

Scenario1

- 1) VPC Flow logs
- 2) Yes
- 3) Input transformer

Scenario 2:


1. CloudTrail
2. Compromised user policy / inline policy

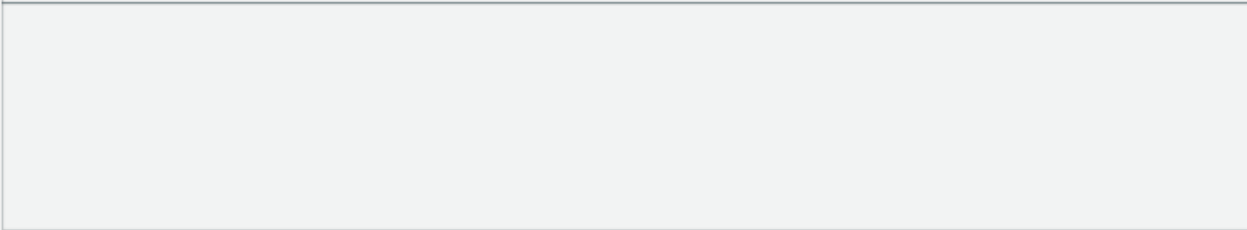
The screenshot shows the AWS IAM console interface for a user's permissions. At the top, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is selected, showing a section for 'Permissions policies (1 policy applied)'. Below this, there is a table with columns for 'Policy name' and 'Policy type'. The table contains one entry: 'CompromisedUserPolicy' with a policy type of 'Inline policy'. Below the table, there is a section for 'Generate policy based on CloudTrail events' with a 'Generate policy' button. The text below the button states: 'No requests to generate a policy in the past 7 days.'

3. To analyze the previous activity of this user to better understand the scope of the compromise

Scenario 3

- 1) Since it is manual, It could take quite a long time to identify the actual issue and might sabotage the workflow of entire system.
- 2) The instance with instance id “i-06b36902e41cac650” is the only one with the IAM role : GuardDuty-Example-EC2-Compromised

	Name	Instance ID
<input type="checkbox"/>	GuardDuty-Example: Malicious Instance: Scenario 1 & 2	i-0321c71005a0750bf
<input type="checkbox"/>	GuardDuty-Example: Compromised Instance: Scenario 1	i-0d0dda14d7d6653a8
<input type="checkbox"/>	GuardDuty-Example: Malicious Instance: Scenario 4	i-08e0ae3be197f0410
<input checked="" type="checkbox"/>	GuardDuty-Example: Compromised Instance: Scenario 3	i-06b36902e41cac650



Instance: [i-06b36902e41cac650](#) (GuardDuty-Example: Compromised Instance: Scenario 3)

Answer private resource DNS name

–

Auto-assigned IP address

 [35.162.23.8](#) [Public IP]

IAM Role

 [GuardDuty-Example-EC2-Compromised](#) 

Instance type

t3.micro

VPC ID

 [vpc-029904510140c88](#)

Subnet ID

 [subnet-079ca4480808t](#)