Ciberseguridad para PYMES

Marc Pomar · CTO @ Kirbic

marc@kirbic.com

Conceptos básicos de ciberseguridad

- Intro Cyber AWS

Preguntas comunes

- ¿Es útil tener un antivirus?
- ¿Es segura la red de mi empresa?
- ¿Necesito usar una VPN?
- ¿En caso de ataque que tengo que hacer?

Email

Correo Seguro

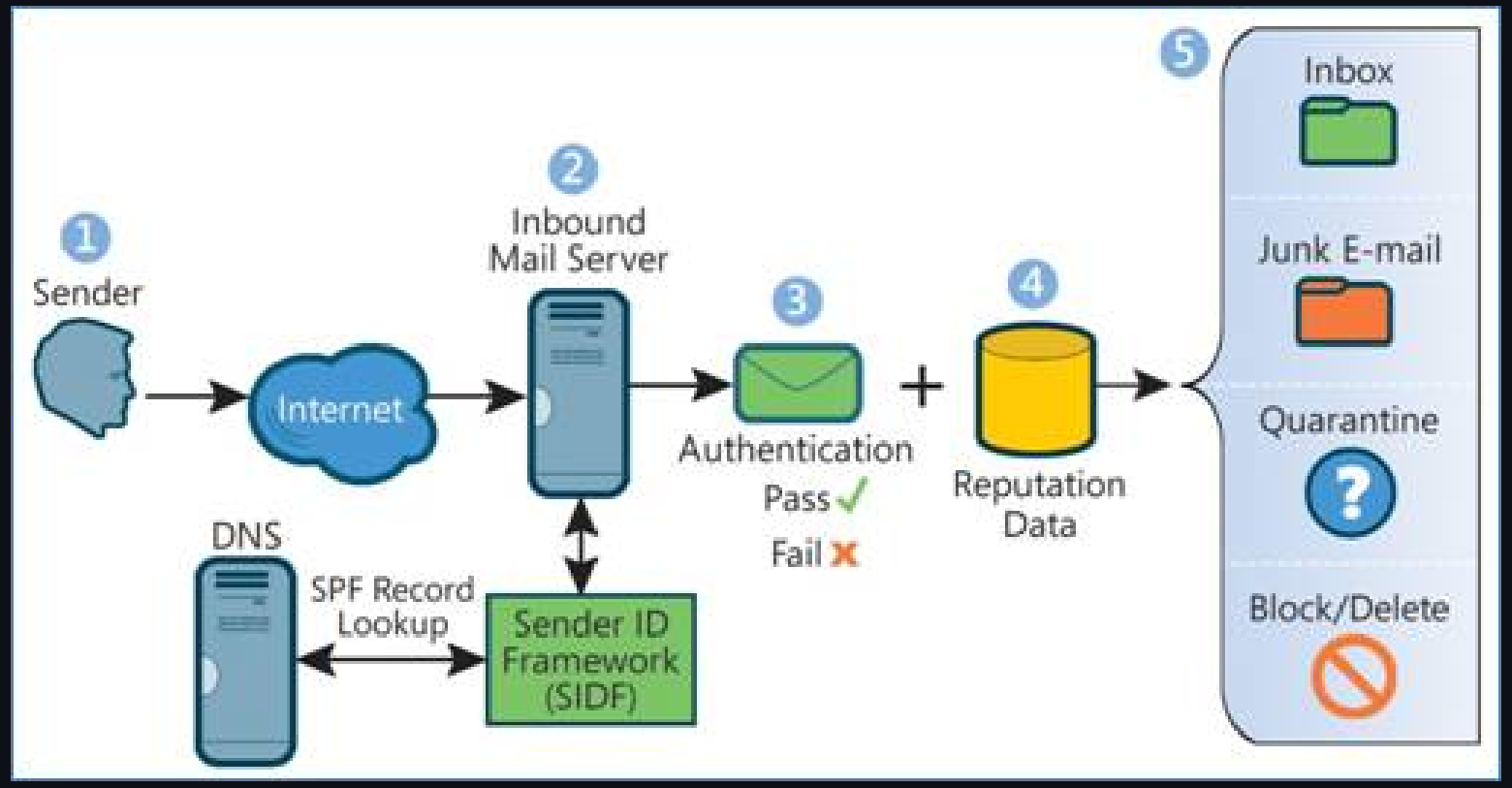
- Checkear servidores DNS de correo en mi dominio

```
dig kirbic.com MX
```

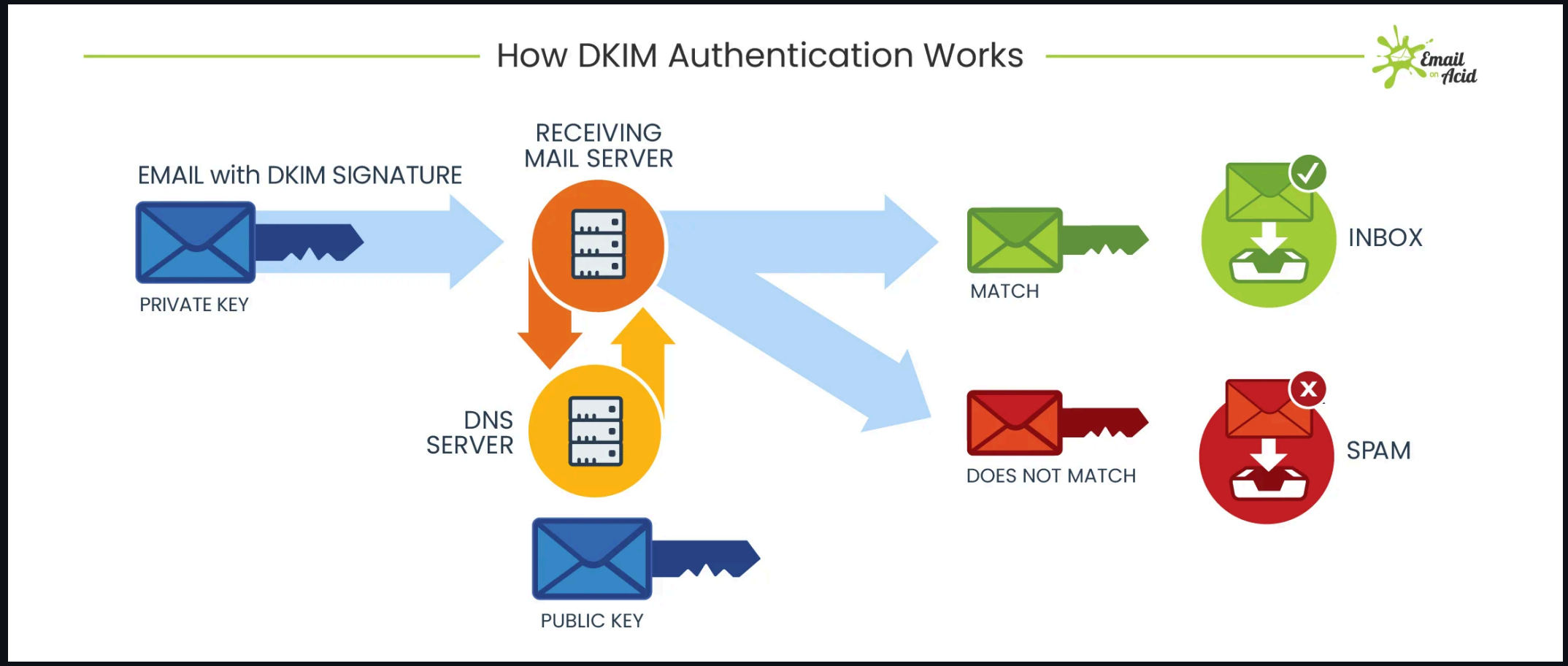
- Blacklists de correo

¿Es mi correo seguro?

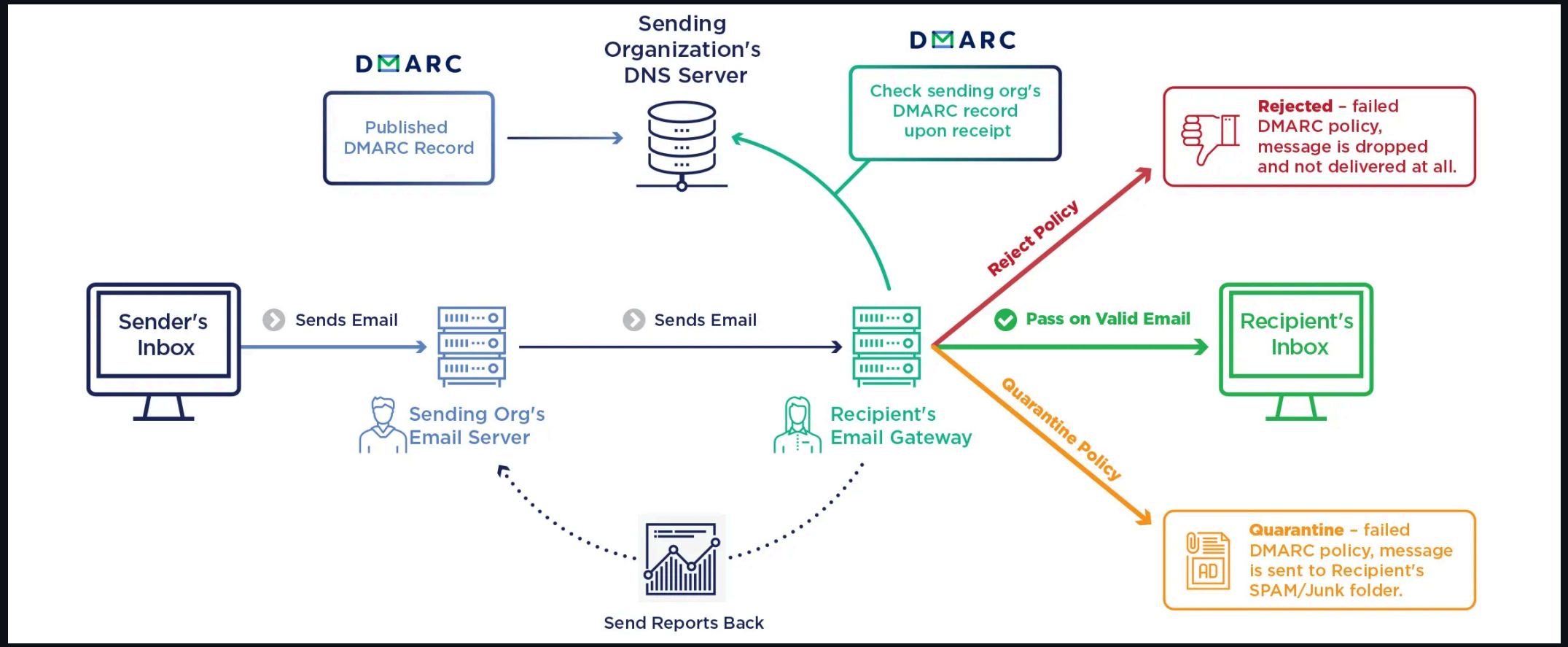
- SFP, verificación de proveedores permitidos



- DKIM: Verificación de claves de correo



- DMARC: Como complemento a SFP y DKIM



Herramientas

- https://www.cloudflare.com/es-es/learning/email-security/dmarc-dkim-spf/
- https://www.diggui.com/
- https://mxtoolbox.com/
- https://dmarcian.com/dkim-inspector/

Ataque: Man in the Middle (MiM)

HOW MAN-IN-THE-MIDDLE ATTACK WORKS

USER

WEB APPLICATION

MAN IN THE MIDDLE

```python
from scapy.all import *

def sniff_and_replace(p):
    if p.haslayer(TCP) and 'example.com' in str(p[IP].src):
        # Interceptamos el paquete y modificamos su contenido
        p[Raw].load = 'Hacked by MIM!'
        sendp(p)

sniff(prn=sniff_and_replace, filter="tcp port 80")
```

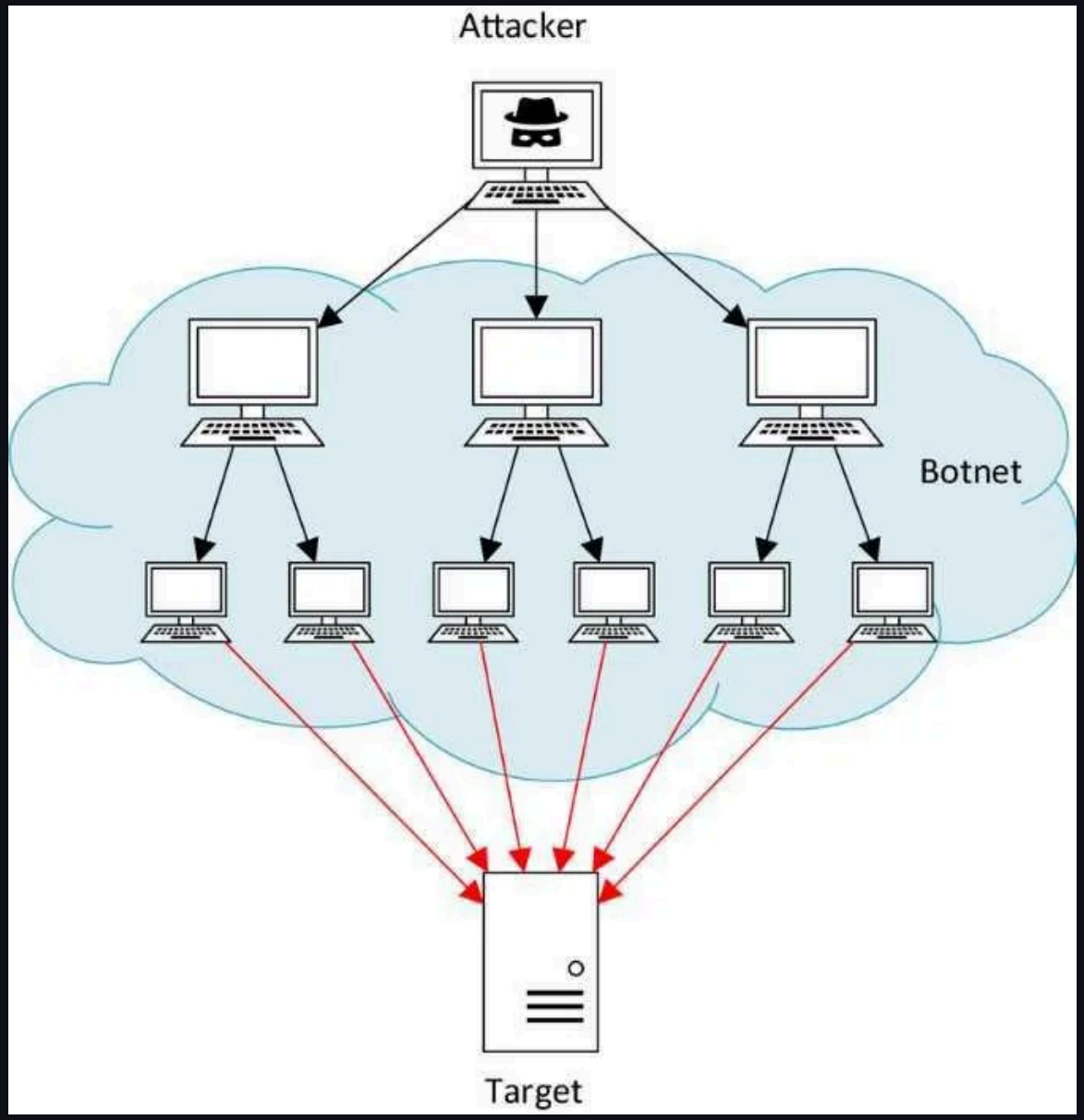
En este ejemplo se utiliza la biblioteca Scapy para capturar paquetes TCP que contengan el dominio example.com en su dirección origen (src). Se intercepta y se modifica su contenido

Ataque: Cross Site Scripting (XSS)

```
import requests

url = "http://example.com/forum.html"
message = "<script>alert('Hacked by XSS!')</script>"
response = requests.post(url, data={"message": message})
print(response.text)
```

Ataques DDoS


Attacker
Botnet
Target

1. **Fail2Ban**: Es un software que protege a los servidores SSH y otros servicios comunes contra ataques bruta mediante el uso de filtros de red y la restricción del acceso basado en reglas. Puede también detectar y bloquear ataques DDoS a través de su integración con iptables.
2. **CSF** (ConfigServer Security & Firewall): Es un paquete de seguridad para Linux que ofrece protección contra ataques como DDoS, brute force, y script kiddies mediante el uso de bloqueos y reglas personalizadas.
3. **Shorewall**: Es una herramienta de red y firewall para Linux. Puede crear políticas de seguridad, permitir el acceso solo a los servicios requeridos y filtrar paquetes innecesarios que podrían ser usados en ataques DDoS.

4. **IPTables**: Es una utilidad de Linux para administrar las reglas de filtro del núcleo en una red, incluyendo el bloqueo de IPs y la aplicación de políticas de seguridad en la entrada, salida y cambio de paquetes de datos.
5. **Mod_Security**: Es un módulo de seguridad web para Apache que protege contra ataques comunes como XSS (Cross Site Scripting), SQL inyección, DDoS, ataques LFI (Local File Inclusion) y muchos más. También puede bloquear IPs específicas que hayan realizado ataques.

Firewall Simple con IPTABLES

```
# Flush todas las reglas existentes en la tabla "filter"
sudo iptables -F

# Agrega una nueva cadena llamada "SSH" a la tabla "filter"
sudo iptables -N SSH

# Agregar una regla para permitir el tráfico entrante del puerto 22 (SSH) y todas las direcciones IP
sudo iptables -A INPUT -p tcp --dport 22 -j SSH

# Agregar una regla para denegar el tráfico entrante en cualquier otro puerto
sudo iptables -A INPUT -m state --state NEW -j DROP

# Establecer la acción por defecto de la cadena "SSH" como permitir pasar el tráfico
sudo iptables -A SSH -j ACCEPT
```

Servidor Web Seguro

ModSecurity es un software de protección web que analiza y filtra las solicitudes HTTP entrantes a tu servidor web, proporcionando una protección contra ataques y vulnerabilidades. Permite personalizar las reglas de seguridad para adaptarse a tus necesidades específicas y ayuda a reducir el riesgo de amenazas en línea.

```
sudo apt-get install libapache2-modsecurity
```

Cifrado HTTPS

Instalar Certbot

```
sudo apt-get install certbot python3-certbot-nginx
```

Solicitar certificado

```
sudo certbot certonly --webroot -w /var/www/html -d "www.example.com" -d "example.com" -m marc@kirbic.com
```

Configurar Servidor Web Nginx

```
ssl_certificate /etc/letsencrypt/live/example.com/fullchain.pem;
ssl_certificate_key /etc/letsencrypt/live/example.com/privkey.pem;
include /etc/letsencrypt/options-ssl-nginx.conf;
ssl_dhparam /etc/letsencrypt/ssl-parameters.pem;
```

Ejemplo

Sistemas IDS: Suricata

Prevención

- Firewall: Linux iptables, Mikrotik, etc
- WAF
- Sistemas IDS
- Auditoria de ciberseguridad

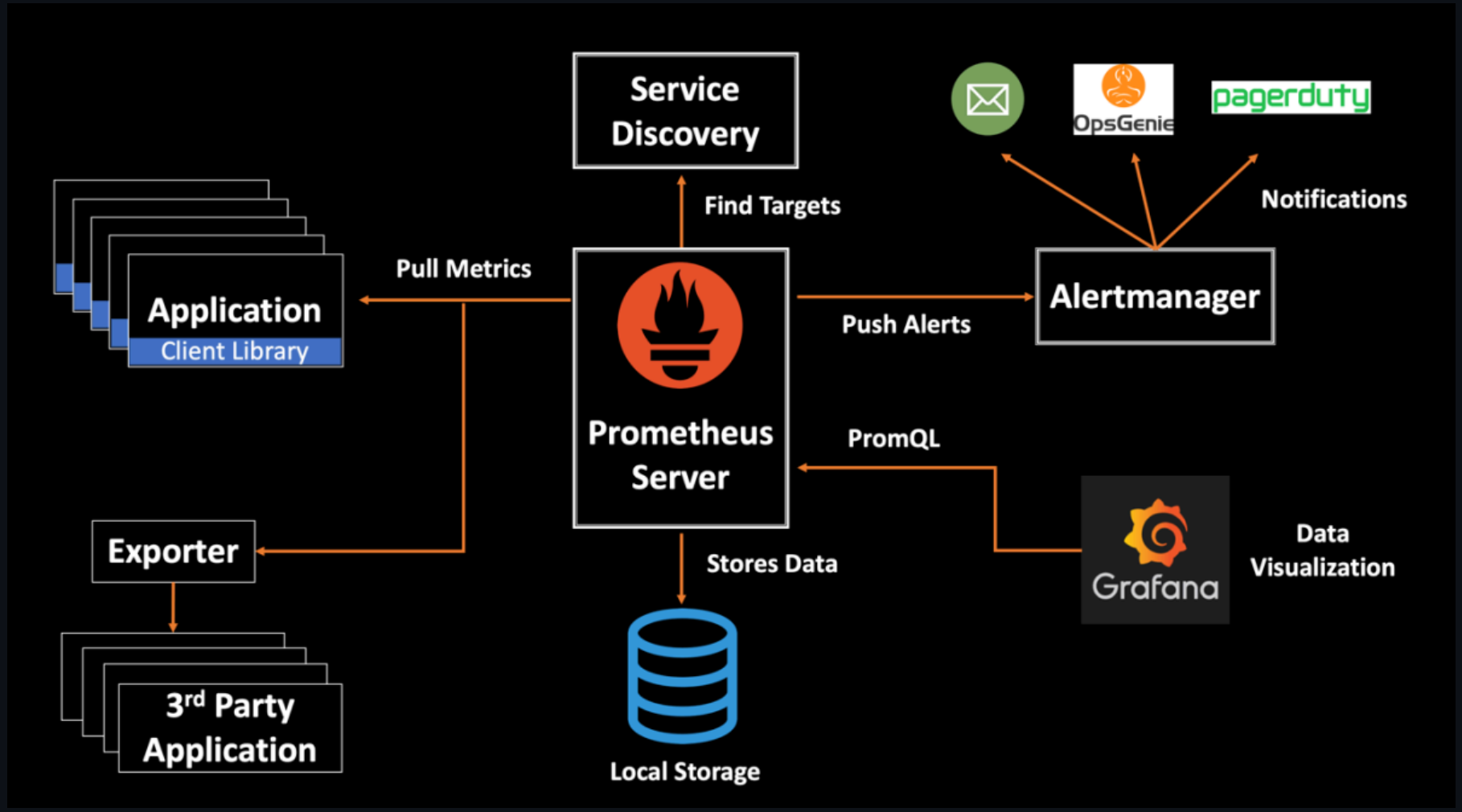
Backups

> Se que voy a perder información, pero ¿cuanto estoy dispuesto a perder?

- Backups en varias ubicaciones
- Hacer pruebas de recuperación
- Medir tiempos RPO y RTO

Observabilidad y Monitorización

Prometheus


Service Discovery
Find Targets
Pull Metrics
Application
Client Library
Prometheus Server
Push Alerts
Alertmanager
Notifications
OpsGenie
pagerduty
PromQL
Grafana
Data Visualization
Exporter
3rd Party Application
Stores Data
Local Storage

Sentry