Projet de certificat Google

Rapport d'audit cybersécurité de Botium Toys (Simulation académique)

Réalisé par :

Nada Maach

August 11, 2025

Contents

1 Périmètre et Limites

Cet audit a été réalisé exclusivement dans un cadre académique dans le cadre d'un projet de formation en cybersécurité. Il ne constitue pas un audit professionnel officiel et ne s'aligne pas intégralement avec des référentiels spécifiques (par exemple ISO 27001, NIST CSF). Le périmètre, la méthodologie et les résultats sont limités aux ressources et scénarios simulés fournis, et peuvent ne pas refléter la posture complète de sécurité de l'organisation dans un contexte réel.

2 Résumé Exécutif

Ce rapport a été préparé pour Botium Toys dans le cadre du projet de certification professionnelle Google Coursera. L'audit vise à aider l'équipe dirigeante à développer une stratégie robuste de cybersécurité en identifiant les lacunes, évaluant les contrôles existants et fournissant des recommandations opérationnelles.

Les recommandations sont catégorisées comme suit :

- **Non-Technique (NT)** – Politiques, gouvernance et sensibilisation.
- **Technique (T)** – Outils, systèmes et configurations.
- **Physique (P)** – Sécurité des locaux et matériels.

La mise en œuvre de ces recommandations renforcera la posture de sécurité de l'entreprise, réduira les risques, et assurera la conformité aux réglementations applicables telles que PCI DSS, RGPD et SOC.

3 Synthèse des Recommandations

3.1 Gouvernance et Gestion des Risques (NT)

- Assigner clairement la responsabilité de la cybersécurité à des personnes ou équipes désignées.
- Mettre en œuvre un contrôle d'accès basé sur les rôles (RBAC) avec des principes de Zero Trust et de moindre privilège afin de garantir que seuls les utilisateurs autorisés accèdent aux informations sensibles, y compris les données relatives aux cartes bancaires des clients (conformité PCI DSS, SOC).
- Appliquer la séparation des tâches (SoD) pour prévenir les fraudes et erreurs opérationnelles.
- Maintenir un registre à jour des actifs incluant matériels, logiciels, données, processus, personnes et tiers.

- Adopter une politique de classification et d'étiquetage de l'information basée sur les niveaux de sensibilité, incluant la classification des données personnelles et des informations de paiement pour soutenir la conformité RGPD et PCI DSS.
- Réaliser des évaluations formelles des risques au moins annuellement, en suivant la méthodologie ISO/IEC 27001.
- Établir un processus d'amélioration continue avec des revues régulières des politiques, risques et contrôles.

3.2 Politiques, Procédures et Sensibilisation (NT)

- Documenter toutes les politiques, procédures et instructions de travail en matière de sécurité, incluant celles spécifiques à la confidentialité des données et à la sécurité des paiements.
- Développer et appliquer une politique de gestion des systèmes hérités assurant une surveillance, maintenance et mises à jour régulières.
- Mettre en œuvre une politique formelle de gestion des changements pour contrôler les mises à jour des systèmes et logiciels.
- Fournir une formation de sensibilisation à la cybersécurité lors de l'intégration des employés et des sessions de recyclage annuelles.
- Inclure dans les formations les bonnes pratiques sur la sécurité des mots de passe, des simulations de phishing et les procédures de remontée des incidents.
- Former le personnel sur les exigences réglementaires relatives à la gestion des données clients européennes (RGPD) et des informations de paiement (PCI DSS).

3.3 Gestion des Incidents, Reprise et Continuité (T/NT)

- Maintenir et tester régulièrement un Plan de Réponse aux Incidents (PRI) définissant les rôles, chemins d'escalade et canaux de communication.
- Documenter les Plans de Reprise d'Activité (PRA) et de Continuité d'Activité (PCA), incluant :
  - Objectif de Temps de Reprise (RTO)
  - Objectif de Point de Reprise (RPO)
  - Durée Maximale Tolérable d'Interruption (MTD)

- Définir et suivre des indicateurs additionnels comme le Temps Moyen de Détection (MTTD) et le Temps Moyen de Réponse (MTTR) pour améliorer l'efficacité de la gestion des incidents.

3.4 Contrôles Techniques Clés (T)

- Mettre en œuvre et appliquer une politique de mot de passe appuyée par un système de gestion des mots de passe.
- Déployer une authentification multi-facteurs (MFA) pour les systèmes critiques et comptes sensibles.
- Établir des configurations de base sécurisées et maintenir une gestion des correctifs pour tous les systèmes.
- Chiffrer toutes les données sensibles au repos et en transit en utilisant des standards reconnus (ex. AES-256, TLS 1.3) pour protéger les données de paiement et personnelles (PCI DSS, RGPD).
- Réaliser des scans de vulnérabilités et tests d'intrusion réguliers avec des outils comme Nessus ou SolarWinds.
- Déployer et maintenir des systèmes de détection/prévention d'intrusion (IDS/IPS) intégrés aux processus de réponse aux incidents.
- Mettre en place une solution centralisée de gestion des informations et des événements de sécurité (SIEM) pour l'agrégation des logs et la détection avancée des menaces, soutenant la conformité SOC.

3.5 Gestion des Accès et des Identités (T)

- Maintenir une politique documentée de contrôle d'accès garantissant que les droits utilisateurs correspondent aux besoins métiers et aux exigences de conformité (SOC).
- Effectuer des revues périodiques des accès et révoquer rapidement les comptes inactifs ou inutilisés.

3.6 Gestion et Stockage des Données (NT/T/P)

- Mettre en œuvre une politique de rétention des données conforme aux exigences légales et métiers, précisant les durées de conservation et les méthodes de suppression sécurisée conformément au RGPD et PCI DSS.
- Appliquer des procédures de suppression sécurisée et d'élimination des dispositifs pour prévenir toute fuite de données.

- Classifier et protéger les données sensibles, y compris les données personnelles identifiables (DPI) et données personnelles sensibles (DPS), selon les exigences de confidentialité, intégrité et disponibilité.
- Maintenir un inventaire détaillé des données pour assurer le suivi précis de toutes les données personnelles et informations de paiement, facilitant la gestion des droits des personnes concernées et la conformité PCI DSS.

3.7 Sécurité Physique (P)

- Sécuriser les salles serveurs, bureaux et zones de stockage.
- Appliquer une politique de bureau et écran clair.
- Contrôler les accès visiteurs et tenir un registre des accès physiques.

3.8 Conformité Légale, Réglementaire et Tierce Partie (NT)

- Préparer la conformité au RGPD et autres réglementations applicables.
- Désigner un Délégué à la Protection des Données (DPD) ou rôle équivalent si applicable.
- Réaliser des évaluations des risques liés aux fournisseurs tiers et intégrer des exigences contractuelles de sécurité, en s'assurant que les tiers manipulant des données sensibles ou de paiement respectent les normes PCI DSS, RGPD et SOC.

4 Conclusion

En mettant en œuvre ces recommandations, Botium Toys pourra significativement améliorer sa posture de cybersécurité, renforcer sa résilience opérationnelle et maintenir la conformité avec les lois et standards applicables, notamment PCI DSS, RGPD et SOC. L'organisation devrait prioriser les actions selon la criticité des risques, la disponibilité des ressources et les échéances réglementaires, avec un suivi régulier lors des comités de gouvernance.