Security in GCP

By Carly Schneider

Spotify®

Hi, my name is Carly

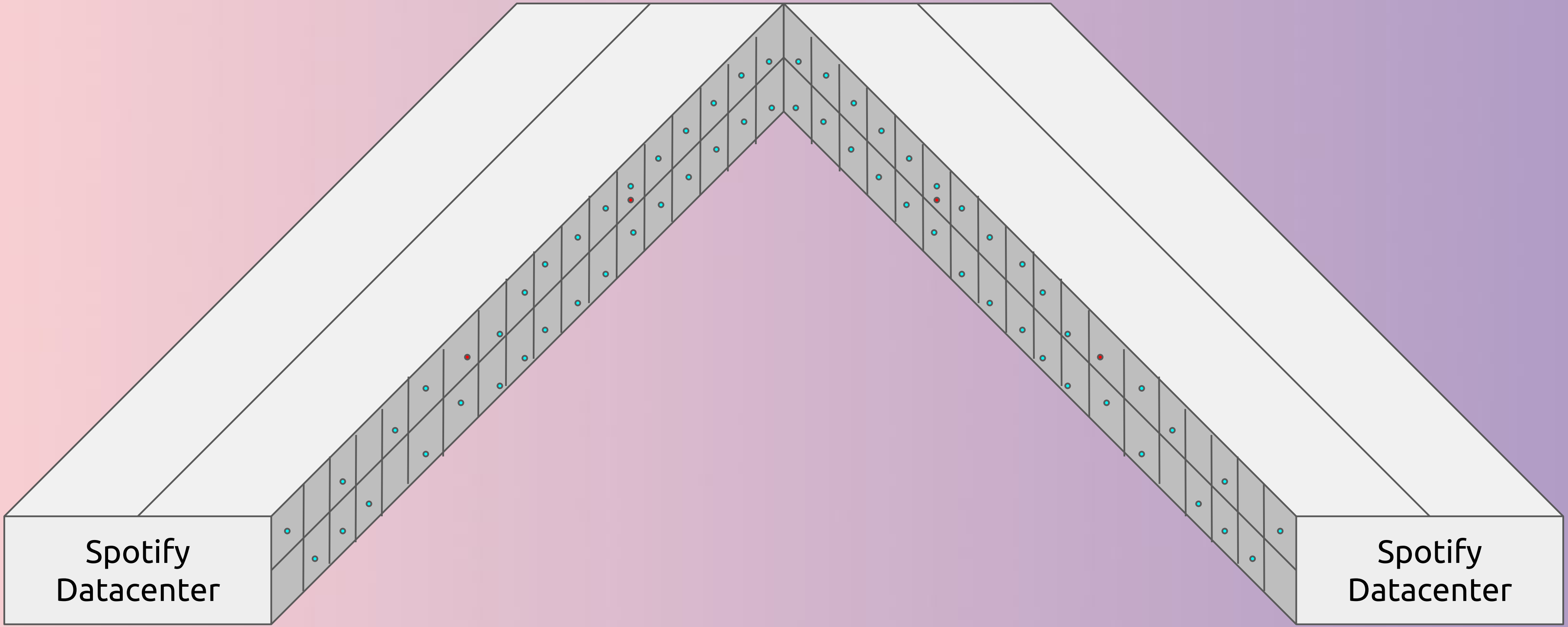
I am from New York

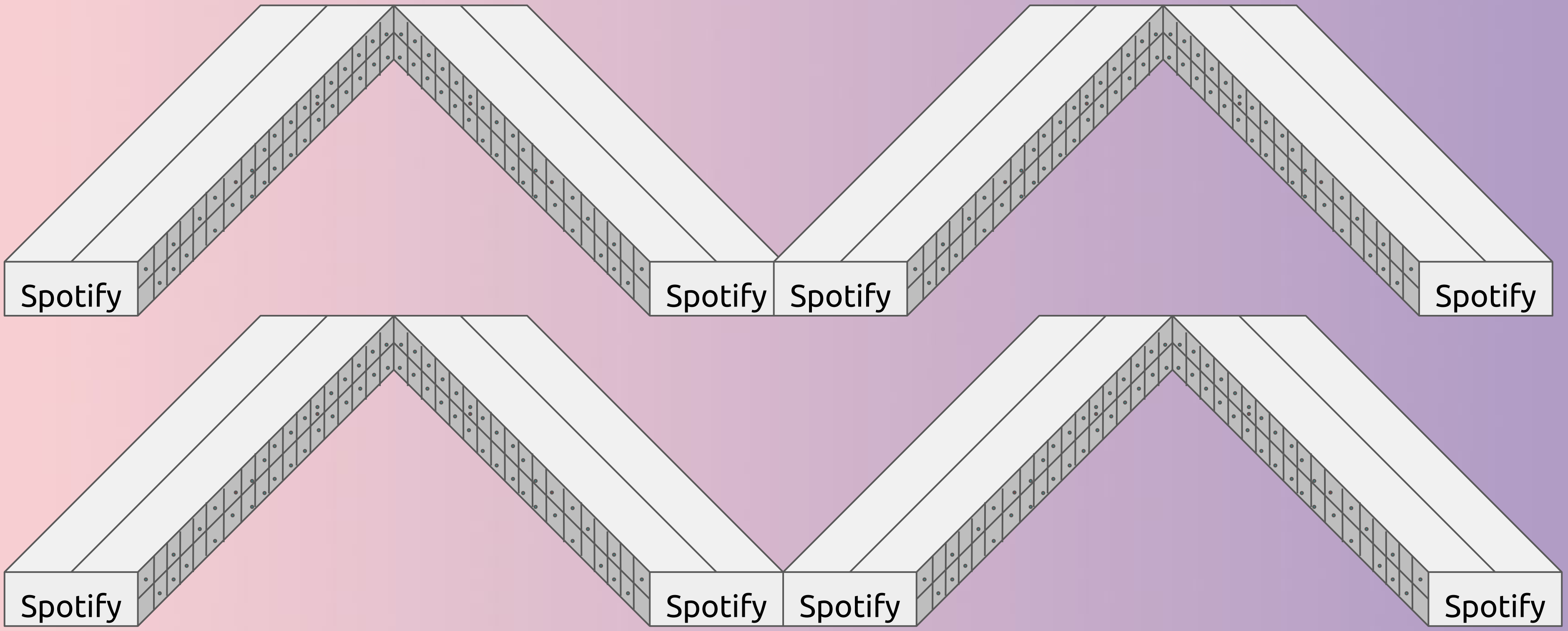
Work at Spotify as a security engineer

Usually likes to take things apart

Spotify used to have their own datacenters

A Spotify Datacenter




Spotify
Spotify
Spotify
Spotify
Spotify
Spotify
Spotify
Spotify

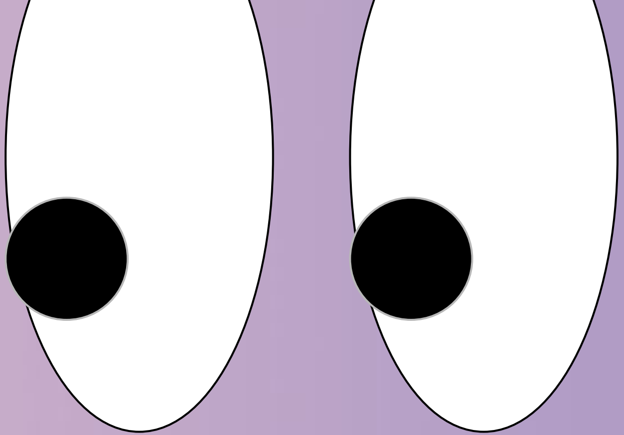
So we switched to the cloud!

The New Landscape of Security Concerns

- Intrusion detection - For Google
- Visibility into what engineers are doing - For Us

Visibility (Security vs Culture)

- Engineers can do whatever they want
- ‘Trust but verify’



Risks?

- Engineers make mistakes

Forseti!

https://github.com/GoogleCloudPlatform/forseti-security

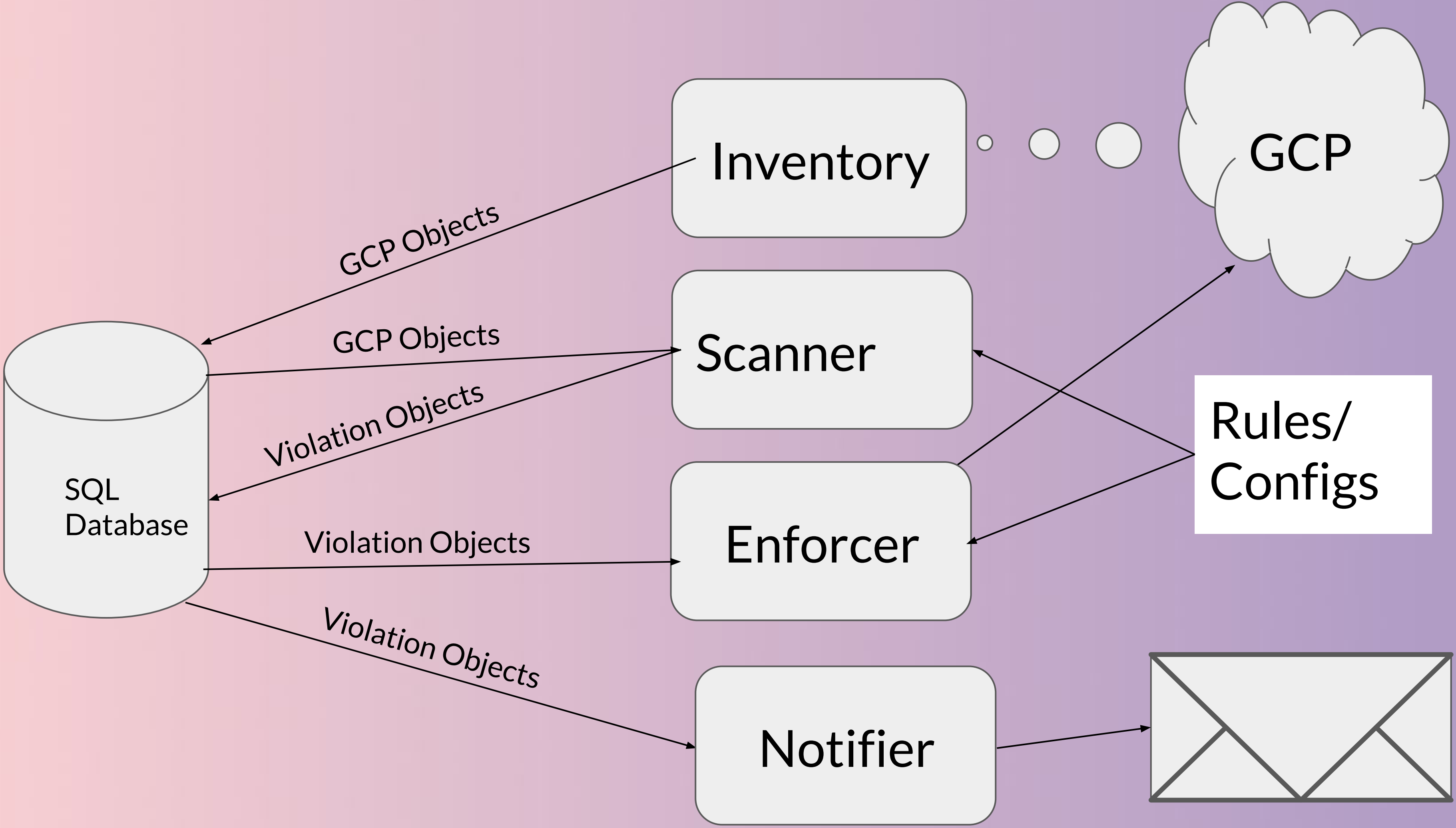
What is Forseti?

- Forseti is an open source toolkit to help secure GCP

- Collection/library of open source tools to help us secure our GCP environment

Goals of working on Forseti

- ‘Rules’ we could change and customize
- Default allow - then create warnings if need be
- An automatic notification system


Inventory
GCP
GCP Objects
Scanner
GCP Objects
Violation Objects
SQL Database
Rules/ Configs
Enforcer
Violation Objects
Violation Objects
Notifier

Inventory

- Takes a snapshot of all the resources
- Turn different GCP resource APIs into ‘pipelines’
- Put each pipeline into a object
  - Objects are stored in a SQL database

Scanner

- Compare rules to what is in each object
- Create a ‘violation’ object when something is violated

Enforcer

- Automatically fix things
- Optional

Notifications

- Looks up the owner of the violating object and notifies them
- Ensures violations have not been broken before
- CCs security if something is not fixed immediately

What are the misconfigurations ?

What are the security implications?

Rules For Data Storage

- BigQuery/Bucket/Cloud SQL Rules
- Engineers own their data
- These rules search for all public objects
- Sometimes they need to be public on purpose

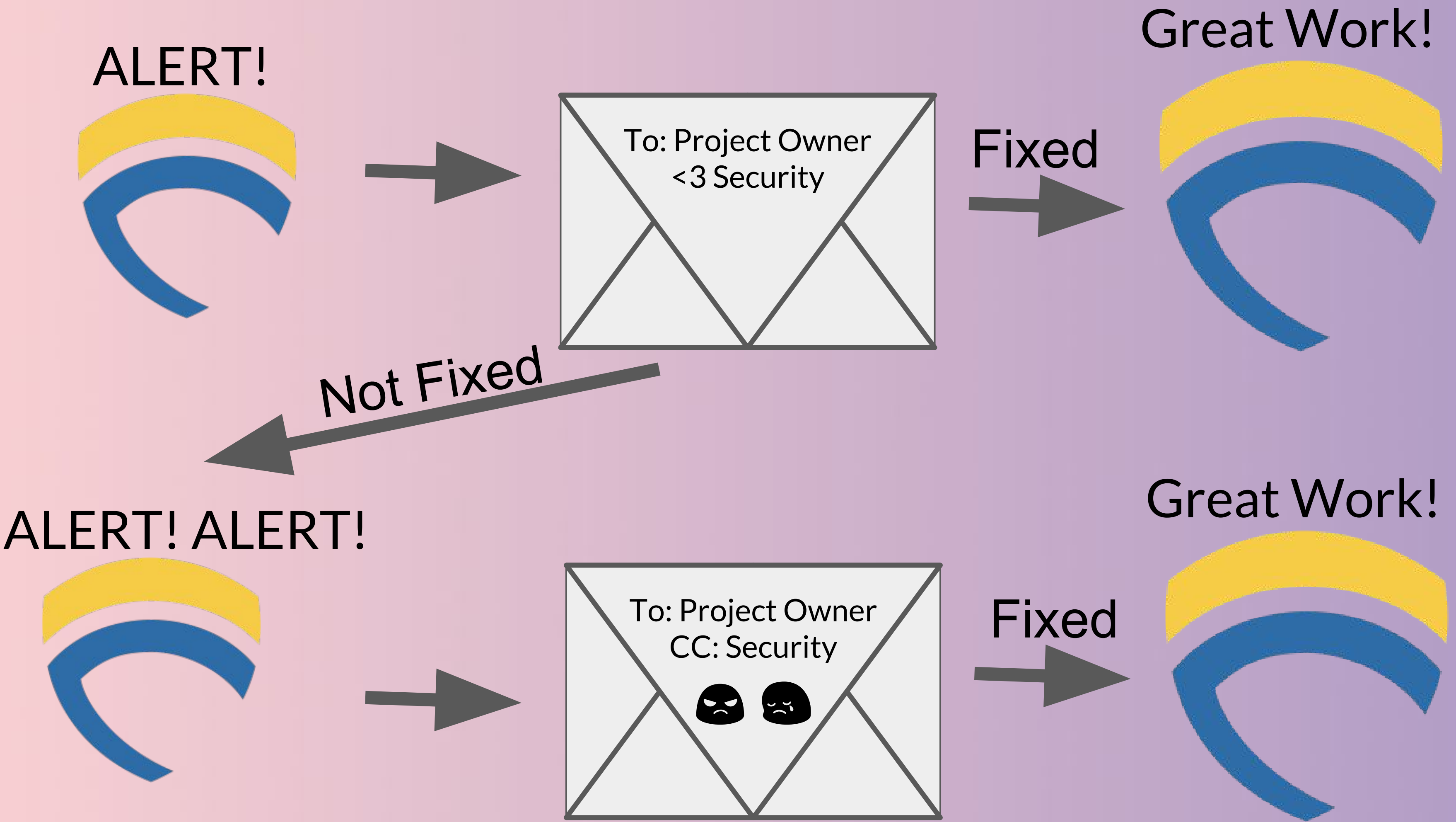
Permission Rules

- Group rules
- Allow only people from the correct org to be part of groups
- IAM rules
- Control admins for different resources

Network Rules

- Monitor which instances are talking outside of their defined network
- Control our perimeter

So how does this actually work?



ALERT!

To: Project Owner
<3 Security

Fixed

Great Work!

Not Fixed

ALERT! ALERT!

To: Project Owner
CC: Security

Fixed

Great Work!

What did we learn?

- Engineers have a lot of legitimate reasons to do seemingly sketchy things
- Auto notifications are the only ways this can scale

Thanks!

github.com/GoogleCloudPlatform/forseti-security

@_5chn31d3r_

carlys@spotify.com