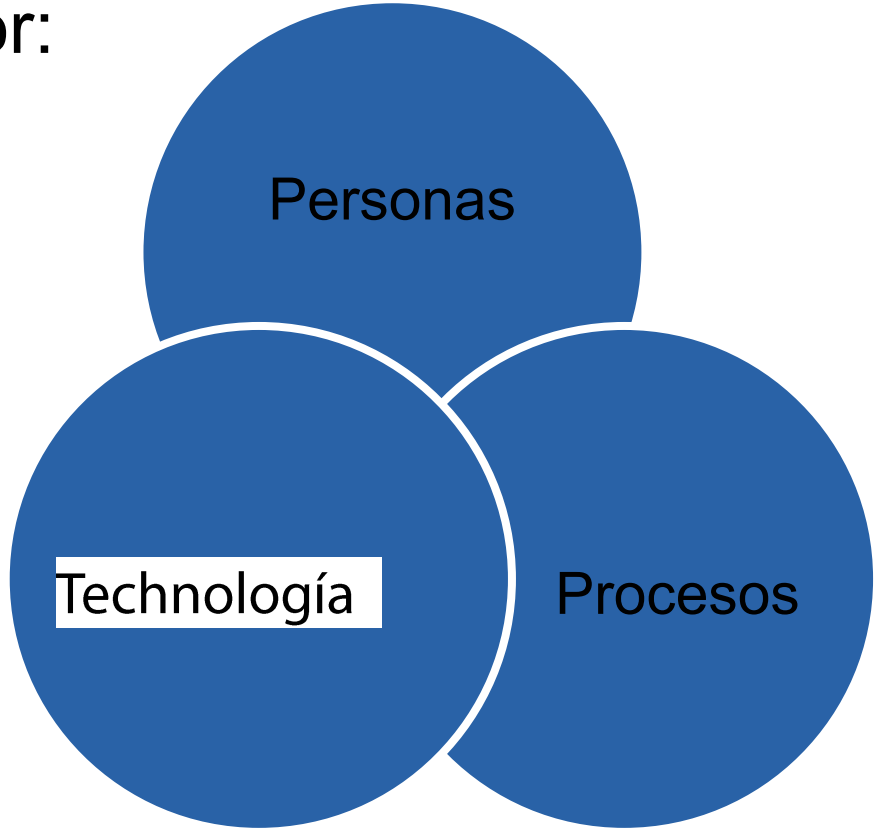
Monitoreo Continuo bajo GDPR

Darragh Delaney
Director of Product Management

NETFORT
know your network

GDPR y Tecnología

El GDPR, como cualquier actividad de negocio está controlado por:



Pero la tecnología tiene un papel

La Brecha de Seguridad en Talk Talk* 2016
(*operador britanico)

- Talk Talk sufrió una multa récord en 2016 por la Oficina del Comisionado de Información del Reino Unido

  "El fallo de TalkTalk de implantar las medidas más básicas de ciberseguridad permitió a los hackers penetrar los sistemas de TalkTalk con facilidad".

  "A pesar de su experiencia y recursos, cuando se trataba de los principios básicos de la ciberseguridad, TalkTalk fue encontrada débil "

- La multa de £400k (€ 440.000) se aplicó por el fallo de no tomar las medidas adecuadas de protección (las había pero aún eran pocas)

- Si se aplicase la misma multa bajo GDPR esta equivaldría £59 millones (€ 64,9 millones) (4% de sus ingresos)

- Con el GDPR se esperan multas más duras

Consciente de los riesgos

- Destrucción, pérdida, alteración, difusión no autorizada de datos personales sea accidental o illegal.

- Depende de una buena ejecución de las Operaciones de Seguridad (SecOps)
  - Parcheo
  - IAM (Gestion de identidades y accesos)
  - Cifrado
  - Monitorización, etc…

- ¿Ha evaluado el impacto de los datos destruidos por WannaCry?

Tecnología GDPR

La monitorización continua es vital para construir y mantener redes seguras – Arquitectura SOAPA

- Monitorizar el acceso de usuarios a los datos
- Informes Forenses
- Protocolos utilizados
- Exfiltración de datos
- Detección de Ransomware

NetFort proporciona Monitoreo Continúo

- Pasivo
- Para todos los dispositivos (sin agentes ni software de Endpoint)
- Dentro de la red
- Usuarios, aplicaciones, datos, inventario

Dos casos de uso importantes

1. Saber lo que esta en tu red

   "Sólo puedes proteger lo que conoces"

   LANGuardian es excelente para:

   - Auditar accesos a datos no estructurados
   - Saber qué aplicaciones dispositivos y usuarios hay en la red
   - Identificar qué protocolos se utilizan (SSL1.0, SMBv1)

Dos casos de uso importantes

2. Saber lo que está pasando en tu red

- ¿Quién está accediendo a los datos?
- ¿Ha habido cambios en el inventario?
- ¿Ha ocurrido algún comportamiento anómalo?
- ¿Ha habido conexiones a servidores externos?

Breve Demo

- Inventario de datos no estructurados (ficheros y carpetas)
- GeoIP y connexiones externas
- Detección de Ransomware
- Detección de protocolos débiles (SMBv1, SSL1.0, SHA1)