

# Recap 2025 - Dossier 'sensible' mais drôle

Tout est inventé. Toute ressemblance avec des faits réels serait un heureux hasard.

1.	Top incidents absurdes 2025
2.	Mots de passe de l'année
3.	Phishing Awards 2025
4.	KPI qui piquent les yeux
5.	Procurements surprenants
6.	Minutes du comité de crise
7.	Journal SOC: perles et memes
8.	Annexes: snippets croustillants

# 1. Top incidents absurdes 2025

- 1 Janvier: panne globale causee par un script nomme `do_not_run.sh` execute 'pour voir'.
- 2 Mars: serveur de recette devenu prod apres un copier-coller ambitieux.
- 3 Mai: mot de passe change en reunion, oublie avant la fin du point.
- 4 Juillet: coupure reseau apres qu'un switch ait 'mange' un post-it important.
- 5 Octobre: page de statut tombe en panne en annonçant que tout va bien.

Note: incidents purement fictifs. N'essayez pas chez vous.

## 2. Mots de passe de l'annee

Categorie	Candidat	Commentaire
Le classique persistant	Password2025!	Ajoute un ! et appelle ca Zero Trust
Le saisonnier	HiverHiverHiver	Helas, change au printemps
Le film culte	DunePartTwo2	Spoiler inside the hash
Le meeting	OnVoitCaPlusTard	Jamais change depuis 2023
Le secure-ish	Gaufre-7-Limace	Au moins ca se retient

### 3. Phishing Awards 2025

Notre palmares des emails les plus 'convaincants' (mais totalement inventes):

Prix	Sujet	Technique
Grand Prix	Votre colis attend sur le bureau du PDG	Urgence + familiarite
Mention speciale	Facture en retard: 0,02 EUR	Montant ridicule donc probable
Prix design	Invitation a la soiree theme cyber licornes	Curiosite + RSVP
Prix nostalgie	Votre compte Minitel est suspendu	Absurdite calculée

Conseil serieux: verifier le domaine, les pieces jointes, et les liens raccourcis.

## 4. KPI qui piquent les yeux

Indicateur	Valeur 2025	Objectif 2025	Status
Temps moyen de 'oups' detecte	7 min	< 5 min	Orange
Reunions ou la mitigation est 'en cours'	104	12	Rouge
Alertes resolues par cafe	68%	50%	Vert
Incidents survenus un vendredi 17h	11	0	Rouge
Docs mis a jour avant incident	1 sur 5	5 sur 5	Orange

## 5. Procurements surprenants

- Lot 'cables reseau' commande en rose uniquement pour maintenir la morale.
- Pare-feu 'edition collector' avec autocollants holographiques.
- Sonde IDS qui clignote plus fort quand c'est critique. Scientifique donc fiable.

Note: pas d'achat reel; tout est invente pour le sourire.

## 6. Minutes du comite de crise (extrait)

08:31 - 'Quelqu'un a touche a quelque chose ?' - silence apprecie.

08:39 - 'On redemarre et on voit.' - phrase celebre.

09:05 - 'Qui a les droits admin ?' - tout le monde regarde ses chaussures.

09:42 - 'Le post-mortem sera lundi.' - note: lundi  $f(t+14)$ .

## 7. Journal SOC: perles et memes

[Logbook] Analyste: 'Pourquoi le playbook dit Etape 3: improviser ?'

[Radio] 'On a perdue la prod.' 'Pas grave, on a la pre-prod.' 'On l'a perdu aussi.'

[Tip] Si c'est marqué 'urgent urgent urgent', c'est probablement 'non urgent'.

[Meme] Diagramme: securite vs 'ca marche chez moi' -> triangle impossible.



## 8. Annexes: snippets croustillants (fictifs)

```
# nginx.conf (extrait fictif)
server {
listen 443 ssl;
server_name portal.example.test;
# TODO: activer HSTS avant 2030
add_header X-Frame-Options SAMEORIGIN;
add_header X-Content-Type-Options nosniff;
}
```

```
# crontab (extrait inventé)
# m h dom mon dow command
0 2 * * * /usr/local/bin/backup.sh
15 4 * * 1 /usr/local/bin/rotate-secrets.sh
0 9 * * * echo 'Ne jamais tester en prod' # auto-rappel
```

Rappel: tout contenu est humoristique et fictif. A utiliser pour de la sensibilisation légère.