

16 février 2026 | Office fédéral de la cybersécurité OFCS



Rapport annuel 2025

Office fédéral de la cybersécurité OFCS



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
Protection de la population et des sports DDPS
Office fédéral de la cybersécurité OFCS

Contenu

Préface	3
Chiffres clés majeures de 2025	4
Objectives de l'OFCS	5
<i>Vision</i>	5
<i>Mission</i>	5
Resources financières	6
<i>Dépenses en 2025</i>	6
<i>Utilisation des ressources financières par tâche</i>	7
<i>Structure du personnel</i>	7
Activités de l'OFCS selon les quatre piliers stratégiques	8
Rendre les cybermenaces compréhensibles	8
<i>Renforcement de la cybersécurité préventive</i>	8
<i>Projet de concept d'urgence cyber à l'intention des communes</i>	9
<i>Mise en oeuvre de la cyberstratégie nationale (CSN)</i>	10
Moyens pour prévenir les cyberattaques	11
<i>Échanges d'informations sur le Cyber Security Hub (CSH)</i>	11
<i>Cyber Threat Intelligence</i>	11
<i>Initiatives sectorielles</i>	12
<i>Guichet unique suisse pour les cyberincidents</i>	13
<i>Introduction de l'obligation de signaler</i>	14
Réduire les dommages liés aux cyberincidents	15
<i>Alertes relatives aux cybermenaces graves désormais aussi via Alertswiss</i>	15
<i>Engagements de l'OFCS lors d'événements de grande envergure</i>	15
<i>Échange d'informations</i>	15
Augmenter la sécurité des produits et services numériques	16
<i>Open Source</i>	18
<i>Bug Bounty</i>	16
<i>Gestion axée sur les effets de l'OFCS</i>	17
Publications et références	18

Préface

Chères lectrices, chers lecteurs,

L'année 2025 a été marquée pour l'Office fédéral de la cybersécurité (OFCS) par une phase de consolidation et de renforcement de notre mandat. Après la phase de mise en place, nous avons pu consolider les processus clés et développer de manière ciblée la collaboration au sein du Département fédéral de la défense, de la protection de la population et des sports (DDPS), ainsi qu'avec nos organisations partenaires. Les structures mises en place ont fait leurs preuves et permettent une exécution fiable et cohérente de nos tâches.

Une étape déterminante a été l'introduction de l'obligation de signaler les cyberattaques contre des infrastructures critiques. Neuf mois après son entrée en vigueur, la mise en œuvre fonctionne : les incidents sont signalés dans les délais, les instruments prévus sont utilisés et la collaboration avec les exploitantes et exploitants d'infrastructures critiques est établie. La communication proactive via les associations professionnelles et les vidéos explicatives complémentaires ont joué un rôle particulièrement décisif dans le bon déroulement de cette introduction. Sur cette base, la Suisse dispose désormais de processus de notification et d'assistance stables dans ce domaine important pour la sécurité.

Les quelque 65'000 signalements volontaires montrent que les cyberrisques sont désormais bien présents dans les esprits et que la population agit de manière proactive. Ces signalements contribuent de manière essentielle à l'élaboration d'une image de la situation actuelle et à une meilleure appréciation de la menace, permettant à l'OFCS d'adapter de manière ciblée ses mesures d'information et de prévention. L'OFCS a également accordé une attention particulière au développement de la plateforme numérique nationale Cyber Security Hub (CSH). Des fonctionnalités améliorées et de nouveaux formats d'échange ont été introduits, renforçant la collaboration intersectorielle et facilitant l'accès à des informations spécialisées pertinentes. Les instruments de contrôle de la stratégie nationale en matière de cybersécurité (NCS) ont également été développés : ils comprennent plus de 90 projets avec des partenaires issus des autorités, de l'économie et de la société. En outre, la mise en place de nouveaux Cyber Security Centers (CSC) spécifiques à certains secteurs, tels que le « Healthcare-CSC », a renforcé la mise en œuvre conjointe de la NCS.

Ces prestations ont été fournies dans un contexte marqué par des incertitudes financières. La décision du Parlement d'augmenter de 10 millions de CHF le budget de l'OFCS pour 2026 et de 5 millions supplémentaires à partir de 2027 constitue un signal fort de confiance et permet de compenser des sous-financements, de réaliser les investissements nécessaires et de mettre en œuvre durablement de nouvelles tâches légales, en particulier celles liées à l'obligation de signaler. Cette décision s'accompagne d'attentes claires en matière d'impact, de fiabilité et de gestion responsable des ressources confiées. Les objectifs à long terme demeurent inchangés et pourront désormais être atteints avec une plus grande confiance.



Je remercie l'ensemble des collaboratrices et collaborateurs ainsi que nos organisations partenaires pour leur engagement et leur coopération constructive. Ensemble, nous apportons une contribution essentielle à la cybersécurité de la Suisse.

Florian Schütz
Directeur de l'Office fédéral de la cybersécurité

Chiffres clés majeurs de 2025



18.4 millions de CHF

de dépenses



71

collaboratrices et collaborateurs
(dont 4 stagiaires universitaires)



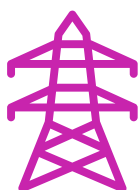
64'733

signalements volontaires de cyberincidents



501

contacts avec les médias



222

signalements de cyberattaques dans le cadre de l'obligation de signaler

Nouveau



2'347'618

analyses de signalements concernant des appareils infectés par des logiciels malveillants



1'600

entreprises sur le Cyber Security Hub



400

participantes et participants en moyenne aux échanges en ligne bi-hebdomadaires de situation

Nouvellement enregistrés



525

signalements de vulnérabilités par des pirates éthiques



17'468

systèmes de commande et de contrôle d'attaquants identifiés et bloqués



Par rapport à 2024

Situation en décembre 2025

Objectifs de l'OFCS

Vision

La cybersécurité est une tâche commune à la politique, à l'économie, aux hautes écoles et à la société. Nombreuses sont les organisations et personnes qui ont du mal à estimer les cyberrisques et à les éviter. L'opacité qui entoure la sécurité des produits numériques mène à l'insécurité chez les consommateurs et à leur vulnérabilité. En raison de l'interconnexion croissante des réseaux, des systèmes insuffisamment protégés peuvent servir de vecteurs pour provoquer des dommages à grande échelle.

La Vision de l'OFCS est d'améliorer la cybersécurité en Suisse, en collaboration étroite avec tous les acteurs concernés.

Mission

L'OFCS a pour mission principale de renforcer la cybersécurité des infrastructures critiques, de l'économie, du système éducatif, de la population et des autorités en coordonnant la mise en œuvre de la cyberstratégie nationale (CSN).

Pour ce faire, il oriente ses prestations selon les quatre piliers stratégiques suivants :

Les quatre piliers stratégiques

1 Vulgarisation des cybermenaces

L'OFCS vulgarise en fonction des groupes cibles les corrélations complexes qui mènent aux cybermenaces. Il permet ainsi d'instaurer un dialogue constructif sur la cybersécurité entre le monde de la politique, celui de l'économie et la société. Cela permet à chacun d'eux d'assumer sa propre responsabilité dans la diminution des risques systémiques.

2 Mise à disposition de moyens empêchant les cyberattaques

L'OFCS réduit la surface d'attaque des personnes et organisations suisses dans le cyberspace. Il signale des attaques et fournit des informations, voire des instruments, permettant de les éviter plus facilement.

3 Réduction des dommages dus aux cyberincidents

L'OFCS aide les personnes et organisations touchées par des cyberincidents à réduire les dommages et à circonscrire tout risque d'extension à d'autres victimes.

4 Augmentation de la sécurité des produits et prestations numériques

L'OFCS incite les fournisseurs à proposer des produits ou prestations sûrs à des prix abordables et encourage les modèles économiques correspondants. Il favorise la transparence pour les utilisateurs, de sorte que ceux-ci puissent, au regard de la cybersécurité, opter en toute connaissance de cause pour une variante ou pour une autre.

Ressources financières

Dépenses en 2025

En 2025, les comptes définitifs de l'OFCS s'élevaient à 18.4 millions de francs suisses, dont 13,0 millions pour les frais de personnel et 5,4 millions pour les dépenses matérielles et opérationnelles. Sur les dépenses matérielles et opérationnelles, 3,8 millions de francs suisses ont été consacrés à l'informatique, dont 1,2 million pour l'exploitation et 2,6 millions pour les développements ultérieurs. Le budget consacré aux développements a été augmenté de 2,5 millions de francs suisses grâce à l'utilisation de réserves affectées. L'OFCS a ainsi disposé de moyens suffisants pour développer les systèmes informatiques existants en vue de l'introduction, au 1er avril 2025, de l'obligation de signaler les cyberattaques contre les infrastructures critiques.

1,8 million de francs suisses ont été consacrés au développement du Cyber Security Hub (CSH). 0,1 million de francs suisses supplémentaires ont été affectés à la plateforme d'analyse des cyberincidents (CyARC). 0,5 million de francs ont été utilisés pour la mise en œuvre de programmes de bug bounty afin d'identifier et de corriger les vulnérabilités des systèmes informatiques de l'administration fédérale. Les fonds restants dans le domaine informatique ont été utilisés pour des services destinés aux infrastructures critiques ainsi que pour des contrôles de cybersécurité dans les domaines des périphériques, du photovoltaïque et de l'open source.

Sur les autres dépenses matérielles et opérationnelles d'un montant de 1,6 million de francs suisses, 0,4 million de francs suisses ont été consacrés à des prestations externes. Sur ce montant, 0,2 million de francs suisses ont été utilisés pour le développement des processus GEVER et 0,2 million de francs pour le développement d'un modèle cible open source. Les dépenses pour les voyages et la participation à des conférences se sont élevées à 0,3 million de francs suisses. Le reste des fonds a été utilisé pour les frais de location, les fournitures de bureau, la bureautique et les imprimés.

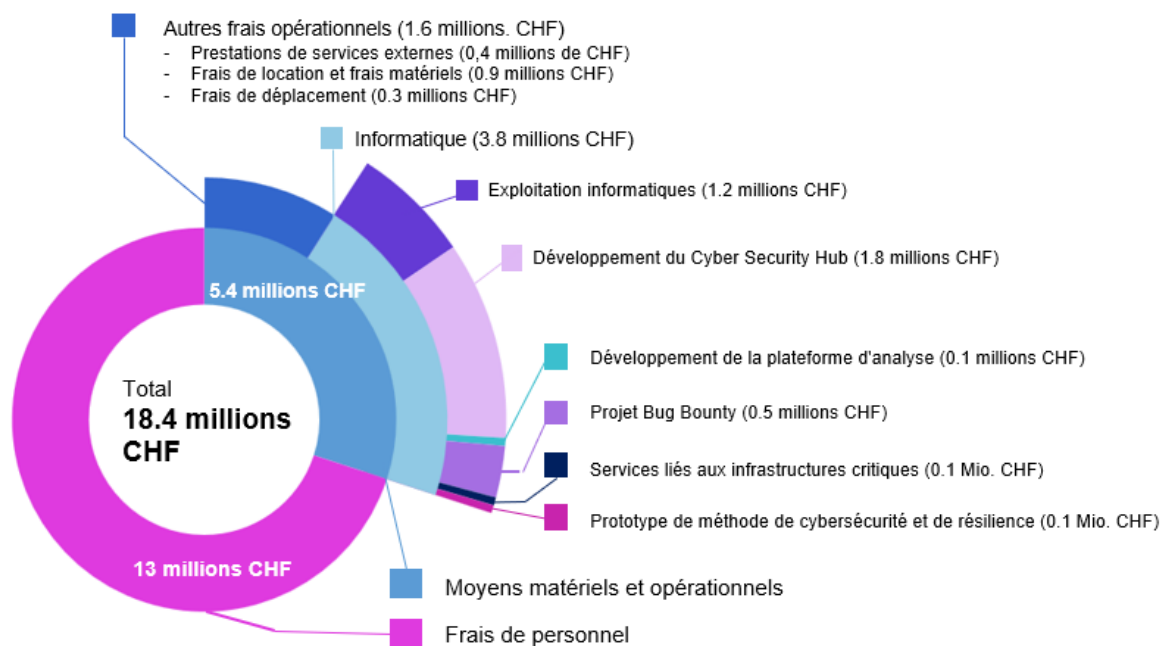


Illustration 1: Ressources financières OFCS - Comptes 2025

Utilisation des ressources financières par tâche

La majeure partie des moyens matériels et opérationnels a été utilisée pour la mission principale de l'OFCS. Les fonds ont été consacrés à la prévention, au traitement et au suivi des cyberincidents. Les frais administratifs ont été réduits à un minimum et s'élevaient à 9 % en 2025.

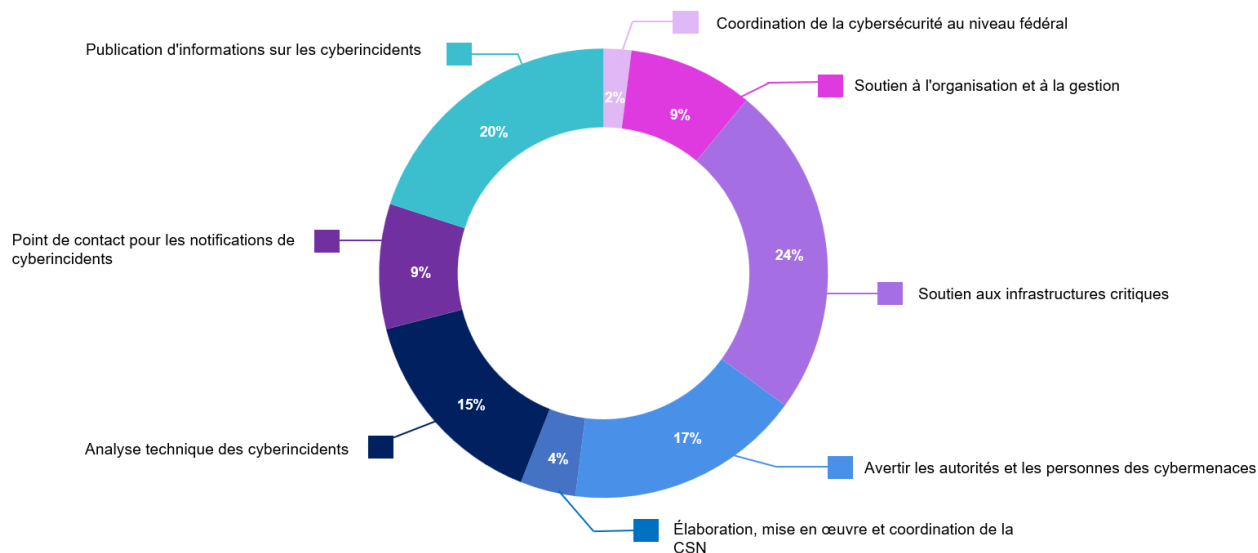


Illustration 2 : Répartition des moyens financiers par tâche

Structure du personnel

Les dépenses liées aux ressources humaines se sont élevées à un total de 13 millions de francs suisses. Elles ont été réparties entre 71 postes, dont quatre stagiaires universitaires.

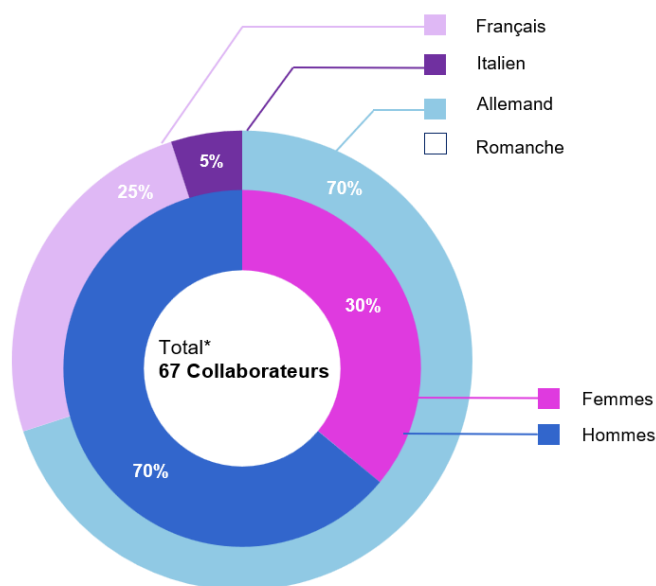


Illustration 3 : Effectif OFCS en décembre 2025
*hors stagiaires universitaires

Activités de l'OFCS selon les quatre piliers stratégiques

1 Vulgarisation des cybermenaces

Un objectif clé de l'OFCS est de permettre à ses groupes cibles de se protéger efficacement contre les cybermenaces. En 2025 également, l'OFCS a accordé une attention particulière au développement et à la mise à disposition ciblée d'informations sur les cybermenaces et sur les mesures de protection possibles.

Pour la communication à destination du grand public, l'OFCS utilise en particulier son site Internet, sur lequel sont publiés en continu des avertissements actuels, des rétrospectives hebdomadaires, des informations destinées aux médias ainsi que de brèves analyses techniques. En 2025, plusieurs campagnes de sensibilisation ont été menées à l'intention du grand public. La campagne « S-U-P-E-R » a été poursuivie. La présence pour la première fois de l'OFCS à la foire grand public BEA 2025 a en outre permis de sensibiliser un public encore plus large aux enjeux de la cybersécurité. Dans le cadre du « Mois de la cybersécurité » (Cyber Security Month), la campagne suisse de cette année a mis l'accent sur les thèmes des données en ligne et du phishing. En collaboration avec l'organisation partenaire Netpathie ainsi qu'avec l'ambassadeur de la campagne Ivano Somaini, divers contenus ont été élaborés, notamment des vidéos, des quiz, des autocollants ainsi qu'un « Brown Bag Lunch » en ligne consacré aux risques liés au partage excessif (oversharing) et à l'utilisation consciente des données numériques.

Afin de soutenir les entreprises et les communes, l'OFCS s'est en outre engagé en 2025 dans de nombreuses manifestations d'information et de formation continue. En collaboration avec des partenaires tels que ITSec4KMU, l'Association Suisse d'Assurances (ASA) ainsi que des associations sectorielles, des exposés spécialisés axés sur la pratique, des démonstrations de hacking et des ateliers ont été organisés. Ceux-ci ont mis l'accent sur le renforcement individuel de la cybersécurité ainsi que sur l'importance de chaînes d'approvisionnement sécurisées.

Renforcement de la cybersécurité préventive

Avec le développement de la méthode de cybersécurité et de résilience (MCSR), l'OFCS a franchi en 2025 une étape importante dans le renforcement de la cybersécurité préventive. Cette méthode offre une approche pratique de la gestion des cyberrisques, axée sur les processus métiers et de production centraux. Elle repose sur une protection de base étendue, s'aligne sur les normes internationales et renonce à une quantification des risques. L'évaluation de la cyberrésilience développée par l'OFCS comprend un catalogue de contrôle structuré qui permet aux organisations de procéder à une auto-évaluation systématique et servira de base à la comparaison avec d'autres organisations. L'évaluation de la cyberrésilience va être testée dans le cadre d'un projet pilote dans le canton d'Argovie avec des communes et des entreprises dans des conditions réelles afin de perfectionner conjointement la méthode et l'outil.

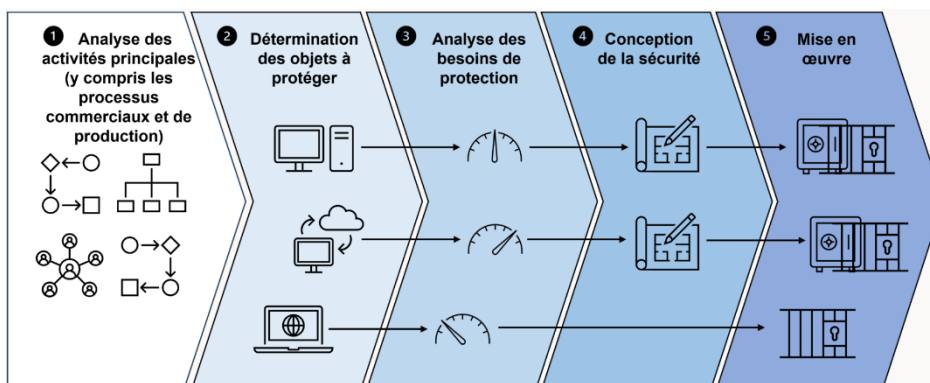


Illustration 4 : Méthode de cybersécurité et de résilience OFCS

Projet de concept d'urgence cyber à l'intention des communes

Les cyberincidents survenus par le passé ainsi que l'enquête communale 2025 de « Myni Gmeind » ont montré que de nombreuses communes peuvent mieux se préparer aux cyberincidents. Afin de permettre aux communes et aux organisations en Suisse de renforcer leur cyberrésilience, l'OFCS a élaboré, en collaboration avec son réseau de partenaires, un modèle de concept d'urgence, des outils pratiques ainsi qu'une vidéo explicative, et les a publiés sur le site Internet de l'OFCS. Les contenus ont été approfondis dans le cadre de deux Brown Bag Lunches en ligne.

Les concepts d'urgence constituent un élément essentiel d'une gestion efficace des risques. Ils permettent d'éviter d'analyser uniquement a posteriori des problèmes potentiels et leurs impacts, mais d'y faire face de manière proactive. En abordant précocement les risques potentiels, les concepts d'urgence permettent d'identifier et de mettre en œuvre des mesures préventives. Ils comprennent l'organisation de crise, un concept de communication de crise ainsi que des contacts d'urgence centraux et des mesures concrètes. Ces éléments constituent la base d'une réaction coordonnée et appropriée dans des situations critiques en termes de temps.

Le processus structuré développé (voir infographie ci-dessous) permet une approche pragmatique de la préparation, de la gestion et du suivi de cyberincidents potentiels.

Grâce à une approche pratique et pragmatique, le concept et les outils associés ont pu être diffusés rapidement.

Les enseignements tirés du projet ne bénéficient pas uniquement aux communes. À partir de 2026, ils seront également adaptés et mis à disposition des PME.

Un groupe d'experts se consacrera en continu à l'optimisation et à l'enrichissement des outils, afin d'intégrer les retours issus de la mise en œuvre ainsi que les nouvelles exigences en matière de cybersécurité.



Illustration 5 : aperçu du concept d'urgence OFCS

Mise en œuvre de la cyberstratégie nationale (CSN)

En 2025, la mise en œuvre opérationnelle de la cyberstratégie nationale (CSN) était au premier plan. Sur la base de la création du comité de pilotage l'année précédente, les structures de gouvernance ont été consolidées et développées de manière ciblée pour la mise en œuvre de la CSN afin de renforcer la coordination entre les nombreux acteurs concernés. À cette fin, des formats d'échange réguliers ont été créés pour favoriser le dialogue et la coopération. L'un des principaux résultats de ces travaux est la conception d'un forum de mise en œuvre de la CSN, qui sera lancé en 2026. Ce forum servira de plateforme pour examiner les progrès réalisés dans la mise en œuvre de la CSN, donner des impulsions pour de nouvelles mesures et soutenir le développement stratégique de la CSN. Une étape importante dans cette voie a été l'atelier de lancement organisé en décembre 2025, auquel ont participé une soixantaine de partenaires de mise en œuvre. L'objectif était de définir les formats des futurs forums. Les discussions ont souligné la grande importance de telles plateformes pour une mise en œuvre réussie de la CSN. Les enseignements tirés sont désormais pris en compte dans la préparation des forums de mise en œuvre réguliers prévus à partir de 2026.

Grâce au développement de la gestion du portefeuille CSN, le portefeuille de mise en œuvre comprend désormais plus de 90 projets, soutenus par plus de 70 partenaires de mise en œuvre et répartis entre les cinq objectifs stratégiques. Un aperçu des projets actifs est disponible sur le site Internet de l'OFCS.¹ En outre, un processus clairement structuré pour l'intégration de nouveaux projets² a été élaboré et publié, afin que les acteurs intéressés puissent appréhender de manière transparente les critères d'intégration dans le portefeuille.

CNCS 2025

Le 25 septembre 2025, le Réseau national de sécurité et l'OFCS ont organisé la Conférence nationale sur la cybersécurité (CNCS) à Berne sur le thème «Cyberrésilience : réglementation ou responsabilité individuelle ?». Environ 250 participants issus de la politique, de l'administration, des milieux économique et scientifiques ont discuté de l'équilibre entre les obligations légales et la responsabilité individuelle de la prise de mesures pour renforcer la résilience numérique. L'événement a offert une plateforme pour l'échange de bonnes pratiques et d'idées pour le développement de la CSN. Des contributions issues de la politique, de la recherche et de la pratique ainsi que des sessions en petits groupes sur la réglementation et la responsabilité individuelle ont souligné la responsabilité conjointe de tous les acteurs.



¹ [Mise en œuvre de la CSN](#)

² [Nouveaux projets CSN](#)

Échange d'informations sur le Cyber Security Hub (CSH)

Le Cyber Security Hub (CSH) est la plateforme centrale pour l'échange opérationnel d'informations entre l'OFCS et les exploitants d'infrastructures critiques. En 2025, le développement technique du CSH s'est poursuivi et a été concentré sur l'obligation de signalement prévue par la loi sur la sécurité de l'information (LSI). Depuis avril 2025, le CSH dispose d'une procédure multilingue de signalement des cyberincidents, qui comprend le signalement initial et le signalement final. Celle-ci a été intégrée dans les processus existants de l'OFCS. En août, la fonction « Share with NCSC » a également été mise en service. Elle permet de transmettre à l'OFCS, via un canal sécurisé, des informations supplémentaires pertinentes pour l'évaluation de la situation en matière de cybermenaces ou pour les mesures de protection des infrastructures critiques. Fin novembre 2025, environ 40 notifications avaient été reçues via ce canal.

En 2025, l'OFCS a également poursuivi les formats établis. Il s'agit notamment du rapport hebdomadaire sur la cybersécurité, qui résume en deux pages les événements et développements les plus importants et informe plus de 6 000 utilisateurs dans environ 1 600 organisations via le CSH. En complément, l'OFCS a poursuivi ses échanges en ligne réguliers sur la cybersécurité. Trente-neuf échanges ont eu lieu en allemand et en français, avec en moyenne près de 400 participants. Ceux-ci offrent à la communauté CSH une plateforme centrale pour un dialogue continu, l'échange d'informations sur les développements et les incidents actuels, ainsi que la mise en réseau des organisations participantes.

Cyber Threat Intelligence

Dans le domaine de la Cyber Threat Intelligence, l'OFCS a réalisé des progrès importants en matière de détection et d'endiguement de cybermenaces complexes. Il convient de souligner en particulier l'identification et l'analyse d'un vaste réseau dit ORB (Operational Relay Box). Il s'agit d'infrastructures dissimulées utilisées par des acteurs soutenus par des États afin de masquer des cyberattaques. L'OFCS a pu identifier un réseau comprenant plus de 2 000 systèmes compromis et partager les enseignements tirés dans le cadre de la coopération internationale. L'utilisation abusive de ces systèmes a ainsi pu être efficacement limitée.

Parallèlement, l'OFCS a observé une menace croissante pour la Suisse de la part du groupe connu sous le nom de « Trader Traitor », derrière lequel se trouvent vraisemblablement des groupements nord-coréens. Leurs activités visent notamment des entreprises actives dans les domaines de la finance et des cryptomonnaies. Les attaquants recourent en particulier à des méthodes de « social engineering », en contactant de manière ciblée des spécialistes au moyen de prétendues offres d'emploi et en les incitant à exécuter des logiciels malveillants.

L'OFCS suit ces menaces de manière continue et a mis en œuvre, durant l'année sous revue, plusieurs mesures techniques de sensibilisation à l'intention des organisations partenaires. Grâce à la diffusion ciblée d'avertissements et d'indicateurs techniques, l'OFCS a apporté une contribution importante à la prévention des infections et au renforcement des capacités de défense des organisations concernées.

Initiatives sectorielles

En 2025, le programme des Cyber Security Centres (CSC) a continué d'être développé. Les Cyber Security Centres sont des centres de compétences et de coopération dans le domaine de la cybersécurité, mis en place dans différents secteurs économiques et d'infrastructures. Le concept vise à regrouper les connaissances propres à une branche ou à un secteur et à les relier à l'OFCS.

L'accent a été mis sur le renforcement de la coopération entre l'OFCS et le Swiss Financial Sector CSC (FS-CSC). Grâce à un nouvel accord de coopération, les deux organisations unissent leurs forces pour lutter de manière ciblée contre les cyberrisques croissants dans le secteur financier. Au cœur de ce partenariat se trouve un échange d'informations structuré : les analystes du FS-CSC ont accès aux données pertinentes de l'OFCS et établissent sur cette base des rapports de situation et des analyses pour la place financière suisse. Ces conclusions sont intégrées dans le travail des membres et dans le CSH et renforcent l'évaluation globale de la situation. Outre le secteur financier, deux autres centres sectoriels ont été créés : le Healthcare-CSC et le Rail ISAC. À l'issue de la phase pilote, le Healthcare-CSC a été fondé en août 2025 sous la forme d'une association regroupant 18 hôpitaux. Il favorise l'échange d'informations sur les menaces, les mesures de protection communes et les bonnes pratiques dans le domaine de la santé.



Illustration 6 : Signature du nouvel accord de coopération avec le FS-CSC

Parallèlement, une plateforme a été mise en place avec le Rail ISAC afin d'aider le secteur ferroviaire suisse à se défendre contre les cyberattaques.

En complément des CSC, l'OFCS a encouragé les échanges sectoriels avec les organisations d'approvisionnement en électricité en organisant deux tables rondes. Celles-ci ont permis de communiquer sur la situation actuelle en matière de menaces et de faciliter les échanges entre les participants sur des questions spécifiques au secteur.

Guichet unique suisse pour les cyberincidents

L'OFCS reçoit des annonces volontaires de la population et des entreprises en Suisse via ce point de contact. En 2025, l'OFCS a reçu 64 733 signalements, ce qui lui a permis d'identifier à un stade précoce les évolutions et les nouveaux dangers sur Internet et de publier les avertissements correspondants. En outre, grâce aux informations contenues dans les signalements volontaires, des rapports sur les dangers actuels ont pu être publiés chaque semaine sur le site Internet de l'OFCS.

Les tentatives de fraude ont été les plus fréquemment signalées. Une autre tendance claire a été l'évolution dans le domaine des attaques de phishing. Si des courriels de phishing génériques ont continué d'être détectés, on observe une nette tendance vers des méthodes d'attaque de plus en plus personnalisées. Les tentatives de fraude liées aux petites annonces en ligne ont notamment augmenté de manière significative. En outre, les tentatives de fraude et de phishing par téléphone se sont également généralisées. La barrière linguistique, qui était jusqu'à présent considérée comme un obstacle, joue un rôle de moins en moins important.

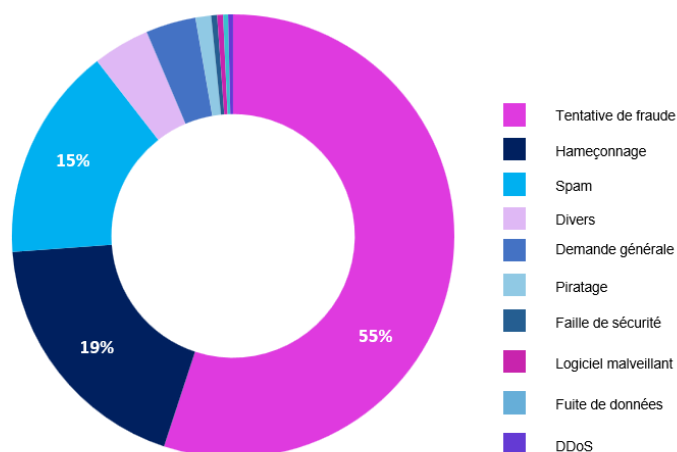
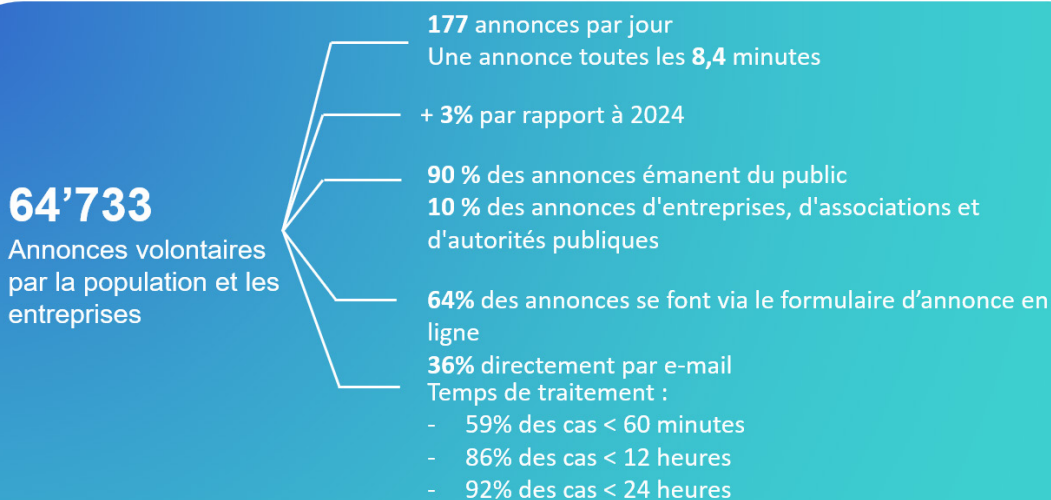


Illustration 7 : Annonces volontaires par catégories principales

Une autre constatation intéressante est l'utilisation accrue de l'intelligence artificielle (IA) par les acteurs criminels afin de rendre les escroqueries plus réalistes et plus convaincantes. L'IA est particulièrement utilisée dans le domaine de la fraude à l'investissement en ligne, par exemple pour créer de faux entretiens ou des contenus publicitaires d'apparence professionnelle.

Au cours de l'année, le formulaire d'annonce public a été adapté aux nouvelles exigences. L'obligation légale de signalement est désormais entièrement intégrée dans le formulaire d'annonce public. De plus, la possibilité de rediriger les déclarants vers le site Internet de Suisse ePolice, où il est possible de déposer une plainte en ligne pour certaines infractions, a été améliorée. La communication avec les personnes effectuant les annonces a également été optimisée : les réponses standards ont été entièrement remaniées et mieux adaptées aux besoins d'information des utilisateurs. Au niveau du traitement interne, les processus ont été encore optimisés, ce qui a permis de réduire le temps de traitement moyen par cas.



Introduction de l'obligation de signaler

Depuis le 1er avril 2025, l'obligation légale de signaler les cyberattaques visant les infrastructures critiques est en vigueur en Suisse. Les exploitantes d'organisations soumises à l'obligation de signaler – par exemple dans les domaines de l'approvisionnement en énergie ou en eau potable, des transports ou des administrations cantonales et communales – doivent désormais signaler les cyberattaques à l'OFCS dans un délai de 24 heures après leur découverte.

Cette nouvelle obligation a été introduite dans le cadre d'une révision de la loi sur la sécurité de l'information (LSI) et est inscrite aux articles 73 et suivants de la LSI. L'obligation de signaler est précisée par la nouvelle ordonnance sur la cybersécurité (OCyS), également entrée en vigueur le 1er avril 2025. Les organisations soumises à l'obligation de signaler sont définies à l'article 74b LSI, tandis que les exceptions sont réglées à l'article 16 OCyS.

Afin de rendre le processus de signalement aussi simple que possible, l'OFCS met à la disposition des organisations soumises à l'obligation de signaler le Cyber Security Hub (CSH) en tant que plateforme centrale de signalement, ainsi que des vidéos explicatives et des fiches d'information d'accompagnement. Ces efforts ont porté leurs fruits : les organisations concernées ont respecté leurs obligations dans les délais impartis et les signalements ont été effectués dans le cadre prévu. Jusqu'à la fin de l'année 2025, 222 signalements ont été reçus. Les signalements transmis permettent à l'OFCS d'améliorer l'analyse de la situation des cybermenaces en Suisse. Ils contribuent à identifier et à analyser précocement des schémas d'attaque visant les infrastructures critiques, ce qui permet d'alerter en temps utile les organisations potentiellement concernées afin qu'elles puissent prendre des mesures de prévention et de défense appropriées.

Les organisations les plus nombreuses à avoir signalé des incidents sont celles de l'administration publique, du secteur de l'information et de la communication, ainsi que les entreprises financières et les compagnies d'assurance. L'analyse des cas signalés montre que les types d'attaques les plus fréquents sont le piratage (19,5 %), suivi par les attaques DDoS (17,6 %) et le vol de données d'accès (11,8 %). Les logiciels malveillants (9,5 %), les attaques par ransomware (9,2 %) et les fuites de données (8,8 %) ont également fait l'objet d'un nombre croissant de signalements.

Le 1er octobre 2025, les dispositions relatives aux sanctions sont également entrées en vigueur. Elles prévoient des amendes pouvant aller jusqu'à 100 000 francs suisses en cas de non-respect de l'obligation de signalement après une procédure de mise en demeure. Les premiers mois montrent toutefois que les organisations soumises à l'obligation de signalement prennent la nouvelle réglementation au sérieux et assument leur responsabilité en matière de cybersécurité nationale.

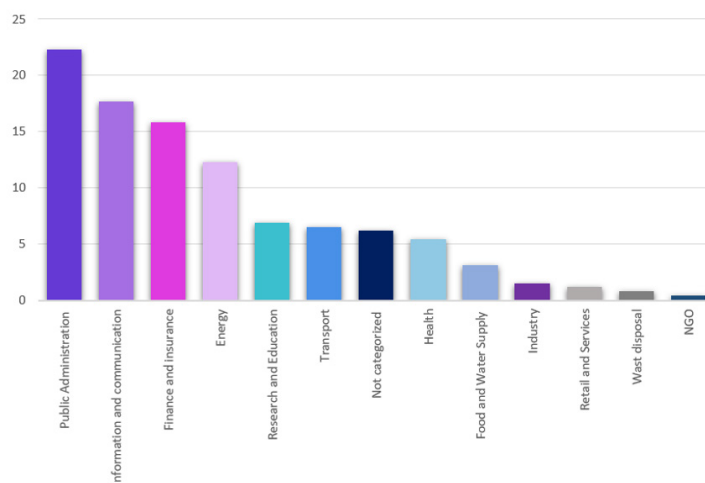


Illustration 8 : Signalements d'attaques traités par secteur principal en pourcentage

3 Réduction des dommages dus aux cyberincidents

Alertes relatives aux cybermenaces graves désormais aussi via Alertswiss

Afin d'alerter encore plus efficacement la population et les entreprises face à des cybermenaces graves, l'OFCS a renforcé sa collaboration avec l'Office fédéral de la protection de la population (OFPP). Depuis la mi-septembre, des alertes peuvent également être diffusées via l'application Alertswiss ainsi que la plateforme Internet Alertswiss. Un canal supplémentaire est ainsi disponible pour informer rapidement la population, l'alerter et la protéger au moyen de recommandations d'action concrètes en cas de cyberattaques de grande ampleur ou de nature nouvelle.

Engagements de l'OFCS lors d'événements de grande envergure

En 2025 également, l'OFCS a assuré la coordination centrale de la cybersécurité au sein du réseau de situation cyber lors de trois événements de grande envergure : le Forum économique mondial (WEF) en janvier, le Concours Eurovision de la chanson (ESC) en mai et l'Euro féminin de l'UEFA en juillet. Un élément central de ces engagements a été la détection précoce et l'analyse des menaces. L'OFCS a évalué des indicateurs et des signalements, élaboré des scénarios de menace et transmis en temps utile des avertissements aux exploitantes d'infrastructures critiques afin qu'elles puissent prendre des mesures de protection préventives. En parallèle, un soutien opérationnel a été fourni, allant de recommandations techniques à la coordination de la réponse aux incidents, jusqu'à une assistance directe dans la gestion d'attaques en cours.

Les engagements ont été menés dans le cadre étroit du réseau de situation cyber et en étroite collaboration avec les organisateurs, la police et d'autres autorités fédérales. Grâce à des conférences de situation communes, des canaux de communication coordonnés et des processus de signalement standardisés, les délais de réaction ont pu être réduits et les flux d'information sécurisés.



Échange d'informations

La plateforme MISP (Malware Information Sharing Platform) exploitée par l'OFCS a également été utilisée en 2025 comme instrument central pour l'échange automatisé d'informations techniques sur les cyberincidents. Elle soutient la protection proactive des infrastructures critiques suisses en permettant un flux d'informations rapide entre les partenaires nationaux et internationaux ainsi que les organisations concernées. Des informations techniques sur 4615 incidents de cybersécurité (événements MISP) ont été échangées via la plateforme. Il s'agit d'informations provenant tant de la Suisse que de l'étranger. En outre, l'OFCS a intégré 30 nouveaux exploitants d'infrastructures critiques suisses à la plateforme MISP. Outre la plateforme MISP qui est réservée aux exploitants d'infrastructures critiques, l'OFCS exploite trois autres plateformes de ce type pour d'autres groupes d'intérêt, tels que les corps de police cantonaux et nationaux.

4 Augmentation de la sécurité des produits et prestations numériques

Les vulnérabilités des logiciels et du matériel constituent des vecteurs d'attaque centraux pour les cyberattaques. L'OFCS met donc l'accent sur la vérification ciblée de composants critiques sur lesquels reposent l'administration et l'économie. Au cours de l'année sous revue, deux priorités ont été au premier plan : le programme établi de prime aux bogues (bug bounty) de l'administration fédérale et un projet pilote relatif à la sécurité des logiciels open source.

Open source

Les logiciels libres (Open Source Software, OSS) jouent déjà aujourd'hui un rôle important dans l'exploitation sécurisée des infrastructures critiques, car les logiciels utilisés actuellement ont souvent recours à des logiciels libres. Afin de renforcer activement la sécurité des logiciels libres, l'OFCS a mené, en collaboration avec l'Institut national de test pour la cybersécurité (NTC), un projet pilote dans le cadre duquel les applications « TYPO3 » et « QGIS » ont été testées à titre d'exemple. L'étude a confirmé que même les projets bien établis présentaient des failles importantes. Celles-ci ont été corrigées dans le cadre du projet, en collaboration directe avec les communautés de développeurs. L'OFCS utilise désormais ces conclusions pour élaborer les bases d'un soutien durable de la Confédération en matière de sécurité des logiciels libres.

L'OFCS a également introduit une stratégie open source contraignante et établi le principe de travail « open source par défaut ». L'OFCS renforce ainsi l'interopérabilité et la capacité d'innovation de ses produits et crée des bases ouvertes pour les projets, les architectures et les achats.

Bug Bounty

Le programme Bug Bounty de l'administration fédérale s'est imposé comme un instrument efficace et un complément indispensable aux tests de sécurité classiques. Des hackers éthiques vérifient les systèmes de la Confédération selon des règles clairement définies. Comme les primes (« bounties ») ne sont versées que pour les vulnérabilités techniquement validées ayant un impact démontrable, ce modèle est extrêmement rentable. Les ressources financières sont ainsi utilisées de manière ciblée là où il existe des risques réels. Le programme Bug Bounty permet d'identifier régulièrement des vulnérabilités pertinentes et critiques qui ne sont pas toujours détectées lors des tests conventionnels. En 2025, l'OFCS a reçu au total 525 signalements de vulnérabilités potentielles. Après analyse et vérification, 328 signalements ont été reconnus comme valables et ont donné lieu à des mesures visant à corriger ou à améliorer la sécurité au sein de l'administration fédérale. Des primes d'un montant total d'environ 260 000 francs suisses ont été versées pour ces signalements.

L'OFCS poursuit le programme Bug Bounty et s'engage à ancrer ce type de programme comme un instrument établi de la sécurité de l'information en Suisse.

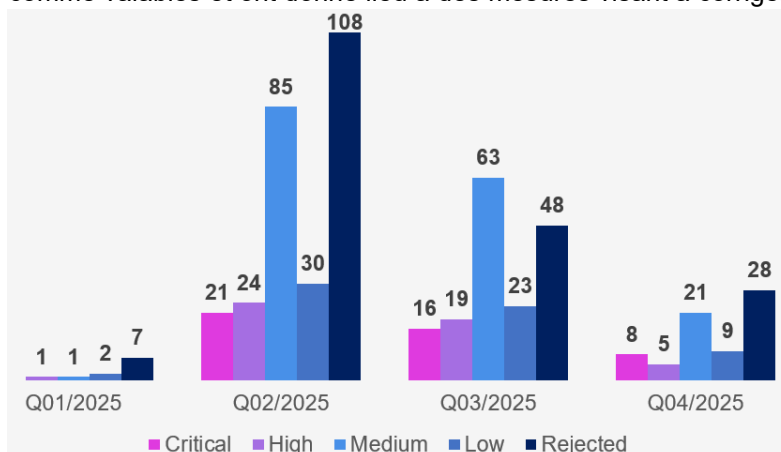


Illustration 9 : Vulnérabilités signalées et leur classification

Gestion axée sur les effets de l'OFCS

Dans le cadre de son concept d'exploitation, l'OFCS développe et optimise en permanence ses instruments de planification et de pilotage. Cela s'inscrit notamment dans une volonté de transparence et de traçabilité, dans le contexte global de l'administration fédérale.

La gestion axée sur les effets de l'OFCS inscrit la mission de base, ainsi que l'ensemble des activités clés qui y sont liées, dans un processus structuré et aligné, et offre une visibilité sur les différents niveaux d'effets. Les outputs renseignent sur les prestations et les produits fournis par l'office, tandis que les outcomes et les impacts se concentrent sur les effets à moyen et long terme recherchés auprès des groupes cibles concernés et de certaines parties de la société. Le long des activités clés de l'office, l'ensemble des chaînes d'effets est géré de manière cohérente dans le portefeuille organisationnel et relié à des programmes, des projets et d'autres initiatives.

La mise en œuvre coordonnée et ciblée des thèmes stratégiques dans le cadre du mandat légal continue de s'effectuer au sein de l'office selon la méthodologie OKR (Objectives & Key Results). La priorisation, la planification et le pilotage rigoureux, sur une base trimestrielle, des ressources financières, humaines et temporelles nécessaires, ainsi que le contrôle associé sous la forme de la vérification de l'atteinte des résultats, garantissent une mise en œuvre efficace de la stratégie. Après son introduction l'année précédente, cette méthode de gestion a pu être davantage ancrée en 2025. Un accent particulier est notamment mis sur la collaboration coordonnée, tout en favorisant l'autonomie des équipes au sein de l'OFCS.

Grâce à sa vue d'ensemble, la gestion axée sur les effets offre une approche globale des activités de l'organisation et permet d'appréhender les changements éventuels de manière holistique, afin d'en déduire des pistes de solution appropriées. L'objectif est que les instruments de planification et de pilotage de l'OFCS fournissent en permanence une orientation claire et soutiennent une capacité d'action dynamique.

Dans son ensemble, la gestion axée sur les effets permet une vision globale des activités de l'office. Elle crée de l'orientation, rend les interconnexions visibles et permet de détecter les évolutions à un stade précoce afin d'y réagir de manière ciblée. Elle constitue ainsi la base d'une action apprenante et orientée vers les effets, et soutient l'OFCS dans l'accomplissement fiable, transparent et ciblé de son mandat, aujourd'hui comme à l'avenir.

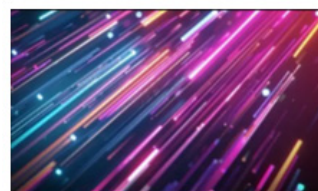


Illustration 10 – 14 : OKR OFCS

Publications et références

Publications de l'OFCS en 2025

- [Le concept d'urgence, clé de la cyberrésilience](#)
- [Premier rapport de mise en œuvre de la stratégie nationale en matière de cybersécurité \(NCS\)](#)
- [Considérations technologiques : ordinateurs quantiques et cryptographie post-quantique](#)
- [Considérations technologiques : cybersécurité et cyber-résilience](#)
- [Considérations technologiques : clés d'accès](#)
- [Communiqués de presse](#)
- [Mesurabilité et vérifiabilité de la sécurité informatique](#)
- [Considérations technologiques : informatique confidentielle](#)
- [Considérations technologiques : cloud computing](#)
- [Considérations technologiques : SCION](#)
- [Rétrospectives hebdomadaires](#)
- [Rapport semestriel 2024/2](#)
- [Rapport semestriel 2025/1](#)
- [Stratégie open source BACS](#) (disponible uniquement en allemand)

Articles scientifiques

A. Grünert, J. B. Michael, R. Oppliger, and R. Rytz, "On the measurability and testability of IT security," *Computer*, vol. 57, no. 3, pp. 120–126, Mar. 2025, <https://ieeexplore.ieee.org/document/10896924>