ДиалОгНаука

ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ МОНИТОРИНГА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БАЗЕ РЕШЕНИЙ HP ARCSIGHT ESM И HP ARCSIGHT LOGGER

Чехарин Родион

ЗАО «ДиалогНаука»

ДиалогНаука

О компании «ДиалогНаука»

- Создано в 1992 году СП «Диалог» и Вычислительным центром РАН
- Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были ревизор ADinf, Doctor Web и Aidstest
- В настоящее время ДиалогНаука является системным интегратором в области информационной безопасности

ДиалОгНаука

Основные направления деятельности

- проведение аудита информационной безопасности
- разработка системы управления безопасностью в соответствии с ISO 27001
- разработка Политик информационной безопасности и других нормативных документов, регламентирующих вопросы защиты информации
- проектирование, разработка и внедрение комплексных систем обеспечения информационной безопасности
- поставка программного и аппаратного обеспечения в области защиты информации
- техническое сопровождение поставляемых решений и продуктов

ДиалогНаука

SIM, SEM, SIEM

1. Security Information Management (SIM, «управление информацией безопасности») обеспечивает:
   - сбор, хранение и анализ данных (взятых из журналов)
   - подготовка отчётов по соответствию нормативным требованиям

   Служит для:
   - управления журналами
   - создание отчётов и выполнение аналитических исследований по событиям безопасности
2. Security Event Management (SEM,«управление событиями безопасности») обеспечивает:
   - мониторинг событий безопасности в реальном времени
   - выявление и реагирование на инциденты безопасности
   - Служит для:
     - мониторинга событий безопасности в реальном времени
     - помощи персоналу в выявлении внешних и внутренних угроз, и реализации эффективных ответных мер

- Security Information and Event Management = SIM + SEM

ДиалОгНаука

Современные проблемы информационной безопасности

Большое количествево разнородных устройств безопасности

- **90%** используют межсетевые экраны и антивирусы
- **40%** используют системы обнаружения вторжений (IDS)
- количество сетевых устройств растет
- больше оборудования означает большую сложность

Очень много событий по безопасности !

- один межсетевой экран может генерировать за день более 1 Гигабайта данных в Log-файле
- один сенсор IDS за день может выдавать до 50 тыс. сообщений, до 95% ложных тревог!
- сопоставить сигналы безопасности от разных систем безопасности практически невозможно

Слишком много устройств, слишком много данных…

Ответные действия на угрозы безопасности должны быть предприняты немедленно!

ДиалогНаука

Борьба службы информационной безопасности проходит на разных фронтах

- Необходима работа:
  - Защита от неправомерных действий конечных пользователей
  - Управление обновлениями и уязвимостями ПО
  - Борьба с червями …..
  - Вирусы
  - Попытки оценить соответствие существующей системы предъявляемым требованиям (Compliance)
  - Управление изменениями (Change Management)
  - Управление инцидентами
  - Огромные объемы информации ….
- Ограниченный бюджет
- Проблемы с сетевым и IT департаментами
  - Нет прямых коммуникаций, непонимание…
  - Борьба за влияние, сваливание проблем ….
- Оценки соответствия стандартам безопасности добавляют напряжение ….

ДиалогНаука

Предпосылки для использование SIEM

- Организации имеют инфраструктуру безопасности от разных производителей и не могут интегрировать их журналы регистрации для полной оценки обстановки по безопасности.
- Большое количество журналов безопасности позволяет злоумышленнику обойти администратора безопасности.
- Большое количество ложных срабатываний современных систем обнаружения вторжений, обусловлена их ориентацией на обнаружение конкретных сигнатур или на обнаружение сетевых аномалий, а не на обнаружение конкретных угроз.
- Производители только могут управлять своим оборудованием и чаще всего не могут охватить все нужды больших компаний.
- Ограниченные бюджеты по безопасности.

ДиалогНаука

Требования к SIEM

1. Мы хотим получать на консоль только значимые события - при этом необходимо не забывать, как эта информация будет представлена - только в виде скоррелированных событий или позже можно получить информацию в оригинале?
2. Должно быть централизованное хранилище данных от всех систем - самое неудобное - это большая база данных с которой сложно обращаться, соответственно работа с базой событий должна быть по максимально простой.
3. Должно быть ранжирование угроз, основанное на серьезности ущерба, что позволяет администратору сфокусироваться на реальных угрозах, исключая ложные угрозы - соответственно система должна учитывать анализ рисков, проведенный в компании и получать информацию от систем анализа безопасности;
4. Система должна быть масштабируемой и при необходимости распределенной – не каждый вендор может предоставить действительно масштабируемую систему.
5. Необходим мониторинг на уровне приложений (например, SAP и т.п.) - вопросы работы с приложениями являются одними из самых трудных в таких системах.
6. Необходимы решения по мониторингу инсайдерской активности - должны поддерживаться системы анализа контента, а также специфических функций отдельных приложений.
7. Решение должно иметь возможность анализировать поддерживаемый уровень безопасности сравнивать их с нормативными требованиями законодательства или отраслевым и международным нормам (ISO 27001 и др.…)

ДиалогНаука

Особенности сбора событий ИБ

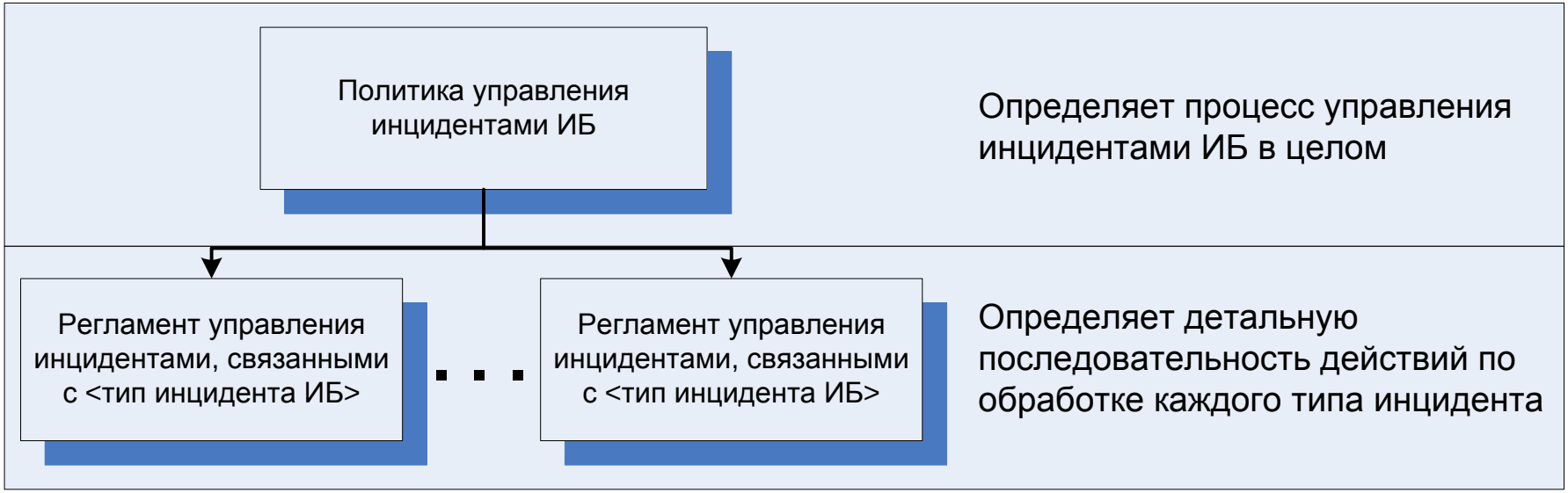
1. Эффективный сбор и хранение информации о событиях безопасности:
   - Нет политики аудита
   - Нет понимания объёмов журналов и сроков их хранения
2. Разнородность событий
   - Множество протоколов и форматов
   - Неструктурированность данных
   - Закрытые форматы журналов
3. Хранение данных
   - Сроки хранения
   - Способы работы со значительными объёмами данных

ДиалогНаука

Основные этапы внедрения SIEM

- Проведение обследования
- Разработка комплекта нормативных документов
- Разработка технических и системных решений
- Поставка оборудования и программного обеспечения
- Установка и базовая настройка системы
- Опытная эксплуатация

Разработка нормативных документов



ДиалогНаука

Формирование списка типовых инцидентов ИБ

- Определение типов основных инцидентов ИБ
- Определение списка событий, которые ведут к инциденту ИБ
- Определение источника инцидента ИБ
- Определение и приоритезация рисков, связанных с инцидентами ИБ

ДиалогНаука

Практический опыт внедрения SIEM

- Выделение зоны мониторинга
  - Либо сегмент сети, либо «боевые» серверы, сетевое оборудование
- Создание перечня объектов мониторинга
  - Зачатую происходит аудит или инвентаризация
- Оценка состояния журналирования
  - Регулярное непонимание со стороны службы IT – вплоть до саботажа
- Оценка регламентирующих документов
  - Чаще всего их нет, или в них один «воздух»
- Оценка технических требований к Системе мониторинга
  - Сложно добиться данных от IT, помогает только пилотное внедрение
- Техническое задание, Пояснительная записка, ПМИ
- Стандарт настройки аудита в наблюдаемых системах
  - Зачастую IT активно протестует, а СБ настаивает на глобальном аудите
- Регламент обработки инцидентов
  - Нет формализованного процесса, или стороны не могут прийти к соглашению
- Установка ПО
- Подключение источников событий информационной безопасности
- Реализация функционала
  - Обычно занимает около 6 мес, всегда перетекает из стадии внедрения в стадию техподдержки

ДиалогНаука

Эксплуатация SIEM
Основные трудности

- Отсутствие или бесполезность регламентирующих документов
- Персонал
  - Квалификация
    - Сотрудники ИБ слабо \ фрагментарно разбираются в прикладном администрировании, а зачастую и в IT-ландшафте предприятия
    - IT – считает основно задачей «что бы всё летало»
  - Взаимодействие служб
    - Формализм
    - Антагонизм
  - Объектовая безопасность
- Отечественная «криптография»
- Унаследованные приложения

Практический опыт:

Основные применения СМ Интеграция с IdM

Identity management – системы управления учётными записями пользователей.

Предназначены для создания автоматизированного, единообразного механизма создания, удаления и поддержания в актуальном состоянии данных об учётных записях пользователей на разнородных прикладных системах

СМ: Интеграция с IdM

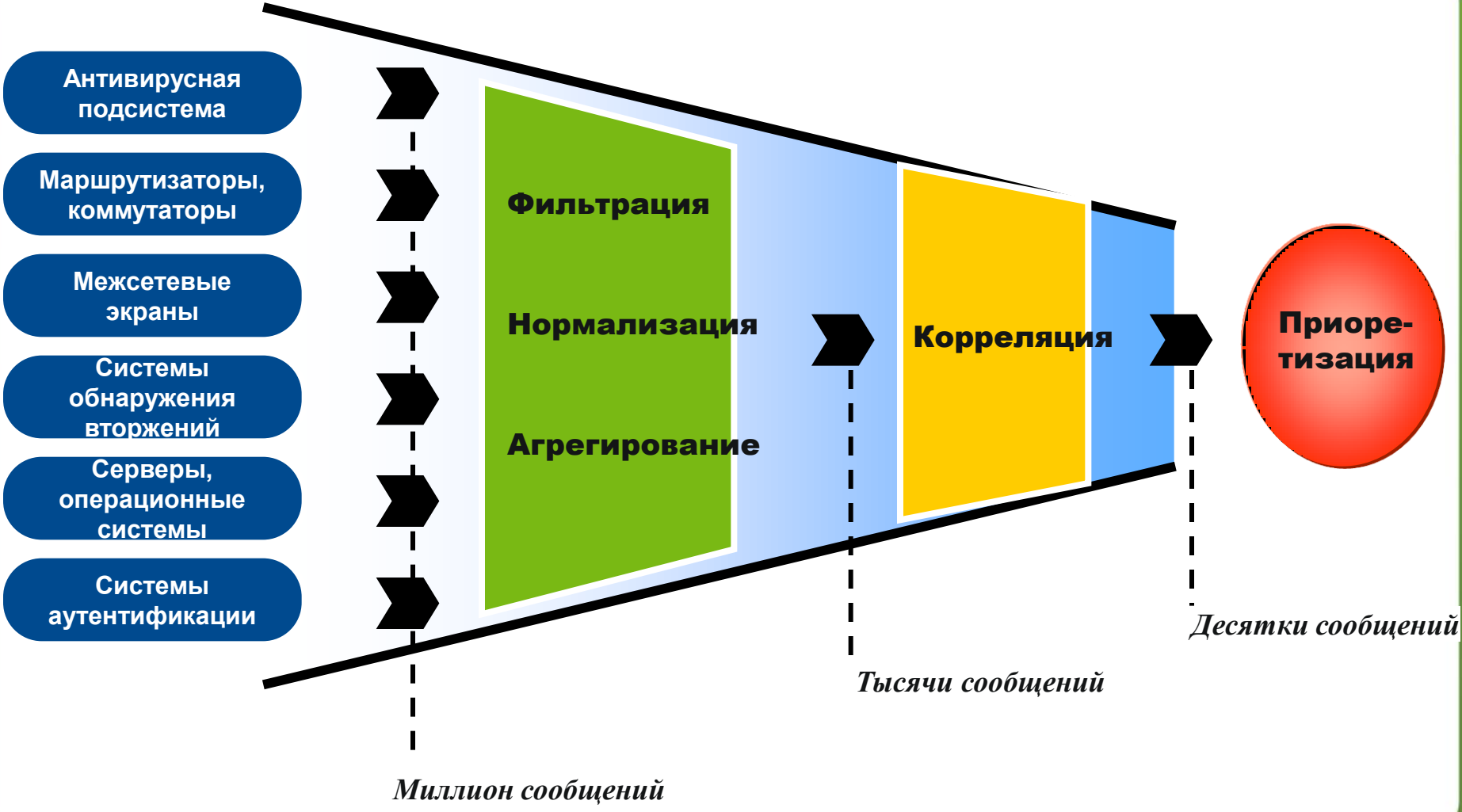
Чёткое сопоставление сотрудника и его учётных записей, их ролей и привилегий в прикладных системах.

Ответы на вопросы:

- «Что делал на всех серверах вчера сотрудник N?»
- «Кто реально обладает доступом к самой главной СУБД?»
- «Откуда столько «мёртвых душ?»

ДиалОгНаука

Принцип работы SIM\SIEM



HP ArcSight

Гибкая платформа для отслеживания актуальных угроз и рисков

- Единая точка мониторинга
- Анализ событий в реальном времени
- Реакция в кратчайшие сроки для предотвращения потерь
- Оценка эффективности мер защиты приложений, процессов, пользователей и технологий в целях улучшения и модернизации

ДиалогНаука

Важность централизованного контроля и управления безопасностью

Центр управления создаёт единую систему контроля информационной безопасности

Сетевые устройства	Системы безопас-ности	Физический доступ	Мобильные устройства	Серверы	Рабочие станции	Учётные записи	Email	Базы данных	Приложе-ния

ДиалогНаука

ArcSight ESM Архитектура

Интуитивное администрирование

Простота использования

ArcSight Console™

ArcSight Web™

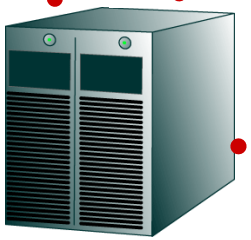
Интеллектуальная обработка

Эффективное хранение данных

ArcSight Pattern Discovery™

ArcSight Interactive Discovery™

ArcSight Manager™



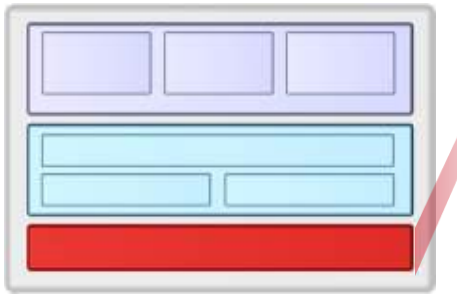
Archive and Retrieval

Гибкое подключение новых источников

SmartConnector

FlexConnector

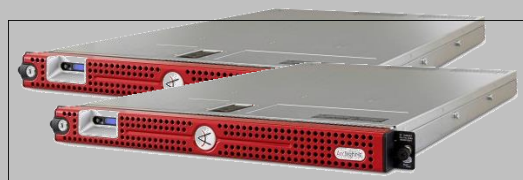
Уровень интеграции



Connectors

- Собирают журналы в оригинальных форматах более чем с 300 систем
- Приводят события к единому формату
- Передают события на Manager по защищённому, отказоустойчивому протоколу
- FlexConnector Wizard для добавления новых типов источников

Доступны в виде:



Стоечные устройства

Устройства для филиального офиса

Отдельное ПО

Преимущества: Анализ событий независимо от типа устройства

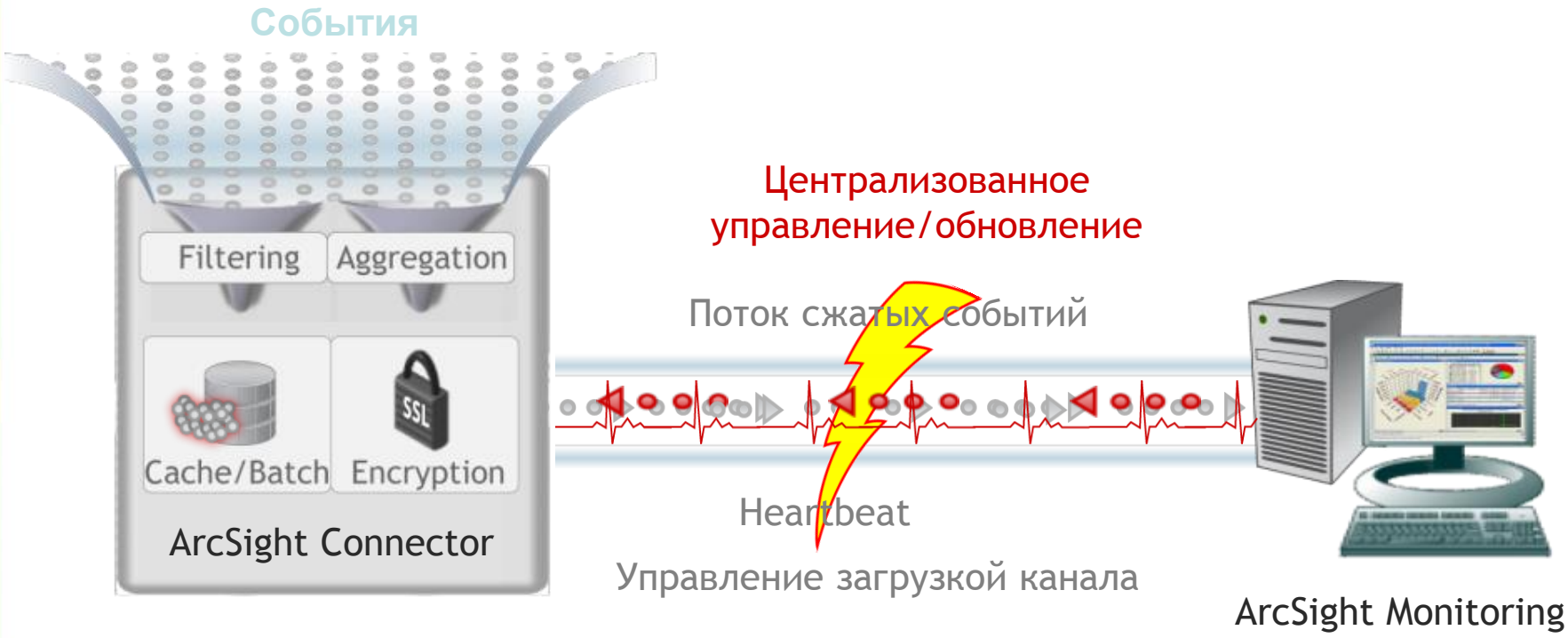
ДиалогНаука

Поддерживаемые устройства

Access and Identity	Data Security	Integrated Security	Network Monitoring	Security Management	Web Cache
Anti-Virus	Firewalls	Log Consolidation	Operating Systems	Switch	Web Filtering
Applications	Honeypot	Mail Relay & Filtering	Payload Analysis	VPN	Web Server
Content Security	Host IDS/IPS	Mail Server	Policy Management	Vulnerability Mgmt	Wireless Security
Database	Network IDS/IPS	Mainframe	Router		

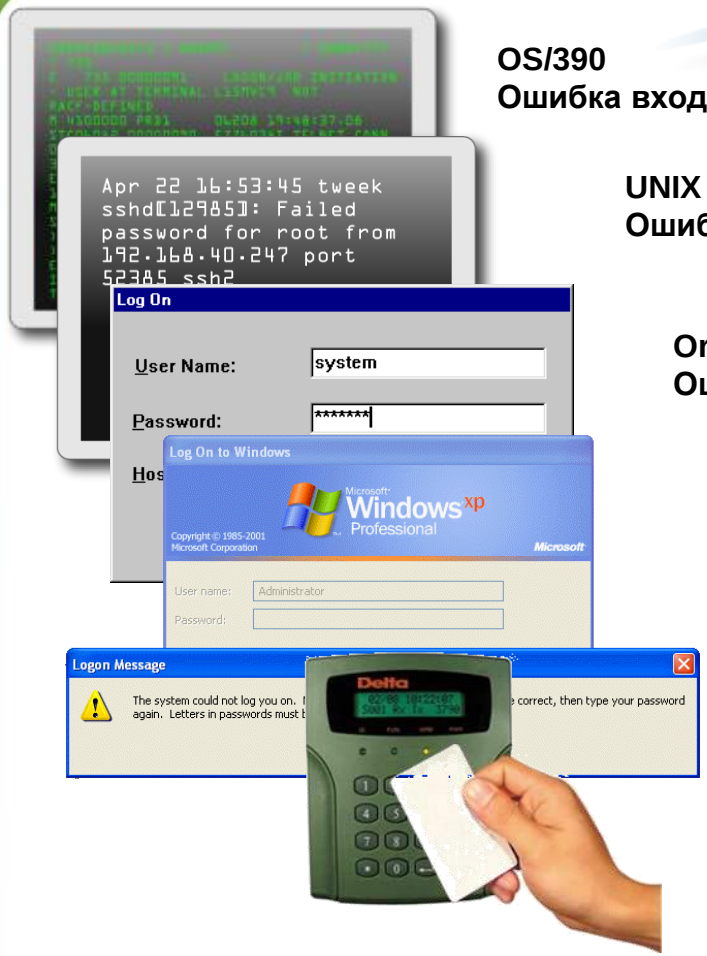
ДиалогНаука

Отказоустойчивая архитектура сбора событий



ДиалогНаука

Нормализация



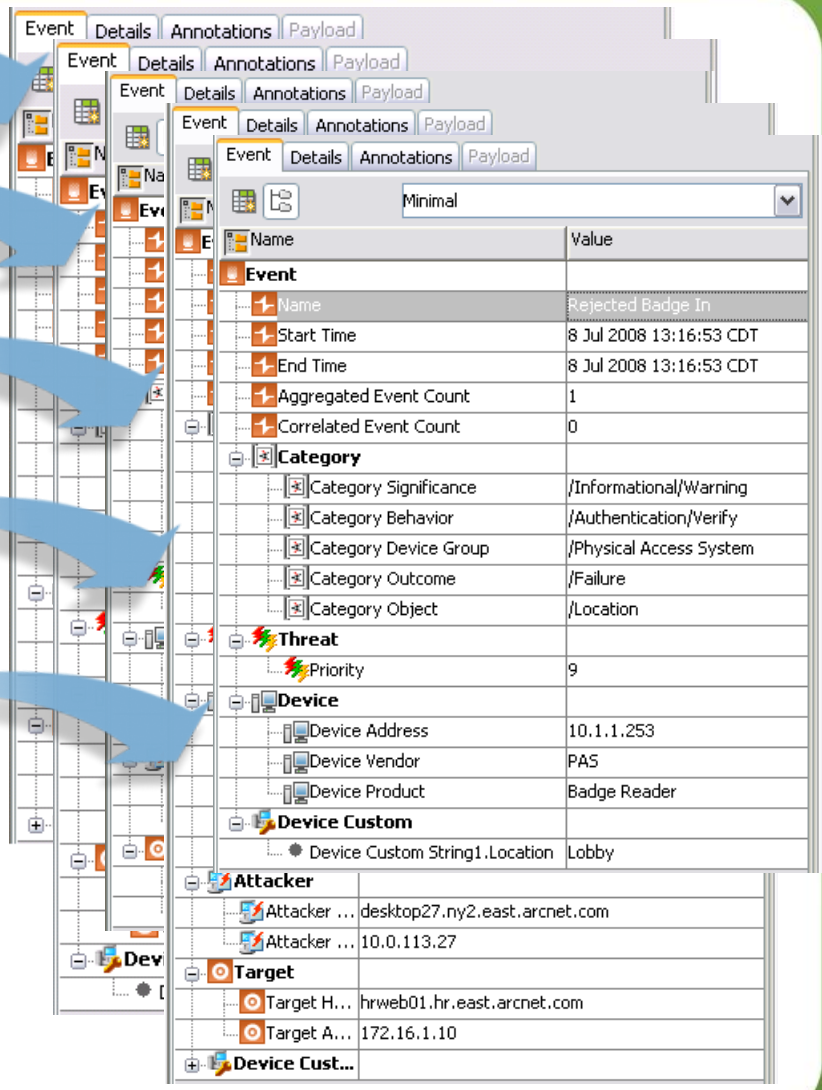
OS/390
Ошибка входа

UNIX
Ошибка входа

Oracle
Ошибка входа

Windows
Ошибка входа

HID-карты
Вход запрещён



ДиалогНаука

Модель ресурса и модель пользователя

Модель ресурса

Важность ресурса

Репозиторий ресурсов

Уязвимости
Подверженность ресурса атакам

Критичность ресурса
Насколько критичен данный ресурс для бизнеса?

Модель пользователя

Сопоставление
Кто стоит за данным IP-адресом?

Политики
Каково влияние события на бизнес?

Роль
Соответствует ли активность роли сотрудника?

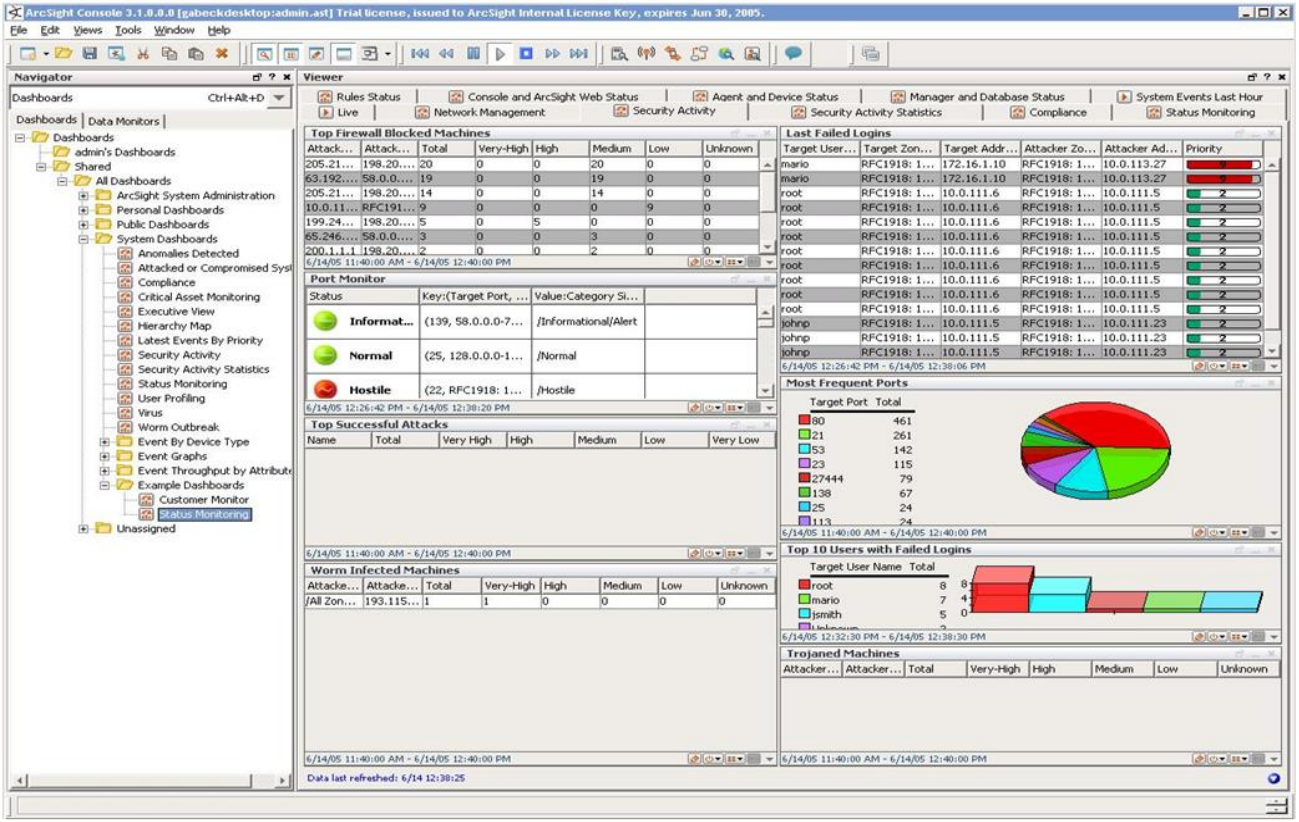
Профиль пользователя
С чем обычно работает данный пользователь?

- Чёткое понимание рисков и последствий
- Снижение количества ложных срабатываний
- Концентрация внимания на действительных угрозах и рисках

ДиалОгНаука

Визуализация
Консоль реального времени

- Разделение событий по категориям
- Возможность корреляции событий в реальном режиме времени, как по ресурсам, так и по злоумышленникам
- Возможности подробного анализа
- Возможность создания коррелированных отчетов

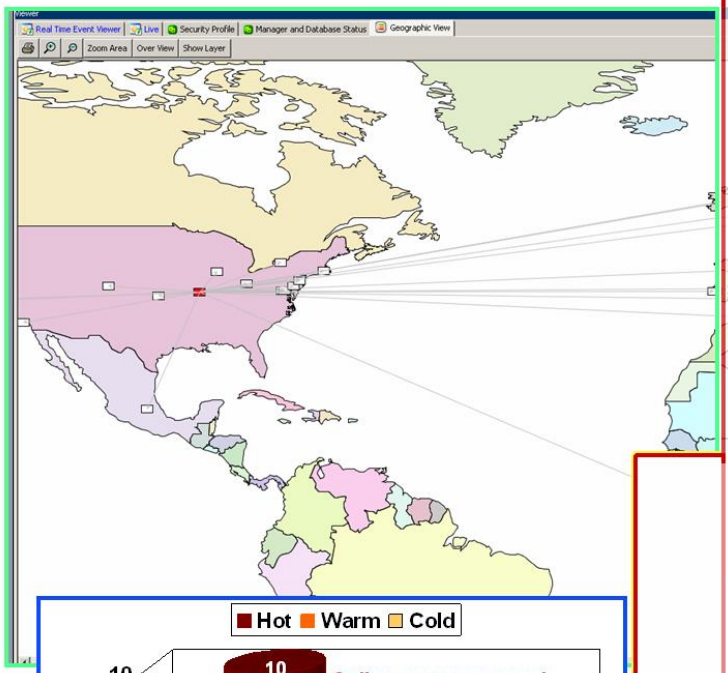


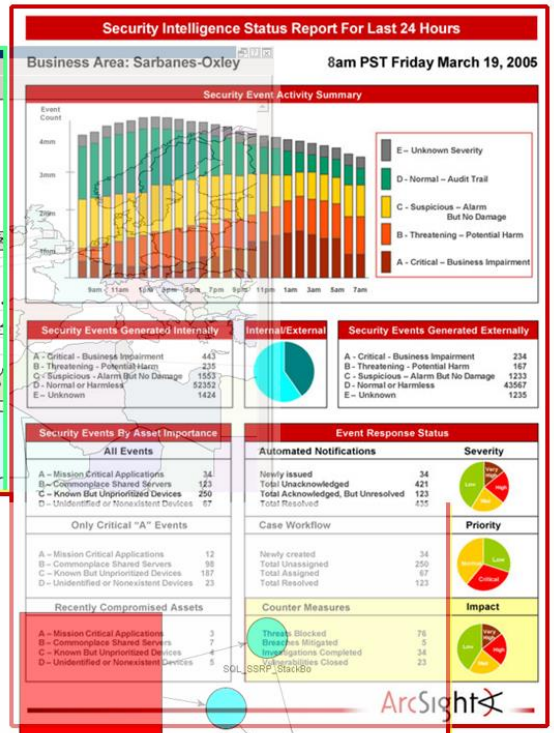
Категоризация событий обеспечивает мгновенную идентификацию атаки

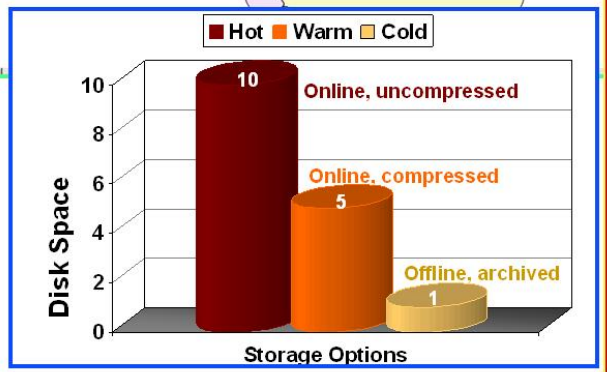
ДиалОгНаука

Глобальный режим наблюдения отклонений безопасности

- Интерфейс реального времени с географическим расположением объектов и представлением отклонений в параметрах безопасности
- Отображение событий по подразделениям или устройствам
- Выбор между опасностью события или его категорией
- Интуитивно понятный инструментальный интерфейс для подготовки табличных и графических отчетов о безопасности или показ карты нарушений безопасности



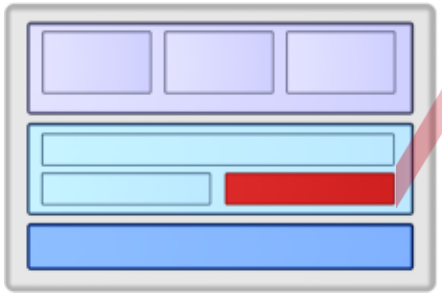




ДиалОгНаука

Управление журналами работы

ArcSight Logger



L750MB – хранение 50ГБ журналов, до 750 Мб данных в день – **49$**

- Эффективное, автоматизированное хранение терабайтных объёмов журнальных данных
- Оригинальный или нормализованный формат событий
- Встроенные отчёты для управления информационной безопасностью
- Получение данных одним запросом с нескольких устройств
- Встроенные политики автоматизированного хранения и очистки журналов

Доступен в виде:

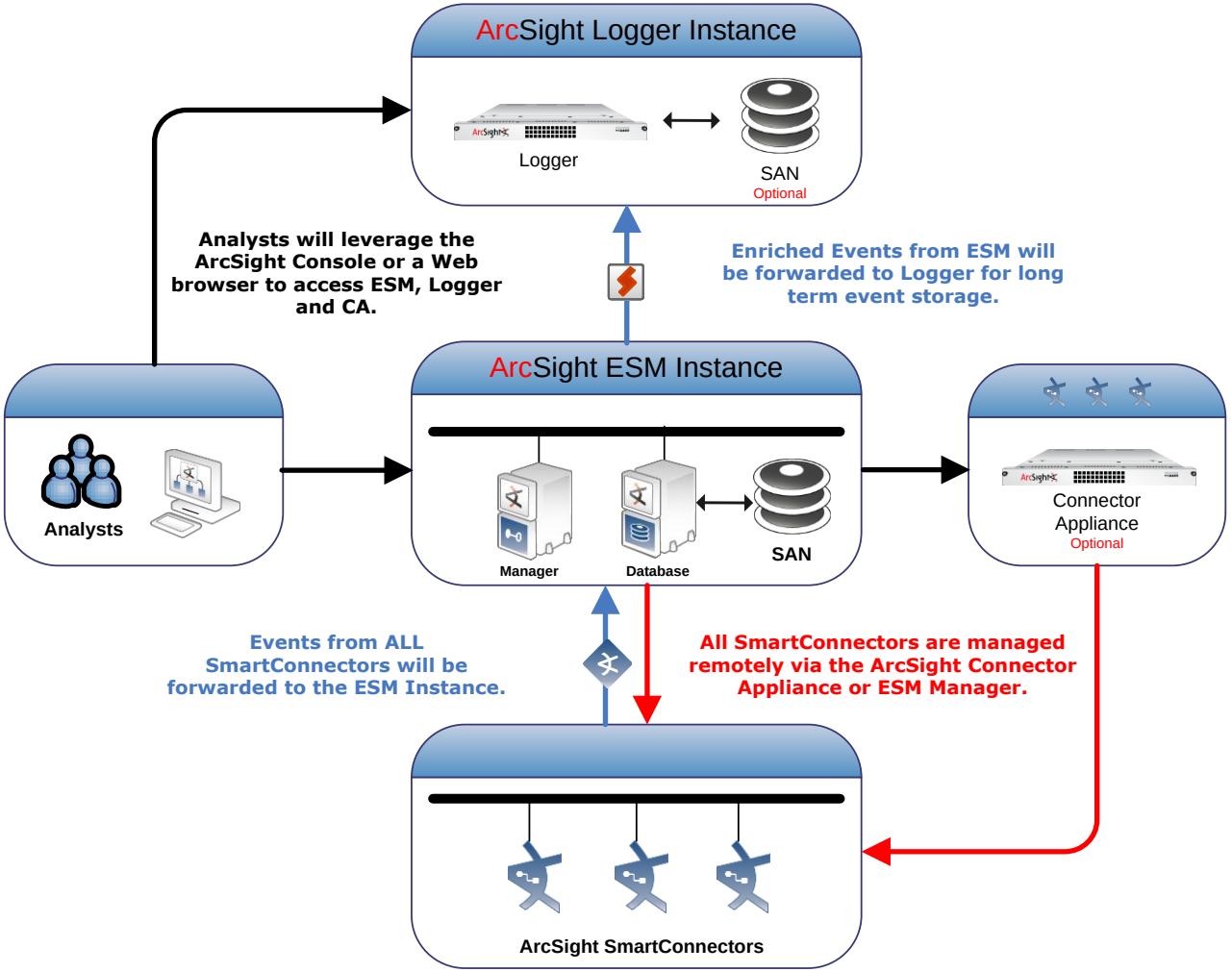
Система хранения и управления данными журналов (До 35 ТБайт)

Устройство хранения данных журналов в составе SAN

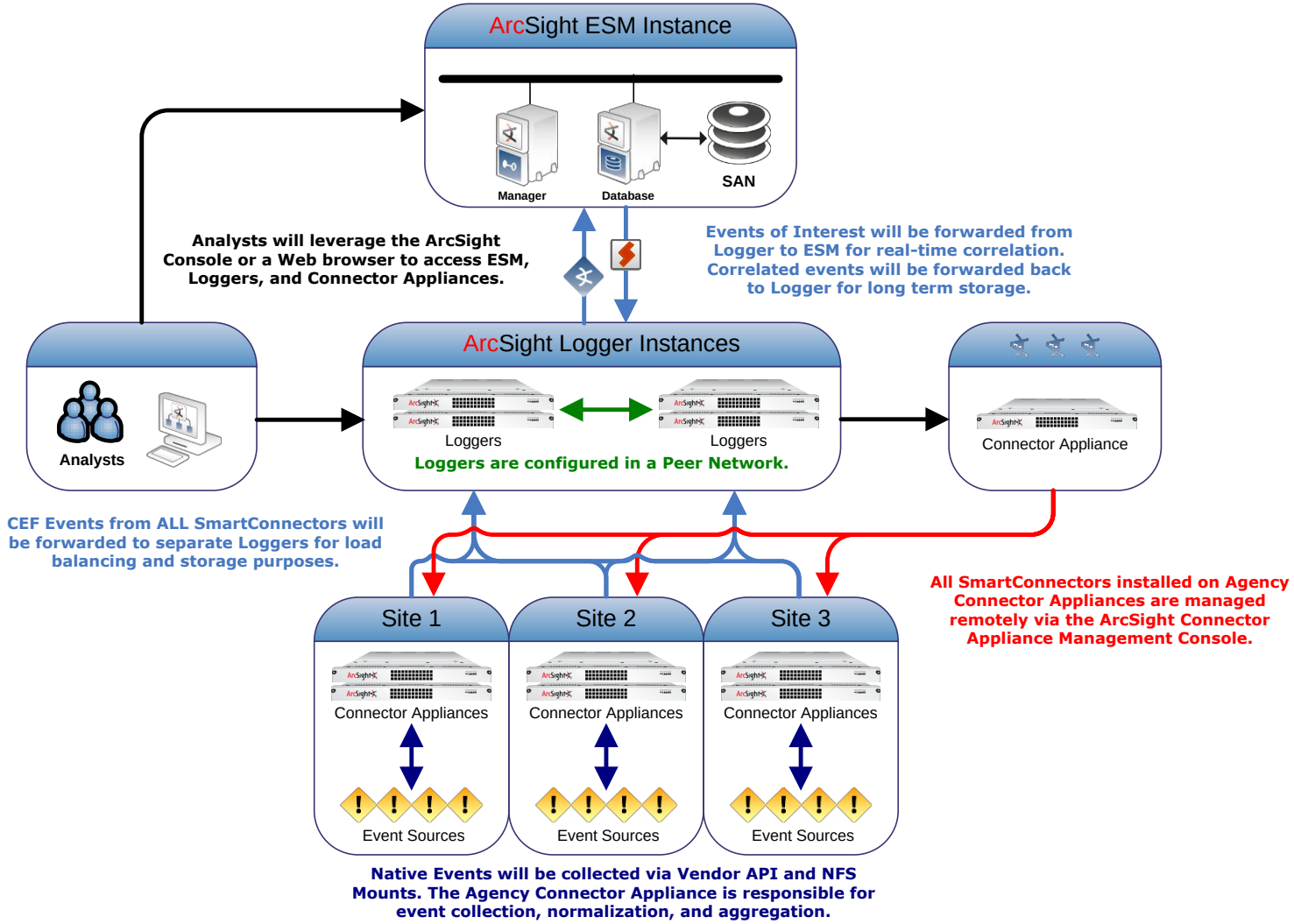
Отдельное ПО

Региональное устройство хранения и управления данными журналов

Использование ESM и Logger

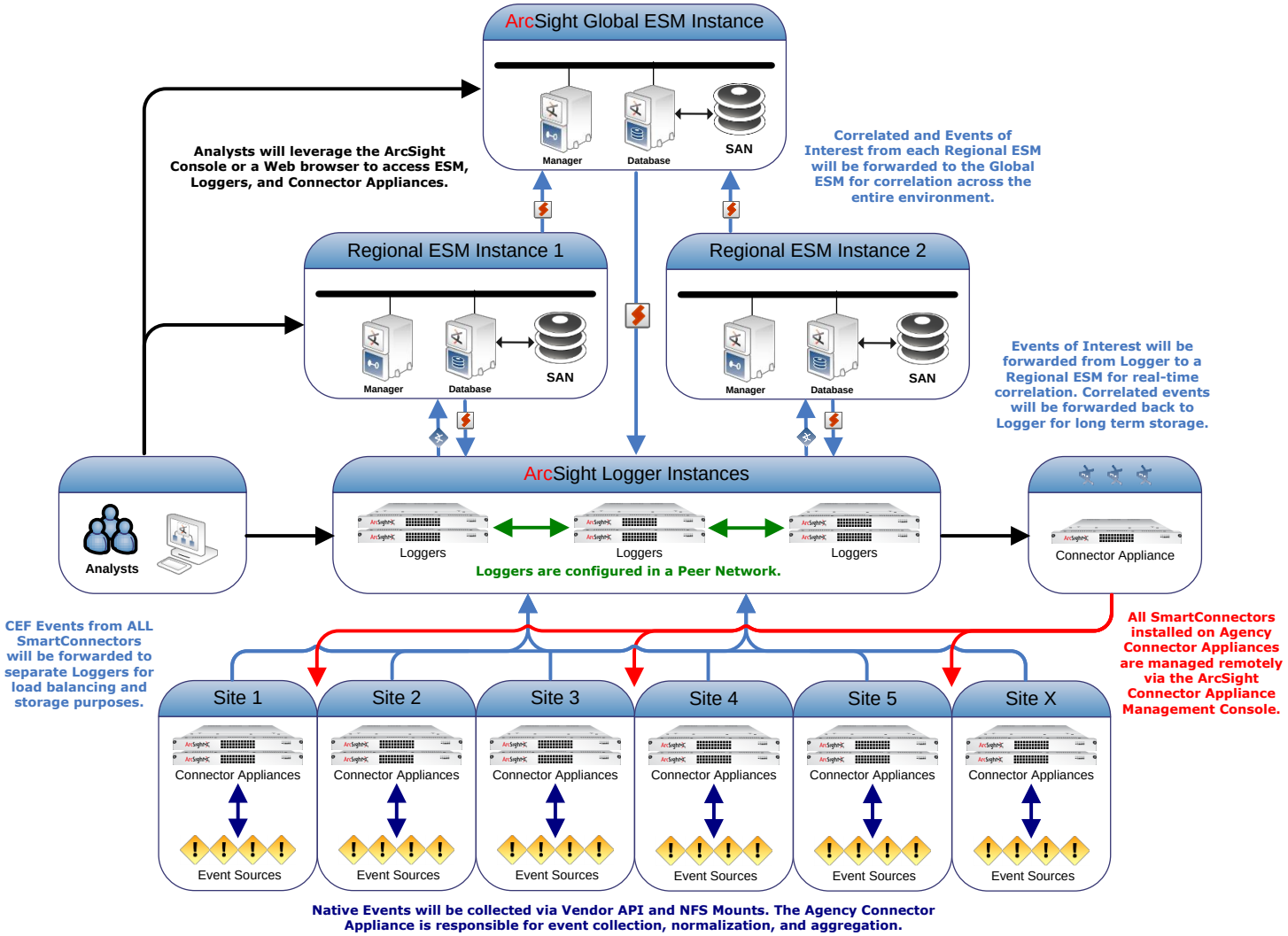


ESM & Logger: Фаза 1

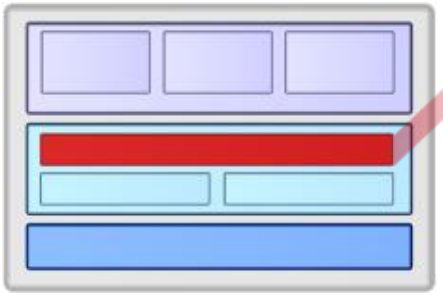


ДиалогНаука

ESM & Logger: Фаза 2



Эффективное направленное реагирование



ArcSight Threat Response Manager

- Создание карты сети для получения точного местонахождения пользователя и определения степени влияния проблемы
- «Помещение» пользователей или устройств в карантин на основе обработки кейса или в автоматическом режиме
- Выдача рекомендаций (списка действий) для ручного решения проблемы

Доступен в виде:

Устройство для интеграции с ArcSight ESM

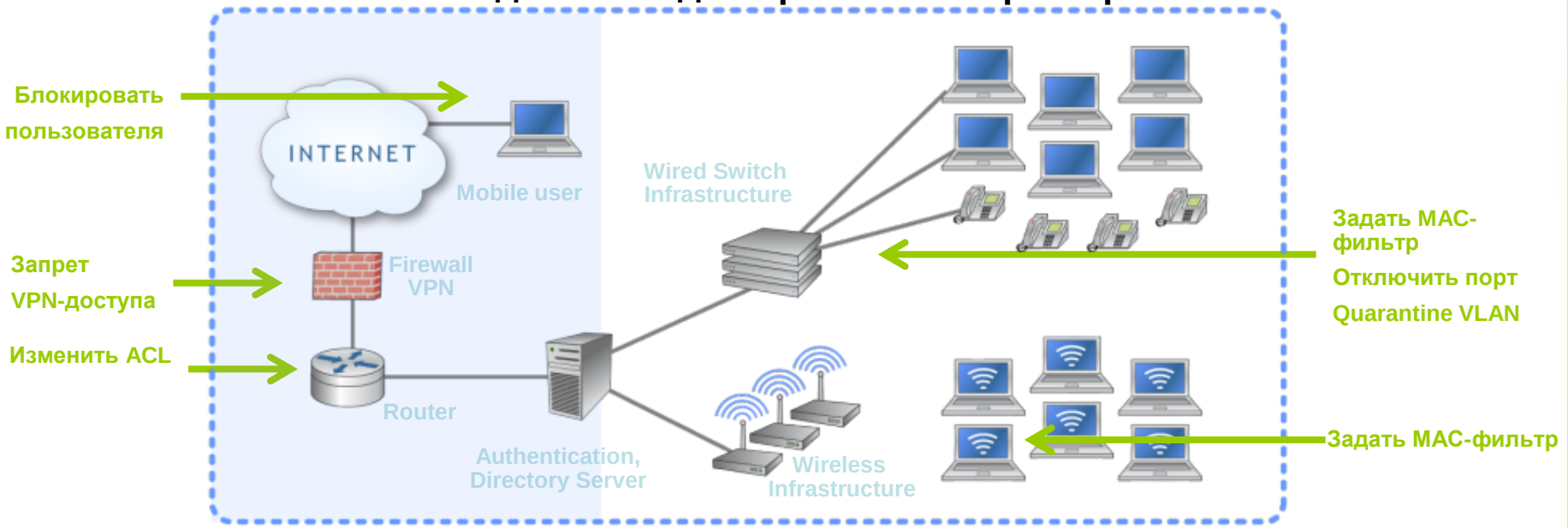
Гибкая, эффективная локализация проблем

ДиалогНаука

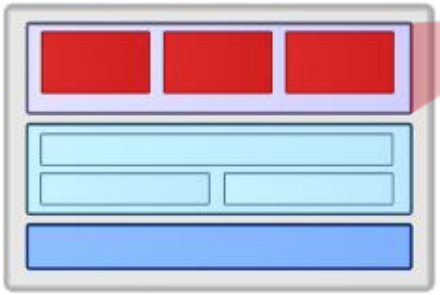
Принцип работы ArcSight Threat Response Manager

- **Локализация**
  - Определение адреса узла и получение списка коммутаторов/маршрутизаторов, с которыми связан данный узел
- **Анализ**
  - Поиск ближайшей к узлу «контрольной точки»
  - Поиск оптимального способа карантина узла
- **Реагирование**
  - Применение MAC-фильтра
  - Отключение порта
  - Ограничение VLAN
  - Изменение ACL
  - Блокировка учётной записи пользователя

Несколько воздействий для правильного реагирования



Дополнительные пакеты ArcSight



Дополнительные пакеты ArcSight

- Набор правил, отчётов, графических панелей и коннекторов
- Стандарты: оценка соответствия стандартам и\или законодательству
- Бизнес: решение наиболее распространённых задач защиты информации

Доступны в виде:

Отдельного ПО

Стандарты:

SOX/JSOX IT Gov
PCI FISMA

Бизнес:

IdentityView
Fraud Detection
Sensitive Data Protection

Предустановленного устройства

ДиалОгНаука

Спасибо за внимание!

Ваши вопросы…

117105, г. Москва, ул. Нагатинская, д. 1
Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75
http://www.DialogNauka.ru
e-mail: Rodion.Chekharin@DialogNauka.ru