RETEX 24h IUT 2025 - Cyber

Lucas Tesson, Nicolas Faugeroux, Richard Chauve

CTFer.io, en collaboration avec l'Université Claude Bernard Lyon 1, IUT Informatique Site de la Doua

Table des matières

1 Contexte

« **CTFer.io** » est une *Organisation Gratuite en Source Ouvertes* (dite sous statut de « FOSS »). Elle rassemble des experts techniques dans la réalisation d'infrastructure d'événements de type « Capture The Flag » (abrégé *CTF*), et accompagne bénévolement des événements publics comme privés, nationaux commme internationaux, depuis 2023 (sa création). Elle fut fondée par Lucas Tesson et Nicolas Faugeroux. En début 2025, Richard Chauve rejoint l'équipe.

« **24h IUT 2025** » est un événement annuel ouvert aux étudiants des parcours Informatique des IUT de France (incluant les DOM-TOM). L'édition 2025 est à charge de l'IUT Lyon 1 sur son site de La Doua (Villeurbanne). Ses acteurs principaux sont : Nadège Bazin, Antony Busson, Nicolas Buyle-Bodin, Noura Faci, Samba Ndiaye, Adrien Peytavie, Vincent Vidal, Rémi Watrigant, et Lionel Pozet.

L'« **ENSIBS** » est une école d'ingénieurs notamment connu pour son parcours Cyberdéfense dont sont issues les collaborateurs de **CTFer.io**. L'école a fourni gracieusement la majorité du matériel exploité lors de l'événement pour constituer l'infrastructure. Les membres de la White Cell ayant procédé au prêt de matériel sont : Elian Privat, Bertrand Rougeron, et Lionel Delaby.

Lors des **24h IUT 2025**, **CTFer.io** est en charge de l'organisation de l'épreuve de Cyber, ainsi que de la propagation du réseau, de l'authentification des participants et de la sécurisation des flux.
Pour porter l'événement nous l'avons axé autour d'une histoire (dit « lore ») annoncée en Figure 1.

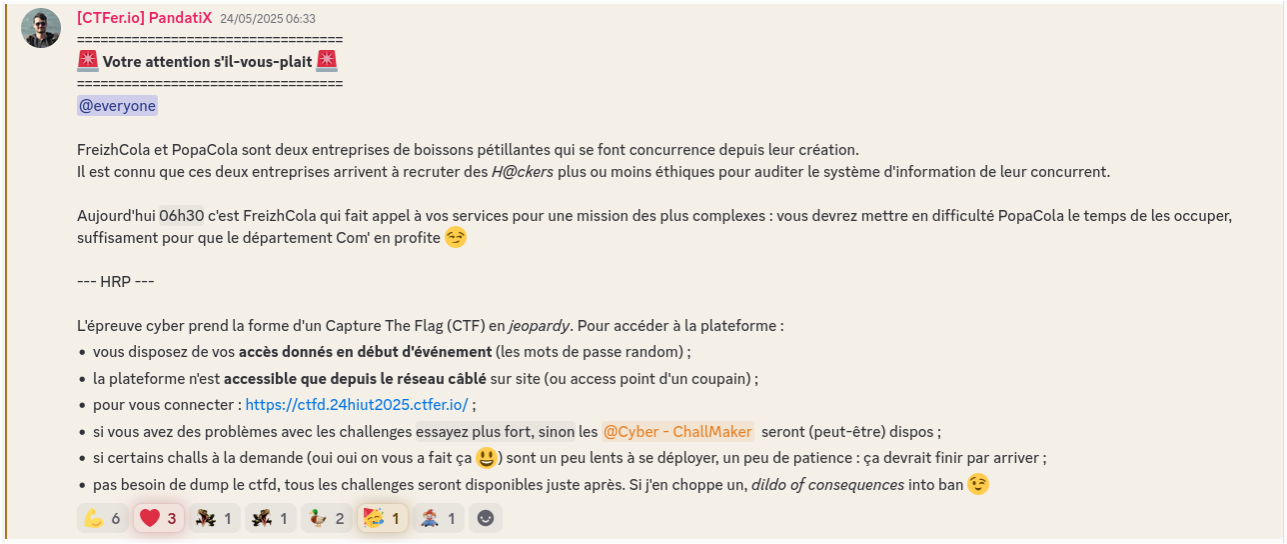


FIGURE 1 – Annonce du lancement de l'événement, accompagné du lore.

2 Objet

Le RETEX (**RET**our d'**EX**périence) est une documentation réalisée après la fin de l'événement, dont l'objectif est de détailler et expliquer les architectures, innovations, développements, réfléxions et actions entreprises par *CTFer.io*. De plus, il contient les observations et remarques organisationnelles et techniques sur l'événement, ainsi que des pistes d'améliorations pour les futures éditions. Toutefois, le RETEX n'a pas vocation à être exhaustif, ou un tutoriel pour reproduire une telle infrastructure et organisation.

Ce document est premièrement à visée interne, et constitue la conclusion d'un événement. Ensuite, il est à visée des participants pour étayer leur compréhension de l'environnement dans lequel ils ont opéré. Enfin, il est à visée des autres organisateurs, accompagnants, et externes à l'événement, désireux de comprendre l'apport de *CTFer.io* à l'événement.

L'un d'eux est la maîtrise d'infrastructure d'événements de type Capture The Flag (abrégé « CTF »). Ainsi, sur les 32 challenges de l'événement (29 joués), 10 d'entre eux requérait des infrastructures, et 9 à la demande. Le tout était à gérer pour 162 participants répartis en 41 équipes.

Ce RETEX commencera par un grande section d'architecture en Section 3, puis d'une analyse du déroulé de l'événement en Section 4, d'une section particulière dédiée aux incidents et leur analyse en Section 5, et enfin d'un retour global en Section 6.

3 Architecture

Cette section reprend la mise en place de l'infrastructure. Elle commence par la Section 3.1 détaillant le montage physique, puis par la Section 3.2 expliquant une grande partie du montage logiciel.

3.1 Architecture physique

Lors des 24h IUT 2025, nous disposions d'un serveur T320 utilisé habituellement pour héberger les infrastructures de développement de CTFer.io. Toutefois, pour atteindre les capacités de production pour 160 participants, nous avions besoin de plus grands moyens. Pour ce faire, l'ENSIBS nous a gracieusement prêté une baie conçue pour être à la fois réinstallée au besoin, mais aussi facilement projetée sur des événements : la baie « Boo » de Donk'esport. À cela, l'ENSIBS ajoute plusieurs serveurs raquables, ainsi qu'un serveur au format tour. Ainsi nous atteignons une capacité de calcul de 204 CPUs et 800 Go de RAM. En réorganisant les disques des serveurs raquables, nous moyennons pour chaque serveur un RAID0 de 2 To. Cela était nécessaire pour les Lab AD (Section 3.2.3), dû aux estimations de 80 VM de 20 Go, soit 1.6 To de charge potentielle.

Pour le transport, l'UCBL1 a loué un fourgon de 13m^3. Sans hayon, la baie et ses serveurs, si montés et câblés, serait trop lourde à lever. Ainsi elle est transportée vidée de ses serveurs et équipements réseaux, en dehors de son onduleur. Chaque serveur est transporté individuellement dans un carton, protégé par des mousses adaptées. Les équipements réseaux disposaient d'un carton mutualisé. Cela réduit les risques de basculement de la baie par l'abaissement de son centre de gravité et l'éclatement de son poids au sol. L'alternative d'une chèvre mécanique [1] était une piste, mais n'a pas été poursuivie manque d'en posséder une.

Lors du premier jour sur site, nous avons ainsi déchargé le matériel, raqué, câblé, configuré et testé l'ensemble de l'infrastructure. Grâce à l'anticipation des configurations en amont du déplacement, nous avons gagné énormément en temps de configuration et tests. Sans cela, il aurait été inenvisageable de nous déplacer si peu de temps sur site. En fin de première journée, l'infrastructure en Figure 2 était installée.

FIGURE 2 – Infrastructure physique globale, comprenant la baie Boo, son onduleur, ses 3 équipements réseau (et pare-feu de secours non raccordé), ses 5 serveurs format raquable, ainsi que les 2 serveurs externes format tour.

Ainsi, la configuration matérielle est la suivante.

Aruba 1830 Switch switch chargé d'aggréger les liens au sein de la baie ;

1. https://fr.wikipedia.org/wiki/Ch%C3%A8vre_(outil)

Netgear MS510TX switch câblant les liens des labs AD (Section 3.2.3) ;

Fortigate 101E firewall de cœur ;

Dell Poweredge T320 serveur contenant le lab, permettant de (re)déployer les L3 ;

2 Dell R440 + R430 serveurs de calcul pour les cluters Kubernetes ;

Dell R420 servant aux labs AD, en particulier à la VM « Hacker » ;

HP DL360 Gen10 servant aux labs AD, en particulier aux serveurs ADDS et ADSRV ;

Tower le serveur format tour, servant aux labs AD, en particuler aux serveurs ADDS et les Clients Windows.

Dû à un incident sur la connexion Internet du campus de La Doua, nous avons pu prendre le temps de procéder au câblage de la baie. Les câbles ont été passés pour ne pas entraver le passage des serveurs (léger déplacement sur rail pour maintenance), puis vérouillés pour la lisibilité avec des colliers Colson. Une photo de la façade est en Figure 3.

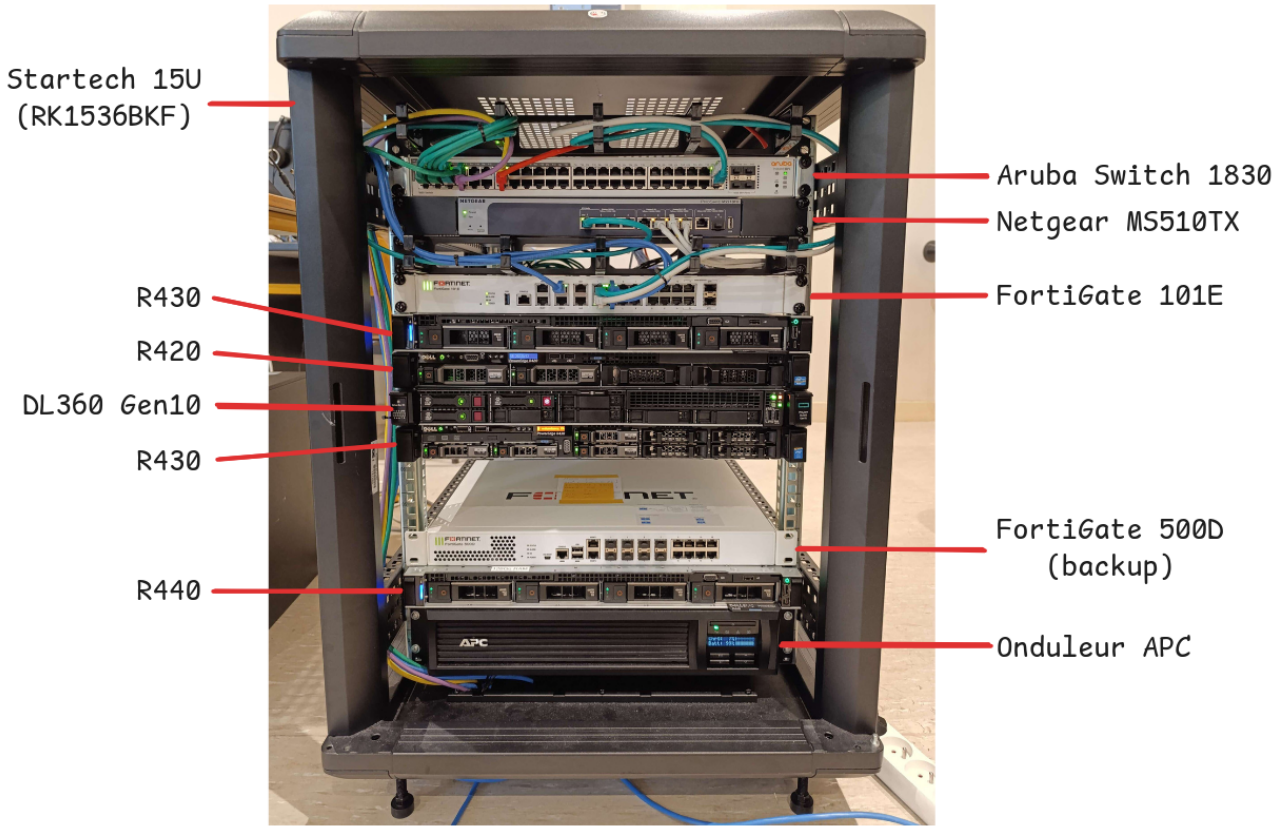


FIGURE 3 – Câblage frontal de la baie.

La configuration réseau du matériel en Figure 3 est détaillé en Figure 4.

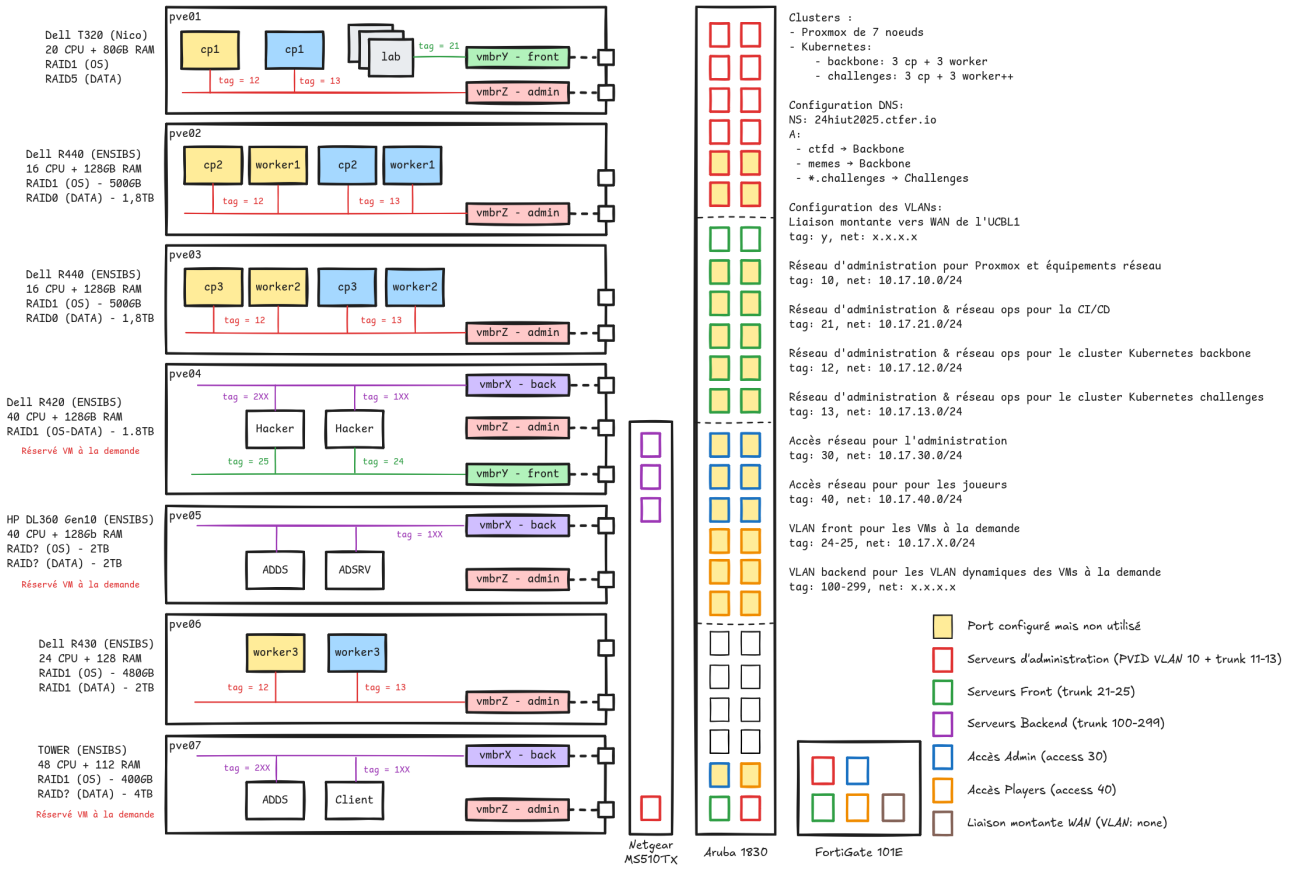


FIGURE 4 – Répartition des charges logiques sur les équipements physiques.

3.2 Architecture logique

Du point de vue logique, l'infrastruture s'axe autour de 2 clusters Kubernetes :

Backbone contenant l'ensemble des services essentiels : plateforme de CTF, bases de données, monitoring, etc. ;

Challenges contenant les challenges déployés à la demande s'hégergeant sur Kubernetes (80% des challenges avec infrastructure).

La présence de 2 clusters est issue d'une analyse de risque portant sur le co-hébergement d'applicatifs sensibles (plateforme de CTF et monitoring, en particulier) avec des applicatifs vulnérables (challenges). En cas de compromission d'un challenge, un attaquant pourrait pivoter vers des services sensibles outrepassant les mesures de sécurité. La mesure atténuatrice a été le déploiement d'un second cluster. Cela est opérationellement facilité par le composant *L3* permettant de déployer un cluster Kubernetes on-premise à la demande en moins de 30 minutes, conforme aux pratiques de CTFer.io.

Pour que Chall-Manager déploie ses applicatifs du cluster « backbone » vers le cluster « challenges », nous avons priorisé la PR #652. Celle-ci permet de passer un `kubeconfig`, qui sera monté dans le filesystem à un point de montage consensuel, i.e. que les outillages vont naturellement retrouver. Ce mécanisme est illustré par la Figure 5.

Afin de déployer la pile applicative au complet (depuis un Kubernetes vierge), nous avons combiné les différents outils nécessaire au sein d'un même programme Pulumi : *fullchain*. Nous déployons ainsi un CTFd [2] répliqué, montons un volume partagé et répliqué par Longhorn [3], une base MariaDB [4], un cluster Redis [5], Chall-Manager et son janitor [6], ainsi qu'une pile OpenTelemetry [7] comprenant un Prometheus [8], un OpenTelemetry Collector [9]

2. `https://ctfd.io/`
3. `https://longhorn.io`
4. `https://mariadb.org/`
5. `https://redis.io/`
6. `https://github.com/ctfer-io/chall-manager`
7. `https://opentelemetry.io/`
8. `https://prometheus.io/`
9. `https://opentelemetry.io/docs/collector/`

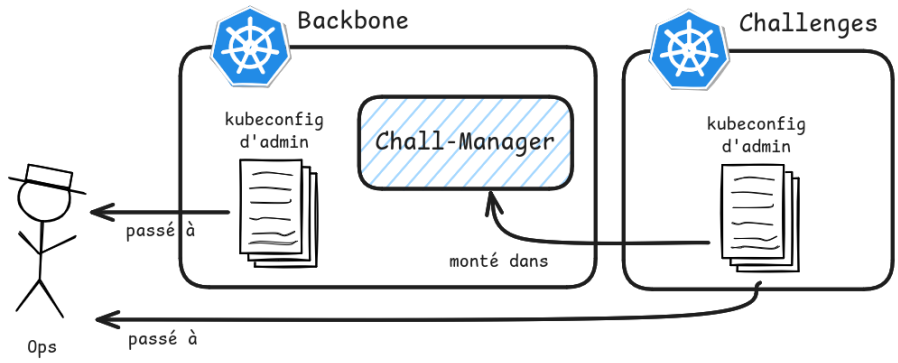


FIGURE 5 – Passage des `kubeconfigs` entre les deux clusters Kubernetes et les Ops.

et un Jaeger [10]. Pour des besoins de mesures en production à des fins expérimentales, nous montons aussi un volume qui exposera les mesures de couverture de code par un environnement `Romeo` [11]. Un extrait de toute cette architecture est en Figure 6.

Bien que la pratique de tout déployer en un seul outil aille à l'encontre des pratiques Micro-Services de séparation des préoccupations où une équipe se dédie à un Micro-Service, cette pratique répond au besoin de rapidement déployer des infrastructures réplicables de production. Dans le contexte d'événements éphémères, comme celui-ci, cela réduit le temps requis pour un passage en production tout en assurant sa réplicabilité. Typiquement, cela nous a permis de rapidement remonter l'infrastructure lors de l'incident majeur de 05h23 (Section 5.2).

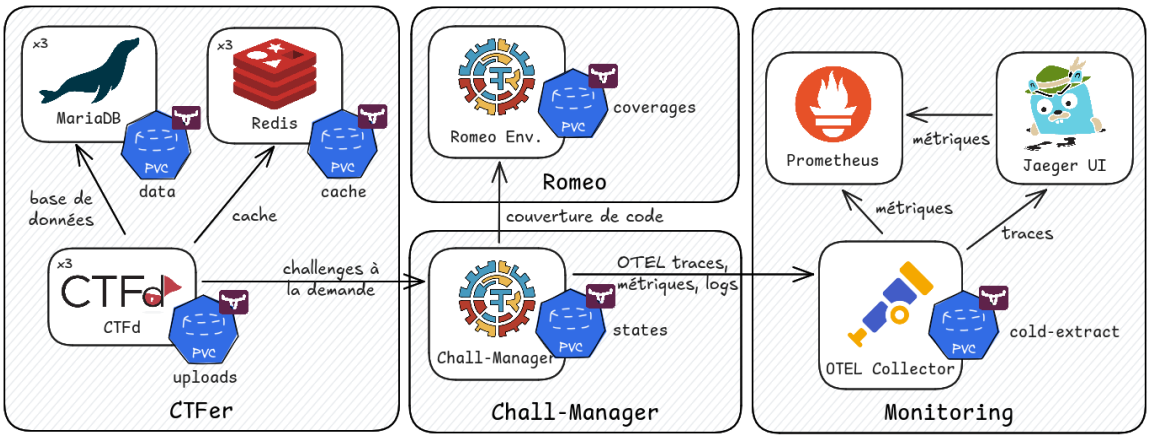


FIGURE 6 – Extrait de l'infrastructure déployée par la *fullchain*.

Ensuite, nous devons configurer la plateforme pour obtenir un système prêt à la production. L'une des pistes d'améliorations évoquée au RETEX de l'édition 2023 était le manque d'outillage concret permettant de tracer les ressources de CTFd, en particulier pour les challenges. En 2 ans, nous avons eu le temps d'éditer le provider Terraform pour CTFd [12], les bridges Pulumi [13], ... Pour atteindre cet objectif nous avons développé l'outil *ctfops* capable de déployer la configuration de CTFd via un compte de service, ainsi que les challenges. Cela facilite grandement l'effort de configuration de la plateforme, passant d'heures de configuration manuelle (à fort potentiel d'erreur) et requérant une connaissance des outils (leurs menus en particulier), à une configuration automatique (rapide en temps humain, sans erreurs).

Enfin, une dernière étape est la configuration des joueurs. En effet, l'événement étant sur liste d'inscription, nous disposons en amont d'une liste de participants, des équipes, des affiliations et rôles de chacun. En consommant ces informations, nous pouvons ainsi pré-créer les équipes, comptes, ... à la fois sur la plateforme de CTF mais aussi pour les accès réseau 802.1x. Ainsi, nous avons développé le programme Pulumi *players* [14] procédant à cette configuration. En cas d'ajout ou de modification dans la liste d'inscription, il devient alors simple de mettre à jour la production sans devoir tout rééditer. Une particularité de cette édition est la participation

10. `https://www.jaegertracing.io/`
11. `https://github.com/ctfer-io/romeo/tree/main/environment`
12. `https://github.com/ctfer-io/terraform-provider-ctfd`
13. `https://github.com/ctfer-io/pulumi-ctfd`
14. `https://github.com/ctfer-io/24hiut2025/tree/main/infra/players`

d'une équipe hors catégorie, constitué de personnels de l'UCBL1. Pour les accès réseau, un simple programme [15] permet de consommer la sortie de *players* pour générer une liste de tickets d'authentifications au format pdf, ensuite imprimés, découpés, et délivrés aux participants lors de leur arrivée. Un des effets de la pré-création des participants et équipes sur CTFd est la réduction de la charge au lancement : un simple login est moins couteux à gérer (principalement de la lecture en base de données) qu'un ensemble de créations de ressources (par essence, de l'écriture en base de données). Ainsi, on évite un pic de charge au lancement de l'événement. Sans cela, il faudrait mettre en place du prescaling (e.g. un Cron trigger de KEDA) et s'assurer que des outils comme `ctfdump` ne sont pas utilisés. Enfin, un autre avantage est la possibilité de retirer l'inscription des équipes, évitant ainsi que l'une d'elle crée un second compte pour consommer des aides ou des instances de challenges sans affecter son classement général.

Cet ensemble cohérent de programmes Pulumi compose la pile applicative exploitée lors de cet événement, et est rappelée dans la Figure 7.

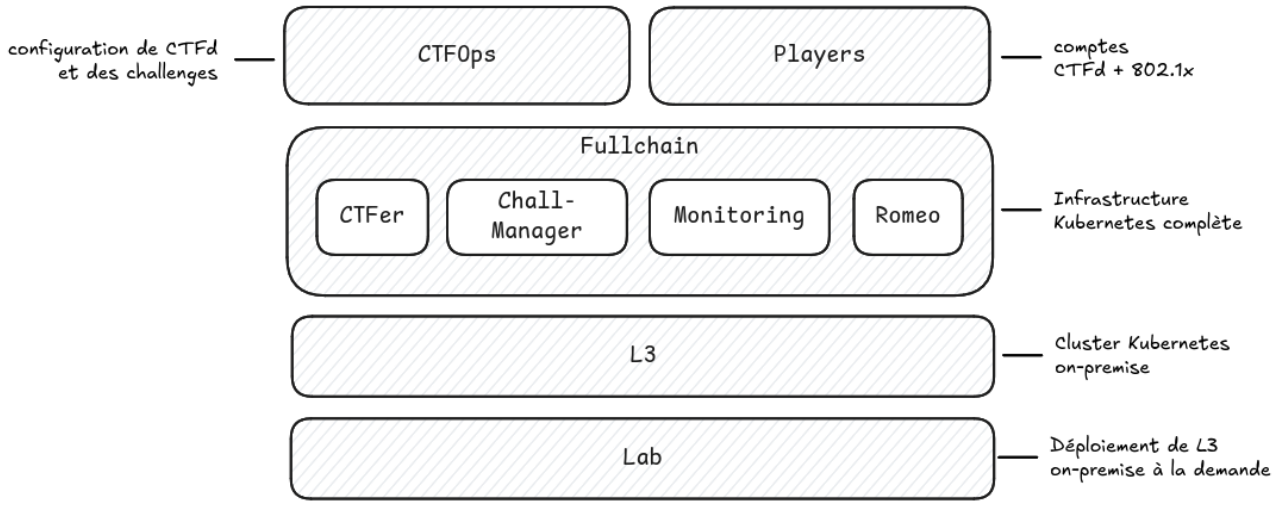


FIGURE 7 – Pile des programmes Pulumi utilisés pour l'infrastructure de production des 24h IUT 2025.

Dans les prochaines sous-sous-sections, nous portons une attention particulière à la construction de 3 infrastructures de challenges de l'événement. Leur déploiement est appelé *scénario*. Ceux-ci sont taillés sur-mesure, afin de répondre au mieux aux enjeux de capacités, de montée en charge, et de sécurité (en particulier vis-à-vis de l'isolation des instances). Les scénarios des autres challenges sont cohérents avec les recettes de déploiement habituels, comme celui du `k8s.ExposedMultipod` du SDK [16] de Chall-Manager, et ne seront ainsi pas détaillées.

3.2.1 Kubrac

La particularité du challenge Kubrac [17] est que l'isolation ne se produit pas à l'échelle des Pods et des Services et donc au travers de Network Policies, mais à l'échelle d'un Namespace. Ainsi, il faut créer pour chaque instance un ServiceAccount avec des permissions très spécifiques de lecture dans le Namespace d'instance. Pour créer ce ServiceAccount, Chall-Manager (au travers du scénario) doit lui-même avoir à disposition un ServiceAccount permettant d'en créer d'autres. Ce dernier doit avoir de fortes permissions à l'échelle du cluster, comme celle de créer, modifier et détruire des Namespaces. Cette architecture de comptes de services est représentée dans la Figure 8.

Compte tenu que la compromission (ou une erreur) avec un tel compte de service aurait un potentiel destructeur majeur, nous avons décidé de mettre en place un cluster Kubernetes dédié aux challenges, dans une approche de sécurité en profondeur. Ainsi, dans notre analyse de risque, si les mesures atténuatrices des risques d'évasion d'un environnement de jeu venaient à se produire, cela serait restreint à un cluster Kubernetes n'affectant pas les systèmes principaux (plateforme de jeu, monitoring, ...). De plus, une simple taint des nœuds du cluster n'aurait pas suffit à isoler en profondeur, puisque les Service Accounts n'ont pas le même niveau d'isolation.

De surcroit, l'un des risques présentés par Kubrac est son besoin d'intéragir avec le composant `kube-apiserver`. Ce composant est vital au bon fonctionnement du cluster Kubernetes, et son exposition présente un fort risque

15. `https://github.com/ctfer-io/24hiut2025/tree/main/infra/auth`
16. `https://github.com/ctfer-io/chall-manager/tree/main/sdk`
17. `https://github.com/ctfer-io/24hiut2025/tree/main/challenges/infra/kubrac`

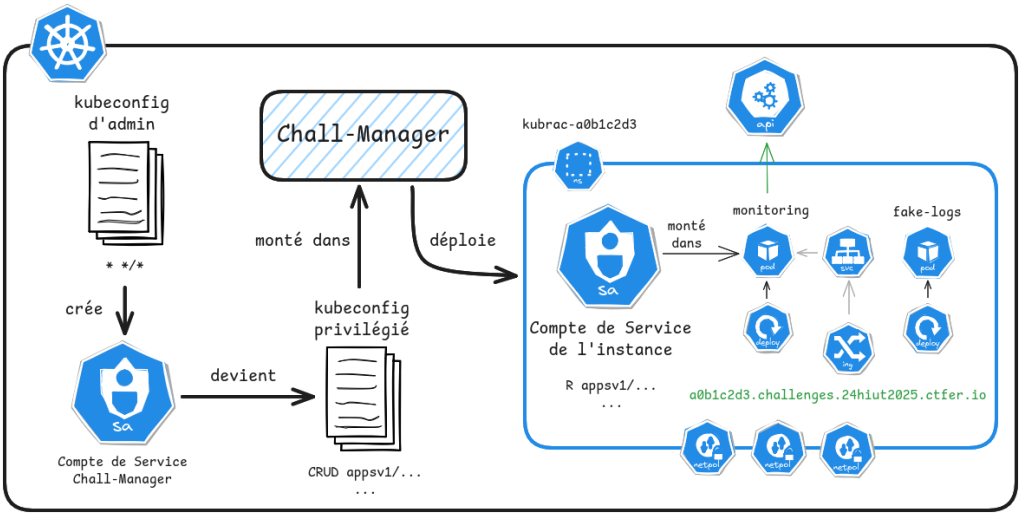


FIGURE 8 – Architecture des comptes de services en restreignant les permissions pour le challenge Kubrac.

pour l'hébergeur. Ce danger vient augmenter le justification d'utiliser un second cluster dédié plutôt que celui de production.

Nous sommes conscient que ce choix peut sembler étonnant, en particulier dû au coût d'infrastructure et de gestion d'un cluster Kubernetes, mais nous voyons à cela 2 intérêts :

1. nous vérifions le fonctionnement d'une isolation par Namespace, ainsi que le fonctionnement des Network Policies Cilium pour le `kube-apiserver` sans affecter la posture de sécurité de la « backbone » ;
2. nous expérimentons la présence de plusieurs environnements Kubernetes en parallèle sur l'infrastructure, en prévision de futurs challenges requérant le passage de ce mécanisme à l'échelle.

Toutefois, nous n'avons pas eu le temps d'expérimenter un cluster Kubernetes sous Talos [18], toujours par soucis d'isolation en profondeur dans une approche de sécurité par défaut. Une autre alternative serait avec du Capsule [19], mais nous n'avons pas eu le temps d'étudier la balance sécurité/maintenance d'un unique cluster Capsule avec plusieurs *Tenants*. Peu importe le choix, les deux approches trouveront leur intérêt, que ce soit pour porter l'infrastructure ou comme contenu de challenge.

3.2.2 Beverage Bazaar

Le challenge *Beverage Bazaar* consiste (du point de vue de son infrastructure) en un serveur FTP accessible via une connexion anonyme ainsi qu'un serveur SSH accessible via un des comptes trouvés sur le serveur FTP. Le challenge contenait une seule image Docker avec les deux services installés.

La particularité de son intégration tient dans le fonctionnement du protocole FTP en mode passif [20] et de la configuration du service `vsftpd`.

Pour que les joueurs puissent accéder aux services, il faut exposer des NodePort(s) (ports exposés au niveau des nœuds *Workers* du cluster Kubernetes). Pour les ports `2100/TCP` et `22/TCP`, nous pourrons utiliser le Port Adress Translation (PAT) effectué par le NodePort pour disposer de plusieurs instances parallèles, et ainsi le fournir via la `connectionInfo` générée par Chall-Manager. Les joueurs peuvent joindre le conteneur via les commandes `ssh -l xx <hostname> -p xxxxxx` ou `ftp <hostname> xxxxx`.

En mode passif du FTP, c'est le serveur qui fournit le port d'échange de données au client dans une plage de ports disponibles, une fois le premier contact effectué. Lorsque le client va demander l'ouverture d'une session FTP, le client lui renvoie un port sur lequel procéder pour les futurs échanges, au sein d'une plage. Cette plage est à configurer via les attributs `pasv_min_port=xx` et `pasv_max_port=xx` dans le fichier `/etc/vsftpd.conf`.

En prenant le problème à l'envers, on commence par créer une *Service*, puis on configure `vsftpd` pour qu'il utilise le `NodePort` assigné par le cluster comme plage d'une unique valeur. Enfin, on lance le conteneur. De cette façon, le conteneur va être ciblé par le service malgré l'inversion de l'ordre de création, tout en permettant de le configurer avec ses informations d'écoute réseau.

En rédigeant le scénario, et avec les retours d'une charge de production, nous avons identifié plusieurs problèmes rémanents à cette architecture :

18. `https://www.talos.dev/`
19. `https://projectcapsule.dev/`
20. `https://fr.wikipedia.org/wiki/File_Transfer_Protocol`

— Nous ne pouvons pas configurer de plage de NodePort, nous devons donc nous limiter à une plage d'un seul port. Pour monter à l'échelle sur ce mécanisme, il faudra multiplier les Services ;
— Le fait d'avoir un seul port dans la plage pouvait entraîner des conflits si deux joueurs d'une même équipe se connectaient simultanément au serveur FTP, le deuxième joueur ne recevant pas de port par le serveur ;
— Les clients lourds tel que *Filezilla* ne fonctionnent pas correctement avec les comptes anonymes, alors que la CLI `ftp` de Linux ne pose pas de problèmes (en particulier lors des tests amont).

Ceux-si sont tellement spécifiques qu'ils ne seront probablement pas corrigés dans les outils.

3.2.3 Lab AD

Les « LAB » consistent en un réseau de machines virtuelles (VM) formant un environnement cohérent pour une épreuve de CTF.

Bien que non joués lors des 24H IUT en raison d'un incident sur l'infrastructure (voir Section 5.2) et d'une erreur Proxmox liée aux informations de connexion, la construction des LAB représente en elle-même une innovation pour l'équipe de CTFer.io, et relève d'un caractère rare dans les CTF (en particulier dû au coût d'infrastructure et à la complexité de mise en place). En ce sens, leur mise en œuvre mérite d'être détaillée.

Pour les **24h IUT 2025**, deux challenges « LAB » Active Directory (« AD ») étaient prévus :

`Entraînement` :
— 1 VM Windows Server avec les rôles de contrôleur de domaine ;
— 1 serveur web IIS.

`CronPa-Cola` :
— 1 Windows Server contrôleur de domaine ;
— 1 Windows Server avec un IIS vulnérable utilisant un compte local privilégié permettant d'élever les privilèges vers un compte administrateur du domaine ;
— 1 Windows 11 client du domaine contenant le flag sur le bureau.

Pour les construire, nous devons combiner plusieurs rôles :

ChallMaker : **Clément Viard** aka **KlemouLeZozo**
— Configuration du challenge (AD, IIS, comptes utilisateurs, etc.) ;
— Installation des drivers *virtio* pour Windows ;
— Configuration réseau statique ;
— Fourniture d'une ou plusieurs VM préconfigurées (image disque ou backup Proxmox).

Ops : **Nicolas Faugeroux**
— Génération des templates de VM à partir des dumps du ChallMaker sur l'infrastructure cible ;
— Création du scénario Pulumi pour cloner les VM Windows ;
— Estimation en coût d'infra reliée au mana ;
— Ajout d'une VM de rebond « Hacker » avec un compte généré aléatoirement et un serveur VPN installé dynamiquement.

Admin : **Lucas Tesson**
— Calibration de la difficulté en fonction des autres challenges pour la cohérence globale.

Hors de la complexité inhérente au challenge, détaillons en premier lieu l'infrastructure logique.

Pour intégrer ces environnements dans un CTF, une approche est de segmenter les accès entre les équipes via des accès non prédictibles. Une VM de rebond a été ajoutée à chaque LAB, connectée à la fois au réseau contenant les VM - dit réseau « back » - et au réseau d'accès pour les joueurs - dit réseau « front ». Pour faciliter les connexions, une configuration OpenVPN pouvait être récupérer dès la première connexion à la machine d'entrée.

La VM de rebond est une VM Linux avec :
— Un compte et mot de passe aléatoires générés via Cloud-Init ;
— Une adresse IP statique sur le réseau « back » ;
— Une adresse IP dynamique via DHCP sur le réseau « front ».

Le réseau « front » est partagé entre toutes les instances via leur VM de rebond respective (même VLAN, même réseau, IPs différentes). Le réseau « back » est quant à lui segmenté à la couche 2 du modèle OSI (VLAN différent, même réseau, mêmes IPs). Chaque VLAN doit être unique par instance pour segmenter les environnements, nécessitant l'utilisation d'un service externe. La Figure 9 représente ces différentes séparations.

Pour cette édition, un système a été rapidement développé et nous utilisions la fonction `GetAvailableId(min, max)` pour avoir un nouveau identifiant à la fois de VM mais également de `vlanId`.

Désormais, du point de vue physique, nous procédons pour la mise en place sur le cluster Proxmox comme s'en suit :
— Répartition des VM sur plusieurs nœuds pour éviter les *OOM* [21] ;

21. `https://en.wikipedia.org/wiki/Out_of_memory`

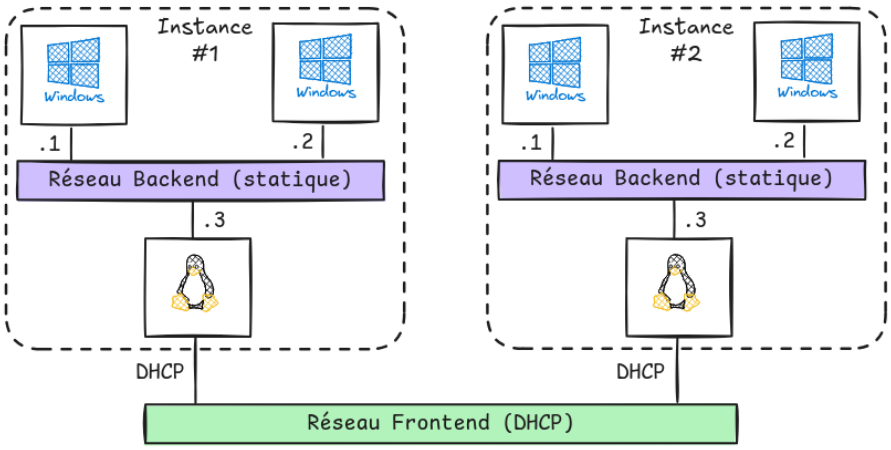


FIGURE 9 – Montage système d'un Lab AD.

— Génération des VLAN ID selon un interval $[min : max]$ en fonction du challenge (100 VLAN par challenge, soit 100-199 pour CronPa-Cola et 200-299 pour Entraînement) ;
— Configuration des VLANs sur un switch dédié (NETGEAR MS510TX), le switch ARUBA n'étant capable d'en gérer que 64.

La Figure 10 représente ces montages.

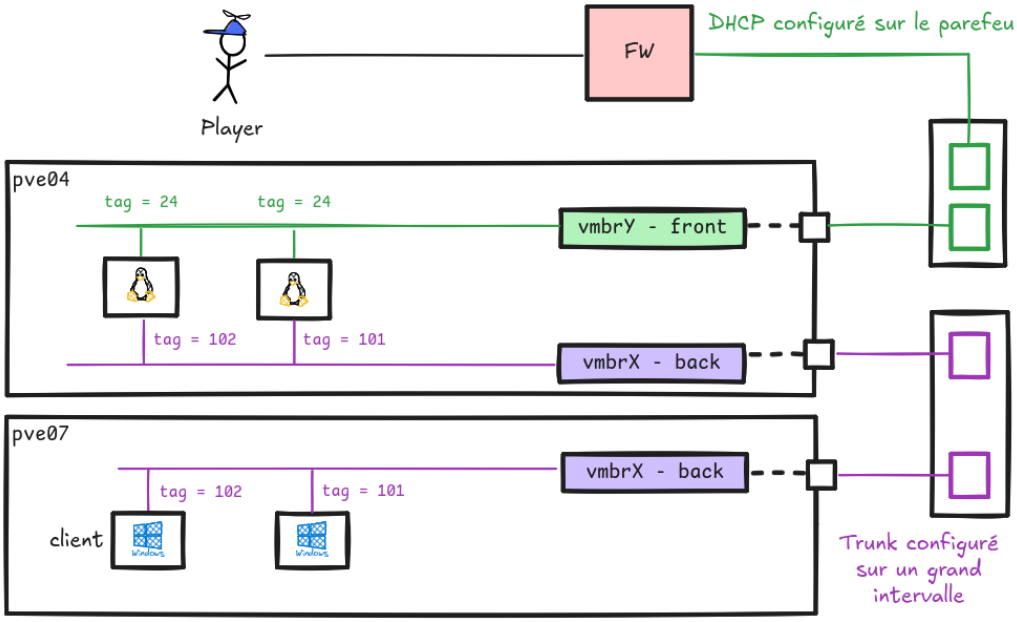


FIGURE 10 – Montage physique d'un lab AD.

Malgré tout cela, au moment de l'événement nous avons découvert que le déploiement à l'échelle ne fonctionnait plus. Cela est dû à un mauvais cocktail de bugs :

Problème avec le Pooler les instances de LAB devaient utiliser la feature du Pooler pour fournir des instances à la demande. Cependant, la mise à jour des informations du Pooler entraînait la mise à jour des instances dû à l'utilisation des additionals globaux dans `ctfops`, ainsi que d'additionals customs spécifiques au compte de service Proxmox ;

Mauvaise gestion de la mise à jour du scénario : le système d'attribution d'ID (`VmId` ou `VlanId`) n'était pas tracé comme une ressource Pulumi, retournant un nouvel ID à chaque exécution du scénario. Le `VmId` changeant, les VM devaient être re-crées à chaque fois ;

Absence d'informations de connexion : bien que les VM soient créées et fonctionnelles, les informations de connexion (format `ssh -l user 10.17.x.x`, `password=x`) n'étaient pas affichées sur CTFd. L'équipe de CTFer.io, disposant de ces informations, a proposé aux joueurs de les contacter directement pour continuer l'épreuve. Peu de joueurs utilisant Discord, et après 2h d'inactivité sur ce challenge, il a finalement été décidé de le masquer. S'en est suivi la suppression des instances existantes afin de simplifier

l'infrastructure en cours de fonctionnement. Entre temps, les mêmes tests ont été réalisés sur le deuxième challenge CronPa-Cola, mais les mêmes symptômes étaient présents sur ce challenge. Face à la complexité de ce second et la prise de risque, il a aussi été retiré de la compétition.

4 Analyse du déroulé de l'événement

Dans cette section, nous détaillons par liste à puces les éléments positifs comme négatifs vécus lors de l'événement. Par la suite, nous proposerons des pistes d'améliorations répondant à ces remarques.

4.1 Points positifs

1. superbe accueil de **Nadège Bazin**, qui se poursuit jusqu'à la fin ;
2. remise des prix efficace : moins de 30 minutes après la fin de l'épreuve de cyber, pas de longs discours ;
3. les cartons et mousses pour déplacer les serveurs → moins lourds, moins d'impact de vibrations ;
4. la salle (S26) est proche de l'accès camion, facilitant les aller-retour ;
5. la remontée du bug de softlock du plugin CTFd pour Chall-Manager (Issue #141) a permis de déployer rapidement un fix (PR #145), moins performant à l'échelle mais suffisant dans la majorité des cas ;
6. l'infrastructure a correctement tenu (CTFd, Chall-Manager, plugin CTFd pour Chall-Manager, parefeu, switch, ...). Dans le cas de CTFd, et malgré les limits très basses, cela reste le cas. Il faudra tout de même augmenter les capacités maximales selon les recommandations ;
7. bon ressenti des participants, malgré des latences passagères du réseau (coupures lors des maintenances en direct) ;
8. l'incident majeur de 05h23 a été surmonté par un travail d'équipe (communication interne et externe, prise d'informations, facilitation des efforts individuels) bien qu'un manque de prise de recul est notable (tout n'aurait pas eu besoin d'être refait, mais l'automatisation réduit fortement l'impact de cette erreur) ;
9. les limites d'une infrastructure auto-hébergée commencent à se ressentir (gestion des VLANs, résilience des équipements, transport, ...). Il faudrait commencer à se tourner vers un sponsor de hosting pour les challenges à la demande (e.g. AWS, GCP, OVH, Scaleway, Exoscale, ...) ;
10. le serveur de memes a été apprécié par les participants, malgré le taunt d'avoir eu des challenges cachés depuis le début (1 participant semble avoir découvert le premier 2h après son annonce, soit 10h avant le lancement de l'épreuve Cyber) ;
11. les ChallMakers ont tous joués le jeu du lore de l'événement : PopaCola vs. FreizhCola ;
12. le câble HDMI sans fil de **Richard Chauve** permet d'exploiter facilement le projecteur de la salle, en particulier pour debug à plusieurs ;
13. découverte d'un bug dans `ctfops` pour la gestion du `mana_cost`, fix à 02h00 → bonne réactivité.

4.2 Points négatifs

1. les repas (CROUS) ne sont ni nutritifs ni sains (petit déjeuner aux portions ridiculement faibles, pommes non mûres, sandwichs presques vides pour soir et midi) ;
2. surpris par l'absence de flags pour des challenges jugés non difficiles, semblant montrer un niveau disparate entre IUTs. Cela était déjà pris en compte avec un tier de challenges très accessibles ;
3. prise de retard dans l'extinction de la baie dû au remplissage du scoreboard au dernier moment (excel sur sharepoint). Un meilleur mécanisme (export automatisé, ou géré par un externe) serait à envisager ;
4. la salle est trop lointaine des participants (RDC vs. +1) ;
5. le pooler met à jour les instances en pool même s'il n'y a pas eu de changement d'additionals. Dans le cas où le scénario n'est pas idempotent, cela peut aboutir à la re-création des ressources ;
6. CTFd requests/limits trop faibles. Voir doc officielle ;
7. `ctfops` prend trop de RAM (∼32 Go) → consomme le swap, donc devient très lent ;
8. la gestion des permissions Discord n'a pas eu le temps d'être auditée en amont de l'envoi du lien aux participants. Il aura fallu corriger des permissions une fois en production (e.g. les participants peuvent mentionner `@everyone`, mais ne peuvent pas mentionner les `ChallMakers`) ;
9. le lien entre Discord et CTFd est difficile lors des questions des participants ;
10. manque d'une procédure pour le 802.1x, DoH, DNS, OVPN ;
11. réseau câblé pas clair pour les participants (consignes RJ45 envoyé à T-1j) ;

12. bug sur le timeout qui défaut à 0 lors du lancement de `ctfops` ;
13. manque de temps sur la configuration du monitoring, le panneau Grafana n'a pas été réalisé ;
14. les challs n'ont pas été suffisament testés, en particulier sur la totalité de l'intégration à CTFd (lancement d'instances, *connection infos* non vides, validation des flags, ...) ;
15. manque de coordination avec le SMIR (jeudi aprèm câblage solo du SMIR, tests réseau vendredi en fin de matinée après être allé les chercher) ;
16. la salle de repos est trop près, la salle de pilotage est bruyante ;
17. demande d'analyse des flux (e.g. utilisation de ChatGPT) → hors de notre cadre + est un outil comme un autre, ne doit pas être bani ;
18. des participants (et organisateurs) ont relevé un manque d'OSINT, jugé souvent plus accessible ;
19. augmentation du timeout gunicorn pour uploader des fichiers plus gros (voir Issue #1379) ;
20. déploiement de l'infrastructure peu sécurisé par défaut → vers Iter.2 ;
21. manque de suivi dans le temps des ChallMakers ;
22. peu de suivi d'un scribe pour la réalisation du RETEX → doit être construit a posteriori, ce qui est couteux en temps ;
23. le challenge RETEX a été baclé par une moitié des équipes → formulaire envoyé en fin d'événement ? ;
24. changer le prix des hints selon la difficulté (easy, medium, hard, insane) ? ;
25. existence d'un RETEX 24h du point de vue des profs/orgas de La Doua ? ;
26. absence de merch au lore des 24h ;
27. absence d'une explication rapide (vidéo ?) du concept de CTF et les règles de l'événement ;
28. manque d'un challenge d'introduction avec flag dans les consignes ;
29. mauvais encodage en base de données pour les caractères spéciaux → passer mariadb en `utf8mb4` (e.g. équipes hiéroglyphes devant changer de nom, emoji retiré dans un énoncé) ;

4.3 Pistes d'améliorations organisationnelles

1. ne pas annoncer la partie cyber sur le site de l'événement sans la validation de l'équipe en charge. Cela évite d'annoncer de mauvaises catégories de challenges, ou de fausses consignes ;
2. proposer des plats nutritifs et un minimum sains, faits en volume, comme de la paella, ou un buffet (édition 2023) ;
3. la cohésion est difficile entre *CTFer.io* et les participants, tout comme avec les autres organisateurs. Il n'est pas important d'être proche du camion puisqu'on ne bouge que 2 fois (arrivée et départ) ;
4. il faudrait faire une revue des permissions Discord en amont de l'envoi aux participants ;
5. avoir des procédures simples pour les participants, relatives à l'utilisation du DoH, 802.1x, OVPN, ... ;
6. avoir un planning de suivi des challenges et ChallMakers dès le départ ;
7. assignation du rôle de scribe en amont de l'événement, selon le planning de réalisation des tâches → éviter les périodes omises du RETEX ;
8. la seule utilisation d'un modèle CTF jeopardy place l'événement dans une monotonie de l'écosystème → proposer d'autres modèles de jeu ? Attaque/Défense ? ;
9. proposer des goodies en lien avec l'événement, ainsi qu'en bonnes dimensions (e.g. 1 casquette pour 4 participants, sans compter les accompagnateurs) → ancrer l'événement dans le temps et les esprits ;
10. placer au même niveau l'ensemble des organisateurs, ainsi que permettre à CTFer.io de chercher des sponsors techniques pour l'événement ;
11. il faudrait prévoir une checklist des actions techniques et organisationnelles à réaliser, pour qu'elle ne soit qu'à dérouler même lors d'une situation de stress (e.g. règles parefeu,

4.4 Pistes d'améliorations techniques

1. étiqueteuse (câbles RJ45, serveurs, ...) ;
2. puit de logs ? en particulier pour le pare-feu ;
3. Forti → switch, puis switch → mur : tester la connexion utilisateur nécessitait de débrancher le downstream users donc 162 personnes ;

4. la sécurisation des images Docker tournant sur le cluster Kubernetes était largement insuffisante : users/groups non root, annotations de namespaces, etc. ;
5. `ctfops` doit être profilé pour comprendre la sur-consommation des ressources ;
6. lien entre Discord et CTFd via de l'OIDC ? ;
7. pré-construire le dashboard de monitoring ;
8. avoir une procédure de test d'intégration des challenges ;
9. la sécurisation de l'infrastructure par défaut doit prendre plus de place dans les futurs travaux ;
10. faire des disk clone pour les VM PVE. Sans clone, les VM Linux ne peuvent pas passer en production cas trop lentes (pourrait avoir causé le problème de `connection_info` vide après l'incident de 05h23) ;
11. l'architecture des Labs AD (Section 3.2.3) est extrêment figée et dépendante de l'infrastructure physique (magic values dans les scénarios et additionals). Elle souffre ainsi d'un manque d'équilibrage de charge. Une solution pourrait être de passer par un orchestrateur, en particulier Kubernetes via du Kata [22] ou `Kubevirt` [23] ;
12. annonce avec règles principales (e.g. comportement du scoring dynamique) → vidéo ? ;
13. challenge d'introduction qui nécessite d'aller lire le réglement ;
14. challenge RETEX plus clairement annoncé → éviter les fausses soumissions ;
15. méthode de scaling de l'infrastructure backbone (i.e. CTFd, Redis, MariaDB, KEDA, ...) ;
16. faire des simulations pour la méthode de scoring (challenges dynamique, prix des hints, ...) ;
17. vérifier le déploiement des outils selon leurs recommandations ;
18. procéder à un pré-run de l'infrastructure cible (sans pooler) pour assurer de la bonne configuration de l'intégralité du système, puis en activant un minimum le pooler ;
19. Chall-Manager n'a pas de mécanisme de gestion de secrets. Nous devons propager les secrets (e.g. pour les Labs AD) via les additionals des scénarios.

5 Incidents

5.1 Suivi des ressources ctfops

Juste avant l'incident majeur de 05h23 (Section 5.2), aux alentours de 05h00, une modification des fichiers du challenges « Turbo Timer » a eu lieu manuellement, suite à une incompréhension mutuelle au sein de l'équipe CTFer.io. Des fichiers tracés par `ctfops` ont été manuellement supprimés de CTFd, et un nouveau a été créé. La suppression manuelle des fichiers a été réalisée, mais les refresh de Pulumi montraient bien la présence d'un nouveau fichier inconnu qu'il n'était pas possible d'importer. Ne sachant pas réimporter le fichier manuellement, nous avons attendus de trouver une bonne solution.

Dans cette situation, cela poussait à supprimer le challenge manuellement sur CTFd, ainsi que les ressources associées dans la state Pulumi (opérations manuelles prenant plusieurs minutes, requerant une compréhension fine de `ctfops` et Pulumi).

Remarque

À tête reposée, une solution est devenue évidente : supprimer manuellement le fichier ajouté manuellement sur CTFd, puis laisser `ctfops` avec la state sans les 2 anciens fichiers le réimporter afin de la tracer. Face à la fatigue et l'importance de l'incident en parallèle, nous n'avons pas pris le temps d'y réfléchir.

5.2 Incident majeur 05h23

Cette section détaille l'incident majeur survenu juste avant le lancement de l'épreuve cyber, ses raisons et les actions prises. L'analyse est menée a posteriori.

Pour contextualisation, l'arrivée sur site le mercredi a servi à l'installation du matériel et sa configuration, et jeudi à l'installation de le pile applicative.

Le vendredi 23 mai 09h30, l'équipe CTFer.io a débuté les nombreux efforts restants d'infrastructure. Ceux-ci incluaient en particulier le redéploiement de toute la stack technique (`L3, fullchain, ctfops, players`), ainsi que la validation d'intégration et de solvabilité des 32 challenges. La majorité des challenges ont pu rapidement être validés, mais les besoins en infrastructures de 10 d'entre eux ont repoussé la réalisation de l'action. De plus,

22. `https://katacontainers.io/`
23. `https://kubevirt.io/`

le lancement des premières épreuves, les erreurs de connexions au réseau propagé par câble et authentifié en 802.1x a été une nouveauté pour certains, ce qui a occupé plusieurs heures l'équipe d'organisation.

Aux alentours de 02h00 l'intégralité des challenges avaient été intégrés et testés. Vers 04h00 nous passons à l'analyse du reste d'infrastructure à disposition (CPUs et RAM). Nous convenons des réglages à apporter au *Pooler* de `Chall-Manager`[24] pour assurer une meilleure disponibilité des challenges à la demande (instance disponible instantanément). Le Pooler a pour rôle de pré-déployer un ensemble donné d'instances dans lesquelles les participants vont piocher dès que nécessaire. L'anticipation du besoin amène à une augmentation majeure des performances en production, par la nullification du temps d'attente. Nous priorisons le lab Active Directory (AD) « Entrainement » de difficulté « Hard » qui devrait être accessible aux joueurs dès le lancement, et pour lequel nous attendons environ 15 tentatives potentielles en moins de 10 minutes. Nous estimons le niveau trop élevé pour que la majorité des équipes le solve, donc nous ne procédons pas à du pré-provisionning (démarrer une instance pour chaque équipe, ayant un fort impact matériel).

Nous procédons au réglage du pooler à `min=15,max=20` permettant d'en avoir 15 à disposition, tout en limitant l'action du pooler à 20 pour éviter de self-DoS le cluster Proxmox avec trop de création de VMs en parallèle. Pour cela nous réglons le `mana` de chaque équipe à **5**, tout comme le `mana_cost` des labs AD. Nous appliquons la mise à jour des réglages via `ctfops`. Nous observons quelques secondes plus tard les logs de lancements de 15 instances par `Chall-Manager`, et dans la foulée 30 VMs (2 VM par lab AD), confirmant la prise en compte des réglages. Après plus de 20 minutes d'attente nous choisissons de procéder par augmentation itérative de la pool afin de ne pas surcharger le cluster Proxmox (un lab prend 5 minutes tout seul, donc les performances ont été gravement réduites avec la parallélisation). En modifiant les réglages du pooler à `min=5,max=20` nous observons la demande de suppression des 30 VMs, mais aussi la création de 30 VMs, surchargeant instantanénement le cluster Proxmox (60 VMs où la configuration avait été faite pour 40, soit 150% de charge sur le coup).

Face à ce comportement anormal, nous décidons de stopper manuellement les VMs, et d'en supprimer la trace manuellement dans Chall-Manager. Pour ce dernier, l'API étant soft-lock dû aux actions manuelles entreprises sur le cluster Proxmox, nous devons passer par le filesystem. Cette opération étant à risque, nous arrêtons toute activité parallèle, permettant de supprimer l'intégralité du dossier du challenge AD (instances comprises) et les fichiers de stacks de Pulumi. Enfin, nous supprimons le challenge sur CTFd, non sans erreur puisque Chall-Manager n'avait plus la connaissance du challenge. La modification des réglages du pooler est aussi appliquée manuellement par un export de la state Pulumi de `ctfops`, la suppression des ressources, puis le réimport. Enfin un refresh est mené pour vérifier la validité des informations locales.

> Remarque
>
> La suppression manuelle des fichiers de Chall-Manager était une grande prise de risques, bien que maîtrisée. Toutefois, la manipulation dans CTFd n'avait pas été travaillée, menant à cette inconsistance.

Face à l'incompréhension du comportement soudainement anormal du pooler, nous retentons la manipulation directement avec 5 VMs, puis 10. Le même effet se produit. Quelques minutes plus tard, Chall-Manager ne répond plus aux appels API depuis le plugin. En accédant directement à l'API de Chall-Manager nous découvrons que c'est là aussi le cas. En cherchant l'origine sur la vue k9s du cluster « backbone » nous découvrons dans le namespace `ctf-xxxxxx` que cela semble être le cas de CTFd, sa base de données MariaDB, Chall-Manager, et la présence anormale d'une vingtaine de janitors en « Running » (le cas nominal étant de 3 en « Completed »). Cette prise de connaissance de l'état du cluster a lieu à **05h20**, soit 40 minutes avant l'événement.

Face aux erreurs qui s'accumulent, les volumes Longhorn qui commençaient à se rapprocher de leur limite, et les dernières configurations effectuées manuellement en moins de 24h, nous décidons hativement de détruire l'intégralité de la stack jusqu'à la `L3`. Il faut alors remonter au plus vite la stack. Immédiatement nous prévenons d'un retard au lancement à anticiper autour de 30 minutes, nous laissant 1 heure pour procéder à la réinstallation complète. Grâce à l'automatisation, nous avons en seulement quelques minutes une nouvelle infrastructure prête pour la charge, mais non configurée. En parallèle, la préparation de la nouvelle configuration de `players` est réalisé, et exécutée dès que le CTFd est disponible. Pour procéder à la réinstallation sans regénérer les accès (mots de passe) des participants, nous avons dû procéder à un export de la state, puis la suppression des ressources reliées à CTFd comme s'en suit, et enfin son réimport.

```
cat state.json | jq '
.deployment.resources |= map(
  select(
    .type != "ctfd:index/bracket:Bracket" and
    .type != "ctfd:index/user:User" and
    .type != "ctfd:index/team:Team"
  )
```

24. `https://github.com/ctfer-io/chall-manager`

```
)
'
```

Ensuite, dû à une surconsommation de ressources par `ctfops` saturant la RAM et le SWAP, nous devons procéder à la configuration catégorie par catégorie (voir challenge par challenge) sur CTFd, et chaque itération prend plusieurs minutes. Ainsi, il est estimé qu'une durée de 1h de calcul est attendue. En tablant sur les lenteurs de gestion des fichiers, nous commençons par procéder à la création des challenges ne requérant pas d'infrastructure à la demande (les scénarios étant des fichiers), du lot `T0`. Autour de 06h00, nous disposons de 2/3 des challenges configurés sur CTFd, mais il reste les plus longs. Nous décidons, vu la charge que cela représente déjà pour CTFd et Chall-Manager, de poursuivre en mode dégradé (lancement repoussé de 30 minutes).

A 06h32 l'intégralité des comptes et des challenges, en dehors des 2 labs AD, est configuré. Nous annonçons alors le lancement de l'épreuve (Figure 1). Pour les derniers ajustements (consignes, fichiers, flags, visibilité, ...) nous procédons encore une fois via `ctfops`.

Aux alentours de 7h30, une fois la charge descendue , nous décidons une dernière fois de procéder à la création des challenges « Entrainement » et « CronPa-Cola ». Par erreur, celle-ci est recréée avec une pool de 15 instances. La mise à jour de la pool avec le réglage `min=0,max=0` reproduit le bug précédent, surchargeant le cluster Proxmox. Nous procédons alors comme avant pour supprimer les instances et l'existence du challenge dans les différents systèmes. Afin de nous assurer que cela se produise sans impact sur les challenges adjacents, déjà en production, nous coupons les flux vers la plateforme.

Remarque

L'indisponiblité de la plateforme était volontaire, nécessaire, et maitrisé. Certains ont interprété cela comme un Déni de Service, ou un Déni de Service Distribué. Toutefois, aucune attaque n'a affecté la disponibilité des services lors de l'événement.

Dans la seconde vague de challenges, à 10h03, nous intégrons les challenges « Entrainement » et « CronPa-Cola ». Il sera découvert bien plus tard qu'aucune information de connexion n'est renvoyée aux participants. Puisque aucune instance n'a été déployée, nous finissons par le retirer).

Nous relevons dans un premier temps que ces erreurs sont fortement dû à un faible temps présent sur site en amont de l'événement. Spécifiquement, aucun test de charge n'a permis d'assurer le bon dimensionnement de l'infrastructure en amont de la charge de production. Heureusement aucun problème relié à la charge n'a été relevé.

6 Retour global

Organiser une telle épreuve est toujours un challenge de grande ampleur. Sur 5 mois, il aura fallu trouver le matériel, prévoir les déplacements, planifier finement plusieurs jours et en particulier ceux sur site, installer le matériel, recruter des créateurs de contenus (ChallMakers), concevoir les épreuves, partager l'expertise, intégrer les travaux, effectuer de la communication externe, développers des fonctionnalités, ...

La liberté qui nous a été confiée dès le départ a été une nécessité pour avancer convenablement. À cela, la collaboration avec les différents collaborateurs de l'UCBL1 aura facilité l'intégration sur site. Pour ces deux, nous remercions l'ensemble des acteurs avec lesquels nous avons travaillé.

Nous sommes aujourd'hui heureux d'avoir participé à la découverte de la cybersécurité pour de nombreux étudiants, en partageant une nuit d'exercice. Cela aura été l'occasion d'expérimenter nos efforts des 2 dernières années, piloté par notre RETEX de l'édition 2023. Dans cette lancée, nous espérons pouvoir expérimenter de nouvelles approches et outils lors d'éditions à venir.

Annexes

A Chronologie

— `07/01/2025 08:42` Mail de **Noura Faci** pour demander la collaboration de *CTFer.io* à l'*IUT Doua* pour la réalisation de l'infrastructure, en particulier pour l'épreuve Cyber ;
— `07/01/2025 16:02` Réponse de *CTFer.io*, posant 5 questions pour confirmer le niveau de maturité de la préparation de l'événement, autour de 5 axes :

1. le plan de communication dont pourra profiter *CTFer.io*, ne se faisant pas rémunérer ;
2. le matériel disponible sur place ;
3. échanges avec la *DSI* de l'université pour la gestion des flux, des accès internet, ... ;
4. début de travaux sur la conception d'épreuves ;
5. volume d'étudiants/participants.

Le RETEX de l'édition 2023 est transmis pour comprendre l'intérêt de ces questions.
— `08/01/2025 00:22` Réponse de **Noura Faci** attestant d'un premier jet de plan de communication. L'*IUT Doua* prend en charge la réalisation de l'épreuve Algo/Prog, et ne sait pas s'ils doivent faire appel à un prestataire externe pour les challenges ;
— `08/01/2025 08:29` **Lucas Tesson** clarifie que *CTFer.io* peut constituer un *roster* de ChallMakers sur la base de son réseau ;
— `08/01/2025 09:49` **Noura Faci** laisse champ libre à *CTFer.io* sur la constitution de l'épreuve Cyber ;
— `09/01/2025 18:53` **Noura Faci** demande à ce que *CTFer.io* clarifie ses attentes en terme de retombée au travers du plan de communication ;
— `09/01/2025 11:30` **Lucas Tesson** clarifie le statut de sponsor de l'événement ainsi que la volonté d'Open Source de l'événement (dont fait partie ce RETEX) ;
— `20/01/2025 12:37` **Noura Faci** et **Anthony Busson** rencontrent **Lionel Pozet** qui avait collaboré avec *CTFer.io* lors des 24h IUT 2023. Sont clarifiés les aspects d'infrastructure, et un premier contact avec le *Centre Inter-établissement pour les Services Réseaux* (CISR) est lancé ;
— `27/01/2025 09:19` Première vague de recrutement de ChallMakers ;
— `29/01/2025 13:49` **Lucas Tesson** crée le Discord d'organisation de l'épreuve Cyber des 24h IUT 2025 ;
— `10/02/2025 11:00` Réunion Infra/Plateforme. Résumé de la réunion :
  — Présentation de la Direction Artistique de l'épreuve Cyber ;
  — On attend 120 participants ;
  — On estime à 2.000€ la note de frais globale pour l'organisation de l'épreuve Cyber (location d'un camion, essence et péages, repas, ...) ;
  — L'hébergement sera à titre gracieux chez de la famille à Lyon ;
  — **Lionel Pozet** doit clarifier la gestion du réseau avec le *CISR* ;
  — **Lucas Tesson** va rentrer en contact avec l'*ENSIBS* pour effectuer une demande de prêt de matériel (baie « Boo » de *Donk'esport* et serveurs additionels) ;
  — **Noura Faci** et **Lionel Pozet** doivent clarifier la localisation des participants et des administrateurs de l'événement ;
  — **Lionel Pozet** va regarder pour de potentiels serveurs de prêt ;
  — l'hébergement de l'épreuve web reste en suspens. Les participants ont été informés qu'ils devraient avoir une solution d'hébergement, et *CTFer.io* alerte que tout hébergement consommera des ressources qui ne seront pas disponibles pour l'épreuve Cyber ;
  — **Lucas Tesson** transmet CTFd [25] pour l'épreuve d'Algo/Prog, et suggère de l'héberger sur l'infrastructure finale.
— `10/02/2025 13:22` **Lucas Tesson** contacte **Elian Privat** pour demander un prêt de matériel de l'*ENSIBS*, en particulier de la baie « Boo » de *Donk'esport* et de serveurs additionels du 19 au 26 mai inclus ;
— `17/02/2025 13:23` **Elian Privat** demande à ce que l'accord de **Thomas Poulain** (*Donk'esport*) soit obtenu avant l'accord de l'*ENSIBS* ;
— `17/02/2025 15:38` **Lucas Tesson** demande à **Thomas Poulain** de *Donk'esport* si la baie « Boo » peut être empruntée le temps de l'événement. Il est précisé qu'elle sera intégralement décomissionnée de toutes ses données et configurations avant et après utilisation ;
— `20/02/2025 14:51` **Thomas Poulain** valide l'emprunt de la baie et demande vérification de la couverture par l'assurance de l'*ENSIBS* pour un tel emprunt ;
— `20/02/2025 15:03` **Lucas Tesson** confirme l'accord de **Thomas Poulain** et demande à **Bertrand Rougeron** d'augmenter au maximum les capacités RAM des serveurs de prêt ;

25. `https://ctfd.io`

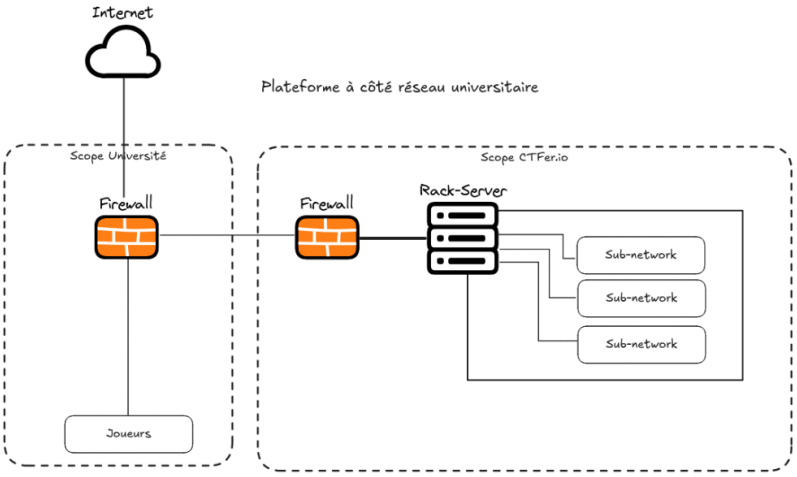
— `06/03/2025 12:21` **Bertrand Rougeron** confirme le prêt de deux R440 et un R430 ;
— `08/03/2025 01:30` **Noura Faci** fait part des avancées de l'épreuve Algo/Prog, et l'utilisation de CTFd et VMWare. La limitation d'isoler une réponse par équipe est pointée du doigt. Il est demandé des nouvelles quant au prêt de matériel par l'*ENSIBS* ;
— `08/03/2025 09:06` **Lucas Tesson** partage l'existence de Chall-Manager pour répondre à la problématique de réponse unique par équipe, mais il est noté que le besoin ne correspond pas exactement. Il reste en suspens l'hébergement de l'épreuve Algo/Prog et de ses potentiels services, ainsi que de l'épreuve Web. Il est demandé si le site d'accueil sera équipé d'un réseau ondulé ;
— `08/03/2025 09:15` **Lionel Pozet** confirme que le bâtiment ne dispose pas de réseau ondulé ;
— `08/03/2025 09:34` **Noura Faci** transmet les informations aux équipes Algo/Prog et Web, et demande si l'*IUT Doua* doit toujours procéder à de la recherche de matériel ;
— `08/03/2025 10:09` **Lucas Tesson** confirme que le matériel de l'*ENSIBS* devrait suffir ;
— `08/03/2025 11:50` **Noura Faci** demande au secrétariat de l'*IUT Doua* de préparer le déplacement de *CTFer.io* ;
— `01/04/2025 16:01` **Victor Royer** propose le premier challenge (Reverse / Reverse The Duck) ;
— `01/04/2025 16:44` **Bertrand Rougeron** a monté les RAM à 128Go sur les R440 et le R430 ;
— `04/04/2025 15:43` **Noura Faci** propose une réunion pour que les avancées respectives soient partagées ;
— `07/04/2025 13:27` **Lucas Tesson** demande au ChallMaker **Titouan Demais** si son cercle proche (de l'*ESNA*) peut rejoindre les ChallMakers et combler les manques de challenges ;
— `09/04/2025 12:06` **Lionel Pozet** confirme avoir avancé avec le *CISR*, qui souhaiterait partir sur le *Modèle B* d'infrastructure (Figure 12). Le *CISR* va configurer un firewall pour laisser passer tous les flux, il reviendra donc à *CTFer.io* de gérer la configuration (DHCP et DNS en particulier) et la sécurité des flux. Le *CISR* aimerait savoir quel nom de domaine *CTFer.io* compte utiliser ;
— `10/04/2025 09:41` **Lucas Tesson** contacte la *COREP Lyon* pour un devis d'impression de 200 stickers *CTFer.io* ;
— `10/04/2025 15:04` **Lucas Tesson** confirme la prise en compte du *Modèle B*, et demande s'il y aura un adressage IP spécifique, si l'authentification 802.1x (comme pour l'édition 2023) conviendra aux attentes du *CISR* (export des logs du firewall et des identités 802.1x, archivage, signature, transmission, puis destruction des copies locales). Enfin, reste en suspens le câblage RJ45 et la potentielle réutilisation du réseau câblé existant ;
— `10/04/2025 18:17` **Lucas Tesson** fait une demande d'accès anticipé aux serveurs hors baie « Boo » afin de débuter les travaux d'infrastructure ;
— `14/04/2025 10:00` Réunion de suivi du projet 24h IUT 2025. Résumé de la réunion :
  — Passage de 120 à 160 participants, ainsi que 2 internes hors compétitions (*SMIR*) ;
  — **Lucas Tesson** doit faire réaliser 2 devis pour la location d'un camion ;
  — **Lucas Tesson** doit transmettre la méthode de scoring pour évaluer les participants selon les épreuves, afin d'avoir une cohérence globale avec les autres épreuves ;
  — Pour le déplacement de **Richard Chauve**, l'*IUT Doua* pense procéder à un remboursement via Note De Frais.
— `14/04/2025 10:59` **Lucas Tesson** transmet les paramètres de scoring (`value=500`, `decay=26`, `minimum=50`) ;
— `14/04/2025 13:21` **Laurent Glatigny** confirme la disposition des participants et de *CTFer.io*, ainsi que du changement de serrure pour la sécurisation de la pièce ;
— `14/04/2025 15:47` **Vincent Vidal** demande confirmation à **Lucas Tesson** que l'algorithme de scoring dynamique est à décroissance parabolique *a contrario* de ce que laisse indiquer le nom *logarithmic* ;
— `15/04/2025 09:38` **Lucas Tesson** demande confirmation à **Laurent Glatigny** des salles S315 vs S312 pour les participants, compte tenu de l'isolation géographique de la S135 ;
— `15/04/2025 09:56` **Laurent Glatigny** confirme la disposition des salles ;
— `15/04/2025 10:32` premier challenge accepté de **Richard Chauve** (Misc / Bottle Flip Challenge) ;
— `16/04/2025 16:12` **Nadège Bazin** contacte *CTFer.io* pour lancer la création des comptes d'agents extérieurs de l'UCBL1 ;
— `16/04/2025 15:34` **Lucas Tesson** transmet 2 devis à **Noura Faci** et **Nadège Bazin** pour la location du camion, effectués auprès de *Leclerc* et *RentACar* (valides 24h) ;
— `16/04/2025 18:35` R430 PSU1 claque. L'inspection visuelle du serveur ne montre pas de dégât en dehors de la PSU. Elle est retirée et l'alimentation bascule sur la PSU2 ;
— `16/04/2025 19:44` **Lucas Tesson** transmet un compte rendu à **Elian Privat** et **Bertrand Rougeron** après l'allumage des premiers serveurs de prêt. Il est noté que pour le R430, la DIMM A3 semble hors service, et est mise de côté ;
— `17/04/2025 09:23` **Bertrand Rougeron** confirme que le matériel avait été testé. Il est demandé de ramener le R430 et sa PSU1 pour inspection ;
— `17/04/2025 10:19` **Lucas Tesson** demande à ce que le matériel reste à *CTFer.io* suite à la bascule effective sur PSU2 et les besoins d'infrastructures en amont ;

— `17/04/2025 12:38` **Nadège Bazin** confirme la volonté de signer le devis de Leclerc (11 m^3, 532€). Pour cela, il est demandé à **Lucas Tesson** de compléter le formulaire d'agent extérieur à l'*UCBL1* afin de réaliser un Ordre de Mission ;
— `17/04/2025 14:54` **Bertrand Rougeron** accorde la continuité du prêt du R430 ;
— `17/04/2005 15:00` **Lucas Tesson** transmet ses informations pour la création de son profil agent extérieur à l'UCBL1 ;
— `23/04/2025 13:52` **Lucas Tesson** demande à avoir accès à la liste des participants afin de pré-configurer le matériel de production (CTFd et les accès 802.1x) ;
— `23/04/2025 15:09` **Noura Faci** transmet la liste des participants, accompagnateurs et internes (participants hors compétition) ;
— `24/04/2025 10:26` **Noura Faci** demande la prise en compte de la modification d'un nom d'équipe ;
— `24/04/2025 14:23` **Nadège Bazin** confirme que *Leclerc* ne répondra pas favorable à la demande de location, ne souhaitant pas travailler avec des collectivités. Il est demandé de trouver de nouveaux prestataires qui acceptent de travailler avec un bon de commande collectivité et payés à l'issue de la prestation après dépôt de facture sur Chorus Pro, par virement bancaire (donc nécessitant un RIB) ;
— `25/04/2025 15:48` **Nadège Bazin** a trouvé un autre prestataire : *AP Location*. **Lucas Tesson** confirme les critères de 11 m^3 avec second conducteur, pour 1900 km ;
— `05/05/2025 10:03` **Lucas Tesson** procède à la commande de 230 stickers 1.97" × 1.97" du logo de *CTFer.io* auprès de *Stickermule* ;
— `05/05/2025 10:40` **Lucas Tesson** relance **Bertrand Rougeron** pour des rails pour R440 et les clés de la baie « Boo », ainsi que **Elian Privat** pour confirmer l'emprunt de la baie du 19 au 28 inclus ;
— `06/05/2025 09:24` **Noura Faci** demande la prise en compte de la modification d'un nom d'équipe ;
— `06/05/2025 11:15` **Bertrand Rougeron** confirme qu'il n'y a plus de rails pour R440 à disposition ;
— `07/05/2025 13:44` **Nicolas Faugeroux** fait les demandes de certificats à *Let's Encrypt* en DNS01 pour `*.24hiut2025.ctfer.io` et `*.challenges.24hiut2025.ctfer.io` ;
— `09/05/2025 14:35` **Lucas Tesson** rappel à **Bertrand Rougeron** et al. de l'*ENSIBS* l'emprunt de la baie « Boo », en particulier pour veiller à la disponibilité des clés ;
— `10/05/2025 23:35` **Adrien Peytavie** invite *CTFer.io* à rejoindre le serveur Discord des 24h IUT 2025 ;
— `12/05/2025 11:09` Les clés de la baie « Boo » ont été retrouvées. **Lucas Tesson** récupère le FortiGate 101E et le Aruba 1830 Switch en avance afin de pré-configurer les VLANs et le 802.1x ;
— `12/05/2025 13:00` **Lucas Tesson** croise **Thomas Poulain** et informe de la récupération du matériel dans la baie. Il sera transmis les mots de passe BIOS des serveurs de la baie au plus tôt, s'il y en a ;
— `13/05/2025 11:17` **Nadège Bazin** confirme la réservation de l'utilitaire auprès de *AP Location*. Le laisser-passer ne sera pas requis sans déplacement du camion sur les dates annoncées ;
— `13/05/2025 11:53` **Lucas Tesson** contact **Lionel Pozet** pour demander la présence d'un extincteur CO2 pour atténuer les risques physiques de l'hébergement de la baie « Boo » ;
— `14/05/2025` plan d'installation (salle, prises élec, prises RJ45) ; récupération des 230 stickers en point relais ;
— `16/05/2025 14:42` passage du `minimum` de 50 à 100 points afin de favoriser la consommation d'aides (*hints*) par les débutants ;
— `16/05/2025 14:58` **Adrien Peytavie** invite les participants sur le Discord officiel de l'événement ;
— `19/05/2025` récupération de la baie à Vannes, départ pour Esvres (∼3h de route). Soufflage serveurs ;
— `19/05/2025 16:41` rapport de bug avec effet de softlock dans le plugin CTFd pour Chall-Manager (Issue #141) ;
— `20/05/2025 19:29` création d'une solution au bug de softlock dans le plugin CTFd pour Chall-Manager(PR #145) ;
— `20/05/2025` ajout des catégories de challenges sur le discord de l'événement. Départ de Esvres, arrivée à Lyon (∼5h de route). Récupération T320 **Jérémy Tesson** ;
— `21/05/2025 08:30` installation sur site, application du plan physique ;
— `21/05/2025 10:00` câblage de la baie ;
— `21/05/2025 11:00` récupération des informations de configuration réseau upstream via le *SMIR* (du *CISR* ; interface : **Lionel Pozet**) ;
— `21/05/2025 14:00` début de mise en cluster des Proxmox ;
— `21/05/2025 15:09` tower enfin allumée ;
— `21/05/2025 16:40` RAM R440 B3 : KO ;
— `21/05/2025 17:00` perte d'internet (mise sous cluster des 7 serveurs : OK) ; câblage ;
— `21/05/2025 17:58` fin du câblage de la baie et ses 2 serveurs tours externes ;
— `21/05/2025 19:00` redéploiement `L3` pour *dev1* (« backbone ») → augmenter la taille disque ;
— `21/05/2025 21:00` descente de **Richard Chauve** en train ;
— `22/05/2025 07:30` redéploiement `L3` pour *dev2* (« challenges »), puis *fullchain* ;
— `22/05/2025 09:09` configuration des registres OCI pour Docker et Helm dans la *fullchain* (PR #3) ;

— 22/05/2025 11:30 challenge « Entrainement » OK (2 VMs PVE) ;
— 22/05/2025 14:00 challenge « CronPa-cola » OK (4 VMs PVE) ;
— 22/05/2025 16:21 préparation de l'augmentation de la taille des PVC pour le stockage de la prod (PR #70) désormais configurable ;
— 23/05/2025 08:45 arrivée sur site ;
— 23/05/2025 10:59 augmentation du nombre de workers CTFd (PR #71) désormais configurable. Augmentation de la taille des PVCs dans la fullchain ;
— 23/05/2025 14:00 DEBEX, épreuve Algo&Prog ;
— 23/05/2025 16:19 découverte d'un bug dans Chall-Manager (Issue #701) lors de la suppression d'un challenge avec instances en cours de création (race condition) ;
— 23/05/2025 18:00 annonce serveur de memes (`memes.24hiut2025.ctfer.io`) ;
— 23/05/2025 21:46 **Richard Chauve** relève que le compte du challenge « Entrainement » est déjà Domain Admin retirant l'intérêt du challenge. Le ChallMaker (**Clément Viard**) est immédiatement prévenu ;
— 23/05/2025 21:55 confirmation de l'erreur de version de l'image disque du challenge « Entrainement » en production ;
— 23/05/2025 22:00 bascule épreuve Web, **Nicolas Faugeroux** reçoit des demandes d'ouverture de flux (de nombreux ports standards ayant été ouverts en amont, les demandes sont rares) ;
— 23/05/2025 22:05 **Nicolas Faugeroux** est taské sur le patch ;
— 23/05/2025 22:37 **Nicolas Faugeroux** et **Clément Viard** sont en vocal pour tenter de corriger le challenge « Entrainement » ;
— 23/05/2025 23:11 patch du challenge « Entrainement » et mise à jour du scénario de déploiement ;
— 24/05/2025 02:00 **Richard Chauve** procède à la fin des tests d'intégration des 32 challenges ;
— 24/05/2025 05:00 **Richard Chauve** modifie les fichiers du challenge « Turbo Timer » manuellement, **Lucas Tesson** tente une modification manuelle de la state de `ctfops` ;
— 24/05/2025 05:20 **Nicolas Faugeroux** découvre que les latences des dernières minutes est dû au `node3` du cluster Kubernetes « backbone » qui ne répond plus (plus d'espace) ;
— 24/05/2025 05:23 **Lucas Tesson** détruit manuellement l'installation précédente, et relance `fullchain` puis `ctfops` ;
— 24/05/2025 05:43 **Richard Chauve** annonce un incident sur l'infrastructure et décale le lancement du CTF de 30 minutes ;
— 24/05/2025 06:33 **Lucas Tesson** annonce le lancement du CTF, du lore et des consignes (Figure 1) ;
— 24/05/2025 10:03 ajout de la seconde vague de challenges, dont les challenges Active Directory (« Entrainement » et « CronPa-Cola ») ;
— 24/05/2025 14:00 FINEX, extraction scoreboard (export logs FW, export CTFd, export OpenTelemetry logs/traces/metrics, export Victor CM), récupération de la baie ;
— 24/05/2025 14:13 publication du repository sur GitHub (ctfer-io/24hiut2025) ;
— 24/05/2025 21:05 publication du détail des résultats : scoreboard complet, taux de résolutions, distribution des scores, taux de bonnes réponses ;
— 25/05/2025 dodo + piscine ; départ de Richard en train ;
— 26/05/2025 09:30 départ Lyon pour Esvres (∼5h de route) ;
— 26/05/2025 14:46 **Stéphane Balmain** transmet les photos spécifiquement réalisées pour l'infrastructure ;
— 26/05/2025 15:02 **Stéphane Balmain** transmet l'ensemble des photos de l'événement aux organisateurs ;
— 26/05/2025 18:05 **Nicolas Faugeroux** procède à la révocation des certificats Let's Encrypt pour `*.24hiut2025.ctfer.io` et `*.challenges.24hiut2025.ctfer.io` ;
— 26/05/2025 20:00 publication LinkedIn ;
— 26/05/2025 10:00 **Nicolas Faugeroux** procède à la réinstallation des disques, des RAIDs, et des serveurs Proxmox de l'*ENSIBS* ; **Lucas Tesson** procède à l'écriture du RETEX ;
— 26/05/2025 16:43 **Lucas Tesson** contact *ctfsearch.com* pour ajouter les 30 Write-Ups des challenges dans leur base ;
— 28/05/2025 09:06 retour Vannes (∼3h route), dépot baie ;
— 28/05/2025 14:30 retour Rennes, nettoyage et rendu du camion de location, rangement du matériel ;
— 03/06/2025 16:00 publication du RETEX ;

B Modèles d'infrastructures

Infrastructure « Modèle A »



➢ **UCBL**

[?] routage (eduroam + filaire)

[-] ouverture de flux (matrice de flux qui peut évoluer selon les joueurs cf. édition 2023)

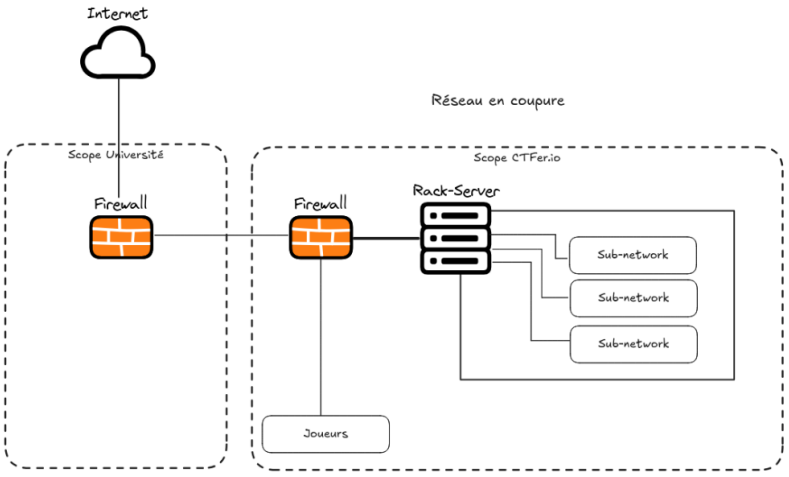
➢ **CTFer.io**

[+] Pas besoin de gérer l'accès internet (accès eduroam)

[-] dépendant de la configuration eduroam

FIGURE 11 – Modèle A d'infrastructure proposé au CISR.

Infrastructure « Modèle B »



➢ **UCBL**

[+] accès joueurs vers plateforme géré par CTFer.io

[-] ouverture de flux (matrice de flux qui peut évoluer selon les joueurs cf. édition 2023)

➢ **CTFer.io**

[+] autonomie sur l'accès à la plateforme

[-] contrainte d'authentification et export de logs à la DSI

[-] flux vers internet pour les joueurs (autorisé sur les 2 FW)

FIGURE 12 – Modèle B d'infrastructure proposé au CISR.

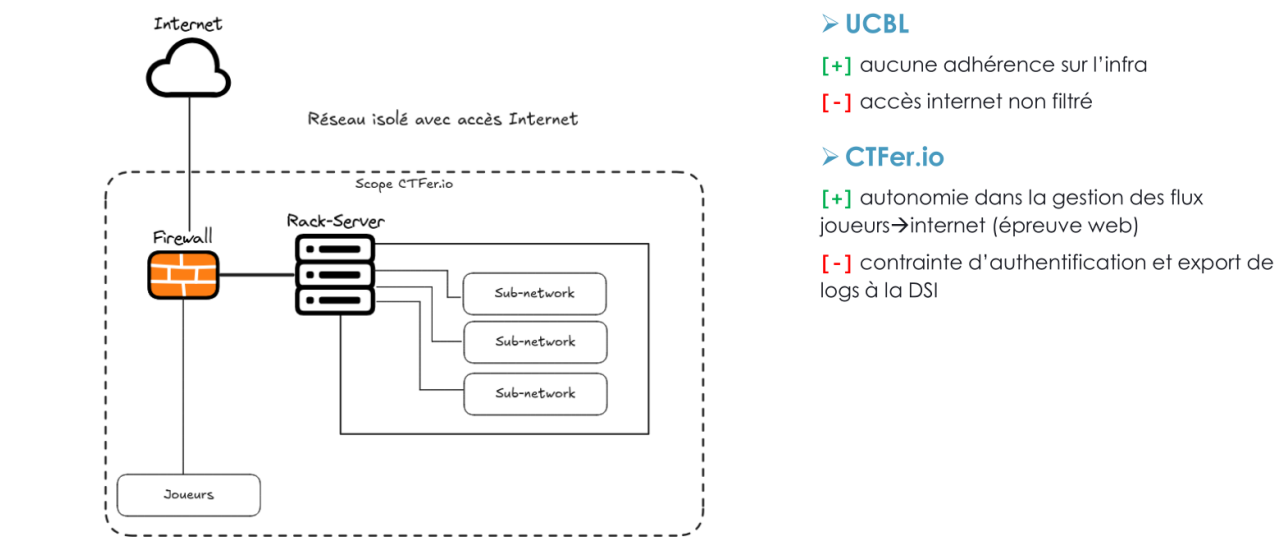


FIGURE 13 – Modèle C d'infrastructure proposé au CISR.

C Résultats

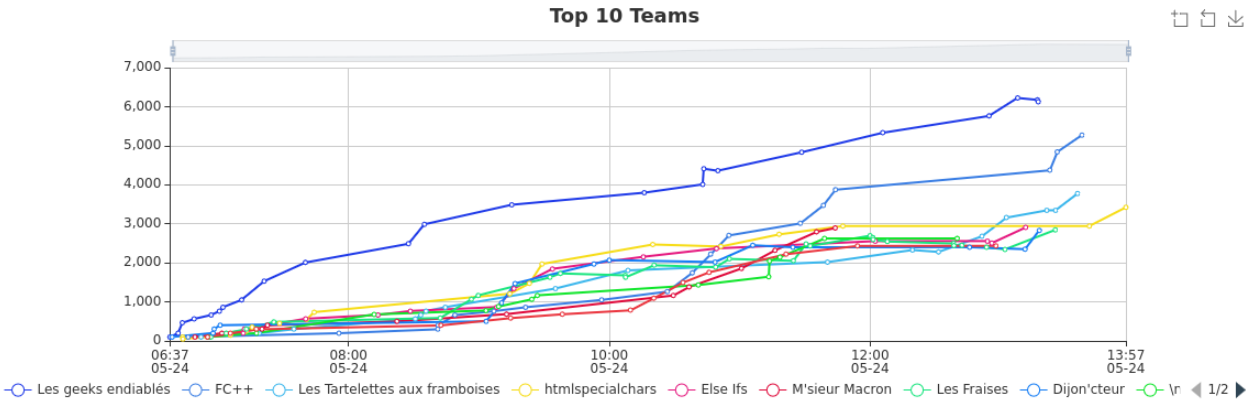


FIGURE 14 – Scoreboard en fin d'événement.

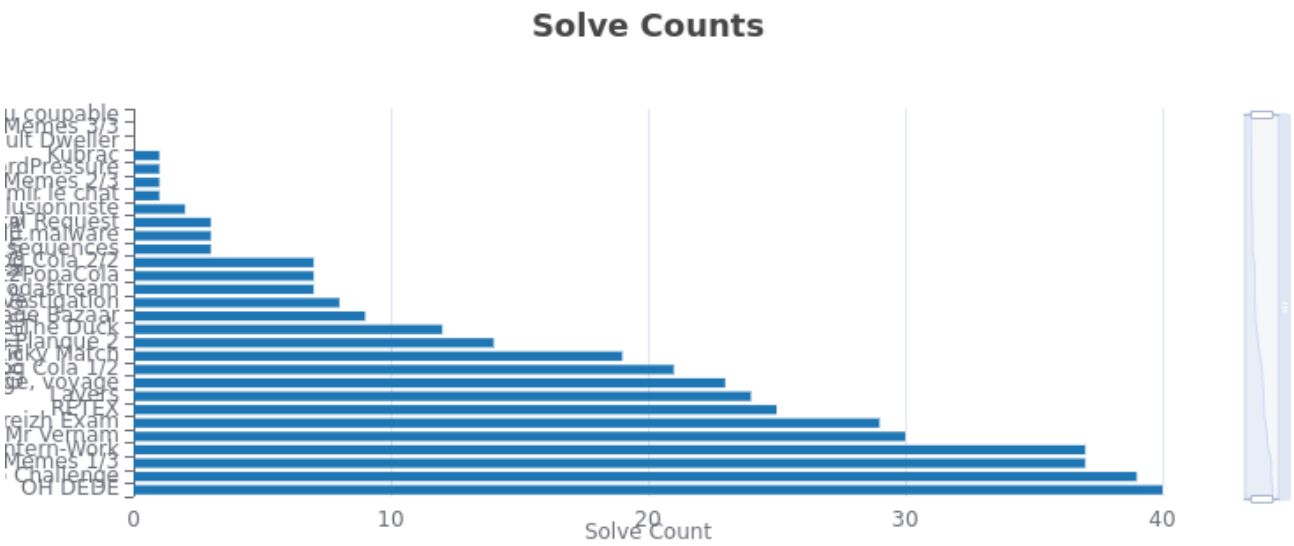


FIGURE 15 – Nombre de résolutions.

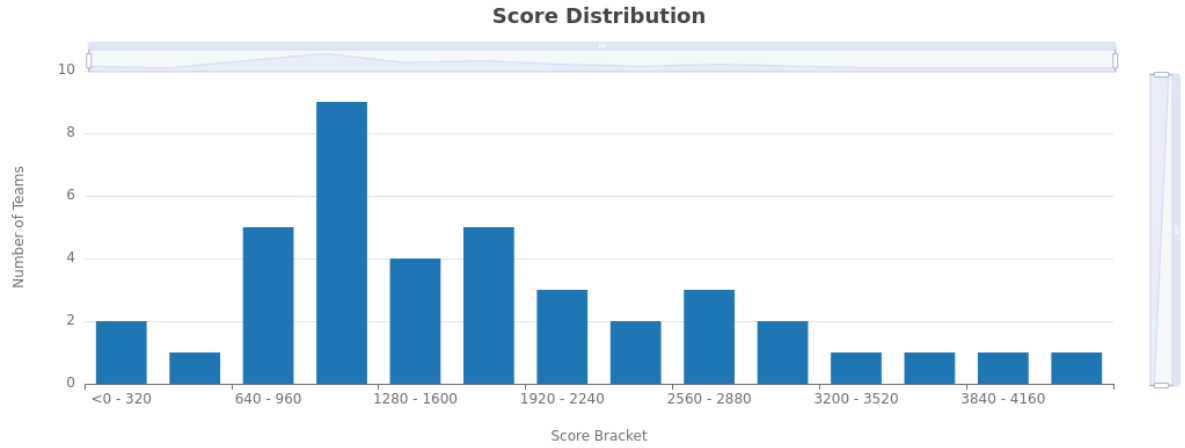


FIGURE 16 – Distribution des scores.

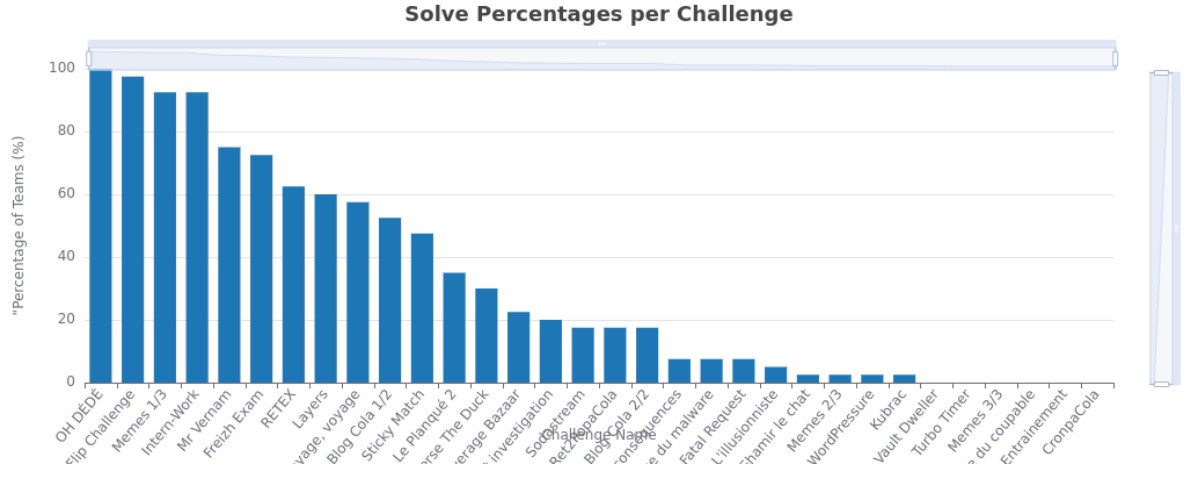


FIGURE 17 – Pourcentages de résolutions par challenge.