Inteligencia en Seguridad:

¿Cómo encontrar atacantes y anomalías en un mar de eventos de Seguridad?

Sergio Hrabinski

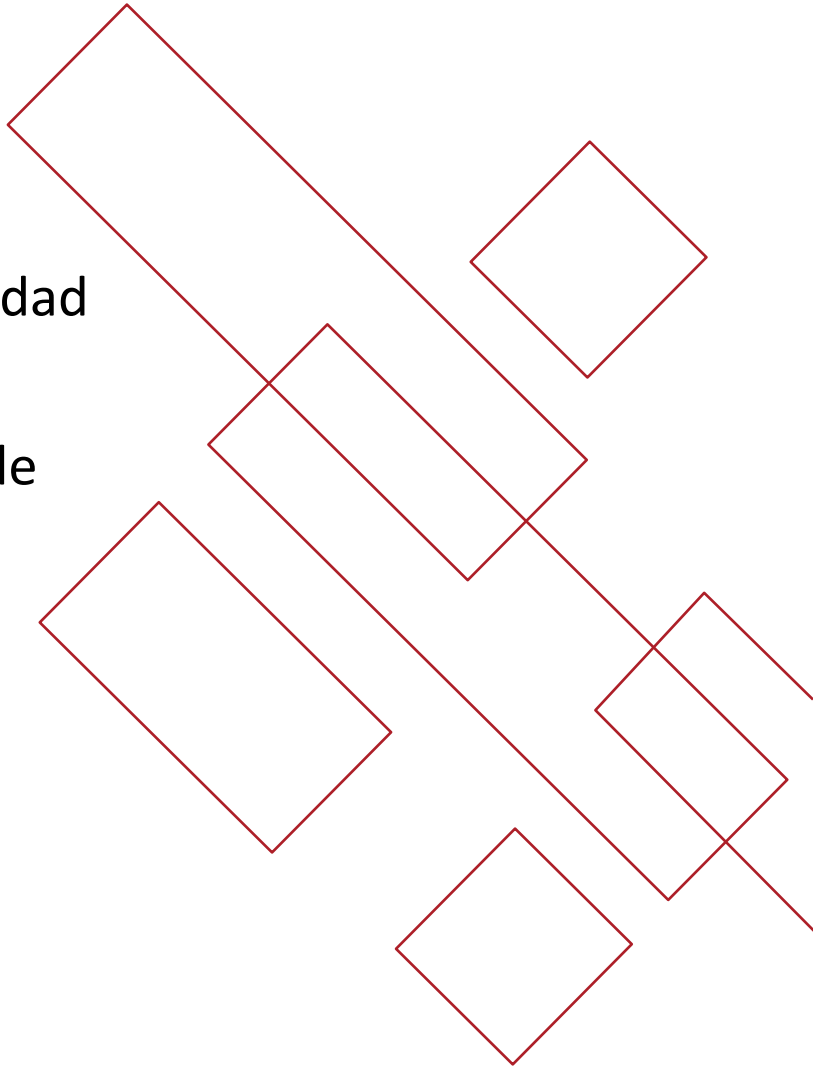
Socio

xelere

Making IT better

Agenda

- Los temas de preocupación en la seguridad
- El sistema de seguridad inmune
- Cómo identificar amenazas en un mar de eventos
- La seguridad analítica
- La seguridad cognitiva



Temas claves en el ámbito de la seguridad

Optimizar el programa de seguridad

Pasar del “compliance” a la gestión de riesgos

Detener amenazas avanzadas

Usar seguridad analítica e integrada

Proteger activos críticos

Usar controles que prevengan acceso no autorizado y pérdida de datos

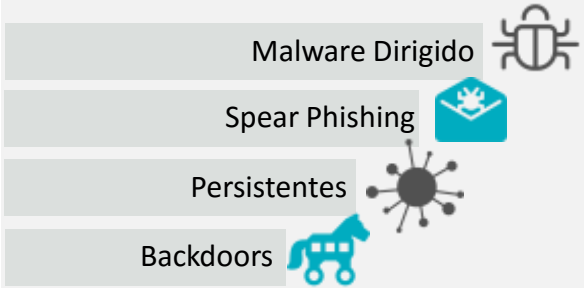
Resguardar la nube y los dispositivos móviles

Fortalecer la postura de seguridad y facilitar la apertura de la red

xelere

Desafíos

Evolución de ataques



- Gran incremento en la cantidad de ataques.
- Ataques cada vez más sofisticados.
- Considerable aumento de la cantidad de malware.
- Brechas de seguridad diarias.

Soluciones complejas

- Permanentes cambios en la infraestructura tecnológica.
- Múltiples soluciones de diferentes proveedores.
- Soluciones no integradas complicadas de administrar.
- Herramientas insuficientes.

Recursos Reducidos

- Nuevos retos para el equipo de seguridad.
- Dificultad a la hora de encontrar personal calificado.
- Nuevas demandas de monitoreo y auditorías.

La seguridad como sistema inmune

Malware protection

Incident and threat management

Identity management

Data monitoring

Device management

Transaction protection

Access management

Firewalls

Data access control

Privileged identity management

Entitlements and roles

Sandboxing

Security research

Endpoint patching and management

Antivirus

Vulnerability assessment

Content security

Log, flow and data analysis

Criminal detection

Application security management

Anomaly detection

Network visibility

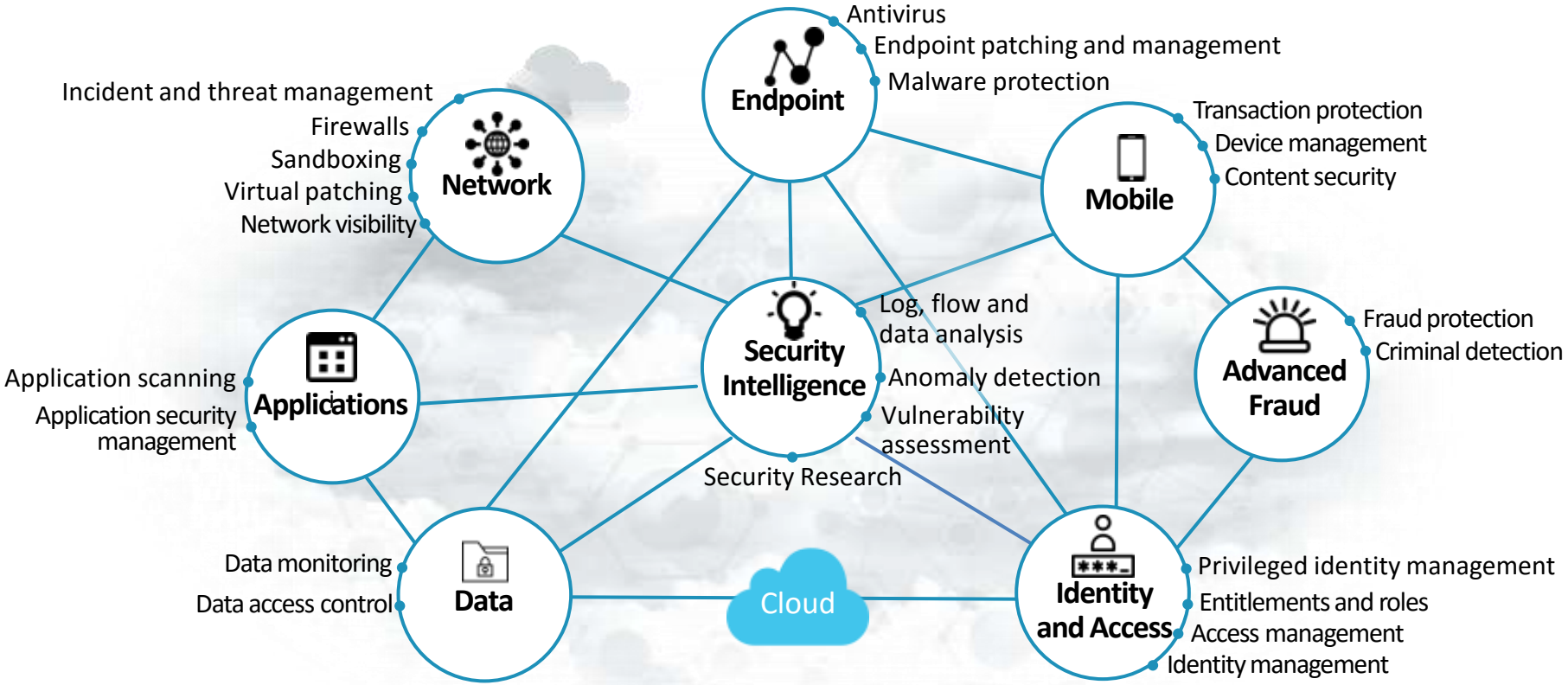
Application scanning

Virtual patching

Fraud protection

xelere

La seguridad como sistema inmune



xelere

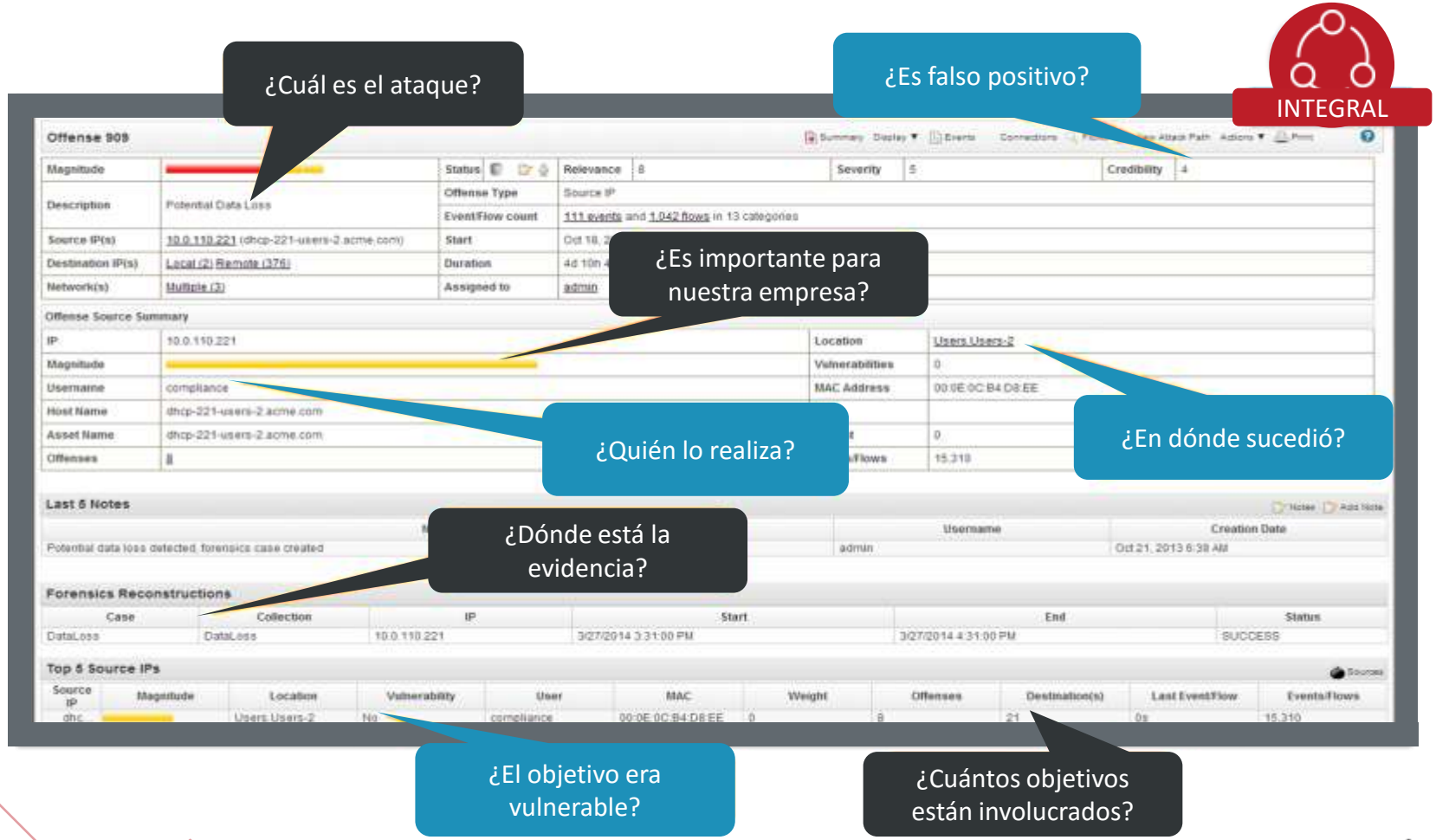
¿Qué es un SIEM y por qué lo necesito?

- **SIEM**, significa Security Information and Event Management
- Provee análisis en tiempo real de los datos de seguridad generados por aplicaciones y dispositivos de la red.
- Obtiene y almacena información de múltiples fuentes (miles).
- Correlaciona los datos en tiempo real, aplicando capacidades analíticas avanzadas para determinar cuándo están ocurriendo situaciones anómalas o posibles ataques.
- Genera alertas si se detecta actividad sospechosa.
- Almacena datos a largo plazo, proveyendo un rápido acceso cuando se necesite para soportar investigaciones forenses.
- Es un requerimiento para demostrar cumplimiento con múltiples estándares y regulaciones: HIPAA, PCI DSS, SOX, etc.

Inteligencia integrada que identifica automáticamente las ofensas

xelere

Generación de ofensas que ayudan a prevenir y remediar incidentes



Preguntas Clave

¿Cuáles son los principales Riesgos y vulnerabilidades?

¿Estamos preparados para protegernos contra amenazas avanzadas?

¿Qué incidentes de seguridad están sucediendo ahora?

¿Cuál fue el impacto en la organización?

FASE PREVENTIVA / PREDICTIVA

- Visibilidad sobre el estado de seguridad de la organización.
- Detectar desviaciones y generar advertencias tempranas de APTs.
- Priorizar las vulnerabilidades para optimizar los procesos de remediación y mitigar las exposiciones críticas.

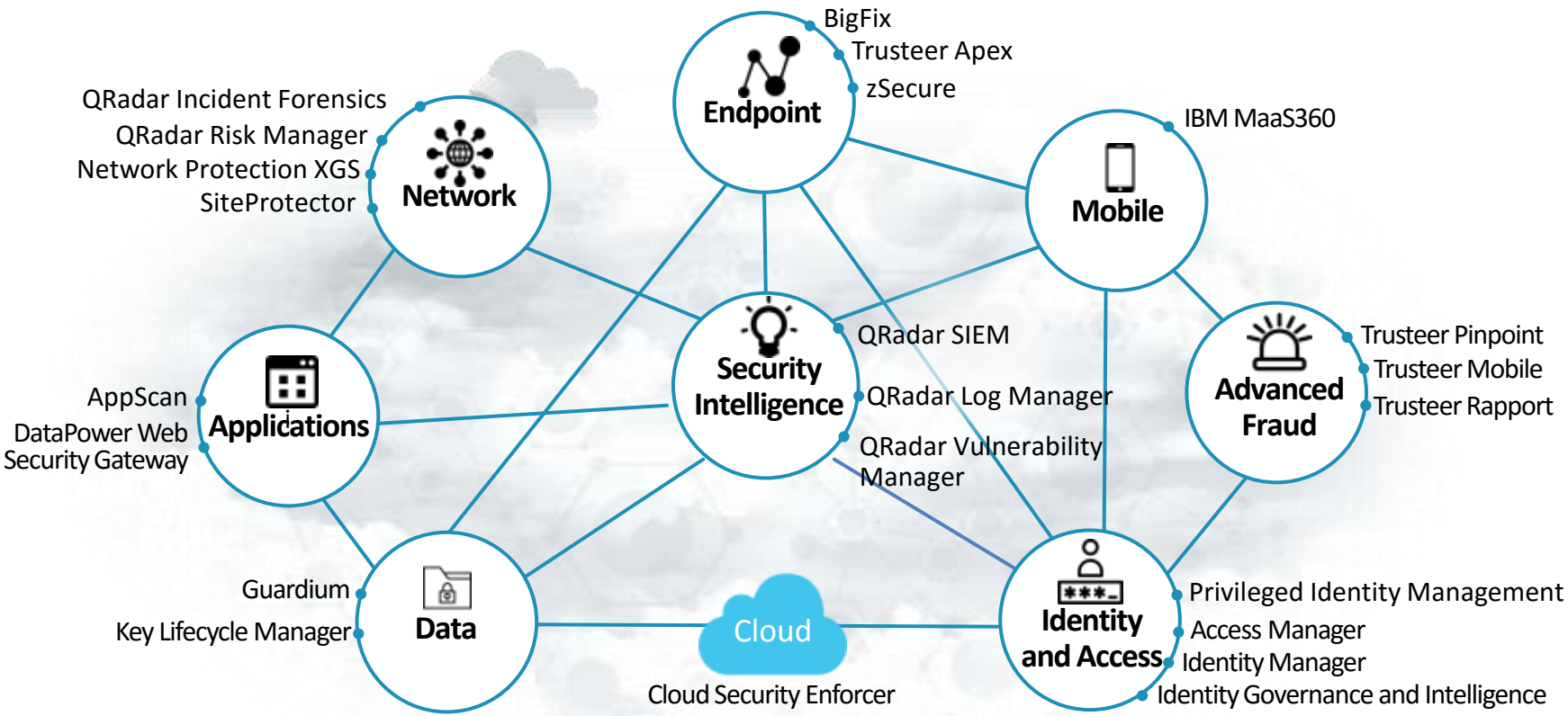
FASE DE REMEDIACIÓN / REACTIVA

- Detectar automáticamente las amenazas, optimización para analizar rápidamente el impacto y alcance.
- Visibilidad completa a través de análisis avanzado semi automático.
- Investigación forense, reduce el tiempo para encontrar la causa-origen; permitiendo utilizar los resultados para conducir rápidamente a la remediación.

Vulnerability Manager | Risk Manager | SIEM | Log Manager | Incident Forensics

xelere

Expandir el valor de las soluciones a través de la integración

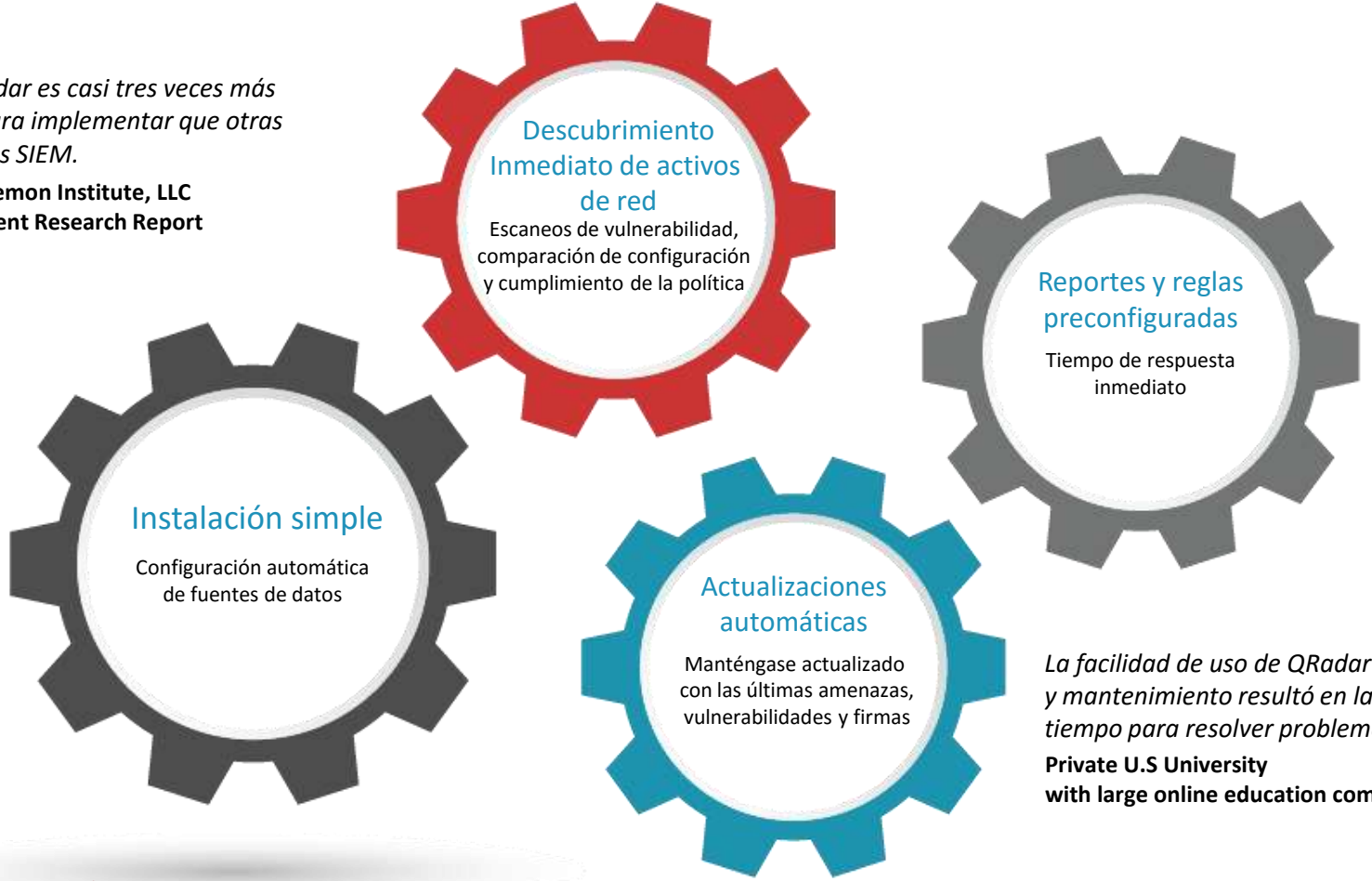


xelere

Fácil de administrar e implementar

IBM QRadar es casi tres veces más rápido para implementar que otras soluciones SIEM.

2014 Ponemon Institute, LLC
Independent Research Report



La facilidad de uso de QRadar en Instalación y mantenimiento resultó en la reducción del tiempo para resolver problemas de red.

Private U.S University
with large online education community

xelere

QRadar es líder en la categoría SIEM del Cuadrante Mágico de Gartner, ocupando el primer lugar por segundo año consecutivo

xelere

Evolución del paradigma de Seguridad: Seguridad Cognitiva

Perimeter Controls
Pre-2005

Deploy static defenses to guard or limit the flow of data, including firewalls, antivirus, software and web gateways.

Security Intelligence
2005+

Leverage analytics to collect and make sense of massive amounts of real-time data flow, prioritizing events and detecting high-risk threats in real-time.

Cognitive Security
2015+

Interpret, learn and process security intelligence that was designed by and for humans, at speed and scale like never Before.

xelere

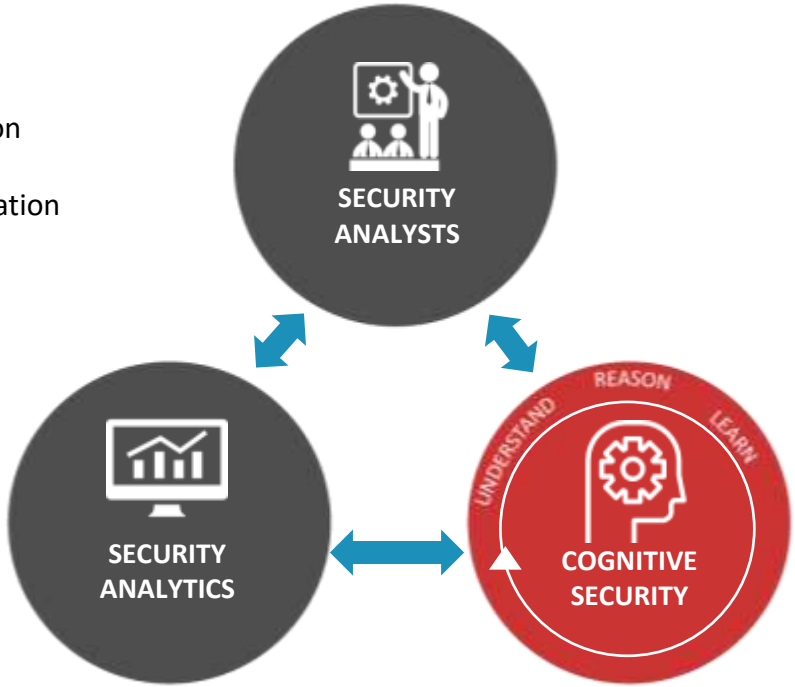
La utilización de sistemas cognitivos para potenciar la capacidad de los analistas de Seguridad, ayudándolos a explotar al 100% las soluciones tecnológicas

Human Expertise

- Common sense
- Morals
- Compassion
- Abstraction
- Dilemmas
- Generalization

Security Analytics

- Data correlation
- Pattern identification
- Anomaly detection
- Prioritization
- Data visualization
- Workflow



Cognitive Security

- Unstructured analysis
- Natural language
- Question and answer
- Machine learning
- Tradeoff analytics

xelere

Muchas gracias!

Contáctanos:
seguridad@xelere.com
www.xelere.com

xelere
Making IT better