

HACKER
VAILLANT



SOMMAIRE

Pitch

Présentation de l'équipe

Charte graphique

Présentation du projet

Valeur ajoutée du projet

Le travail de l'année

Rétroplanning

Budget & partenariats

PITCH DU PROJET



PRÉSENTATION DE L'ÉQUIPE



Ange Brochard M2



Jérémie Garçon B1



Damien Giarmo B1



Lenaig Plantec M1



Ewen Rolland B3



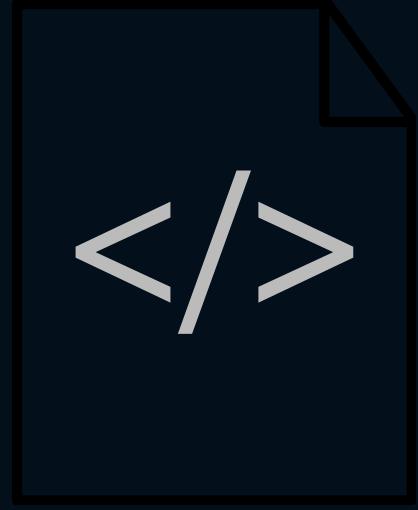
Tristan Geray B3



Rayan Deschamps B1



Dorian Le Bleis-
Michaud-Thomin B1



PRÉSENTATION DE L'ÉQUIPE

Section développement :



Alexandre Plessis M2



Enzo Turpin B1



PRÉSENTATION DE L'ÉQUIPE

Section Infrastructure :

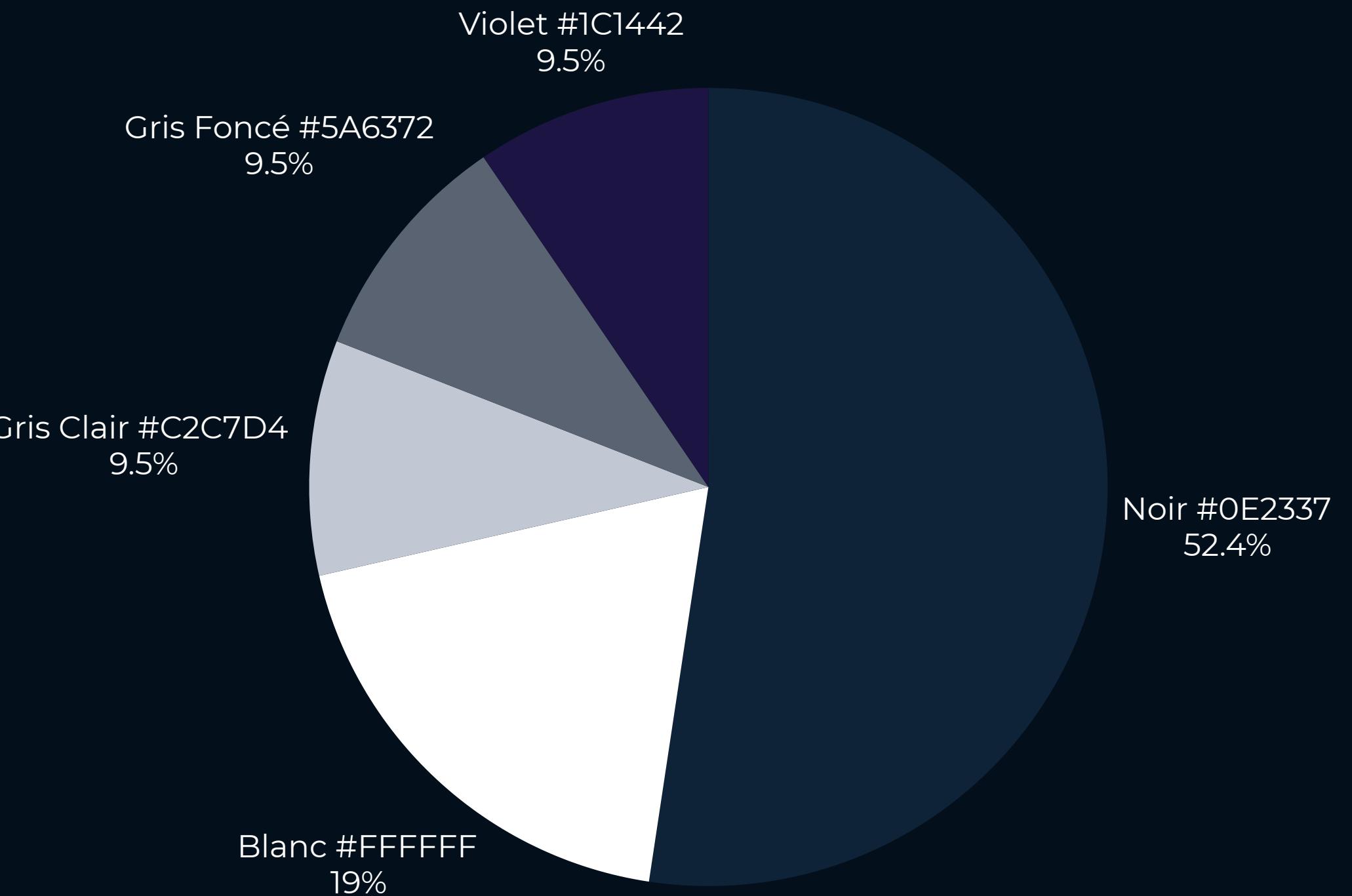


BASILE ESNAULT M2

CHARTE GRAPHIQUE

CHARTE GRAPHIQUE

Palette de couleur :



TYPOGRAPHIES

LOGO ET TITRES

TEXTES

BEBAS NEUE

A B C D E F G H I J K L M N O P Q R S T U V W Y X Z

0 1 2 3 4 5 6 7 8 9

OPEN SANS

A B C D E F G H I J K L M N O P Q R S T U V W Y X Z

a b c d e f g h i j k l m n o p q r s t u v w x y z

0 1 2 3 4 5 6 7 8 9

LOGO :



PRÉSENTATION DU PROJET

2 axes majeurs :

- Plateforme CTF
- Initiation à la cybersécurité

STRENGTHS

Mentora
Serveur déjà hébergé
Créer une plateforme qui va apporter du plus pour les JPO
Plateforme évolutive
Formation pratique

OPPORTUNITIES

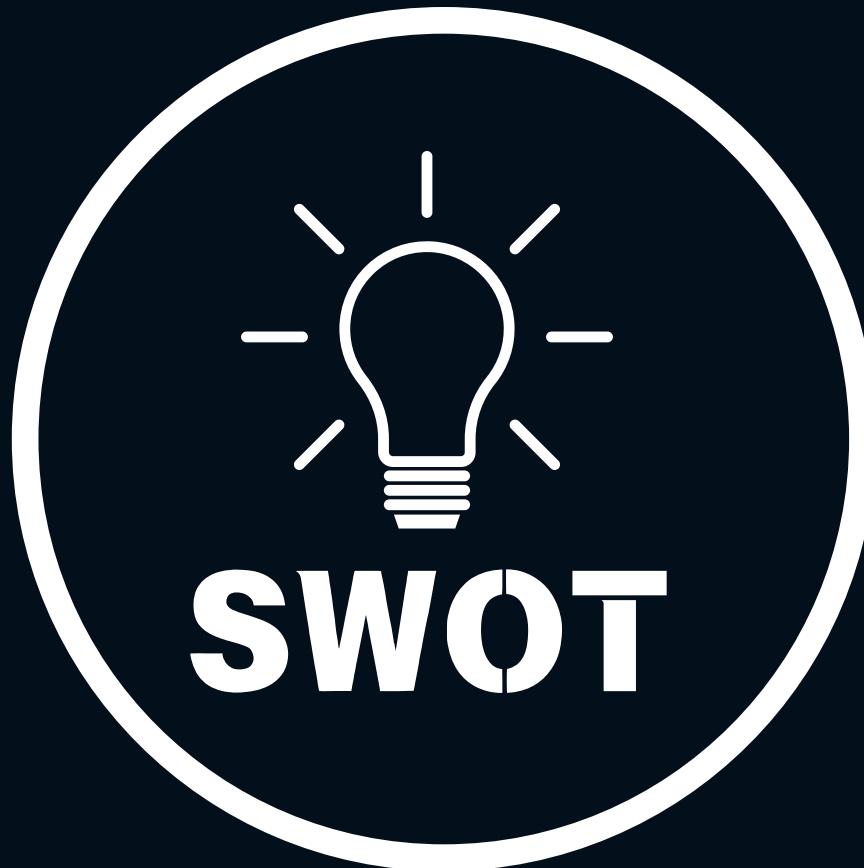
Augmenter la visibilité de l'école
Créer des partenariats /Collaborations externe
Évolution technologique
Élargissement de la communauté

WEAKNESSES

Communication et Cybersécurité
Dépendance à l'investissement des étudiants

THREATS

Pérennité de la plateforme
Sécurité de la plateforme
Évolution des attaques

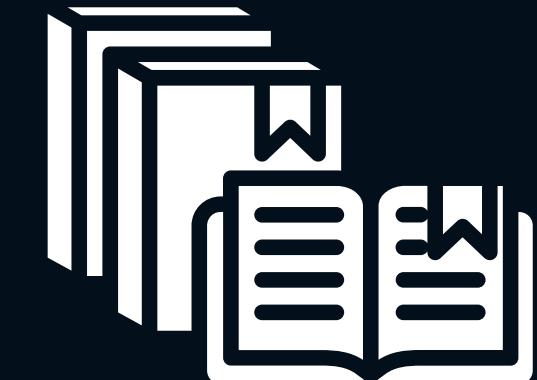


LA VALEUR AJOUTÉE DU PROJET



Apprentissage

- Travail en équipe
- Développer des compétences en cybersécurité
- Promouvoir l'éthique en cybersécurité
- Faciliter l'accès aux ressources externes



LA VALEUR AJOUTÉE DU PROJET

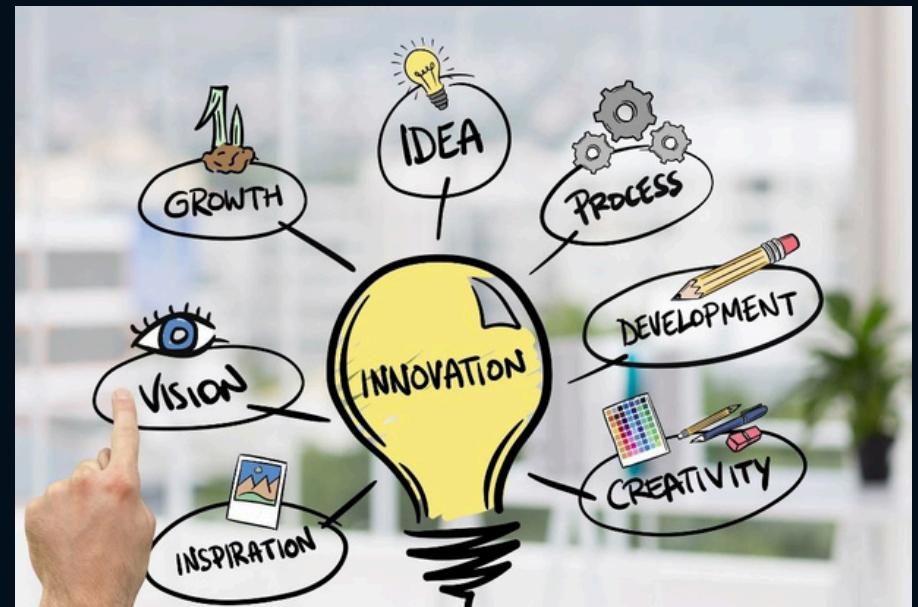


Attentes de l'année

- Créer une plateforme interne de défis
- Organiser et ou participer à des CTF
- Promouvoir la filière cybersécurité (JPO)
- Page de veille (actualités cybersécurité)

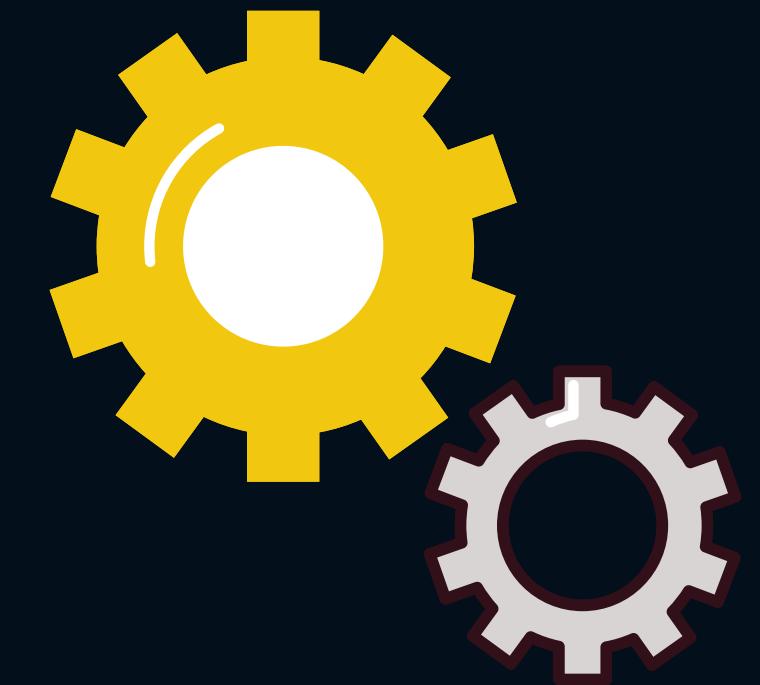


PLATEFORME ÉVOLUTIVE



Contenu Innovant

Ajout de challenges par les étudiants de l'équipe



Outils et Ressources

Page de recensement des différents outils

Page pour mettre en pratique les compétences acquises



Veille Automatique

Page de veille avec flux RSS



RÉALISATION CYBER 2023/2024

EXEMPLE D'ACTIVITÉ SUR DES PLATEFORMES ET DÉFIS

CISCO - mot de passe

15 Points 🐾

Tous les hash n'en sont pas.

Auteur

Thanatos, 10 juillet 2013

Niveau ⓘ

███

Énoncé

Trouvez le mot de passe "Enable".

Démarrer le challenge

2 ressource(s) associée(s)

- Cisco passwords (Réseau)
- Cisco passwords encryption facts (Réseau)

Validation

Entrer le mot de passe

Tache 1 Plan

Démarrer la machine



Avez-vous ce qu'il faut pour pirater cette machine Windows ?
It might take around 3-4 minutes for the machine to boot.

Répondre aux questions ci-dessous

Hachage NTLM de l'utilisateur "Lab" déchiffré

Connectez-vous pour répondre.. Connectez-vous pour répondre..

racine.txt

Connectez-vous pour répondre.. Connectez-vous pour répondre..



Challenge crypto et analyse :

Je voudrais les mdp, vous pouvez bruteforce .

- 1) 3ed7dceaf266cafef032b9d5db224717
- 2) 2ee06c175deb75478d2755406356ec279472d424
- 3) ++++++[>+>++++>++++++>++++++<<<-]>>>+++++++-,------
--,++++++++-,++++++++-,-,<<+,>>-----,-----,++++++++-,<<,>>-----
,+++,-+-,------,++++++++-.
- 4) <▷○▽△ <▽○<▽○▽▷>▽
- 5) bsqbsq ndnd b dakdmd jqd bh fh, kdvpv idaahyd usqm gpmd jqd cd lrho dav nhvihx

LES PROJETS RÉALISÉS

(Projet 1)



Participation à une enquête créée par Ange :

Le but étant de trouver le mots de passe pour déverrouiller la session

osint, brute force, etc...

ACTIVITÉ DGSE

Simulation d'enquête
de la DGSE

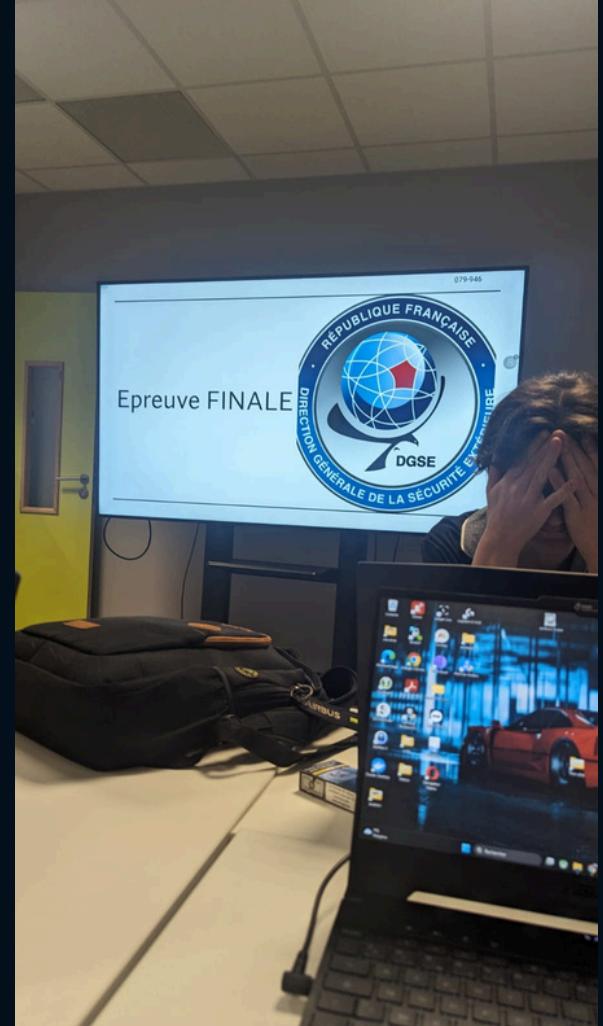
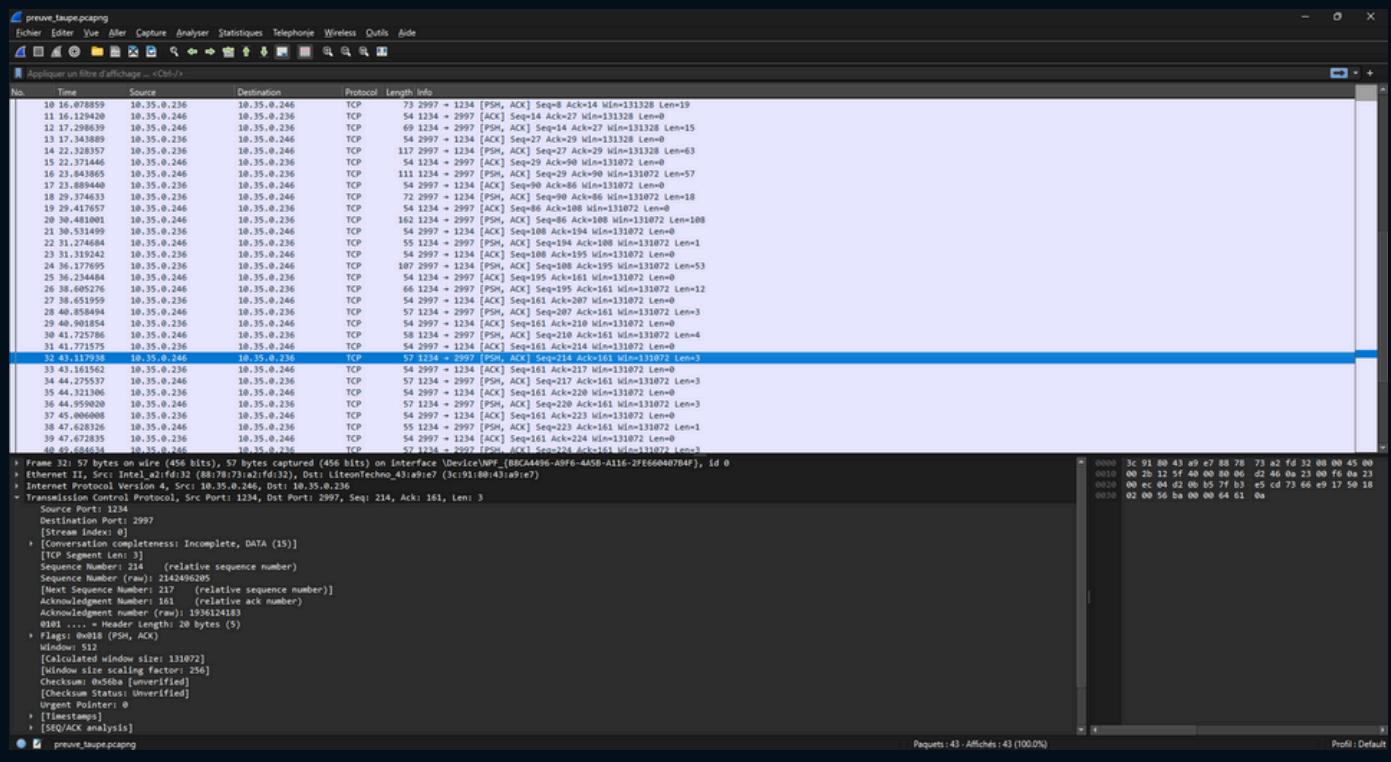
(Projet 2)



```
[root@DESKTOP-EM21BRD]~]
# nmap --script=mysql-info,mysql-databases 172.232.49.198
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-10 11:14 CEST
Nmap scan report for 172-232-49-198.ip.linodeusercontent.com (172.232.49.198)
Host is up (0.066s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
25/tcp    filtered  smtp
80/tcp    open     http
443/tcp   open     https
554/tcp   open     rtsp
3000/tcp  open     ppp
3306/tcp  open     mysql

Nmap done: 1 IP address (1 host up) scanned in 3.55 seconds

[root@DESKTOP-EM21BRD]~]
#
```

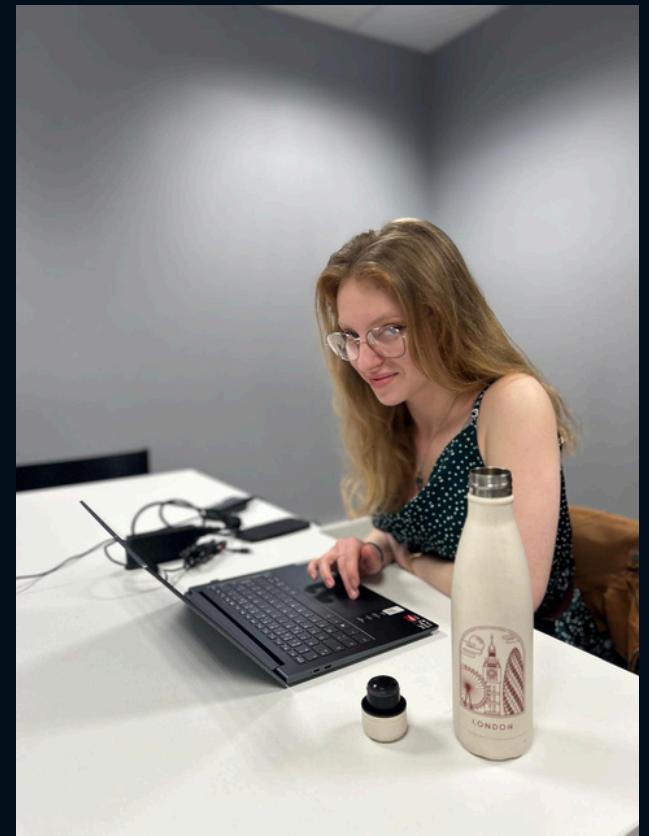


brute force
physique/numérique,
osint, analyse de
données, web...



LA VALEUR AJOUTÉE DU PROJET

Participation CTF YNOV x Seela avec une partie de l'équipe Hacker Vaillant



LA VALEUR AJOUTÉE DU PROJET

Autres CTF



RÉALISATION DEV 2023/2024

La Maquette



MAQUETTES - PAGE D'ACCUEIL

L'équipe

Ringe Brochard
Chef d'équipe réputé pour ces connaissances exceptionnelles dans le domaine de l'Osint. Si vous avez une empreinte digitale, il vous pistera où que vous soyez. Fuir est inutile, il trouvera votre adresse, votre voiture, votre dernier passage en train ou en avion. Il est déjà trop tard.

Nom Prénom
Chef d'équipe réputé pour ces connaissances exceptionnelles dans le domaine de l'Osint. Si vous avez une empreinte digitale, il vous pistera où que vous soyez. Fuir est inutile, il trouvera votre adresse, votre voiture, votre dernier passage en train ou en avion. Il est déjà trop tard.

Anciens CTF

01/01/1970
1^{re} place !

01/01/1970
1^{re} place !

01/01/1970
1^{re} place !

Header

Filtre chall

All | Osint | Misc | Web | Réseau | System | Stegano

Rangée chall

Test
Description rapide du challenge

Test
Description rapide du challenge

Button filtre

All | Osint | Misc | Web | Réseau | System | Stegano

Chall

Test
Description rapide du challenge

Test
Description rapide du challenge

Liste des Challenges

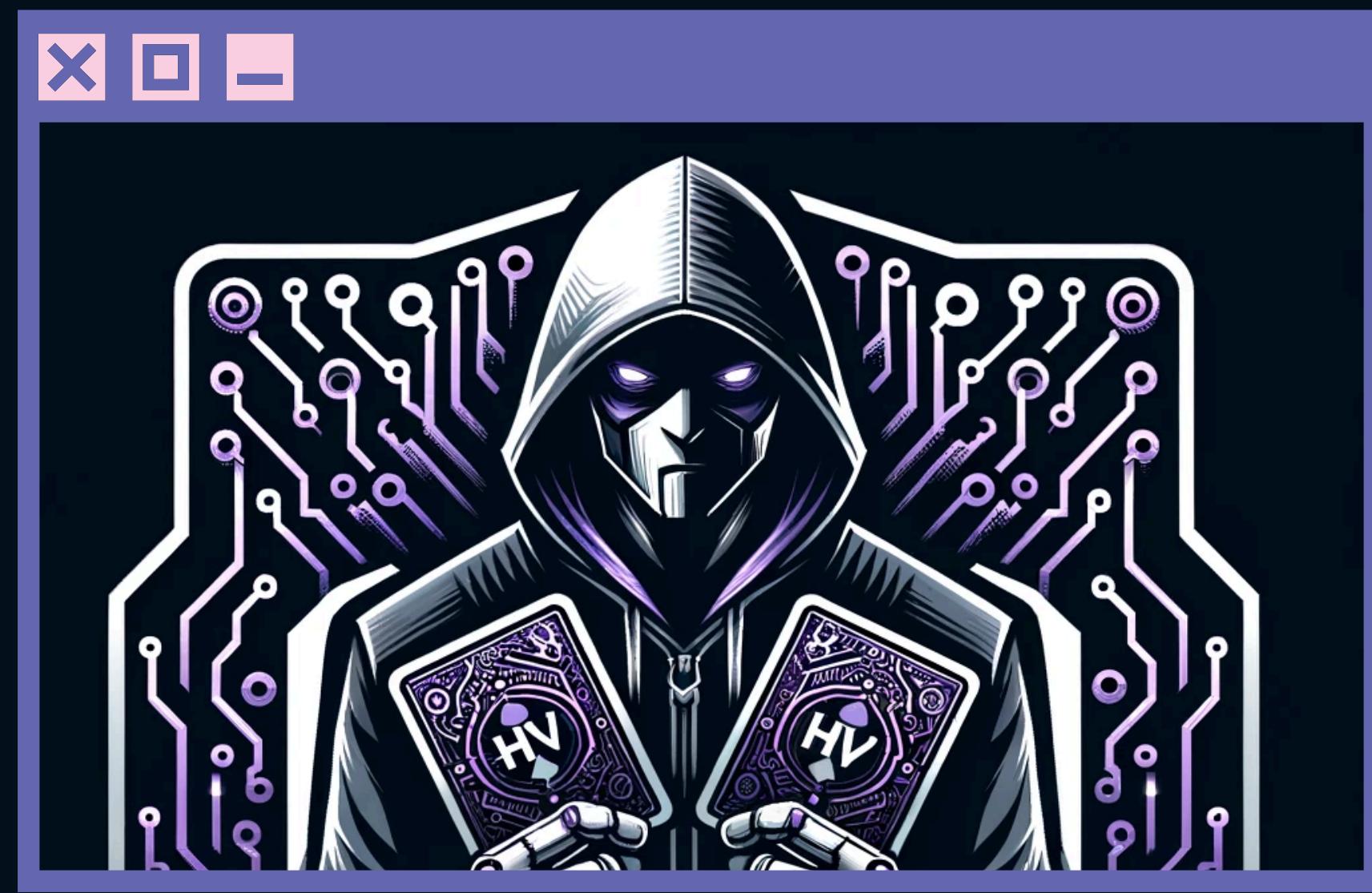
All | Osint | Misc | Web | Réseau | System | Stegano

Test
Description rapide du challenge

Test
Description rapide du challenge

Test
Description rapide du challenge

LA BETA DU SITE WEB



PRESENTATION DU SITE WEB



Home Anciens CTF Challenges Veille

Login

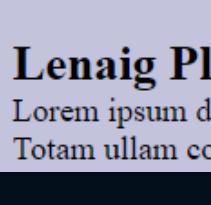
L'équipe



Ange Brochard
Lorem ipsum dolor sit amet consectetur adipisicing elit. Error assumenda deserunt cupiditate non. Illum provident laudantium maiores? Nisi, iure suscipit cum sit saepe magni ipsum nemo a velit fuga commodi.



Basile Esnault
Lorem ipsum dolor sit amet consectetur adipisicing elit. Et placeat dolore iusto dicta dolorem asperiores, porro molestias ad cupiditate consectetur? Modi, nesciunt. Blanditiis ab, quibusdam ullam corrupti non impedit iste?



Alexandre Plessis
Lorem ipsum dolor sit amet, consectetur adipisicing elit. Nam, deserunt distinctio sed odit molestiae labore expedita recusandae fugit voluptatem quidem! Expedita ratione dicta non a blanditiis aut necessitatibus maxime beatae!



Lenaig Plantec
Lorem ipsum dolor sit, amet consectetur adipisicing elit. Vel eius fuga itaque voluptas atque mollitia ut voluptate delectus beatae, ipsam deleniti veritatis? Totam ullam commodi sunt minima consectetur suscipit vitae.

LISTE CTF



Home Anciens CTF Challenges Veille

Login

Anciens CTF



Cliquez pour télécharger

1ère place !

Lorem ipsum dolor sit amet consectetur adipisicing elit. Error assumenda deserunt cupiditate non. Illum provident laudantium maiores? Nisi, iure 01/01/1970
suscipit cum sit saepe magni ipsum nemo a velit fuga commodi.



Cliquez pour télécharger

1ère place !

Lorem ipsum dolor sit amet consectetur adipisicing elit. Error assumenda deserunt cupiditate non. Illum provident laudantium maiores? Nisi, iure 01/01/1970
suscipit cum sit saepe magni ipsum nemo a velit fuga commodi.



Lorem ipsum dolor sit amet consectetur adipisicing elit. Error assumenda deserunt cupiditate non. Illum provident laudantium maiores? Nisi, iure 01/01/1970
suscipit cum sit saepe magni ipsum nemo a velit fuga commodi.

CHALLENGES CYBER



Home Anciens CTF Challenges Veille

Login

Challenges

Hacker Vaillant

Stéganographie

CHALLENGE STÉGANO 1

<http://hacker-vaillant.fr/>

Stéganographie

La stéganographie est l'art de cacher des données secrètes au sein de supports ordinaires, tels que des images ou du texte.

Hacker Vaillant

Cryptographie

CHALLENGE CRYPTO 1

<http://hacker-vaillant.fr/>

Cryptographie

La cryptographie consiste à rendre des données illisibles à toute personne non autorisée en les chiffrant à l'aide d'algorithmes, assurant ainsi la confidentialité des informations.

Hacker Vaillant

web

CHALLENGE WEB 1

<http://hacker-vaillant.fr/>

web

Un challenge cyber en web consiste à résoudre des problèmes de sécurité sur des applications web en exploitant des vulnérabilités pour renforcer les compétences en sécurité informatique.

Hacker Vaillant

Osint

CHALLENGE OSINT 1

<http://hacker-vaillant.fr/>

Hacker Vaillant

forensic

CHALLENGE FORENSIC 1

<http://hacker-vaillant.fr/>

Hacker Vaillant

Réseau

CHALLENGE RÉSEAU 1

<http://hacker-vaillant.fr/>

VEILLE AUTOMATIQUE



Home Anciens CTF Challenges Veille

Login

Veille

Filtres

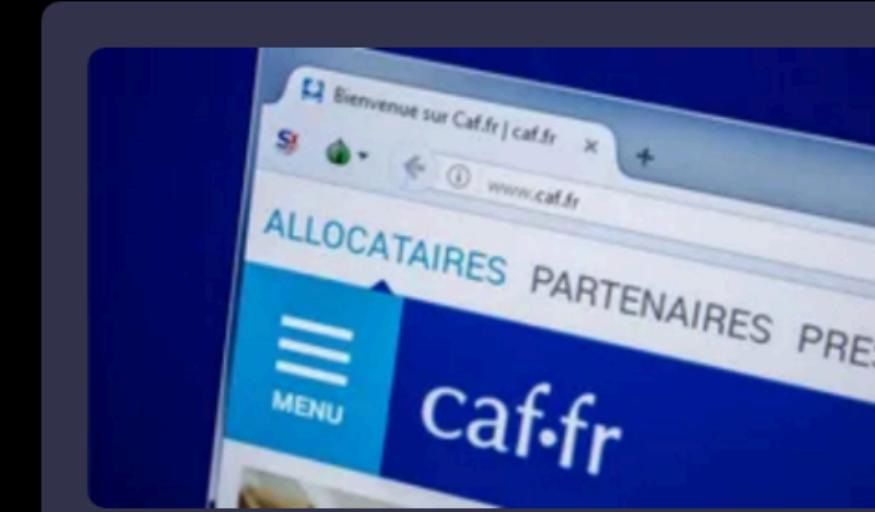
Catégories

- Hacking
- Nouvelles Technologies
- IA



Le clonage de voix, une menace déjà bien réelle pour les entreprises

Bref résumé de l'article 1...



La CAF victime d'une cyberattaque, les hackers revendiquent 600.000 comptes touchés

Bref résumé de l'article 1...

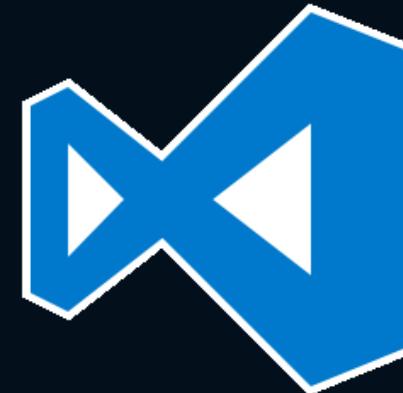
OUTILS DEV

Maquette



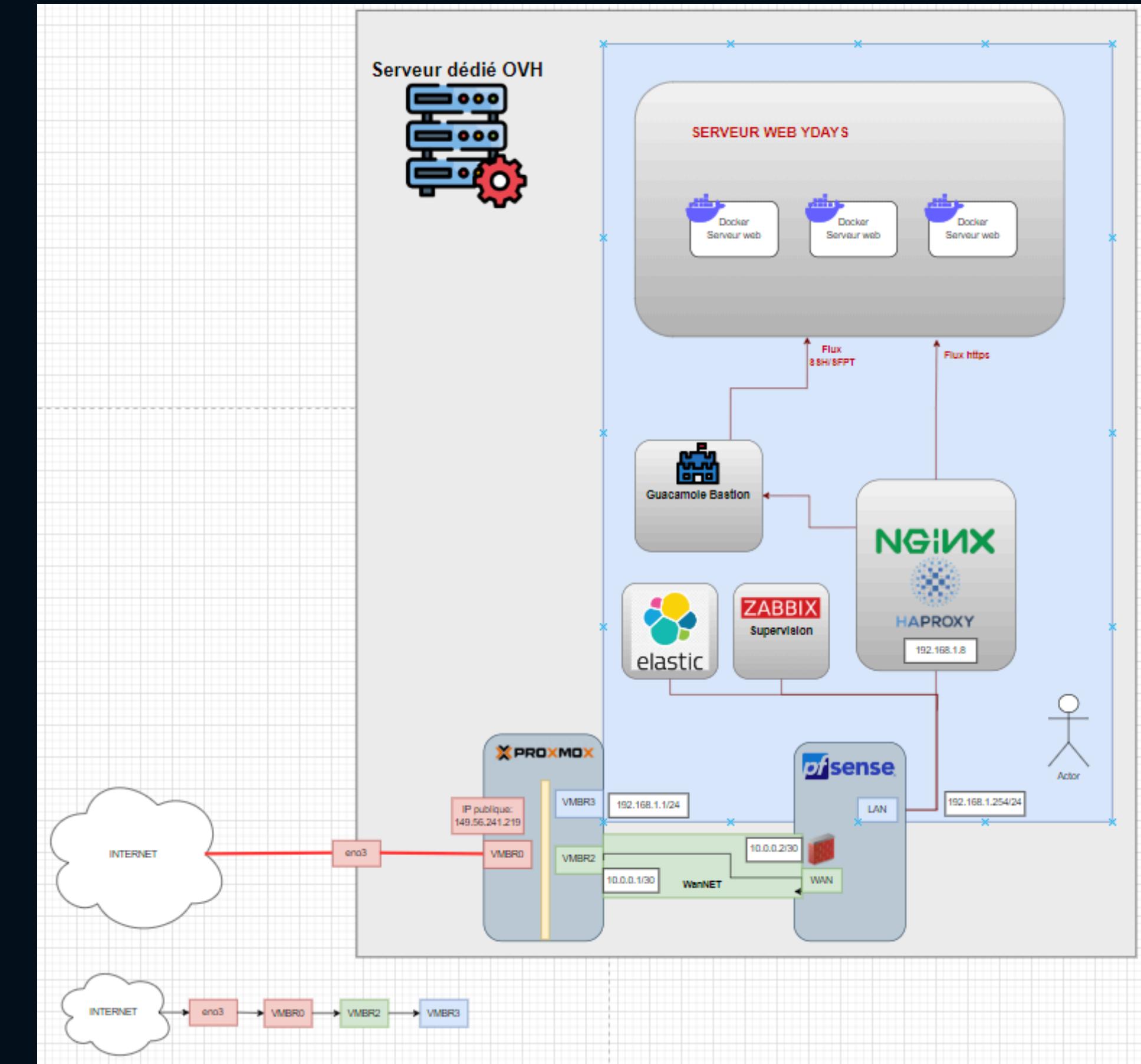
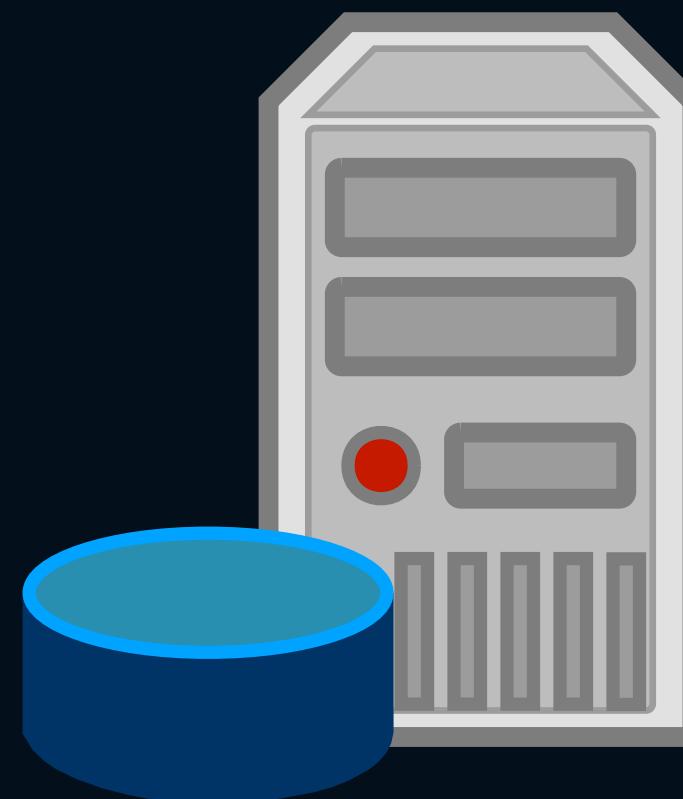
L'OUTIL FIGMA

Site Web



PLATEFORME DE VIRTUALISATION

HÉBERGEMENT YDAYS



PROXMOX Virtual Environment 8.0.9 Search

Pool View 

Datacenter

- GOAD
 - 112 (WinServer2019x64-cloudinit-qcow2)
- Pool_Admin
 - 111 (TRAEFIK)
 - 100 (PfSenseFW) ●
 - 101 (guacamole) ●
 - 102 (Debiancoucou35) ●
 - 103 (Debian-Web) ●
 - 106 (Nginx) ●
- Pool_Eleves
 - 107 (kalaJeremy)
 - 108 (testeLouisN)
- Pool_Hacker-Vaillant
 - 119 (BLOODHOUND)
 - 120 (OPENVAS)
 - 109 (CTFD-hacker) ●
 - 114 (KALIBAZ)
 - 115 (KALINATHANNE)
 - 116 (KALIANGE)
 - 117 (KALIALEX)
 - 118 (KALI2K24)
 - 121 (WinBloodHound)
- Pool_Profs
- Pool_Ydays_Featuring
 - 105 (featuring-back) ●
 - 104 (featuring) ●
- 110 (provisioning)
- 113 (DC-W2K19)
- 122 (kaliantoine)

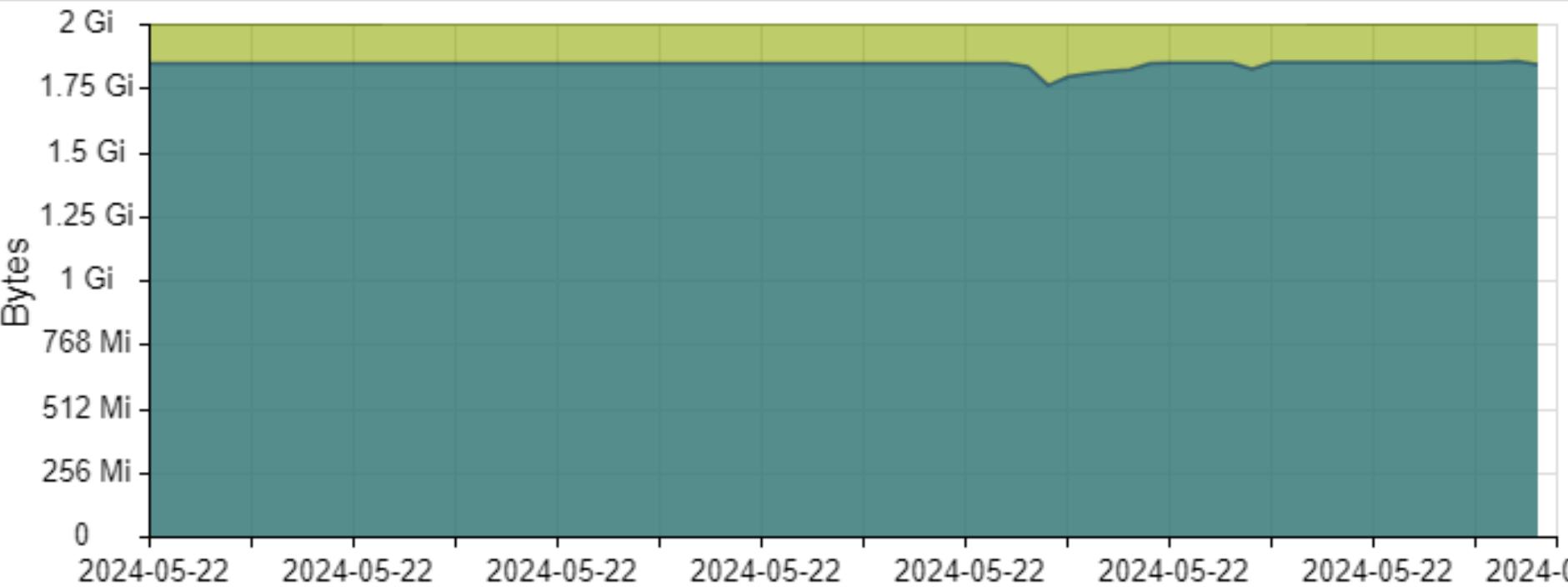
Virtual Machine 102 (Debiancoucou35) on node 'Proxmox-Ynov' admin 

 Summary 
 Console
 Hardware
 Cloud-Init
 Options
 Task History
 Monitor
 Backup
 Replication
 Snapshots
 Firewall
 Permissions

Debiancoucou35 (Uptime: 152 days 16:36:50) Notes  

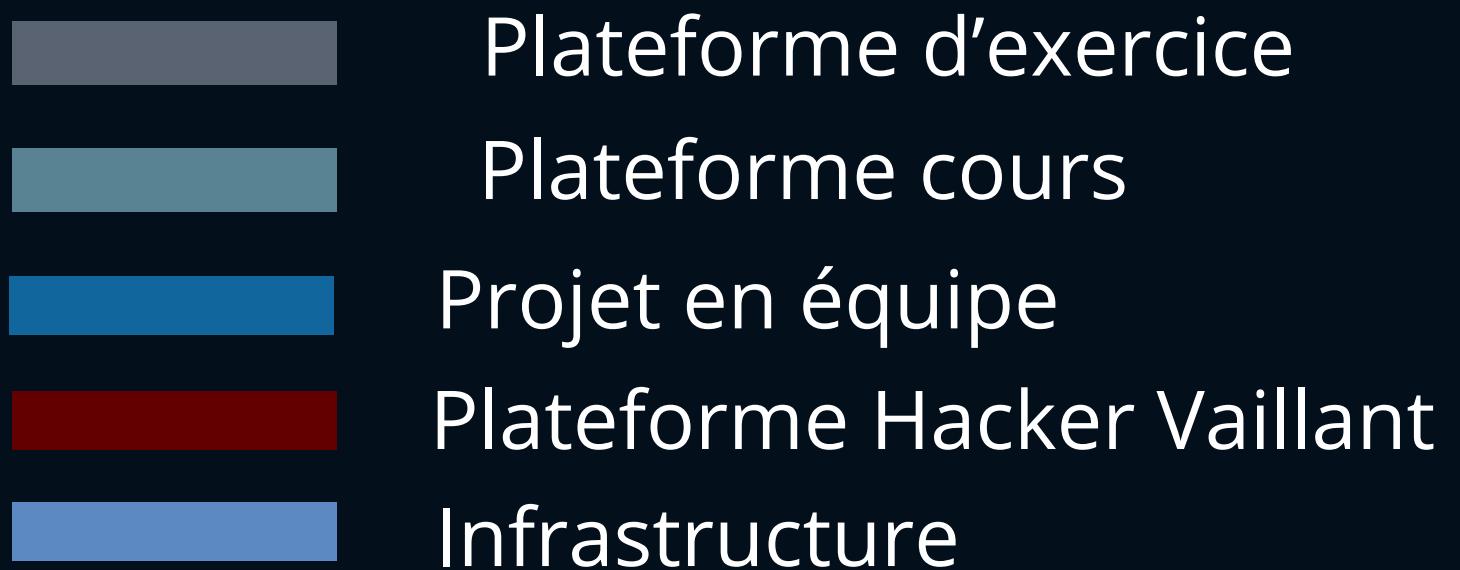
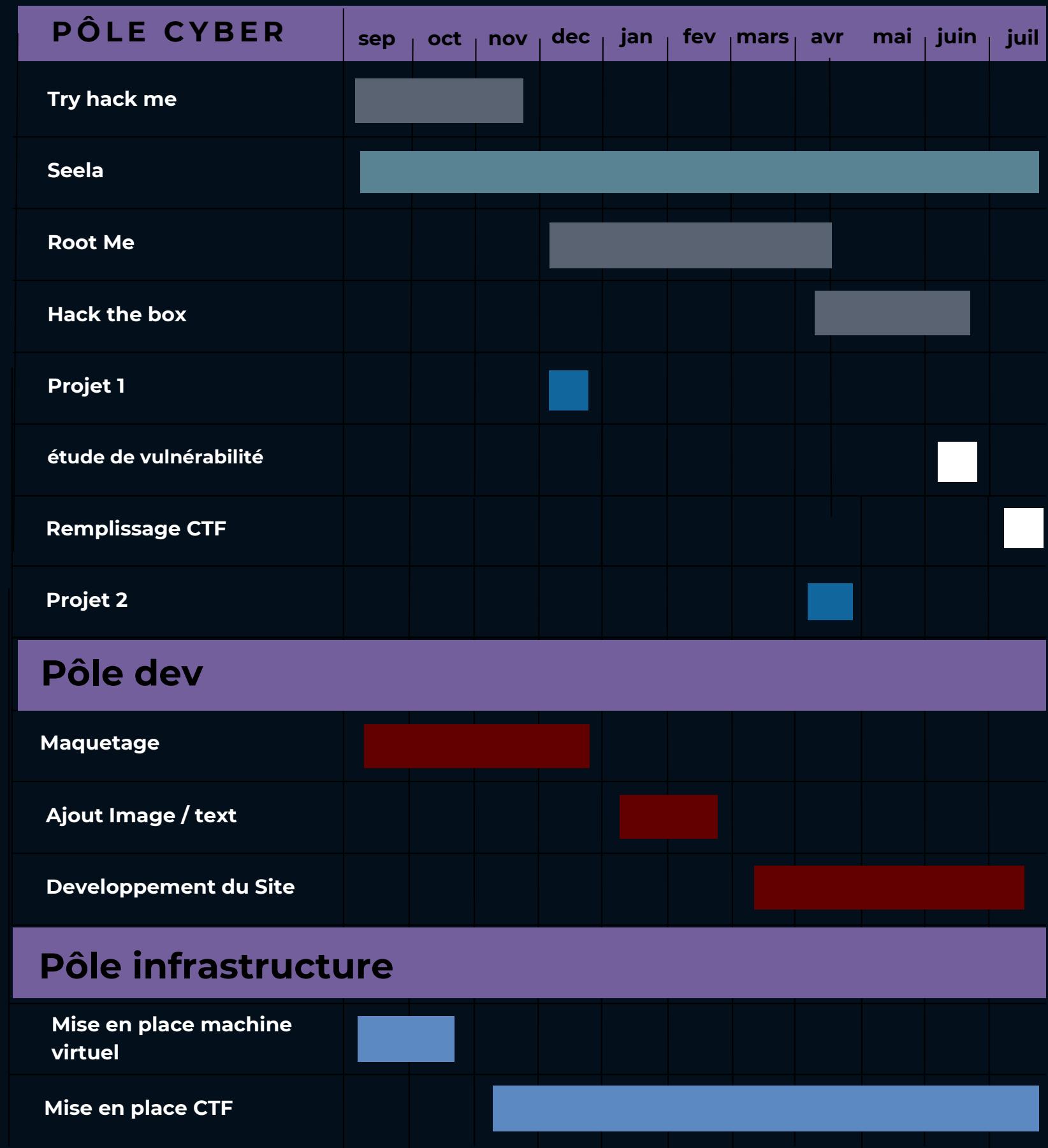
 Status	running	mdp : coucou35
 HA State	none	
 Node	Proxmox-Ynov	
 CPU usage	4.65% of 1 CPU(s)	
 Memory usage	91.97% (1.84 GiB of 2.00 GiB)	
 Bootdisk size	32.00 GiB	
 IPs	No Guest Agent configured	

Memory usage   



The chart displays memory usage in bytes over a period of approximately one month. The Y-axis ranges from 0 to 2 GiB in increments of 0.25 GiB. The X-axis shows dates from May 22, 2024, to June 19, 2024. A light blue area represents the total memory available, and a darker blue line represents the used RAM. The usage fluctuates between 1.75 GiB and 2.0 GiB, with a notable dip around May 28th.

RÉTROPLANNING



BUDGET

Dépenses actuelles :

Hébergement :

Référence	Numéro de commande	Date d'émission	Montant HT	Montant TTC	Solde	Statut	Actions
FR61180265	200388753	29 nov. 2023	493.87 €	592.64 €	0.00 €	Payée	...

Visualisation des dépenses



Achat / abonnement logiciel

- (TryHackMe 1549,29€ /an pour une équipe de 10 pers)



Matériel

- (FLipper 0, switch, ... 220 €)



Participation CTF

- ± 5000€ / an

PARTENARIATS



Et peut-être vous ...

LA PROJECTION DE HACKER VAILLANT

Mise en place de la plateforme,

Recrutement de nouveaux étudiants (cyber & dev),

Ajout de challenges CTF sur la plateforme,

Utilisation plateforme pour les JPO,

Création CTF

NEXT 

MERCI DE VOTRE ATTENTION

