Rapport de Projet

Module : Introduction to Cloud and Cloud Security

Nom et Prénom : Bensefia Walid
Spécialité : Data Science & Intelligence Artificielle

15/06/2023

Contents

1 Task 01 : construction de la fonction Lambda

1.1 Fonction Lambda

Ce code représente une fonction Lambda qui envoie un message à un canal Slack lorsqu'une découverte GuardDuty est détectée. Voici une explication détaillée du code:

1. **Les imports:** Le code importe les modules nécessaires, notamment `json` pour traiter les données JSON, `os` pour accéder aux variables d'environnement, et `WebhookClient` de la bibliothèque `slack_sdk.webhook` pour envoyer des messages à Slack via un webhook.

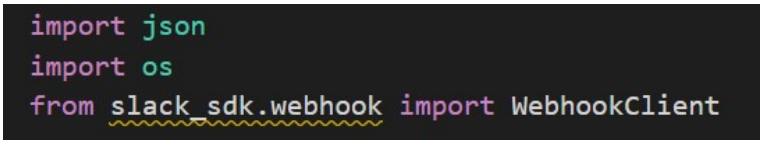

Figure 1: Imports

2. **Les variables d'environnement:** Le code récupère les URL du webhook Slack (`SLACK_WEBHOOK_URL`) et le nom du canal Slack (`SLACK_CHANNEL`) à partir des variables d'environnement de la fonction Lambda.

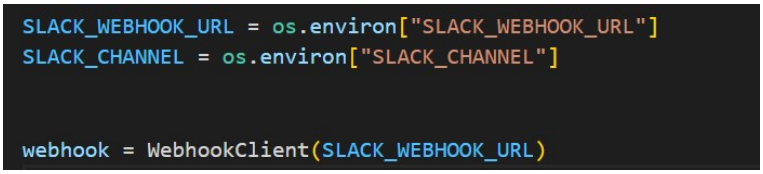

Figure 2: Variables d'environnement

3. **La fonction send_slack_message:** Cette fonction construit un message de notification Slack à partir des paramètres passés en tant qu'arguments kwargs. Les paramètres sont utilisés pour remplir les détails spécifiques de la découverte GuardDuty dans les blocs du message Slack. Les blocs sont ensuite envoyés à Slack à l'aide du webhook.

Figure 3: Fonction SendSlackMessage

4. **La fonction lambda_handler:** Cette fonction est l'entrée principale de la fonction Lambda. Elle est appelée lorsque la fonction Lambda est déclenchée par un événement, comme une notification SNS. Le code extrait les informations nécessaires de l'événement, telles que l'ID du compte, la région, le type de découverte, le type d'utilisateur, le nom d'utilisateur, la description et la gravité. Ces informations sont ensuite passées à la fonction `send_slack_message` pour envoyer le message à Slack

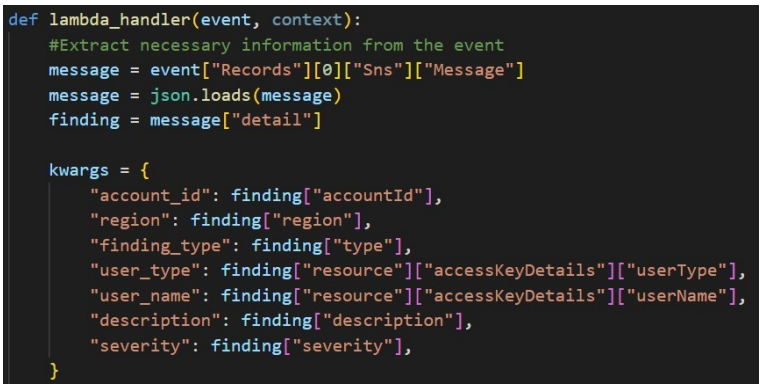

Figure 4: Fonction LambdaHandler

5. **La réponse de la fonction:** Une fois le message envoyé à Slack, la fonction renvoie un dictionnaire JSON contenant le code d'état HTTP 200 et le corps de la réponse "message sent !".

Figure 5: Réponse de la fonction

1.2 Configuration d'un evenement de test

En utilisant le GradDuty Finding sample que vous nous avez fourni :

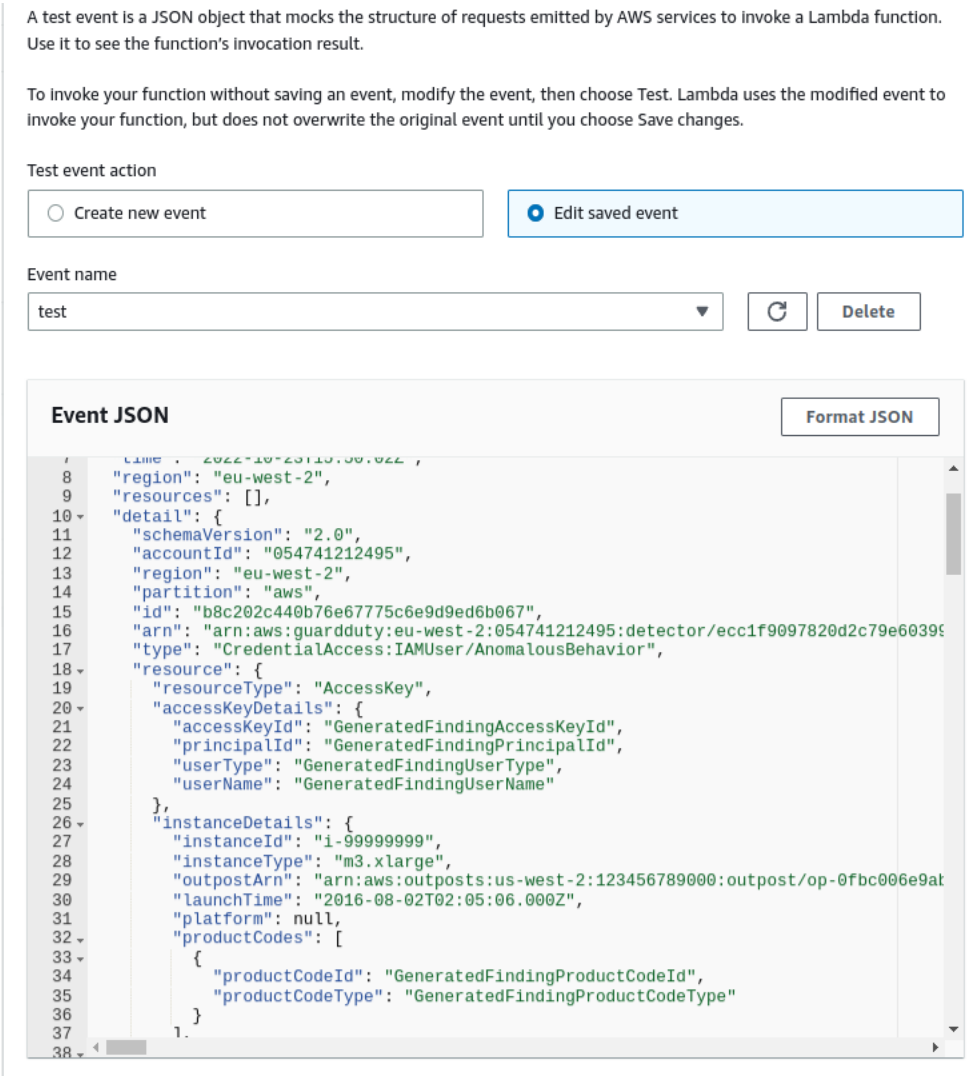

Figure 6: Configuration d'un évènement de test

Ce code va générer des *Findings*, qui seront envoyés au canal Slack de notre groupe.

2 Task 02 : Remédier à un *Finding*

2.0.1 Compréhension du Finding :

Voici l'un des **Findings** dont nous avons été notifié sur notre canal Slack :

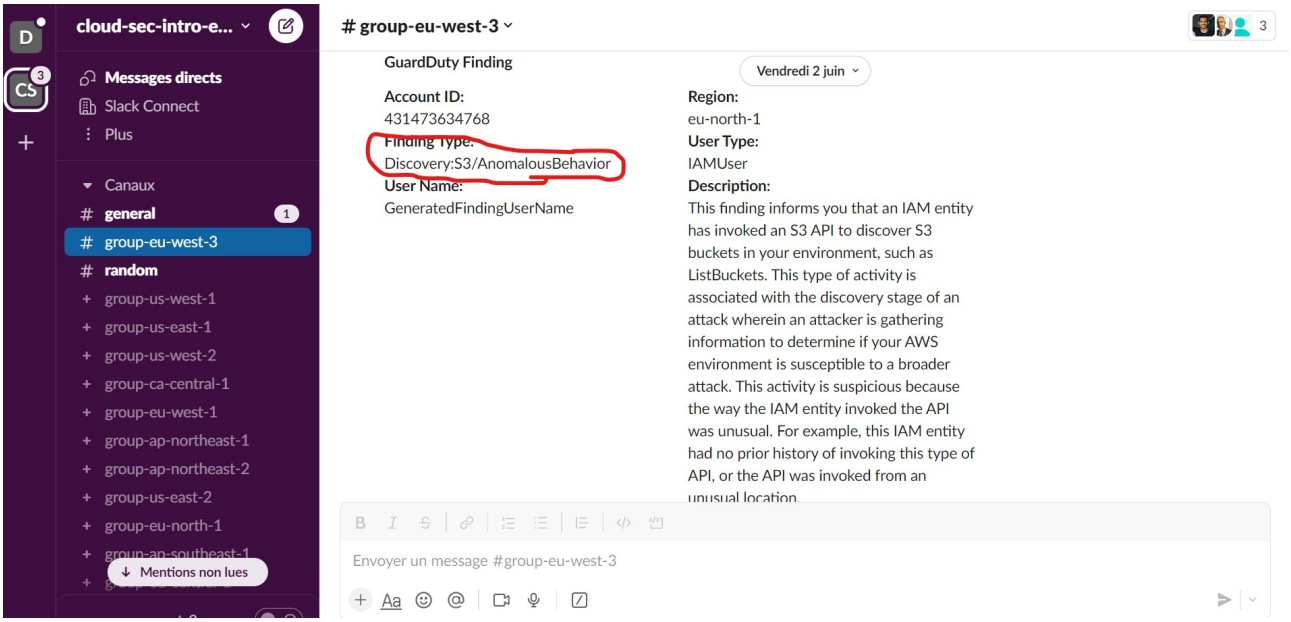

Figure 7: Exemple de *GuardDuty Finding*

Finding Type : Discovery:S3/AnomalousBehavior

Ce résultat indique qu'une entité IAM a invoqué une API S3 de manière anormale pour découvrir des objets S3 dans mon environnement, telle que ListObjects. Cette activité est associée à l'étape de découverte d'une attaque, dans laquelle un attaquant recueille des informations pour déterminer si mon environnement AWS est susceptible d'être la cible d'une attaque plus large. Cette activité est suspecte car l'entité IAM a invoqué l'API d'une manière inhabituelle. Par exemple, une entité IAM sans historique antérieur invoque une API S3, ou une entité IAM invoque une API S3 à partir d'un emplacement inhabituel.

Ce type d'API a été identifié comme anormal par le modèle d'apprentissage automatique (ML) de détection d'anomalies de GuardDuty. Le modèle ML évalue toutes les demandes d'API dans mon compte et identifie les événements anormaux associés aux techniques utilisées par les adversaires. Il analyse divers facteurs des demandes d'API, tels que l'utilisateur qui a effectué la demande, l'emplacement à partir duquel la demande a été faite, l'API spécifique demandée, le bucket demandé et le nombre d'appels API effectués.

2.0.2 Remédiation recommandées :

Pour remédier à un compartiment Amazon S3 compromis dans mon environnement AWS, voici les étapes recommandées :

1. Identifier la ressource S3 concernée : À partir des résultats de GuardDuty, je peux repérer le compartiment S3 concerné en vérifiant son nom, son ARN (Amazon Resource Name) et son propriétaire, qui sont fournis dans les détails du résultat.

2. Identifier la source de l'activité suspecte et l'appel API utilisé : Les détails du résultat de GuardDuty fournissent des informations sur la source de l'activité suspecte, qu'il s'agisse d'un rôle IAM, d'un utilisateur ou d'un compte. J'identifie également l'appel API utilisé. Des détails supplémentaires tels que l'adresse IP distante ou les informations de domaine source peuvent être disponibles pour évaluer si la source était autorisée.

3. Déterminer si l'appel API provenait d'une source autorisée à accéder à la ressource identifiée : Selon le type de source, je m'interroge sur les points suivants :

    - Si un utilisateur IAM était impliqué, je considère la possibilité que ses informations d'identification aient été compromises.
    - Si un API a été invoqué par une source sans historique préalable d'utilisation de ce type d'API, j'évalue si cette source a réellement besoin d'autorisations pour cette opération et si les permissions du compartiment S3 peuvent être encore restreintes.
    - Si l'accès a été effectué par le nom d'utilisateur ANONYMOUS_PRINCIPAL et le type d'utilisateur AWSAccount, cela indique que le compartiment est public. Je revois alors les recommandations de sécurité pour trouver des solutions alternatives pour le partage des ressources S3.
    - Si l'accès a été effectué par un appel PreflightRequest réussi avec le nom d'utilisateur ANONYMOUS_PRINCIPAL et le type d'utilisateur AWSAccount, cela indique que le compartiment a une politique de partage de ressources entre origines (CORS) configurée. Je m'assure que cette politique est intentionnelle et je revois les recommandations de sécurité pour le partage des ressources S3.

4. Déterminer si le compartiment S3 contient des données sensibles : J'utilise Amazon Macie pour déterminer si le compartiment S3 contient des données sensibles, telles que des informations personnellement identifiables (PII), des données financières ou des informations d'identification. Je peux activer la découverte automatique des données sensibles pour mon compte Macie et examiner les détails du compartiment S3 pour mieux comprendre son contenu. Alternativement, je peux créer et exécuter une tâche de découverte de données sensibles pour inspecter les objets du compartiment S3.

5. Si l'accès était autorisé, je peux ignorer le résultat