



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

Roque C. Juárez

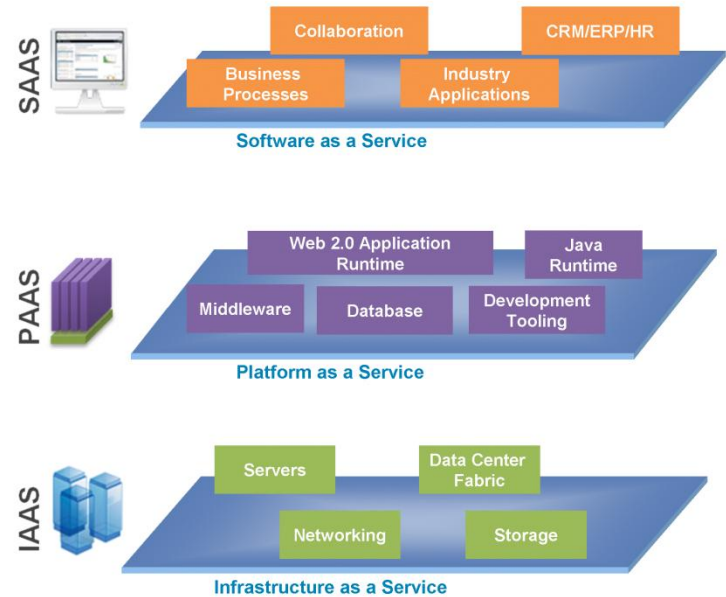
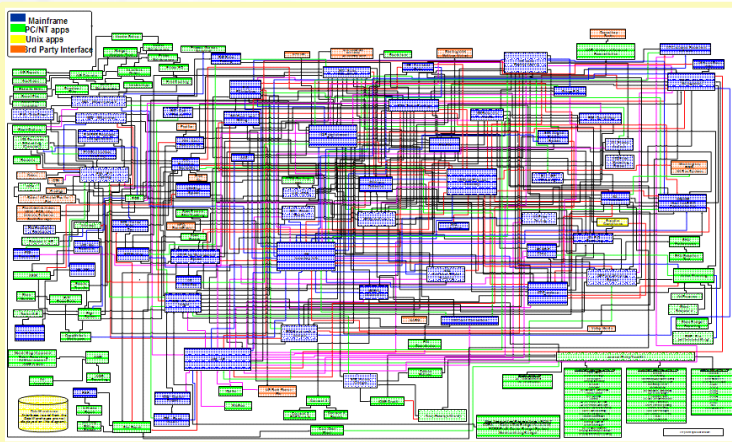
Consultor de Seguridad de la Información

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

## La seguridad no fué un proyecto



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



¿estamos solamente para operar?

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

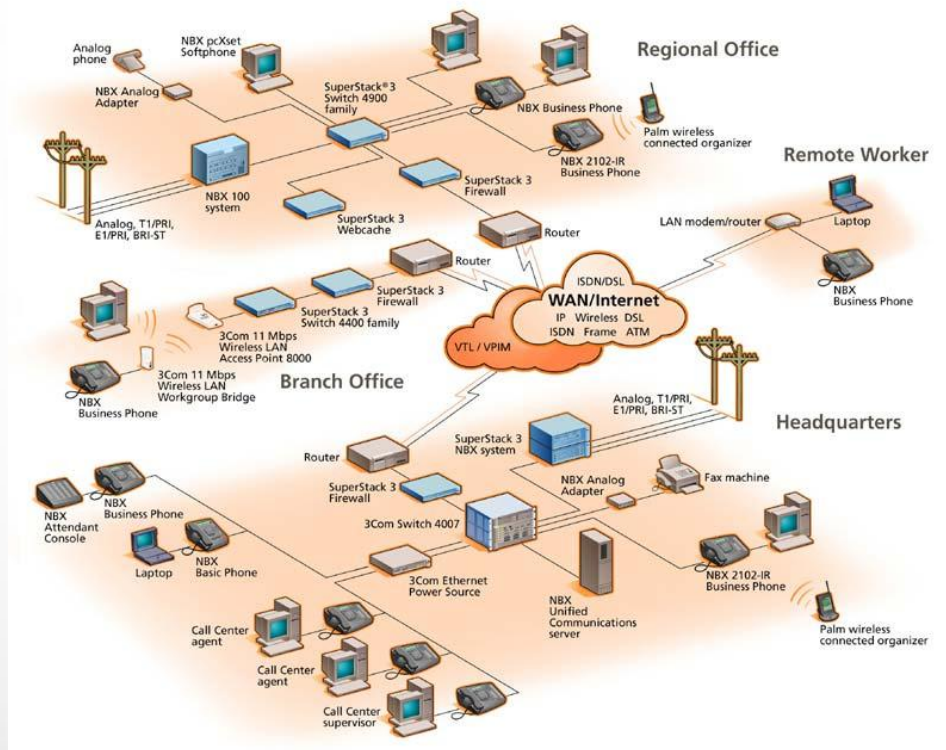




- Se cumple con las regulaciones de la industria... por nuevas que estas parezcan.



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



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





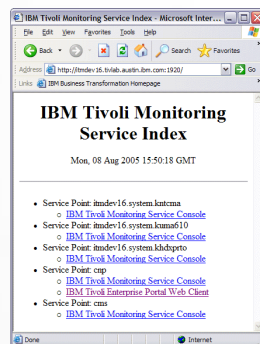
«La seguridad de la información tiene un contexto y medición operativos»

## Caminando a la gestión de seguridad

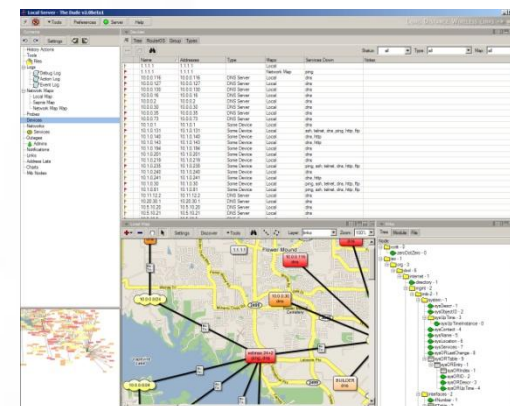


# Caminando a la gestión de la seguridad

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



**Log Management**



Summary	Daily	Weekly	Monthly	Yearly
Service:	IT17			
Host (group):	server1			
Check period:	5:00:00			
Last check:	4:59:36 ago			
# of checks:	1020			
# of outages:	0			
# of failed checks:	0			
Uptime:	99.712 %			
Avg. response time:	0.201 s			

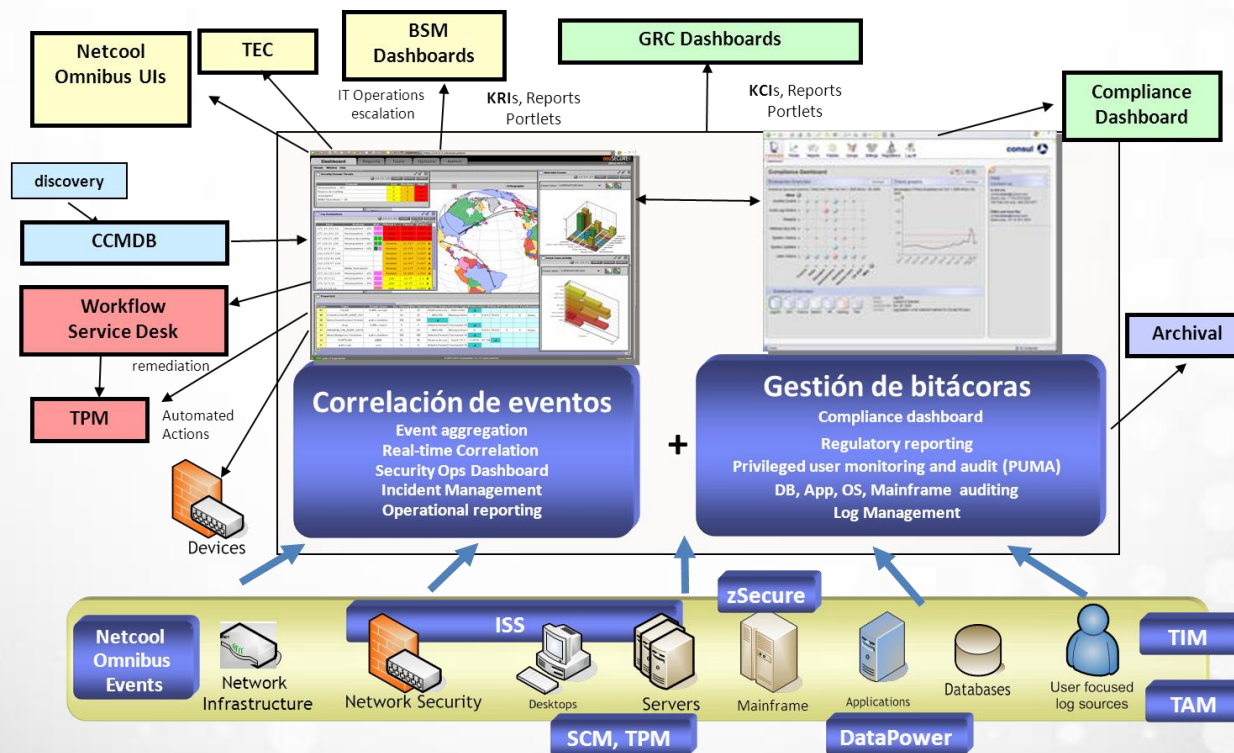
  

Day	Total checks	Outages	Failed checks	Avg. response time	Uptime
2007.03.01	289	0	0	0.206	100 %
2007.03.02	289	0	0	0.205	100 %
2007.03.03	289	0	0	0.205	100 %
2007.03.04	289	0	0	0.205	100 %
2007.03.05	289	0	0	0.204	100 %
2007.03.06	285	0	0	0.208	100 %
2007.03.07	291	0	0	0.200	99.696 %
2007.03.08	289	0	0	0.203	100 %
2007.03.09	287	0	0	0.200	100 %
2007.03.10	291	0	0	0.20	100 %
2007.03.11	294	0	0	0.205	100 %
2007.03.12	294	0	0	0.209	99.289 %
2007.03.13	290	0	0	0.205	100 %
2007.03.14	289	0	0	0.195	99.322 %
2007.03.15	288	2	4	0.261	98.611 %



# Caminando a la gestión de la seguridad

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





- Definir cursos de acción para tratamiento de incidentes.

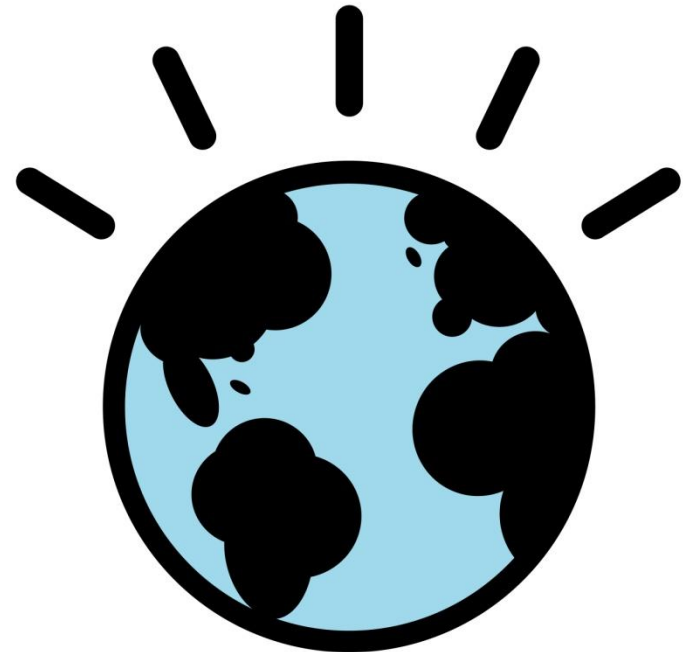


# Caminando a la gestión de la seguridad

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



## Seguridad más inteligente

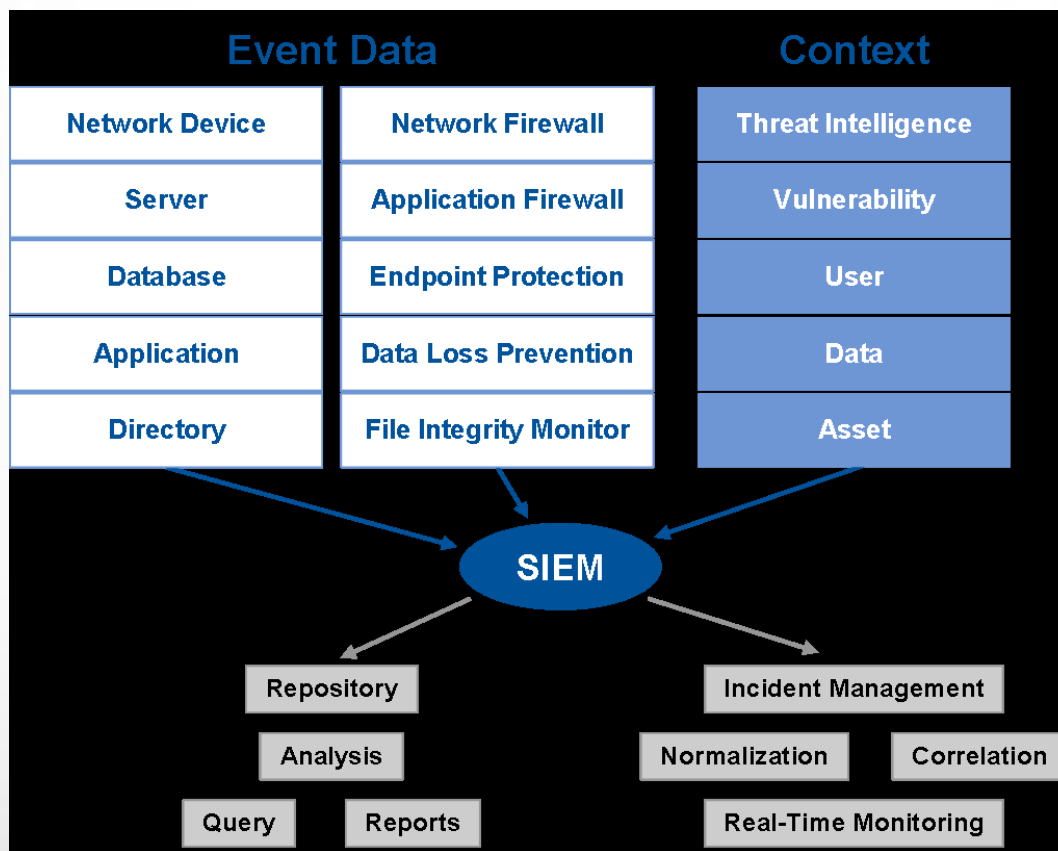


- ¿Qué es la inteligencia?

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



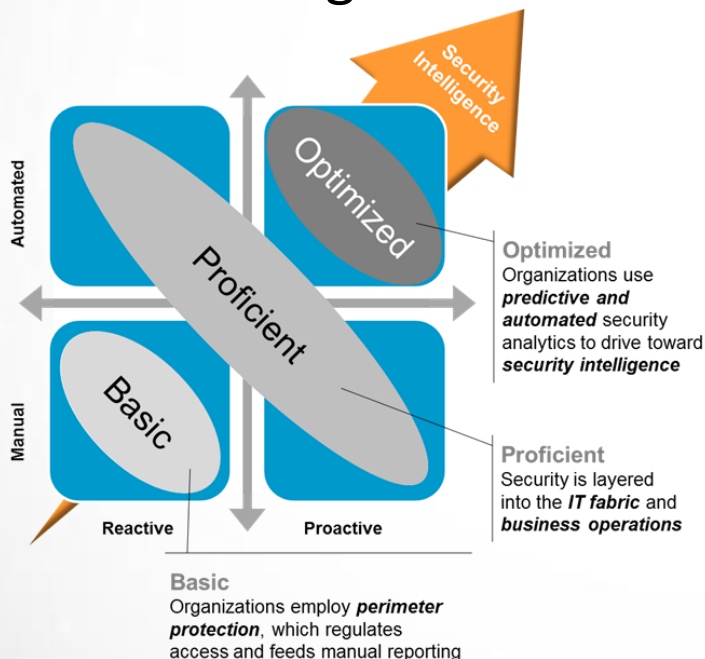
- El modelo actual de SIEM tiene alcances limitados.



- 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



- 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

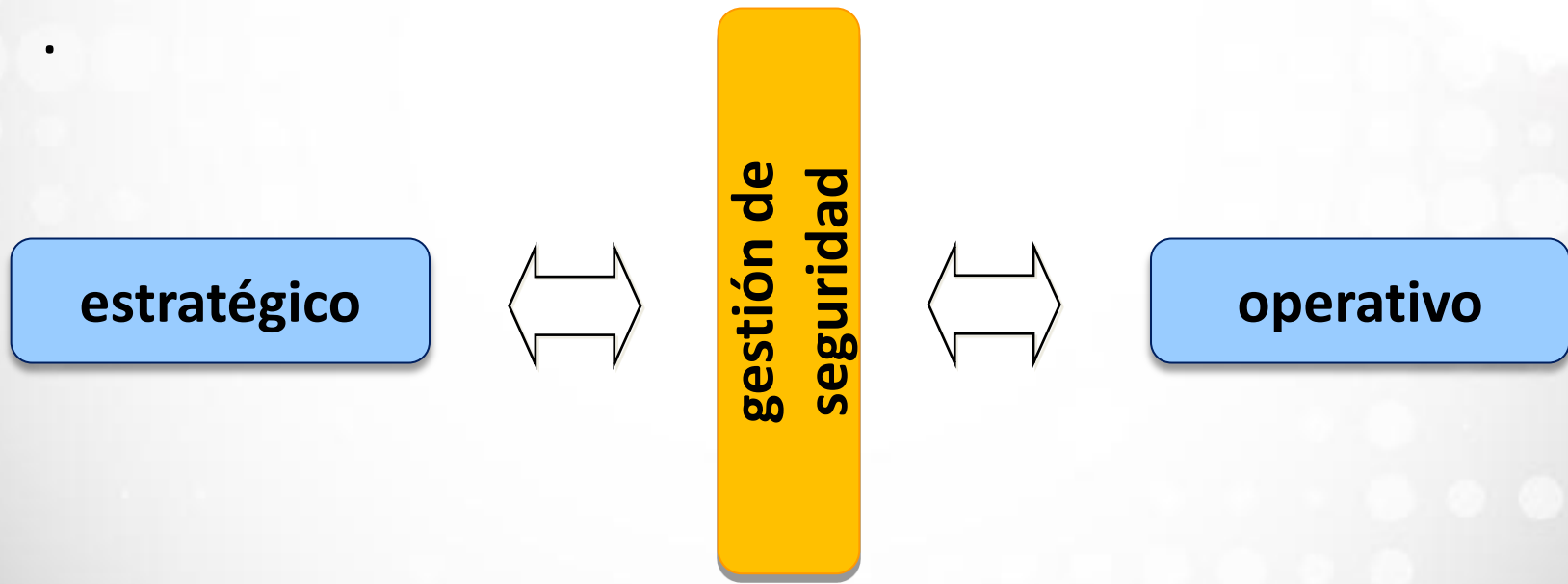
SPSS Predictive Analytics solving insider threat

Hybrid scanning capabilities from Rational AppScan

Identity Governance to build integrated access processes

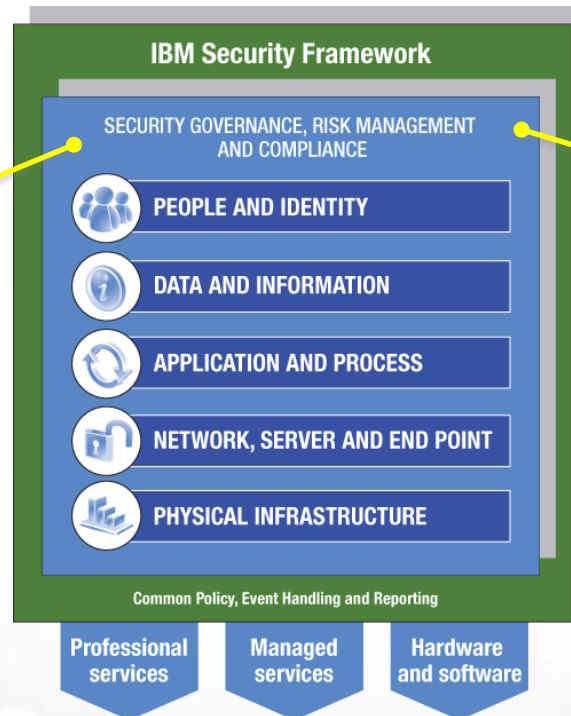
- La seguridad de la información se establece de forma práctica con tres componentes fundamentales:

- .





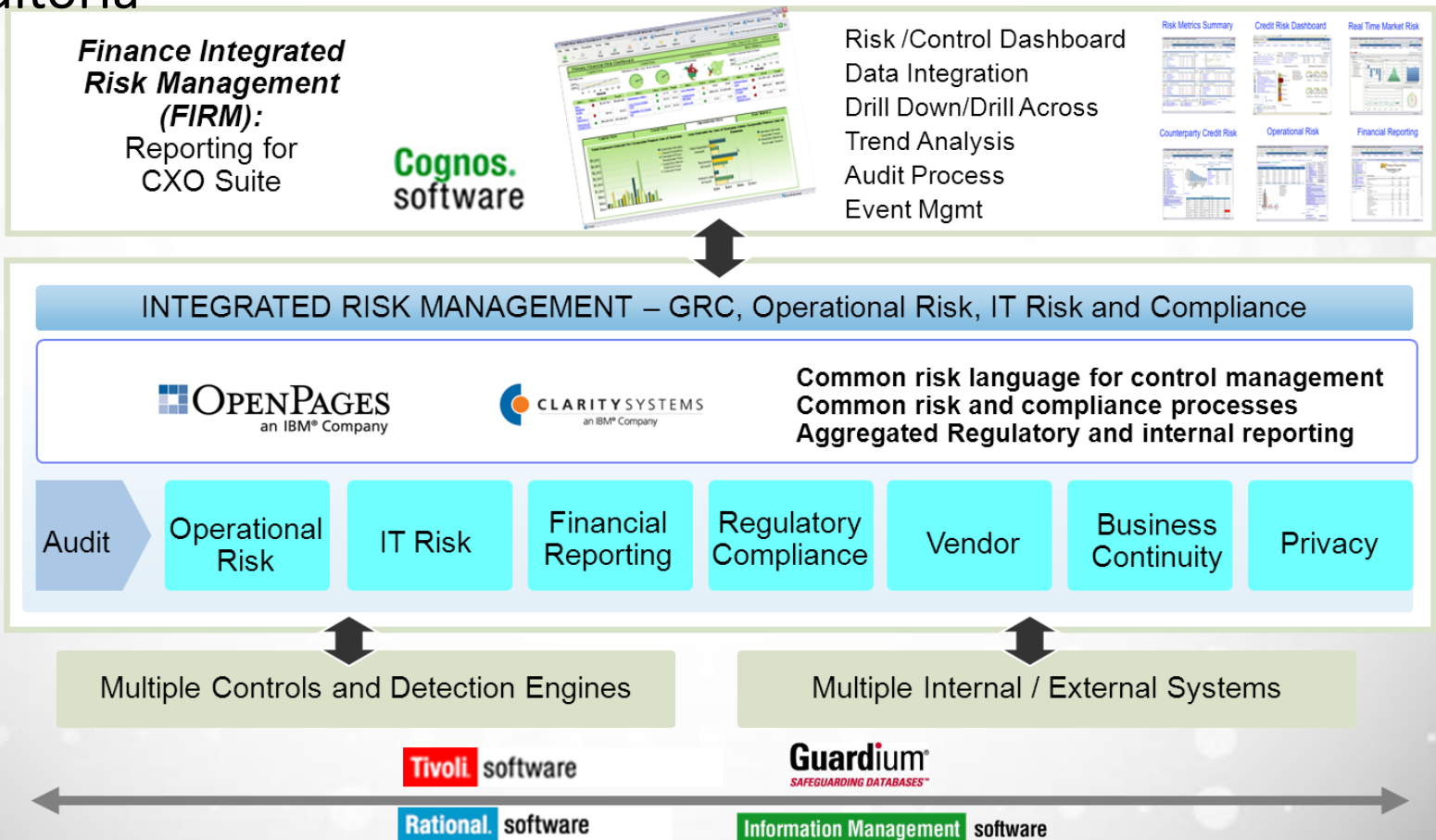
- El portafolio de IBM crece para atender estos requerimientos de los clientes.



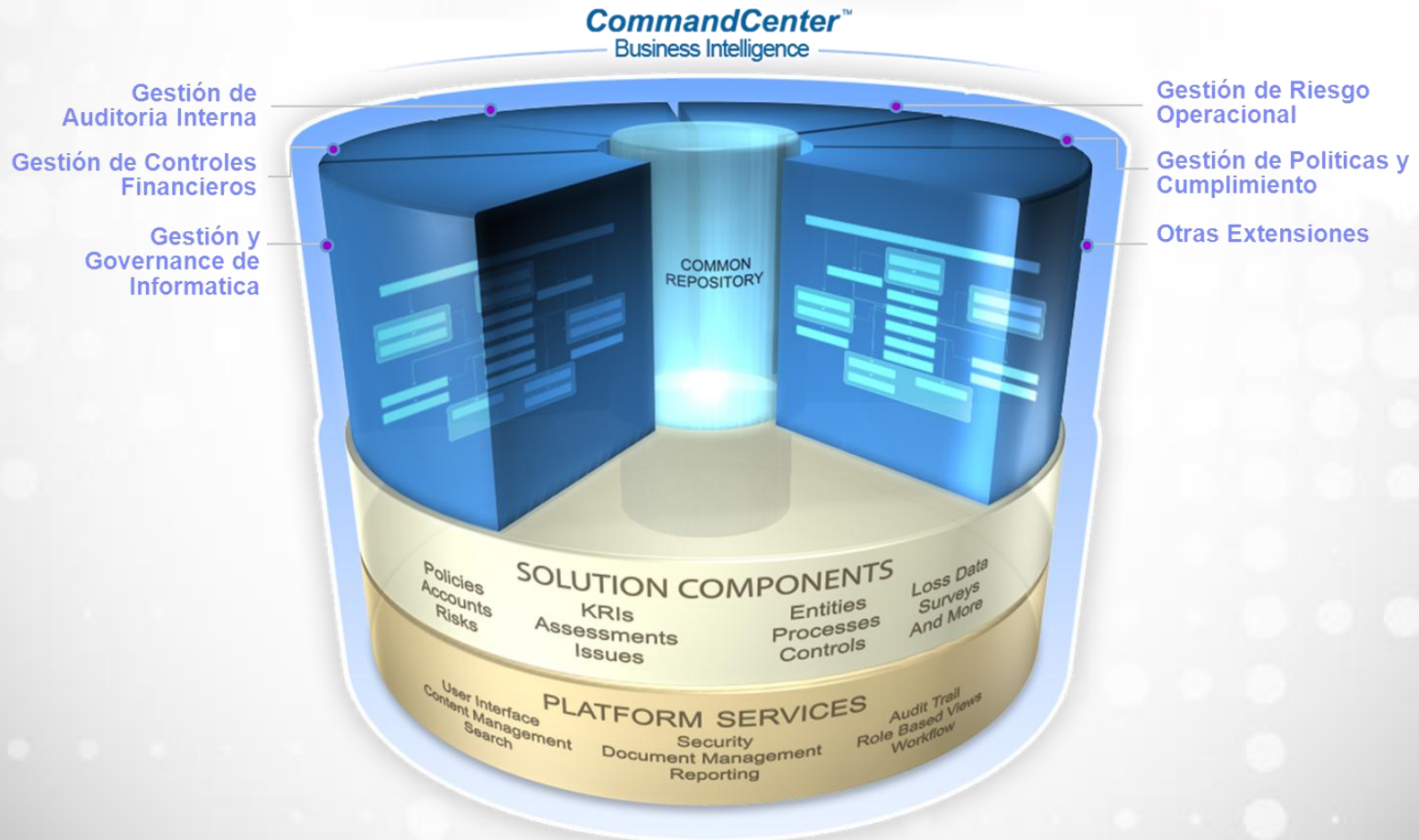
 **OPENPAGES**  
an IBM® Company

 **1Q Labs**  
*Total Security Intelligence*

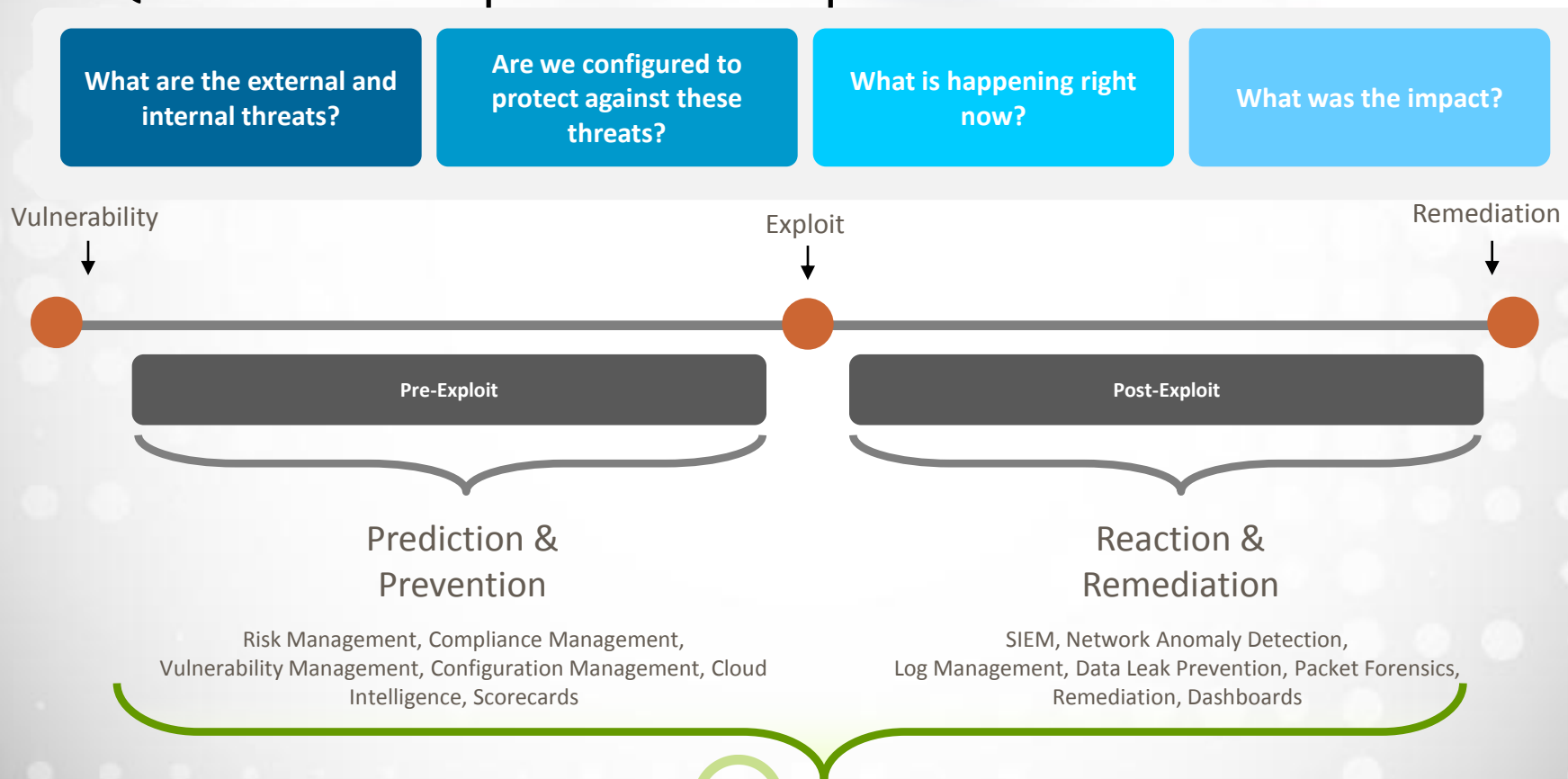
- Open Pages – Riesgo operacional, Riesgo TI, Controles Financieros, Auditoría



- Open Pages – Permite la gestión integrada de riesgos



- Q1 Labs – Se amplia el ciclo de protección.





- Q1 Labs – Se amplia el ciclo de protección.

## Security Information and Event Management



- Sophisticated event analytics
- Asset profiling and flow analytics

## Log Management



- Turnkey log management
- Upgradeable to enterprise SIEM

## Risk Management



- Predictive threat modeling & simulation
- Scalable configuration monitoring & audit

## Network Activity and Anomaly Detection



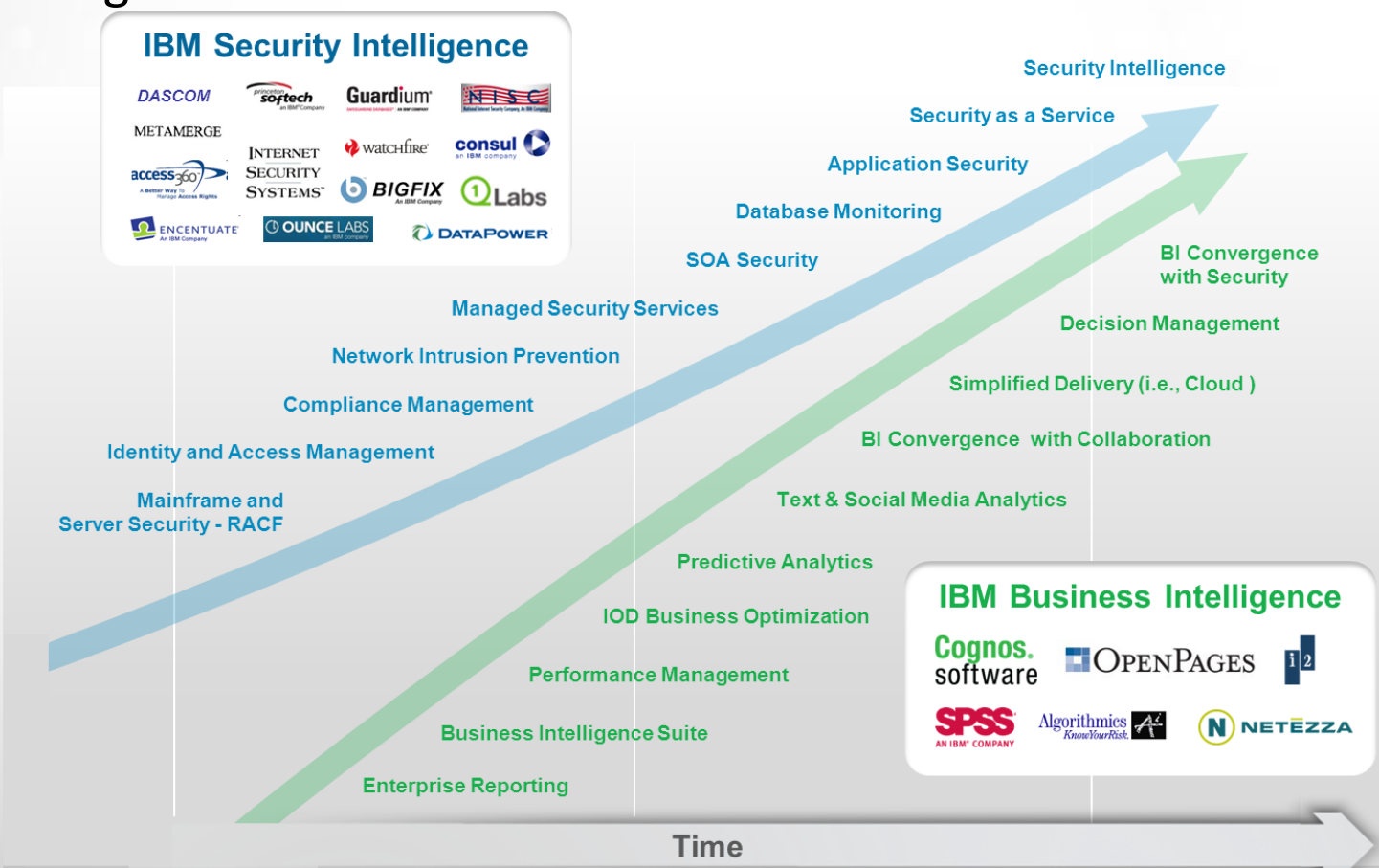
- Network analytics
- Behavioral and anomaly detection

## Network and Application Visibility

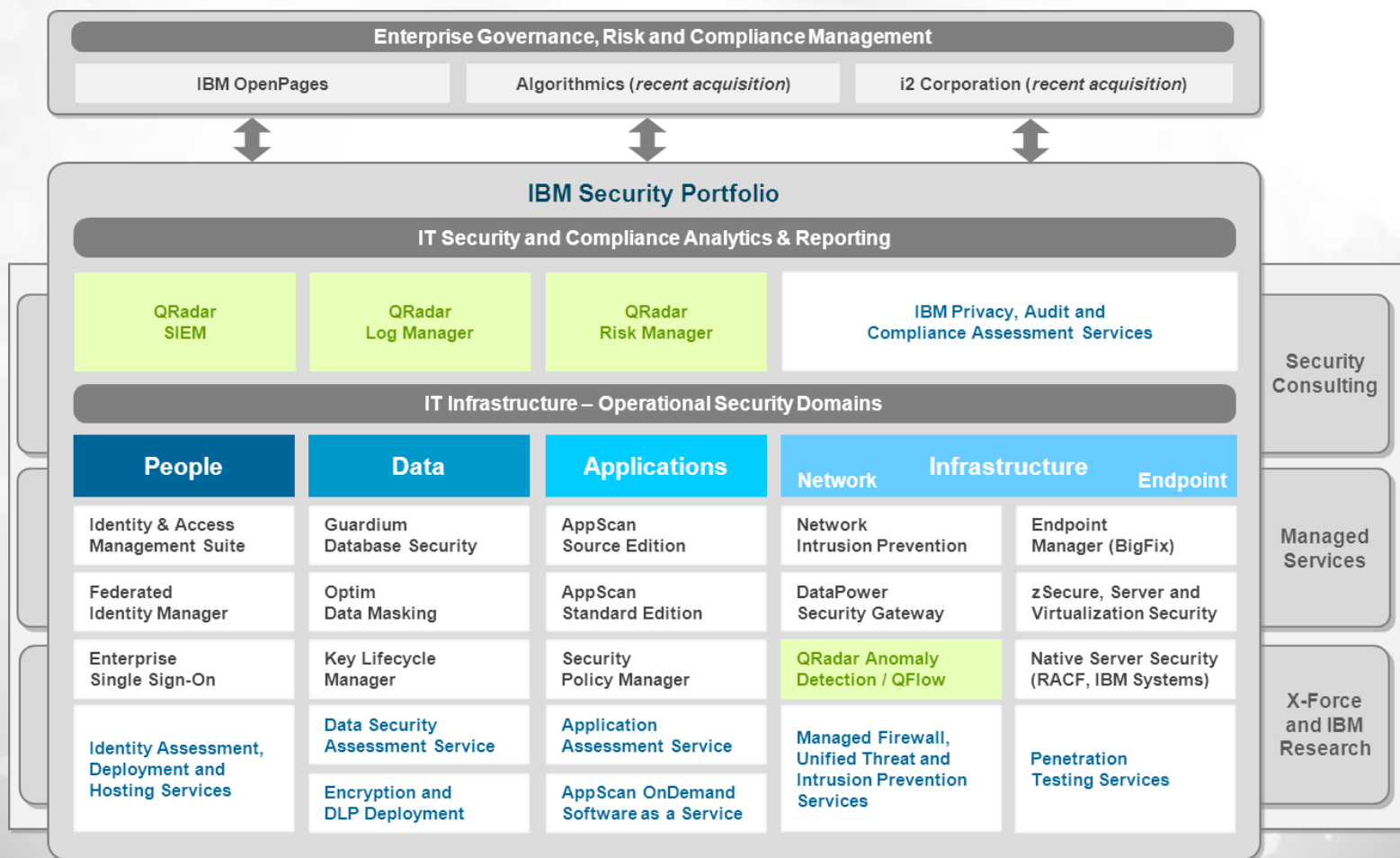


- Layer 7 application monitoring
- Content capture


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



- El portafolio más completo de seguridad de la información.



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

	People	Data	Applications	Infrastructure
	<b>Governance, risk and compliance</b> <b>Advanced correlation and deep analytics</b> 			
<b>Optimized</b>	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Secure systems
<b>Proficient</b>	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management
<b>Basic</b>	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus

## Consideraciones finales



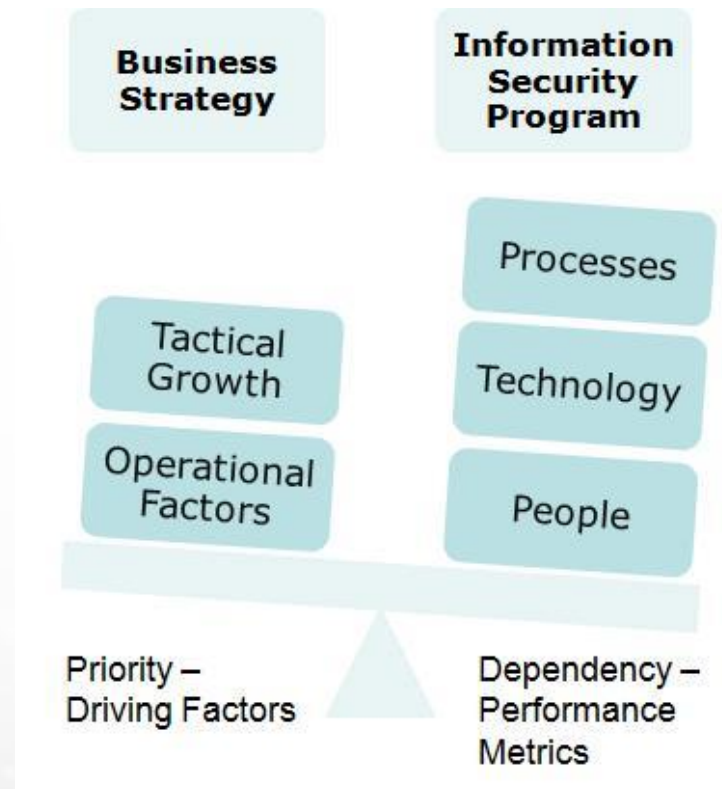


- Es fundamental impulsar los proyectos de SIEM y correlación de eventos.



**Son la materia prima para inteligencia de seguridad.**

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



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



**La inteligencia de seguridad se basa en soluciones efectivas que permitan explotar el talento de los responsables 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](mailto:rjuarez@mx1.ibm.com)