Centre Réseau & Informatique Commun

A Mmes & MM. les utilisateurs du Système d'Informations

CNRS Grenoble − Polygone Scientifique

Grenoble, décembre 2024

Rapport d'activités 2024

Contexte général

Une nouvelle fois, l'année 2024 a démarré dans un contexte particulièrement sensible au niveau de la cyber sécurité. Afin de maintenir un SI performant et sécurisé nous avons dû rester vigilants tout au long de l'année.

De plus l'absence prolongée de Guillaume Gielly a rendu la situation très complexe. En effet l'ensemble de ses activités ont reposé sur Dominique Fournier, avec l'aide de Grégory Arnéodo et de Clara-Lou Pahisa.

À partir de janvier 2025. Un nouveau collègue va arriver pour reprendre cette mission : il s'agit de Giovanni Bonsignore, en CDD pour un an. Bienvenue à lui !

La suite de ce bilan décrit dans le détail les aspects techniques et organisationnels mis en œuvre en 2024.

Activités liées aux Systèmes

Plateforme de messagerie Zimbra

Notre plateforme Zimbra a été migrée en version 10 sur une plateforme Ubuntu 22. Cette migration est toujours un moment compliqué pour nous puisqu'il faut transférer l'ensemble des mails sur un nouveau serveur, tout en limitant la coupure de service pour nos utilisateurs.

La société qui développe Zimbra nous avait imposé cette migration avant fin 2024. Cette opération a été un franc succès et notre infrastructure est à nouveau supportée par l'éditeur.

Outil de suivi des consommations électriques

Un outil basé sur Grafana a été mis en place afin de donner aux laboratoires une visualisation graphique et au format tableau des valeurs des consommations électriques du site. Il permet de repérer les pics et les tendances, mais aussi de fournir les données brutes pour les laboratoires qui le souhaitent.

Cet outil ne permet pas de gérer le prix payé, seulement les index de tous les compteurs du site. La partie facturation est un travail a temps plein et ne peut être mené avec les moyens actuels.

Activités liées au Réseau

Mise en place d'un nouveau pare-feu

Nos équipements de routage fournissant l'accès Internet à l'ensemble des unités avaient atteint leur fin de vie après 7 ans de travail sans faute. Ils ont été remplacés par deux firewall Fortinet qui assurent le routage mais aussi ajoutent une couche de filtrage de sécurité.

Chaque laboratoire connecté sur les équipements aura la possibilité de mettre en place des règles de filtrage en plus de leur propre pare-feu. C'est la recommandation de l'ANSSI qui est ainsi déployée, afin qu'une faille dans un pare-feu n'ouvre pas l'accès à l'ensemble de l'infrastructure.

Déploiement de Mercator

Mercator est un outil permettant de visualiser les différents équipements de notre infrastructure, d'établir les connexions entre ces différents équipements, de voir les services qui sont activés sur chacun.

Il a été déployé et peut être utilisé par un Prestataire de Réponse à Incident de Sécurité. C'est l'outil qui est recommandé par l'ANSSI.

Notre alternante, Malika Mebrouk, va travailler sur 2025 afin de rendre cet outil plus automatique.

Activités liées à la Sécurité

Plusieurs chantiers liés à la sécurité ont été conduits.

Test d'une solution de Network Detection and Response

Un NDR (Network Detection and Response) est un outil qui analyse les flux réseaux afin de découvrir des ordinateurs qui seraient compromis.

Pour être plus précis un NDR permet de détecter et de contenir les activités malveillantes post-intrusion, telles que les rançongiciel, le vol de données, ainsi que les attaques internes.

Contrairement à un antivirus le fonctionnement du NDR repose essentiellement sur l'identification de modèles de comportement anormaux et d'anomalies plutôt que sur la détection de signatures

Nous avons mis en test pendant un mois un équipement sur le réseau du CRIC afin de mesurer sa capacité de réaction face aux incidents.

Malheureusement, nous n'avons pas valider la solution à cause de coût sur le long terme trop élevé. Ceci nous oblige à choisir une autre solution.

Nous allons reprendre ce projet avec un autre prestataire pendant l'année 2025.

Analyse des logs et sécurisation de Kubernetes

La conférence des Journées Réseaux de l'Enseignement Supérieur a eu lieu en décembre 2024, à Rennes. Nous avons présenté deux projets : l'analyse de logs et la sécurisation des environnements Kubernetes.

Ce moment a été très instructif et nous avons pu discuter de nos projets avec des personnes ayant les mêmes objectifs.

Et dans le futur ?

En 2025, nous aurons à nouveau plein de projets intéressants :

Nous allons changer deux serveurs de Virtualisation (les anciens ont été achetés en 2009),

Nous allons travailler sur le plan de mise en sécurité avec tous les téléphones du site,

Une ré-écriture de l'application Visiteurs est prévue, afin d'être à jour des bibliothèques nécessaires à son fonctionnement. Nous en profiterons pour rajouter des éléments de sécurité complémentaires.

Comme indiqué précédemment, nous allons reprendre notre travail sur la mise en place d'une solution NDR.

Enfin, nous accompagnerons de la migration de la messagerie @cnrs.fr vers le Zimbra de Renater.