Abusing the Replicator

Silently Replicating Data with the S3 Replication Service

Kat Traxler – Vectra AI

About Me

Kat Traxler

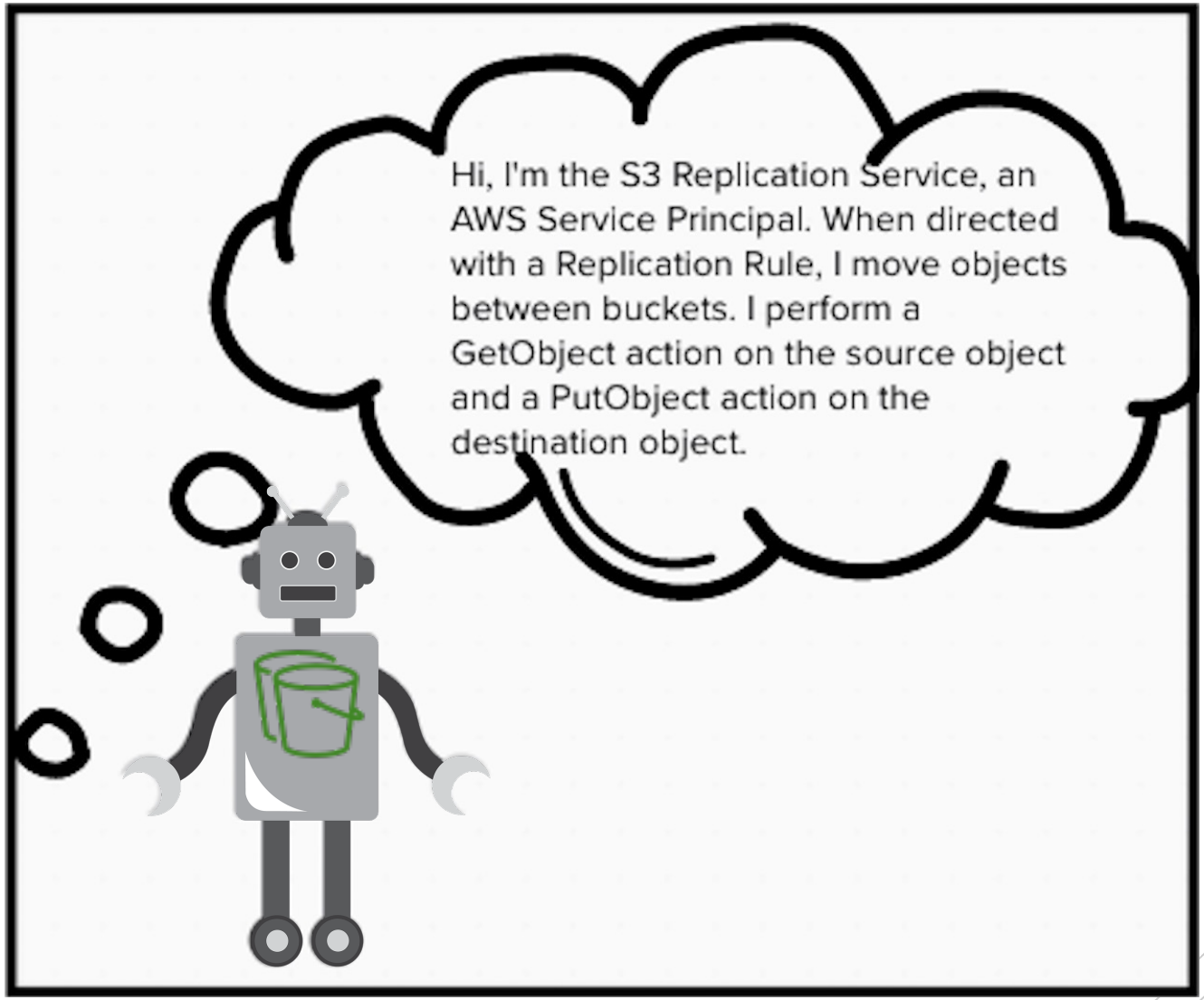
- Principal Cloud Security Researcher – Vectra AI
- SANS SEC549 Enterprise Cloud Security Architecture Author
- Public speaker on AWS, GCP threats
- Avid gardener, dog mom and yogi

S3 Replication Service

For Good, For Evil, For Confounding Defenders

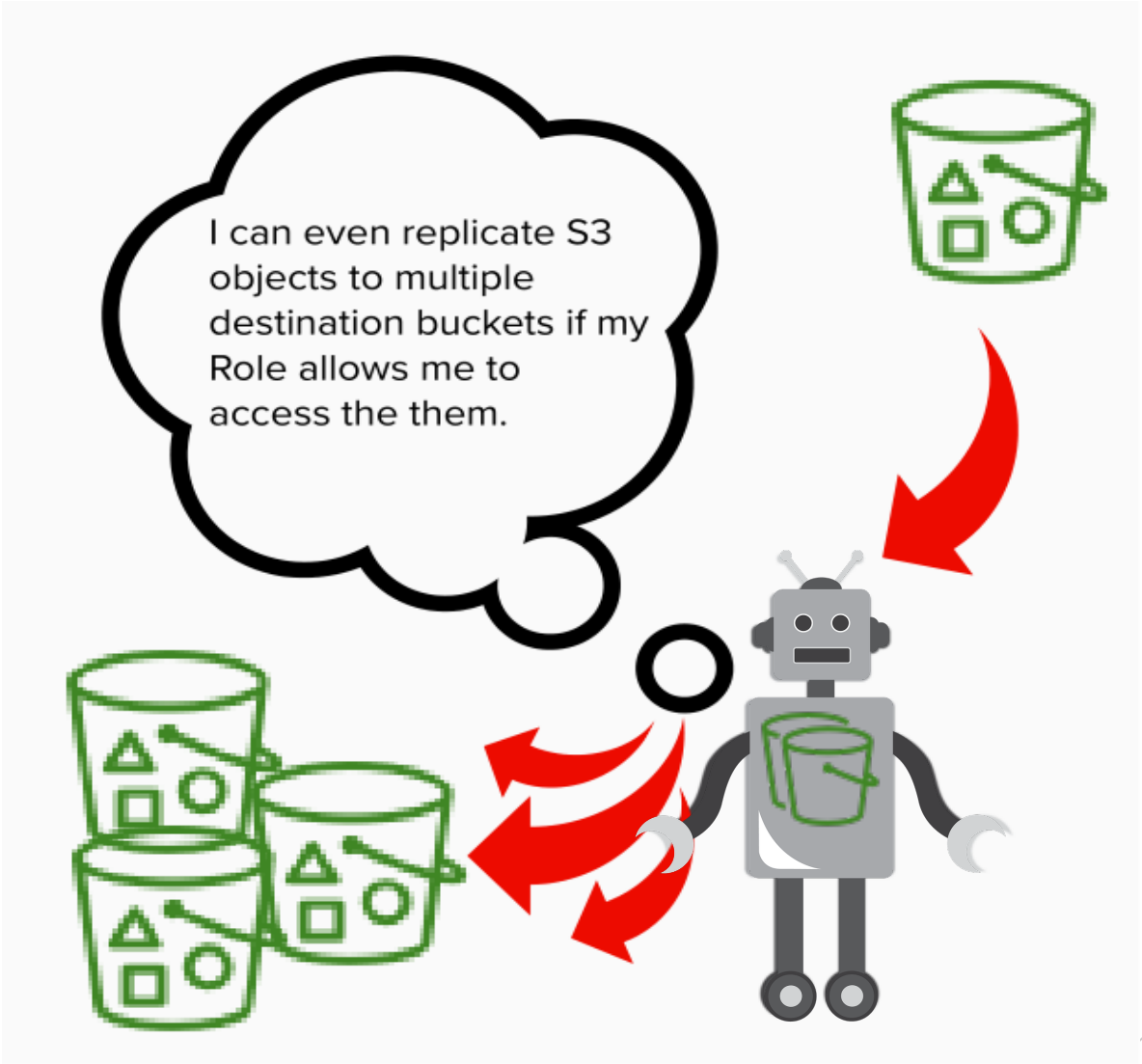
S3 Replication Service - Intro

The Replication Service, like the 'hand-of-god', moves objects between buckets



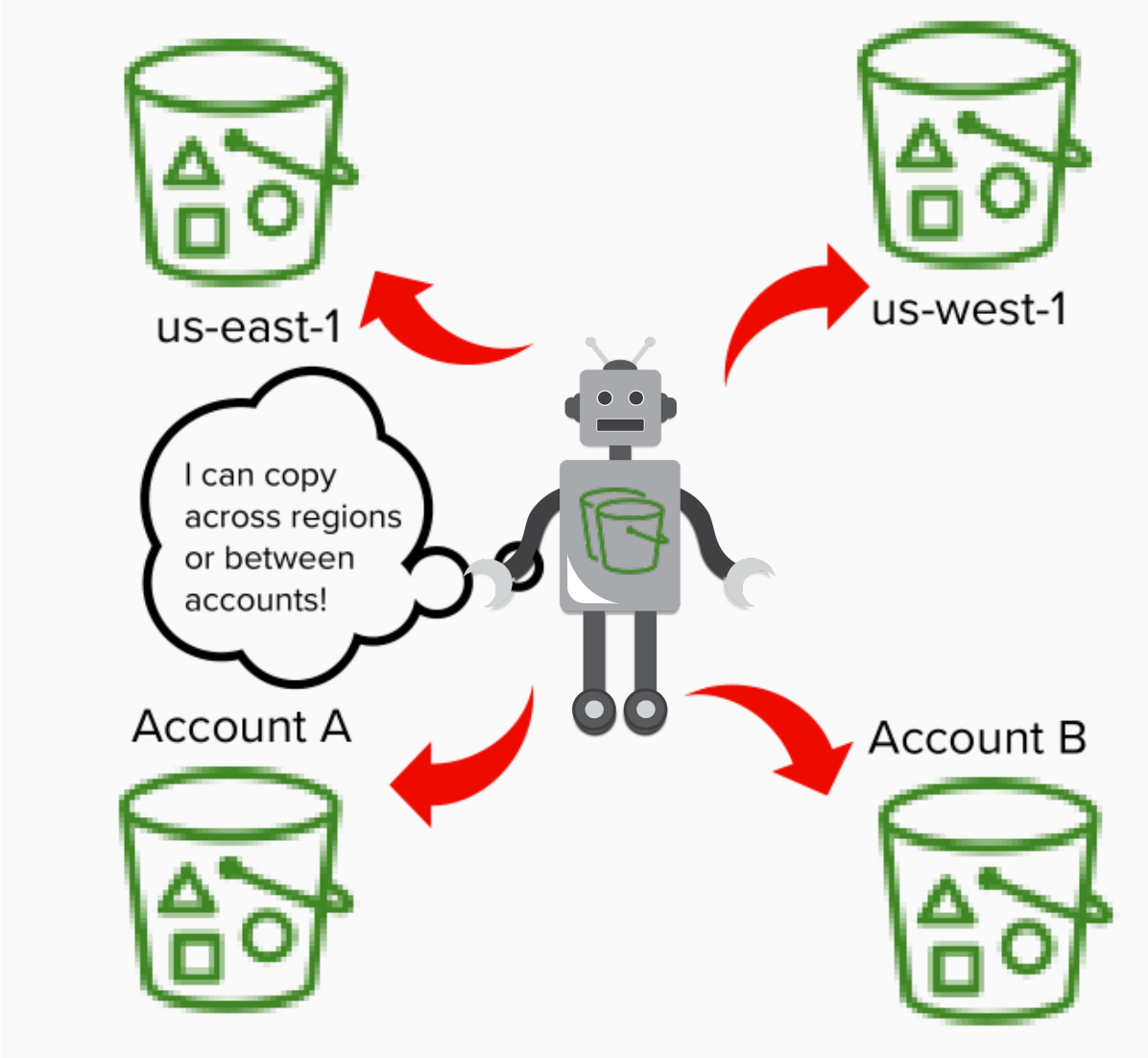
S3 Replication Service - Intro

The Service can replicate to multiple destinations if directed!



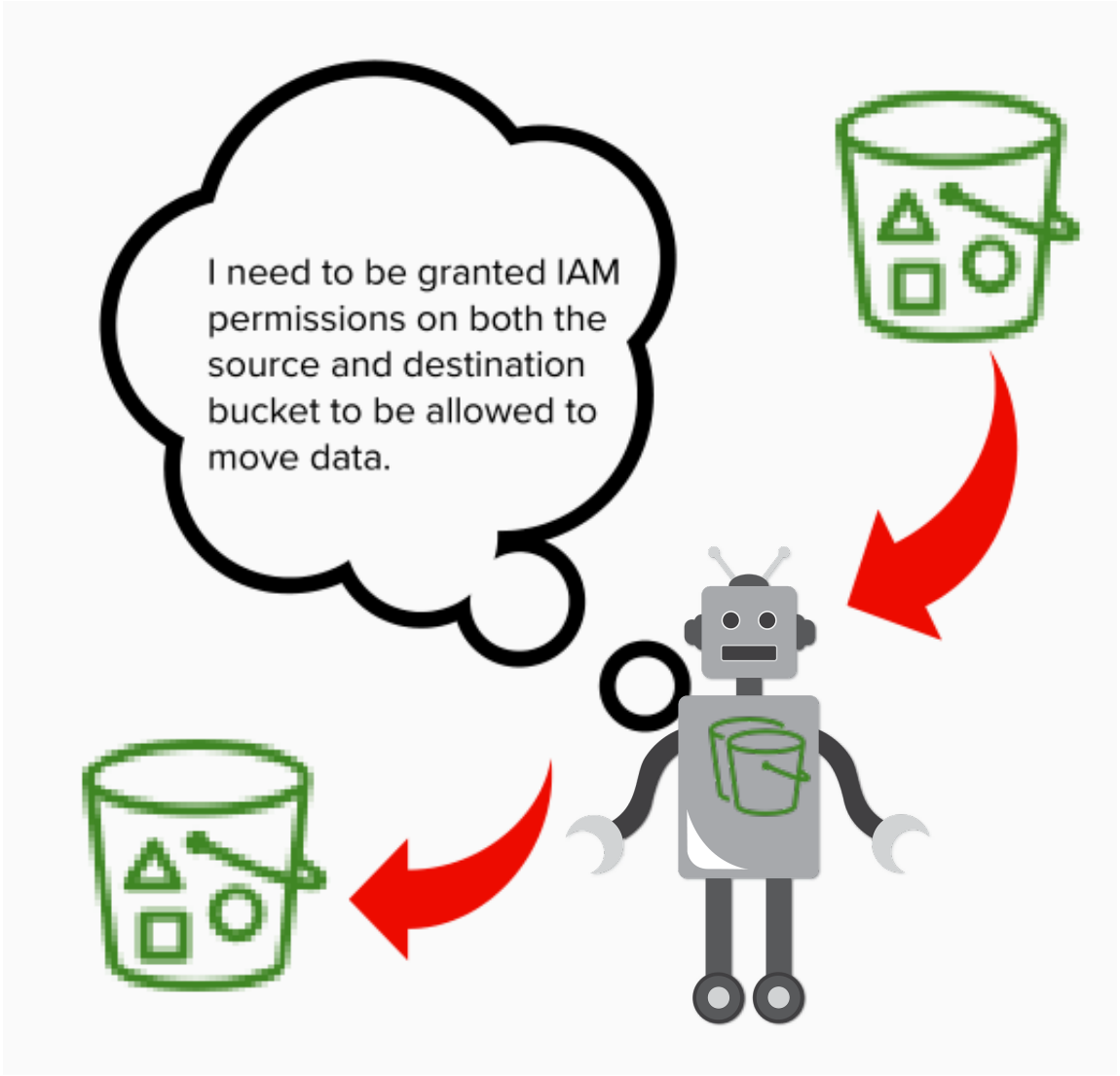
S3 Replication Service - Intro

Capable of being a truly cross-regional, cross account service



S3 Replication Service - Intro

The Replication Service needs explicit permissions to Get and Replicate them



S3 Replication Service - Intro

What a helpful service !

S3 Replication For Evil

We should be wary of ANY entity with the ability to copy data

S3 Replication For Evil

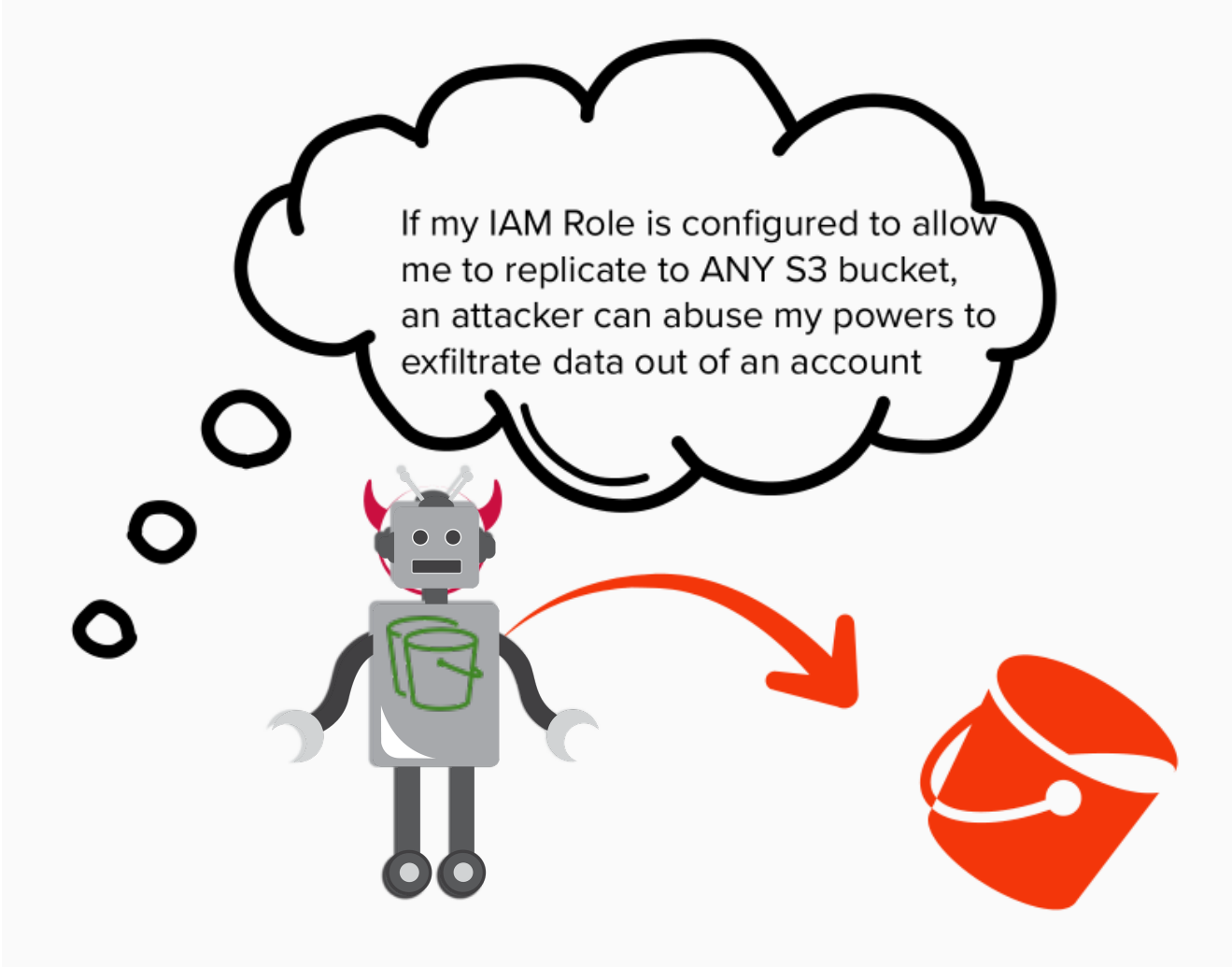
Affecting confidentiality is a primarily motivator for attackers

S3 Replication For Evil

They could update Replication Rules to copy data maliciously

S3 Replication For Evil

Copying data to an attacker-controlled bucket requires the Service have permissions to act on the external bucket



S3 Replication For Evil

For example, an IAM Policy allowing the S3 Replication Service to Replicate on “*” resources

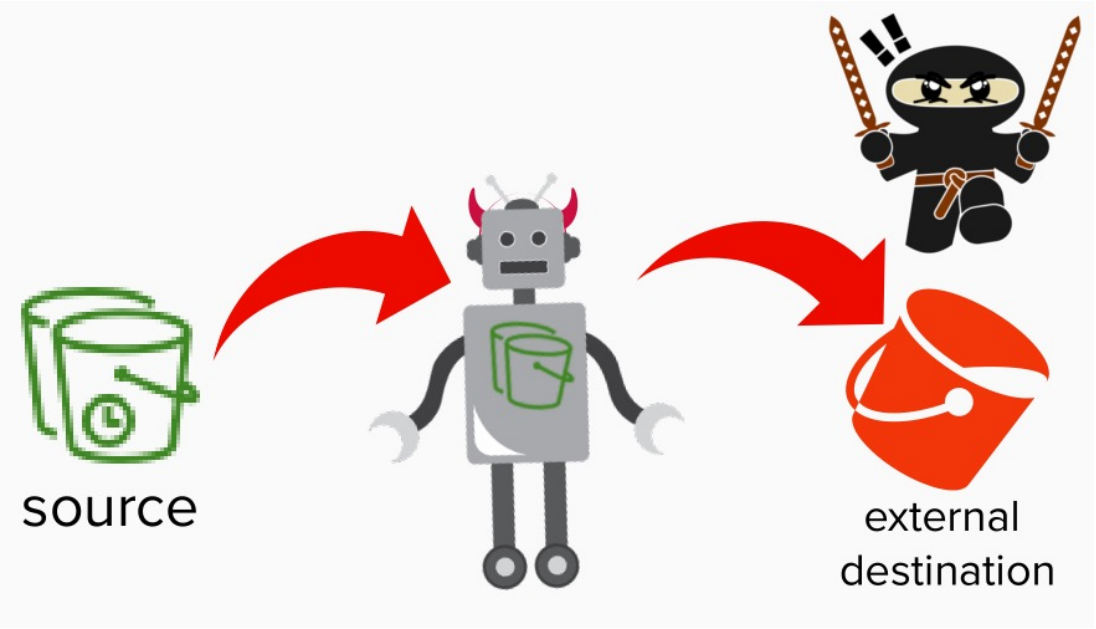
S3 Replication For Evil

The ability to update replication rules is all that's required to copy data out of an Account

s3:PutReplicationConfiguration
iam:PassRole

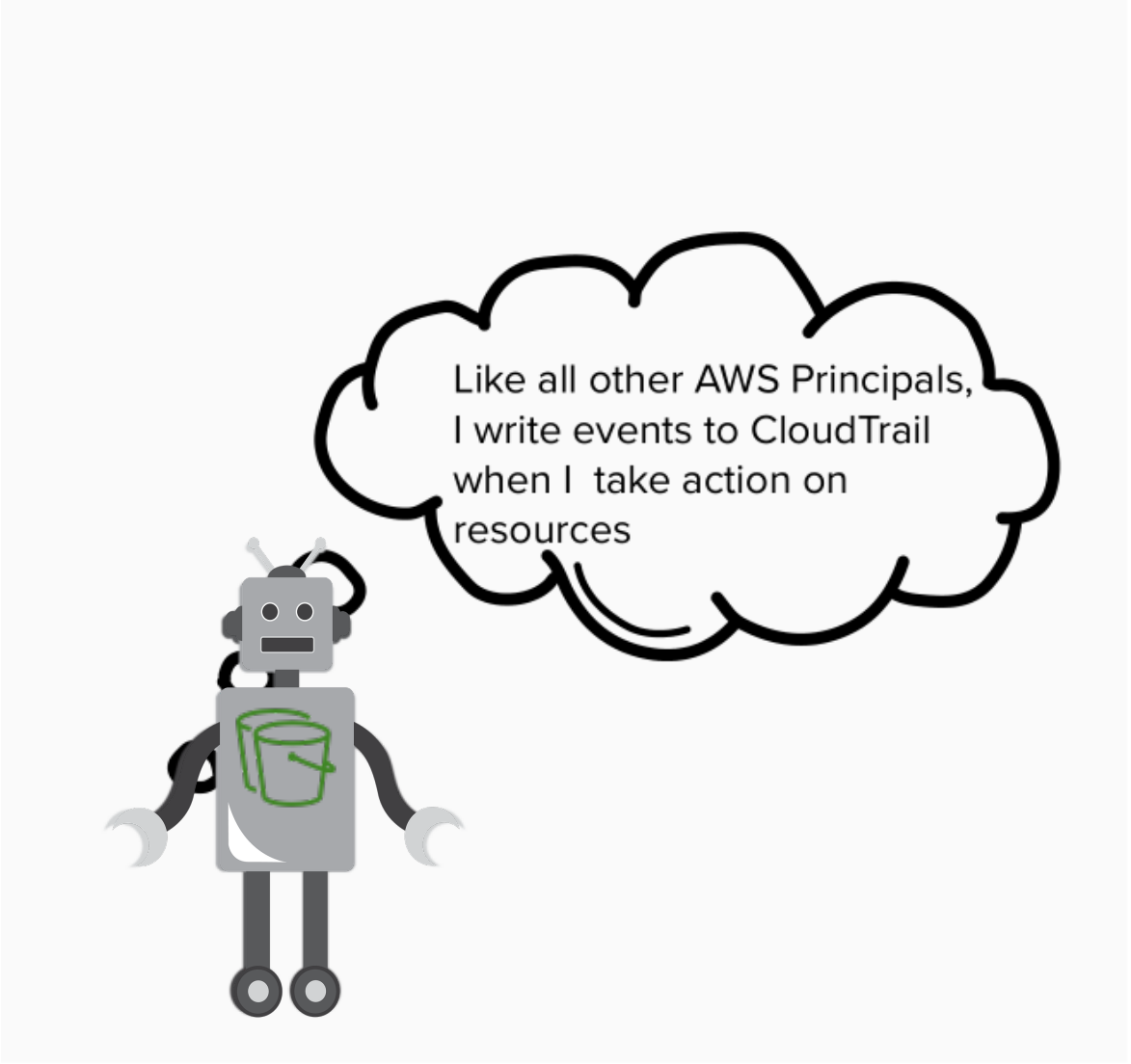
S3 Replication Service

For Good, For Evil, For Confounding Defenders



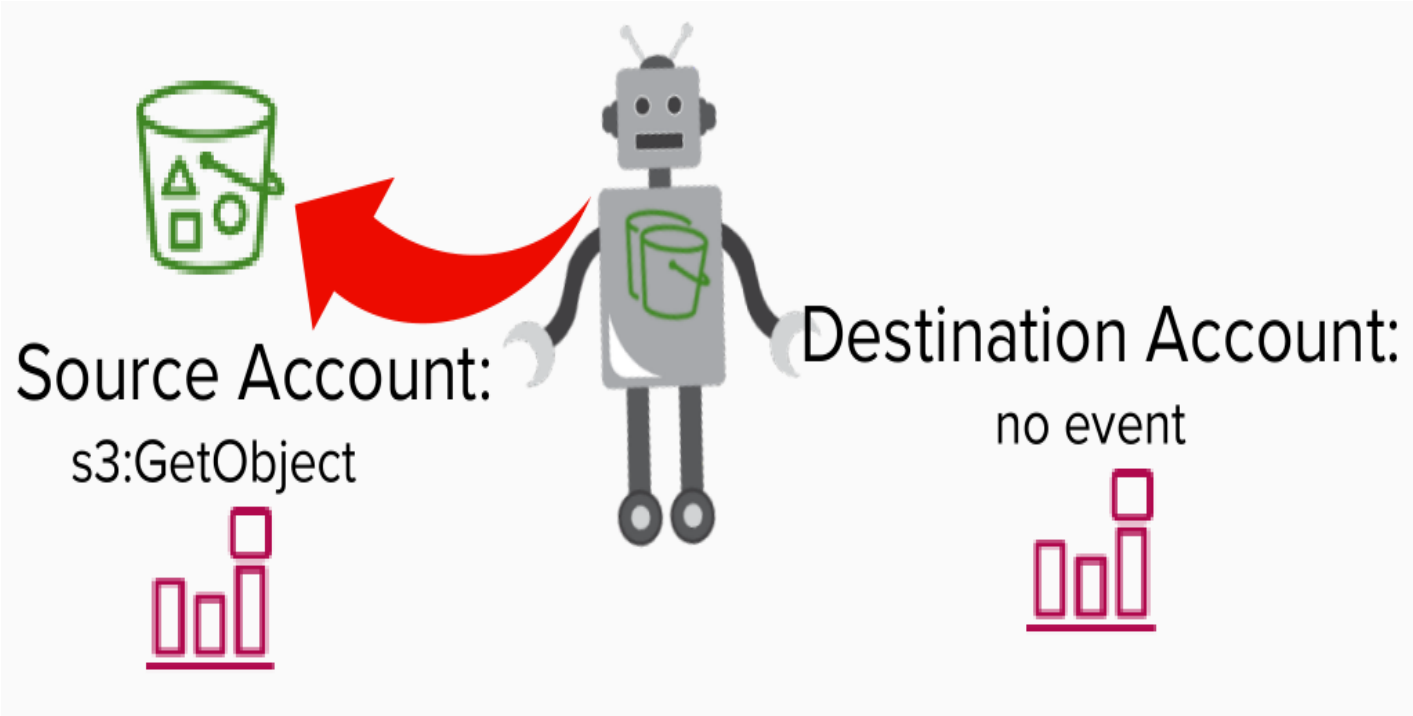
S3 Replication – The Ghost Service

S3 Replication Service writes its events to CloudTrail like all other Principals



S3 Replication – The Ghost Service

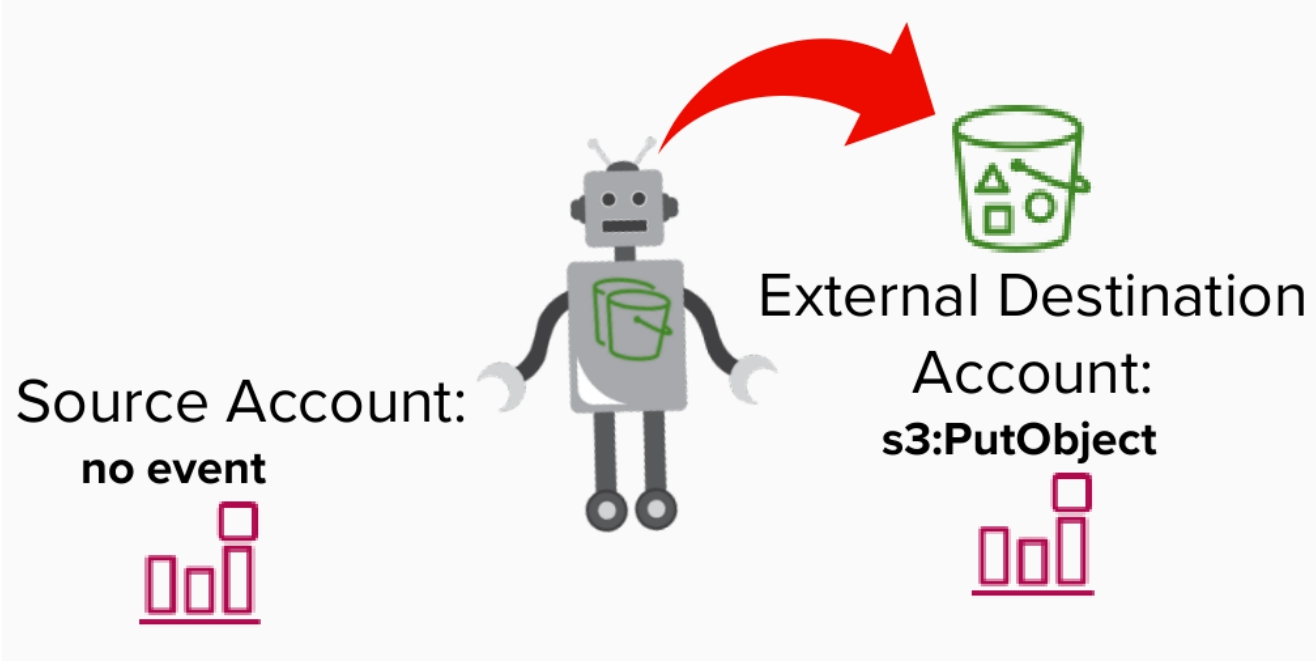
S3 Replication Service writes its **GetObject** events in the Source Account



Behavior as of 7/25/2021

S3 Replication – The Ghost Service

S3 Replication Service writes its **PutObject** events in the Destination Account



Behavior as of 7/25/2021

S3 Replication – The Ghost Service

When data is copied, there is no record of the external bucket in the source account CloudTrail Logs

Behavior as of 7/25/2021

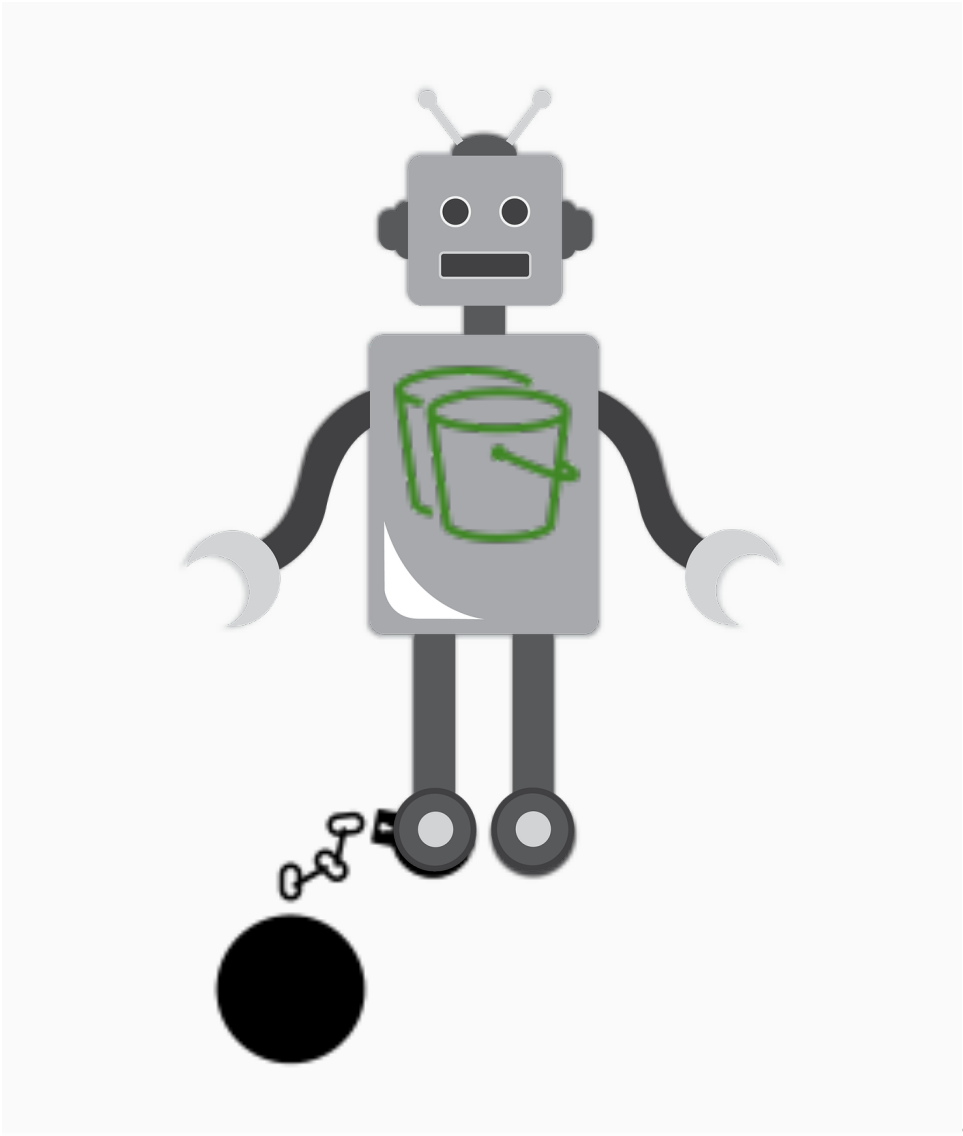
S3 Replication – The Ghost Service

This gap in logging creates allows for the copying data without recording an event

Shackling The Replication Service

- Restrictive IAM Roles for the S3 Replication Service

- SCP enumerating a known list of S3 buckets the Service can replicate to

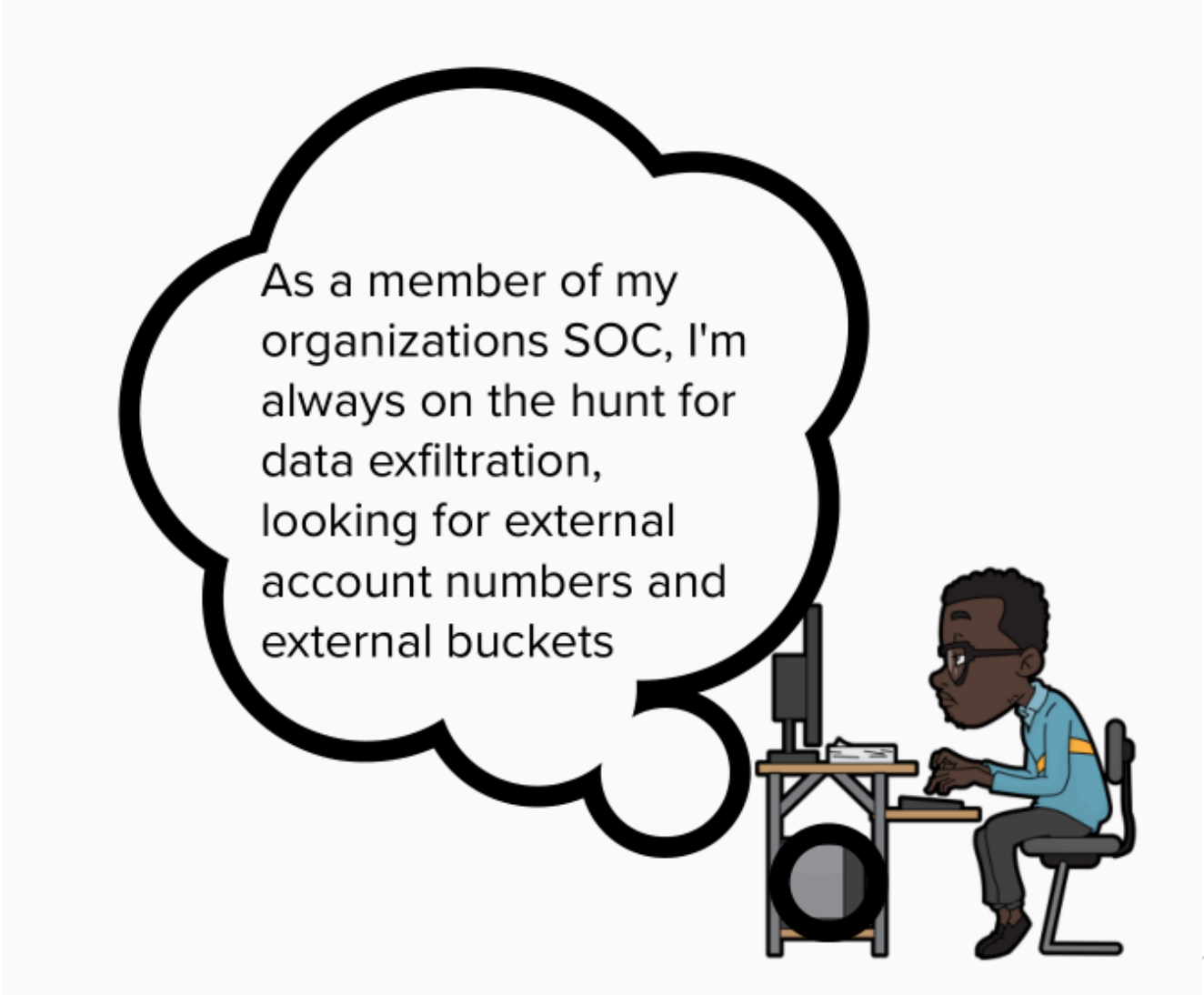


S3 Replication - Evading Detection

Does this matters to the Threat Hunters and Cloud Defenders?

S3 Replication - Evading Detection

They’re role is look for indicators of compromise – regardless of preventive controls

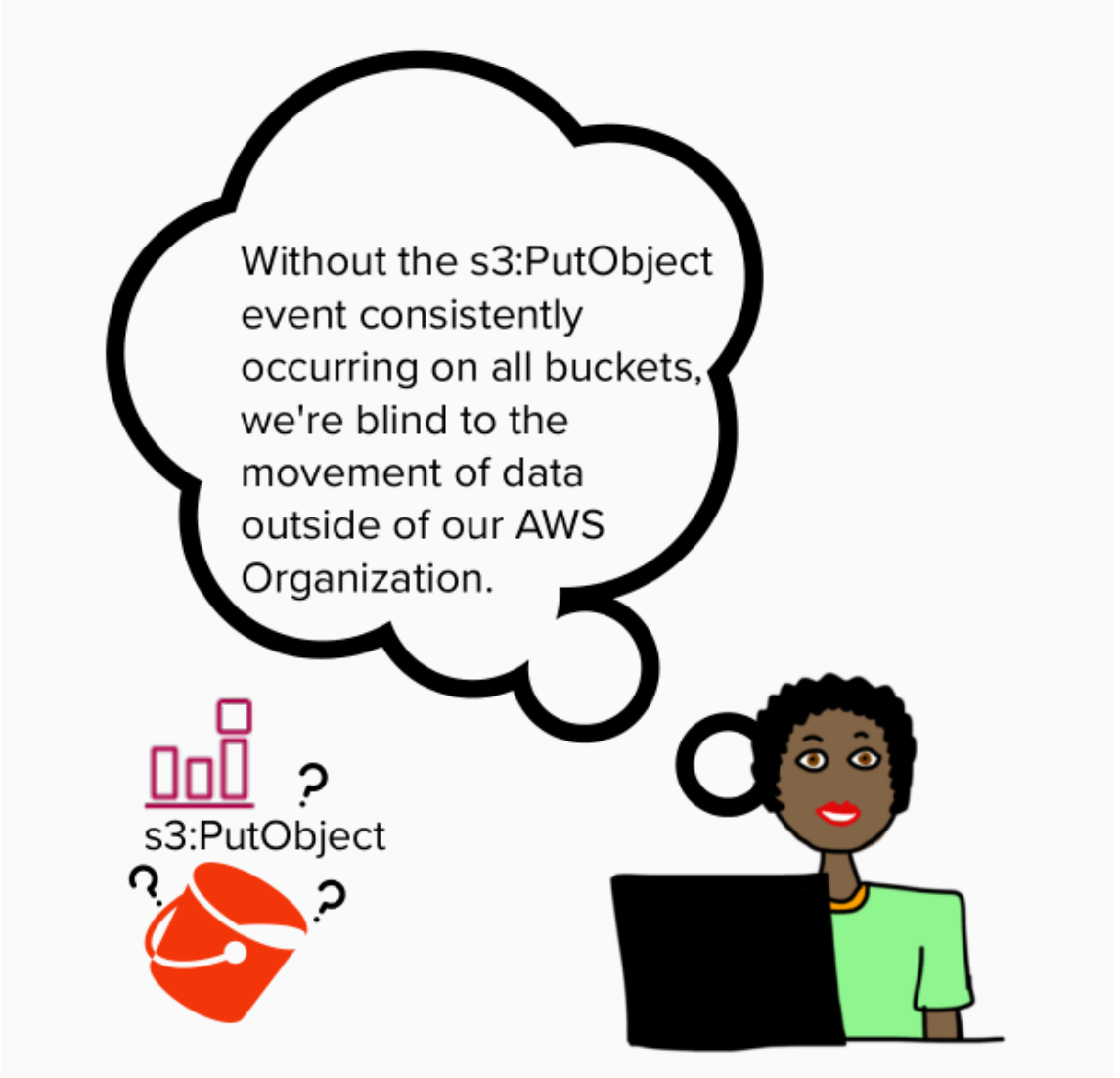


S3 Replication - Evading Detection

CloudTrail data events are supposed to be the bellwether for data exfiltration

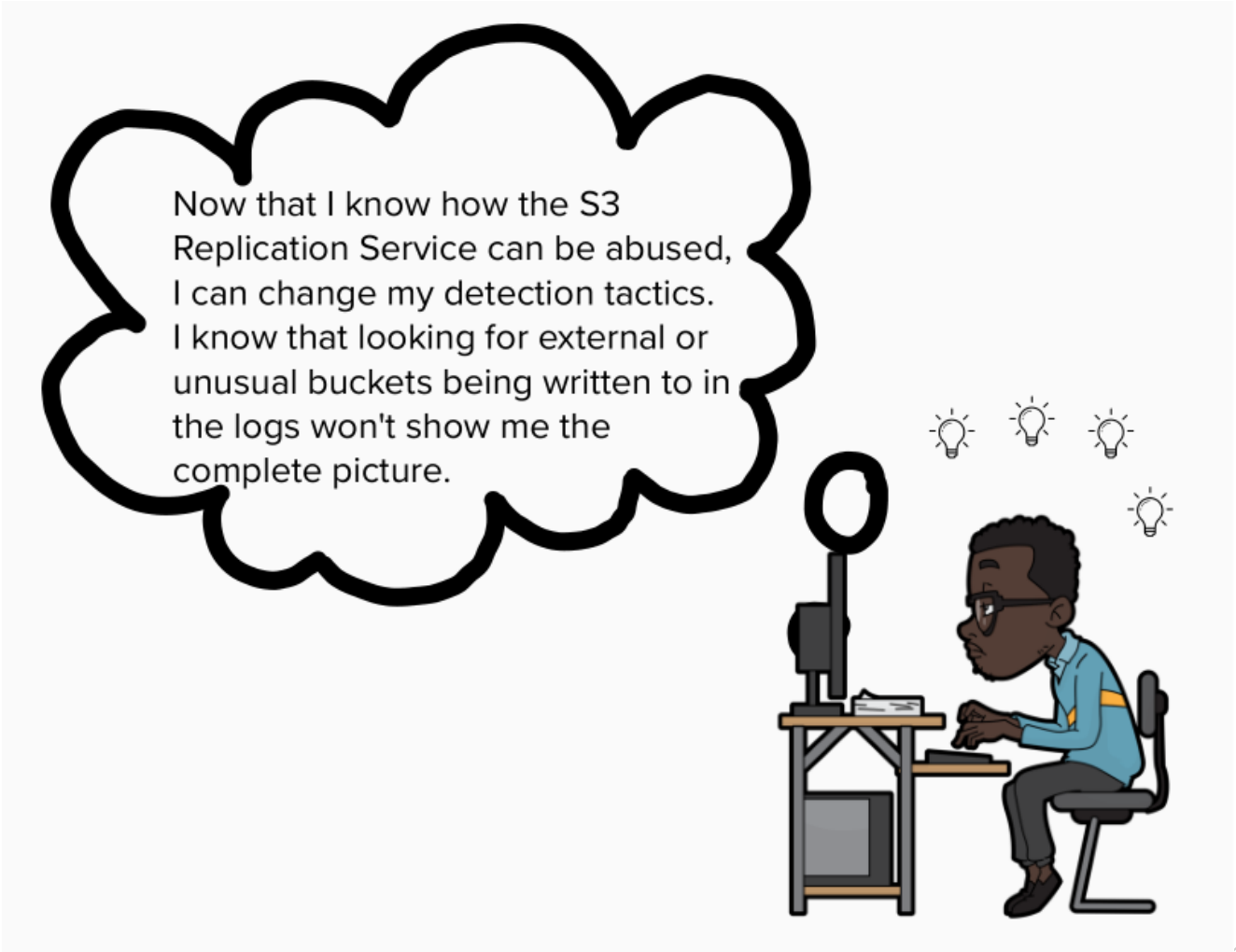
S3 Replication - Evading Detection

They might have been missing data exfiltration via the Replication Service



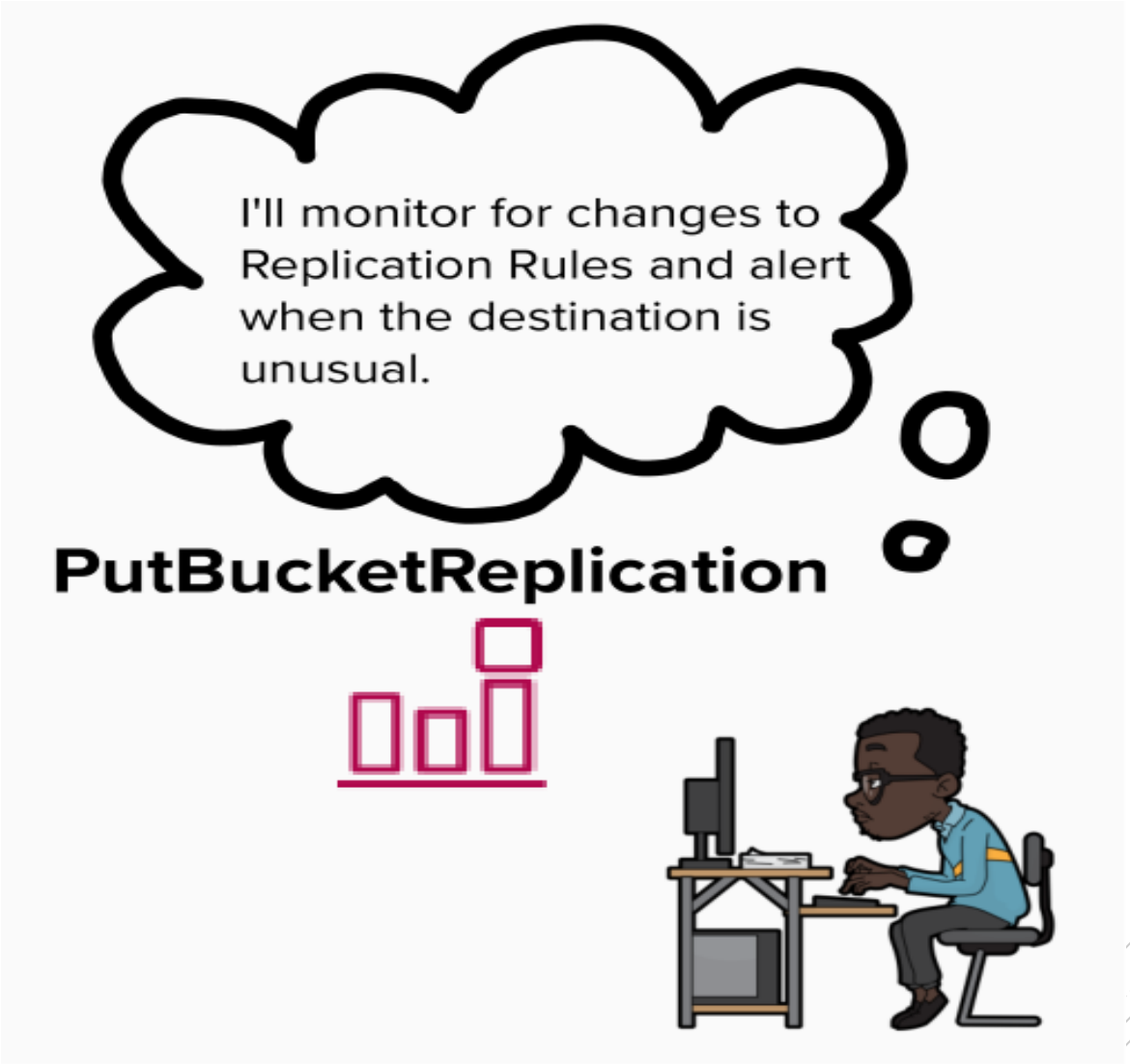
S3 Replication - Evading Detection

Additional alerting is required to watch for the updating of Replication Rules



S3 Replication - Evading Detection

Monitor for external buckets in the PutBucketReplication event



Reporting Timeline

- 10/19/21 - [Vectra]: Initial vulnerability report submitted, and receipt acknowledged same day.
- 10/20/21 - [AWS]: Responded with their indication that they do not believe this to be a vulnerability
- 10/20/21 - [Vectra]: Requested confirmation that AWS does not consider the lack of logging a vulnerability. Indicated that I will depict AWS response to this report as 'won't fix' in any public disclosure.
- 10/26/21 - [AWS]: AWS asked where I would publish the disclosure and if they could have an advance copy of the text.
- 10/26/21 - [Vectra]: Acknowledged they could receive an advance copy of any public disclosure.
- 2/2/22 - [Vectra]: Re-sent the original vulnerability report to an internal contact on the AWS Security team suggesting they put in a request for enhanced logging on the S3 replication service.
- 2/3/22 - [AWS]: Acknowledged they put in the ticket internally.

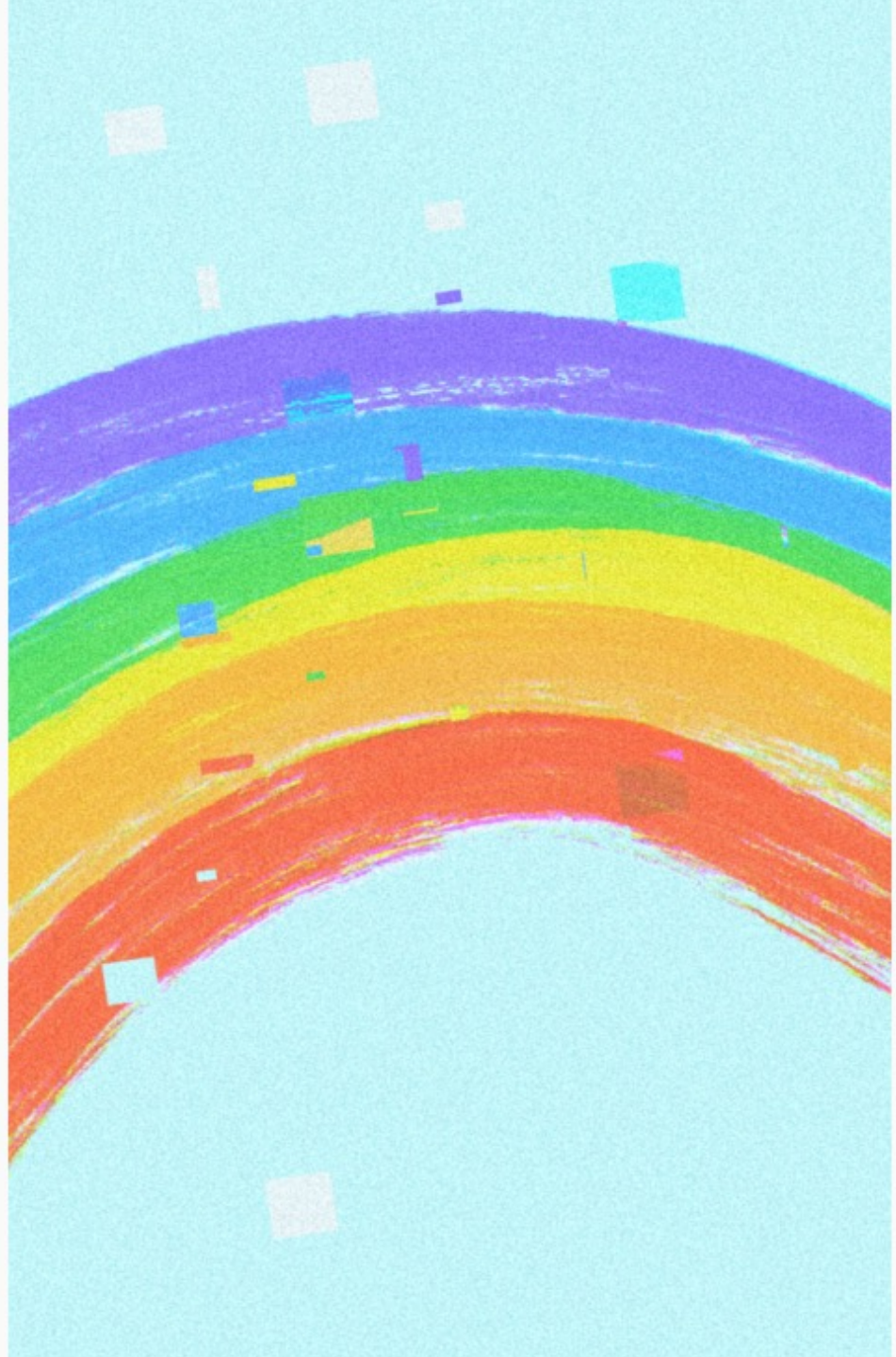
What did we learn…..

"Everything changes all the time and in different places"

What did we learn…..

The ‘on behalf of’ problem in systems is a hard.

It’s challenging from an identity perspective and it’s hard to accurately attribute actions



What did we learn…..

Defenders need reliable ways to monitor for the copying of data

Regardless of any guardrails in place which would prevent exfiltration

QUESTIONS ?

You're the best. You really really are