ИНФОСИСТЕМЫ ДЖЕТ

17 лет на рынке информационной безопасности

Решения Imperva для защиты СУБД

Бейбутов Эльман

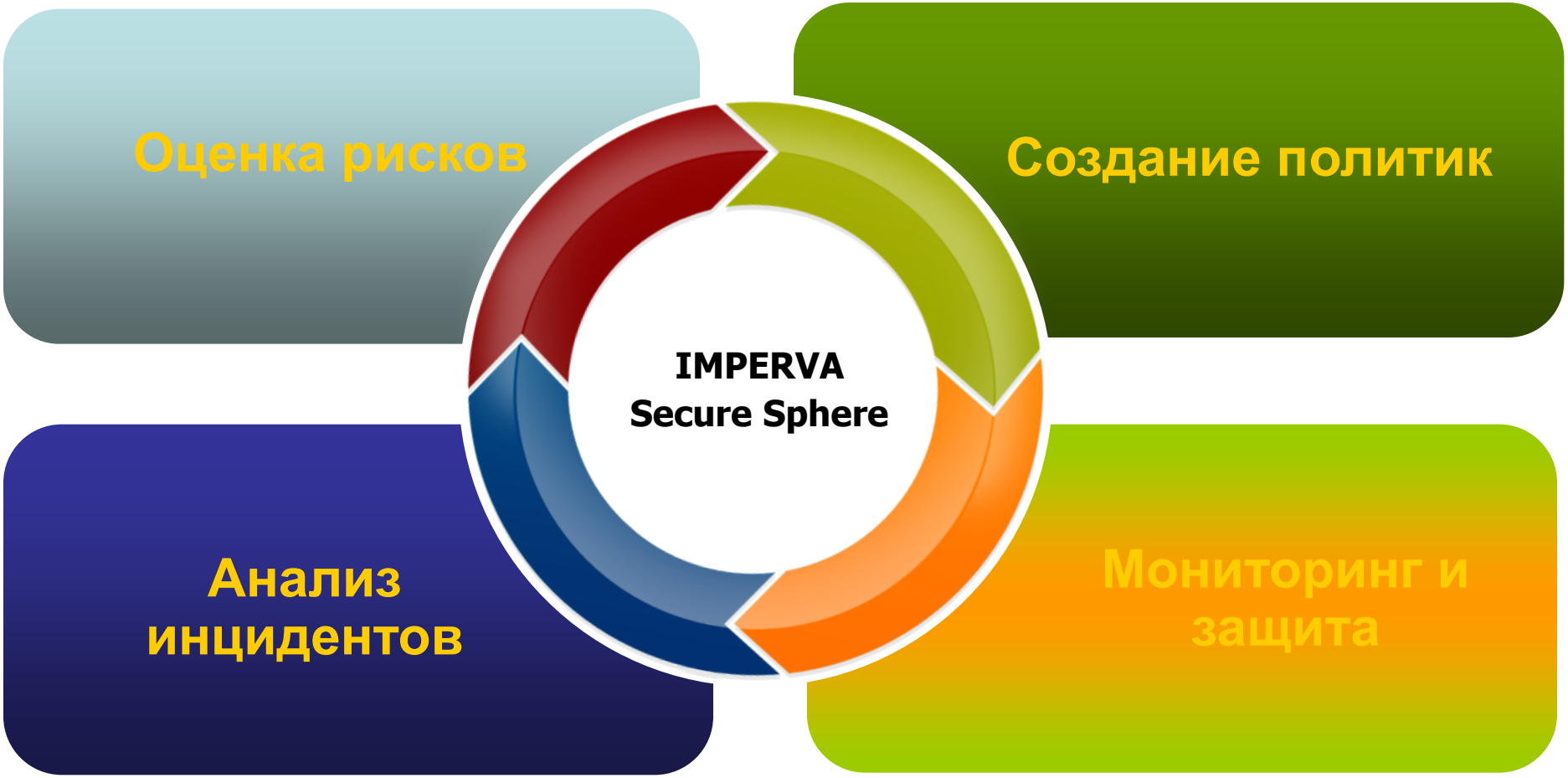
Руководитель направления защиты БД и SOC

10 апреля 2014 г.

Комплекс решений Imperva SecureSphere

© 2014 Инфосистемы Джет

LifeCycle защиты СУБД



© 2014 Инфосистемы Джет

ИНФОСИСТЕМЫ ДЖЕТ

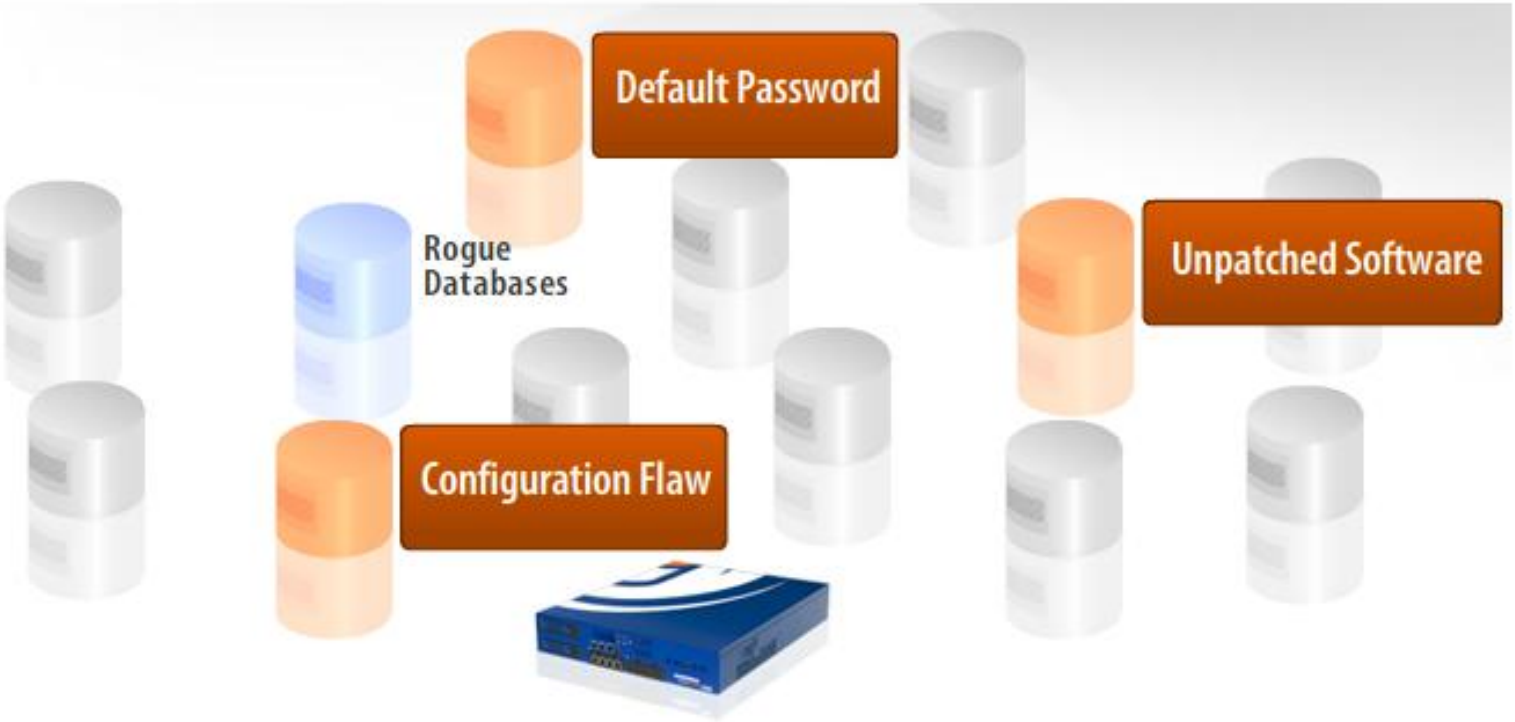
17 лет на рынке информационной безопасности

Imperva Secure Sphere

Поиск СУБД и анализ рисков ИБ

Обнаружение СУБД

Обнаружение СУБД → Поиск уязвимостей → Анализ конфигураций



© 2014 Инфосистемы Джет

Аналитика прав доступа пользователей
Принцип Need to Know

Unified View: Who, What, When

SKO URM 1 - Effective Rights Raw Data

Filter: Account Department is [RnD] and Object Category is [credit cards] and Sensitive ...

Select Columns | 1 | Showing records 1-3 out of 3 available | Show Paths

Account Name	Department	Priv Type	System Priv.	Object Name	Schema Name	Object Type	Sensitive Object	Object Category	Object Last Used
acourtney	RnD	SELECT	Normal Priv.	fulcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31
atipton	RnD	SELECT	Normal Priv.	fulcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31
eho	RnD	SELECT	Normal Priv.	fulcustomerdata	skotrain	Table	Sensitive	credit cards	2009-12-31

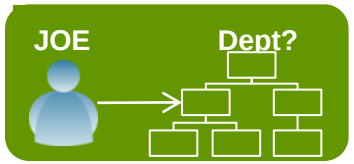
User | **Right** | **Sensitivity** | **Usage**

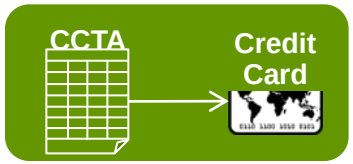
Classification, URM (DB)

Who Is? | Sensitive Data? | What rights?

DAM

When Used?





© 2014 Инфосистемы Джет

ИНФОСИСТЕМЫ ДЖЕТ

17 лет на рынке информационной безопасности

Imperva Secure Sphere

Мониторинг и защита СУБД

Полный аудит всех запросов

SecureSphere ведет мониторинг и запись запросов

Есть возможность сохранения ответов СУБД

Полная запись запросов

Event Date and Time	Source IP	User	Destination IP	Service	Source Application	Query
User: erez (7)						
June 10, 2010 5:09:54 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	CREATE OR REPLACE FUNCTION MYFUNC
June 10, 2010 5:09:01 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	select * from table_users
June 10, 2010 5:08:51 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT ATTRIBUTE,SCOPE,NUMERIC_VAL
June 10, 2010 5:08:51 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT CHAR_VALUE FROM SYSTEM.PRO
June 10, 2010 5:07:22 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT ATTRIBUTE,SCOPE,NUMERIC_VAL
June 10, 2010 5:07:22 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT CHAR_VALUE FROM SYSTEM.PRO
June 10, 2010 4:58:55 PM	192.168.0.110	erez	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	SELECT "SPW_LANGUAGE","SPW_WORD",
User: foo (18)						
March 31, 2010 10:44:49 PM	10.77.126.93	foo	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	drop table testpriv
March 31, 2010 10:44:41 PM	10.77.126.93	foo	11.11.199.122	Solaris Oracle Service	sqlplusw.exe	truncate table testpriv

Когда | Кто | Куда | Как | Что

© 2014 Инфосистемы Джет

Что увидел пользователь?

Сохранение ответов СУБД

- Запись полного ответа, полученного от СУБД

January 6, 2009 12:13:05 PM	8648289488017971556	194.90.240.3	webuser	10.10.1.2	MsSql			getCities 0
January 6, 2009 12:04:38 PM	8648289488017875206	194.90.240.3	webuser	10.10.1.2	MsSql			getCities 0
January 6, 2009 12:10:19 PM	8648289488017941706	192.168.114.12	Mark	192.168.112.8	MsSql			sp_Get_Products_By_Depts
January 6, 2009 12:06:24 PM	8648289488017906205	192.168.114.11		192.168.112.8	MsSql			dbo.EBGAMES_SP_GET_CUSTOMERREVIEWS
January 6, 2009 12:13:26 PM	8648289488017975472	194.90.240.3	webuser	10.10.1.2	MsSql			getCitiesKiosk
January 6, 2009 12:13:24 PM	8648289488017974083	194.90.240.3	webuser	10.10.1.2	MsSql			getCitiesKiosk

Auto2 Audit All Po

1 2 3

Ответ СУБД

Order_In_Response	Name	Manufacturer	Availability_Date	Availability	List_Price	Pf_Id	web_dept	Web_Sub_Dept
1	Wave Race 64 - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	399	130517	Nintendo 64	Sports
2	Wayne Gretzky's 3D Hockey - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	130520	Nintendo 64	Sports
3	Blast Corps - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	130526	Nintendo 64	Shooters
4	Tetrisphere - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	999	130528	Nintendo 64	Puzzle
5	Star Wars: Shadows of the Empire - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	299	130530	Nintendo 64	Simulation
6	NBA Hangtime - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	131100	Nintendo 64	Sports
7	Turok - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	132728	Nintendo 64	Shooters
8	Hexen - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	133917	Nintendo 64	Shooters
9	Lamborghini - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	299	134604	Nintendo 64	Sports
10	Doom 64 - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	999	134836	Nintendo 64	Shooters
11	WarGods - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	134964	Nintendo 64	Fighting
12	Top Gear Rally - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	299	135086	Nintendo 64	Sports
13	Robotron X - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	135088	Nintendo 64	Platform
14	Dark Rift - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	135362	Nintendo 64	Fighting
15	Multi Racing Championship - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	136980	Nintendo 64	Sports
16	Mission Impossible - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	136982	Nintendo 64	Shooters
17	Clayfighter 63 1/3 - Pre-Played	TRADE IN-NINTENDO 64	N/A	1	499	137107	Nintendo 64	Fighting

© 2014 Инфосистемы Джет

Инновационные технологии Imperva

- Идентификация пользователей
- Virtual Patching
- Динамическое профилирование

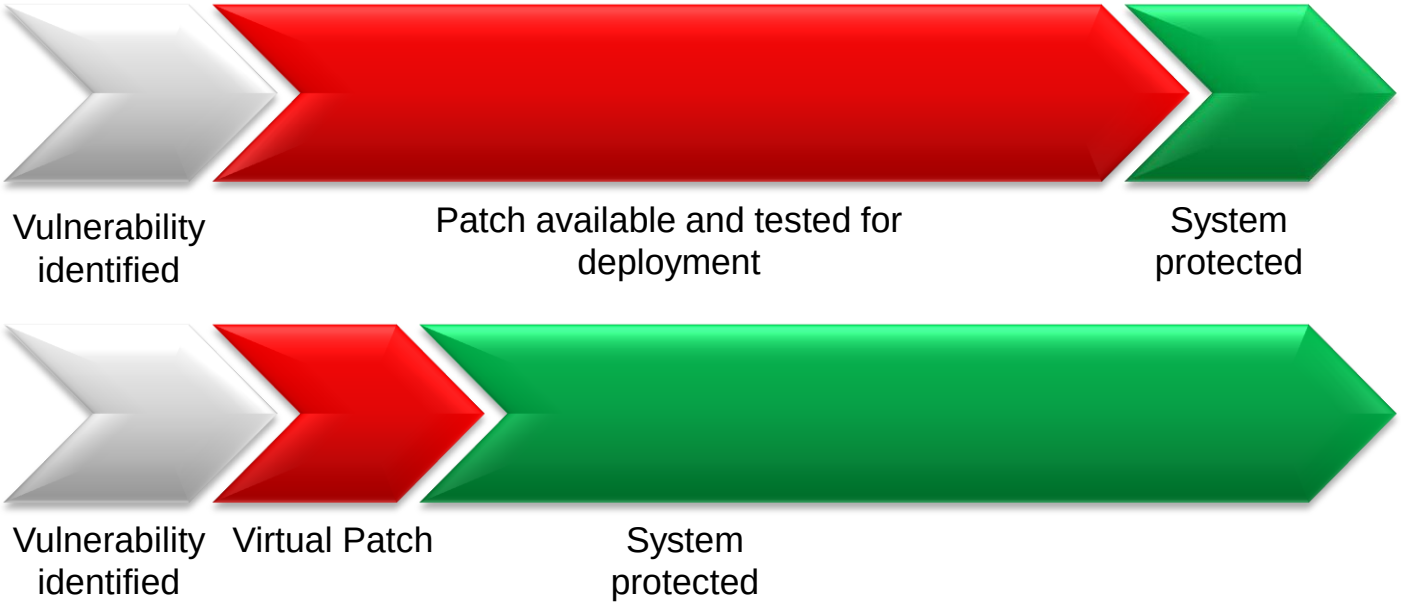
© 2014 Инфосистемы Джет

Virtual Patching

Обнаружение уязвимостей

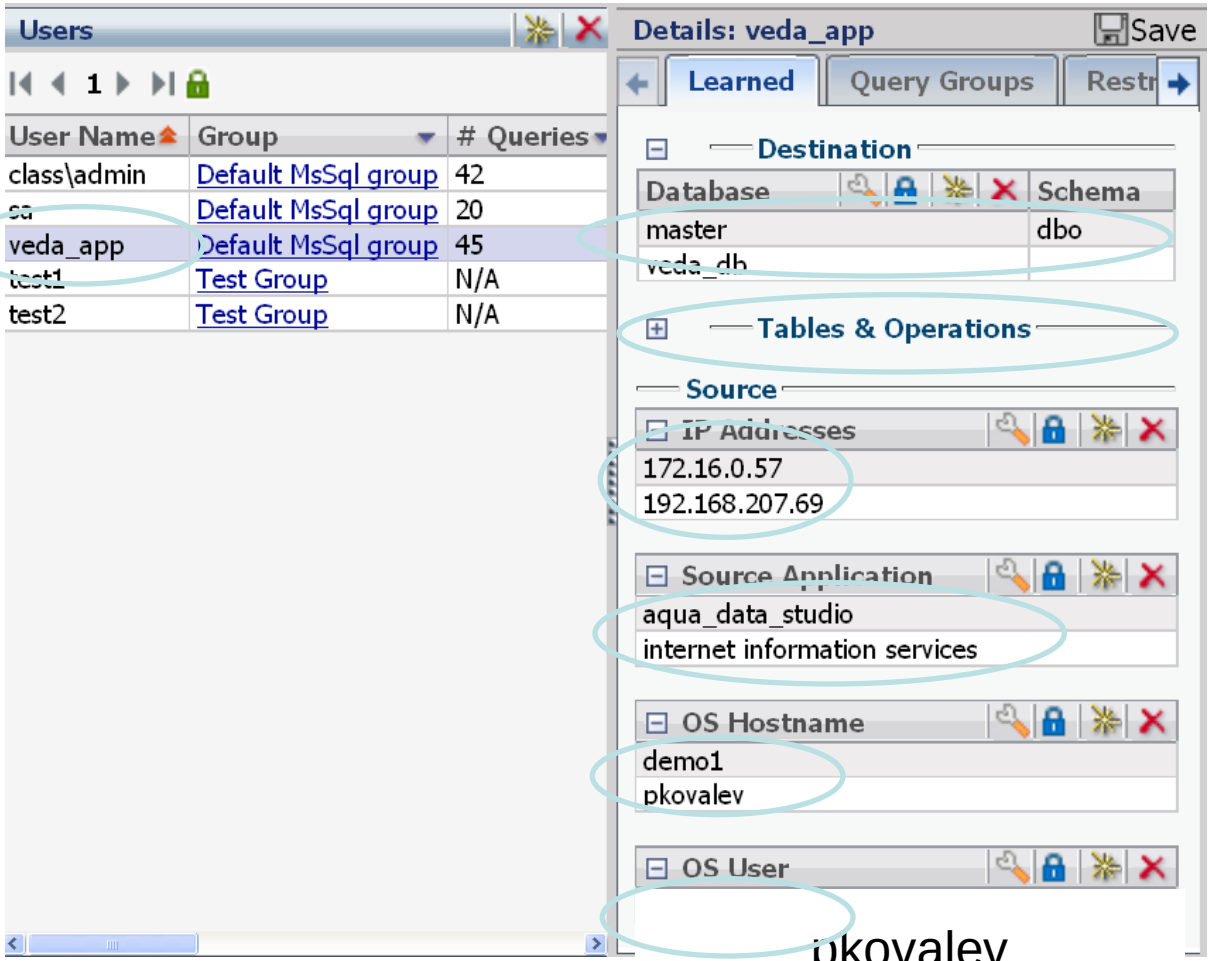
Блокирование попыток использования известных уязвимостей

Сокращение времени незащищенности СУБД во время тестирования и применения патчей безопасности



© 2014 Инфосистемы Джет

Профилирование действий пользователей баз данных



Пользователь БД

Имя БД/Схема

Таблицы и операции

Адрес источника

Приложение

Имя хоста

Пользователь ОС

© 2014 Инфосистемы Джет

ИНФОСИСТЕМЫ ДЖЕТ

17 лет на рынке информационной безопасности

Еще немного причин применения Imperva DAM / DBF

Зачем это бизнесу?

Защита активов

- *Требуется осуществлять мониторинг запросов и реагировать на инциденты ИБ с целью предотвращения и минимизации рисков компрометации прикладных бизнес-систем*

Регуляторные риски

- *Необходимо соблюдать требования обязательных стандартов ИБ по аудиту обращений к конфиденциальной информации, хранящейся в СУБД (PCI DSS, СТОБР ИББС, Защита ПДн)*

Контроль эффективности ИБ

- *Требуется регулярная отчетность о выявленных нарушениях политики ИБ компании в части доступа к конфиденциальной информации, хранимой в СУБД*

© 2014 Инфосистемы Джет

Зачем это подразделениям информационной безопасности?

Технический контроль организационных мер защиты	• *Необходимо реагировать (уведомлять или блокировать) на запросы к СУБД, нарушающие политику ИБ*
Контроль администраторов СУБД	• *Требуется осуществлять мониторинг действий привилегированных пользователей, в том числе работающих локально на сервере СУБД*
Персонификация запросов к СУБД	• *Требуется идентификация конечных пользователей, формирующих запрос к СУБД из-под служебной учетной записи бизнес-приложений*
Определять места хранения конф. Информации	• *Необходимо обнаружение конфиденциальной информации в СУБД в автоматизированном режиме*

© 2014 Инфосистемы Джет

Зачем это подразделениям информационных технологий?

Снижение нагрузки на СУБД из-за аудита

- *Необходимо снизить нагрузку на сервера БД при включении опций аудита СУБД*

Контроль администраторов СУБД

- *Необходимо проводить анализ изменения настроек СУБД в случае нарушения доступности и целостности СУБД*

Инвентаризация СУБД

- *Необходимо проводить регулярный анализ имеющихся в инфраструктуре СУБД, отслеживать изменения в сети и появление тестовых или временных копий СУБД, занимающих вычислительные ресурсы.*

© 2014 Инфосистемы Джет

ИНФОСИСТЕМЫ ДЖЕТ

17 лет на рынке информационной безопасности

Вместо заключения

Почему Imperva Secure Sphere?

Полный цикл защиты

- Комплексный подход от обнаружения СУБД в ИТ-инфраструктуре
- До активной защиты на основе политик ИБ

Интеграция с любым Web-приложением

- Идентификация пользователей в 3-х звенной архитектуре web-сервисов
- Корреляция web-запросов и данных от СУБД

Передовые технологии

- Динамическое профилирование поведения пользователей web-приложений и СУБД
- Виртуальный патчинг известных уязвимостей
- Аналитика прав доступа пользователей

Удобная система хранения данных аудита

- Данные аудита хранятся в плоских файлах
- Нет ограничений на объем и время хранимой информации (внешние каталоги)!!!
- Повышенная отказоустойчивость и доступность

© 2014 Инфосистемы Джет

Почему Imperva Secure Sphere?

Удобный интерфейс

- Объекты защиты заводятся как прикладные группы
- Множество продуманных меню

Удобная подготовка отчетности

- Необходимые параметры выбираются из списков
- Нет необходимости работать с переменными

Повышенная отказоустойчивость

- Агенты могут быть автоматически отключены при превышении выделенного ресурса мощности
- Хранение данных аудита в обычных файлах

Легкая настройка при установке

- Динамическое профилирование
- Понятная архитектура

© 2014 Инфосистемы Джет

ИНФОСИСТЕМЫ ДЖЕТ

Контакты:

Бейбутов Эльман

elman@jet.su

+7 985 721 66 22