



Présentation de l'audit de sécurité de l'infrastructure

Objectif :

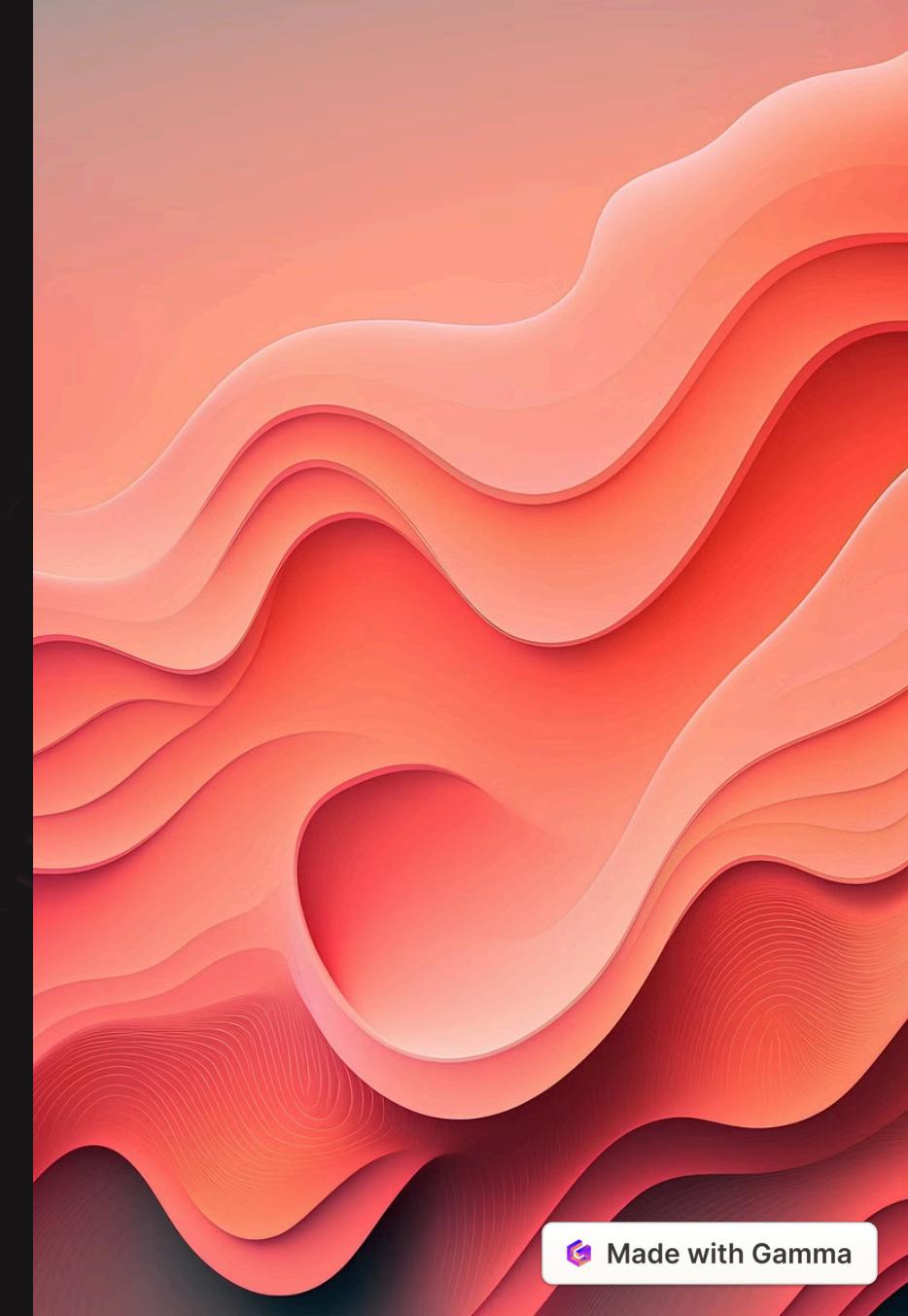
Identifier les vulnérabilités, analyser les risques et proposer des solutions de rémédiation

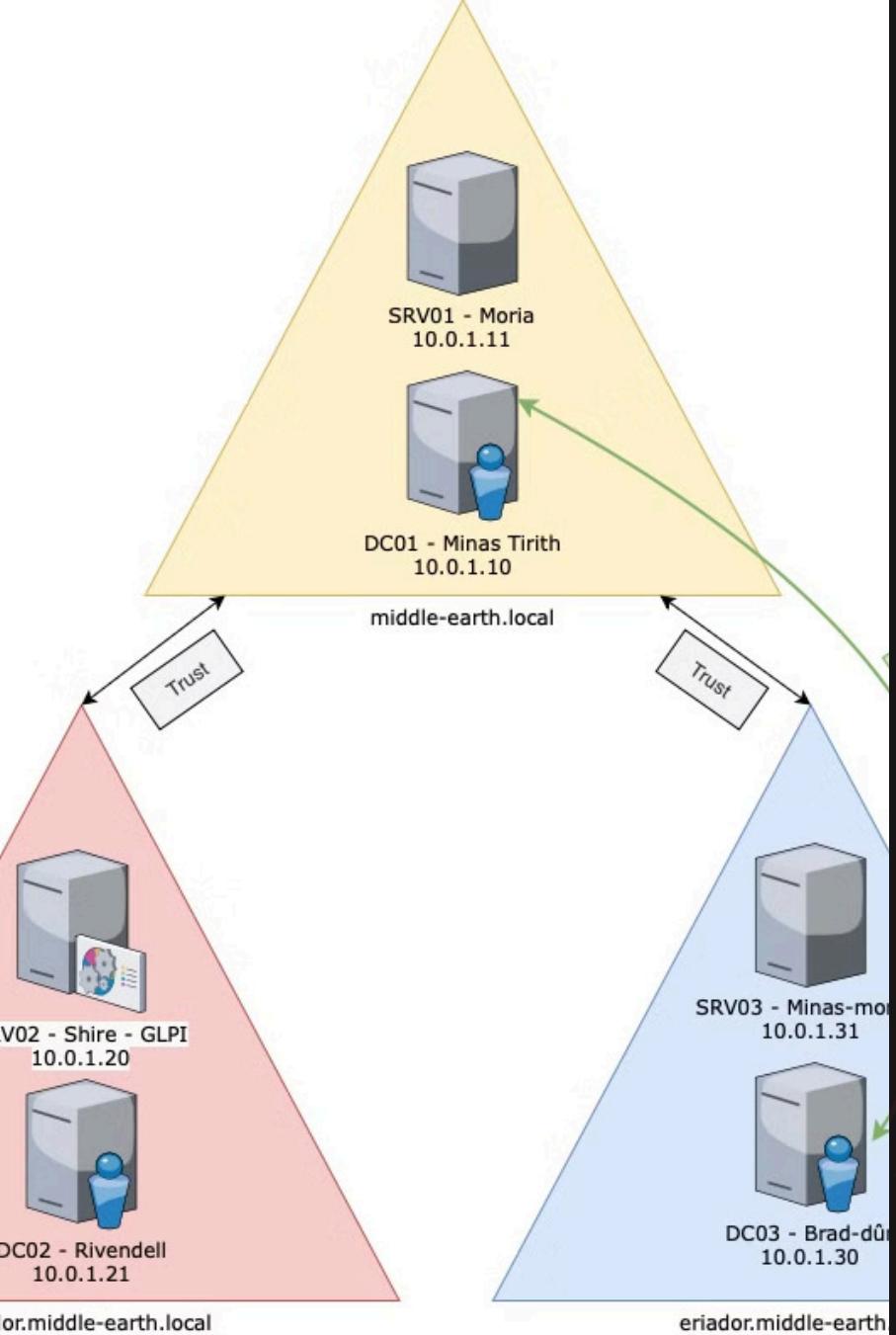
1 Test d'intrusion

2 Rapport de compromission

3 PSSI

Politique de Sécurité des Systèmes de l'information





Contexte du Test d'Intrusion

Périmètre

Audit réalisé sur le serveur GLPI, les services associés et l'environnement réseau

Objectif

Evaluer la sécurité du serveur et des services critiques

Phases du Test d'Intrusion

👀 Reconnaissance

Identification des services et version en cours d'exécution

🔒 Evaluation des vulnérabilités

Détection des failles via Nessus et Linpeas

🎯 Exploitation

Tentative d'exploitation pour évaluer les risques

⚠️ Post-exploitation

Analyse des conséquences des vulnérabilités exploitées

Présentation des vulnérabilités

3 vulnérabilités critiques découvertes

Présentation des preuves, des impacts et des recommandations



Vulnérabilité 1 - *htmLawed*

- **Command injection** dans la bibliothèque tierce htmLawed utilisée par GLPI
- **Preuve** : Exécution de code à distance via l'exploitation de la faille dans le fichier hemLawedTest.php
- **Impact** : Prise de contrôle complète du serveur, permettant à l'attaquant d'exécuter des commandes arbitraires
- **Rémédiation** : Mise à jour de GLPI vers la version 10.0.3 ou suppression du fichier vulnérable

```
meterpreter > shell
Process 32214 created.
Channel 1 created.
whoami
www-data
ls
LICENSE-GPL2
LICENSE-LGPL3
htmLawed.php
```

Vulnérabilité 2 - *Mots de passe en clair*

- **Mots de passes stockés en clair** dans les fichiers de configuration de GLPI
- **Preuve** : Fichiers accessibles par le compte www-data
- **Impact** : Accès non autorisé à la base de données, compromettant des informations sensibles
- **Rémédiation** : Chiffrement des mots de passe, gestion sécurisée des secrets

```
cat config_db.php
<?php
class DB extends DBmysql {
    public $dbhost = 'localhost:3306';
    public $dbuser = 'glpi';
    public $dbpassword = 'bx05jHJs1bVCgFo';
    public $dbdefault = 'glpi';
    public $use_timezones = true;
```

Vulnérabilité 3 - *Mots de passe par défaut*

- Utilisation des **mots de passe par défaut** pour plusieurs comptes GLPI
- **Preuve** : Mots de passes déchiffrés rapidement via un outil de brute force
- **Impact** : Accès initial facilité pour un attaquant, compromission possible du serveur GLPI
- **Rémédiation** : Remplacement immédiat des mots de passe par des mots de passe forts et uniques

```
ali)-[~/Documents/Jedha]
format=bcrypt hash.txt

lt input encoding: UTF-8
ssword hashes with 4 different salts (bcrypt [Blowfish 32/64 X3])
ration count) is 1024 for all loaded hashes
OpenMP threads
with single, rules:Single
r Ctrl-C to abort, almost any other key for status
  (post-only)
ly 3 candidates buffered for the current salt, minimum 9 needed for perfo
  (tech)
ly 4 candidates buffered for the current salt, minimum 9 needed for perfo
  (glpi)
  (normal)
00 DONE 1/3 (2024-07-09 16:21) 12.50g/s 50.00p/s 68.75c/s 68.75C/s normal
show" option to display all of the cracked passwords reliably
pleted.
```

De l'Identification à l'Analyse de Compromission

Focus sur les indicateurs de compromission détectés

Importance de la détection rapide pour minimiser les impacts



Time	Delta	Source	Destination	Protocol	Length	Info
18 2024-07-10 15:52:30,325731	0.000000	0.0.0.1.12	10.0.1.208	HTTP	341	POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/
25 2024-07-10 15:52:30,342324	0.016593	10.0.1.208	10.0.1.12	HTTP	144	GET / HTTP/1.1
32 2024-07-10 15:52:36,362453	6.020129	10.0.1.12	10.0.1.208	HTTP	69	Continuation
38 2024-07-10 15:52:39,920738	3.558285	10.0.1.12	10.0.1.208	HTTP	73	Continuation
47 2024-07-10 15:52:50,570000	10.6492...	10.0.1.12	10.0.1.208	HTTP	82	Continuation
56 2024-07-10 15:53:01,610152	11.0401...	10.0.1.12	10.0.1.208	HTTP	105	Continuation
65 2024-07-10 15:53:04,974165	3.364013	10.0.1.12	10.0.1.208	HTTP	74	Continuation
80 2024-07-10 15:53:17,275463	12.3012...	10.0.1.12	10.0.1.208	HTTP	73	Continuation
101 2024-07-10 15:53:34,511705	17.2362...	10.0.1.12	10.0.1.208	HTTP	76	Continuation
103 2024-07-10 15:53:39,587424	5.075719	10.0.1.12	10.0.1.208	HTTP	73	Continuation
112 2024-07-10 15:53:47,797652	8.210228	10.0.1.12	10.0.1.208	HTTP	82	Continuation

IoCs - Indicateurs de Compromission

Adresses IP suspectes : 10.0.1.12

```
Hypertext Transfer Protocol
> POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1\r\n
Host: 10.0.1.208\r\n
User-Agent: curl/8.8.0\r\n
Accept: */*\r\n
Content-Length: 93\r\n
Content-Type: application/x-www-form-urlencoded\r\n
\r\n
[Full request URI: http://10.0.1.208/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh]
[HTTP request 1/1]
File Data: 93 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
```

Requêtes HTTP malveillantes : Requête POST exploitant une vulnérabilité Apache (CVE-2021-41773)

```
..z..5...{@....E...
.DC @ @......
....\..e..g.z...
.....S*.N...
..cat /e tc/passw
d.
```

Modification de fichiers critiques : Accès illégal à /etc/passwd



TTPs - Tactiques, Techniques et Procédures

1

Exploitation

Utilisation de la vulnérabilité CVE-2021-41773 pour l'accès initial

2

Techniques

Maintien d'accès persistant

3

Procédures

Commandes exécutées pour explorer le système compromis

Du Diagnostic aux Solutions

Focus sur les solutions pour remédier aux vulnérabilités et prévenir les futures attaques



Contre-mesures et Recommandations

1

2

3

4

GLPI

Mise à jour pour
corriger la vulnérabilité
CVE-2022-35914

Mots de passe en clair

Chiffrement et gestion
sécurisée des secrets

Mots de passe par défaut

Remplacement des
mots de passe forts et
uniques

Surveillance accrue

Mise en place d'une
surveillance en temps
réel



Made with Gamma

De la Rémédiation à la Prévention



Importance d'une politique de sécurité bien définie pour une prévention à long terme et protéger la confidentialité, l'intégrité et la disponibilité des systèmes

PSSI - Politique de Sécurité des Systèmes d'Information

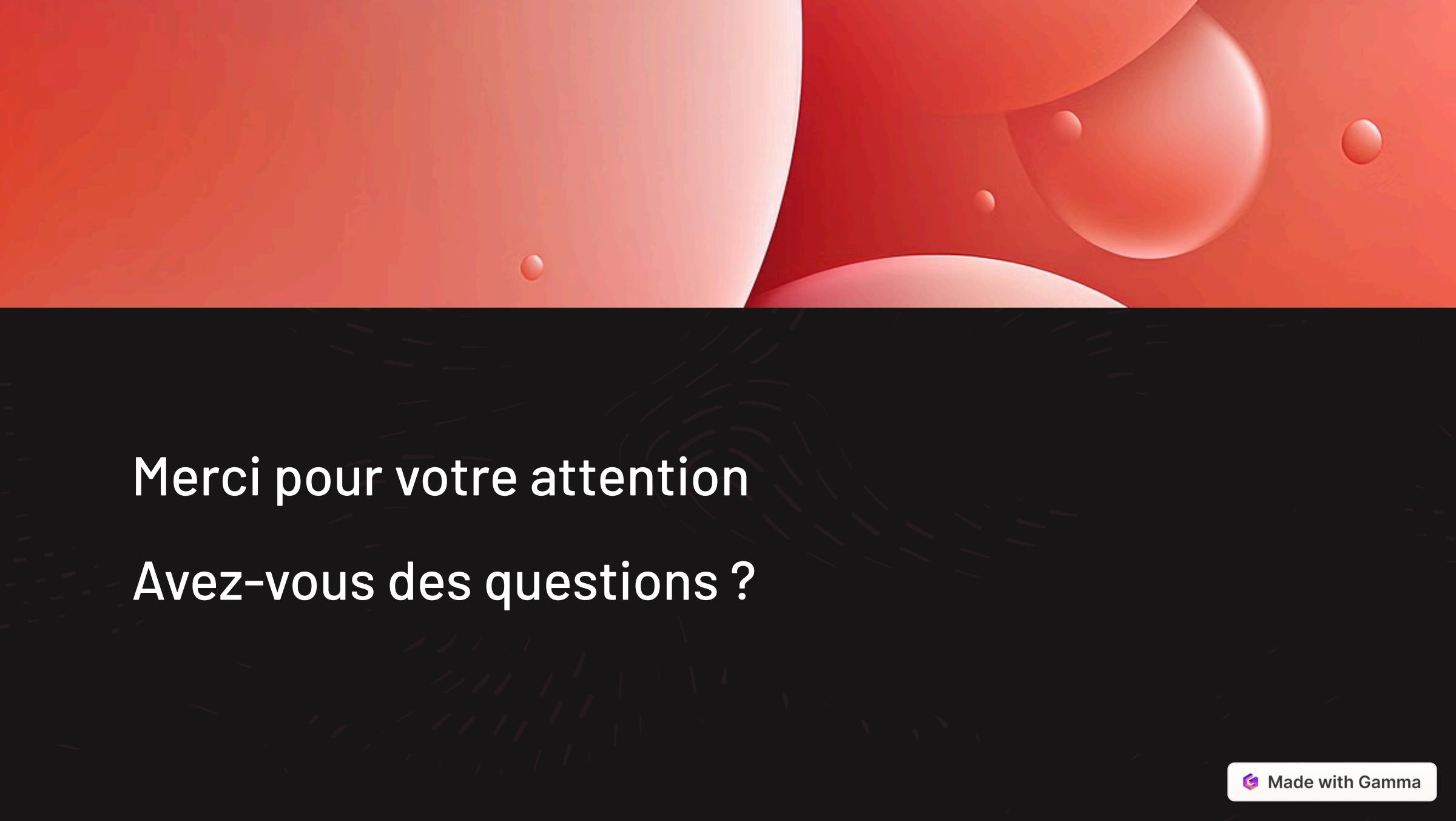
Contrôles clés :

- **Gestion des accès** : RBAC, MFA
- **Protection des données** : Chiffrement, sauvegardes régulières
- **Surveillance continue** : Audits et monitoring des systèmes
- **Conformité** aux réglementations applicables et aux normes RGPD et ISO 27002

Conclusion et Synthèse

Contrôles clés :

- **Résumé des points clés** : Vulnérabilités critiques, risques, et solutions de remédiation.
- **Importance de la sécurité continue** : Une vigilance constante est essentielle.
- **Prochaines étapes** : Implémentation des recommandations et audits futurs.



Merci pour votre attention

Avez-vous des questions ?