Ciber riesgos en la transformación digital

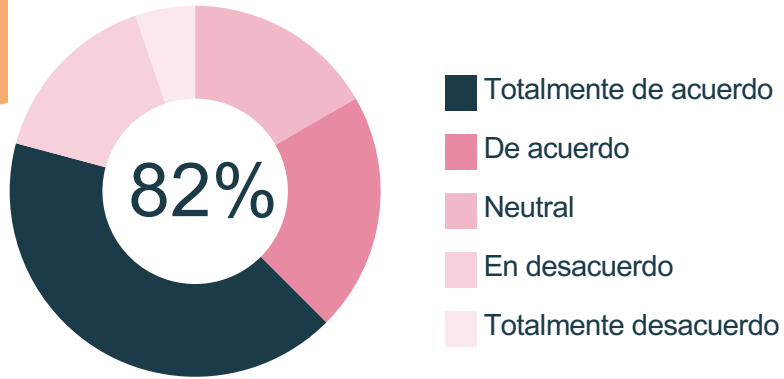
... de la amenaza a la oportunidad

minsait

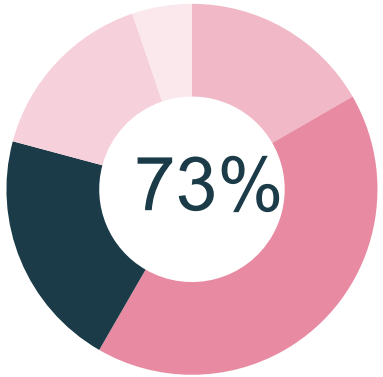
An Indra company

Contexto actual

El **82%** de los profesionales de Riesgos y Seguridad, informan que sus organizaciones consideran las **Brechas de Seguridad** como un **riesgo de negocio** en lugar de un riesgo de TI

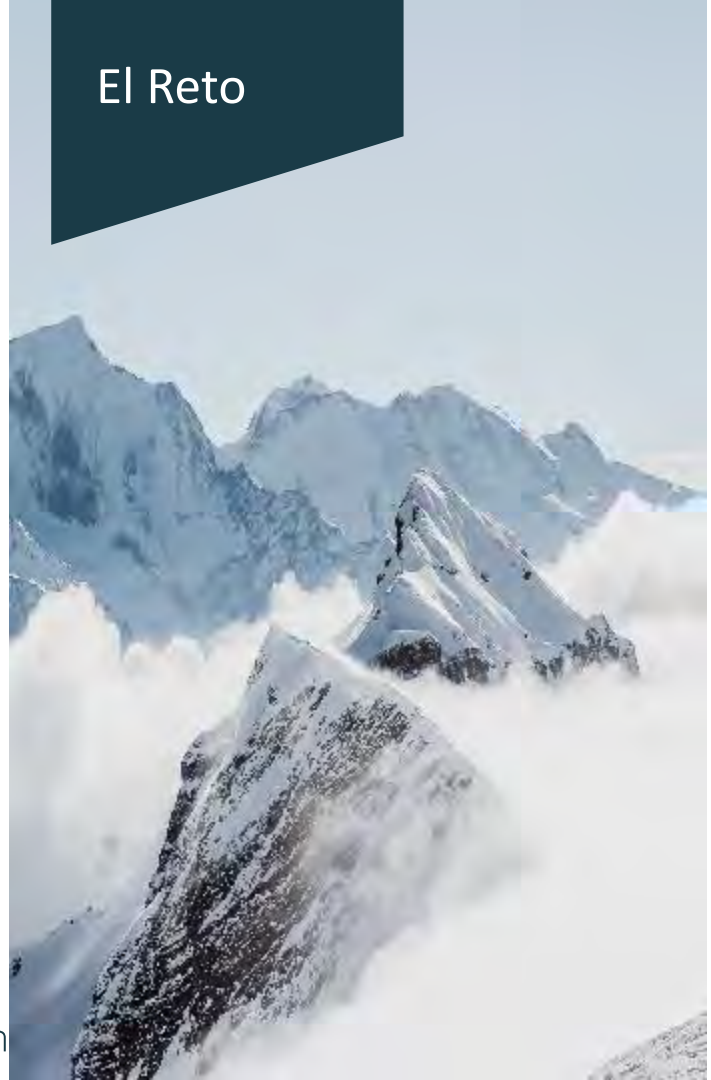


El **73%** de los encuestados concuerda en que la relación entre la Seguridad de TI y el Riesgo de Negocio puede ser **difícil de coordinar**



Fuente: ESG Custom Research, Cybersecurity and Business Risk Survey, March 2018

El Reto



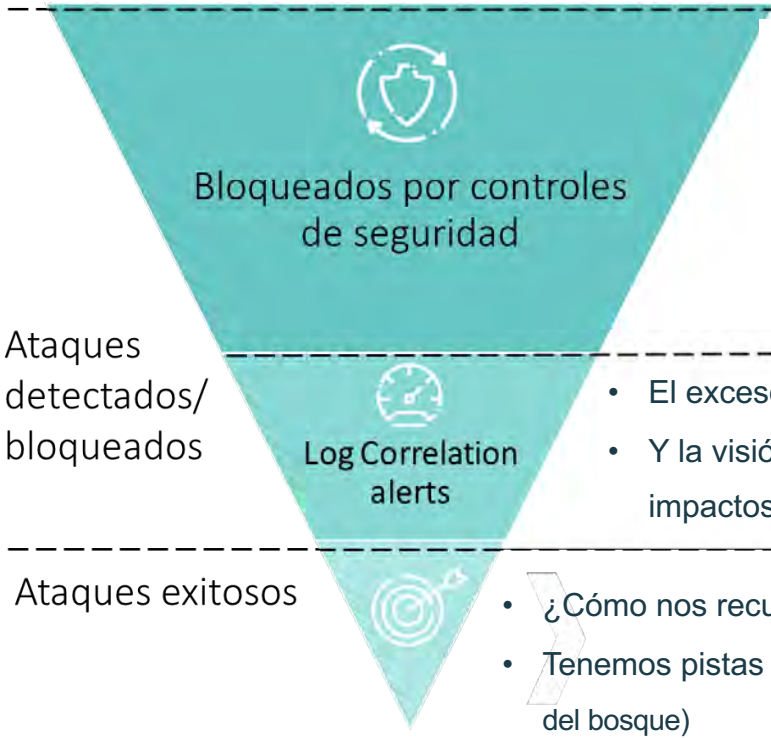
Mi organización invierte en seguridad:

- SIEM, IDS, FW…
- Auditoria.
- Risk Auditoria.
- Gestion de vulnerabilidades.
- Concienciación.
- Pentesting.
- Y muchos más controles… y mucho más gasto.

… aun así, he tenido un incidente…

¿Por qué?

Capacidades de respuesta y detección con un enfoque de riesgos, es la clave para minimizar el nivel de exposición



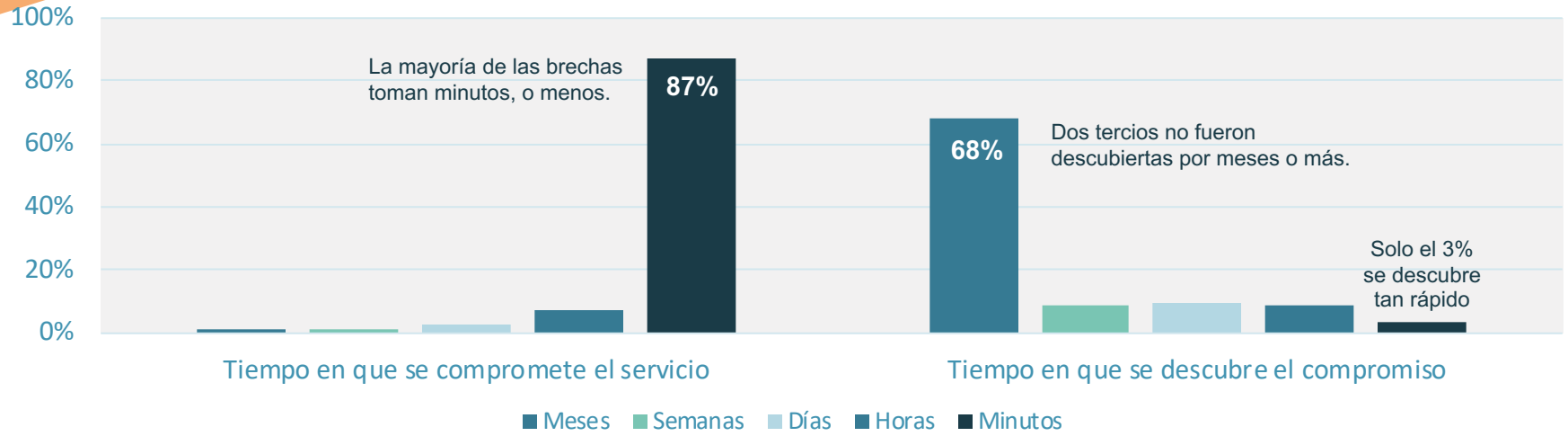
- No se tiene identificada "*la joya de la corona*"
- Dependencia de tecnología basada en firmas
- Respuesta tardía

- El exceso de información desinforma (falsos positivos)
- Y la visión de riesgos? ¿Conocemos los posibles impactos?

- ¿Cómo nos recuperamos?
- Tenemos pistas o historial de los eventos? (solo vemos parte del bosque)

La importancia de incrementar las capacidades de respuesta y detección de incidentes de Ciberseguridad

Las cifras actuales de tiempos elevados de detección y tiempos mínimos de compromiso son factores importantes en la definición de una **estrategia de Ciberseguridad**



En muchas ocasiones no es la organización quien detecta el incidente, es común que sea detectado por un tercero, como una agencia de gobierno, un socio de negocio o inclusive algunas brechas son detectadas por clientes.

Fuente: 2018 Data Breach Investigations Report (Verizon)
https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

Dominios críticos para gestionar el riesgo digital

Gestión de riesgos

Operaciones de seguridad

Acceso a usuarios

¿Qué monitorear?

Sin una estrategia correctamente definida, no sabemos que proteger

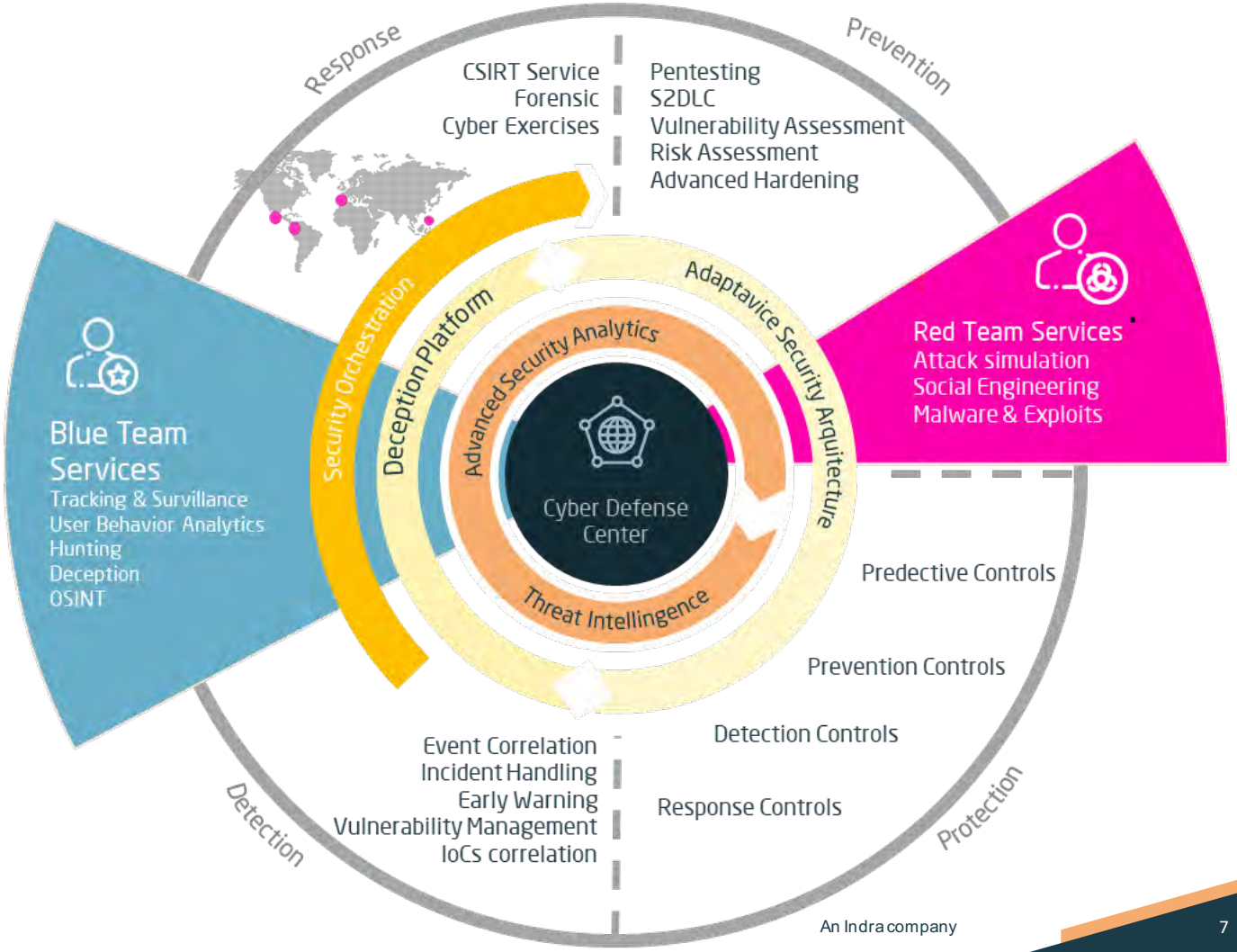
¿Cómo responder?

Confiemos en los terceros que cuentan con capacidades de respuesta y detección

¿Quién lo hizo?

El control de acceso y gestión de identidades es fundamental para prevenir la fuga de información

Estableciendo un framework de Ciberseguridad



Erik Moreno Sánchez

Ciberseguridad México

eemorenos@minsait.com

minsait

An Indra company