RSA enVision – инструмент ИТ директора или «N-in-1 for CIO/CISO»

Александр Иржавский
НТЦ «Вулкан»

Содержание

Управление событиями: ключевой процесс Service Operation

- ИТ – важнейший элемент современного бизнеса
- Эффективность работы ИТ – ключевой фактор успеха
- Информационная безопасность – объективный приоритет

- Операционное управление ИТ и ИБ – это во многом принятие решений на основе информации о событиях на элементах инфраструктуры:
  - телекоммуникационное оборудование
  - операционные системы
  - средства защиты информации
  - приложения

Таким образом, Event Management приобретает особое, очень важное значение. Это относится ко всем уровням управления, от администратора до ИТ-директора.

Event Management в библиотеке ITIL (SO 4.1.1)

«Событие – поддающееся обнаружению явление, имеющее значение для управления ИТ-инфраструктурой и предоставления ИТ-сервисов»

Цели:

- Формирование входной информации для процессов Service Operation
  - Основа для операционного контроля и мониторинга
  - Основа для автоматизации эксплуатационных процедур
- Предоставление данных для оценки и улучшения сервисов

События являются входной информацией для многих процессов. В этом – основа «N-in-1» (см. следующие слайды)

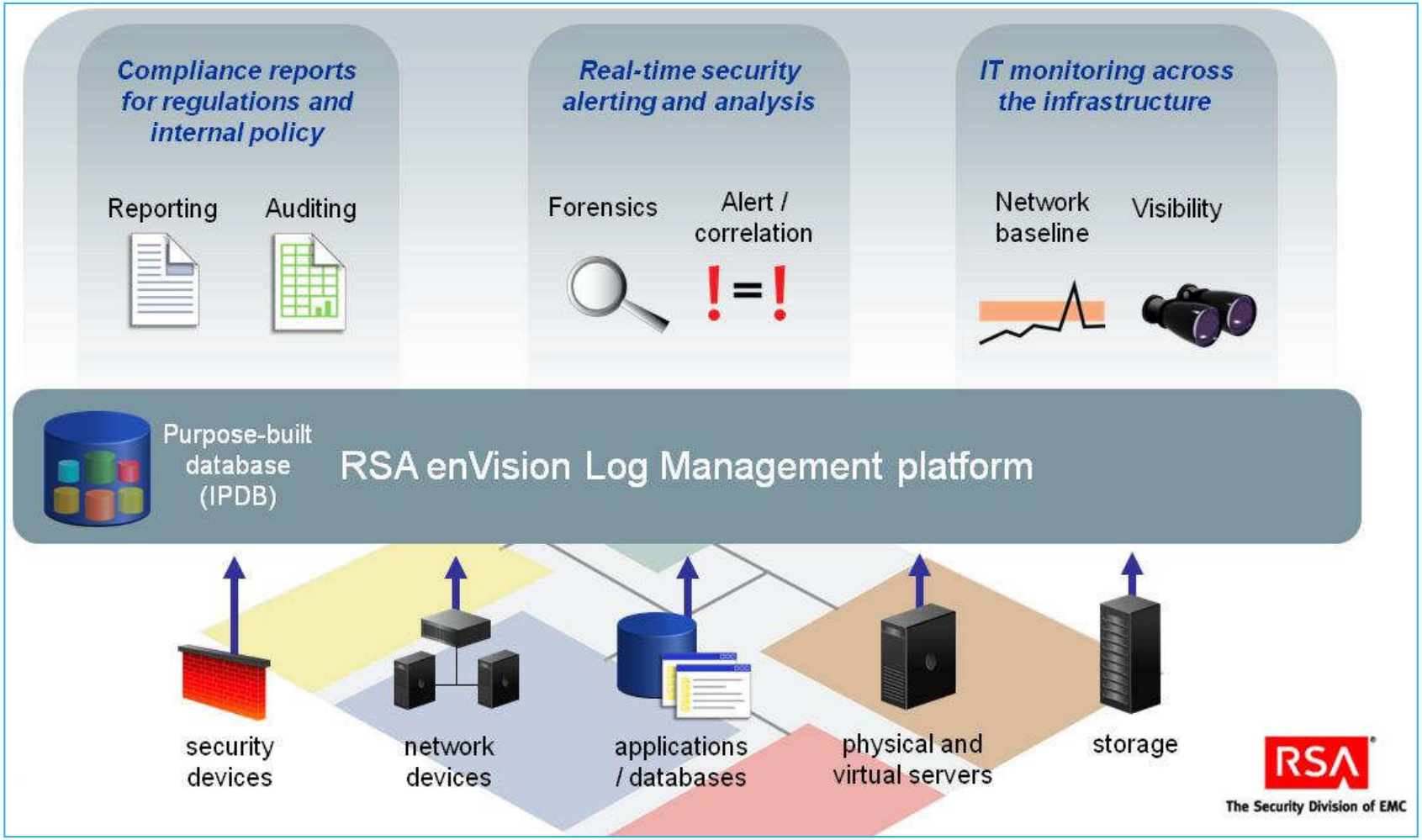
Обычная практика работы с событиями и ее недостатки

- Основной метод – ручной анализ
- Наращивание инфраструктуры + интенсивное использование ресурсов = генерация слишком большого потока информации о событиях
- Как ограничить поток?
  - Фильтрация информации по определенным типам событий
  - Настройка источников информации на генерацию только определенных типов событий
  - Настройка систем обработки событий на прием только определенных типов событий
- Следствие ограничения потока событий – потеря информации
- Противоречие: упрощение текущего наблюдения ,но осложнение детального анализа инцидентов
- Невозможно инициировать события по комбинациям других событий с низким приоритетом

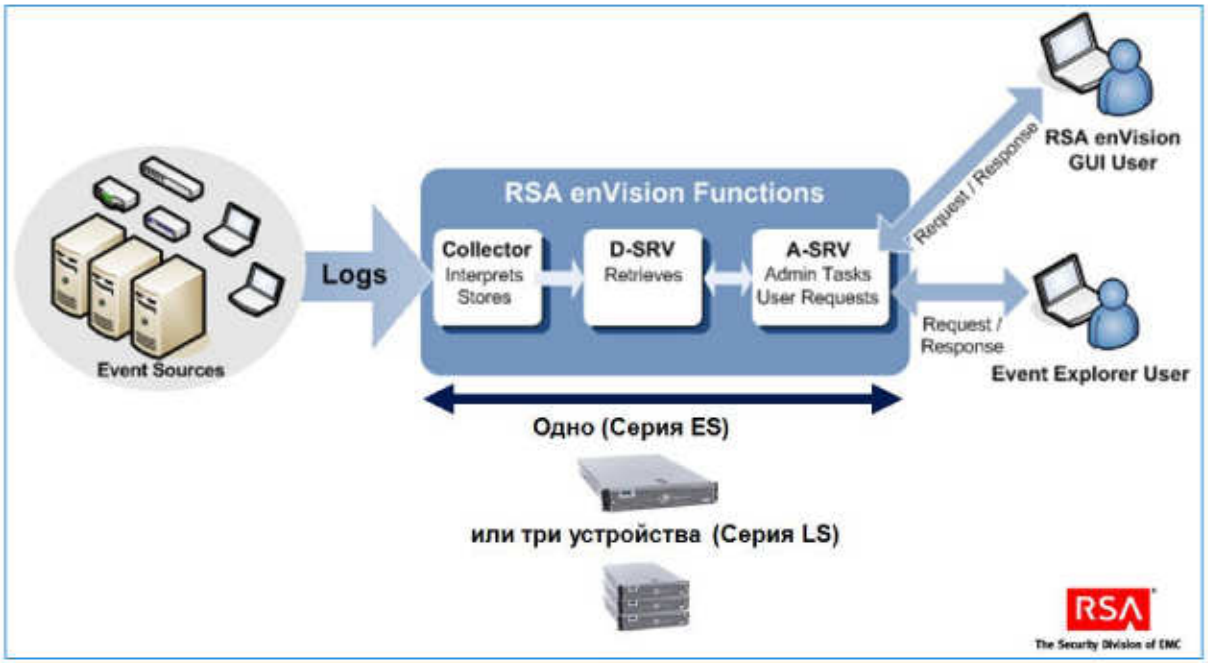
Решение проблемы управления событиями на большой ИТ-инфраструктуре

- Простого Log Management уже недостаточно
- Выход – в использовании многофункциональной системы SIEM
- Эффективное решение – платформа RSA enVision:
  - упрощение соблюдения нормативов и обеспечение соответствия (Simplified Compliance)
  - повышение уровня ИБ и снижение рисков (Enhanced Security)
  - оптимизация IT-инфраструктуры и упрощение ее обслуживания (Optimized IT Oversight)

RSA enVision – взгляд сверху



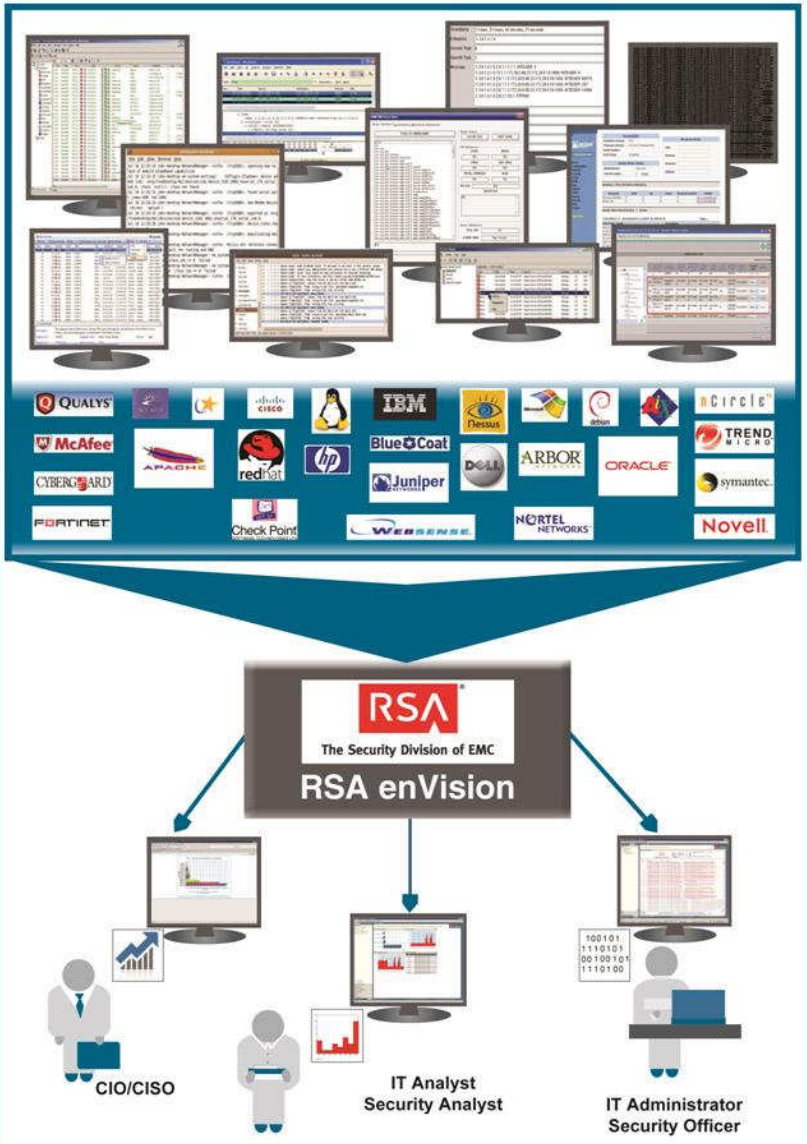
RSA enVision – взгляд сверху (продолжение)



Основные компоненты:

- Collector, LC/RC – коллектор (Local [0-3] / Remote [0-16])
- D-SRV – сервер баз данных [1 из расчета 6144 dev/30000 eps]
- A-SRV – сервер приложений [0-3]

Источники событий и потребители результатов



- Ведется постоянное расширение и обновление поддерживаемых источников
- 6 – 9 новых источников событий в месяц
- 6 – 9 обновлений источников событий в месяц
- Возможность самостоятельной интеграции с источниками событий

Автоматическая и ручная регистрация инцидентов

- Внутренний сервис управления инцидентами Task Triage:
  - Автоматическая группировка событий в задачу, требующую разрешения (по предопределенному набору событий и правил)
  - Ручная группировка событий в задачу, требующую разрешения
  - Регистрация задачи и реализация полного цикла управления инцидентами (через клиентское приложение EventExplorer)
  - Средства мониторинга и оценки уровня обслуживания инцидентов
  - Автоматическая и ручная эскалация инцидентов во внешние системы обработки заявок (ServiceDesk)
  - Обновление задач из внешних систем

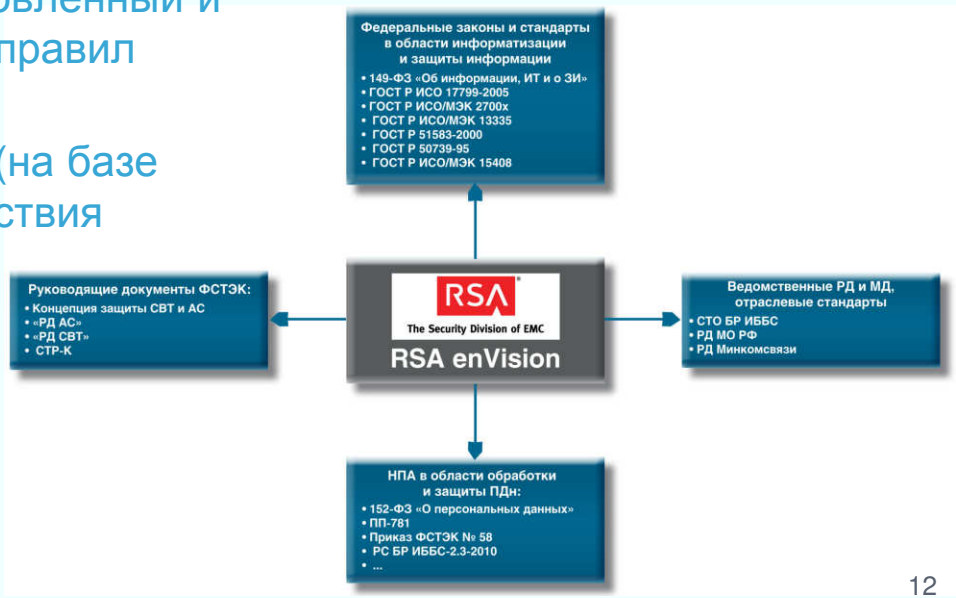
В зависимости от практики построения Service Desk в конкретной организации RSA enVision может выступать как средством инициализации инцидентов, так и средством автоматизации обработки инцидентов безопасности в выделенном «Security Service Desk»

Встроенные отчеты

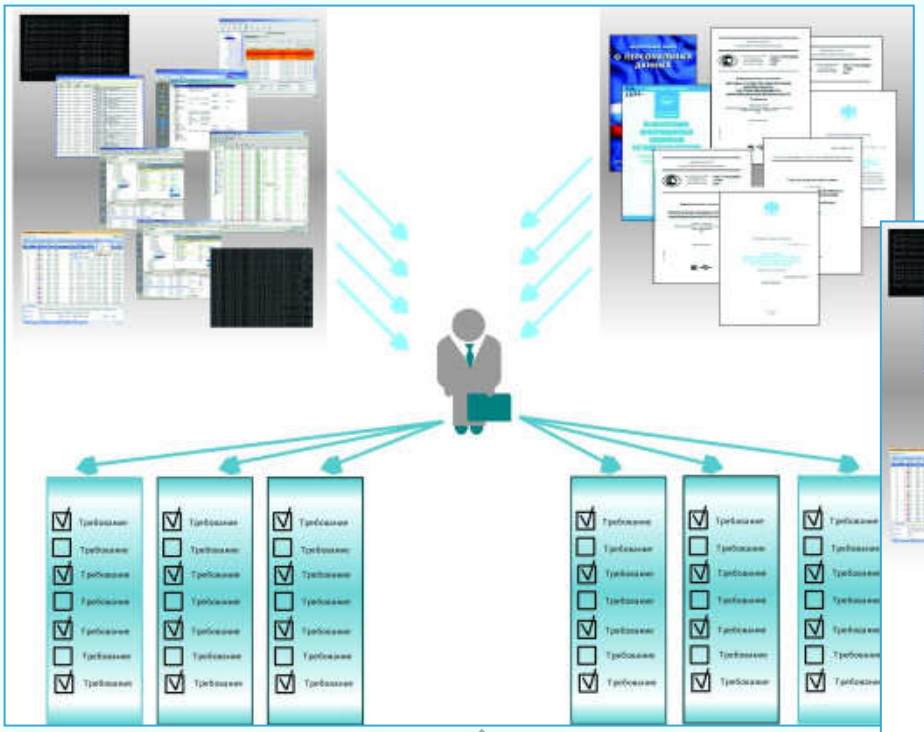
- 1000+ видов встроенных отчетов
- Графическая и табличная форма
- Отчеты разбиты на целевые категории
- Модификация отчета под конкретные условия и требования, либо создание собственной формы отчета – простая и быстрая процедура
- Формирование отчетов возможно как вручную, так и по расписанию
- Пересылка по email или сохранение в заданную область дисковой системы
- Выходные форматы - HTML, PDF, CSV

Соответствие требованиям (Compliance)

- В RSA enVision имеется группа встроенных контролей (ВК)
- ВК – это определенные наборы правил, созданные с учетом принятых к исполнению нормативных требований
- На основании правил ВК система заданным образом реагирует на определенные наборы событий
- Состав ВК варьируется в широком диапазоне в зависимости потребностей служб и принятых нормативов
- В ВК можно задействовать предустановленный и обновляемый набор корреляционных правил RSA enVision
- ВК могут расширяться и дополняться (на базе встроенных ВК) для проверки соответствия самым разным требованиям:
  - ISO 27002
  - PCI DSS
  - *152-ФЗ и безопасность ПДн*
  - *СТО БР ИББС*
  - *Ведомственные требования ИБ*

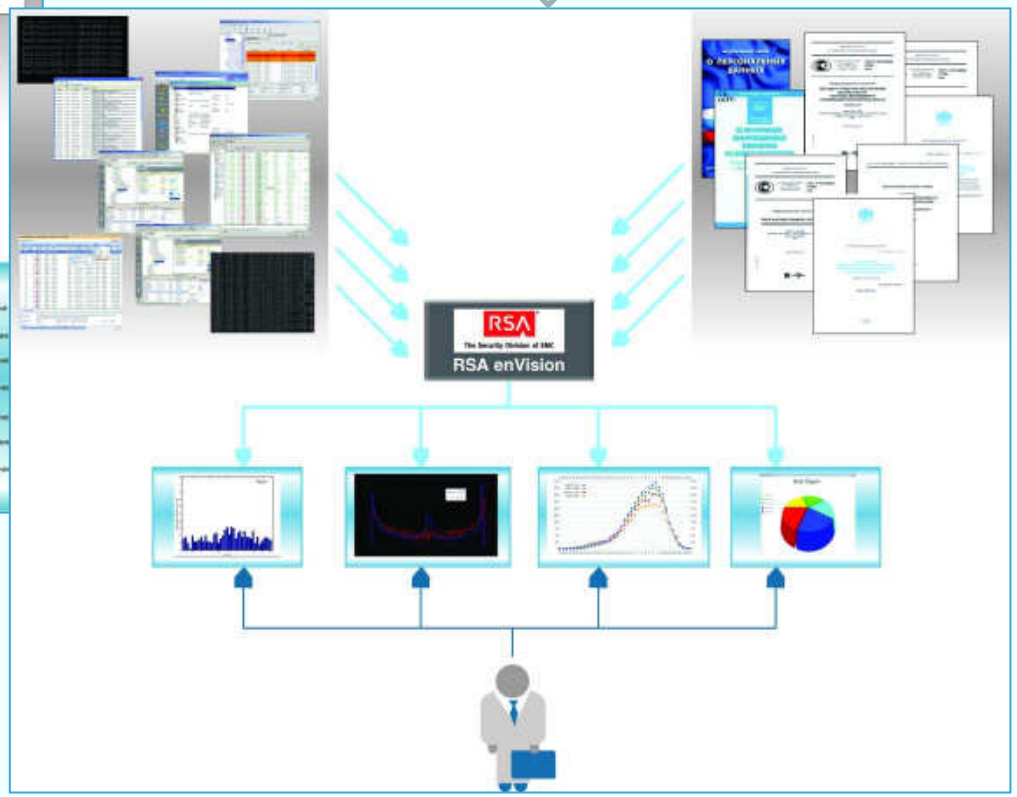


Соответствие требованиям (Compliance)



БЫЛО

СТАЛО



Управление уязвимостями и информацией об активах

- Сервис VAM (Vulnerability and Asset Management) - управление информацией об уязвимостях и активах
- Возможность дополнять, сводить, изменять и оценивать VA-информацию
- Цель - расширение и уточнение представления о контролируемой инфраструктуре и событиях
- Информация об активах (БД активов - ADB) существенно детализирована
- ADB пополняется и модифицируется вручную либо путем и импорта из внешних inventory-систем (VAT, CMDB/CMS etc), наборы атрибутов в ADB легко расширяются
- Информация ADB используется при анализе и обработке инцидентов, например:
  - при группировке критических активов для мониторинга или анализа
  - при фильтрации в корреляционных правилах по заданным атрибутам
  - в рамках привязки уровня важности в сигнальной схеме к требуемым атрибутам
  - при просмотре и анализе описи активов в рамках обработки инцидентов
  - при подготовке отчетов о состоянии активов

Управление уязвимостями и информацией об активах

- enVision способен нормализовать информацию от VAT и IDS/IPS к словарю CVE, затем связать ее с активами из ADB
- Обновления списков уязвимостей и сигнатур для поддерживаемых enVision сканеров и IDS осуществляются периодически с сайта EMC/RSA
- Информация об уязвимостях размещается в специальной базе данных уязвимостей (VDB)
- Записи VDB содержат детальную информацию об уязвимости:
  - Наименование
  - Ссылка CVE
  - Описание
  - Разъяснение воздействия
  - Сведения о возможных потерях
  - Ссылочная и другая информация

Функционал VAM дает возможность полнее и точнее оценить риски, а так же границы и природу инцидентов, повысить эффективность управления ими с одновременным подавлением ложных срабатываний IDS/IPS

Обнаружение критической деятельности

- Понятие «критической деятельности» (КД) определяется индивидуально исходя из:
  - целей и задач организации
  - нормативных требований и политик
  - специфики области деятельности
  - территории присутствия
- КД должна быть предварительно формализована в рамках конкретной организации, затем описана в системе enVision в виде наборов конкретных правил
- Правила определяют, на какие события или их комбинации и каким образом следует реагировать
- Рабочий шаблон - поставляемый с системой набор корреляционных правил + рекомендации по написанию собственных наборов

Обнаружение критической деятельности

- В enVision включены готовые правила для следующих наборов событий:
  - повышение пользовательских привилегий, подключение съемных носителей информации, атаки класса backdoor и попытки подделки журналов регистрации на корпоративных системах
  - внутренние нарушения в сети, например: подделки ARP-запросов, внутренняя активность botnet-ов, сетевая активность по сбору информации
  - внешние нарушения в сети, например: внешняя активность botnet-ов, попытки реализации DoS-атак, попытки перебора паролей, активность из известных «черных списков»
  - инциденты безопасности, относящиеся к списку основных угроз «SANS Top 20»

RSA enVision следует рассматривать как гибкий и мощный инструмент, позволяющий реализовать предварительно формализованные задачи по управлению событиями и информацией безопасности.

Интеграция с другими информационными системами

- RSA enVision поддерживает интеграцию со множеством информационных систем:
  - системы инвентаризации (CMS/CMDB)
  - системы обработки заявок (ServiceDesk, Help Desk)
  - системы управления сетью (NMS – Network Management System)
- Механизмы взаимодействия:
  - Обмен файлами определенных форматов
  - Имеются соответствующие сценарии взаимодействия
  - Возможно использование стандартных механизмов взаимодействия (email, SFTP, SNMP)

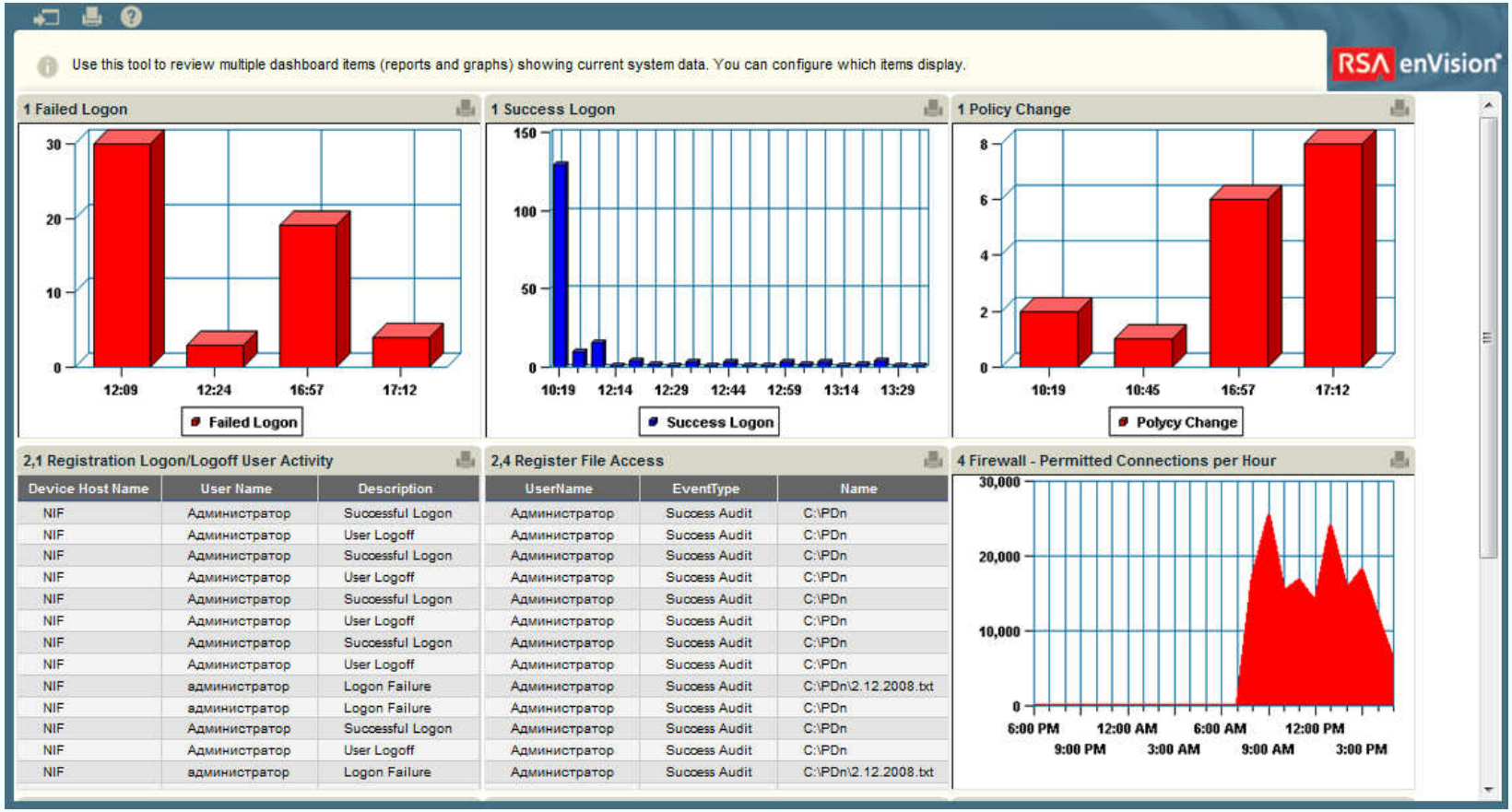
Оптимизация количества персонала

- ИТ-инфраструктура среднего корпоративного уровня: поток событий 500+ EPS
- ИТ-инфраструктура оператора связи: поток событий 2500+ EPS
- Один оператор может за день обработать не более 1000 событий (по материалам SANS)
  - Никакое разумное количество персонала не справится с задачей обработки такой информации без применения специализированных средств
- Системы класса enVision ориентированы на «поиск иголки в стоге сена»
  - N x 10^6 событий на входе сводятся к M x 10^2 значимых и требующих анализа и реагирования событий на выходе
- Задача подтверждения соответствия нормативным требованиям занимает до 20% времени IT-служб (по материалам IDC)
  - enVision позволяет делать это практически в автоматическом режиме при соответствующей настройке системы

Система показателей безопасности

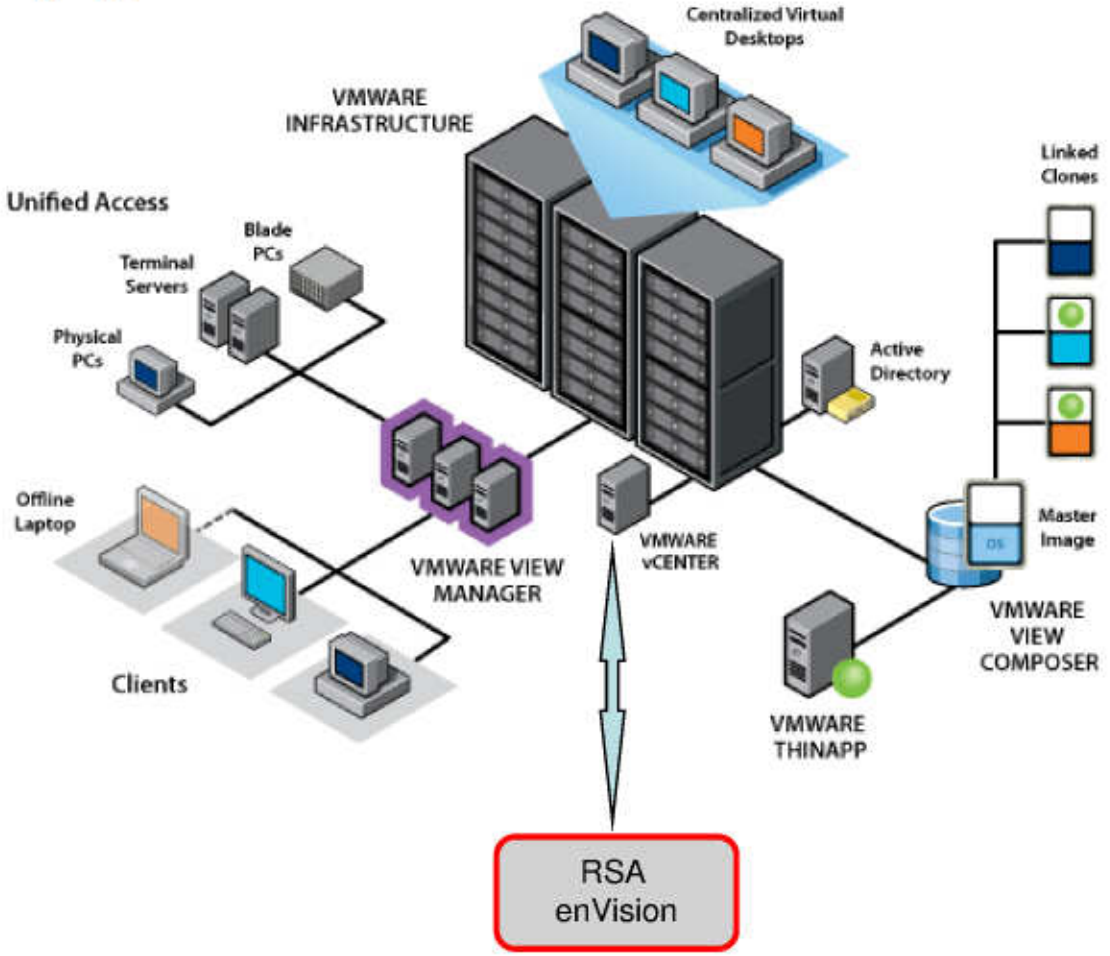
- RSA enVision может предоставить разноплановый набор показателей безопасности
- Форма представления: табличная и графическая
- Режим: мониторинг или отчеты
- Примеры:
  - Список активов, упорядоченный по важности с т.з. бизнеса с оценкой уязвимости по CVS и датой последнего сканирования
  - параметры обработки инцидентов: среднее время реагирования и обработки, распределение по времени и уровню важности, текущие открытые задачи
  - Отклонения метрик от базовых уровней (baseline) и средних значений и их изменение во времени
  - Отчеты соответствия нормативным требованиям (ISO 27002, PCI DSS, 152-ФЗ, СТО БР ИББС и т.д.)
  - Отчеты соответствия собственным заданным показателям ИБ (по изменению конфигураций на критичных системах, эскалации прав и т.д.)

Контрольная панель

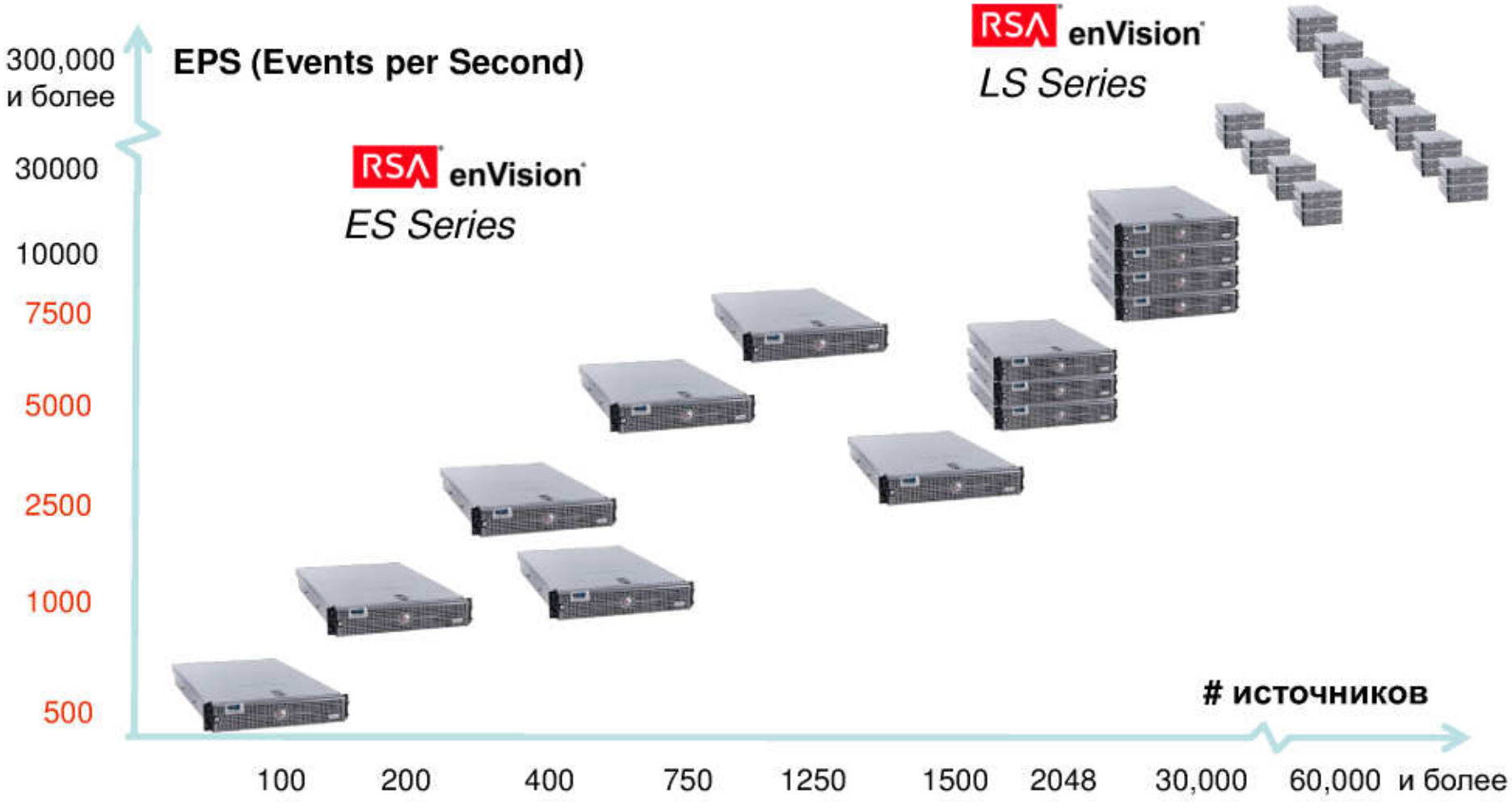


Работа в виртуальных средах

- Коллектор имеет интерфейсы к vCenter Server
- Бесшовная интеграция со средой VMware, установка агентов не требуется
  - Информация о событиях собирается с vCenter и с ESX/ESXi серверов
  - Охватывает 380 различных сообщений



Масштабируемое решение



Гарантированная обработка до 61440 DEV / 300000 EPS в базовой конфигурации. В расширенной - значительно больше

Дифференцируемые планы внедрения

Уровень зрелости	Характеристика уровня	Степень внедрения RSA enVision
0	Non Existent, деятельность не выполняется	Внедрение RSA enVision в качестве корпоративной системы сбора журналов событий (Log Management)
1	Initial, явные свидетельства деятельности	Более широкое использование функциональных возможностей платформы, Advanced LM с функциями сбора, предобработки и хранения журналов событий
2	Repeatable, частично документированная деятельность	Первичная интеграция с процессами Service Operation, простые контроли соответствия (на уровне компании), ИБ-ориентированная отчетность
3	Defined, деятельность документирована и стандартизована	Контроли на уровне отрасли, Enhanced Security за счет полного использования функций корреляции, ранжирования угроз, определения приоритетов событий, мониторинга производительности
4	Managed, выполняется оценка соответствия	Все опции уровня 3 плюс Simplified Compliance, оснащение SOC, а также расширенные функции уведомлений и отчетности. Интеграция с ServiceDesk.
5	Optimized, совершенствование в соотв. с передовым опытом	Максимально широкая интеграция с процессами SO и SD, Optimized IT Oversight, обеспечение функций Analyst Workflow и Context Analysis, оснащение SOC и NOC

Другие ключевые особенности системы

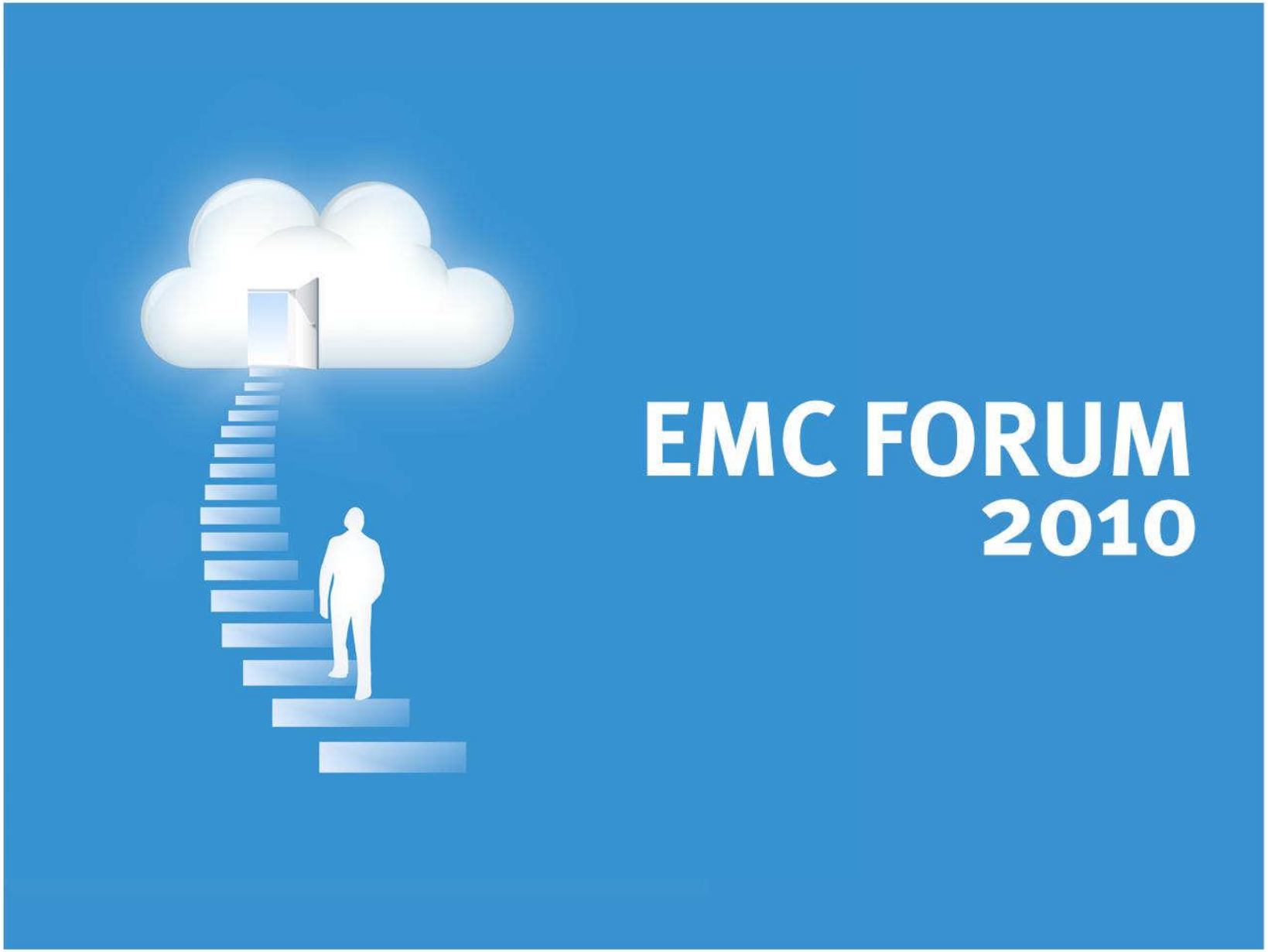
- Сбор сообщений без установки специализированных агентов (UDS - Universal Device Support)
- Автоматическое выявление инцидентов в потоке событий в реальном времени по правилам обработки для наборов дискретных и коррелированных событий
- Поведенческая оценка инфраструктуры в реальном времени, возможность сравнения текущего поведения с зафиксированными базовыми уровнями эксплуатации
- Автоматическое определение базового эксплуатационного уровня контролируемой инфраструктуры и развитые средства контроля статистических отклонений
- Работа со специализированными системами консолидации и обработки событий: Cisco MARS, Cisco Works, McAfee ePO, Microsoft Operations Manager, устройства класса «unified threat management» (Sidewinder, Astaro)

Другие ключевые особенности системы

- «Обучение» системы новым источникам и событиям (ESI – EventSource Integrator)
- Безопасное и эффективное хранение сообщений в их исходном виде без предварительной обработки или фильтрации (при записи в IPDB применяется технология с однократной записью и многократным считыванием WORM)
- Ролевой доступ к функционалу и информации
- Поддержка отказоустойчивых конфигураций
- Высокая гибкость построения распределенной архитектуры
- Низкая стоимость владения: обслуживание RSA enVision не требует наличия высококвалифицированных специалистов и специальных процедур

Спасибо за внимание!

НТЦ «Вулкан»
105318 г. Москва, ул. Ибрагимова, д.31 корп.50
тел./факс+7 (495) 769-83-21
http://www. ntc-vulkan.ru
info@ntc-vulkan.ru


EMC FORUM
2010