



# Dulce Introducción al Cloud (Chaos) Security

Congreso ConfIT  
7/4/2022

Alberto Brezmes  
Head of Security Processes &  
Advanced Architectures

# Un Poquito sobre mi...

Alberto Brezmes

- Estudié en la ETSISI UPM
- Trabajo en Cloud & Security desde ~2013 (aunque empecé con Ginés en el CIC en 2012)



 @brezmes

 brezmes

 alberto-brezmes

 <https://brezmes.github.io/>



# ¿Qué vas a encontrar en esta charla? (y qué no)

## LO QUE SÍ :) :

- ★ Lo que a mi me valió para entender el mundo Cloud y la Seguridad
- ★ Las técnicas mínimas que uso para hacer una evaluación de un entorno Cloud

## LO QUE NO :( :

- ❖ Transparencias bonitas y con transiciones
- ❖ Mucho texto (EN LA DOCU OFICIAL ES MÁS)



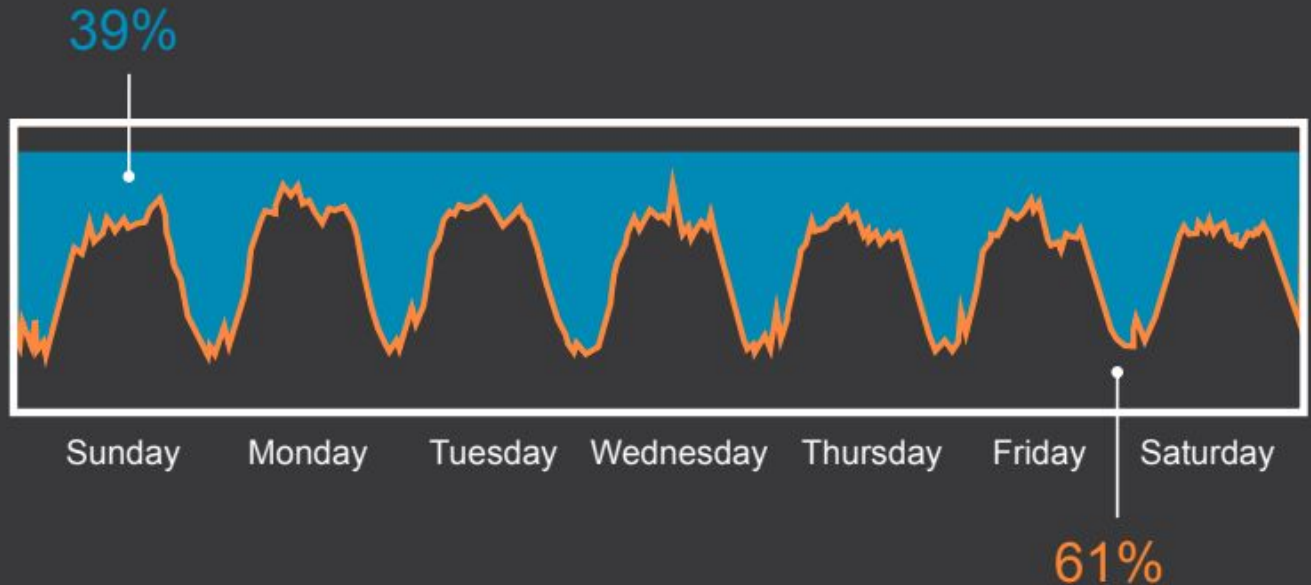
# Dulce Introducción al Cloud (Chaos) Security

- 1. Introducción al Cloud y “al” Security**
2. ¿Qué es el Chaos Engineering?
3. ¿Qué hay en la Comunidad?
4. Hands-on!

# Introducción al Cloud y “al” Security

## Historia de AWS 2010

### TYPICAL WEEKLY TRAFFIC TO AMAZON.COM



# Introducción al Cloud y “al” Security

## Historia de AWS 2010



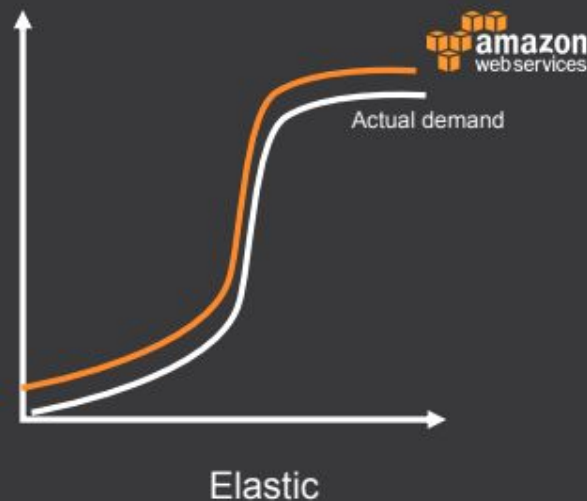
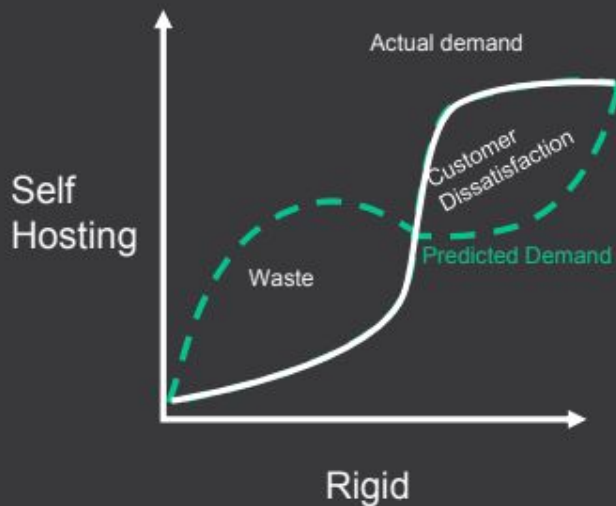
# Introducción al Cloud y “al” Security

## Historia de AWS 2010



# Introducción al Cloud y “al” Security

## Historia de AWS







# Introducción al Cloud y “al” Security

Y después, todos los demás (GCP, Azure...),  
al menos tal y como lo conocemos ahora...



# Introducción al Cloud y “al” Security

## ¿Qué es la nube?

(X)aaS

IaaS

PaaS

SaaS - **Serverless**

## Modelos:

Public

AWS / Azure / GCP ...

Hybrid

Private

Openstack

# Introducción al Cloud y “al” Security

## Empezamos con la seguridad...

Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services



SECURITY **IN**  
THE CLOUD

Security measures that the cloud service provider (AWS) implements and operates



SECURITY **OF**  
THE CLOUD

# Introducción al Cloud y “a” Security

## Shared Responsibility Model



### MANAGED BY CUSTOMERS (IN)

- Configure AWS security features
- Can implement and manage own controls
- Choose additional assurance above AWS
- Gain access to a mature vendor marketplace

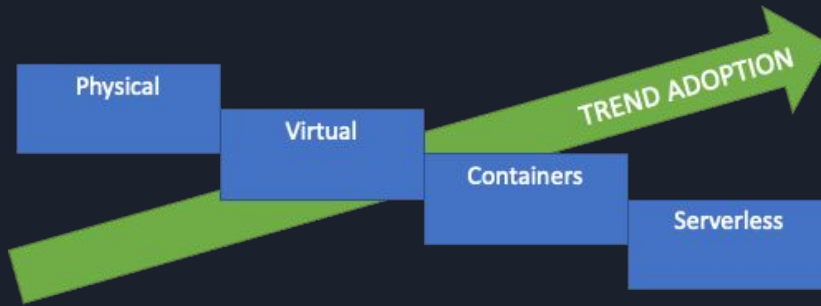


### MANAGED BY AWS (OF)

- Ongoing audit and assurance programs
- Protection of the global infrastructure that runs all of the AWS services
- Protection of large-scale AWS service endpoints
- Culture of security and improvement

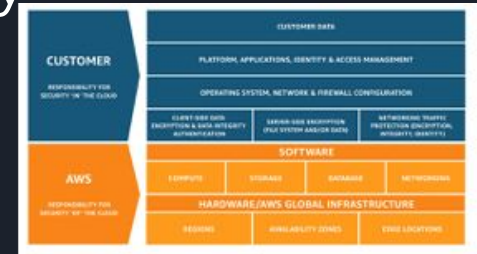
# Introducción al Cloud y “al” Security

## El nuevo paradigma en continua evolución



Most of services are on the first half, but, most of customers are on second half

We need work today on the middle, but to have the focus on the right



AWS Cloud Shared Responsibility Model



Azure Cloud Shared Responsibility Model

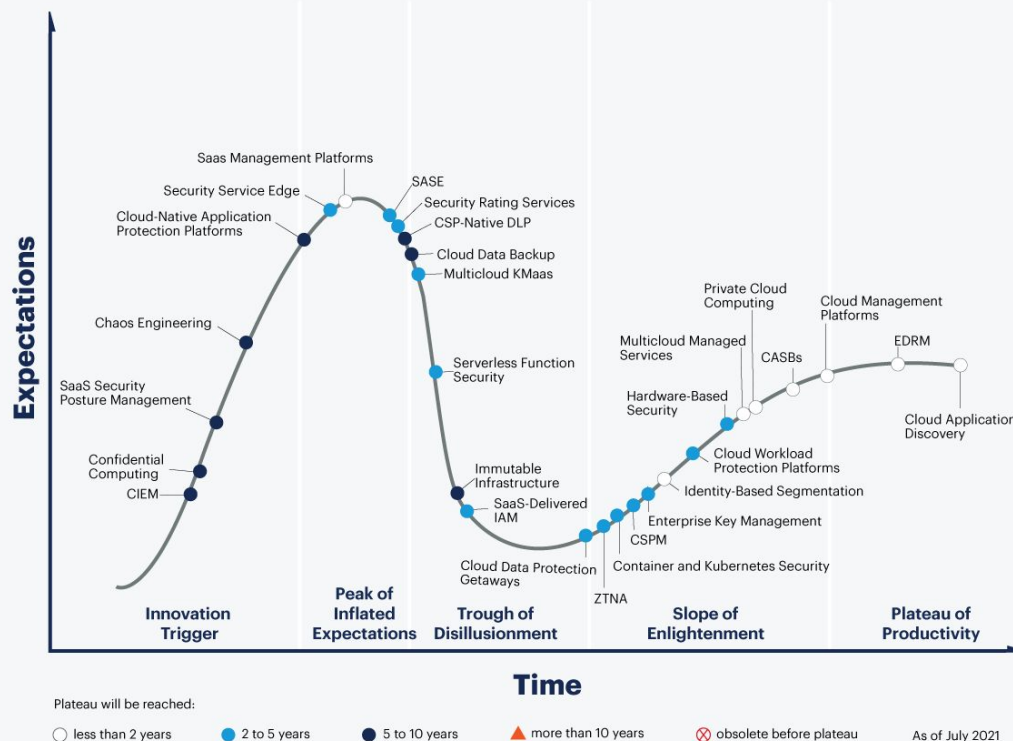


Google Cloud Shared Responsibility Model



# Introducción al Cloud y “al” Security

## Hype Cycle for Cloud Security, 2021



[gartner.com/SmarterWithGartner](https://gartner.com/SmarterWithGartner)

Source: Gartner  
© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and its affiliates in the U.S.



# Introducción al Cloud y “al” Security

## Lo que a mi me interesa de verdad





Introducción al Cloud y “al” Security

Qué es Dev(Sec)Ops?





Introducción al Cloud y “al” Security

# Qué es Dev(Sec)Ops?

DevOps (a clipped compound of development and operations) is a culture, movement or practice that emphasizes the collaboration and communication of both software developers and other information-technology (IT) professionals while automating the process of software delivery and infrastructure changes.

It aims at establishing a culture and environment where building, testing, and releasing software can happen rapidly, frequently, and more reliably.



# Introducción al Cloud y “al” Security

## Y por qué es importante?

**API** (Application Programming Interface), es un conjunto de funciones o procedimientos implementados en un lenguaje de programación capaces de actuar como capa de abstracción entre una librería o biblioteca y un software.

El uso de APIs para el despliegue de infraestructura nos permite mantener una versión de esta al realizarse mediante código, como si de una aplicación en un lenguaje de programación se tratara. Cualquier API de un proveedor de cloud tiene su propio CLI (Common Language Interface) permitiéndonos crear entre otros, recursos de computación, almacenamiento, y redes como aspectos más importantes.



# Introducción al Cloud y “al” Security

## Por esto:

La creación de infraestructura de forma programática nos da las siguientes ventajas:

- Mantenimiento de versiones en el código.
- Análisis de código.
- Auditoría de cambios.



Introducción al Cloud y “al” Security

Volemos a lo que me preocupa

**IAM**

Identity and Access Management (IAM)

- Perfilar el acceso a cualquier recurso que esté disponible

Las principales gestiones que se pueden hacer mediante la consola IAM son:

- Administrar usuarios de IAM y su acceso.
- Administrar funciones de IAM y sus permisos.
- Administración de los usuarios federados y sus permisos.



Introducción al Cloud y “al” Security

Volemos a lo que me preocupa

**IAM**

Identity and Access Management (IAM)

- Credentials Report
- Identity Providers
- Utilities. Reports & Config Enforcement

Y en concreto en AWS el CloudTrail y CloudWatch



Introducción al Cloud y “al” Security

Volemos a lo que me preocupa

# LOGGING & MONITORING

NUESTROS OJOS PARA SABER QUÉ PASA O CUANDO  
HA PASADO ALGO




Introducción al Cloud y “al” Security

Volemos a lo que me preocupa

**NETWORKING**

LO QUE EVITA QUE PASE MUCHO MÁS



# Introducción al Cloud y “al” Security

## INCISO!!

- **Crear cuenta AWS bajo free tier**
  - Cree una cuenta gratuita <https://aws.amazon.com/es/>
- **Instalar docker**
  - MAC <https://docs.docker.com/docker-for-mac/install/>
  - Windows <https://docs.docker.com/docker-for-windows/install/>
  - Linux <https://docs.docker.com/install/linux/docker-ce/ubuntu/>
- **Instalar docker-compose**
  - <https://docs.docker.com/compose/install/>





# Dulce Introducción al Cloud (Chaos) Security

1. Introducción al Cloud y “al” Security
- 2. ¿Qué es el Chaos Engineering?**
3. ¿Qué hay en la Comunidad?
4. Hands-on!



¿Qué es el chaos engineering?

## Contexto

Chaos engineering is the discipline of experimenting on a software system in production in order to build confidence in the system's capability to withstand turbulent and unexpected conditions. —-Wikipedia.



¿Qué es el chaos engineering?

En resumen... esto:

- Fault injection
- Fault tolerance
- Fault-tolerant computer system
- Data redundancy
- Error detection and correction
- Fall back and forward
- Resilience (network)
- Robustness (computer science)



¿Qué es el chaos engineering?

## Comunidad

- Chaos Monkey. Simian Army
- Chaos Machine
- Proofdock Chaos Engineering Platform
- Gremlin
- Facebook Storm

>>ROCKSTAR DAY



# Dulce Introducción al Cloud (Chaos) Security

1. Introducción al Cloud y “al” Security
2. ¿Qué es el Chaos Engineering?
- 3. ¿Qué hay en la Comunidad?**
4. Hands-on!



¿Qué hay en la comunidad?

# Volviendo a Cloud Security

- Chaos Monkey <https://github.com/Netflix/chaosmonkey>
- Security Monkey [https://github.com/Netflix/security\\_monkey](https://github.com/Netflix/security_monkey)
  - AWS
    - Config <https://aws.amazon.com/es/config/>
    - Security Hub <https://aws.amazon.com/es/security-hub/>
    - Control Tower <https://aws.amazon.com/es/controltower/>
      - Landing Zone CAF [https://d1.awsstatic.com/whitepapers/aws\\_cloud\\_adoption\\_framework.pdf](https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf)
  - GCP Asset Inventory <https://cloud.google.com/asset-inventory/docs/overview>



¿Qué hay en la comunidad?

# Volviendo a Cloud Security

CS-Suite <https://github.com/SecurityFTW/cs-suite>

Prowler <https://github.com/toniblyx/prowler>

ScoutSuite <https://github.com/nccgroup/ScoutSuite>



¿Qué hay en la comunidad?

# Volviendo a Cloud Security

CIS Benchmark (registro gratuito)

[https://www.cisecurity.org/benchmark/amazon\\_web\\_services/](https://www.cisecurity.org/benchmark/amazon_web_services/)

CSA Matrix (registro gratuito)

<https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/>

MITRE Attack Cloud Matrix

<https://attack.mitre.org/matrices/enterprise/cloud/>





# Dulce Introducción al Cloud (Chaos) Security

1. Introducción al Cloud y “al” Security
2. ¿Qué es el Chaos Engineering?
3. ¿Qué hay en la Comunidad?
4. **Hands-on!**



HANDS-ON!!

1. Usuario IAM - SecurityAudit
2. Prowler
3. Reports

Un Poquito sobre mi...

Alberto Brezmes

**MUCHAS  
GRACIAS!!**



 @brezmes

 brezmes

 alberto-brezmes

 <https://brezmes.github.io/>