les cantons concernés. À long terme, l'adhésion sera étendue à l'ensemble des acteurs du système de santé en Suisse afin de créer un écosystème national uniforme et résilient.

Pour devenir membre, les hôpitaux et cliniques suisses versent une cotisation annuelle destinée à couvrir les coûts des services fournis. La procédure d'adhésion est disponible sur le site www.h-csc.ch. Le règlement des cotisations de l'association H-CSC ainsi que l'accord de confidentialité peuvent également être téléchargés sur le site.

3 Contexte de la création du H-CSC

3.1 Menaces mondiales

Dans un système de santé de plus en plus numérisé, la technologie et les données sont essentielles à la prestation des soins. La cybersécurité joue un rôle central pour garantir la sécurité des patients, l'efficacité des traitements et la protection des processus de santé, car les cybercriminels ciblent de plus en plus les établissements de santé dans le monde entier.

Ceux-ci constituent des cibles attrayantes en raison de leur dépendance à des systèmes interconnectés, de processus critiques en termes de temps et des risques pour la sécurité des patients. Par ailleurs, l'utilisation d'opérations cybernétiques dans les conflits armés augmente, et les infrastructures civiles critiques – telles que les établissements de santé – sont de plus en plus souvent visées. Ces dernières années, tant le secteur médical que les organisations humanitaires ont été ciblés par des attaques, illustrant leur vulnérabilité dans le cadre de la guerre numérique moderne.

Alors que les cyberattaques par rançongiciel ou logiciel malveillant menacent principalement les données sensibles et les infrastructures dans la plupart des infrastructures critiques, elles peuvent également mettre en danger des vies humaines dans le secteur de la santé. Face à ces menaces, il est essentiel que les établissements de santé suisses renforcent leur cyberrésilience et puissent réagir rapidement et efficacement aux attaques. Compte tenu des ressources limitées, la collaboration entre établissements de santé est indispensable.

3.2 Défis en Suisse

Expertise sectorielle spécifique limitée : Les directives générales en matière de cybersécurité ne prennent pas suffisamment en compte les menaces spécifiques aux établissements de santé, telles que les vulnérabilités des dispositifs médicaux certifiés, la protection de systèmes cliniques critiques comportant des composants logiciels non pris en charge ou la gestion correcte de données sensibles et fortement réglementées sous une pression temporelle constante (par exemple dans les ambulances, les services d'urgence ou les unités de soins intensifs).

Coûts et charges élevés dans les processus d'acquisition : Pour l'évaluation des systèmes et services de sécurité informatique, presque tous les établissements de santé rédigent des cahiers des charges pratiquement identiques. À l'avenir, ces documents pourront être élaborés conjointement via le H-CSC et fournis aux membres sous forme de modèles. Cela réduit la charge des responsables de la sécurité, permet d'économiser du temps et des coûts et améliore la qualité des documents, car il devient possible d'apprendre des erreurs des autres.

L'association H-CSC répond à ces défis et renforce les capacités de cybersécurité des établissements de santé suisses en fournissant des services spécifiques au secteur et en favorisant une collaboration structurée à l'échelle de l'ensemble du secteur.

4 Services

L'association H-CSC met à la disposition de ses membres une large gamme de services afin de les soutenir dans l'amélioration de leur cyberrésilience, indépendamment de leur niveau de maturité actuel. Ces services sont développés avec les membres et pour les membres, afin de garantir qu'ils soient adaptés aux besoins spécifiques du secteur de la santé.

Actuellement, dix services sont disponibles pour les membres, dont les coûts sont en grande partie inclus dans les cotisations. La plupart des services sont proposés en allemand, français et italien ; certains services sont disponibles uniquement en anglais.

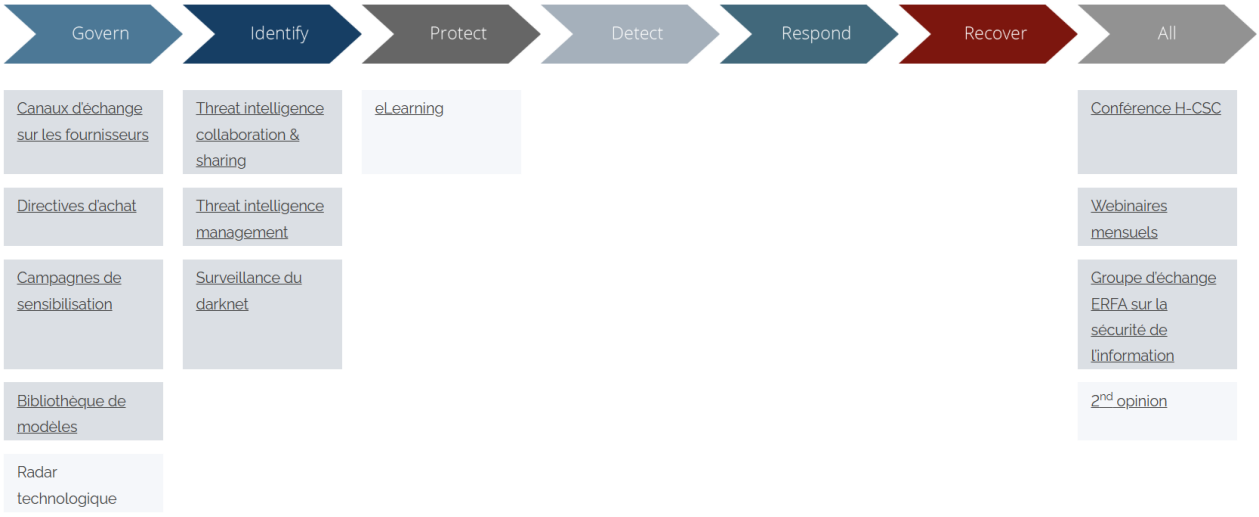

Figure 3 : Aperçu des services de l'H-CSC pour ses membres

4.1 Aperçu des services existants

- Threat intelligence collaboration & sharing : plateforme pour l'échange sécurisé et coordonné d'informations sur les cybermenaces, les IoC et les vulnérabilités. Les membres bénéficient d'une vision commune de la situation et d'une intégration plus simple dans leurs solutions de sécurité existantes.

- Threat intelligence management : accès centralisé à des informations vérifiées et pertinentes pour le secteur concernant les cybermenaces actuelles. Le service permet une détection plus rapide et une prévention efficace des attaques, réduit les efforts manuels et renforce la cyberrésilience individuelle et collective des membres.
- Surveillance du darknet : surveillance continue de sources darknet pertinentes afin de détecter des identifiants compromis et des informations sensibles. Les incidents potentiels sont détectés et signalés précocement, permettant aux établissements concernés de prendre des mesures de protection et de réaction appropriées.
- Canaux d'échange sur les fournisseurs : échange ciblé d'expériences concernant les fabricants, produits et services de cybersécurité. Dans des canaux dédiés, les membres partagent des bonnes pratiques et des évaluations issues de l'expérience terrain.
- Directives d'achat : regroupement des exigences de sécurité des membres afin de créer une voix commune forte sur le marché. La sécurité de l'information est intégrée dès les premières étapes des processus d'acquisition, contribuant à des solutions plus sûres à long terme.
- Campagnes de sensibilisation : collection centrale de campagnes éprouvées issues des membres, comprenant des informations sur les bénéfices, les efforts requis, les matériels et les personnes de contact. Les membres peuvent ainsi identifier rapidement des approches adaptées et réduire leurs efforts de préparation.
- Conférence H-CSC : événement annuel dédié au réseautage, à l'échange d'expériences et à la formation continue par des conférences spécialisées et des discussions.
- Webinaires mensuels : échanges techniques réguliers concernant les services, les positions du H-CSC et les retours d'expérience des membres en matière de cybersécurité dans le secteur de la santé.
- Groupe d'échange ERFA sur la sécurité de l'information : échange d'expériences structuré et confidentiel destiné aux responsables de la sécurité de l'information des établissements de santé, notamment les CISO et responsables de la sécurité IT.
- Bibliothèque : collection centrale de modèles, directives et documents d'exemple provenant des organisations membres concernant l'ISMS, la protection de base IT et la sensibilisation.

Note linguistique : Ce document existe en plusieurs versions linguistiques. En cas de divergence ou d'interprétation, seule la version allemande fait foi.