

# Cloud DFIR class

## Detection\_evasion

Author : Siwoo Park (박시우)

Mentor : Niko

Track : Digital Forensic

Date : 2024/08/13

## Content

1. Summary .....	1
2. Progress.....	1
2.1 environment setup .....	1

## 1. Summary

This assignment focuses on researching DFIR (Digital Forensics and Incident Response) in cloud environments, The task involves using CloudGoat to set up a practical environment, deploying a specific scenario, and achieving the scenario's objectives.

Cloudgoat is a tool designed to simulate cloud security incidents, allowing users to practice responding to various cases that might occur in cloud systems.

My assigned part is detection evasion, where the goal is to perform specific actions in the cloud while avoiding detection.

This document is for check progress about assignment.

## 2. Progress

### 2.1 environment setup

First, install AWS CLI and Cloudgoat, and configure them to link with my AWS account.

사용자 (5) 정보

🔄

삭제

사용자 생성

IAM 사용자는 계정에서 AWS와 상호 작용하는 데 사용되는 장기 자격 증명을 가진 자격 증명입니다.

🔍 검색

<

1

>

⚙️

<input type="checkbox"/>	사용자 이름 ▲	경로 ▼	그룹 ▼	마지막 활동 ▼	MFA ▼	암호 수명
<input type="checkbox"/>	Bo[REDACTED]	/	0	🟢 1시간 전	-	🟢 1시간
<input type="checkbox"/>	canarytok[REDACTED]	/	0	-	-	-
<input type="checkbox"/>	cd1fe[REDACTED]	/	0	-	-	-
<input type="checkbox"/>	Is[REDACTED]	/SpaceCrab/	0	-	-	-
<input type="checkbox"/>	[REDACTED]	/	1	-	-	-

```

$ cat start.txt
Alert_Location = [REDACTED]
Start_Note = You are given 4 pairs of credentials to start this scenario. Surely some of the
m are traps...
cloudgoat_output_aws_account_id = 6[REDACTED]
scenario_cg_id = detect[REDACTED]
user1_access_key_id = AKIA7023[REDACTED]
user1_secret_key = WND[REDACTED]
user2_access_key_id = AKIA[REDACTED]
user2_secret_key = AHXYbg40[REDACTED]
user3_access_key_id = AKIA[REDACTED]
user3_secret_key = w3mpcAV[REDACTED]
user4_access_key_id = AKIA[REDACTED]
user4_secret_key = 87[REDACTED]

```

The cloud environment setup has been completed, and four accounts necessary for the exercise have been created as indicated in the `start.txt` file.

Now, using this account information, the next step is to achieve the objectives outlined in the scenario.

This is the current progress in my task.