

# Gestión y Monitorización de Logs Sentinel

**Jacinto Grijalba González**

Security Solutions

Technology Sales Specialist

[jgrijalba@novell.com](mailto: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

Novell Sentinel Log Manager | admin | help | about | logout

collection | storage | rules | users | search | appliance

Reports | Tags | sev:[0 TO 5] NOT "Collector Message" | Raw Data

Find Reports | Run | Delete | more

Displaying 75 of 11,559 events

REFINE

Field counts based on the first 11,669 events

Fields: clear | add to search

DataContext (0)

EffectiveUser (2)

EffectiveUserName (0)

EventName (627)

InitHostDomain (0)

InitHostName (8)

InitIP (6)

InitServiceName (8)

InitServicePort (286)

InitUserID (0)

InitUserName (18)

ProductName (4)

Severity (8)

TargetDataName (0)

TargetHostDomain (0)

TargetHostName (2)

TargetIP (2)

TargetServiceName (8)

TargetServicePort (7)

TargetUserID (0)

TargetUserName (18)

TaxonomyLevel1 (1)

Search: sev:[0 TO 5] NOT "Collector Message"

last 30 days | include system events | targets(1)

export results | save as report | send results to | all details++

4:47 PM WindowsPROD2  
Message: The Network Location Awareness (NLA) service was successfully sent a start control.

1 The Network Location Awareness (NLA) service was successfully sent a start control. (Operating System : WINDOWS)

6/15/10 4:47 PM SYSTEM WindowsPROD2  
Message: The Network Location Awareness (NLA) service was successfully sent a start control.

0 Password Policy Checking API is called (Operating System : WINDOWS)

6/15/10 4:46 PM SYSTEM WindowsPROD2  
Message: Password Policy Checking API is called: Caller Username: Administrator

5 The DHCP service is not servicing any clients because no configured IP addresses, or there are no active clients.

6/15/10 4:46 PM WINDOWSTEST4  
Message: The DHCP service is not servicing any clients because no configured IP addresses, or there are no active clients.

1 WINS initialized properly and is now fully operational.

6/15/10 4:46 PM WINDOWSTEST4  
Message: WINS initialized properly and is now fully operational.

0 Password Policy Checking API is called (Operating System : WINDOWS)

6/15/10 4:46 PM SYSTEM WindowsPROD2  
Message: Password Policy Checking API is called: Caller Username: Administrator

5 Time Provider NtpClient (Operating System : WINDOWS) is not running.

6/15/10 4:46 PM WINDOWSTEST4  
Message: Time Provider NtpClient: An error occurred during DNS lookup.

0 Password Policy Checking API is called (Operating System : WINDOWS)

6/15/10 4:46 PM SYSTEM WindowsPROD2  
Message: Password Policy Checking API is called: Caller Username: Administrator

1 The Network Location Awareness (NLA) service entered the running state.

6/15/10 4:46 PM WindowsPROD2  
Message: The Network Location Awareness (NLA) service entered the running state.

1 The Network Connections service entered the running state.

6/15/10 4:46 PM WindowsPROD2  
Message: The Network Connections service entered the running state.

0 Password Policy Checking API is called (Operating System : WINDOWS)

6/15/10 4:46 PM SYSTEM WindowsPROD2  
Message: Password Policy Checking API is called: Caller Username: Administrator

Novell Log Manager Report as run on March 29, 2010 at 7:51:17 AM EDT | Page 1 of 1

### Top 10 Dashboard: Previous Month

All Vendors All Products  
February 1, 2010 12:00:00 AM to February 28, 2010 11:59:59 PM EST  
Severity: 1-5 (Advisory - Critical)

Severity: 0 1 2 3 4 5

Top 10 Target IP Addresses

Grouped by Severity Level

Target IP Address	Event Count
15.115.160.14	~45,000
164.99.18.235	~25,000
166.82.223.35	~15,000
164.99.18.1	~10,000
79.99.173.28	~5,000
131.238.84.14	~5,000
131.238.71.138	~5,000
102.161.21	~5,000
10.0.0.1	~5,000
10.0.0.10	~5,000

Top 10 Initiating IP Addresses

Grouped by Severity Level

Initiating IP Address	Event Count
64.93.179.116	~10,000
64.93.225.148	~5,000
10.0.0.6	~5,000
64.93.227.169	~5,000
131.238.234.154	~5,000
64.93.161.103	~5,000
64.93.238.83	~5,000
164.99.18.165	~5,000
164.99.18.17	~5,000
164.99.18.1	~5,000

Top 10 Target Host Names

Grouped by Severity Level

Target Host Name	Event Count
TargetHostname11	~1,500
TargetHostname10	~1,000
58YRHECOM	~500
TargetHostname12	~500
sentinel-2008-64	~500

Top 10 Initiating Host Names

Grouped by Severity Level

Initiating Host Name	Event Count
DUFFAPP03H	~200,000
TestMachine	~50,000
WONG	~50,000
SORTHECOM	~50,000

Top 10 Target User Names

Grouped by Severity Level

Target User Name	Event Count
Desktop01	~1,500
Desktop02	~1,000
Desktop03	~500
llwren	~500
Desktop11	~500
admin	~500
ypyo	~500
Desktop05	~500
Desktop04	~500
chestr2	~500

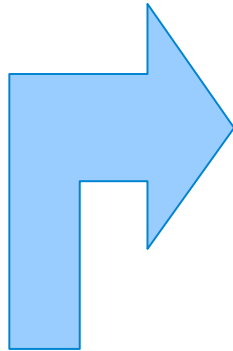
Top 10 Initiating User Names

Grouped by Severity Level

Initiating User Name	Event Count
SYSTEM	~200,000
System	~50,000
cpu_data	~50,000
Administrator	~50,000
inituser02	~50,000
inituser01	~50,000
MSB-0-0-2139	~50,000
J1165-5-10-02	~50,000
Directory Manager	~50,000
admin	~50,000
Unknown	~50,000

# NetIQ® Security Solutions

## NetIQ® Sentinel



### Monitorización y Correlación



### Log Management



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

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

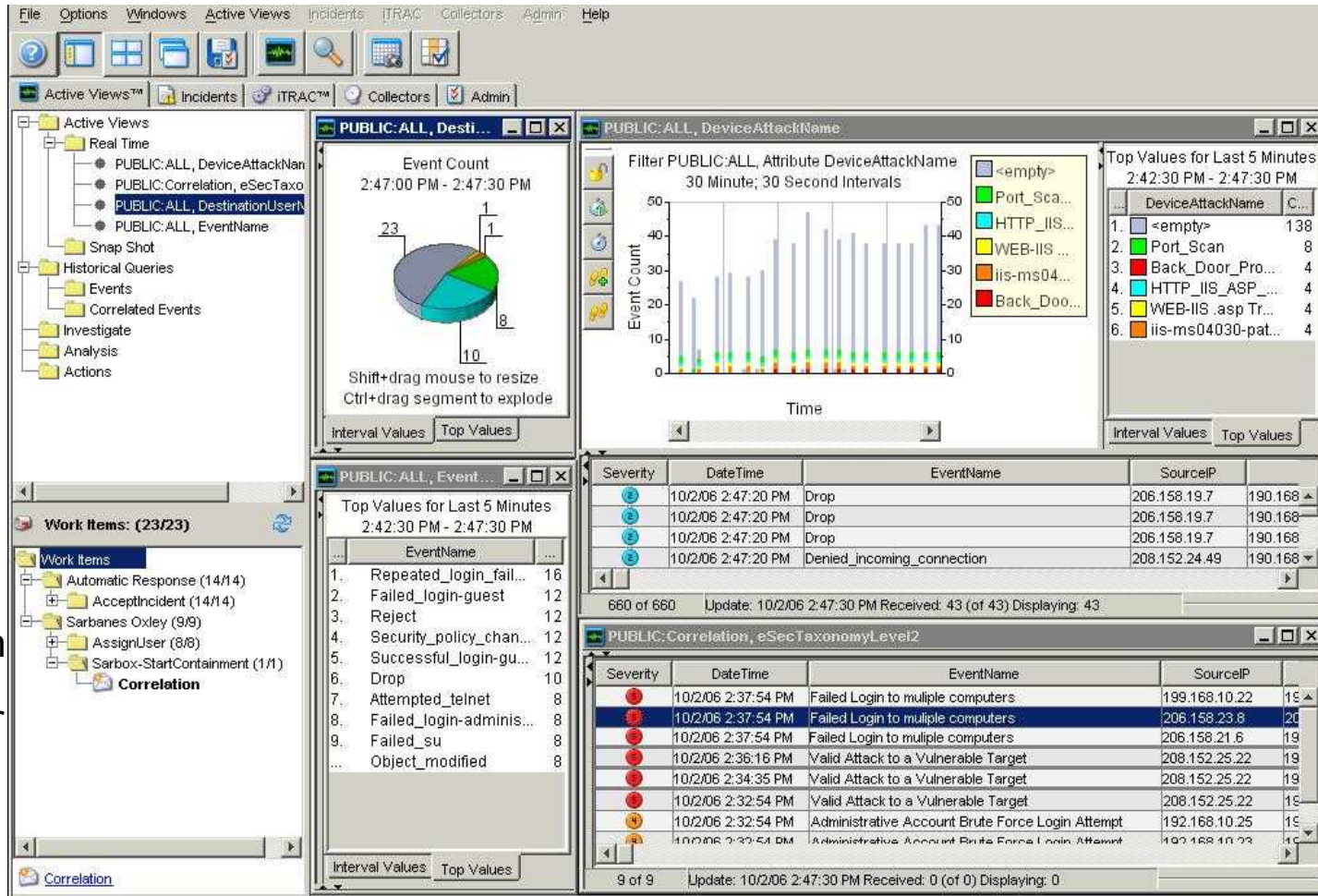
# NetIQ Sentinel SIEM

## Monitorización, Análisis y Correlación

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

### Beneficios:

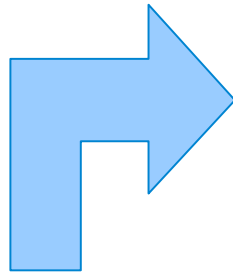
- Identificar tendencias, ataques o violaciones
- Priorizar y gestionar esfuerzos de corrección
- Manipular e interactuar con datos en tiempo real
- Generación manual de incidencias



nivel del  
esquema

# NetIQ® Security Solutions

## NetIQ® Sentinel



### Log Management

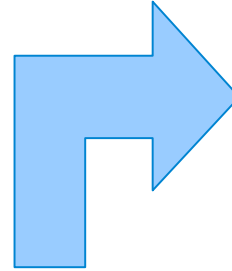


- Informes de auditoría y cumplimiento
- Recolección, Almacenamiento y Análisis
- Analíticas avanzadas

### Monitorización y Correlación



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



### Integración con la identidad



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

# Gestión del riesgo

## Herramientas operativas del día a día

**Address Book**

James Smith  
Project Manager  
Marketing

james.smith@acm  
(202) 555-1212

SHOW: **User Profile** Recent Acti

**Identity GUID** JS-234-99534-R  
**Distinguished Name** JAMES.SMITH.23  
**Work Force ID** 88236  
**Location** New York, NY  
**Mailstop** NYC-1-100  
**Badge ID** 39-4559-3123-3

¿Quién?

**Address Book**

James Smith  
Project Manager  
Marketing

james.smith@acm  
(202) 555-1212

SHOW: **User Profile** **Recent Acti**

**Authentication Information**

JAMES-WS terminal login succe:  
CREDIT-DB1 remote login failer:  
CREDIT-DB1 remote login succe:

**Access Events**

CCDB:db\_users data object near  
CCDB:CCDATA data object read:  
CCDB:CCDATA data object read:

**Permission Changes**

jsmith@CCDB granted read on Cl  
cc-dba@CCDB

¿Como?

**Address Book**

James Smith  
Project Manager  
Marketing

james.smith@acmecorp.com  
(202) 555-1212

SHOW: **User Profile** **Recent Activity** **Accounts**

USER ID	DOMAIN
james.smith	intranet.acmecorp.com
jsmith	timesheet.acmecorp.com
jsmith	projecttrack.acmecorp.com

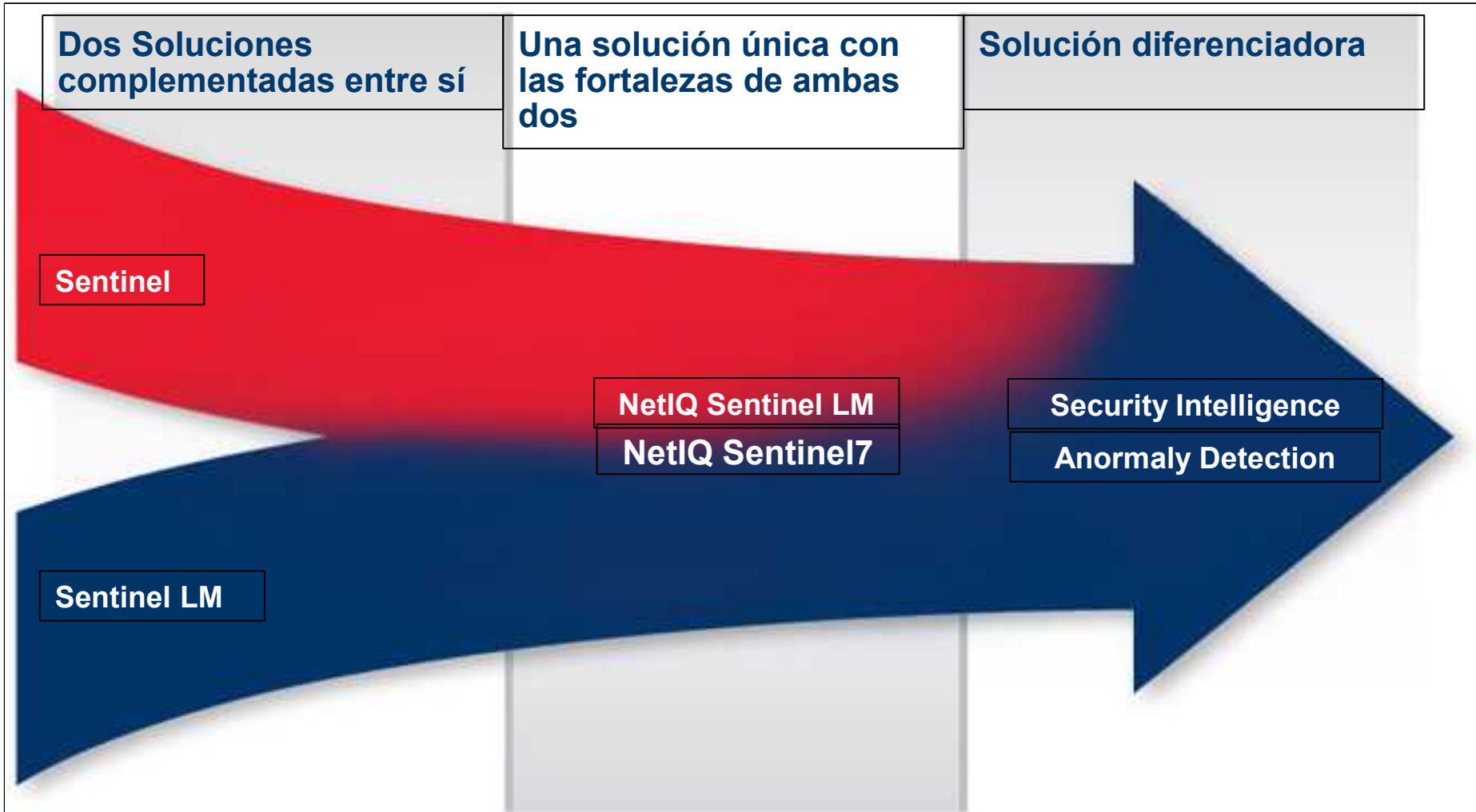
¿Por qué?

# **Nueva Versión Sentinel 7**



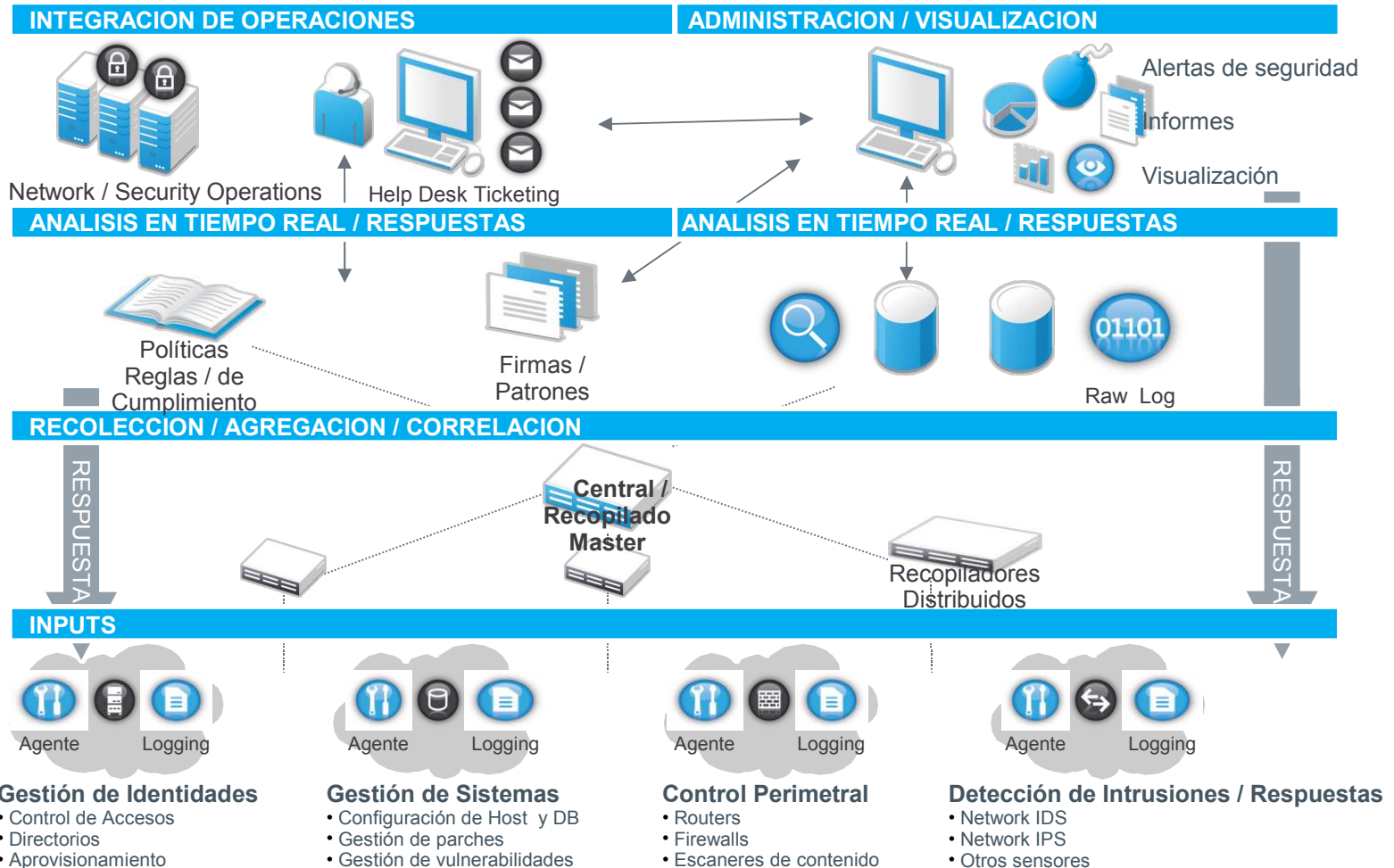
# NetIQ Security Management

**SIM + SEM = SIEM**



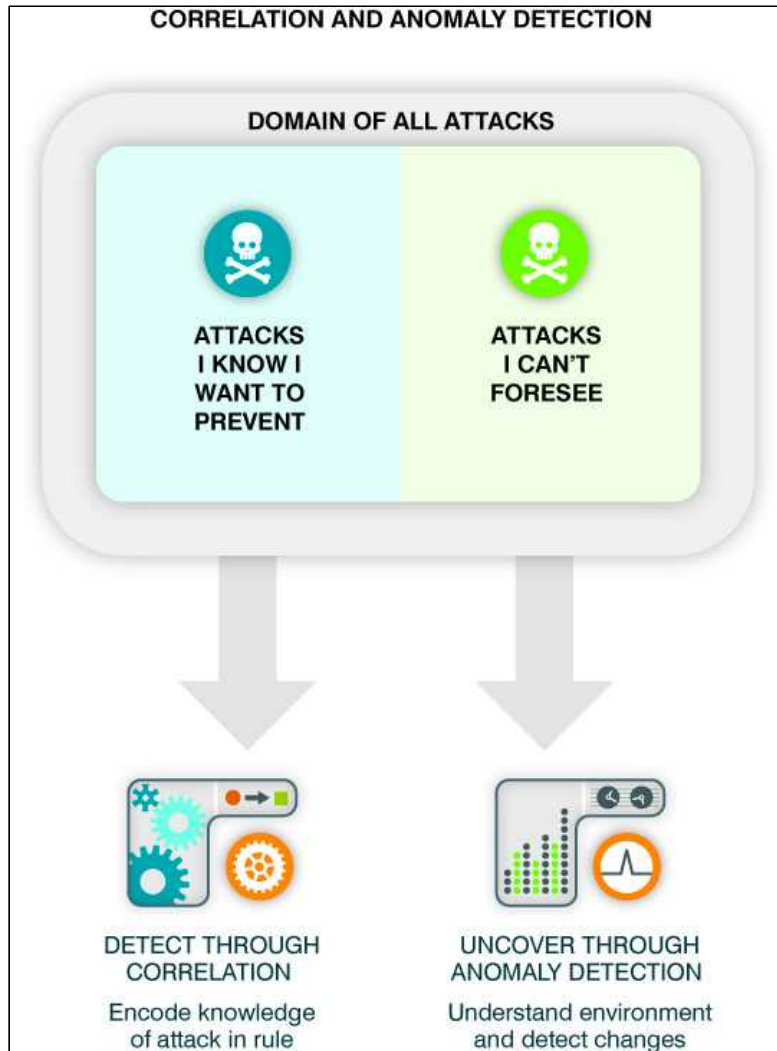
# NetIQ® Security Solutions

## Modelo de referencia de **Burton**



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

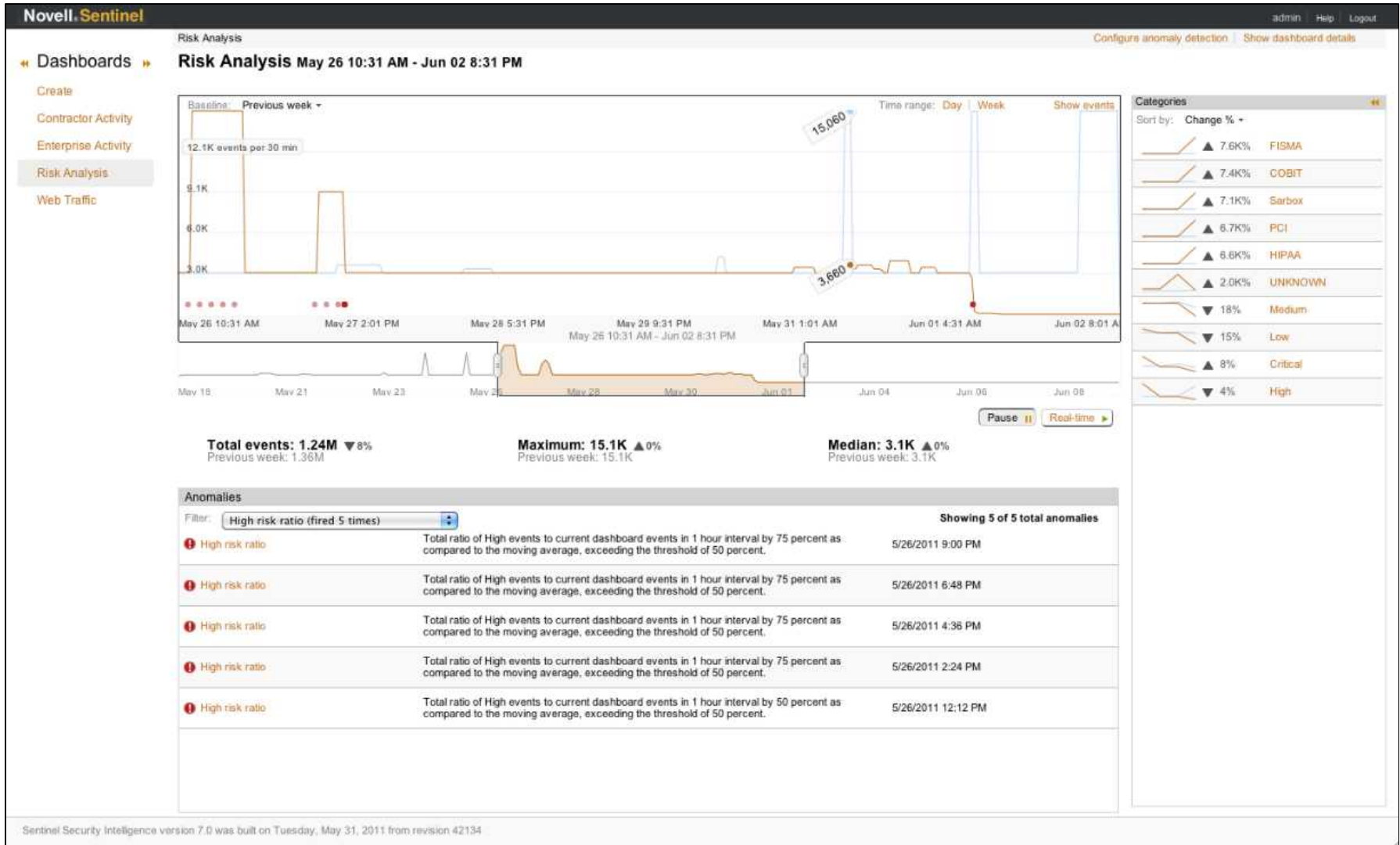
- Relationship between two or more sets of data
- Something I can foresee and want to take immediate action

# 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](mailto:info@netiq.com)  
[NetIQ.com](http://NetIQ.com)

 Join NetIQ's Online  
**QMUNITY**   

<http://community.netiq.com>