Gestión y Monitorización de Logs
Sentinel

Jacinto Grijalba González
Security Solutions
Technology Sales Specialist
jgrijalba@novell.com

NetIQ® Security Solutions

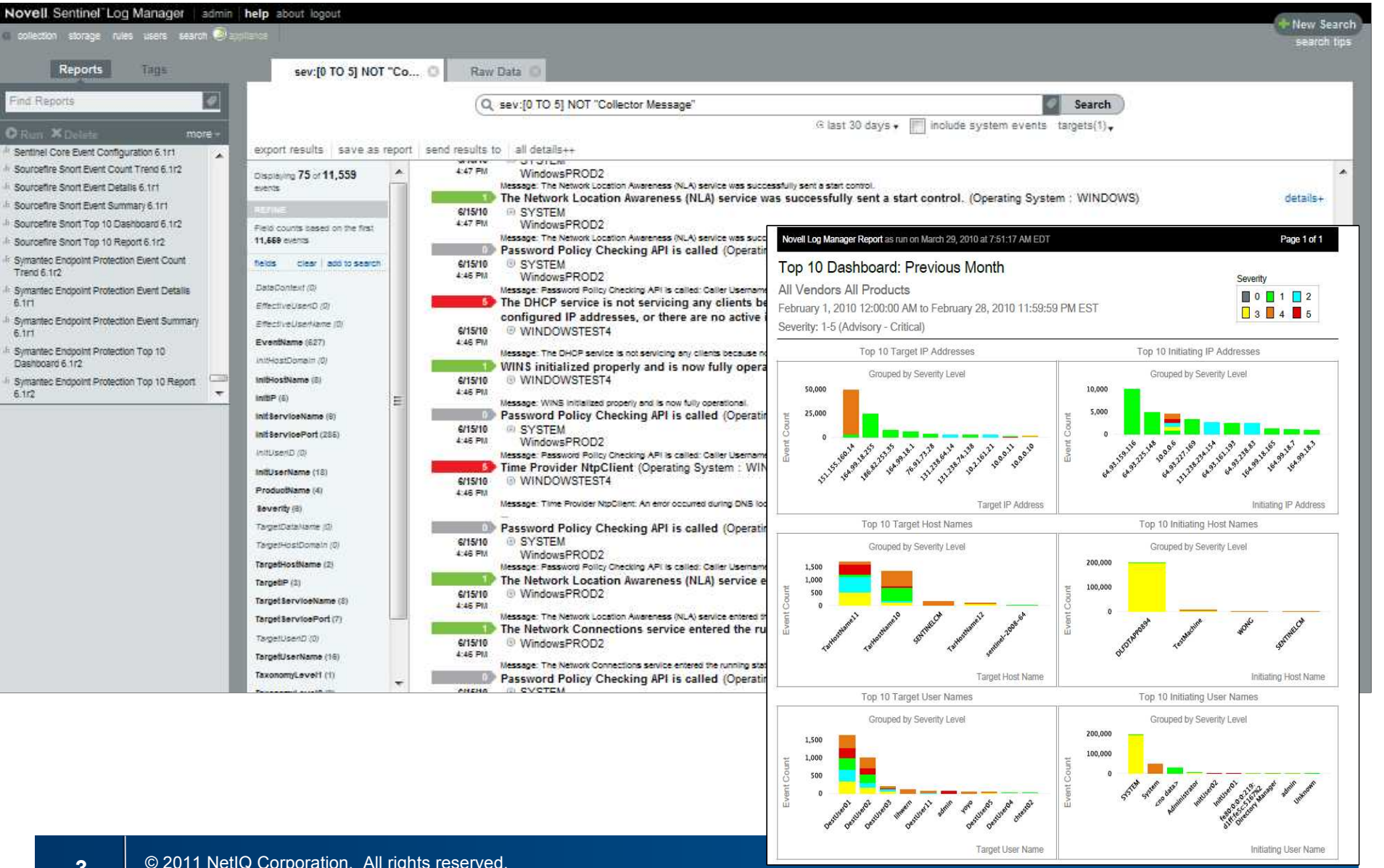
NetIQ® Sentinel

Log Management

- Informes de auditoría y cumplimiento
- Recolección, Almacenamiento y Análisis
- Analíticas avanzadas

NetIQ Sentinel Log Manager

Recopilación, Almacenamiento y Gestión de Logs



NetIQ® Security Solutions

NetIQ® Sentinel

Monitorización y Correlación

- Monitorización en tiempo real
- Análisis de históricos
- Respuestas automáticas

Log Management

- Informes de auditoría y cumplimiento
- Recolección, Almacenamiento y Análisis
- Analíticas avanzadas

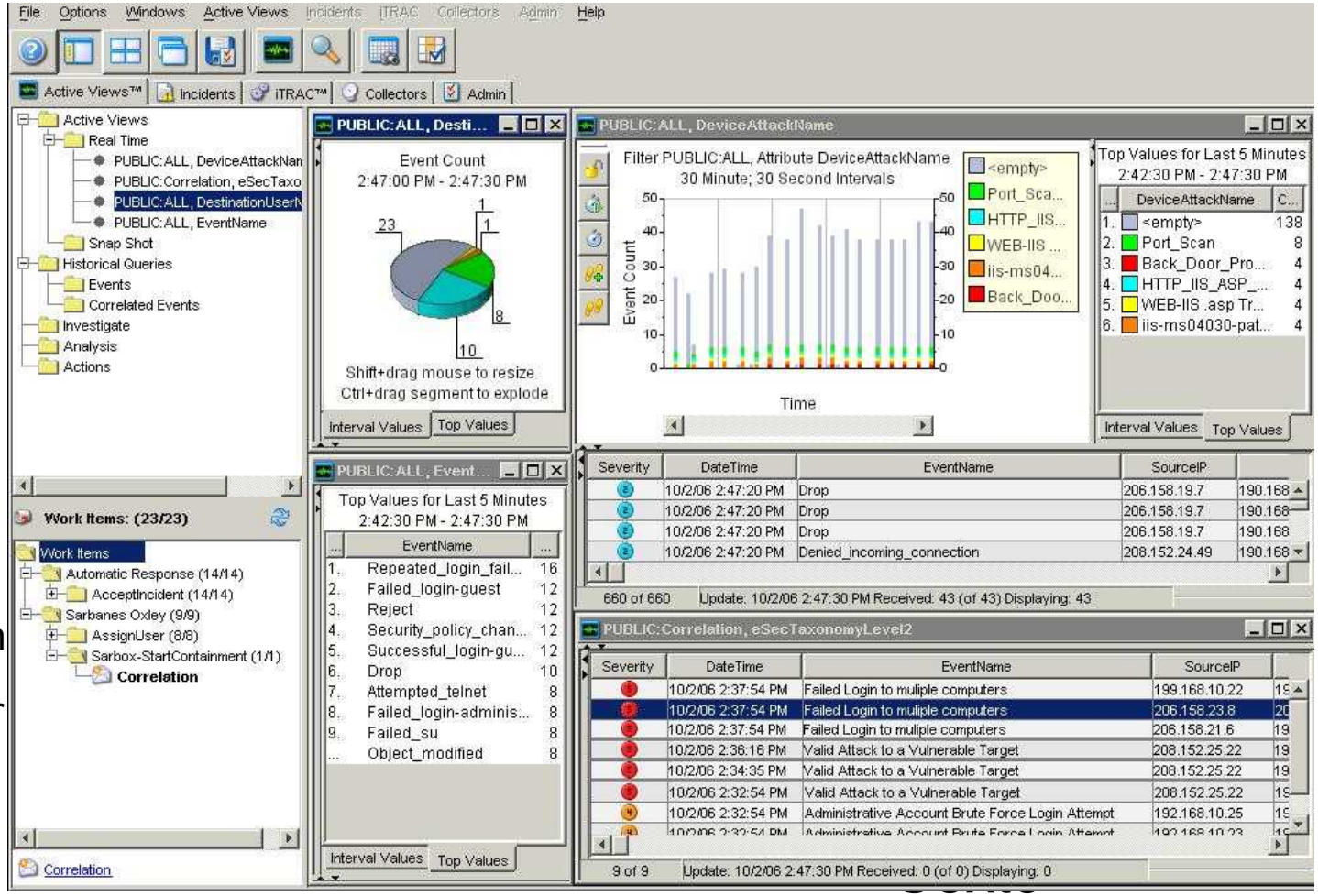
NetIQ Sentinel SIEM

Monitorización, Análisis y Correlación

Descripción: entorno centralizado para visualizar en tiempo real los eventos generados para monitorización, informes y gestión de incidencias

Beneficios:

- Identificar tendencias, ataques o violaciones
- Priorizar y gestionar esfuerzos de corrección
- Manipular e interactuar con datos en tiempo real
- Generación manual de incidencias



nivel del esquema

NetIQ® Security Solutions

NetIQ® Sentinel

Integración con la identidad

- Gestión del riesgo en los accesos a la información
- Monitorización de violaciones de seguridad de la identidad
- Visión global

Monitorización y Correlación

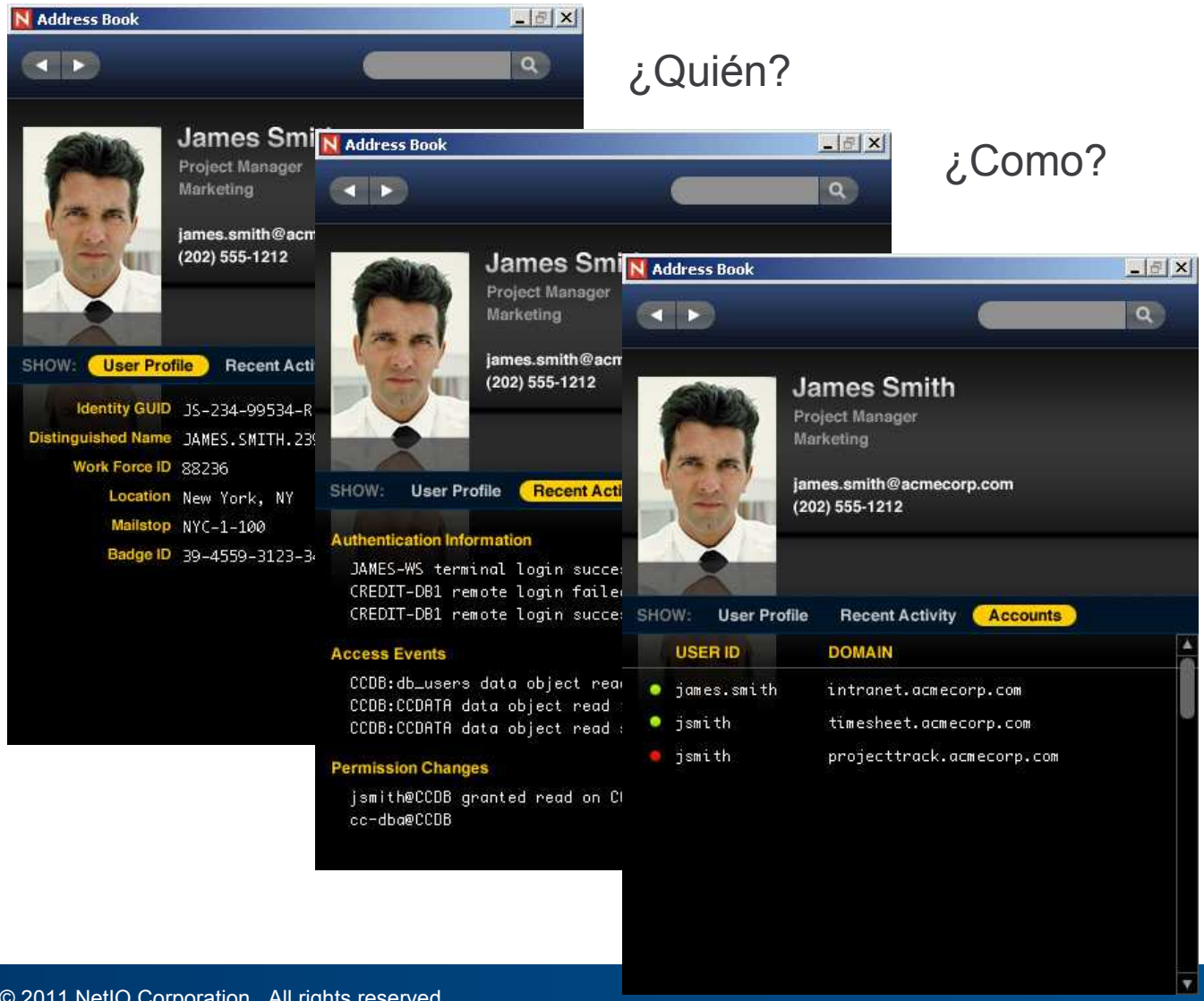
- Monitorización en tiempo real
- Análisis de históricos
- Respuestas automáticas

Log Management

- Informes de auditoría y cumplimiento
- Recolección, Almacenamiento y Análisis
- Analíticas avanzadas

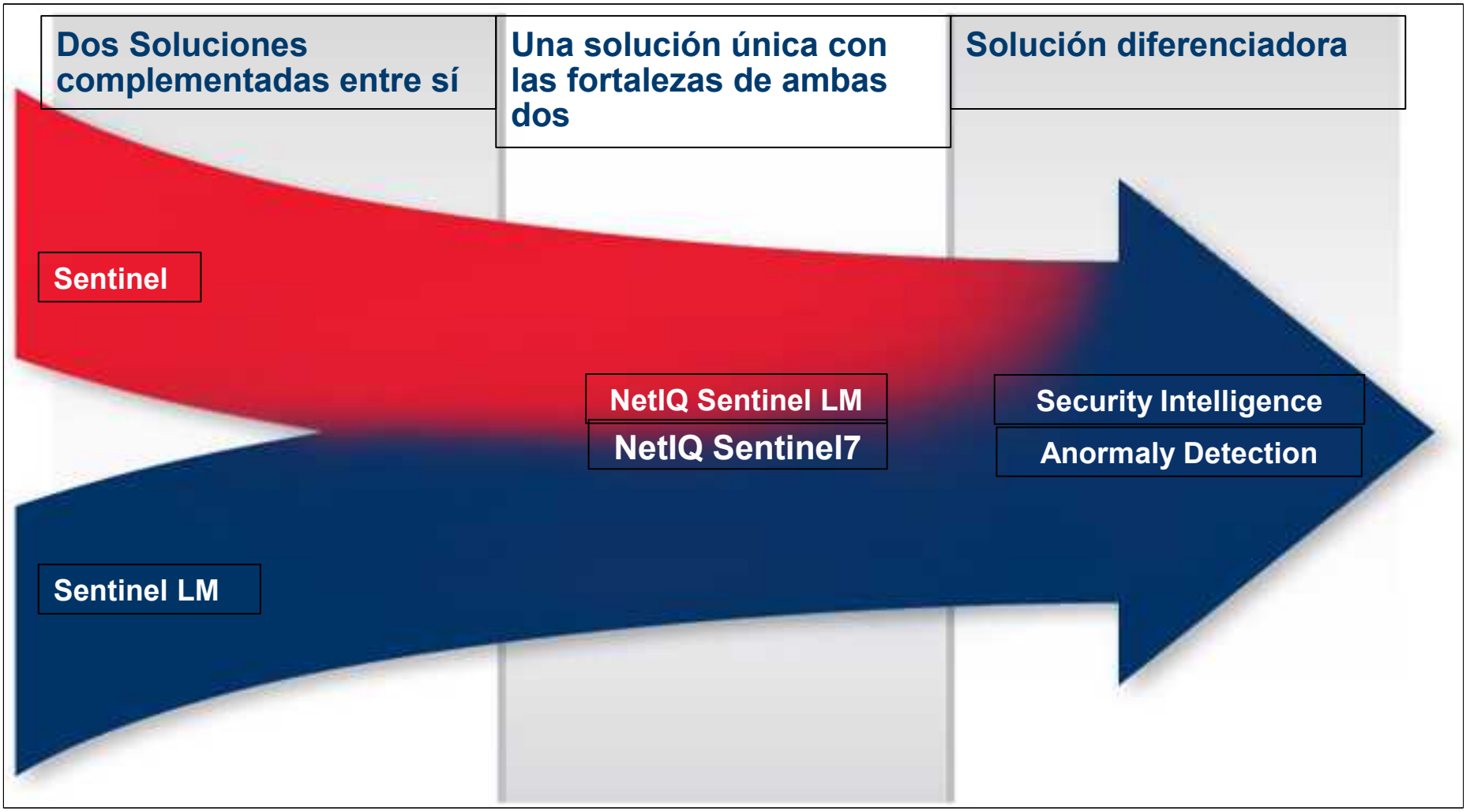
Gestión del riesgo

Herramientas operativas del día a día



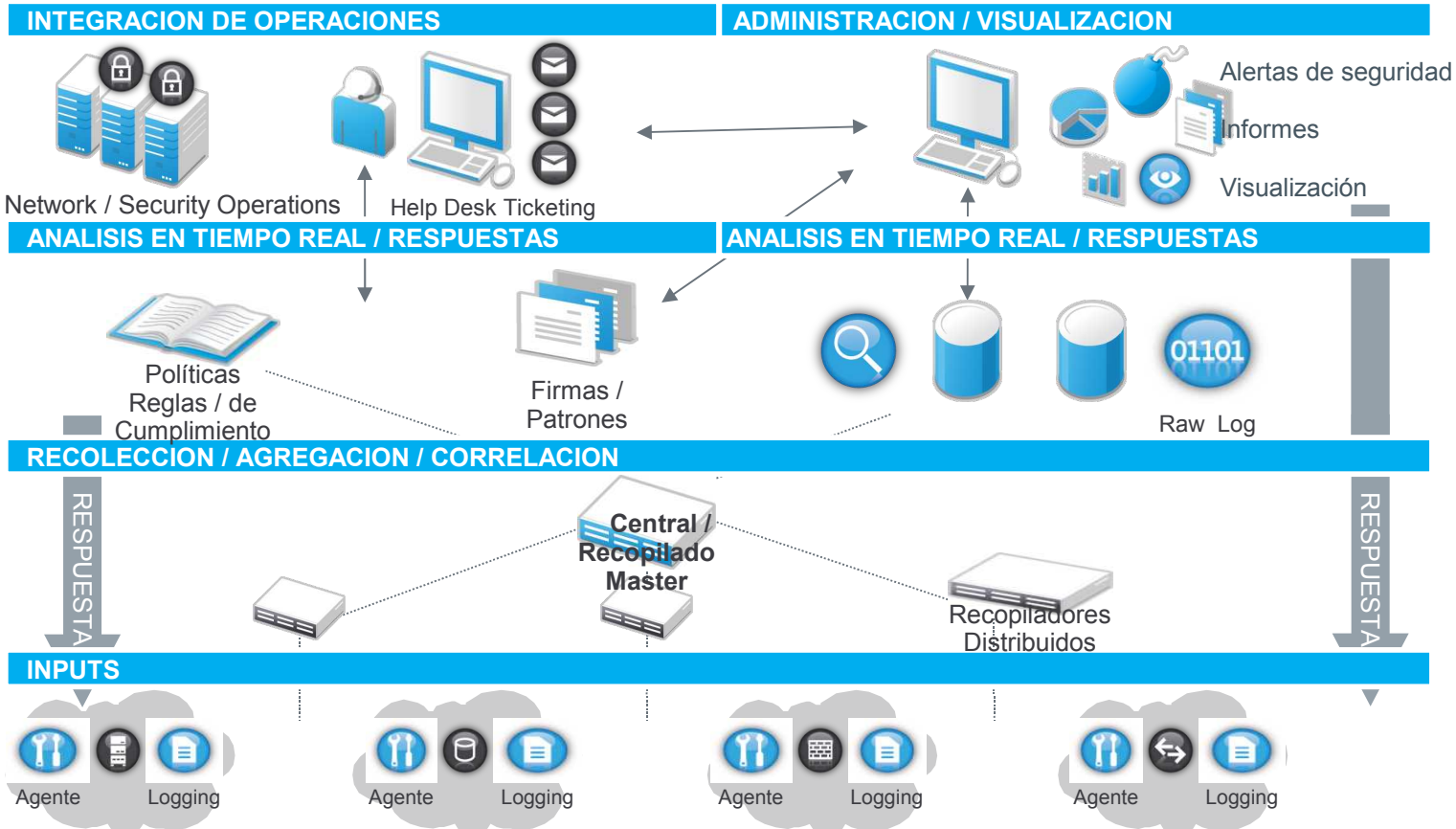
Nueva Versión Sentinel 7

NetIQ Security Management
SIM + SEM = SIEM



NetIQ® Security Solutions

Modelo de referencia de Burton



Gestión de Identidades
- Control de Accesos
- Directorios
- Aprovisionamiento

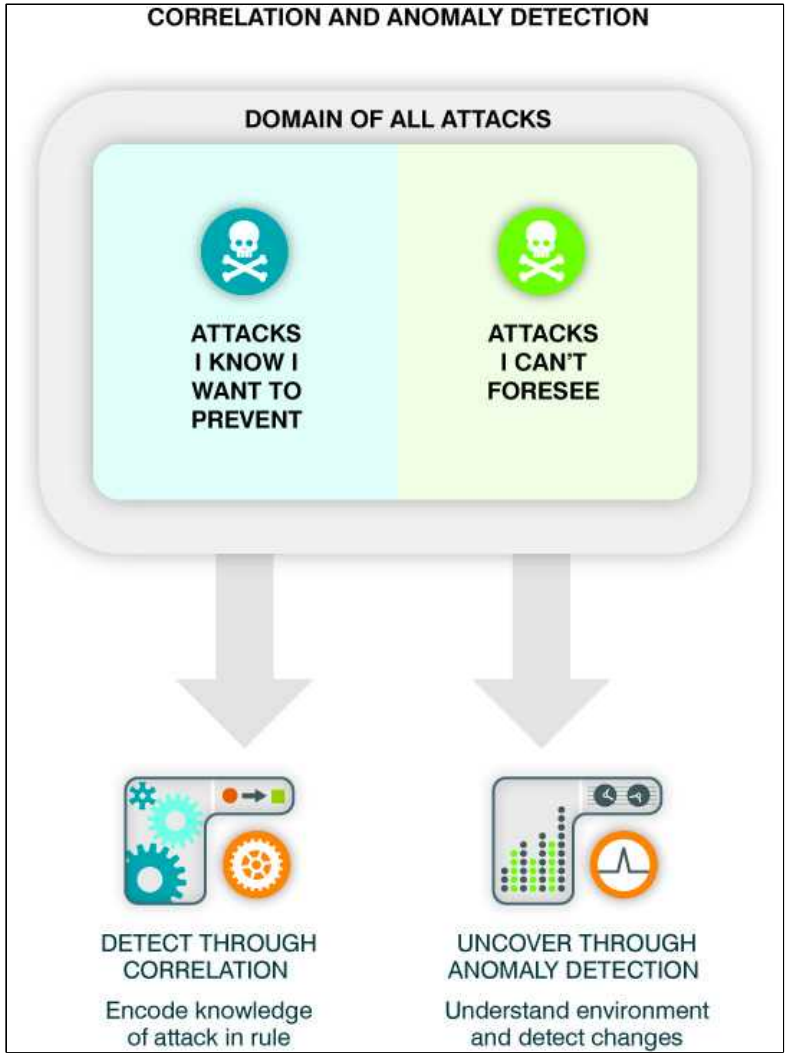
Gestión de Sistemas
- Configuración de Host y DB
- Gestión de parches
- Gestión de vulnerabilidades

Control Perimetral
- Routers
- Firewalls
- Escaneres de contenido

Detección de Intrusiones / Respuestas
- Network IDS
- Network IPS
- Otros sensores

Source: Burton Group – Diana Kelley

What's Happening In My Environment?



Anomaly Detection

- Discrepancy or deviation from an established rule, trend, or pattern
- Something I can't necessarily foresee but I want to monitor

Correlation

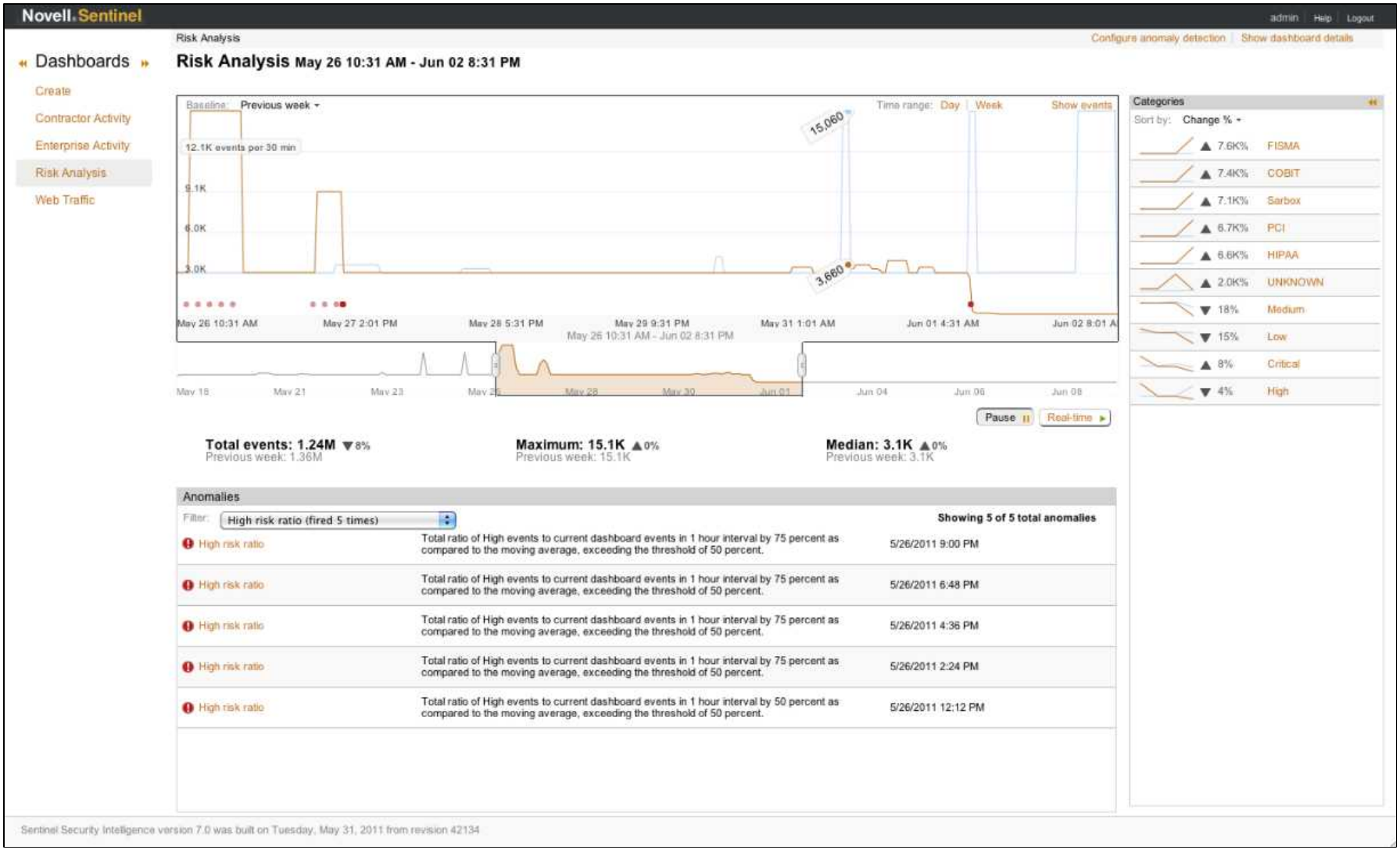
- Relationship between two or more sets of data
- Something I can foresee and want to take immediate action

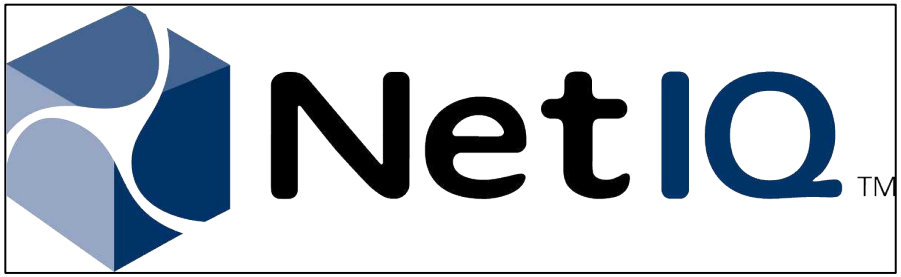
Security Intelligence
Anomaly Detection

Anomaly detection es la manera más eficiente de detectar ataques y descubrir nuevos ataques no identificados en reglas ya existentes

- Rápida detección de anomalías analizando solo cuando los cambios ocurren
- La correlación es un sistema muy efectivo, pero se debe saber la regla que activará un suceso ya descubierto
- Security Intelligence da un valor agregado sin necesidad de construir reglas de correlación.
- Security Intelligence complementa a las reglas de correlación autalimentado el ciclo de ataques conocidos.

Interfaz Security Intelligence





Worldwide Headquarters
1233 West Loop South
Suite 810
Houston, TX 77027 USA

+1 713.548.1700 (Worldwide)
888.323.6768 (Toll-free)
info@netiq.com
NetIQ.com

http://community.netiq.com