TRAILDISCOVER

3 CLOUDTRAIL EVENTS THAT COULD SIGNAL **PERSISTENCE**!

traildiscover.cloud

TRAILDISCOVER

CREATEUSER

What It Means:

The **CreateUser** event logs the creation of a new IAM user in your AWS account.

Why This Event Matters During an Attack:
This is the most commonly used technique by attackers to gain persistence. After initial access, attackers create new IAM accounts to ensure they can re-enter the environment. Sometimes, they use names that resemble legitimate services or tools, making it harder to detect.

TRAILDISCOVER

What It Means:
The **CreateAccessKey** event logs the creation of access keys for an IAM user.

Why This Event Matters During an Attack:
Attackers often create access keys to persist via programmatic access, bypassing login requirements. These keys can be created either for new IAM users created by the attackers or for existing users.

CREATEACCESSKEY

CREATELOGINPROFILE

What It Means:
The **CreateLoginProfile** event logs the creation of a password-based login profile for an IAM user.

Why This Event Matters During an Attack:
Creation of new access keys isn't always possible, as users may already have two active keys, and in some environments, key creation is controlled. Attackers may instead create a login profile by supplying a password. This allows them to access the environment via the AWS console without creating additional disruption.

TRAILDISCOVER