

Documentation : Créer un véritable honeypot avec GitGuardian et GitHub

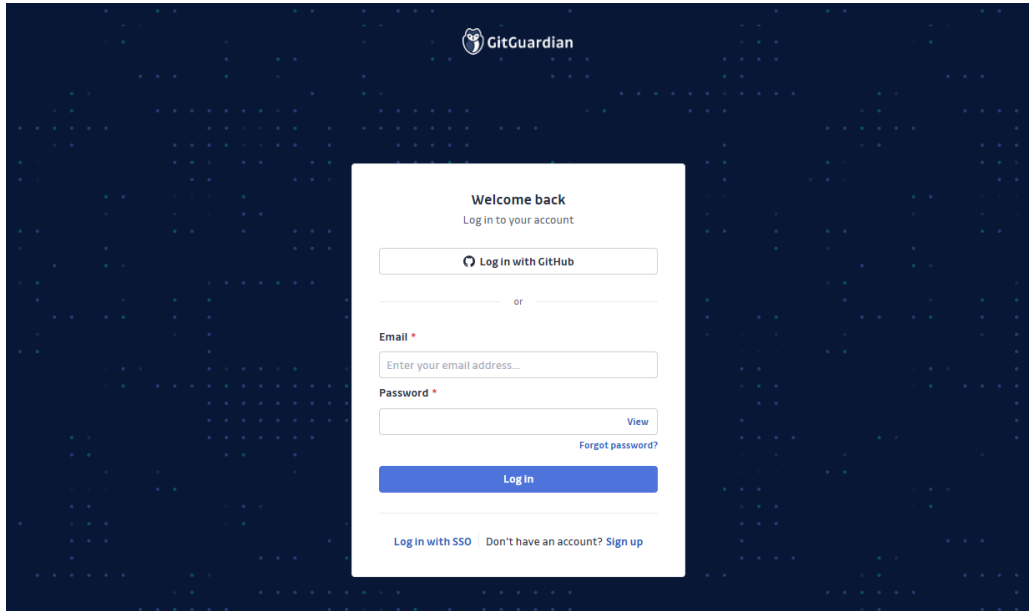
Objectif

Simuler une fuite de clé AWS dans un dépôt GitHub public en utilisant un **honeypot** **GitGuardian**, afin d'observer les réactions des bots et attaquants automatisés.



Étape 1 : Créer un compte GitGuardian

1. Rendez-vous sur <https://dashboard.gitguardian.com>
2. Créez un compte gratuit ou connectez-vous avec votre compte GitHub.



- Une fois connecté, GitGuardian commencera automatiquement à surveiller vos dépôts publics si l'intégration GitHub est activée.

The screenshot shows the 'Internal sources' page in the IAMSecuritec interface. The central table lists six sources, all with a 'Safe' status. The right panel provides a summary of protection metrics: 6 sources integrated, 100% real-time monitoring, 0% sources with honeytokens, and 100% historical scanning success. Below this, it shows details for 0 GitHub organizations and 1 GitHub user with 6 repositories (2 private, 4 public).

Source	Health	INC
iamsecuritec/antoniofos88	Safe	-
iamsecuritec/portfolio	Safe	-
iamsecuritec/azure-ad-demo-public	Safe	-
iamsecuritec/iamsecuritec.github.io	Safe	-
iamsecuritec/zero-trust-sharepoint-app	Safe	-
iamsecuritec/entra-app-security-dashboard	Safe	-

Étape 2 : Créer un honeytoken

- Cliquez sur **Honeytokens** dans le menu latéral.
- Cliquez sur **"Create Honeytoken"**.

The screenshot shows the 'Honeytokens' page. A yellow box highlights the '+ Create honeytoken' button in the top right corner. Another yellow box highlights the table of existing honeytokens, which shows two entries: 'secret-prod-de...' and 'Mysiteweb-de...'. Both are in a 'Revoked' status.

HONEYTOKEN	SOURCE	TAGS	CREATED AT	TRIGGERED AT	STATUS
secret-prod-de... #9e9055e9	iamsecuritec/azure...	.env	Jul 16th, 2025 21:55	—	Revoked
Mysiteweb-de... #15481814	iamsecuritec/azure...	Publicly exposed	Jul 16th, 2025 19:57	Jul 16th, 2025 20:22	Revoked

3. Donnez un nom et une description à votre token (ex. : aws-dev-key-test).
4. Cliquez sur **“Create”**.

Create my honeypot ✕

AWS key ▾

Currently we support only AWS keys. Please [let us know](#) if you would like to see other types of honeypots.

Name *

Honeypot name

Description

Write description note here

Tags

+ Add tag ▾

Cancel **Create my honeypot**

5. GitGuardian générera une fausse clé AWS sous forme de :
6. `AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE`
`AWS_SECRET_ACCESS_KEY=gg-honey-xxxxxxxxxxxxxxxxxxxxxxxxxx`

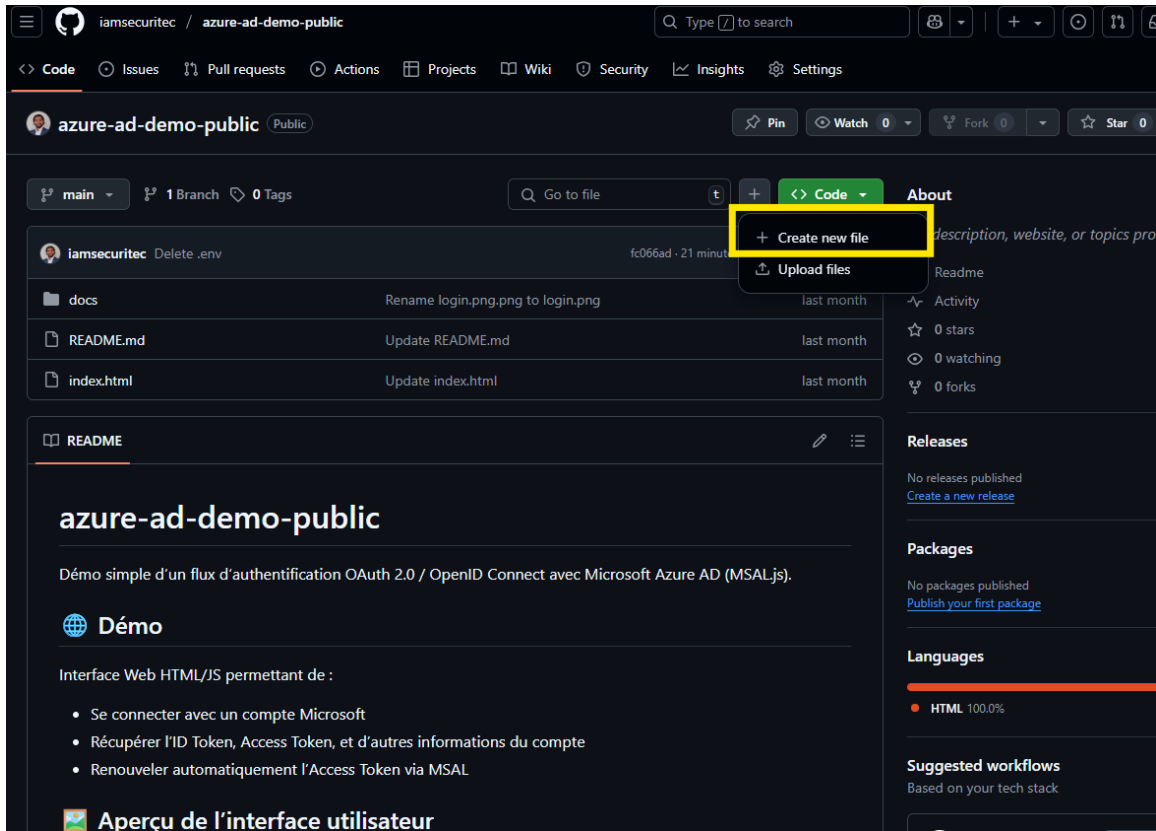
The screenshot displays the iamsecuritec Honeytokens interface. On the left is a dark sidebar with navigation options: 'Get started', 'Monitored perimeter', 'Internal sources', 'Internal monitoring', 'Internal secret incidents', 'Analytics', 'Honeytoken', and 'Honeytokens' (selected). The main content area shows details for a honeytoken named 'secret-prod-demo-auth' (ID: #9e9055e9-e78c-48a1-a5c9-023628334aec). The 'Key' section contains the following AWS credentials:

```
aws_access_key_id = AKIA34UWIKTBPNB0756
aws_secret_access_key = XaiQUTo1kDmgndw6c06jId3tAdP8+TaVh1UK1m53
```

Below the key, it shows 'Created by: Antonio Ferreira' and 'Created on: July 16th, 2025 21:55'. The 'Description' is 'Demo fluxo d'authentification OpendID'. The 'Sources' section lists one source: 'iamsecuritec/azure-ad-demo-public' with '0 open secret incidents' and a '.env' file.

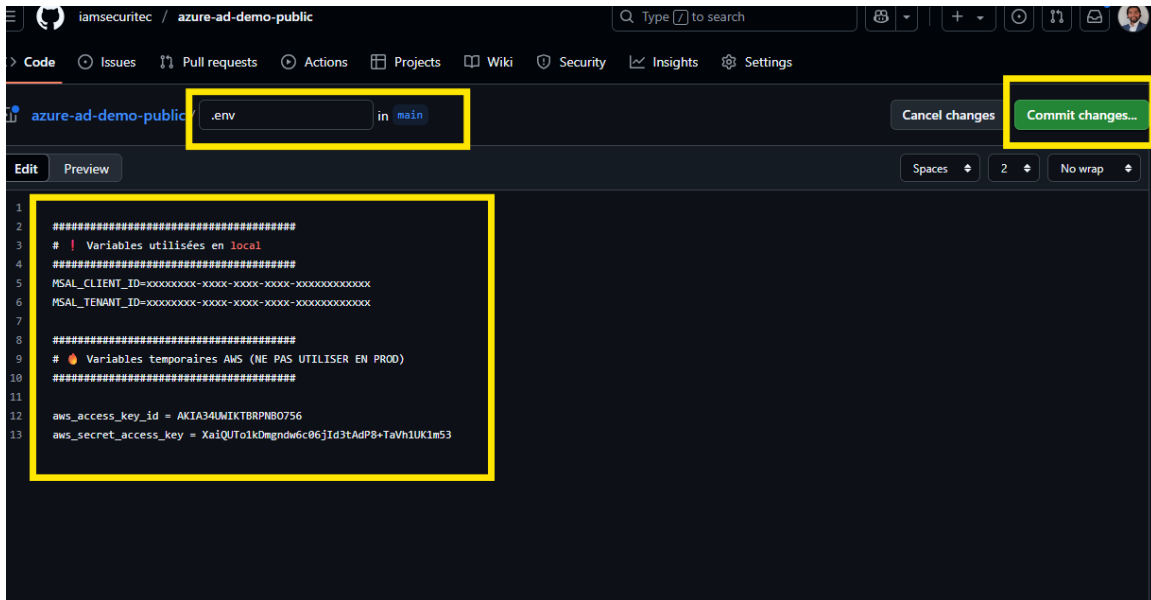
Étape 3 : Injecter le honeypot dans un dépôt GitHub

1. Créez un **vrai dépôt public** sur GitHub (ou utilisez un existant).
Exemple : <https://github.com/iamsecuritec/azure-ad-demo-public>
2. Créez un fichier `.env`



3. Collez le contenu du honeypot en le rendant crédible :
4. Faites un commit :

Astuce : ajoutez un commentaire dans le fichier pour tromper les bots, comme “clé temporaire pour test S3”.



The screenshot shows the GitHub web interface for the repository 'iamsecuritec / azure-ad-demo-public'. The file '.env' is selected for commit in the 'main' branch. The 'Commit changes...' button is highlighted in green. The file content is as follows:

```
1 #####
2 # | Variables utilisées en local
3 #####
4 MSAL_CLIENT_ID=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
5 MSAL_TENANT_ID=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
6
7
8 #####
9 # 🟡 Variables temporaires AKS (NE PAS UTILISER EN PROD)
10 #####
11
12 aws_access_key_id = AKIA34LWIKTBPRNB0756
13 aws_secret_access_key = XaiQUTo1kDmgndw6c06jId3tAdP8+TaVh1UK1m53
```

Étape 4 : Surveillance par GitGuardian

Dès que le dépôt est mis à jour, GitGuardian commence à le surveiller.








Si un acteur externe tente d'utiliser la clé, une **alerte immédiate** sera déclenchée avec :










- IP de l'attaquant
- Pays d'origine
- Outil utilisé (user-agent)
- Appel AWS effectué

100 results / 100 Display 10 results ▾

TIMESTAMP ▾	IP ADDRESS ▾	IP RULES ▾	USER AGENT ▾	ACTION ▾
Jul 16th 22:07	54.39.190.134	GitGuardian Public Monitoring IP	python-requests/2.32.4	GetCallerIdentity
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans
Jul 16th 22:06	104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListBackupPlans

1-10 of 100 < 1 2 3 ... 10 >

Status	is	open	x	+
100 results / 100 Display 10 results ▾				
TIMESTAMP ▾	IP ADDRESS ▾	IP RULES	USER AGENT ▾	ACTION ▾
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListSecrets
Jul 16th 22:06	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListDomainNames
21-30 of 100 < 1 2 3 ... 10 >				

Status	is	open	x	+
100 results / 100 Display 10 results ▾				
TIMESTAMP ▾	IP ADDRESS ▾	IP RULES	USER AGENT ▾	ACTION ▾
Jul 16th 22:04	 104.250.131.250		Boto3/1.34.46 md/Botocore#1.34.46 ua/2.0 os/linux#6.8.0-62-generic md/arch#x86_64 lang/python#3.12.3...	ListServiceQuotas
Jul 16th 22:04	 104.250.131.250		TruffleHog	GetCallerIdentity
Jul 16th 22:03	 54.39.190.134	GitGuardian Public Monitoring IP	python-requests/2.32.4	GetCallerIdentity
Jul 16th 22:03	 135.235.174.25		[mint/1.6.2]	ListBuckets
Jul 16th 22:03	 135.235.174.25		mint/1.6.2	ListHostedZones
Jul 16th 22:03	 135.235.174.25		mint/1.6.2	ListUsers
Jul 16th 22:03	 135.235.174.25		mint/1.6.2	DescribeOrganization
Jul 16th 22:03	 135.235.174.25		mint/1.6.2	GetCallerIdentity
Jul 16th 22:03	 54.39.182.0	GitGuardian Public Monitoring IP	python-requests/2.32.4	GetCallerIdentity
Jul 16th 21:58		AWS Internal IP	AWS Internal	AttachUserPolicy
91-100 of 100 < 1 ... 8 9 10 >				

Exemple de résultats

En moins de **21 minutes**, plus de **100 événements** ont été déclenchés.

Events

▲ This honeytoken has received more than 100 open events. For performance reasons, event reception for this honeytoken is paused. [Learn more](#)

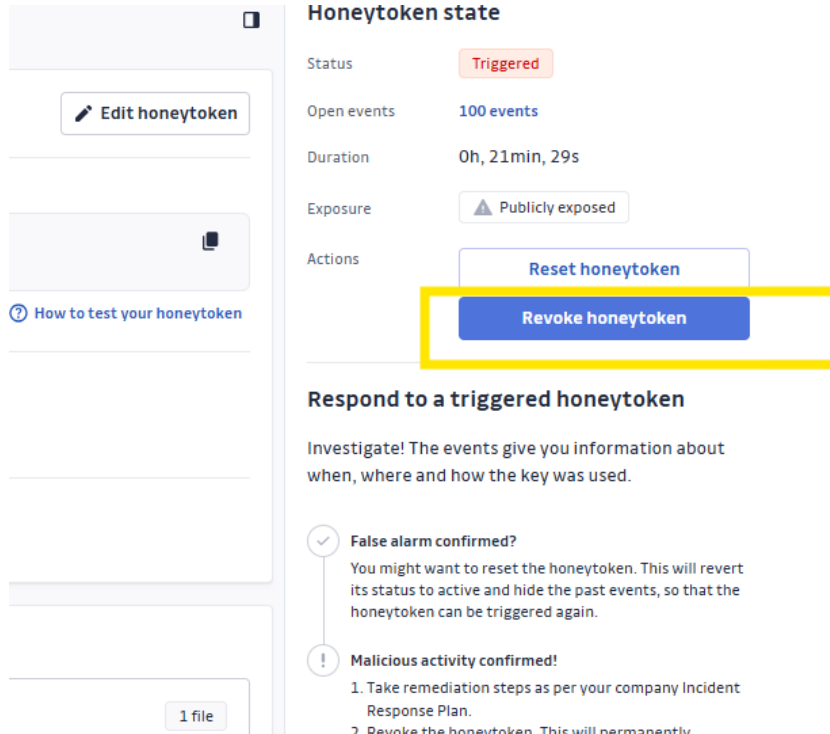
Exemples d'attaques :

Action	Nom de l'action	Signification
GetCallerIdentity	Obtenir l'identité de l'appelant	Vérifie si la clé AWS est valide et identifie l'utilisateur IAM ou le compte AWS associé
ListBackupPlans	Lister les plans de sauvegarde	Recherche les plans dans AWS Backup, pour cibler des données à restaurer ou supprimer
ListSecrets	Lister les secrets	Tente de découvrir les domaines OpenSearch/Elasticsearch disponibles dans le compte AWS
ListDomainNames	Lister les noms de domaine	Enumère tous les utilisateurs du compte AWS pour préparer une escalade de privilèges
ListServiceQuotas	Lister les quotas de service	Permet de voir les limites d'utilisation pour chaque service AWS (utile pour cartographier l'environnement)
ListBuckets	Lister les buckets S3	Enumère tous les buckets de stockage S3, souvent pour préparer l'exfiltration de données
DescribeOrganization	Décrire l'organisation AWS	Fournit des infos sur l'organisation AWS (si AWS Organizations est activé), y compris le compte root
AttachUserPolicy	Attacher une politique à un user	Tente d'accorder plus de privilèges à un utilisateur IAM en attachant une politique
ListUsers	Lister les utilisateurs IAM	Enumère tous les utilisateurs du compte AWS pour préparer une escalade de privilèges

Étape 5 : Clôturer le test

Révoquer le honeypot :

Dans GitGuardian, sélectionnez le token → cliquez sur **Revoke**



Honeypot state

Status **Triggered**

Open events **100 events**

Duration **0h, 21min, 29s**

Exposure **Publicly exposed**

Actions

[Reset honeypot](#)

[Revoke honeypot](#)

Respond to a triggered honeypot

Investigate! The events give you information about when, where and how the key was used.

✓ **False alarm confirmed?**
You might want to reset the honeypot. This will revert its status to active and hide the past events, so that the honeypot can be triggered again.

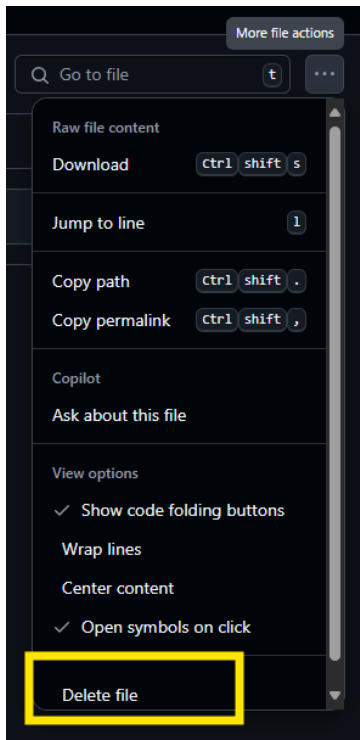
! **Malicious activity confirmed!**

1. Take remediation steps as per your company Incident Response Plan.
2. Revoke the honeypot. This will permanently...

1 file

Nettoyer le dépôt :

- Supprimez le fichier .env ou remplacez le contenu par un place Holder
- Optionnel : réécrire l'historique Git si nécessaire



Conclusion

Ce test démontre qu'un **secret exposé même quelques minutes** peut être :

- Vu
- Testé
- Exploité
par des acteurs automatisés du monde entier.

Utiliser des honeytokens est une excellente stratégie pour :

- Surveiller des fuites
- Former vos équipes
- Tester vos alertes sécurité