Centre Réseau & Informatique Commun

A Mmes & MM. les utilisateurs du Système d'Informations
CNRS Grenoble − Polygone Scientifique
Grenoble, décembre 2025

Rapport d'activités 2025

Introduction

Cette année 2025 a été riche en nouveautés : déploiement de nouvelles mesures de sécurité, arrivée de Malika Mebrouk en CDD après son apprentissage, embauche de Giovanni Bonsignore en CDD, de nouveaux services offerts.
Ces nouveautés servent aussi de moteur à l'activité CRIC : toujours proposer des services mutualisés performants et sécurisés à nos utilisateurs.
Vous trouverez dans la suite de ce document les détails de ces évolutions.
Pour finir, nous vous souhaitons une bonne et heureuse année 2026, sans faille de sécurité informatique.

Contexte général

De nouveaux personnels sont arrivés en 2025 : il s'agit de Malika Mebrouk et Giovanni Bonsignore. Giovanni est arrivé le 1er janvier en CDD pour 12 mois et Malika est arrivée depuis octobre pour 18 mois, à l'issue de son Master en alternance. Ils supportent les infrastructures systèmes et réseau du CRIC. Ces deux CDD permettent à Dominique Fournier de se passer plus de temps sur ses missions de Responsable de la Sécurité des Systèmes d'Information.
La DINUM (DIrection du NUMérique) fournit aux agents de l'état des outils informatiques de qualité. Nous ne pouvons que promouvoir leur usage que ce soit Tchap (pour la partie communication instantanée), Visio (pour les conférences vidéos), Resana (pour les espaces collaboratifs). Ces outils nous ont permis d'arrêter le service BBB CNRS national, dont Dominique Fournier était un des gestionnaires.
En local, du fait de l'augmentation de la taille de l'équipe nous avons mis en place un gestionnaire de ticket, disponible au travers de l'adresse support : CRIC@grenoble.cnrs.fr.

Activités liées aux Systèmes

Mise à jour de l'infrastructure Kubernetes

La première mission de Malika a été de mettre à jour l'infrastructure Kubernetes. En effet, une couche de sécurité supplémentaire a été mise en place afin de bloquer les téléchargements des containers directement depuis Internet. Ainsi, si la plateforme est piratée, les attaquants ne pourront pas aller facilement récupérer des charges depuis les sites extérieurs.

Logiciel de partage de données sécurisé

Un nouveau service a été ouvert : il s'agit d'un logiciel libre installé à l'adresse https ://yopass.grenoble.cnrs.fr qui permet d'échanger des données de manière sécurisée. La donnée est chiffrée sur le poste utilisateur et ne peut être déchiffrée que par le destinataire, et elle ne peut être téléchargée qu'une seule fois.

Messagerie : Ajout de SRS et SPF bloquant

Tous les domaines hébergés sur notre infrastructure ont maintenant une vérification des serveurs autorisés à l'émission. Ainsi un mail venant d'une de nos unités, mais d'un serveur hors de notre périmètre pourra être considéré comme spam par nos correspondants.
Cette fonctionnalité peut poser des problèmes lors des redirections, si les informaticiens des serveurs hébergeant les redirections ne mettre pas en place une mesure technique nommée SRS (Sender Rewriting Scheme), qui vérifie si la redirection est autorisé et corrige le mail si ce n'est pas le cas.
Au CRIC, nous avons mis en place une passerelle SRS qui permet aux personnes ayant mis une redirection que celle-ci fonctionne correctement avec les destinataires.
Messagerie : Blocage automatique en cas d'envoi massif
Les pirates qui récupèrent un couple identifiant/mot de passe l'utilisent immédiatement sur la messagerie pour envoyer du spam en très grand nombre. La réputation de nos serveurs est alors dégradée, ce qui impacte

tous les utilisateurs de la plateforme. Afin de luter contre ce fléau, nous avons mis en place une solution de bannissement du compte envoyant trop de mails dans une période d'une journée.
Pour rappel, l'envoi d'un grand nombre de mails est toujours possible au travers du serveur de listes.
Pensez à utiliser un mot de passe fort et utilisé uniquement sur notre messagerie. Un gestionnaire de mot de passe est aussi précieux pour avoir des mots de passe différents sur tous les sites.

Mise en place du second facteur d'authentification (2FA)

Il est maintenant possible d'activer un second facteur d'authentification (2FA) sur le service nextcloud ou sur le service de messagerie. Le 2FA est un code qui est fourni par une application installée sur votre téléphone. Ce code change toutes les 30s. Si un pirate arrive a obtenir votre identifiant et votre mot de passe, il ne pourra pas avoir accès à votre téléphone, ce qui lui empêchera l'accès à vos données.

Activités liées au Réseau

Mise en place d'un Network Detection and Response (NDR)

Afin de luter contre les machines vérolées connectées à nos laboratoires qui feraient des connexions réseaux vers des serveurs d'envoi de spam, d'attaque, etc, nous avons déployé au CRIC un *Network Detection and Response* (NDR). Cet outil détecte le trafic réseau illégitime et bloque alors l'adresse IP qui l'a produit. Le blocage ne sera activé qu'en 2026, une fois les premières détections validées.

Départ de GreenER / G2ELab / Minatec

Depuis de très nombreuses années, les laboratoires GreenER/G2ELab/Minatec étaient connectés sur nos cœurs de réseau. Ils ont décidé de se connecter derrière les pare-feux de Grenoble INP-UGA, ce qui a été fait sans interruption de service pour les utilisateurs.

Modification des certificats EduRoam

Un changement majeur dans l'infrastructure Eduroam a été le changement de l'autorité de certification vérifiant les serveurs autorisés à authentifier nos utilisateurs. Nous avons quitté Sectigo pour Harica. Ce fut un changement majeur car tous les ordinateurs ou téléphones utilisant ce réseau ont dû être reconfigurés. Un outil est disponible pour le faire : il s'agit du CAT *Configuration Assistant Tool*. Seul l'utilisation de cet outil garantit que votre mot de passe utilisateur ne sera pas transmis à des serveurs pirates qui s'annonceraient comme Eduroam.

Activités liées à la Sécurité

Automatisation de la cartographie

La législation NIS1 et encore plus NIS2 impose de faire des cartographies des services et infrastructures que nous administrons. Cette cartographie est longue à réaliser. Afin d'optimiser notre travail, Malika Mebrouk a écrit un programme qui se base sur les solutions d'inventaire OCS-Inventory pour créer automatiquement certaines cartographies dans Mercator, un outil qui suit les recommandations de l'ANSSI.
Toute la partie physique, les serveurs virtuels, le réseau sont alors automatiquement insérés en quelques minutes. Cela permet de maintenir à jour cette cartographie qui pourra être utilisée le jour où nous auront besoin d'être aidés par un Prestataire de Réponse à Incident de Sécurité.
Cet outil est en cours de diffusion à toutes les unités de la circonscription car il a été présenté à tous les correspondants sécurité informatique. Pour diffusion, cet outil a aussi a été présenté aux autres délégations du CNRS par Dominique Fournier pour une ouverture au national.

Malika a aussi mis à jour le plugin de OCS-Inventory afin de récupérer l'ensemble des règles de pare-feux de l'infrastructure, ce qui permettra de créer automatiquement la matrice des flux autorisés entre nos équipements.

Mise en place d'un Web Application Firewall (WAF)

Afin de protéger les nombreux sites web qui sont hébergés au CRIC, Giovanni Bonsignore a mis en place un Web Application Firewall (WAF). Cet outil libre permet de bloquer les tentatives de piratage de nos sites et les scans qui cherchent des vulnérabilités dans nos serveurs. Cet outil libre et gratuit a été progressivement déployé et bloque quotidiennement des milliers de connexions non souhaitées, tout en laissant passer le trafic légitime.

Mise en place d'un second étage de pare-feu

Nous avons utilisé notre firewall principal pour mettre en place une couche complémentaire de sécurité. Ainsi, deux équipement différents bloquent les attaques venant d'Internet. Il est ainsi possible d'être plus sereins

Et dans le futur ?

En 2026, nous devrons pérenniser les personnes en CDD afin de maintenir une bonne qualité de service.

Dans les évolutions techniques, nous allons devoir envisager de changer notre infrastructure technique hébergeant la téléphonie sur IP.

Nous vous souhaitons encore une bonne et heureuse année 2026, avec peu de failles de sécurité.