# Azure Incident Response

Juan Garrido
@tr1ana


- Juan Garrido
- nccgroup
- Juan.garrido@nccgroup.trust


# Índice

1. Estado de proveedores Cloud. 2018

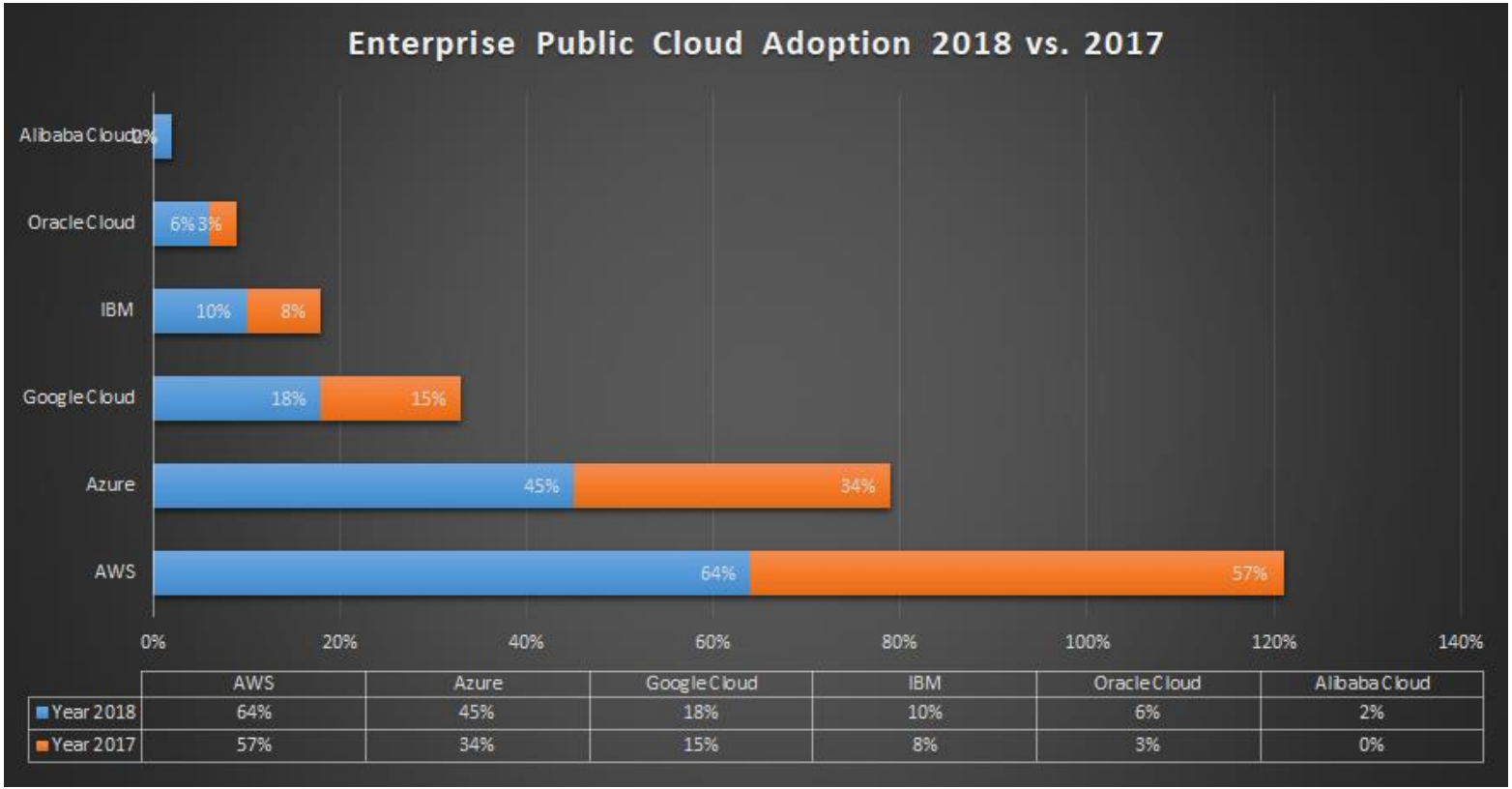
2. Desafíos actuales

3. Respuesta a incidentes en Cloud. Modelo básico

4. Escenarios típicos de ataque

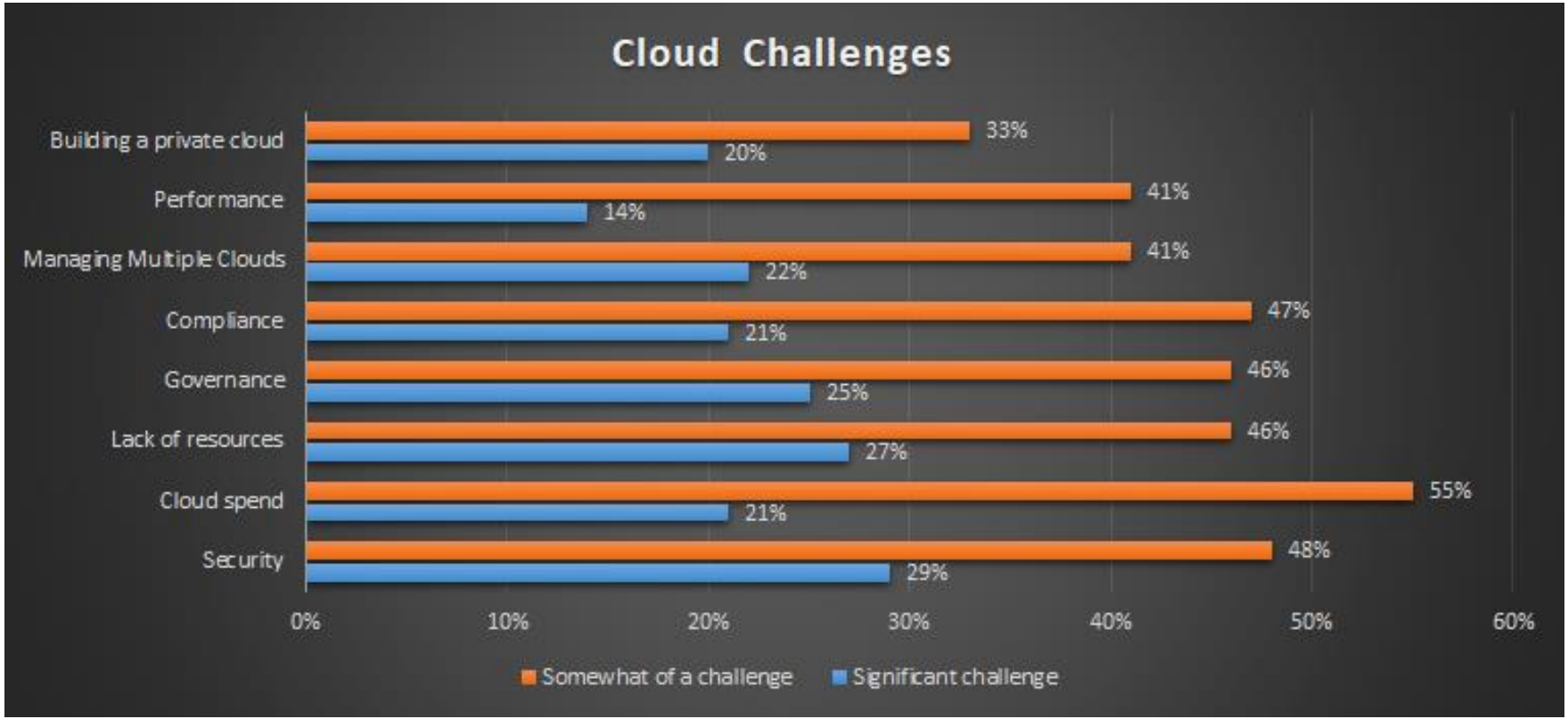
5. Recomendaciones

# Estado de proveedores Cloud. 2018




| | AWS | Azure | Google Cloud | IBM | Oracle Cloud | Alibaba Cloud |
|---|---|---|---|---|---|---|
| Year 2018 | 64% | 45% | 18% | 10% | 6% | 2% |
| Year 2017 | 57% | 34% | 15% | 8% | 3% | 0% |

# Desafíos

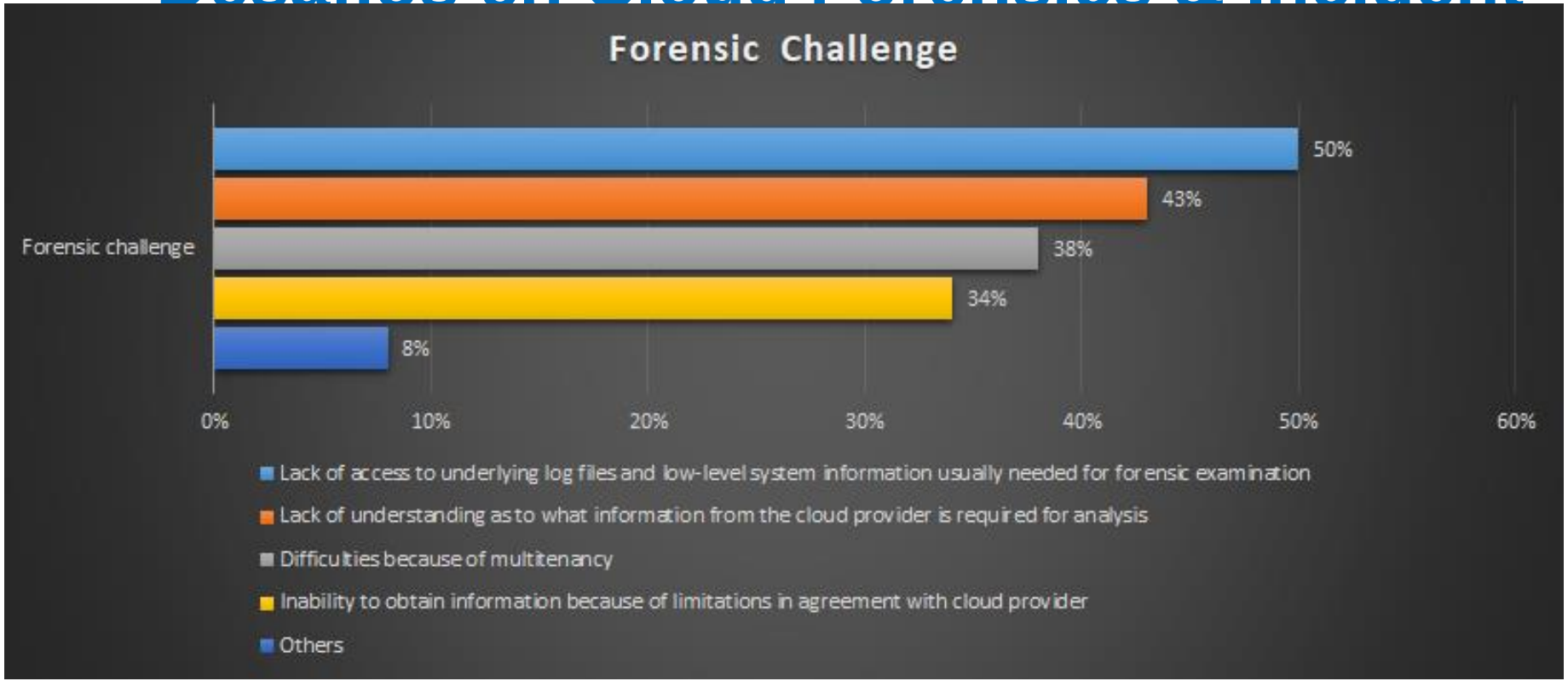

Cloud Challenges
Building a private cloud
33%
20%
Performance
41%
14%
Managing Multiple Clouds
41%
22%
Compliance
47%
21%
Governance
46%
25%
Lack of resources
46%
27%
Cloud spend
55%
21%
Security
48%
29%
0%
10%
20%
30%
40%
50%
60%
Somewhat of a challenge
Significant challenge

# Respuesta a incidents en Cloud. Modelo básico


Identificación

Cierre

# Desafíos en Cloud Forensics & Incident




CIBER_
SEGURIDAD
ccn-cert
centro criptológico nacional
#XIIJornadasCCNCERT
www.ccn-cert.cni.es

# Escenarios típicos de ataque

- Filtración de datos
- Infección de servidores o servicios
- Acceso no autorizado a BBDD

# Incident Response aplicado a VMs

**Identificación**

- Credenciales comprometidas
- Metodología de acceso
- Fugas de información
- Etc..

**Recursos**

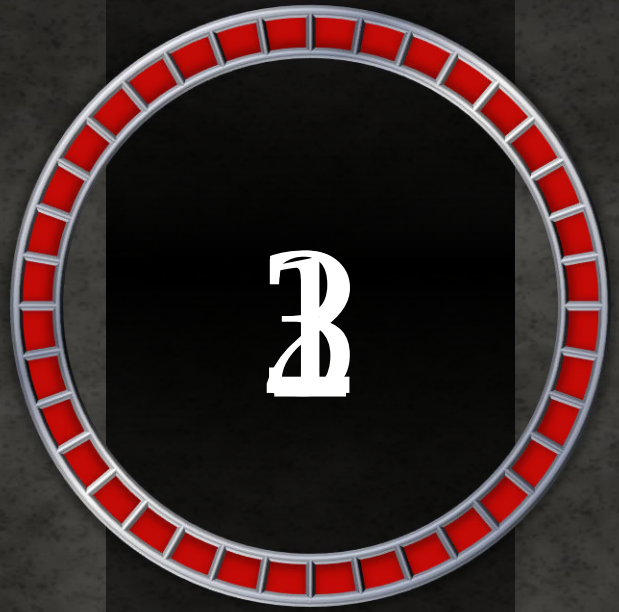
- Azure Identity Reports
- AzureVM Alerts
- Azure Monitor
- Azure Hub
- Azure Insights
- Security Center

**Análisis**

- Uso de credenciales, API keys
- Localización y descarga de Virtual Disk
- Análisis de memoria RAM
- Etc…

**Contramedidas**

- Desactivación de cuentas comprometidas
- Fortificar VM
- Azure Just In Time
- Azure Security Center
- Azure Alerts



# Data Exfiltration & Security Compliance Report

# Incident Response aplicado a Código malicioso

## Identificación

- Identificar y analizar código malicioso
- Detectar posible fuga de información

## Recursos

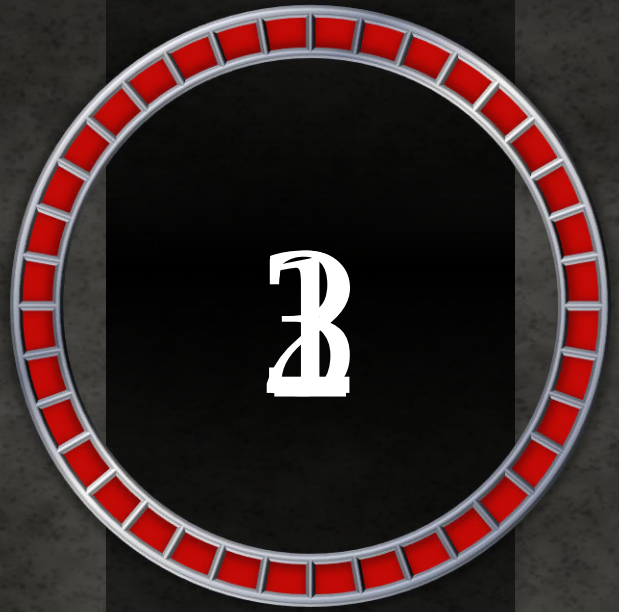
- AzureVM Alerts
- Azure Monitor
- Azure Hub
- Azure Log Forwarding
- Security Center
- Azure Network Watcher

## Análisis

- Análisis de eventos generados por AV/IDS/FW/etc
- Azure Security Center
- Análisis de tráfico
- Análisis de Código malicioso

## Contramedidas

- Desinfectar/Snapshot/Backup/VM
- Fortificar VM
- Azure Just In Time
- Azure Locks
- Azure Security Center
- Azure Identify Protection
- Azure Audit Logs
- Enterprise Wide Policies
- Advanced Threat Detection
- Etc..



# Azure Monitor

# Incident Response aplicado a BBDD

## Identificación

- Identificar acceso no autorizado a BBDD
- Identificar y analizar consultas maliciosas

## Recursos

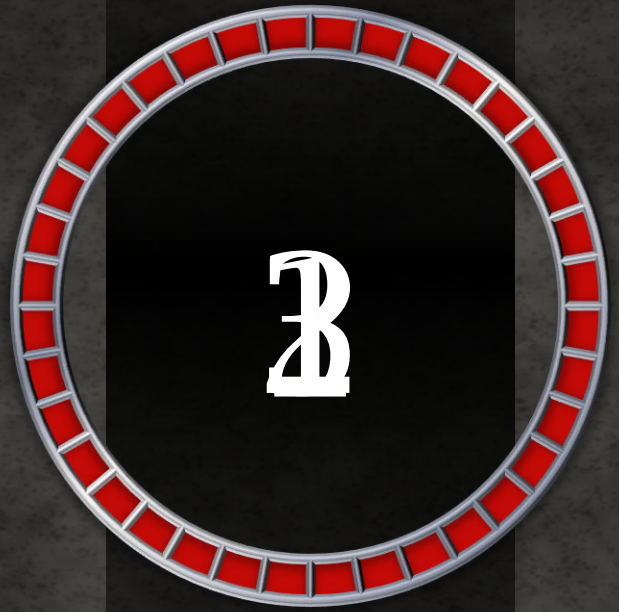
- Azure SQL Audit
- Azure Monitor

## Análisis

- Búsqueda de eventos generados por usuario
- Análisis de consultas realizadas
- Determinar número de servicios comprometidos
- Etc..

## Contramedidas

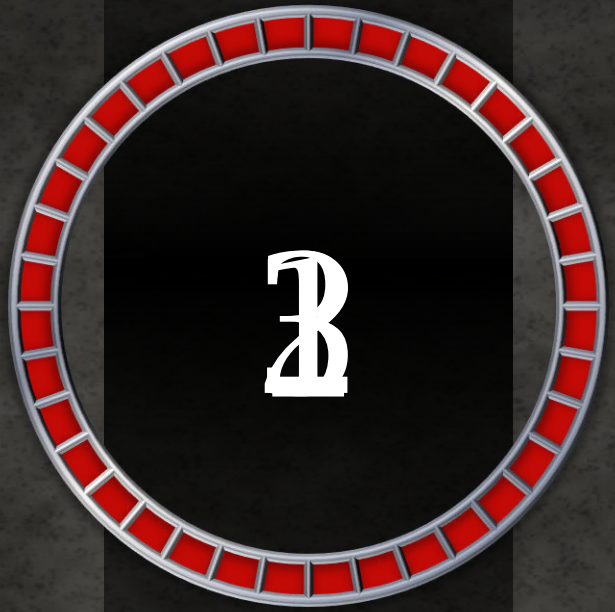
- Desactivar cuentas comprometidas
- Fortificar BBDD
- Advanced Threat Protection
- Data Masking
- Transparent Data Encryption
- Azure Database Auditing
- Azure Locks
- Azure Alerts



# Azure SQL

# Azucar!

- Herramienta de apoyo en auditorías de seguridad basadas en Azure Cloud
  - Desarrollada en PowerShell 3.0
  - Integración con .NET 4.5
- Ventajas
  - Total independencia de módulos de Windows & Azure CMDLets
  - Soporte gubernamental (Azure Government, Azure China, Azure Germany, etc..)
  - Basada en plugins
  - Multi-Hilo
  - Informe de resultados en diferentes formatos



Azúcar!

## Recomendaciones

- Habilita siempre que sea posible las características de seguridad que te ofrezca tu proveedor Cloud
- Habilita autenticación de doble factor para tus usuarios
- Aplica una metodología de acceso a tus recursos (p.ej. Azure Just In time)
- Audita logs de forma regular y aplica alertas basadas en casos de uso
- Despliega políticas globales de seguridad
- Separa Desarrollo y Producción
- Aplica el principio del mínimo privilegio

# Contacto

**Juan Garrido**
Senior Security Consultant
juan.Garrido@nccgroup.trust

# Locations

## North America

Atlanta
Austin
Chicago
Kitchener
New York
San Francisco
Seattle
Sunnyvale

## Europe

Manchester - Head Office
Amsterdam
Antwerp
Basingstoke
Cambridge
Copenhagen
Cheltenham
Delft
Edinburgh
Glasgow
The Hague
Leatherhead
Leeds
London
Luxembourg
Madrid
Malmö
Milton Keynes
Munich
Vilnius
Zurich

## Australia

Sydney