# Objectif

L’objectif de ce document est de souligner les changements significatifs apportés au OpenHack au fil du temps.

Ajoutez une section avec la date de publication de chaque mise à jour majeure du contenu et résumez les principaux changements sous forme de liste à puces.

## Version actualisée de décembre 2021 :

Le OpenHack Serverless a été mis à jour de la manière suivante :

**IaC (Infrastructure as Code) :**

Plusieurs des défis ont été mis à jour afin de fournir un contenu bonus pour les équipes de hackers dont les membres souhaitent explorer l’infrastructure en tant que code pour le serverless.

Nous vous recommandons vivement d’effectuer cette tâche en parallèle une fois les efforts de développement accomplis pour réussir le défi principal. L’exécution séquentielle de contenu peut compromettre la capacité de l’équipe à relever le nombre minimum de défis.

Si votre équipe dispose de ressources intéressées par ce contenu bonus, veillez à encourager une collaboration continue entre ceux qui complètent le contenu du défi principal et ceux qui créent les composants d’IaC.

Les défis étant très ouverts quant à la manière dont ils sont résolus et aux ressources utilisées, il n’est pas toujours possible de disposer d’une liste prescrite de résultats attendus du matériel bonus lié à l’IaC. Vous devrez faire ce qui vous semble adéquat en ce qui concerne ces bonus. Encouragez les équipes à établir des objectifs pour le contenu IaC en fonction des solutions choisies lorsqu’elles discutent de leurs solutions.

**Conteneurs :**

Les défis du OpenHack ne prescrivent pas les composants de calcul serverless exacts à utiliser. À ce titre, les conteneurs constituent une solution viable. Il n’y a rien qui empêche ou empêchait l’utilisation des conteneurs par les hackers. Des liens de référence ont été ajoutés aux défis pour mieux aider les équipes de hackers qui souhaitent utiliser des conteneurs pour résoudre les défis.

**Défi 3 : Développer et créer un ensemble complet d’API pour répondre aux besoins de l’entreprise**

Ce défi a été mis à jour pour inclure les exigences de protection des secrets utilisés pendant le défi. Vous devrez vous assurer que les équipes de hackers utilisent les meilleures pratiques pour gérer leurs secrets tout en résolvant ce défi. Par exemple, encouragez l’utilisation de Key Vault et/ou d’identités de service managées pour la connectivité.

**Défi 4 : Déployer une couche de gestion pour les API pour surveiller et suivre vos API**

Des conseils supplémentaires ont été ajoutés à ce défi en ce qui concerne la configuration des API dans Gestion des API. Le défi est organisé de manière à ce que les hackers soient conscients de la nécessité de réfléchir à la manière dont ils vont configurer ces API pour répondre aux exigences. En tant que coach, vous devez à la fois leur permettre de trébucher sur ce point et ne pas les laisser patauger trop longtemps.

**Défi 8 : Modèles de messagerie et intégration de réseau virtuel**

Ce défi a des exigences mises à jour pour que Service Bus soit configuré pour utiliser des points d’extrémité privés afin de garantir que seul le trafic acheminé par le réseau virtuel est utilisé. Le réseau virtuel a été doté des sous-réseaux nécessaires à cette fin. Les hackers devront s’assurer qu’ils configurent Service Bus avec le point d’extrémité privé approprié, ainsi que les fonctions de publication et d’abonnement de manière appropriée.