Titre projet –   
 Rapport d’audit…

Table of Contents

[1.1 Contexte et périmètre 5](#_Toc97903898)

[1.2 Positionnement des auditeurs 5](#_Toc97903899)

[1.3 Référentiel utilisé 5](#_Toc97903900)

[1.4 Définition des échelles 6](#_Toc97903901)

[2 Synthèse 8](#_Toc97903902)

[3 Priorisation des corrections 9](#_Toc97903903)

[4 Audit 10](#_Toc97903904)

[4.1 Identity and Access Management (IAM) 10](#_Toc97903905)

[4.1.1 Mécanisme d’authentification 10](#_Toc97903906)

[4.1.2 Modèle RBAC 10](#_Toc97903907)

[4.1.3 Utilisateur Break Glass 10](#_Toc97903908)

[4.1.4 Privileged Access Management (PAM) 10](#_Toc97903909)

[4.1.5 Monitoring des accès et de l’activité 10](#_Toc97903910)

[4.2 Infrastructure protection 10](#_Toc97903911)

[4.2.1 Networking 10](#_Toc97903912)

[4.2.2 Firewalling 10](#_Toc97903913)

[4.2.3 WAF 10](#_Toc97903914)

[4.2.4 DDoS protection 10](#_Toc97903915)

[4.2.5 Verrouillage des ressources critiques 10](#_Toc97903916)

[4.3 Data Protection 10](#_Toc97903917)

[4.3.1 Chiffrement au repos 10](#_Toc97903918)

[4.3.2 Chiffrement en transit 11](#_Toc97903919)

[4.4 Gestion des clés de chiffrement 11](#_Toc97903920)

[4.5 Gestion des certificats 11](#_Toc97903921)

[4.5.1 Workload Protection 11](#_Toc97903922)

[4.5.2 Machines Virtuelles & EC2 11](#_Toc97903923)

[4.5.3 Stratégie de backup 11](#_Toc97903924)

[4.5.4 Stratégie de Patch management 11](#_Toc97903925)

[4.5.5 Vulnerability assessment 11](#_Toc97903926)

[4.6 Surveillance et Observabilité 11](#_Toc97903927)

[4.6.1 Détection des menaces 11](#_Toc97903928)

[4.6.2 Centralisation des événements de sécurité 11](#_Toc97903929)

[4.6.3 Notification 11](#_Toc97903930)

[4.6.4 Capacité de réponse et remédiation 11](#_Toc97903931)

[4.7 Conformité 11](#_Toc97903932)

[4.7.1 Monitoring et gestion de la conformité des ressources 11](#_Toc97903933)

[5 Conclusion 13](#_Toc97903934)

[6 Annexes 14](#_Toc97903935)

[6.1 Niveau de risque 14](#_Toc97903936)

[6.2 Impact 14](#_Toc97903937)

[6.3 Vraissemblance 15](#_Toc97903938)

[6.4 Difficulté d’implémentation des corrections 15](#_Toc97903939)

Rédacteur du document

|  |  |  |
| --- | --- | --- |
| Nom | Fonction | Action |
|  |  |  |
|  |  |  |

Historique du document

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Libellé | Date | Modifications |
|  |  |  |  |
|  |  |  |  |

Contexte

## Contexte et périmètre

Dans le cadre de <nom du projet>, <le client> souhaite effectuer un audit de <périmètre de l’audit>.

L’audit a été effectué <accès, code, configuration analysées, etc…).

Le périmètre de l’audit inclut les éléments suivants :

* <élément audité>

## Positionnement des auditeurs

<Présentation du déroulé de l’audit en terme de planning, accès, interactions avec différents collaborateurs du client, contraintes, etc…>

## Référentiel utilisé

* <référentiels utilisés>

## Définition des échelles

**Le niveau de risque lié à chaque non-conformité est apprécié selon l’échelle suivante**

|  |  |
| --- | --- |
| Niveau de risque | Description |
| Mineur | Faible risque sur le système d’information et pouvant nécessiter une correction. |
| Important | Risque modéré sur le système d’information et nécessitant une correction à moyen terme. |
| Majeur | Risque majeur sur le système d’information nécessitant une correction à court terme. |
| Critique | Risque critique sur le système d’information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service. |
| Inconnu | Risque non évaluable dû à une absence ou une connaissance insuffisante du contexte client. |

**La difficulté d’implémentation correspond aux moyens humains et financiers ainsi qu’au niveau d’expertise nécessaires à la correction de la non-conformité selon nos experts.**

|  |  |
| --- | --- |
| Difficulté d’implémentation | Description |
| Facile | Correction nécessitant des compétences simples et de faibles moyens. |
| Modérée | Correction nécessitant des compétences en sécurité des systèmes d’information et des moyens relatifs. |
| Elevée | Correction nécessitant une expertise en sécurité des systèmes d’information, l’utilisation d’outils spécifiques et d’importants moyens. |
| Inconnue | Niveau d’expertise et de moyens inconnu dû à une absence ou une connaissance insuffisante du contexte client. |

# Synthèse

Durant cet audit, **X critères** ont été audités. Ci-dessous leur répartition en fonctions de l’ensemble des composants audités.

Le taux de conformité sur les critères audités est de **27 %** ; un taux <**bon, moyen, faible, relativement …>**.

Parmi les non-conformités existantes, **4** sont jugées **critiques**, soit **16 %.** Elles sont à corriger en priorité.

Ci-dessous une répartition de l’impact des vulnérabilités remontées en fonction des éléments audités.

# Priorisation des corrections

*<Schéma à adapter en fonction du contexte client, des demandes de celui-ci et du type d’audit>*

***Niveau de risque***

***Difficulté d’implémentation des corrections***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Critique |  |  |  |  |
| Majeur |  |  |  | [**A.01**](#A01) |
| Important |  |  |  |  |
| Mineur |  |  |  |  |
| Inconnu |  |  |  |  |
|  | Inconnue | Elevée | Modérée | Facile |

# Audit

## Identity and Access Management (IAM)

### Mécanisme d’authentification

### Modèle RBAC

### Utilisateur Break Glass

### Privileged Access Management (PAM)

### Monitoring des accès et de l’activité

## Infrastructure protection

### Networking

### Firewalling

### WAF

### DDoS protection

### Verrouillage des ressources critiques

## Data Protection

### Chiffrement au repos

### Chiffrement en transit

## Gestion des clés de chiffrement

## Gestion des certificats

### Workload Protection

### Machines Virtuelles & EC2

### Stratégie de backup

### Stratégie de Patch management

### Vulnerability assessment

## Surveillance et Observabilité

### Détection des menaces

### Centralisation des événements de sécurité

### Notification

### Capacité de réponse et remédiation

## Conformité

### Monitoring et gestion de la conformité des ressources

|  |  |  |  |
| --- | --- | --- | --- |
| <Critère audité> | | | |
| ID | **A.01** | | |
| Description | <description du critère> | | |
| Évaluation | **NON-CONFORME** | **Niveau de risque** | **Majeur** |
| Constat | <constat recueilli sur les systèmes ou en atelier pour attester de la non-conformité d’un critère d’audit> | | |
| Recommandations correctives | | **Difficulté d’implémentation des corrections** | |
| <plan d’actions> | | **Facile** | |

|  |  |  |  |
| --- | --- | --- | --- |
| <Critère audité> | | | |
| ID | **A.02** | | |
| Description | <description du critère> | | |
| Évaluation | **CONFORME** | **Niveau de risque** | **N/A** |
| Constat | <constat recueilli sur les systèmes ou en atelier pour attester de la non-conformité d’un critère d’audit> | | |
| Recommandations correctives | | **Difficulté d’implémentation des corrections** | |
| N/A | | **N/A** | |

# Conclusion

# Annexes

## Niveau de risque

Le niveau de risque d’une non-conformité dépend de la matrice suivante :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Critique** | **Important** | **Majeur** | **Critique** | **Critique** |
| **Majeur** | **Important** | **Important** | **Majeur** | **Majeur** |
| **Important** | **Mineur** | **Important** | **Important** | **Majeur** |
| **Mineure** | **Mineur** | **Mineur** | **Important** | **Important** |
|  | **Faible** | **Moyenne** | **Importante** | **Très importante** |

## Impact

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Niveau | Label | Financiers | Image | Juridique & réglementaire | Vie privée des utilisateurs |
| 1 | **Mineure** | Perte de <100K€ | Perte de crédibilité partielle vis-à-vis des clients | Sanction interne | Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments qu’elles surmonteront sans difficulté. |
| 2 | **Important** | Perte entre 100k€ et 500K€ | Campagne de dénigrement | Mise en demeure | Les personnes concernées pourraient connaître des désagréments significatifs qu’elles pourront surmonter malgré quelques difficultés. |
| 3 | **Majeur** | Perte entre 500k€ et 1M€ | Campagne médiatique ponctuelle mais hostile | Incidence réglementaire engageant la direction devant un tribunal administratif ou civil | Les personnes concernées pourraient connaître des conséquences significatives qu’elles devraient pouvoir surmonter mais avec des difficultés réelles et significatives. |
| 4 | **Critique** | Perte > 1M€ | Campagne médiatique hostile et durable | Incidence réglementaire engageant la direction devant un tribunal pénal | Les personnes concernées pourraient connaître des conséquences significatives voire irrémédiables qu’elles pourraient ne pas surmonter. |

## Vraissemblance

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Critique | **4** | **Très importante** | **Importante** | **Importante** | **Moyenne** |
| Importante | **3** | **Importante** | **Importante** | **Moyenne** | **Moyenne** |
| Significative | **2** | **Importante** | **Moyenne** | **Moyenne** | **Faible** |
| Faible | **1** | **Moyenne** | **Moyenne** | **Faible** | **Faible** |
| Probabilité |  | **1** | **2** | **3** | **4** |
| Moyens et compétences | | Faible | Moyenne | Importante | Très importante |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Probabilité | **Faible** | **Significative** | **Importante** | **Critique** |
| Il est rare que le risque se manifeste au cours d’une année 0% - 15% | Il est possible que le risque se manifeste au cours d’une année 15% - 40% | Il est probable que le risque se manifeste au cours d’une année 40% - 75% | Il est sûr que le risque va se manifester au cours d’une année 75% - 100% |
| Moyens et compétences | **Faible** | **Moyenne** | **Importante** | **Très importante** |
| Ne demande aucun matériel particulier et peut-être réalisé sans connaissances particulières | Demande peu de moyens et peut-être réalisés avec peu de connaissances | Demande du matériel et/ou des connaissances de base sur l'environnement cible | Demande des moyens très importants et/ou une maîtrise de l'environnement cible |

## Difficulté d’implémentation des corrections

|  |  |
| --- | --- |
| **Niveau** | **Charge** |
| **Elevée** | +15 JH |
| **Modérée** | Entre 5 et 15 JH |
| **Facile** | - 5 JH |
| **Inconnue** | Manque de contexte pour pouvoir estimer une charge |

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 325,000 team members more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

Get the Future You Want | [www.capgemini.com](https://www.capgemini.com/)



This document contains information that may be privileged   
or confidential and is the property of the Capgemini Group.

Choose an item. Copyright © 2022 Capgemini. All rights reserved.