Botium Toys : portée et objectifs de l'audit

**Résumé :** effectuer un audit du programme de cybersécurité de Botium Toys. L'audit doit permettre d'aligner les pratiques commerciales actuelles sur les normes et les bonnes pratiques du secteur. L'audit est censé fournir des recommandations pour atténuer les vulnérabilités trouvées qui sont classées comme « à haut risque », et présenter une stratégie globale pour améliorer la posture de sécurité de l'entreprise. L'équipe d'audit doit documenter ses constatations, fournir des plans et des efforts de remédiation et communiquer avec les parties prenantes.

**Portée :** (*pour comprendre la portée de l'audit, consultez le support de cours sur l'*[*audit de sécurité*](https://www.coursera.org/learn/cyber-c2/supplement/I8hEO/security-audits)*. Notez que la portée n'est pas toujours la même d'un audit à un autre. Cependant, une fois que la portée de l'audit est clairement définie, seuls les éléments qui en font partie doivent être contrôlés. Dans ce scénario, la portée est définie comme l'ensemble du programme de sécurité de Botium Toys. Cela signifie que toutes les ressources numériques doivent être évaluées en même temps que les processus et procédures internes*).

L'audit informatique interne de Botium Toys évaluera les éléments suivants :

* Autorisations actuelles des utilisateurs dans les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outil de gestion des informations et des événements de sécurité (SIEM).
* Contrôles actuellement mis en œuvre dans les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outil de gestion des informations et des événements de sécurité (SIEM).
* Procédures et protocoles en vigueur pour les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outil de gestion des informations et des événements de sécurité (SIEM).
* Veiller à ce que les autorisations, contrôles, procédures et protocoles en place pour les utilisateurs soient conformes aux exigences de conformité nécessaires.
* Veiller à ce que les technologies actuelles soient prises en compte. Accès au matériel et au système.

**Objectifs :** (*l'objectif d'un audit correspond aux livrables ou aux résultats souhaités. L'objectif d'un audit peut être d'assurer la conformité, d'identifier les faiblesses ou les vulnérabilités d'une entreprise, et/ou de comprendre les défaillances des processus et des procédures et d'y remédier. Dans ce scénario, le responsable informatique a fixé les objectifs. Il attend un rapport sur la posture de sécurité actuelle de l'entreprise et des recommandations pour améliorer la posture de sécurité de l'entreprise, ainsi qu'une justification pour engager du personnel supplémentaire dans le domaine de la cybersécurité).*

Les objectifs de l'audit informatique interne de Botium Toys sont les suivants :

* Adhérer au cadre de cybersécurité du Institut national des normes et de la technologie (NIST CSF)
* Mettre en place un meilleur processus pour leurs systèmes afin de s'assurer qu'ils sont conformes
* Renforcer les contrôles du système
* Mettre en œuvre le concept des moindres autorisations dans le cadre de la gestion des informations d'identification des utilisateurs
* Établir leurs politiques et procédures, y compris leurs playbooks
* Veiller à ce qu'ils respectent les exigences en matière de conformité