



# Histoires d'Erreurs

Dominique Derrier

Pierre Le Calvez

# Dominique Derrier



**Officiellement**  
0x19 XP  
Neotrust  
vCISO  
iso27001 & NIST

OpenSource

CTF Builder/runner  
ESP32, Docker, Vim



# Pierre Le Calvez



Officiellement

0x14 XP

CGI

Vice-Président Cybersécurité

ex-Pentester

Incident Response enthusiast

Amateur Mountain Climber &  
Skimo Fan



# Disclaimer

C'EST PAS BEAU  
DE SE MOQUER



- ➡ Les histoires sont toutes vraies ;
- ➡ C'est drôle mais on ne se moque pas ;
- ➡ On se veut bienveillant ;
- ➡ On peut apprendre de l'erreur des autres ;
- ➡ Attention certaines sections sont NSFW ;
- ➡ Aucun ChatGPT n'a pas été maltraité durant la production de ces slides.

Au Menu



INSERT COIN ;

⚠ WARNING! LOW HEALTH ;

💀 GAME OVER ;



PlayStation  
Help yourself!

PlayStation

Au Menu



INSERT COIN ;

⚠ WARNING! LOW HEALTH ;

💀 GAME OVER ;



PlayStation  
Help yourself!

PlayStation

# Participez

## Le Blackberry

SdCard photos du CEO et sa secrétaire

43

Impossible à récupérer

1

Dans le cloud

0

L'autre

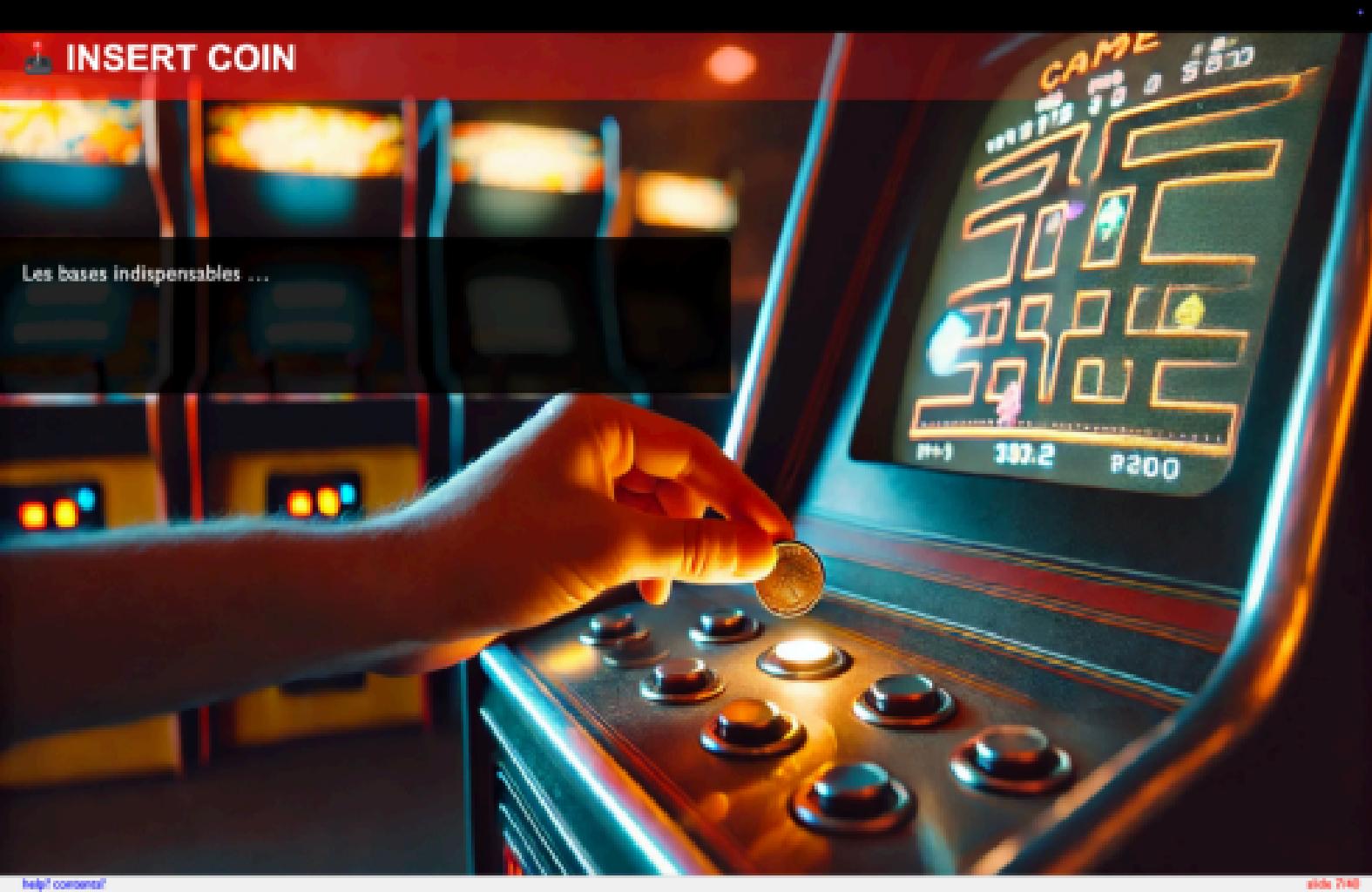
0

44 votes - 44 participants



 INSERT COIN

Les bases indispensables ...



# Mot de passe



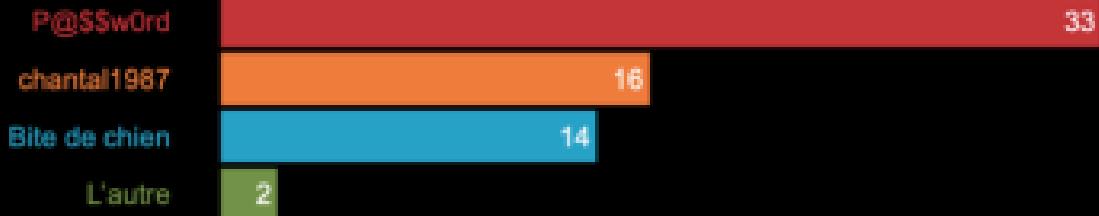
Lors d'un pentest, l'idée est de recueillir un maximum de condensats de mots de passe pour en éprouver la solidité.  
C'est quoi le pire mot de passe que vous puissiez utiliser (et donc cracker)...



# Mot de passe



## Mot de passe



65 votes - 65 participants



# Mise à jour



Le monitoring, MRTG, PRTG, Zabbix, Datadog, Prometheus... Il existe des milliers d'outils pour avoir une visibilité essentielle afin de traiter et d'aider à la gestion des incidents. La mise à jour est nécessaire pour garder une gestion optimale.



# Mise à jour



## Mise à jour



64 votes - 64 participants



# Droit d'admin

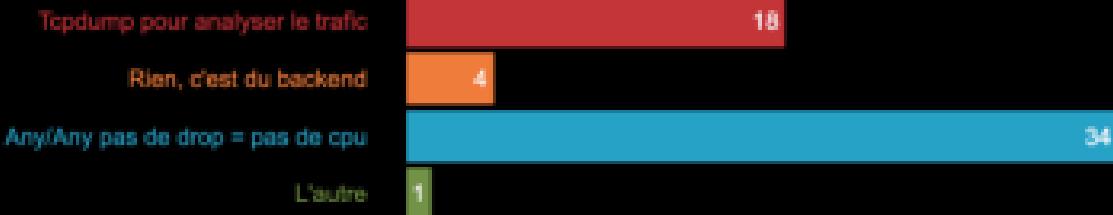


Grosse activité sur le réseau d'administration, celui qui n'est pas connecté à Internet mais il permet de relier l'entreprise à tous ses clients. Le firewall a le CPU dans le tapis. Il y a trop de drops dans les logs qui saturent le CPU.





## Droit d'admin



67 votes - 67 participants



# Sur Le réseau



La lettre de mandat est signée, le test est planifié, l'équipe lance la phase de reconnaissance dans l'entreprise.  
Comme c'est le premier test, l'équipe rouge sait qu'elle va trouver des surprises.

# Sur Le réseau

Mais il y a quoi sur le réseau ?

Une serveur mail configurée

7

La mer noire

0

Le NAS du CIO avec des photos NSFW

51

L'autre

0



100 votes - 59 participants



# Prod Toujours

Le client qui effectue une loterie quotidienne avec 100 000 utilisateurs doit avoir une mise à jour.

La mise à jour a été lancée sur le système.

A priori, le CAB n'a pas été bien réalisé... Évidemment, la machine n'a pas redémarré. Et comme un incident n'arrive jamais seul, La procédure de rollback n'a pas été écrite.



# Prod Toujours



## Prod Toujours



55 votes - 55 participants



**⚠ WARNING! LOW HEALTH**

# WARNING!

Les menaces et incidents à surveiller (ou pas)

**LOW-HEALTH!**

BARTH

15:9-001!!

# Fraude Telephonique



Une compagnie vous appelle pour l'aider pendant une fraude téléphonique. En effet, elle s'est rendu compte de la mise en place d'une redirection téléphonique vers un numéro surtaxé (que vous maîtrisez).

Le client a déjà subi 20 000 \$ de fraude pendant le week-end et vous demande un devis pour l'aider.



# Fraude Telephonique



## La fraude téléphonique

Récupérer le n° de la secrétaire

7

La réponse B

2

5 jours à négocier 10\$ (200k\$ au total)

36

On appelle son opérateur

5



60 vues - 69 participants



# Mysql

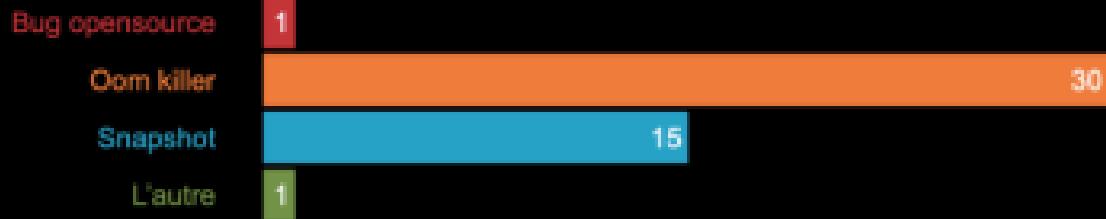
Erreur d'indisponibilité sur un serveur client à forte consultation : la base ne répond plus à la même heure chaque jour. Cela fait plusieurs jours que cela dure.



# Mysql



## Mysql



47 votes - 47 participants



## Rm /save

Pour aller plus vite les administrateurs sont créatifs à faire des raccourcis pour fluidifier leur gestion.

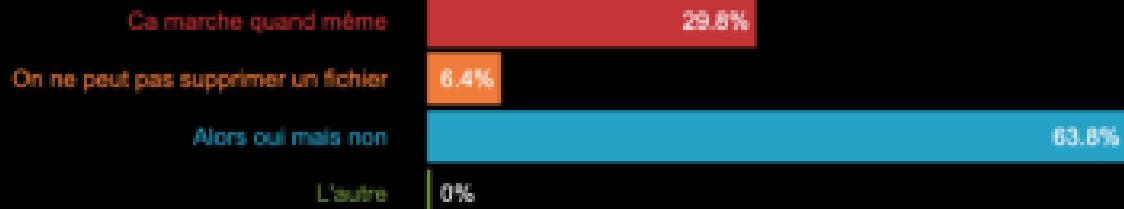
Un admin a fait : ln -s /opt/database1 /osave

Quelques jours plus tard pour faire le ménage un autre a fait : rm /osave/\*





## rm /save



47 votes - 47 participants



# Déclarer ou pas Déclarer



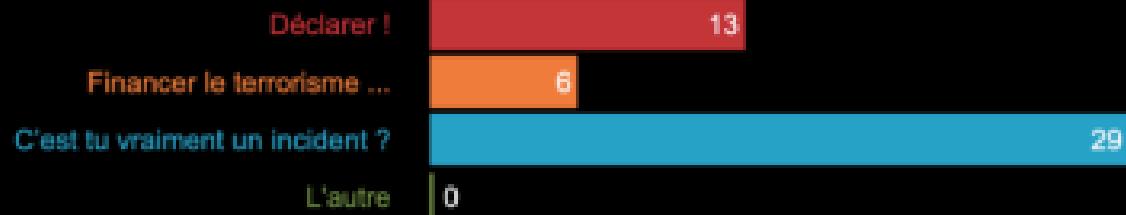
On arrive le lundi matin et il n'y a plus rien qui fonctionne... **C'est le drame...**  
On nous demande une rançon.  
La totalité des fichiers de l'entreprise est chiffrée et, pour les récupérer, il faut payer.  
Alors, que fait-on ?



# Déclarer ou pas Déclarer



## Déclarer ou pas Déclarer l'incident ?



40 votes - 40 participants



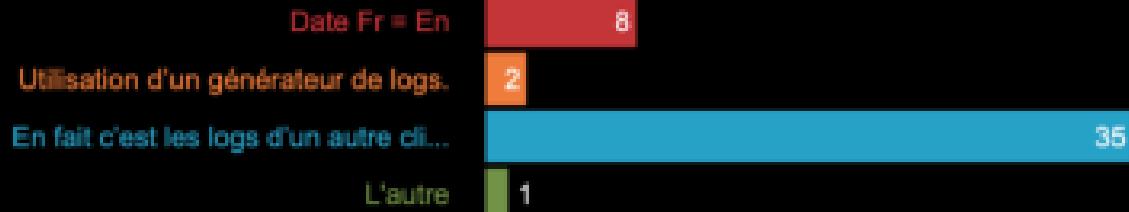


L'équipe utilise une équipe de réponse pour traiter les incidents, un service coûtant plusieurs milliers de dollars par mois. Ils remontent des alertes et déclenchent le plan d'escalade... Mais il est impossible de trouver les traces.





## MDR Team



46 votes - 46 participants



 GAME OVER

INSERT COIN TO CONTINUE.

GAME OVER

GAME OVER!

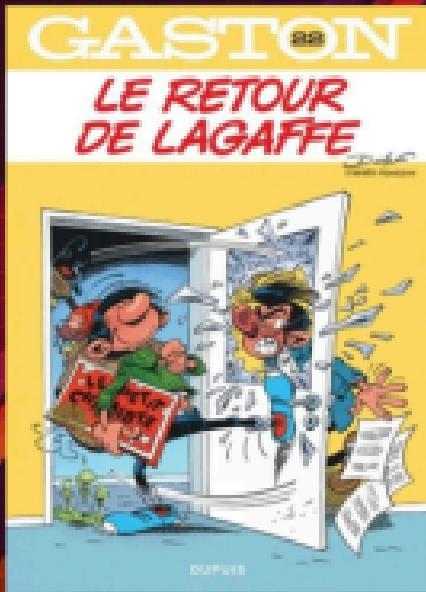
CONTINUE?

9.87

INSTINCT COIN  
TO CONTINUE..

Quand tout part en ville

# Gestion d'incident



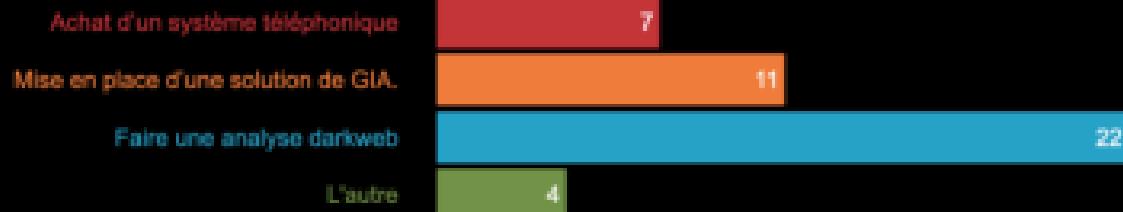
Incident arrive, c'est dans la douleur qu'on apprend le plus vite... et c'est moins le fun.  
Intervention chez un client c'est parti pour organiser, mais il manque quelques éléments.



# Gestion d'incident



## Gestion d'incident



48 votes - 48 participants



# Le Blackberry perdu



Mais où sont jeté les anciens téléphones ? Dans les poubelles bien sûr...

Et à votre avis ... dans un téléphone il y a quoi ?



# Le Blackberry perdu



## Le Blackberry

SdCard photos du CEO et sa secrétaire

43

Impossible à récupérer

1

Dans le cloud

0

L'autre

0

44 votes - 44 participants



# Recovery

L'accident est malheureusement arrivé, il devait arriver car il n'y avait pas de patch, un musée archéologique.

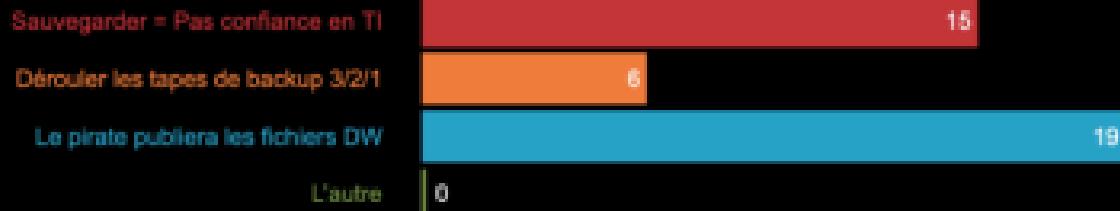
Confinement, éradication et récupération.

C'est le moment de vérifier où sont les sauvegardes... et les retrouver : Mais,





## Recovery / Backup



49 votes - 49 participants



# Phishing

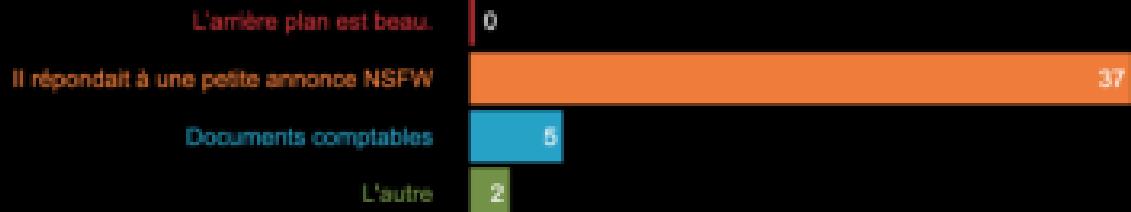
La sensibilisation par le phishing est l'un des premiers outils de sensibilisation marquants pour les équipes et les entreprises de toute taille qui utilisent l'informatique.

Comment une sensibilisation par phishing peut-elle vraiment mal tourner ?



# Phishing

## Le phishing



46 votes - 66 participants



Nous aurions voulu...

Ne pas cliquer ici !



## Le mot de la fin ...

Même si

- l'amélioration continue ;
- l'intelligence artificielle ;

Les questions de sécurité ne vont pas disparaître et les erreurs humaines ne vont pas s'arrêter.

Si l'on ne veut pas continuer à apprendre de ses erreurs, une dose d'humour dans l'amélioration continue est nécessaire pour avancer.

