SERVICE & RISK MANAGEMENT FORUM 2011

Gestión del riesgo del negocio con inteligencia de seguridad de la información

Roque C. Juárez
Consultor de Seguridad de la Información

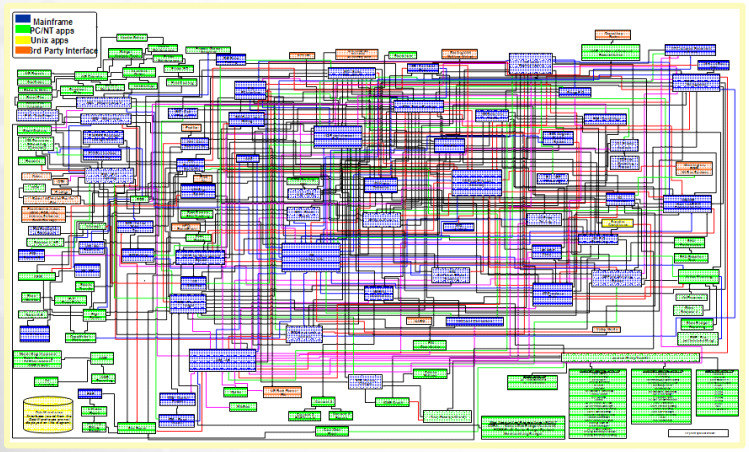
Agenda

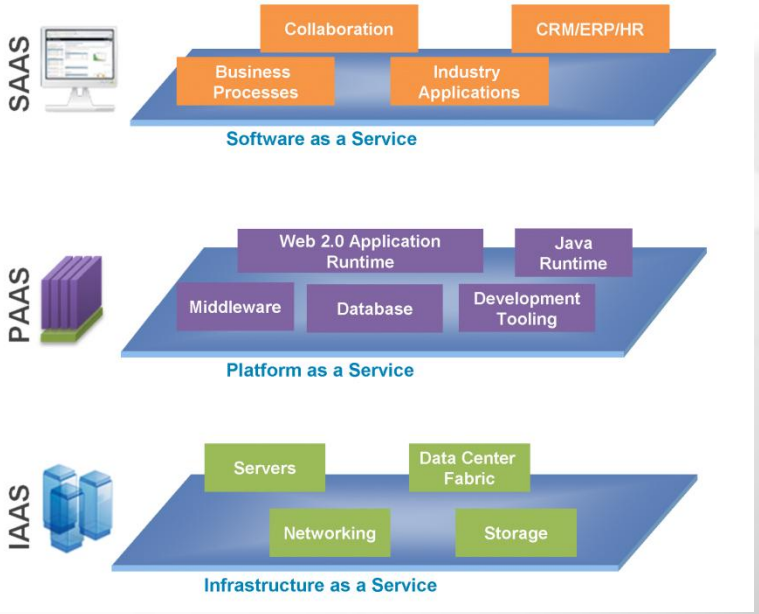
- La seguridad no fué un proyecto
- Caminando hacia la gestión de seguridad
- Seguridad más inteligente
- Consideraciones finales

La seguridad no fué un proyecto

La seguridad no fué un proyecto

- La operación está controlada y dentro de los niveles de riesgo.





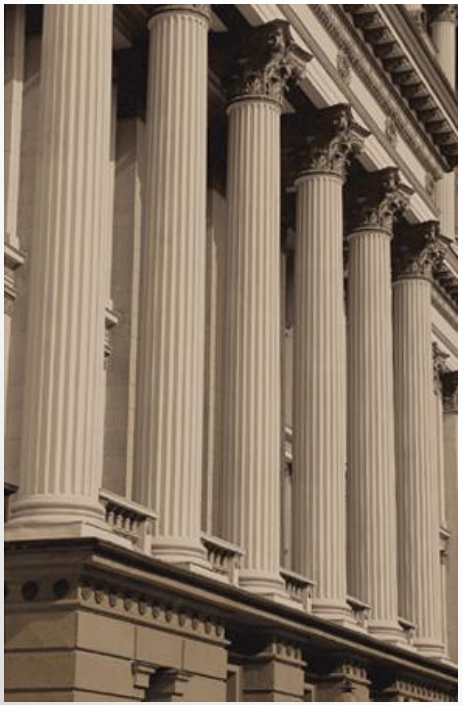
¿estamos solamente para operar?

La seguridad no fué un proyecto

- El marco normativo de seguridad se ha escrito pero no se implementa, y pocas veces se mide.

La seguridad no fué un proyecto

- Se cumple con las regulaciones de la industria… por nuevas que estas parezcan.



ifai

CNBV
COMISION NACIONAL BANCARIA Y DE VALORES

COBIT
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

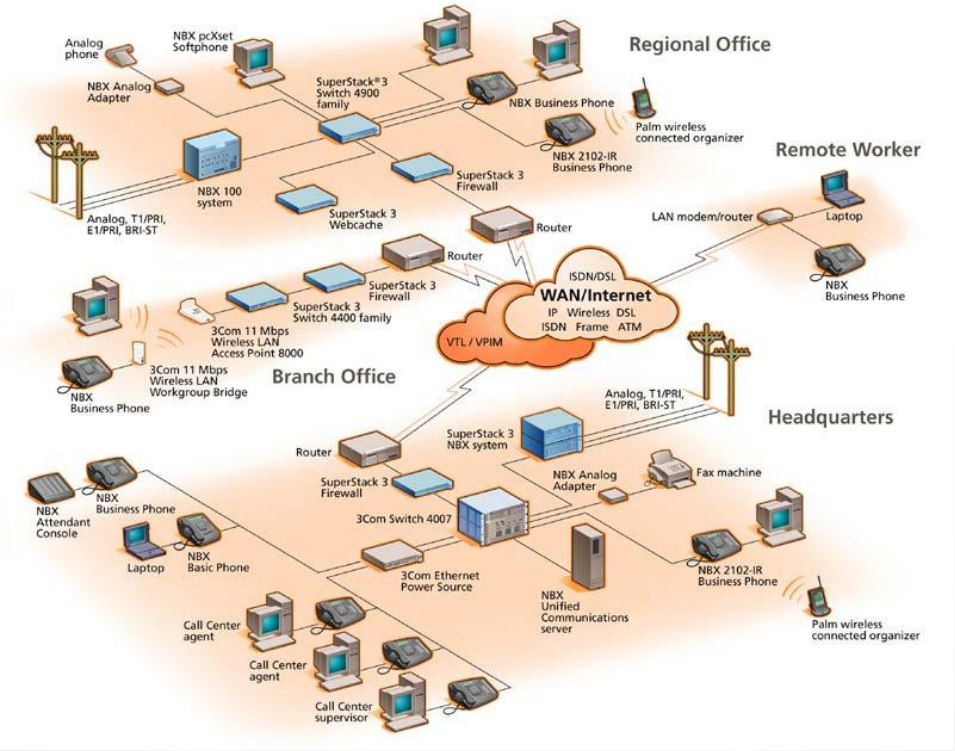
ITIL®

ISO

PCI Security Standards Council

La seguridad no fué un proyecto

- Esquema de aseguramiento en diversas capas de la ***infraestructura.***



La seguridad no fué un proyecto

- Se ejecutan ejercicios de análisis de riesgos y estrategia de seguridad...

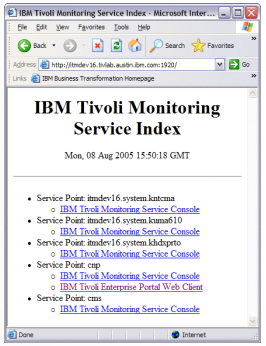
La seguridad no fué un proyecto

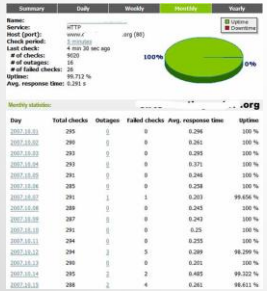
«La seguridad de la información tiene un contexto y medición operativos»

Caminando a la gestión de seguridad

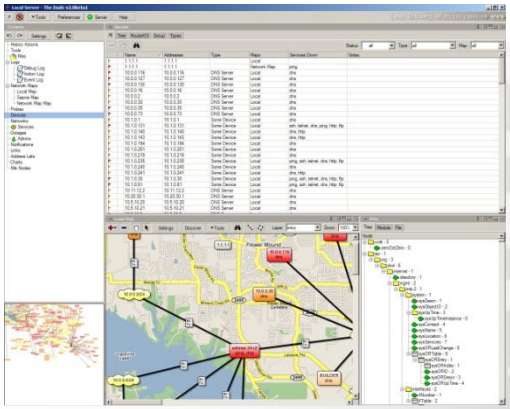
Caminando a la gestión de la seguridad

- Colectar la mayor cantidad de información de la infraestructura de seguridad y de TI.



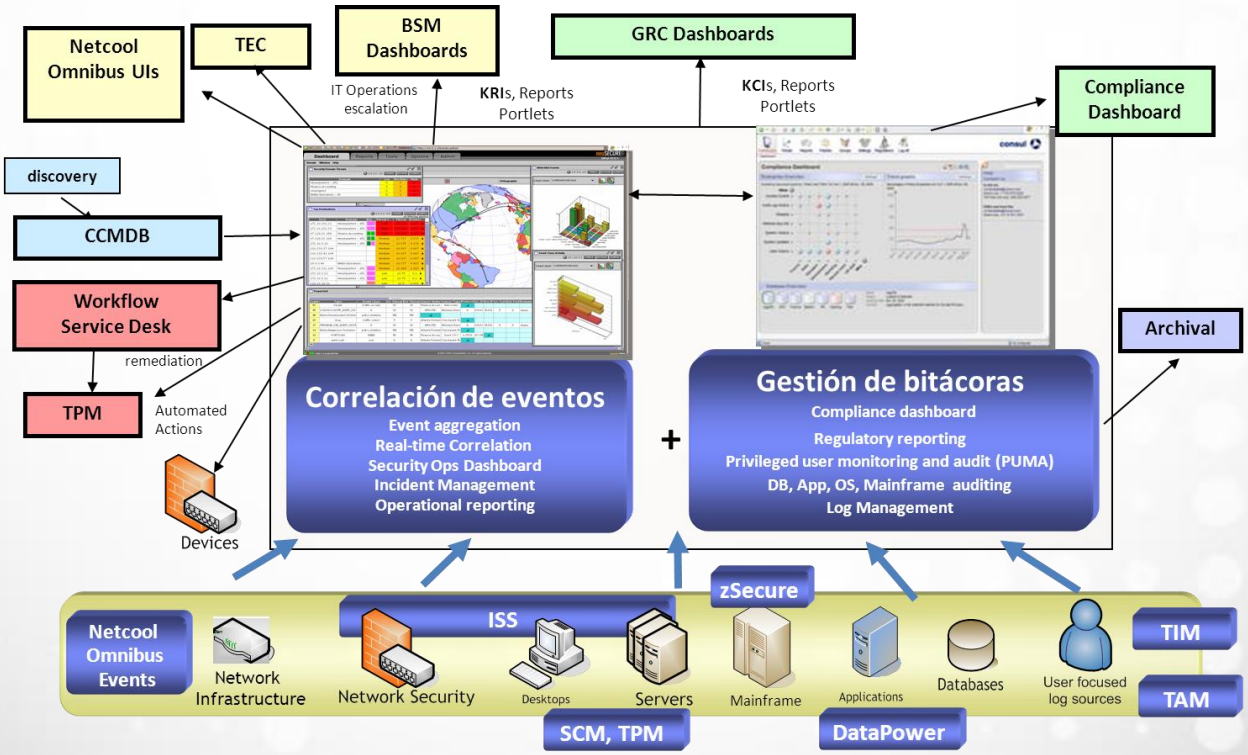


Log Management



Caminando a la gestión de la seguridad

- Correlacionar la información de las pruebas de seguridad y la operación.



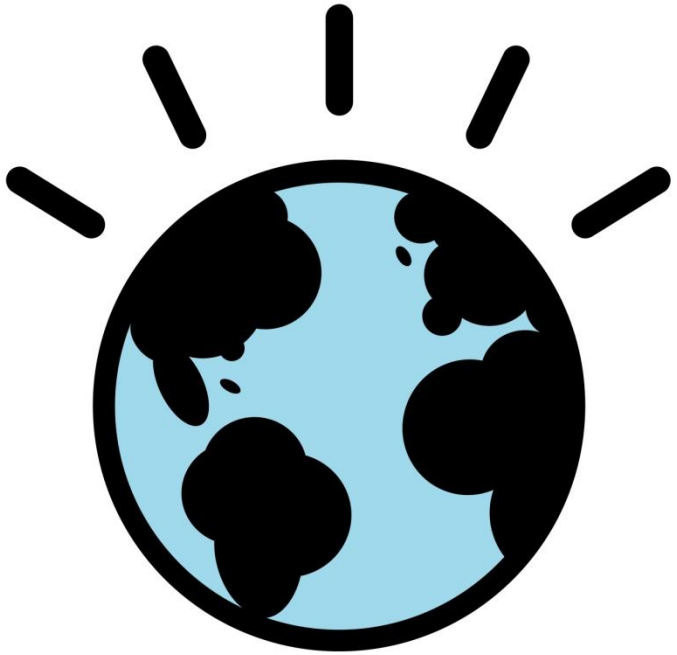
Caminando a la gestión de la seguridad

- Definir cursos de acción para tratamiento de incidentes.

Caminando a la gestión de la seguridad

- Preservar configuraciones, reportes y resultados de brechas de seguridad en la infraestructura.

Seguridad más inteligente



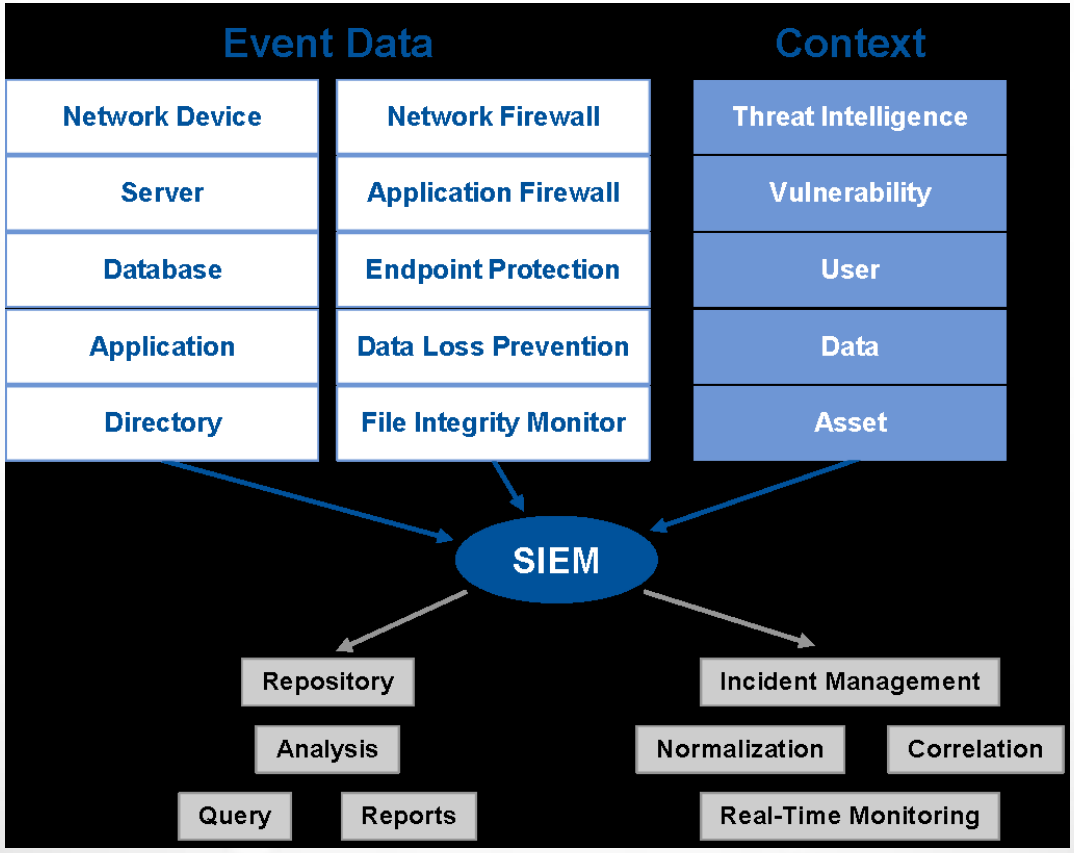
Seguridad más inteligente

- ¿Qué es la inteligencia?

1.f. Capacidad de entender o comprender.
2.f. Capacidad de resolver problemas.
5.f. Habilidad destreza y experiencia.

Seguridad más inteligente

- El modelo actual de SIEM tiene alcances limitados.

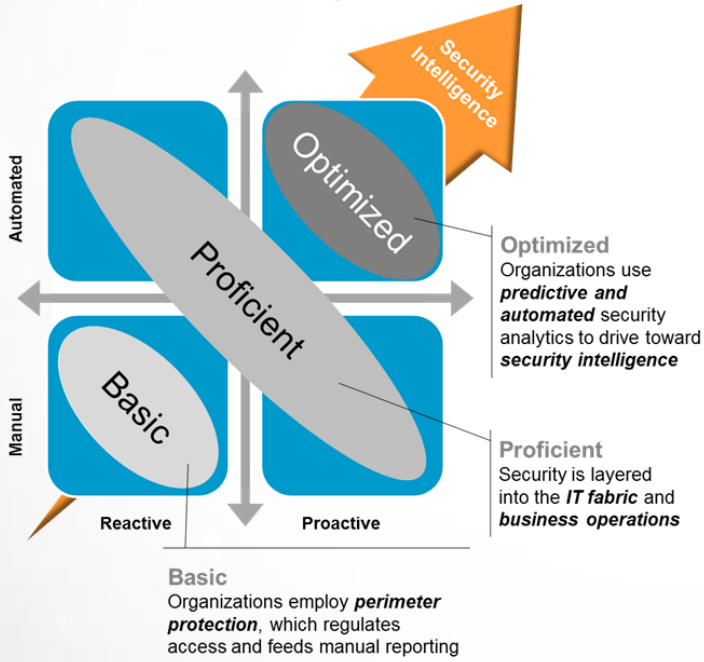


Seguridad más inteligente

- La inteligencia de seguridad debe basarse en:
  - Integración de la información.
  - Correlación de los eventos.
  - Búsquedas dinámicas multidimensionales
  - Contextualizar el estado de seguridad.
  - Respuesta automática

Seguridad más inteligente

- Las organizaciones requieren una visión inteligente(dinámica) de su nivel de seguridad:



IBM Security

Organizations need a new approach to security, one which leverages intelligence in order to keep pace with innovation

IBM Security drives change from a point product strategy to an integrated enterprise security framework, based on key elements that allow for:

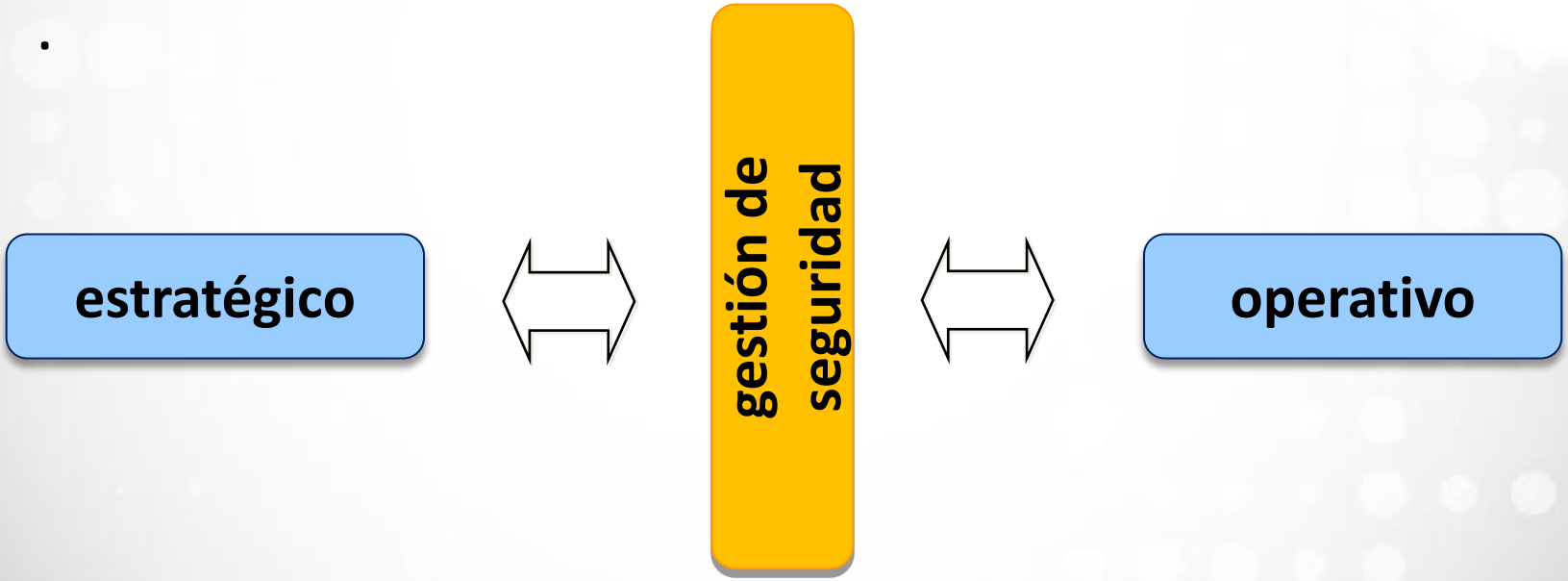
- Translation of data into actionable insights
- Reduced business cost and risk
- Innovation with agility and confidence
- Continuity of operations

Security intelligence highlights at IBM

- 21B events/day correlated in MSS (leveraging Cognos)
- Advanced security analytics with InfoSphere Streams
- SPSS Predictive Analytics solving insider threat
- Hybrid scanning capabilities from Rational AppScan
- Identity Governance to build integrated access processes

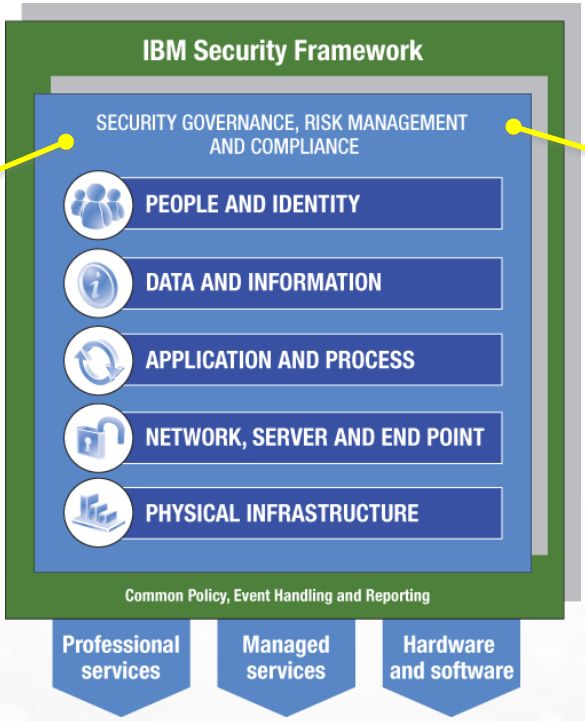
Seguridad más inteligente

- La seguridad de la información se establece de forma práctica con tres componentes fundamentales:
- .



Seguridad más inteligente

- El portafolio de IBM crece para atender estos requerimientos de los clientes.

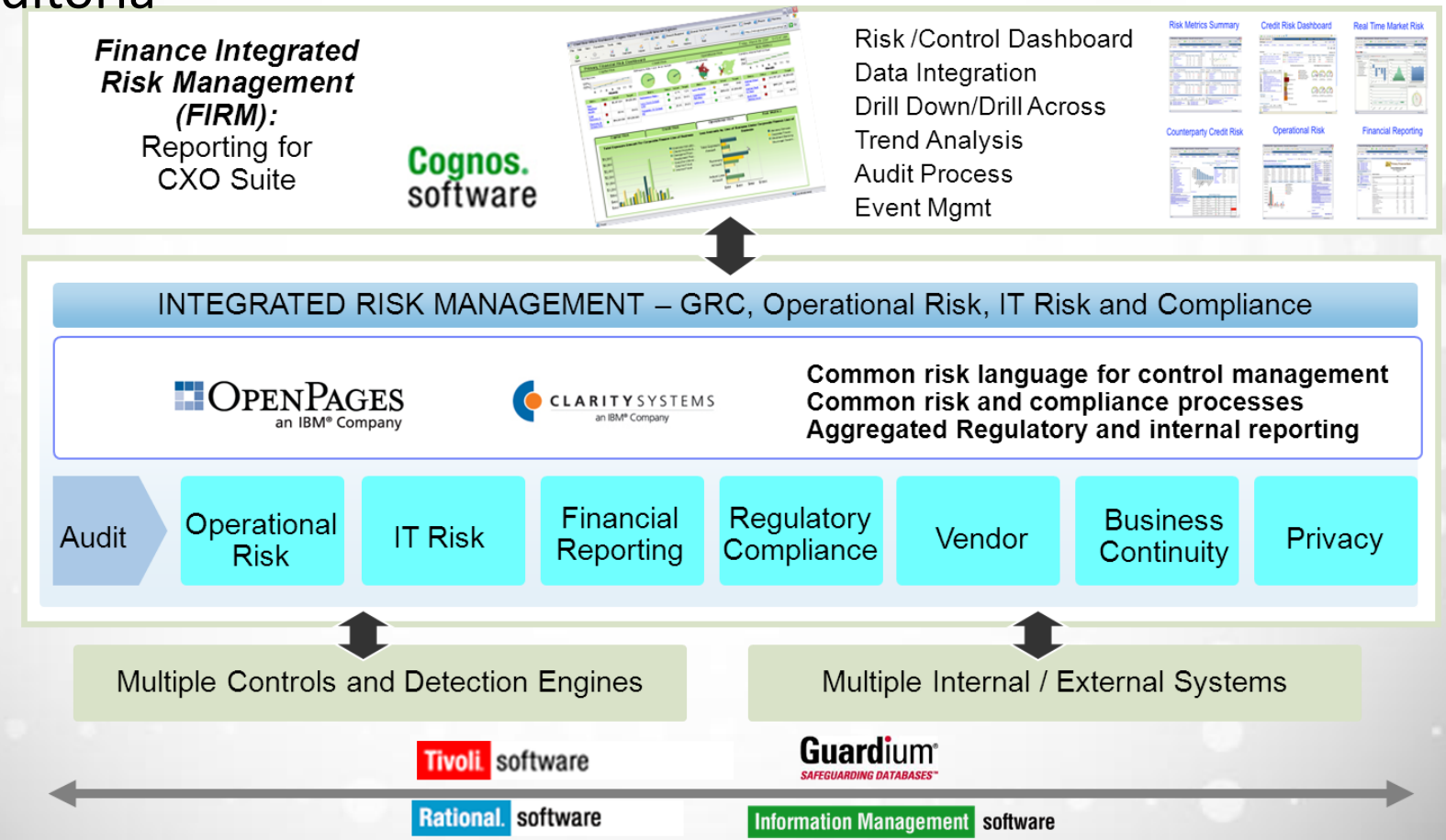


OpenPages an IBM® Company

1Q Labs Total Security Intelligence

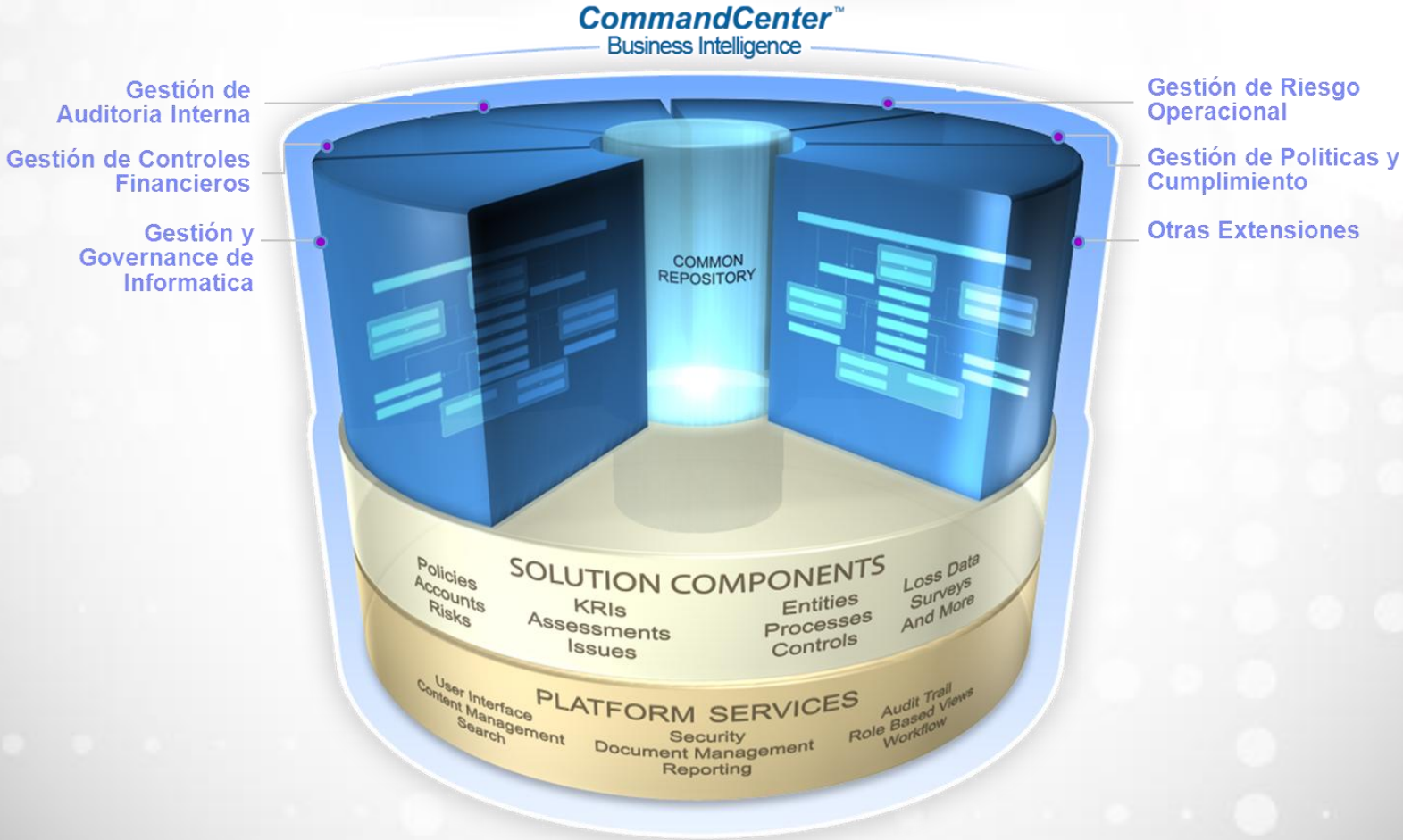
Seguridad más inteligente

- Open Pages – Riesgo operacional, Riesgo TI, Controles Financieros, Auditoría



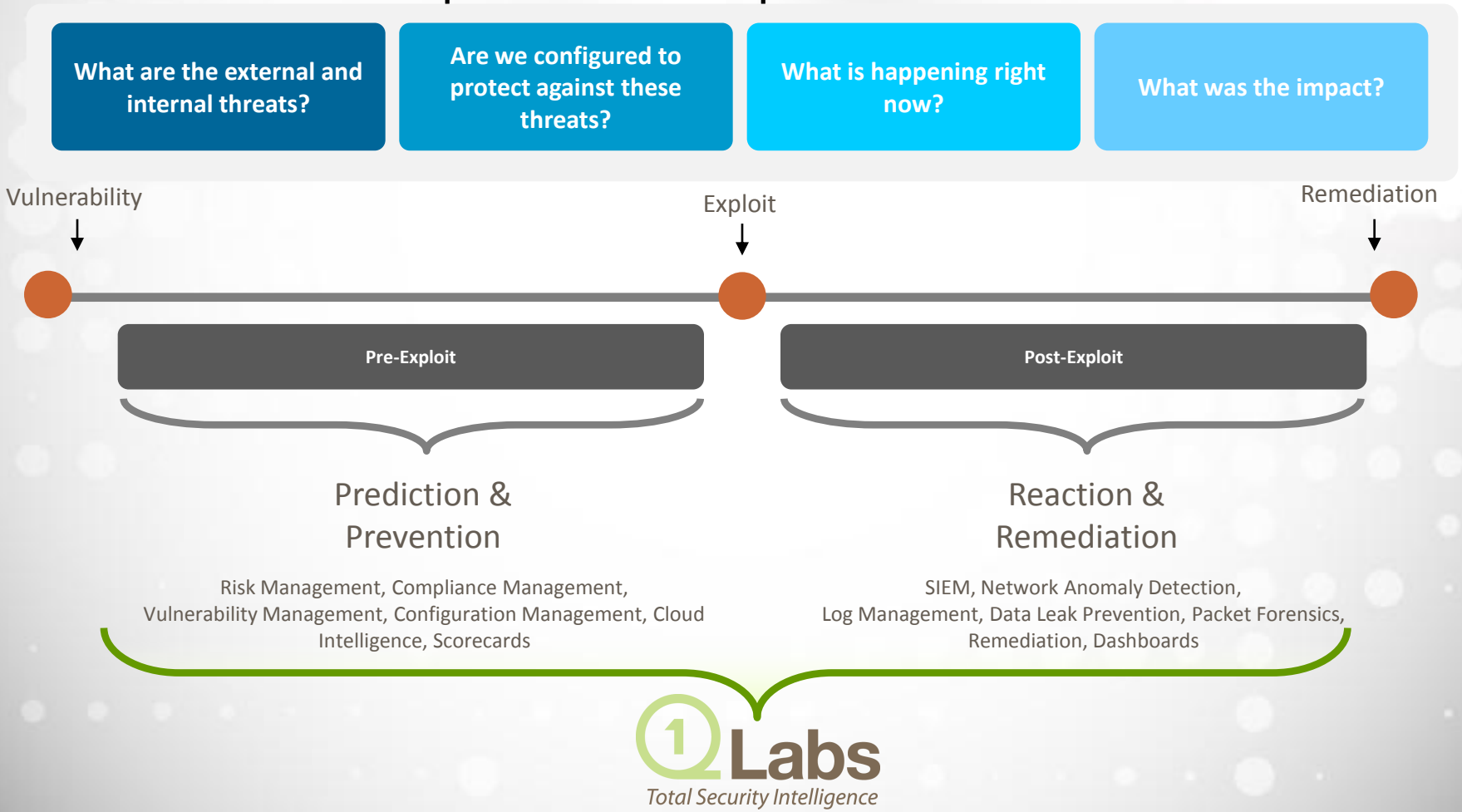
Seguridad más inteligente

- Open Pages – Permite la gestión integrada de riesgos



Seguridad más inteligente

- Q1 Labs – Se amplia el ciclo de protección.

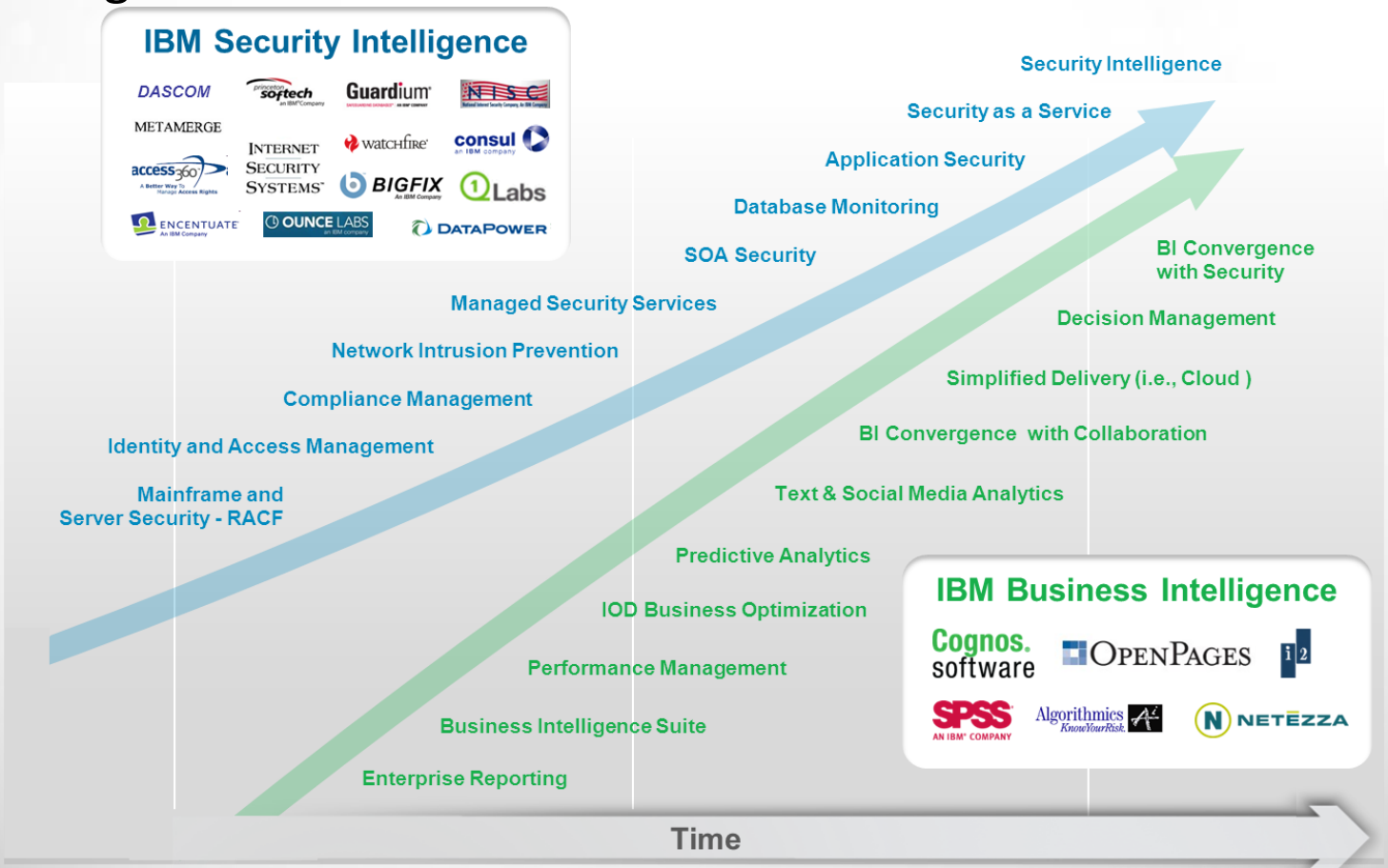


Seguridad más inteligente

- Q1 Labs – Se amplia el ciclo de protección.

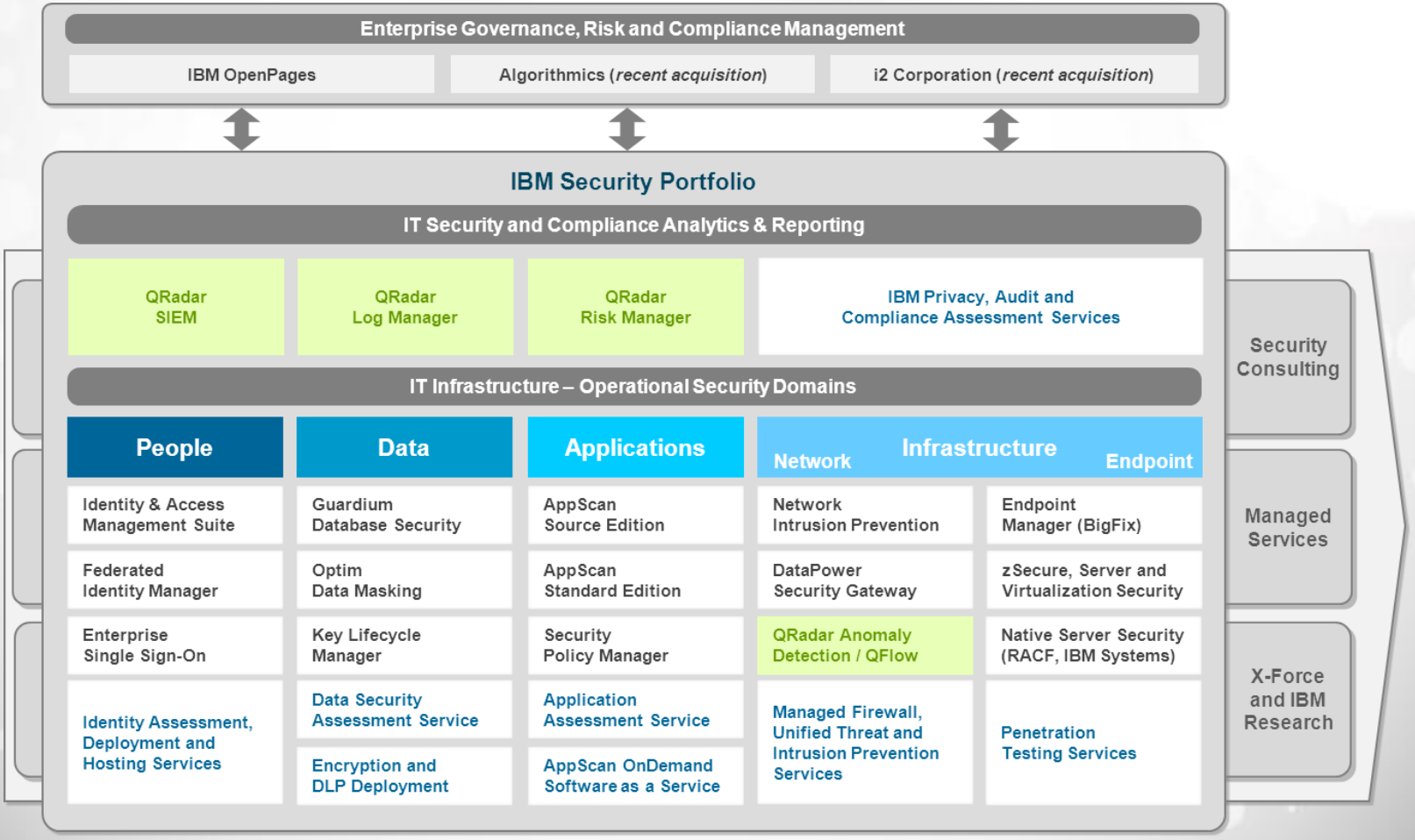
Seguridad más inteligente

- Con IBM se crean capacidades paralelas de inteligencia de seguridad y de negocio.



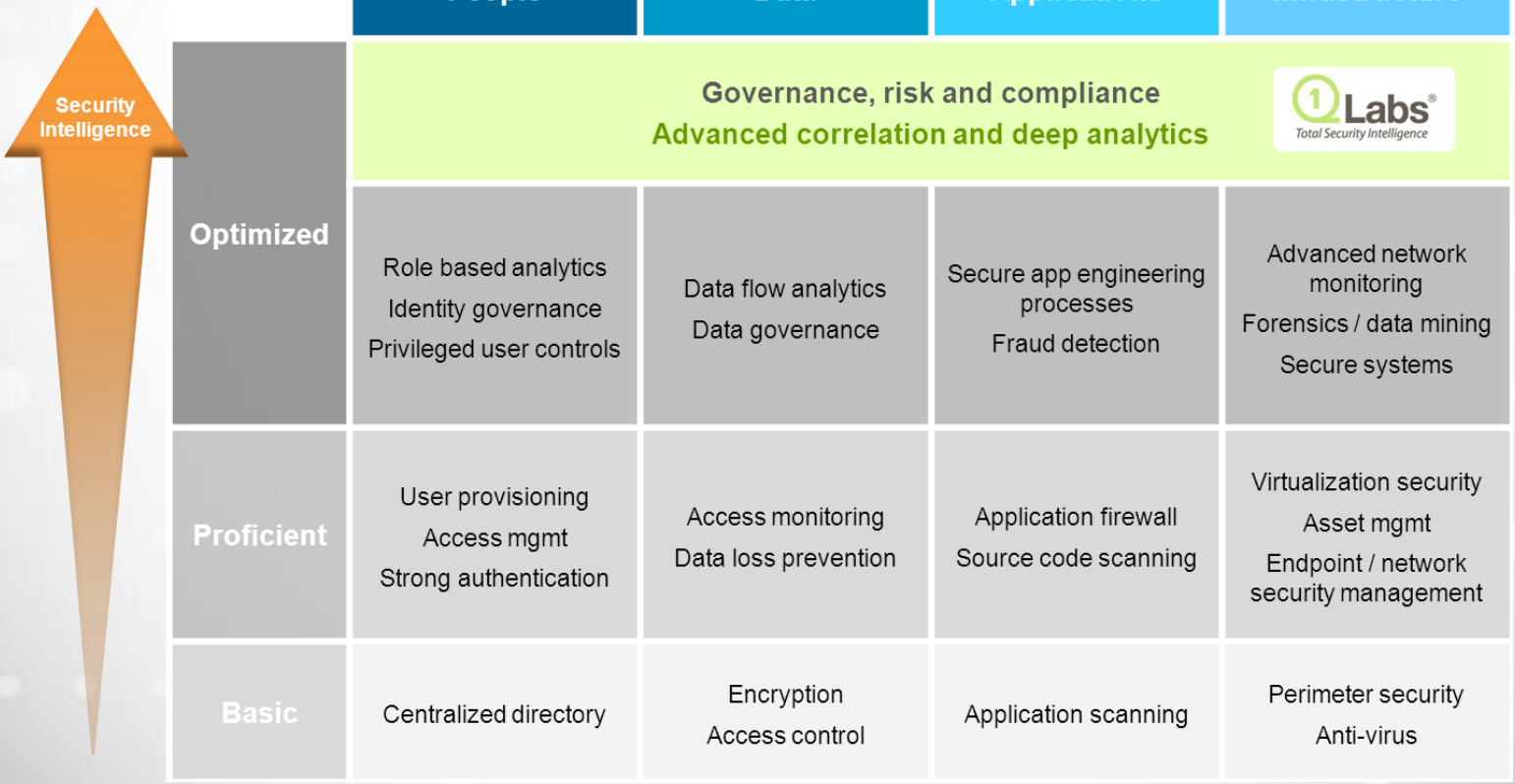
Seguridad más inteligente

- El portafolio más completo de seguridad de la información.



Seguridad más inteligente

- Se aumentan las capacidades de gestión y visibilidad en tiempo real sobre gestión de amenazas, vulnerabilidades y riesgos.



Consideraciones finales

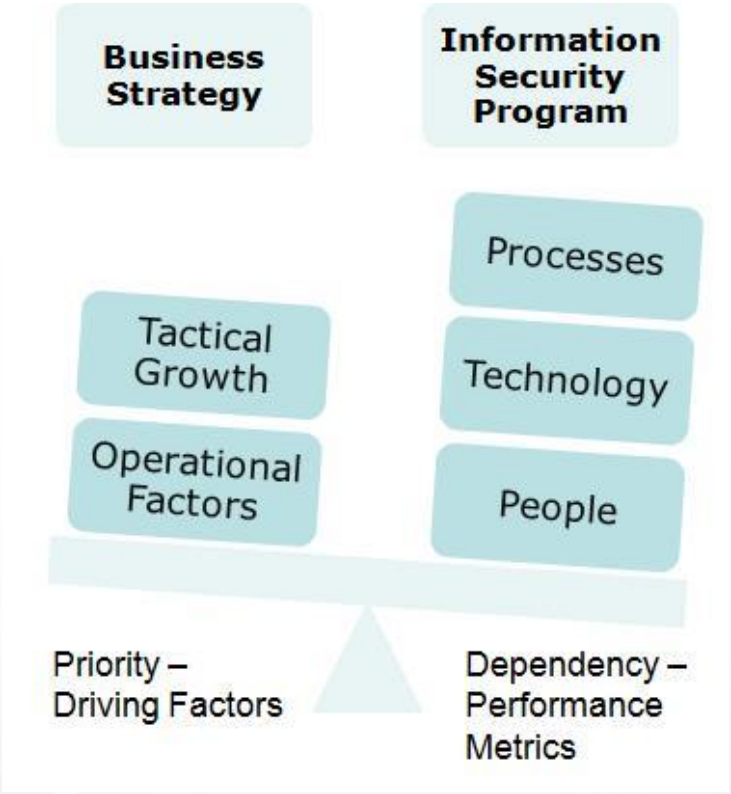
Consideraciones finales

- Es fundamental impulsar los proyectos de SIEM y correlación de eventos.

Son la materia prima para inteligencia de seguridad.

Consideraciones finales

- Es oportuno definir las métricas de seguridad con visión de servicio.



Consideraciones finales

- Se facilita la preservación de evidencias y revisiones de cumplimiento.

SERVICE & RISK MANAGEMENT FORUM 2011

IBM

La inteligencia de seguridad se basa en soluciones efectivas que permitan explotar el talento de los resposables en la organización.

¿¿Preguntas??

¡¡Gracias!!

Roque C. Juárez, CISSP, CISA, CISM, CRISC, CGEIT, ISO 27001 LA
Consultor de Seguridad de la Información
rjuarez@mx1.ibm.com