



NitroSecurity  
Unifying Information Security

# Incorporating Database Security into the SOC/NOC

Suncoast Oracle Users Group  
FL - 8/27/2009

# Agenda



- DB Security Primer
- Integrated DB Security
- DAM Features / Demo

nitrosecurity.com



# Database Security Primer



## Data Discovery

Classify sensitive data



## Vulnerability Assessment

Database & host hardening

## Data Access Policy

Define roles, rights, realms

## Leakage Prevention

Enforce use policy  
De-identify data for sharing

## Database Monitoring

Audit log  
Identify/block attacks

## Protecting Data-at-Rest

Encryption  
Secure backups



# Database Security Challenges

---



## ■ Technical Challenges

- Data is constantly in motion
- Huge volumes of activity to monitor and log
- Compliance mandates segregation of security duties from DBAs
- Log full audit-trail of administrator activity
- Business & DBAs require monitoring without impacting application performance

## ■ Budgetary & Resource Limitations

- Databases (imp nevertheless) are only a component of overall security
- Staffing (need someone other than the DBA) - can it be the SOC/NOC?

## ■ SOC/NOC perception of databases & apps - it's a different beast

- Hard to deploy & manage
- Events not easily understood by SOC/NOC teams

# Top Database Security Threats



- Excessive Privilege Abuse
- Legitimate Privilege Escalation
- Privilege Elevation
- Database Platform Vulnerabilities
- SQL Injection
- Weak Audit Trail
- Denial of Service
- Database Communication Protocol
- Weak Authentication
- Backup Data Exposure



## Primary Use Cases

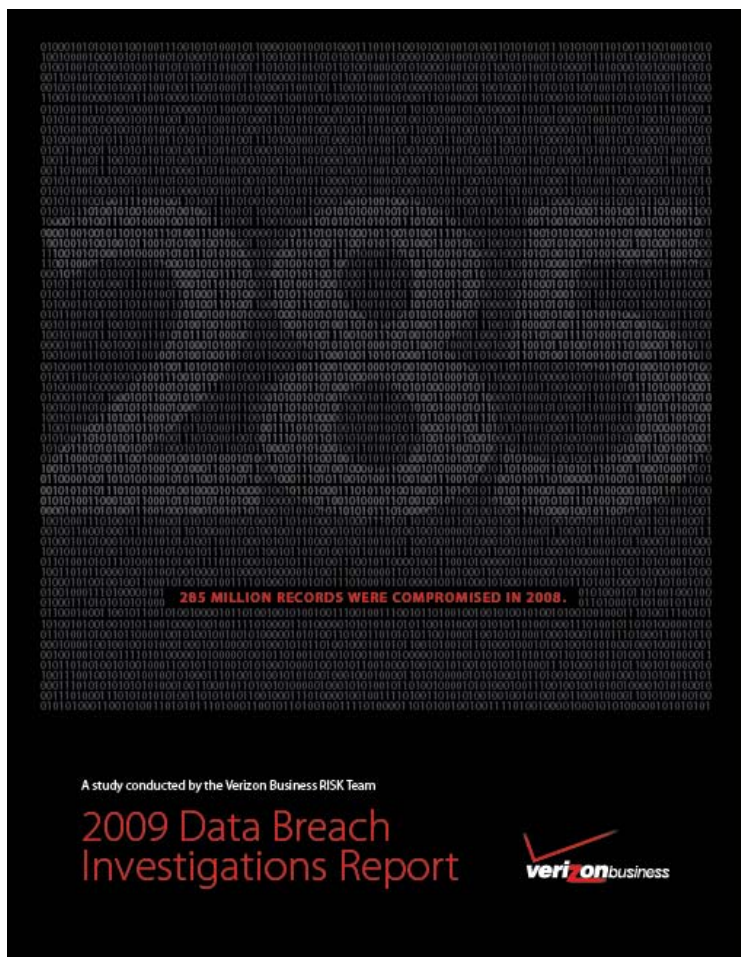
Privileged user monitoring

Fraud detection & monitoring

Database protection

*Source GNC Computer News*

# Verizon Data Breach Investigations Report



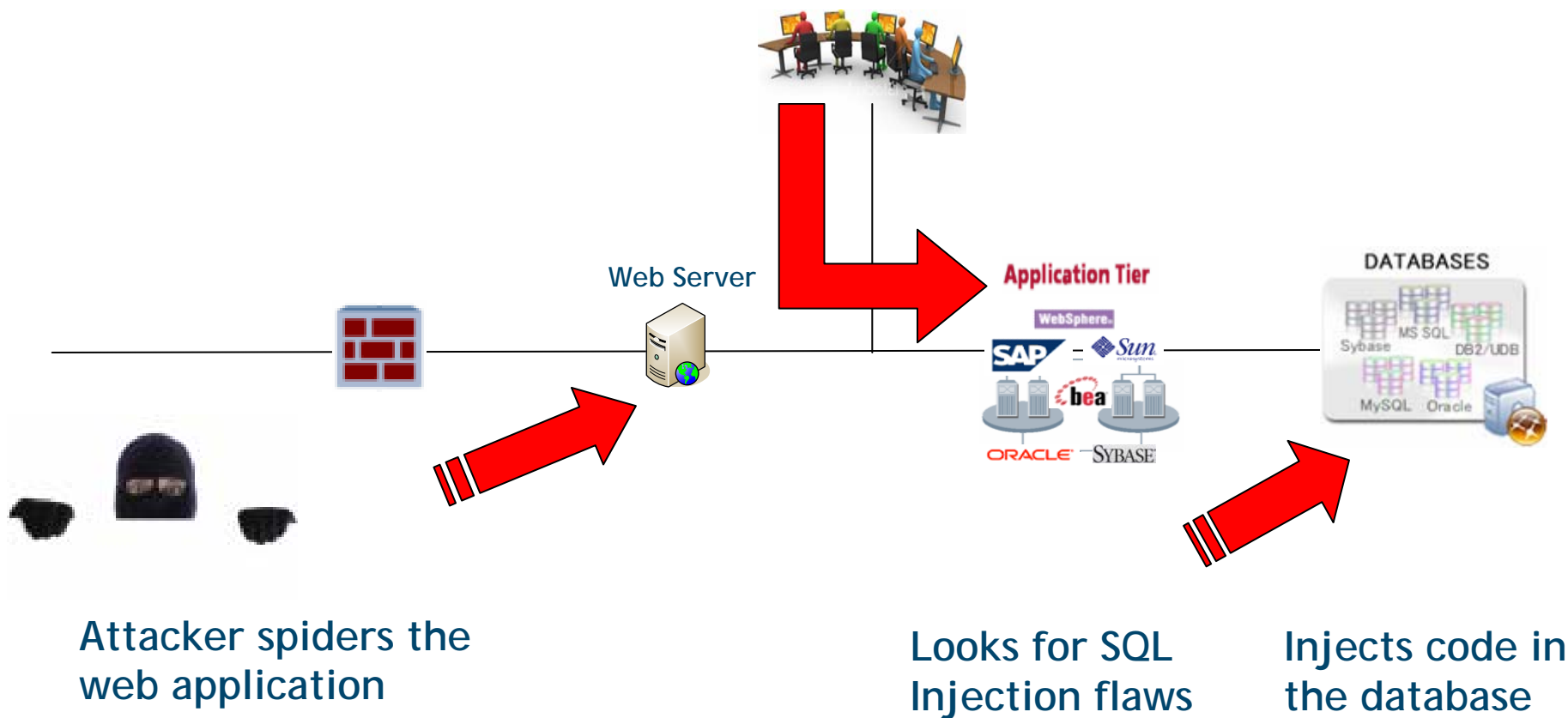
- Most widely used attack path
  - Web application, 79%
- Most widely compromised asset by number of records
  - Database server, 75%
- Most compromised data type
  - Payment card data, 98%
- Type of assets misused
  - Database Server, 23%
- Encryption provides limited effectiveness
- Auditing DDL != Security

# Attack Scenario - Many Ways to Skin a Cat



Waits for user to access the database

Browser executes malicious code

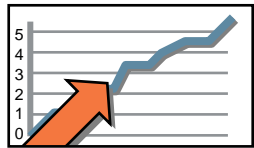


# Role of the SOC & NOC



## NOC

Optimize repeatable tasks



- Availability
- Performance
- Capacity

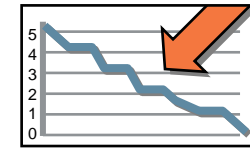
Common  
collection and  
reporting

Different event  
analytics

- 24/7 network security monitoring (SIEM integration)
- Use SIEM for change detection

## SOC

Discover and investigate  
"abnormal" activity



- User
- Payload
- Behavior



**Controlled by IT Security:**

- Privileged user monitoring
- Security incident management

**Workflow integration**

**Source Gartner**



## Role of a DBA in Preventing Breaches

---



- Ensure essential controls are met
- Find, track, and assess data
- Collect and monitor logs
- Audit user accounts and credentials
- Test and review web applications

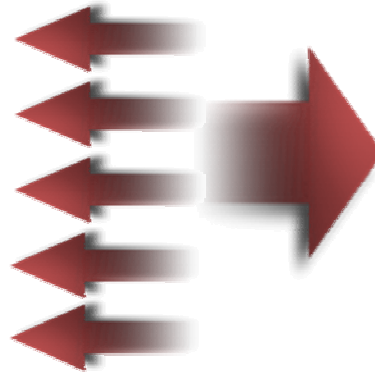
Rise of the Application Security Officer (ASO)  
**ASO's Role: Bridge between SOC/NOC and  
Application Teams**

# Application Aware Baseline Example - Theft of User Credentials



## Violation Check

User → Environment:	✓
User → Terminal:	✗
User → Operation:	✓
Operation → Environment:	✓
User → Object:	NO CHECK



## Sample Result

ACTION value:

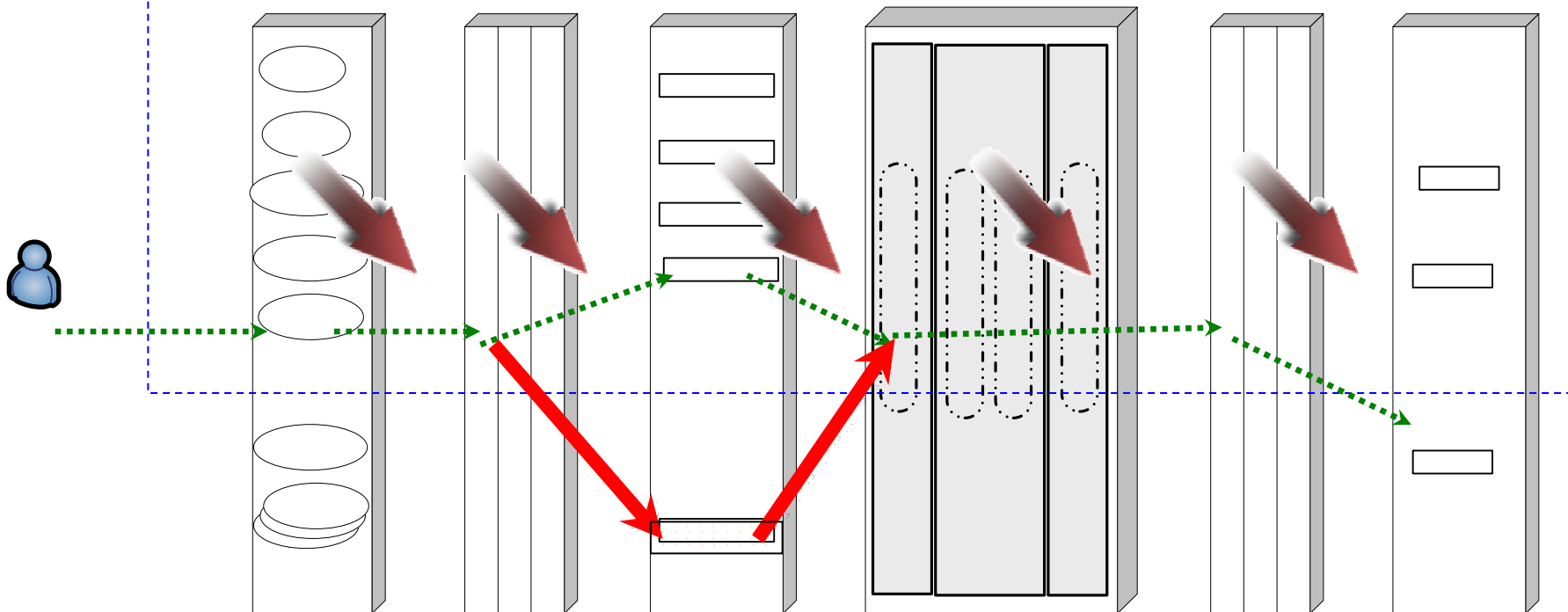
env\_u\_NOVIOL-term\_ISVIOL-op\_  
NOVIOL-env\_op-NOVIOL-obj-NOCHK

VIOLATION value:

ISVIOL



## Application Aware Baseline



# Pitfalls with Native Database Audit Controls



- Performance Impact
- Information in native logs is inferior
- Cannot correlate series of events for root cause analysis
- Cannot discover and prevent database attacks
- Cannot monitor content - who accessed sensitive data?
- Cannot track a person using a generic database login or application
- Cannot mask sensitive content
- Software only solutions (harder to deploy & manage)
- No integration with SIEM, Log Mgmt, Alerting, Enterprise solutions
- No secure central logging, reporting and notification
- Hard to segregate database security duties from the DBA

# Monitoring Technologies



- Requires SIEM, DAM, DLP, Application Monitoring, etc.
- Increased cost from multiple technologies
- Reduced productivity from multiple consoles

Source Gartner

	SIEM	DAM	DLP	Fraud Detection
Application activity				
Application access				
Database activity				
File access				
DB activity: privileged user				
System activity: privileged user				
Network activity: user				

User activity at this layer is not visible

User activity at this layer is visible in a broad set of use cases, but other technologies provide deeper monitoring.

This technology is a primary monitoring method for this layer.

User activity at this layer is visible, but monitoring is limited to the primary use cases of the technology.

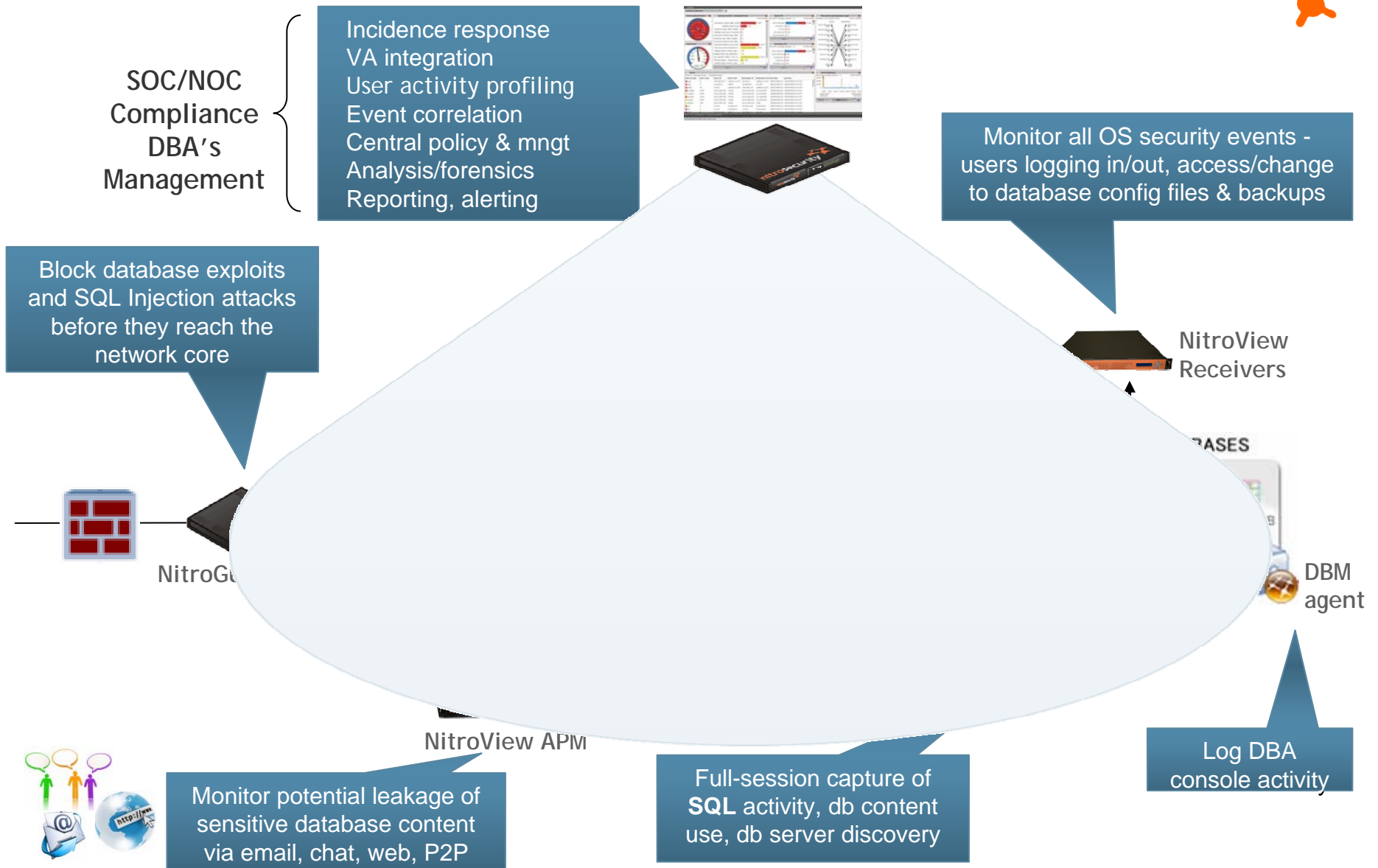
# Security Solution Technologies: Deployment Phases



*SOX, PCI, HIPAA, Breach Disclosure Laws*

- Phase I - VA, Antivirus, Firewall, IPS/IDS, Access Control
- Phase II - SIEM Deployment (Network Perimeter & Host)
- Phase III - Monitor Databases & Applications
- Phase IV - Prevent Leakage of Sensitive Data (DLP)

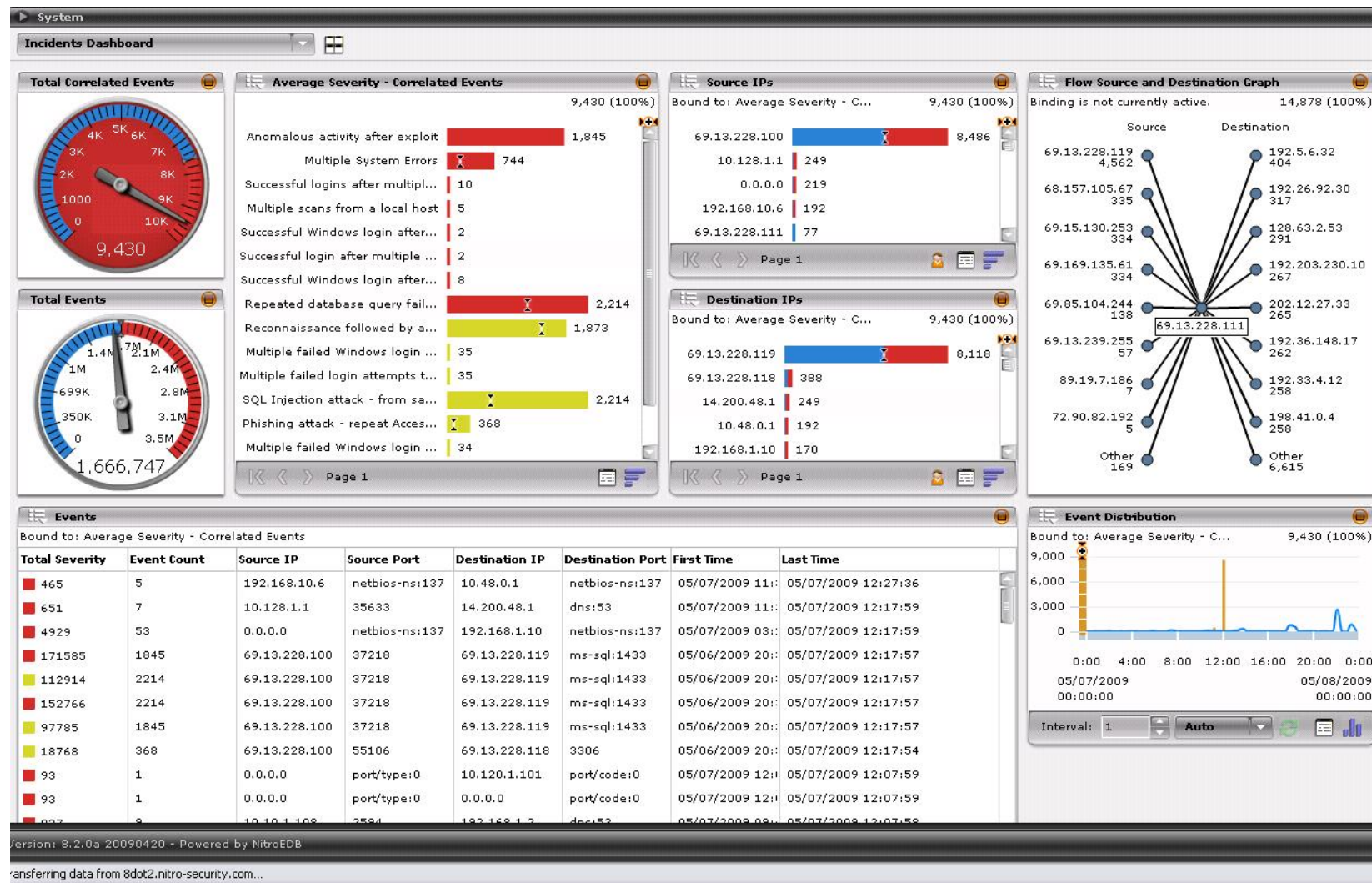
# Integrated Database & Application Security



# Database Activity & Event Correlation



- Advanced Visualization, Activity Baseline, Event Analysis & Drill-down



# Pre-defined Database Views and Graphical Reports



The screenshot displays the NitroView™ interface with the following components:

- System - ngdbm** (selected in the left sidebar)
- DB Schema Changes** (selected in the top menu)
- Database Servers** (selected in the top menu)
- Database Users** (selected in the top menu)

**DB Schema Changes** (Horizontal Bar Chart):

Event	Count
MSSQL - Procedure Dropped	8
MSSQL - View Dropped	8
MSSQL - Function Created	8
MSSQL - Function Dropped	8
MSSQL - Table Dropped	6
MSSQL - Procedure Created	6
MSSQL - Database Dropped	5
MSSQL - Database Created	5
Oracle - Procedure Created	4
Oracle - Procedure Dropped	4
Oracle - Function Dropped	4
Oracle - Trigger Created	4
Oracle - Trigger Dropped	4
MSSQL - View Created	4
MSSQL - Function Altered	4
MSSQL - Trigger Created	4
MSSQL - Trigger Dropped	4
Oracle - View Created	3
Oracle - View Dropped	3
Oracle - Table Altered	1

**Database Servers** (Horizontal Bar Chart):

Server	Count
68.0.40	99
68.0.15	69

**Database Users** (Pie Chart):

User	Count
sa	99
system	42
hr	27

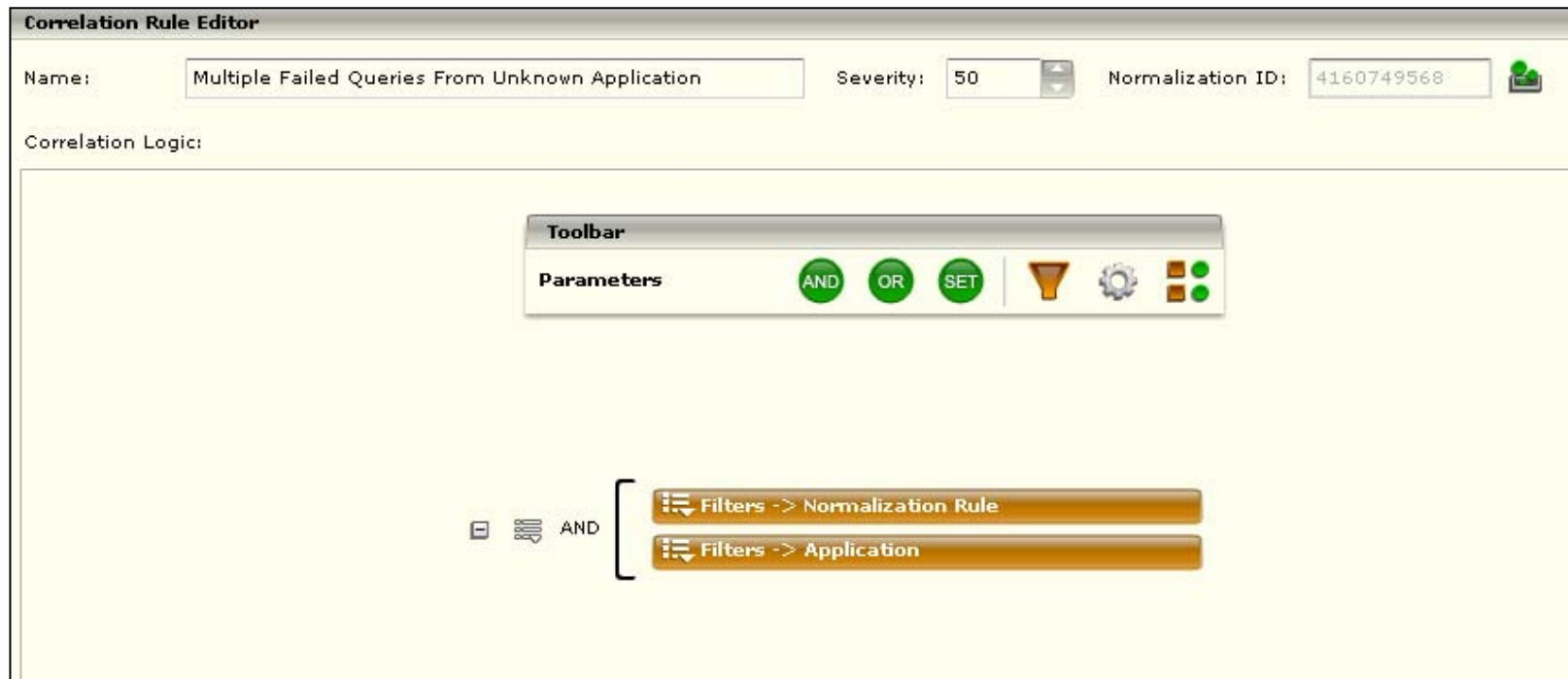


# Correlation Rule Editor



- Correlation with security events, flows, application logs, identity & VA tools
- Over 150 devices support out-of-box

Security  
Correlation



# Central Policy Management & Rollout



**Policy Editor**

File New Edit Tools Operations Search: **Signature ID**

Current Policy: **ngdbm**

**Variable** **Data Source** **Normalized**

**Name**

- Antivirus
- Application\_Devices
- Authentication
- Correlation
  - Correlation Engine
- Database
  - DB2
  - MSSQL**
  - MySQL
  - NitroView Database
  - Oracle
  - Svbase

Name	Action	Severity	Compr...	Copy Packet
MSSQL - Discover Unauthorized Applications	al...	70	off	off
MSSQL - DML Statement	in...	10	off	off
MSSQL - DTS Password Scan	al...	70	off	off
MSSQL - Extended Procedures	al...	70	off	off
MSSQL - Failed Logins	fa...	40	off	off
<b>MSSQL - Failed Superuser Logins</b>	<b>fa...</b>	<b>70</b>	<b>off</b>	<b>off</b>
MSSQL - Failed Transactions	er...	40	off	off
MSSQL - Function Altered	m...	40	off	off
MSSQL - Function Created	add	40	off	off
MSSQL - Function Dropped	re...	40	off	off
MSSQL - Grant ALL	al...	70	off	off
MSSQL - Grant Option	al...	70	off	off

Signature ID: 62-10035

Signature: (("user\_name" EQ "sa") AND (((("message\_number" EQ "18450") OR ("message\_number" EQ "18451")) OR ("message\_number" EQ "18452")) OR ("message\_number" EQ "18456")))

Description: Failed Superuser Login

# Discovery of Sensitive Content



**Policy Editor**

File New Edit Tools Operations Search: **Signature ID**

Current Policy: **ngdbm**

**Variable** **Data Source** **Normalized**

**Name**

- Antivirus
- Application\_Devices
- Authentication
- Correlation
  - Correlation Engin
- Database
  - DB2
  - MSSQL**
  - MySQL
  - NitroView Databa:
  - Oracle
  - Svbase

Name	Action	Severity	Compr...	Copy Packet
MSSQL - Database Backup	w...	40	off	off
MSSQL - Database Configuration Changes	al...	70	off	off
MSSQL - Database Created	add	80	off	off
MSSQL - Database Dropped	re...	80	off	off
MSSQL - Database Restore	w...	40	off	off
MSSQL - DB Server Discovered	n...	15	off	off
MSSQL - DBCC Command	w...	40	off	off
MSSQL - DBCC Permission Denied	cr...	80	off	off
MSSQL - DBO Changed	cr...	80	off	off
<b>MSSQL - Discover Sensitive Data</b>	<b>cr...</b>	<b>80</b>	<b>off</b>	<b>off</b>
MSSQL - Discover Social Security Numbers	cr...	80	off	off
MSSQL - Discover Unauthorized Applications	al...	70	off	off

Signature ID: 62-10003

Signature: ("response\_content" REGEXP "((4\d{3})|(5[1-5]\d{2})|(6011))-?\d{4}-?\d{4}-?\d{4}|3[4,7]\d{13}")

Description: Sensitive Data Access

**Close**

# Application User Tracking



- Correlating the SQL transaction with another data source
- Identifying a user-identifier/token in the SQL

User Identifier Rules. This feature provides a way to discover the real user by looking for a unique identifier in the database queries even when the application accesses the database using a generic login name.

Rule Name	Appli	Expression
Get Real Username from Proc Param	Oracle	spCommitTrade @username=(\w+), @a

**Add**

**Edit**

**Remove**

**User Identifier Rules**

Configure user identifier rule.

Identifier rule name:

Expression:

Application:

Sub String Index:

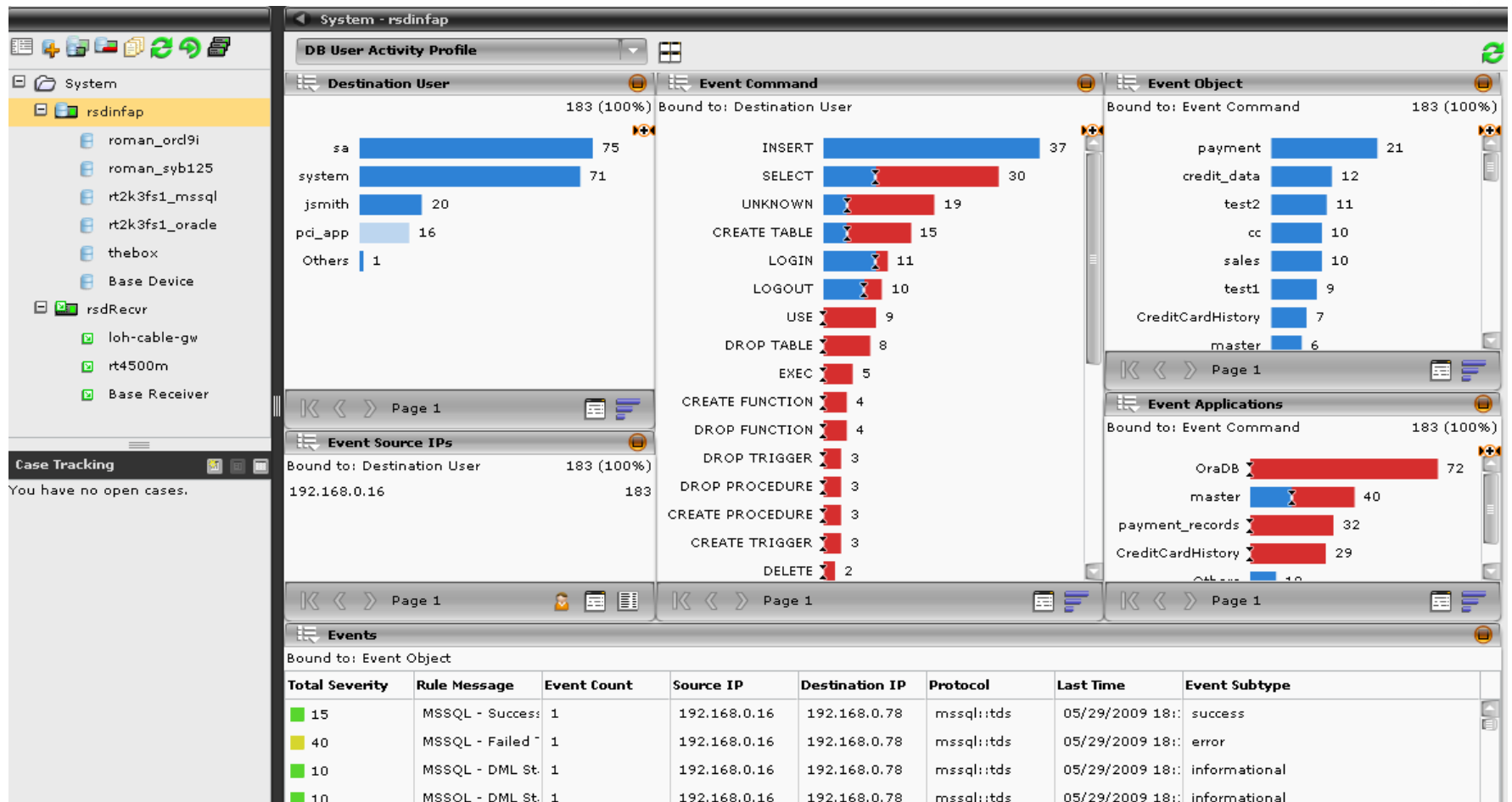
**OK** **Cancel**

# User Activity Profiling



- Commands and objects are accessed by a user and deviation from normal behavior

© 2010



# Sensitive Data Masking



Sensitive Data Masks. This feature prevents unauthorized viewing of sensitive data that may be present in the event record by replacing the sensitive data with a generic user configurable mask.

Mask Name	Expression	Mask
Mask Credit Card Numbers	((((4\d{3}) (5[1-5]\d{2}) (6[01]\d{2}) (7[013]\d{2}))\d{14}))	####-####-####-####
Mask SSN	(\d\d\d-\d\d)-\d\d\d\d\d	###-##-####

**Add**  
**Edit**  
**Remove**

**Sensitive Data Masks**

Configure sensitive data mask.

Sensitive mask name:

Expression:

Sub String Index:

Masking Pattern:

**OK** **Cancel**

# Integrated Agent Management



**Database Servers. The**

Name
penguin_udbv81
roman_orai
roman_syb1192
RT2K3FS1
thebox

**Edit Database Server**

Configure parameters to monitor database activity. If an agent is installed on the database, additional events may be captured.

Enabled: ☒

Database type: **MSSQL**

Database Server Name: thebox

Device URL: (Optional)

IP Address: 192.168.0.75

Virtual LAN ID:

Encoding Option: **None**

Select Special Options: **None**

Port: 1433

The Agent software must be installed on the target database writing these settings to the DBM. To download the software,

Enable Agent: ☒

Database User: sa

Database Password: \*\*\*\*

Audit Settings: **Localhost activity**

Database Path: C:/Program Files/Microsoft SQL Server/MSSQ

Database Name: db\_audit

Instance Name: -

**Add**

**Edit**

**Remove**

**Audit Filters**

Configure comma separated filter strings used for monitoring network traffic. Events will be limited by the provided filters.

Users: sa

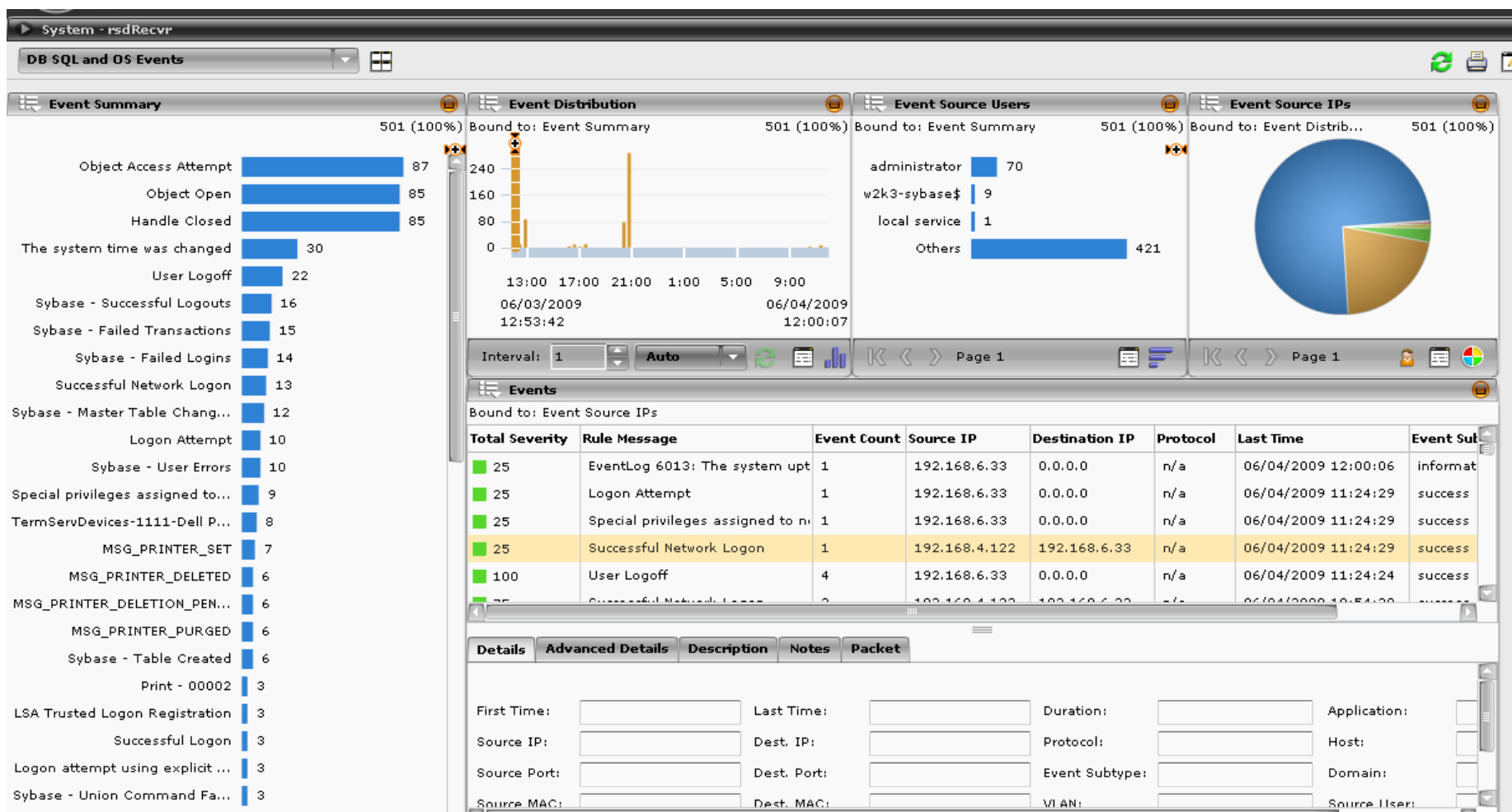
Exclude Applications: Replication%

Objects:

**OK** **Cancel**

**Delete DBM Agent**

# Monitoring of Database Config & Backup Files





# Database Change Control Management



The screenshot shows the NitroSecure ngdbm interface. On the left, a sidebar menu lists various views: Compliance Views, Dashboard Views, Database Views, Event Views, Flow Views, and Device Status. Below these are specific event categories like 'MSSQL - Master Table Changes', 'Oracle - DB Server Discovered', 'MSSQL - Table Created', 'MSSQL - Failed Transactions', and 'Oracle - DML Statement'. The main area displays an 'Event Distribution' chart with a y-axis from 0 to 2,000 and an x-axis showing time from 0:00 to 18:00. A 'Transaction Tracking Rule Editor' dialog box is open in the foreground, prompting the user to fill out a form to create a rule. The form includes fields for Rule Name, Start Query Tag, Stop Query Tag, Normalized ID, Severity, and a Description. The 'Rule Name' field contains 'Tag Change Control Events', 'Start Query Tag' is 'spChangeControlStart', 'Stop Query Tag' is 'spChangeControlEnd', 'Normalized ID' is '0', and 'Severity' is '50'. The 'Description' field contains the text: 'Tag change control events with the number passed as the first argument to the stored procedure'. The dialog has 'OK' and 'Cancel' buttons at the bottom.

# Full Session Detail



- Drill-down from an event to full session detail

**Session Viewer**

View details about the selected session or download a CSV file of the session data. [Download CSV file](#)

<b>Client IP:</b> 192.168.0.16	<b>Client Port:</b> 33280	<b>Client Name:</b> penguin
<b>Server IP:</b> 192.168.0.15	<b>Server Port:</b> 6868	<b>Server Name:</b> roman

<b>Query Num:</b> 0	<b>Message:</b> 5701	<b>Data In:</b> 1222 bytes
<b>Begin Time:</b> 05/29/2009 18:16:10	<b>Severity:</b> 10	<b>Data Out:</b> 320 bytes
<b>Response Time:</b> .4 sec	<b>Database:</b> "-"	<b>Rows:</b> 0
<b>Server Time:</b> .4 sec	<b>Application:</b> "-"	
<b>Query Text:</b> "Login:sa@penguin:33280		
<b>Response Text:</b> Changed database context to 'master'. t in Syscharsets: name = 'utf8', "		

<b>Query Num:</b> 1	<b>Message:</b> 17262	<b>Data In:</b> 96 bytes
<b>Begin Time:</b> 05/29/2009 18:17:14	<b>Severity:</b> 16	<b>Data Out:</b> 316 bytes
<b>Response Time:</b> .3 sec	<b>Database:</b> "-"	<b>Rows:</b> 0
<b>Server Time:</b> .3 sec	<b>Application:</b> "-"	
<b>Query Text:</b> "sp_addlogin kallol,polaris,master		
<b>Response Text:</b> A user with the specified login name already exists. "		

<b>Query Num:</b> 2	<b>Message:</b> 17330	<b>Data In:</b> 80 bytes
<b>Begin Time:</b> 05/29/2009 18:17:14	<b>Severity:</b> 16	<b>Data Out:</b> 338 bytes
<b>Response Time:</b> .3 sec	<b>Database:</b> "-"	<b>Rows:</b> 0
<b>Server Time:</b> .3 sec	<b>Application:</b> "-"	
<b>Query Text:</b> "sp_adduser kallol,kallol		
<b>Response Text:</b> A user with the same name already exists in the database. "		

<b>Query Num:</b> 3	<b>Message:</b> 1805	<b>Data In:</b> 100 bytes
<b>Begin Time:</b> 05/29/2009 18:17:14	<b>Severity:</b> 10	<b>Data Out:</b> 127 bytes
<b>Response Time:</b> .675 sec	<b>Database:</b> "-"	<b>Rows:</b> 0
<b>Server Time:</b> .675 sec	<b>Application:</b> "-"	

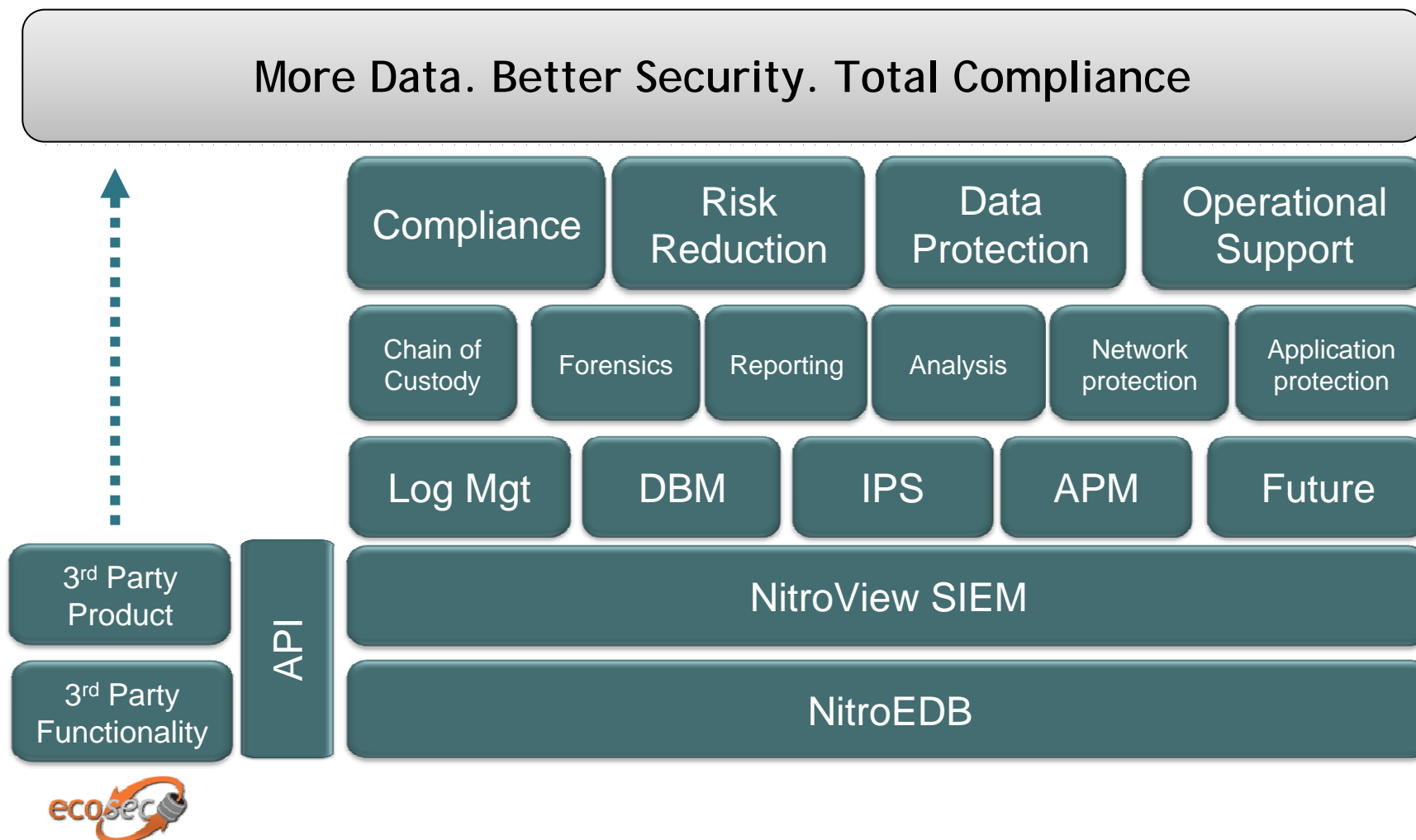
Close

# Full Session Detail



sec_flag	begin_time	end_time	response_time	server_response_time	begin_time_skew	client_ip	server_ip	
	client_port	server_port	query_number	query_exit_status		data_in	data_out	
	packets_out	network_time	client_name	user_name	application_name	server_name	nt_client_Name	
	nt_user_Name	nt_domain_Name	query_type	error_code	error_severity	error_message	client_pid	return_rows
	query_text	database_name	spid					
2	9/6/2005 12:17	9/6/2005 12:17	0.008	0.004	5	192.168.1.5	192.168.1.100	55870
	1433	0	0	615	168	3	2	0.004
	roman	sa	TSQL	192.168.1.100	-	-	-	2
	0	-	14131	0			master	51
2	9/6/2005 12:17	9/6/2005 12:17	0.003	0.001	5	192.168.1.5	192.168.1.100	55870
	1433	1	4096	50	193	2	2	0.002
	roman	sa	TSQL	192.168.1.100	-	-	-	1
	0	-	14131	0	USE Northwind	Northwind	51	0
2	9/6/2005 12:17	9/6/2005 12:17	0.002	0.002	5	192.168.1.5	192.168.1.100	55870
	1433	4	4096	50	17	1	1	0.000
	roman	sa	TSQL	192.168.1.100	-	-	-	1
	0	-	14131	0			Northwind	51
10248	Northwind	51						
2	9/6/2005 12:17	9/6/2005 12:17	0.001	0.001	5	192.168.1.5	192.168.1.100	55870
	1433	15	4096	50	204	1	1	0.000
	roman	sa	TSQL	192.168.1.100	-	-	-	1
	587333632	16						
Error::DELETE statement conflicted with COLUMN REFERENCE constraint 'FK_Order_Details_Orders'. The conflict occurred in database 'Northwind', table 'Order Details', column 'OrderID'. CROW								
			14131	0			DELETE FROM	
			Orders WHERE OrderId IN ( '11072', '11076')	Northwind	51			
2	9/6/2005 12:17	9/6/2005 12:17	0.000	0.000	5	192.168.1.5	192.168.1.100	55870
	1433	16	0	0	0	0	0	0.000
	roman	sa	TSQL	192.168.1.100	-	-	-	0
	0	-	14131	0			Northwind	51

# Web API



# Auto Discovery of Databases & Easy 1-Step Setup



- Database Discovery
- Setup & Configuration
  - Add DBM Device, Add Database Servers, Add Optional Database Agents

The screenshot displays the NitroSecurity management console. On the left, a sidebar lists system components under 'System - ngdbm', including 'penguin\_udbv81', 'roman\_orc9i', 'roman\_syb1192', 'RT2K3FS1', 'thebox', 'Base Device', and 'nsrecv'. Below this is a 'Properties' section with buttons for 'Add Database Server', 'Copy DBM', 'Delete DBM', 'Policy Manager', 'Refresh Devices', 'Get Events', and 'Multi-Device Management'.

The main area is divided into two panes. The top pane, titled 'System - ngdbm', shows a 'Default Summary' and an 'Event Summary' table. The 'Event Summary' table lists various MSSQL events and their counts:

Event	Count
MSSQL - DML Statement	2,711
MSSQL - Master Table Changes	2,711
MSSQL - Table Created	2,711
MSSQL - Failed Transactions	2,711
MSSQL - Login Info Scan	904
MSSQL - Server Configuration Changes	904
MSSQL - Configuration Change	904
MSSQL - Database Configuration Changes	904

The bottom pane, titled 'Event Distribution', shows a bar chart of event counts over time. The x-axis represents time from 0:00 to 18:00 on 02/11/2009. The y-axis represents the count, ranging from 0 to 3,600. The chart shows a peak in activity around 3:00.

On the right, the 'Edit Database Server' dialog box is open, showing configuration parameters for an MSSQL database server named 'thebox'. The parameters include:

- Enabled: ☒
- Database type: MSSQL
- Database Server Name: thebox
- Device URL: (Optional)
- IP Address: 192.168.0.75
- Virtual LAN ID:
- Encoding Option: None
- Select Special Options: None
- Port: 1433
- The Agent software must be installed on the target database prior to writing these settings to the DBM. To download the software, click here.
- Enable Agent: ☒
- Database User: sa
- Database Password: \*\*\*\*
- Audit Settings: Localhost activity
- Database Path: C:/Program Files/Microsoft SQL Server/MSSQ
- Database Name: db\_audit
- Instance Name: -
- Delete DBM Agent