ДиалогНаука

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

Чехарин Родион, CISSP

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

Современные проблемы информационной безопасности

Большое количество 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

Что используется в системе безопасности?

- Межсетевые экраны
- Системы создания VPN
- Anti-virus
- Network IDS/IPS, Router Based IPS
- Host IDS/IPS
- Анализ уязвимостей -Vulnerability Assessment
- Системы управления обновлениями - Patch Management
- Анализ соответствия принятым политиками безопасности - Policy Compliance
- Защищенные маршрутизаторы (Router)
- Управление безопасностью на L2 (Switch)

ДиалОгНаука

Эшелонированная защита

МЭ
VPN
IDS

Авторизация

Антивирусное ПО

Политики доступа

ПЕРСОНАЛЬНЫЕ И СЕКРЕТНЫЕ ДАННЫЕ

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

Почему необходим единый центр управления ?

- 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

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

Система мониторинга: укрупнённый вид

Программно-аппаратное обеспечение

Персонал

Технические специалисты

Специалисты по защите данных

Документация

Политики

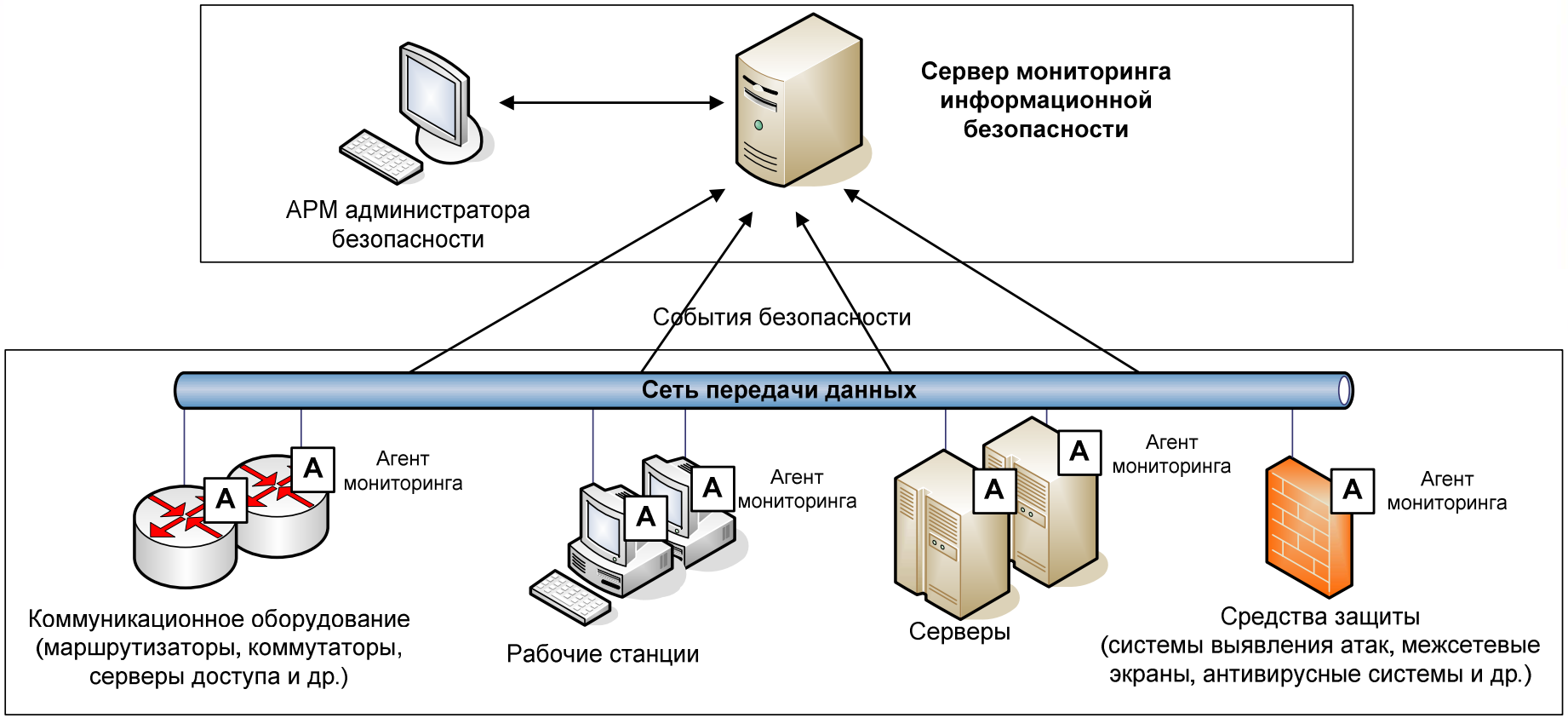
Регламенты

Модели угроз \ нарушителя

Оценка рисков

ДиалогНаука

Архитектура СМ для управления ИБ



ДиалогНаука

Реализация СЦ

Формальный подход

Реалистичный подход

ДиалОгНаука

Основные этапы внедрения СМ

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

ДиалогНаука

Обследование

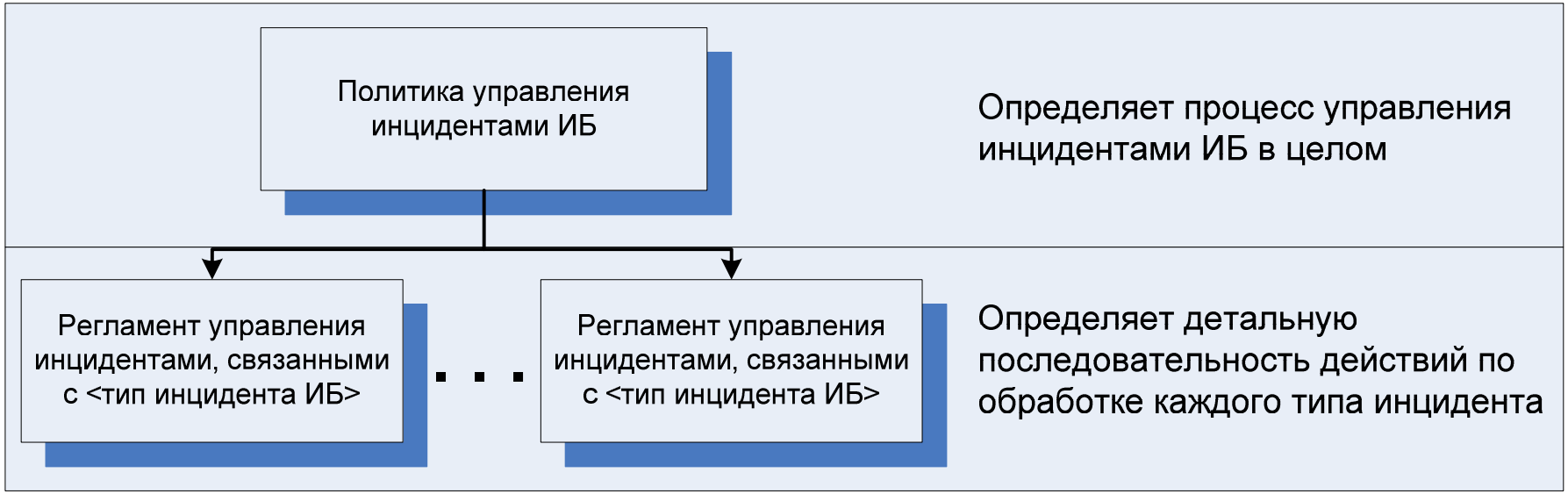
- Сбор информации об источниках, которые необходимо подключить к системе мониторинга
- Определение и согласование для каждого источника списка действий и событий, мониторинг которых будет проводиться
- Определение перечня соответствующих режимов аудита, которые необходимо включить на уровне источника
- Определение объема событий, поступающих со всех типов источников, подключенных к системе мониторинга

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

Разработка нормативных документов



ДиалОгНаука

Разработка технических и системных решений

- Разработка архитектуры системы мониторинга (состав и размещение компонентов) с учетом требований по отказоустойчивости и обеспечению надежности
- Определение функциональных требований к системе мониторинга событий информационной безопасности
- Разработка общесистемных решений по эксплуатации и управлению системой мониторинга
- Определение порядка установки и настройки системы мониторинга

ДиалОгНаука

Установка и настройка системы мониторинга

- Установка аппаратной и программной составляющих системы мониторинга
- Контроль установки режимов аудита на всех источниках, подключаемых к системе мониторинга
- Настройка системы мониторинга (группировка источников событий, настройка параметров архивирования и и резервирования базы событий и др.)
- Разработка эксплуатационной документации на систему мониторинга (инструкция оператору, администратору и т.д.)

ДиалОгНаука

Опытная эксплуатация системы мониторинга

- Тестирование и проверка функциональных возможностей системы мониторинга
- Нагрузочные испытания системы мониторинга
- Отработка регламентов управления инцидентами ИБ
- Перевод системы в промышленную эксплуатацию по результатам тестирования

ДиалогНаука

Практический опыт:

Внедрение СЦ

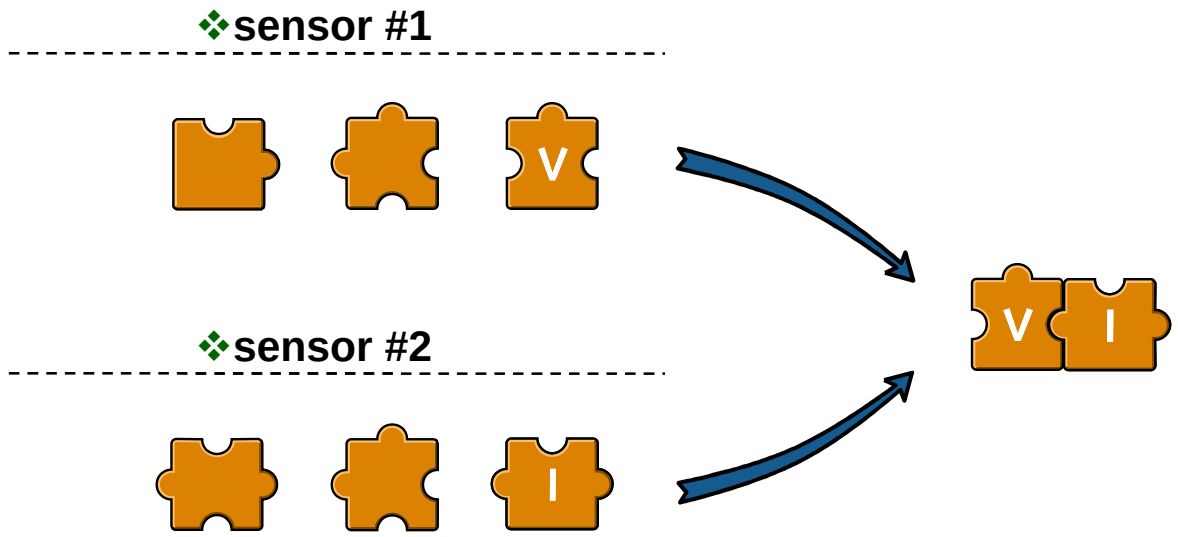
- Выделение зоны мониторинга
  - Либо сегмент сети, либо «боевые» серверы, сетевое оборудование
- Создание перечня объектов мониторинга
  - Зачатую происходит аудит или инвентаризация
- Оценка состояния журналирования
  - Регулярное непонимание со стороны службы IT – вплоть до саботажа
- Оценка регламентирующих 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 техподдежки

Корреляция получаемых событий

- ✓ Микро корреляция – сравнение полей данных от устройств одного типа. Большинство вендоров предоставляют именно такой вид корреляции. Также такой вид корреляции называется элементарной корреляцией.
- ✓ Макро корреляция – сравнение разнородных наборов данных от различных источников.

Типы корреляции

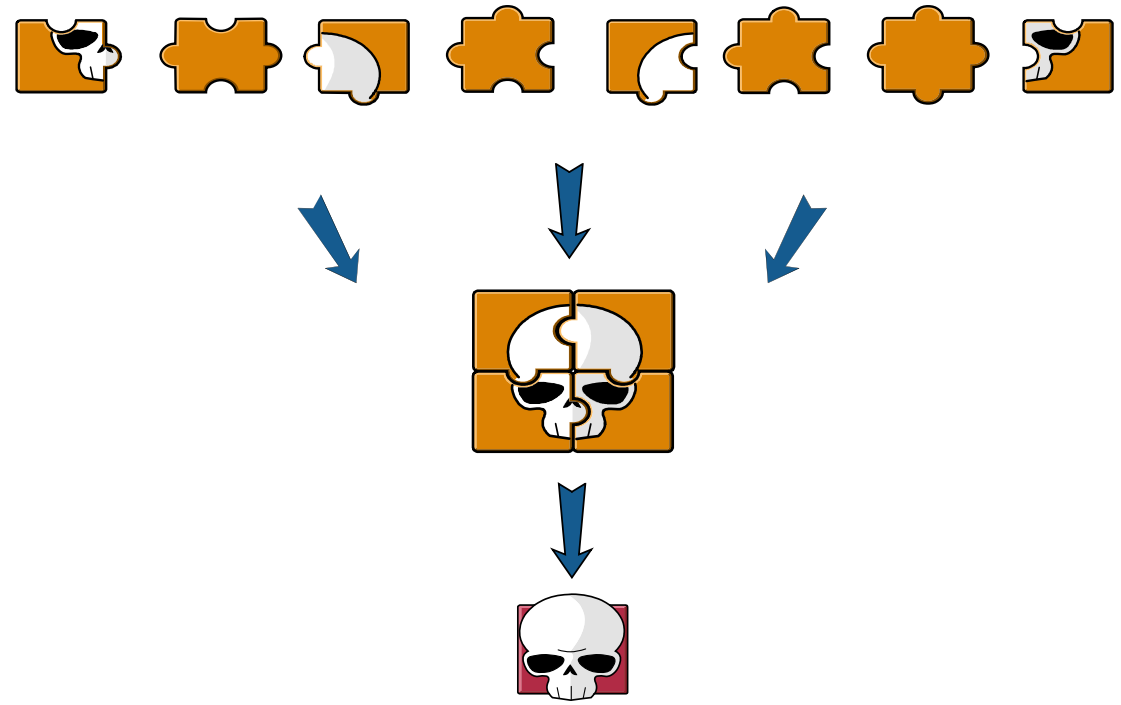
Корреляция по полям данных – *корреляция похожих событий нормализованных данных. Например, все атаки на порт 80 для www-сервера .*



ДиалогНаука

Типы корреляции

Корреляция в соответствии с правилами – *возможность используя специфические правила относить несколько событий к одному событию определенной категории. Часто используется для корреляции событий происходящих в разные промежутки времени.*



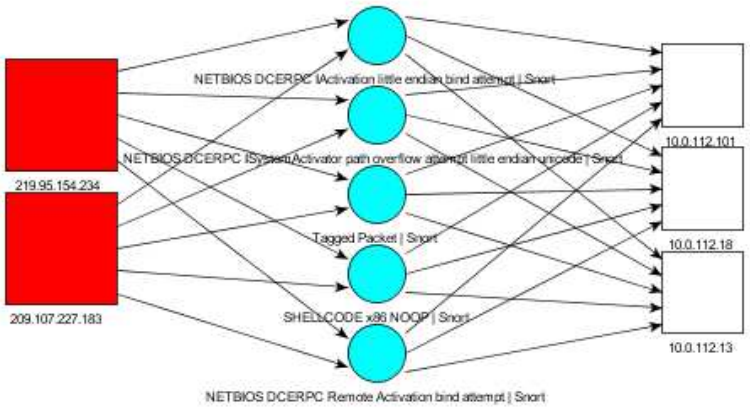
ДиалОгНаука

Практический опыт:

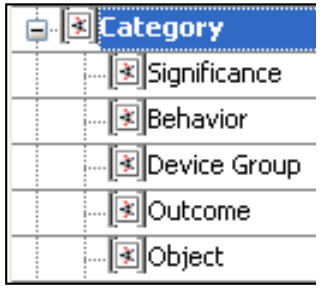
Основные применения СМ

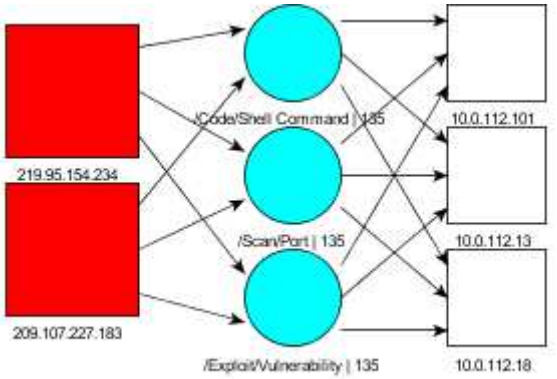
Выявление шаблонов действий, поведения пользователей, доступа к системам

- Повторяющееся поведение, наблюдаемое при различных сетевых транзакциях.
- Транзакция однозначно идентифицируется источником и получателем.
- Поведение идентифицируется по соответствующим полям событий, обычно по названиям событий или их категориям.



Категории:





ДиалогНаука

Практический опыт:

Основные применения СЦ

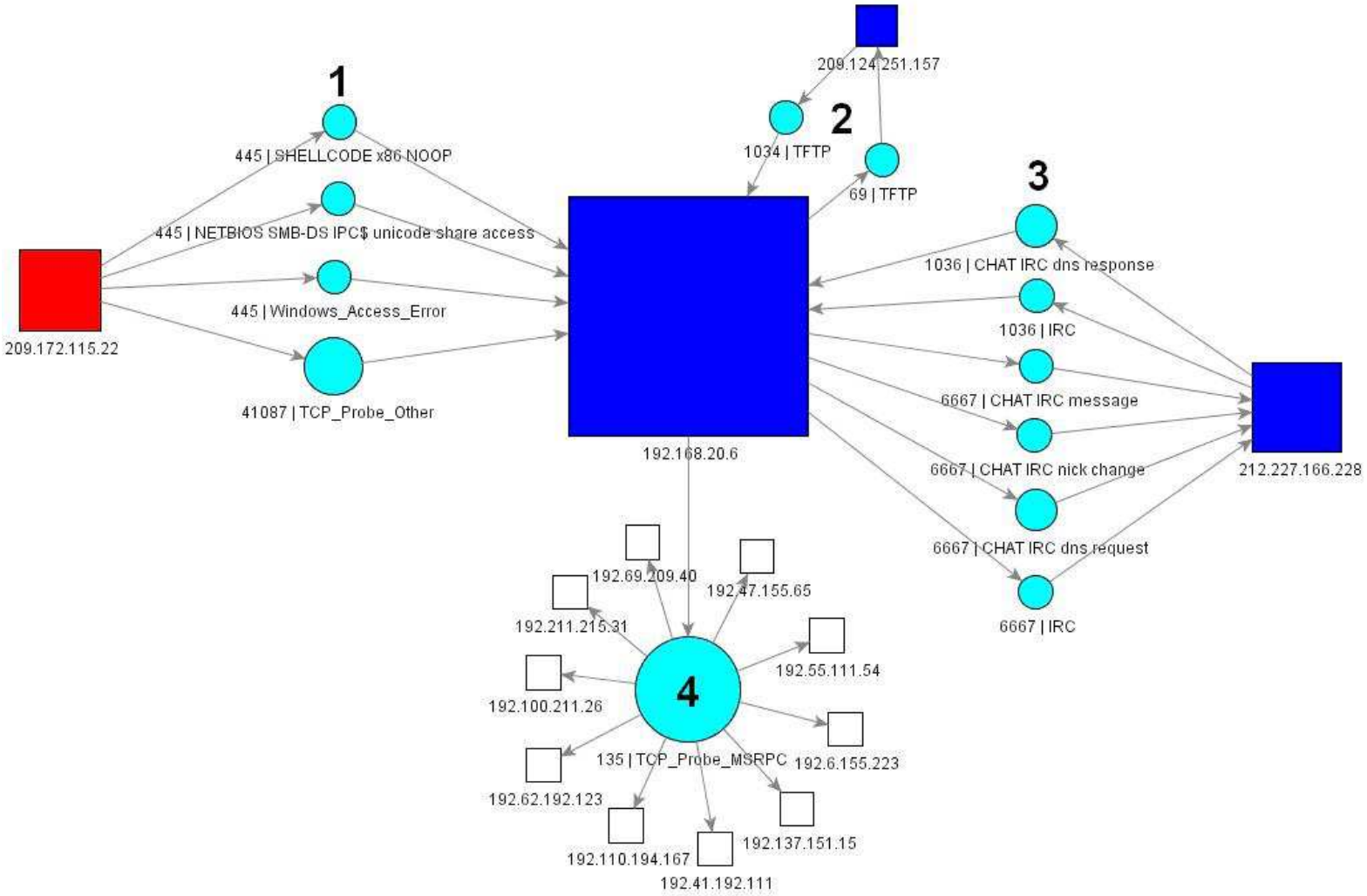
Почему шаблоны поведения представляют интерес:

- Шаблоны предоставляют информацию об атаках или об использовании сети, или нет понимания, что в итоге должно быть найдено
- Шаблоны помогают выявлять первые появления аномалий
- Шаблоны выявляют повторы аномалий – возможное повторение инцидента

Практический опыт:

Основные применения СЦ

Zotob – Реальный пример



ДиалогНаука

Практический опыт:

Основные применения СМ

Name	Device Product
TCP_Probe_Other	RealSecure Network Sensor
(portscan) Open Port	Snort
(portscan) TCP Portscan	Snort
SHELLCODE x86 NOOP	Snort

Zotob PNP Exploit

Name	Device Product
TFTP	RealSecure Network Sensor
Suspicious Communication From Att...	ArcSight

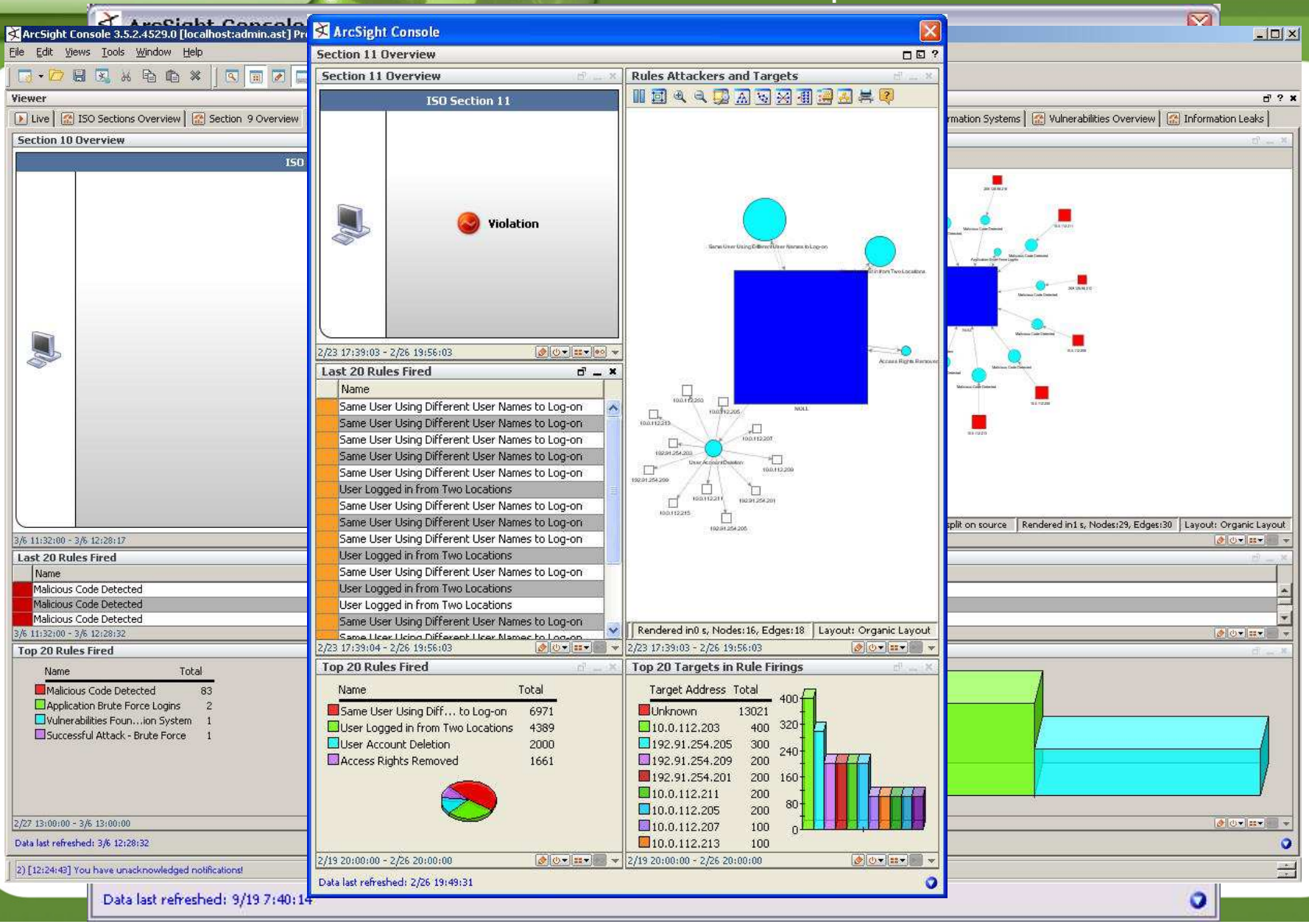
Name	Device Product
CHAT IRC message	Snort
CHAT IRC dns request	Snort
IRC	RealSecure Network Sensor
CHAT IRC nick change	Snort
Suspicious Communication From Att...	ArcSight

Name	Device Product
TCP_Service_Sweep	RealSecure Network Sensor
TCP_Probe_MSRPC	RealSecure Network Sensor
Suspicious Communication From Att...	ArcSight

ДиалогНаука

Практический опыт:

Основные применения СМ
Оценка соответствия



ДиалОгНаука

Практический опыт:

Основные применения СМ
Оценка соответствия

Главы ISO	**Политика безопасности**			**Контроль доступа**		
	Организация информационной безопасности			**Приобретение, разработка и установка систем**		
	Управление ресурсами			**Управление инцидентами информационной безопасности**		
	Безопасность персонала			**Управление бесперебойной работой организации**		
	Физическая безопасность и безопасность окружения			**Соответствие правовым и нормативным требованиям**		
Анализ активности	Бизнес процессы	Мониторинг политик		**Управление рисками**		
	Вход/Выход			**Активность администраторов**		
	Изменение привилегий			**Уволенные сотрудники**		
	Изменения настроек			**Уязвимости**		
Потоки данных	Приложения	Базы данных	ОС	HIDS	IAM	**Уязвимости**
	Межсетевые экраны	**IDS\IPS**		**Сетевое оборудование**		

ДиалогНаука

Практический опыт:

Основные применения CM 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

CM: 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

Пример 1: о возможностях корреляции событий ИБ

Пример 1:

- Будем считать, что некоторая система мониторинга имеет возможность определять географическое расположение объекта по его IP-адресу
- Рассмотрим далее такую ситуацию:

  Система мониторинга регистрирует факт удаленного доступа по VPN-каналу с IP-адреса, который находится за пределами России, а в настройках указано, что данный сотрудник не находится в зарубежной командировке и может удаленно работать только внутри страны, тогда система мониторинга автоматически сигнализирует о возможной компрометации логина и пароля, при помощи которого был выполнен удаленный доступ

ДиалогНаука

Примеры 2-4: о возможностях корреляции событий ИБ

Пример 2:

- Для операторов связи, предоставляющих доступ в Интернет по логину и паролю (через ADSL или Dial-Up), система СЦ при помощи корреляции может выявлять факты одновременного доступа с одним и тем же логином и паролем из географически разных точек, что может являться признаком компрометации

Пример 3:

- Система СЦ при помощи корреляции может сопоставлять зарегистрированные действия пользователей с их должностными ролями. Например, таким образом система СЦ может зарегистрировать факт получения доступа рядового сотрудника к бухгалтерской информации, к которой он не должен иметь доступ

Пример 4:

- Система СЦ при помощи корреляции может выявлять факты доступа к конфиденциальной информации в ночное (или в нерабочее) время

ДиалогНаука

Примеры 5-6: о возможностях корреляции событий ИБ

Пример 5:

- Система мониторинга при помощи корреляции может выявлять факт добавления и удаления у обычного пользователя административных прав в течение заданного промежутка времени. Это может свидетельствовать о том, что пользователю не санкционированно были добавлены права, и после того как он выполнил определённые действия, эти права были удалены

Пример 6:

- Система мониторинга при помощи корреляции событий ИБ может выявить факт доступа к конфиденциальной информации с одним и тем же логином и паролем с разных компьютеров в течение небольшого промежутка времени (например, одного часа)
- Это может свидетельствовать о компрометации логина и пароля пользователя
- Точно также система мониторинга может регистрировать факт доступа к информации с одного компьютера, но с разными логинами и паролями

ДиалогНаука

Пример 7: о возможностях корреляции событий ИБ

Пример 7:

- Предположим, что система обнаружения вторжений, установленная в какой-то автоматизированной системе, регистрирует атаку типа «SQL injection» на сервис СУБД Oracle сервера X
- Поскольку данная атака может нарушить работоспособность базы данных, система обнаружения вторжений устанавливает ей высокий уровень приоритета
- Однако система мониторинга может проверить собственно сам факт наличия на сервере X базы данных Oracle, и только если она действительно установлена, и подвержена указанной атаке, то тогда система SIEM оставляет уровень приоритета без изменений
- В противном случае система мониторинга позволяет понизить уровень приоритета выявленного события

ДиалогНаука

Эксплуатация СМ
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

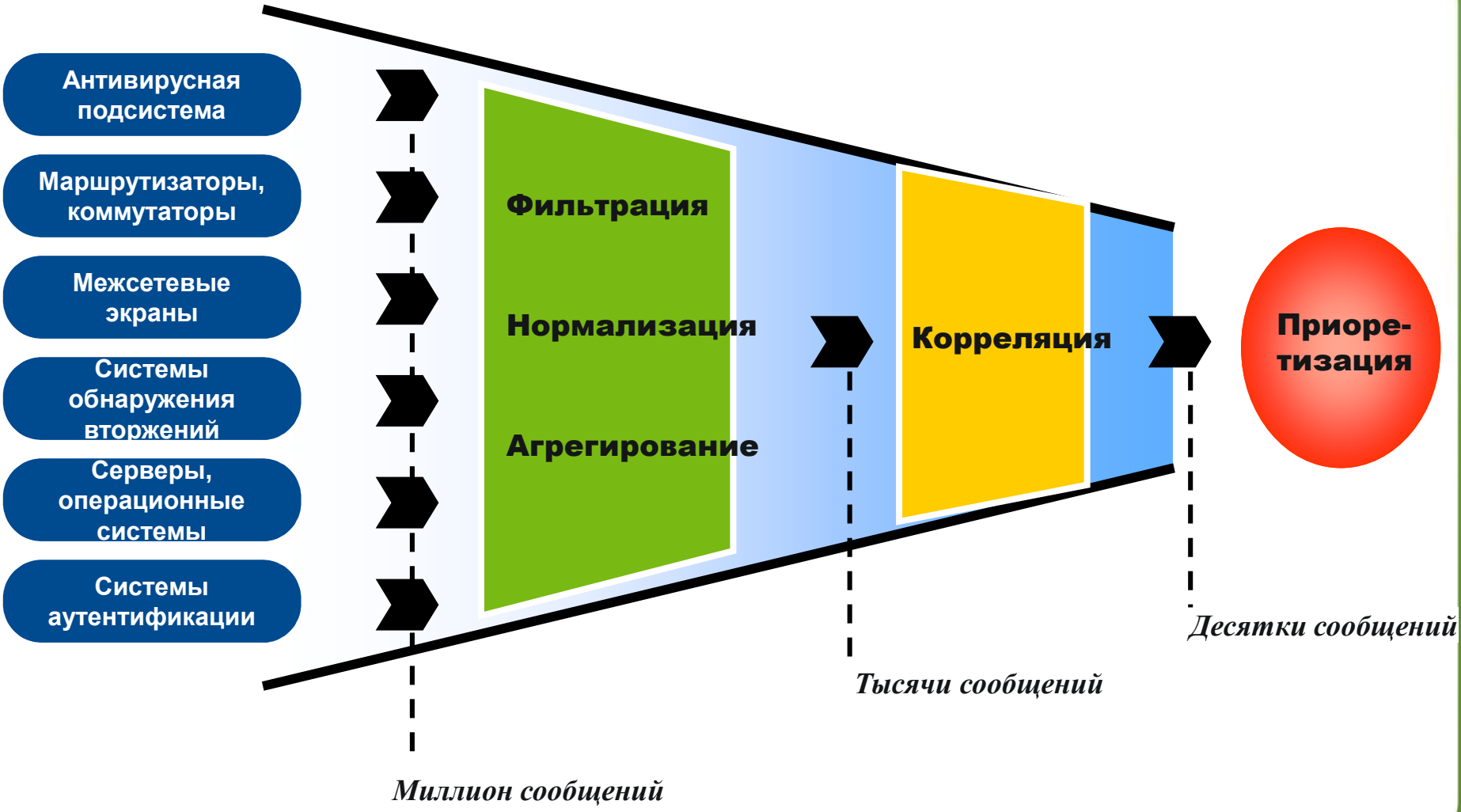
ДиалогНаука

Требования к ПАК СМ

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 специфические функции 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

Принцип работы ПО СМ



ДиалогНаука

Фазы обработки сообщений

- 1. Сбор данных (Collection)
- **Перемещение данных журналов из устройств безопасности или их систем управления в единую базу данных.**

- 2. Нормализация (консолидация) (Consolidation)
- **Сбор данных разных форматов из различных источников приведение (преобразование) данных к единому виду и создание единого лог файла.**

- 3. Агрегирование
- **Процесс удаления дублированных событий для уменьшения количества поступающих данных и экономии времени их последующей обработки и анализа. Агрегирование событий также используется для удаления дублированных событии от множества систем.**

- 4. Корреляция (Correlation)
- **Случайное, взаимодополняющее, эквивалентное или обратное соотношение между двумя сравниваемыми событиями, особенно структурное, функциональное, или качественное.**

- 5. Приоретизация (Prioritization)

ДиалОгНаука

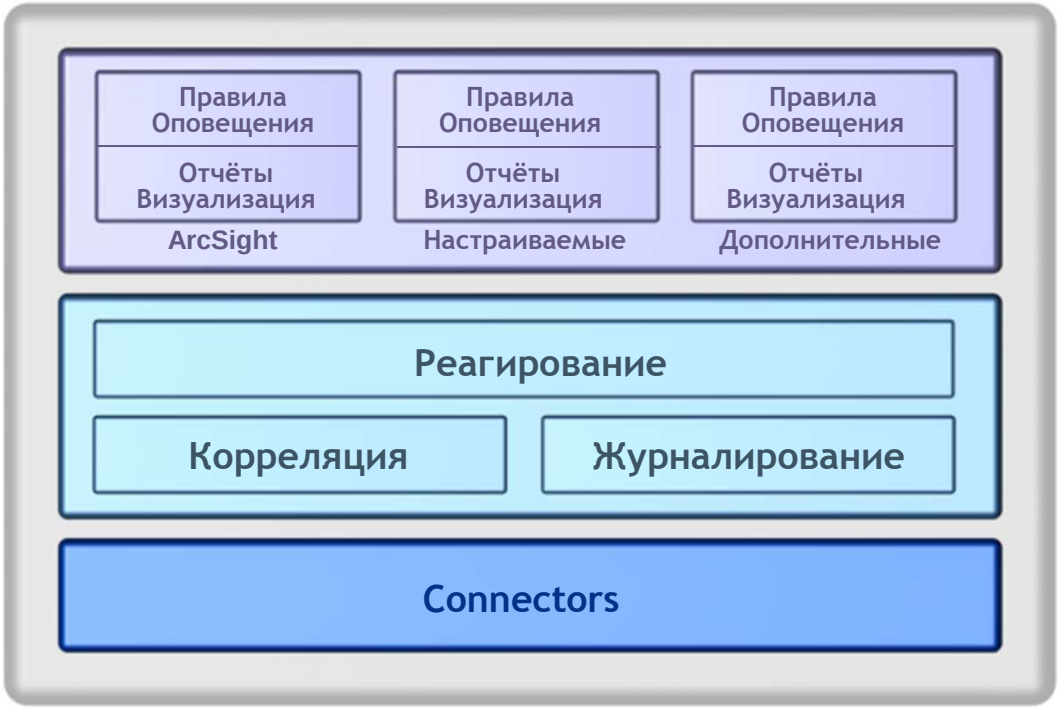
ArcSight ESM Архитектура

Интегрированная платформа для сборки, обработки и оценки информации о событиях информационной безопасности.

Модульный уровень

Уровень ядра

Уровень интеграции



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

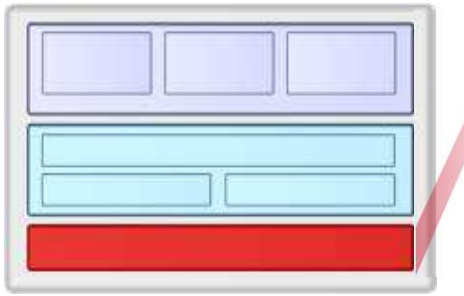
Гибкое подключение новых источников

SmartConnector

FlexConnector

ДиалОгНаука

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

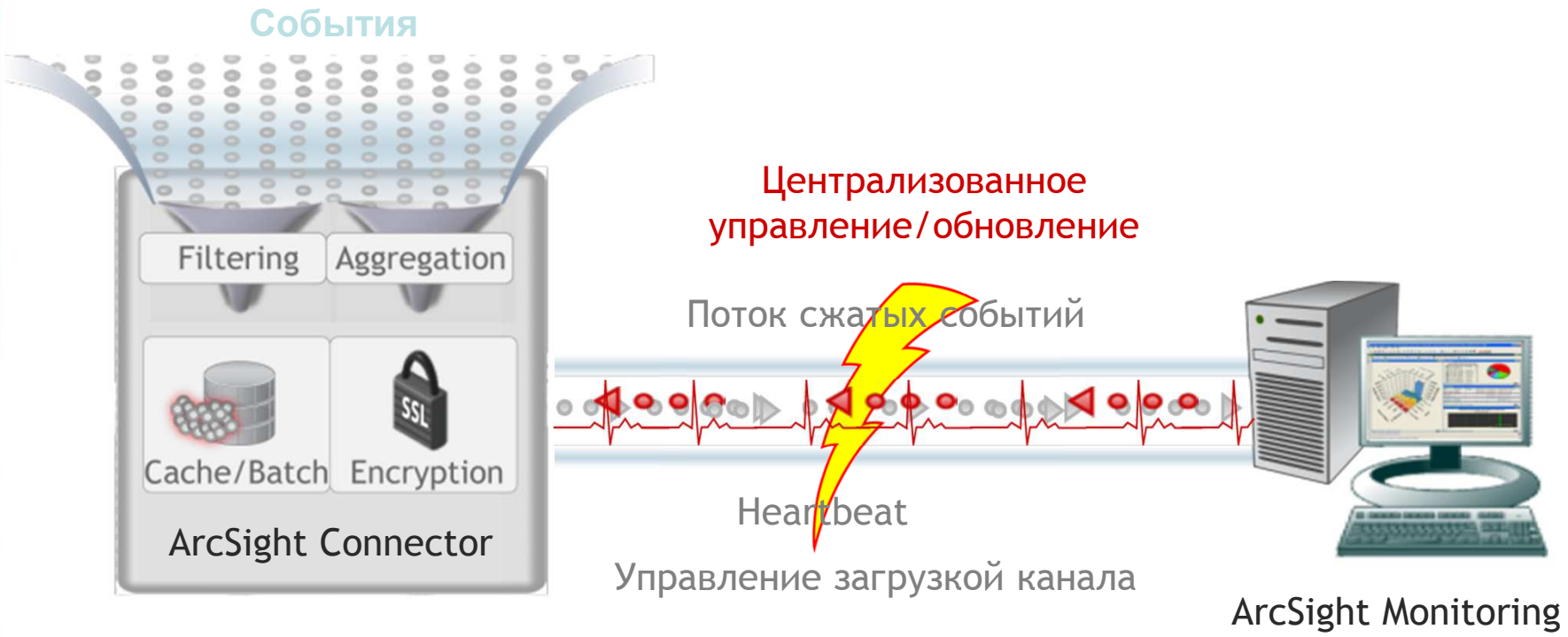
ДиалогНаука

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		

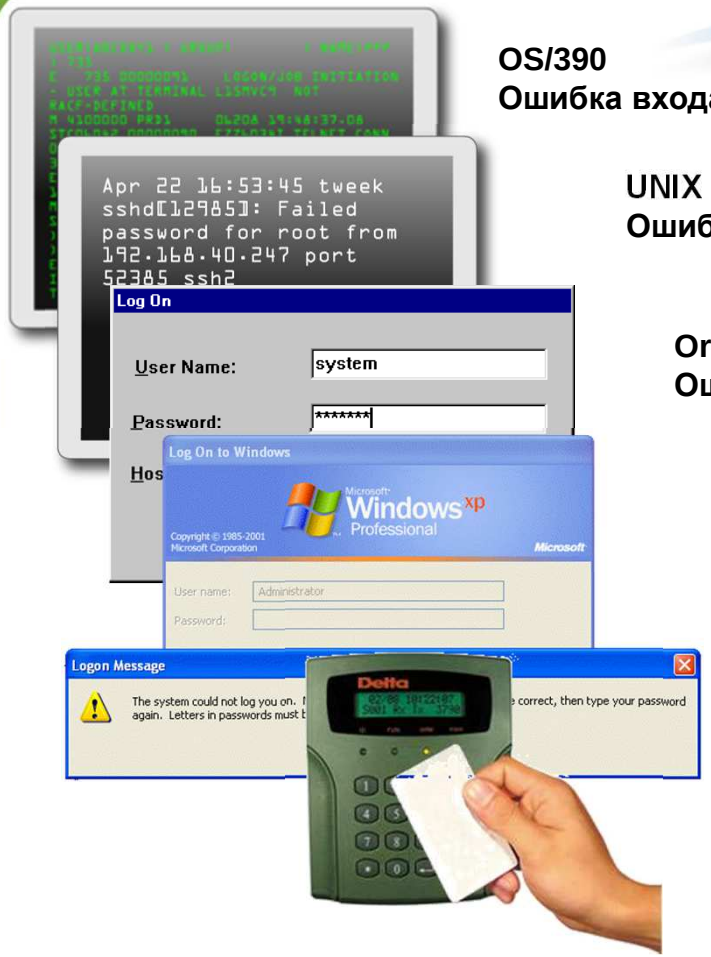
ДиалОгНаука

Отказоустойчивая архитектура сбора событий



ДиалОгНаука

Достоинства: Нормализация



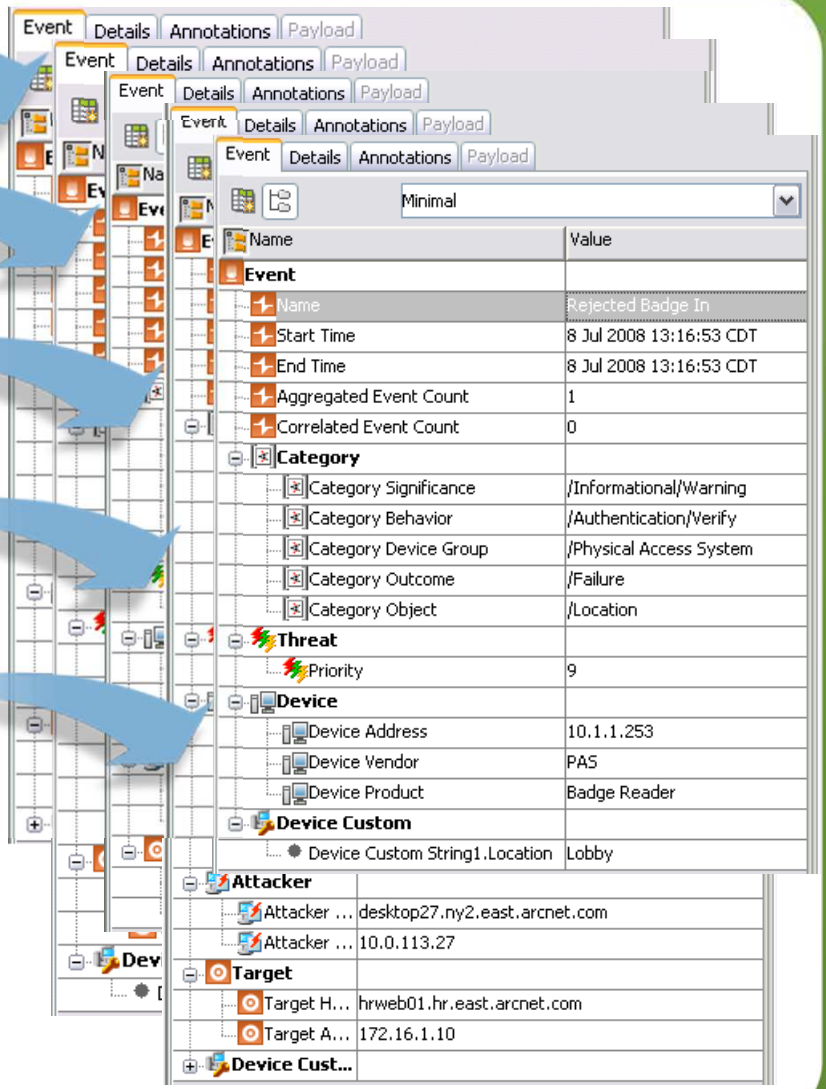
OS/390
Ошибка входа

UNIX
Ошибка входа

Oracle
Ошибка входа

Windows
Ошибка входа

HID-карты
Вход запрещён



ДиалогНаука

Достоинство: Категоризация

- Общая модель событий для всех устройств и программ
- Возможность понять действительную важность событий от различных систем
- Анализ событий независимо от типа устройства

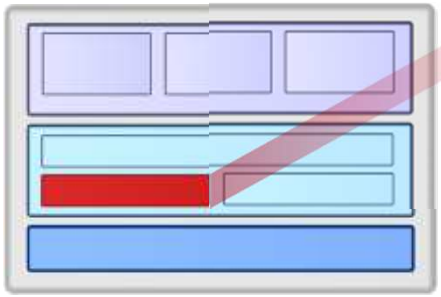
Без категоризации

```
Apr 22 16:53:45 tweek
sshd[12985]: Failed
password for root from
192.168.40.247 port
52385 ssh2
```

Категоризированное событие

CATEGORY	
Significance	/Informational/Warning
Behavior	/Authentication/Verify
Device Group	/Operating System
Outcome	/Failure
Object	/Host/Application/Service
Tuple Description	Failed Login Occurred

Корреляция



ArcSight ESM

- Анализ в режиме реального времени бизнес-событий
- Создание базовых шаблонов поведения
- Гибкая визуализация для разного уровня восприятия
- Корреляция – миллионы событий → инциденты безопасности

Доступен в виде:

Стоечное устройство ArcSight Express

Отдельное ПО

ДиалогНаука

Корреляция

Интеллектуальная корреляция событий в режиме реального времени для выявления необычных событий в сети

Корреляция в оперативной памяти

Более 100+ правил реального времени,
Мониторинг в реальном времени

Статистическая корреляция

Создание шаблонов поведения и выявление отклонений

Историческая корреляция

Корреляция архивный событий, по запросу или по расписанию

Connector Categorization

Active Lists
Динамические списки

Risk Based Prioritization
Отсев ложных срабатываний

Графический интер-фейс для создания правил
Не требует програм-мирования

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?

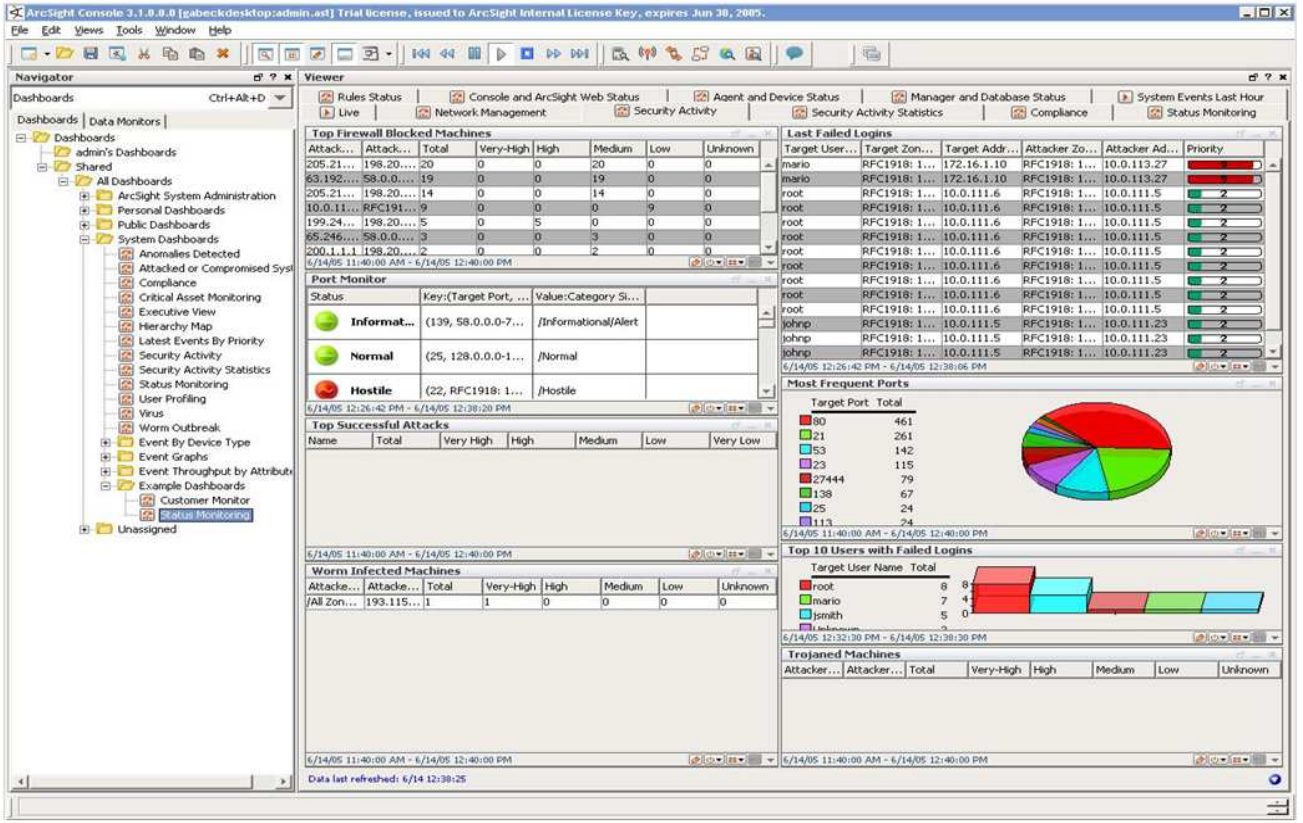
Профиль пользователя
С чем обычно работает данный пользователь?

- 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

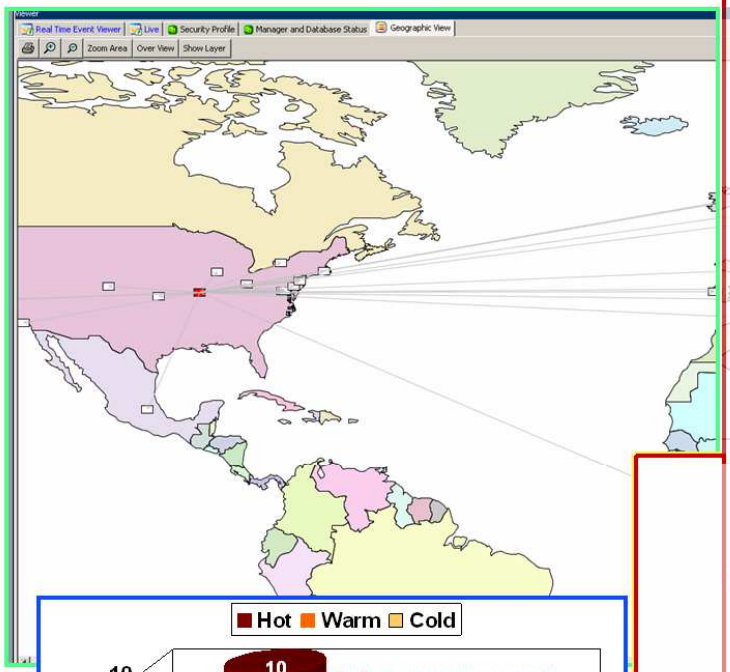


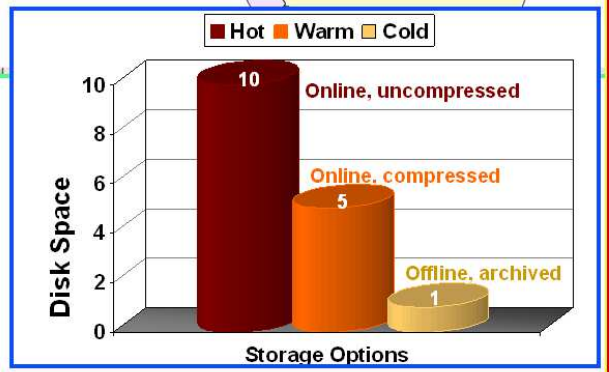
Категоризация событий обеспечивает мгновенную идентификацию атаки

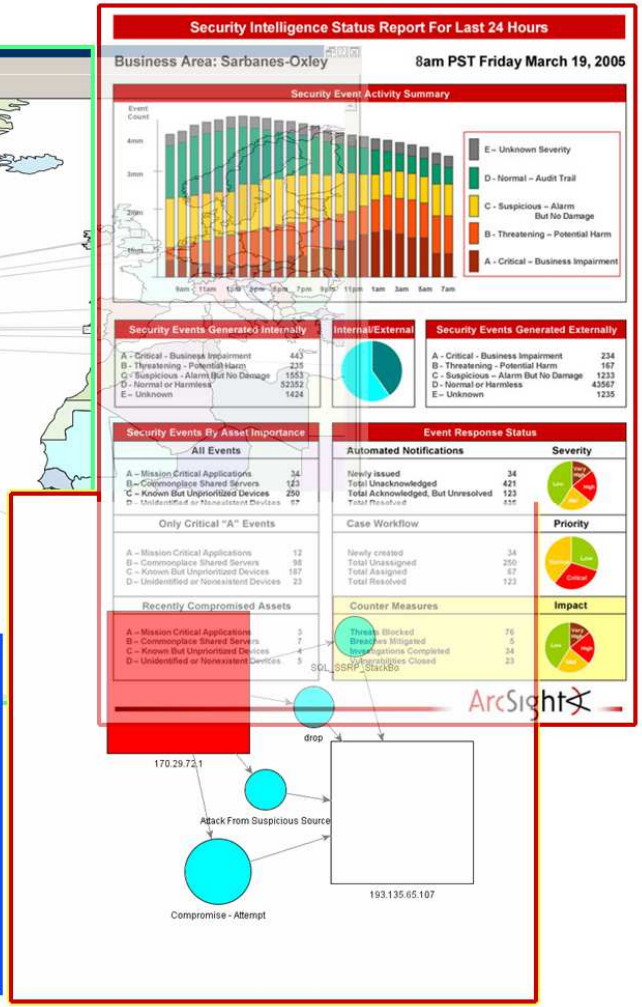
ДиалОгНаука

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

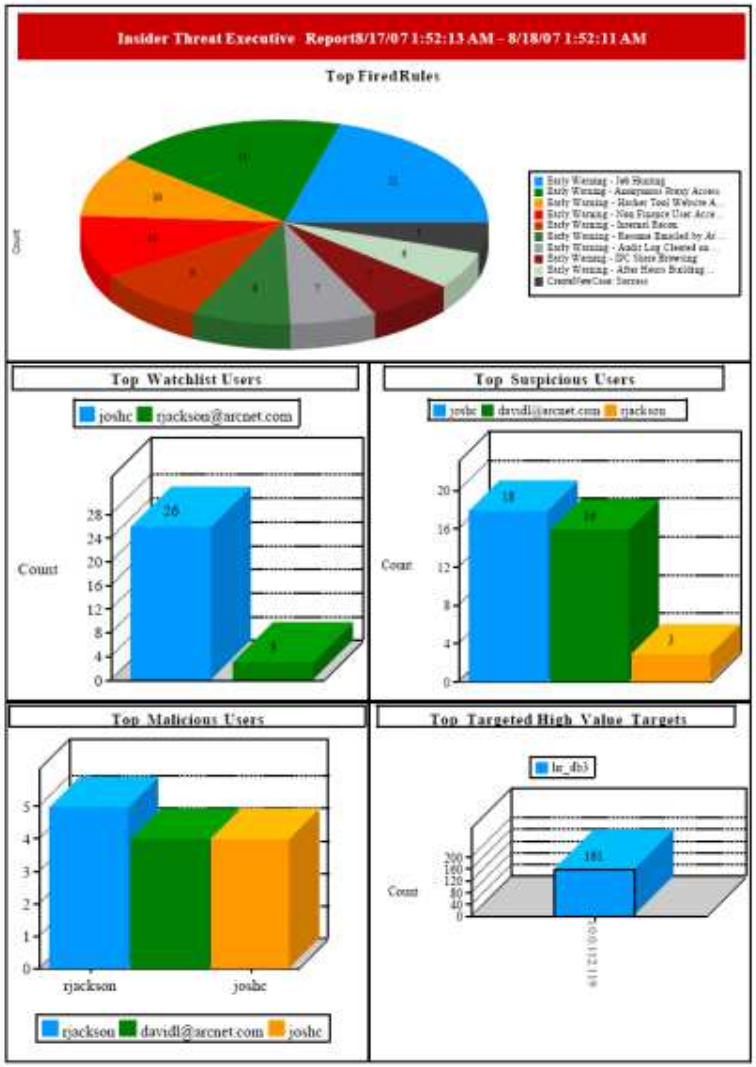






ДиалогНаука

Гибкая система отчётности



Production license, issued to ArcSight MSOC, expires Jan 01, 2010.

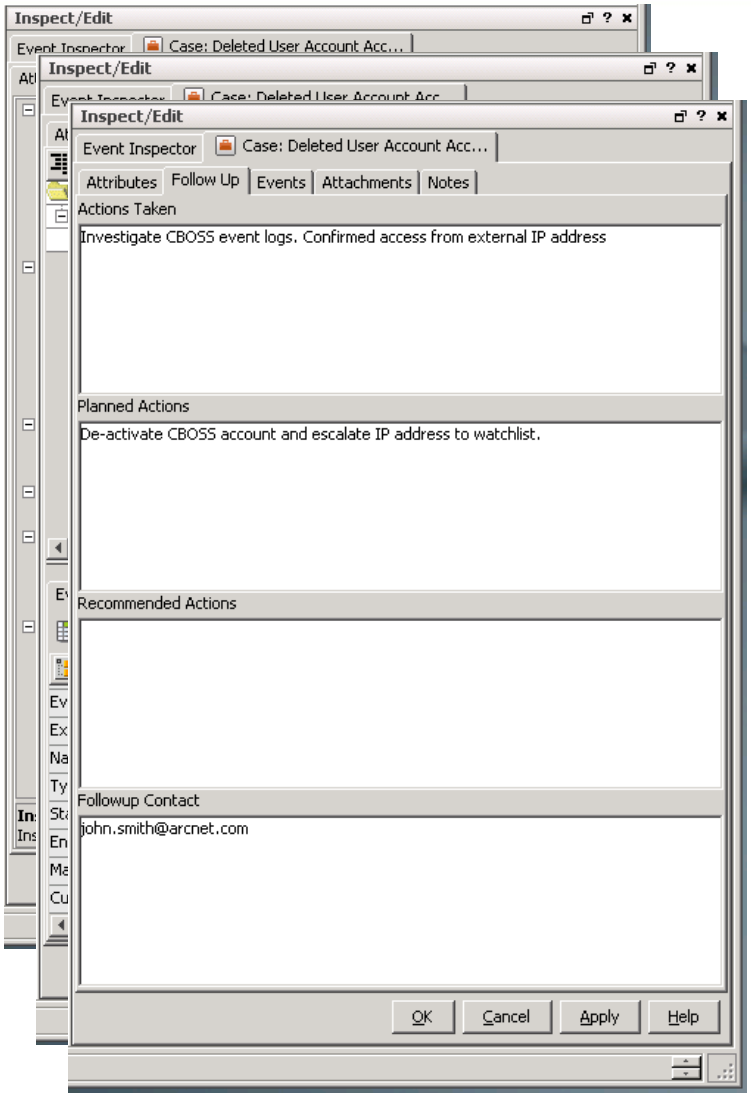
Поиск и анализ трендов

- Простое создание новых шаблонов
- Создание графических отчётов
- Не требует программирование
- Экспорт в различные форматы
  - HTML, XLS, PDF

ДиалОгНаука

Встроенное управление инцидентами

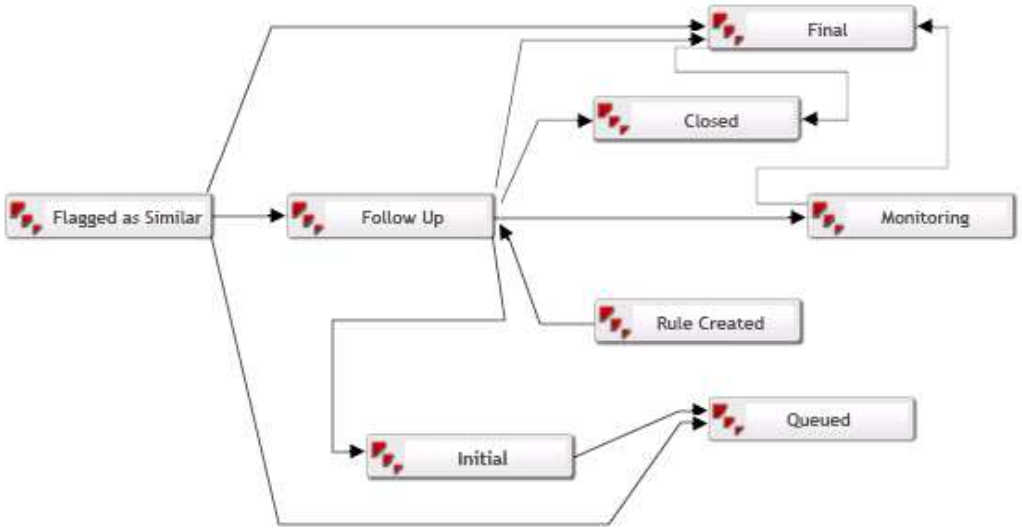
- Аннотации: Отслеживание и проведение инцидента в системе документооборота
- Cases: Создание инцидентов для специфических событий
- Этапы: Обработка инцидентов в соответствии с заданным порядком совместной работы
- Вложения: Дополнительные данные для расследований
- Оповещение в реальном времени
  - Email, пейджер или текстовые сообщения
  - SNMP сообщения

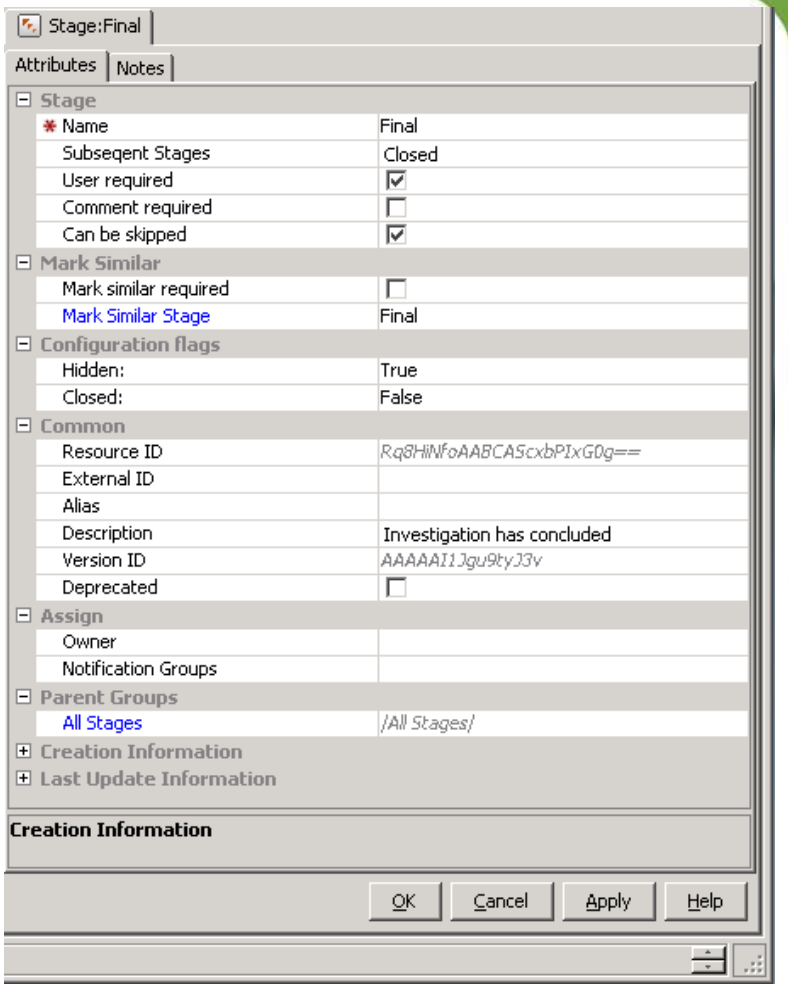


ДиалогНаука

Встроенный документооборот

- Этапы: обработка инцидентов в соответствии с заранее заданным, предназначенном для совместной работы процессом
- Аннотирование инцидентов для более полного анализа
- Интеграция со сторонними система документооборота

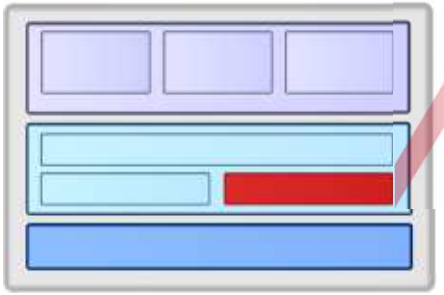




ДиалОгНаука

Управление журналами работы

ArcSight Logger

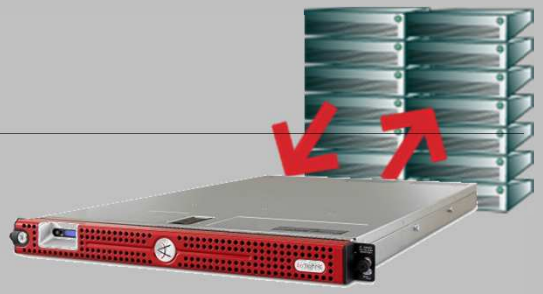


L750MB – хранение 50ГБ журналов, до 750 Мб данных в день – **49$**

- 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)



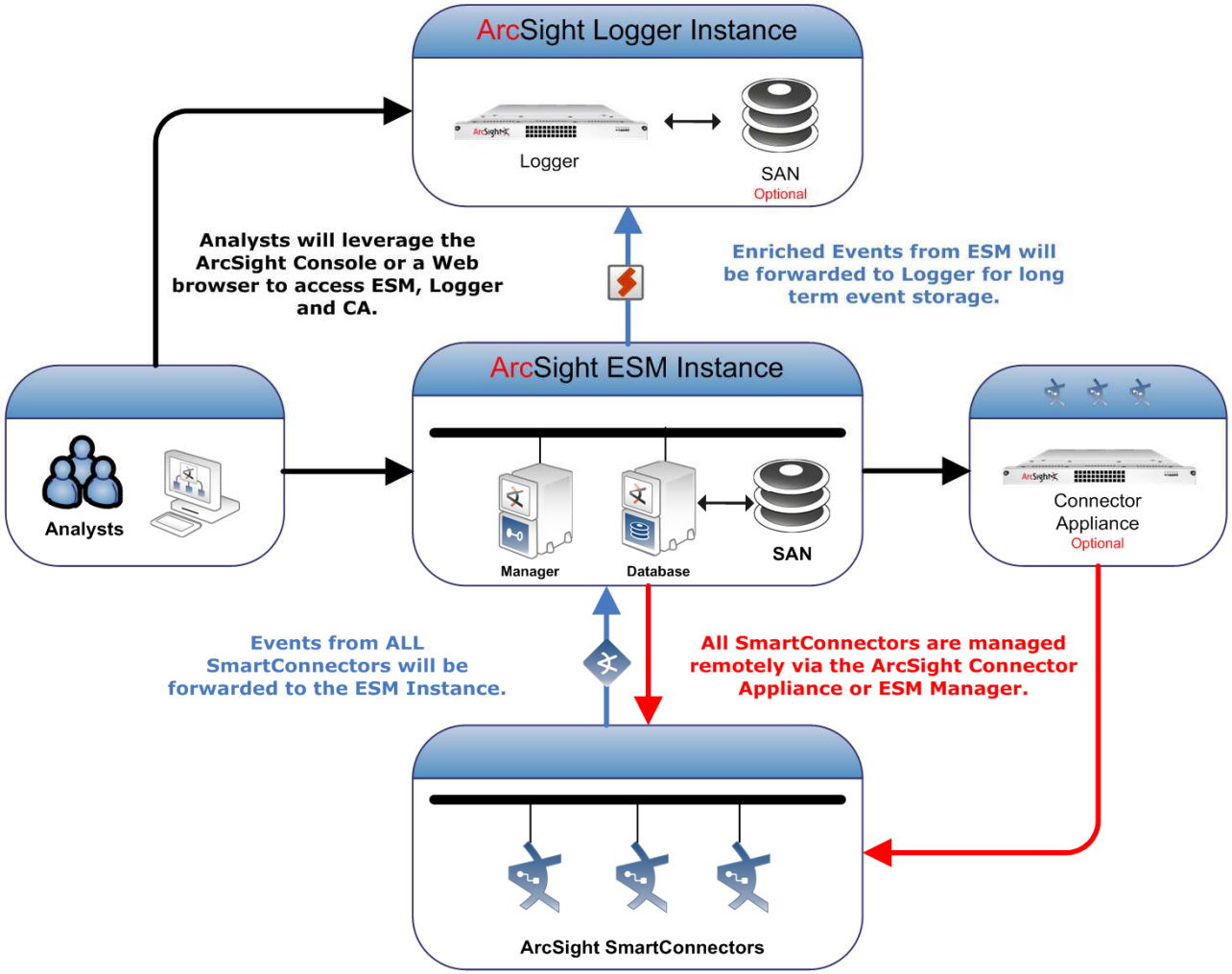
Устройство хранения данных журналов в составе SAN

Отдельное ПО

Региональное устройство хранения и управления данными журналов

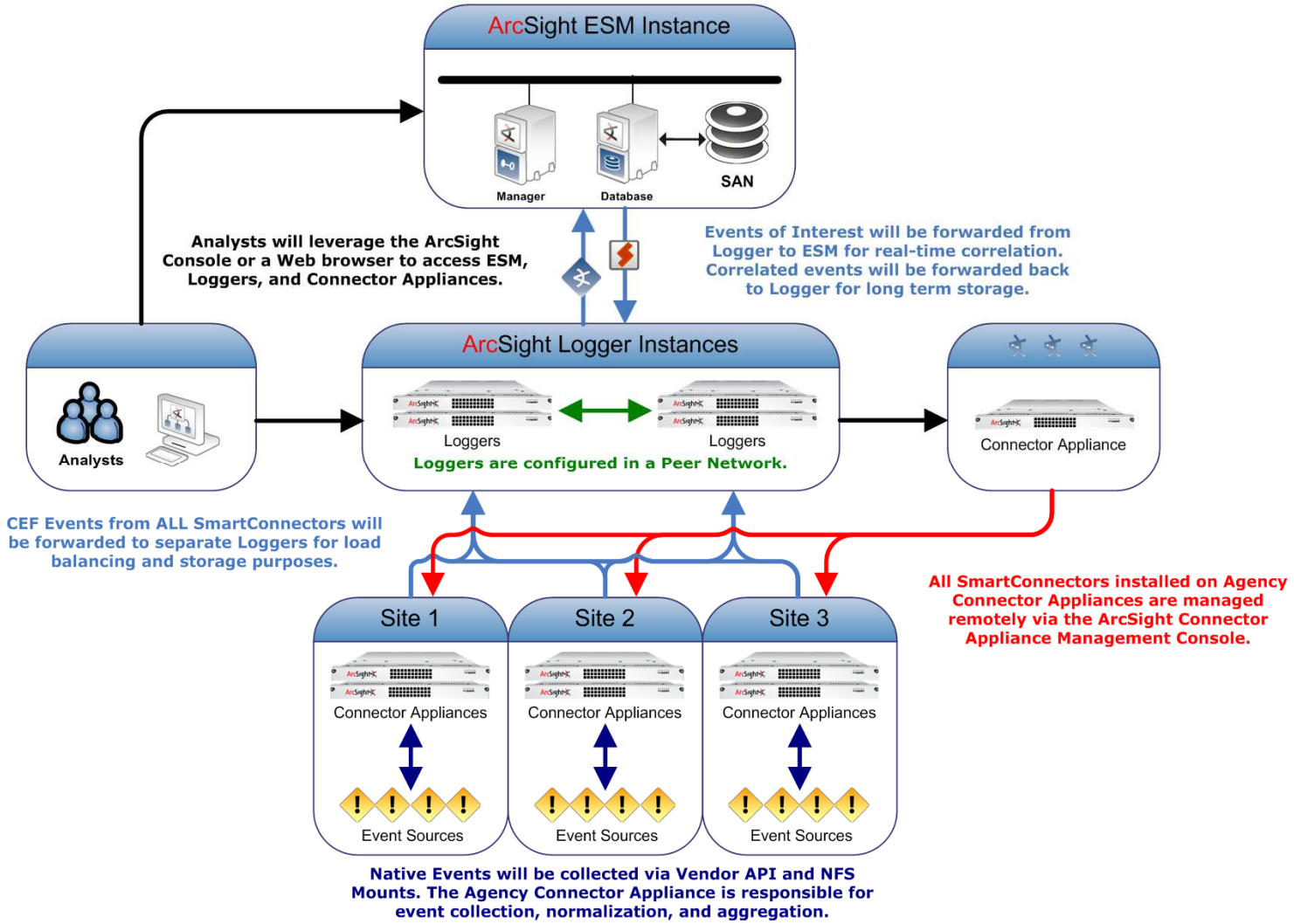
ДиалогНаука

Использование ESM и Logger



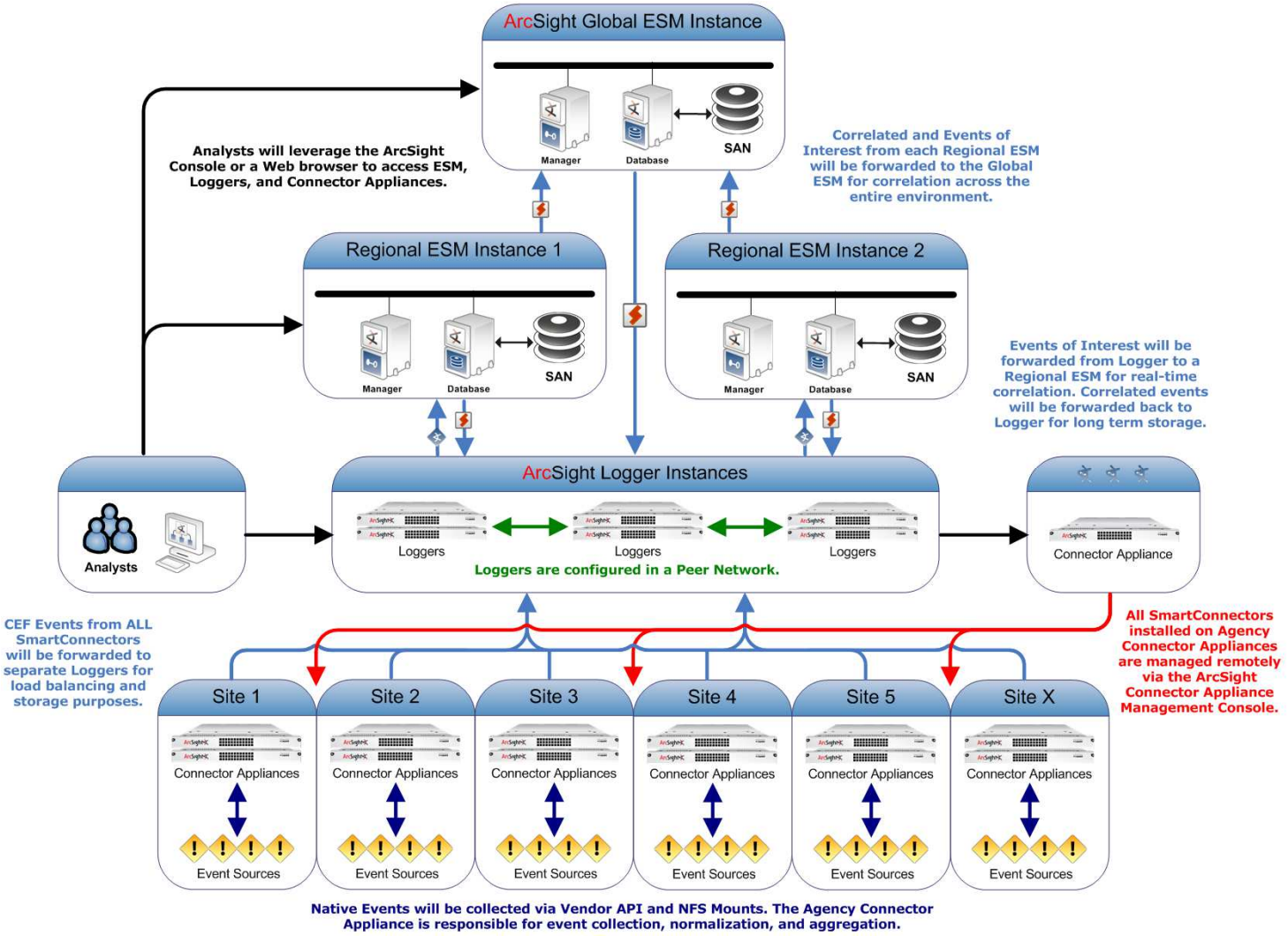
ДиалОгНаука

ESM & Logger: Фаза 1



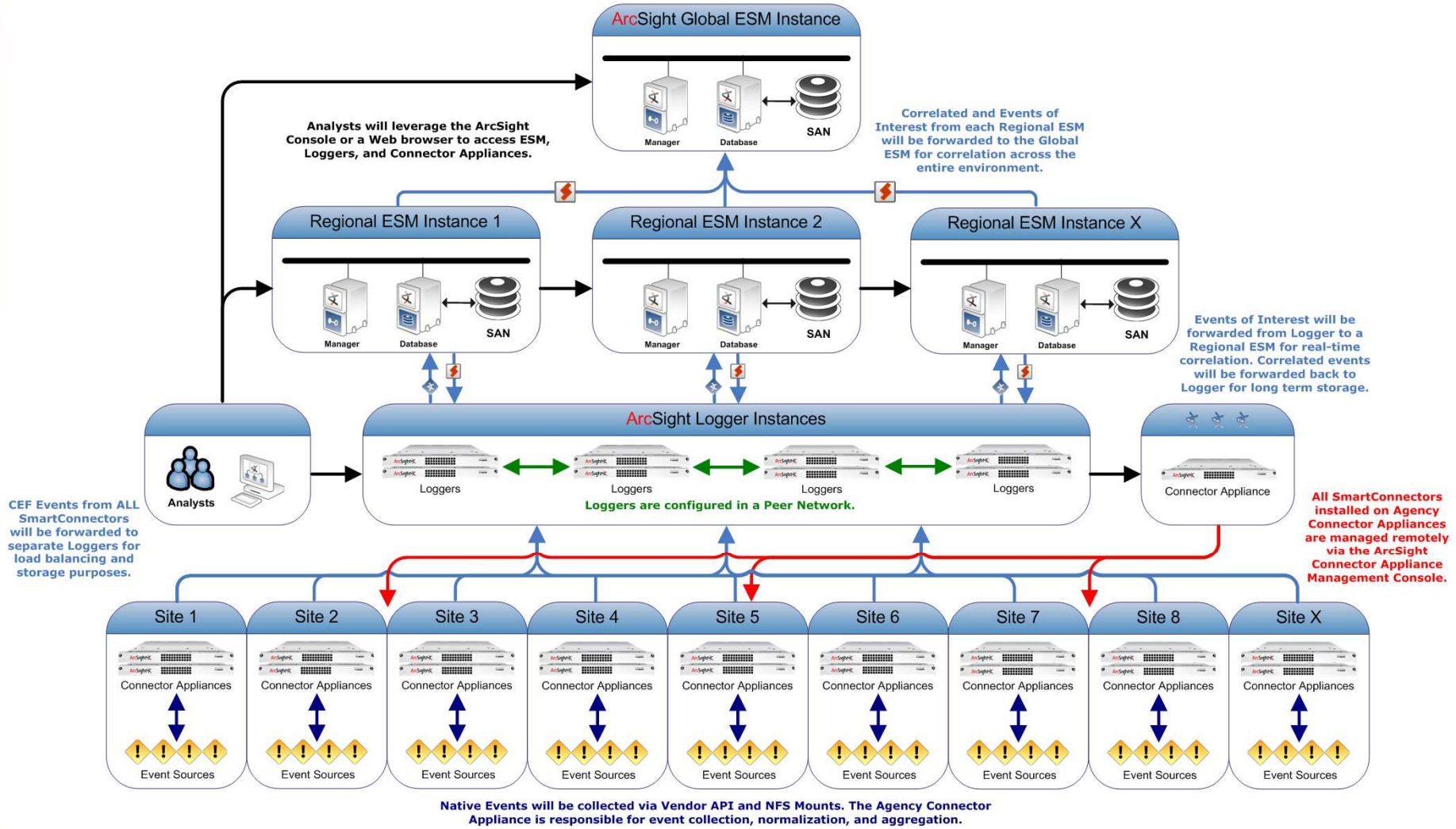
ДиалогНаука

ESM & Logger: Фаза 2



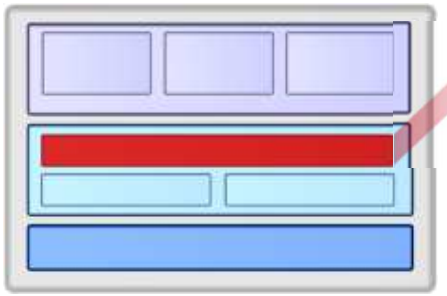
ДиалогНаука

ESM & Logger: Фаза 3



ДиалОгНаука

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:

Стоечное устройство для интеграции с ArcSight ESM

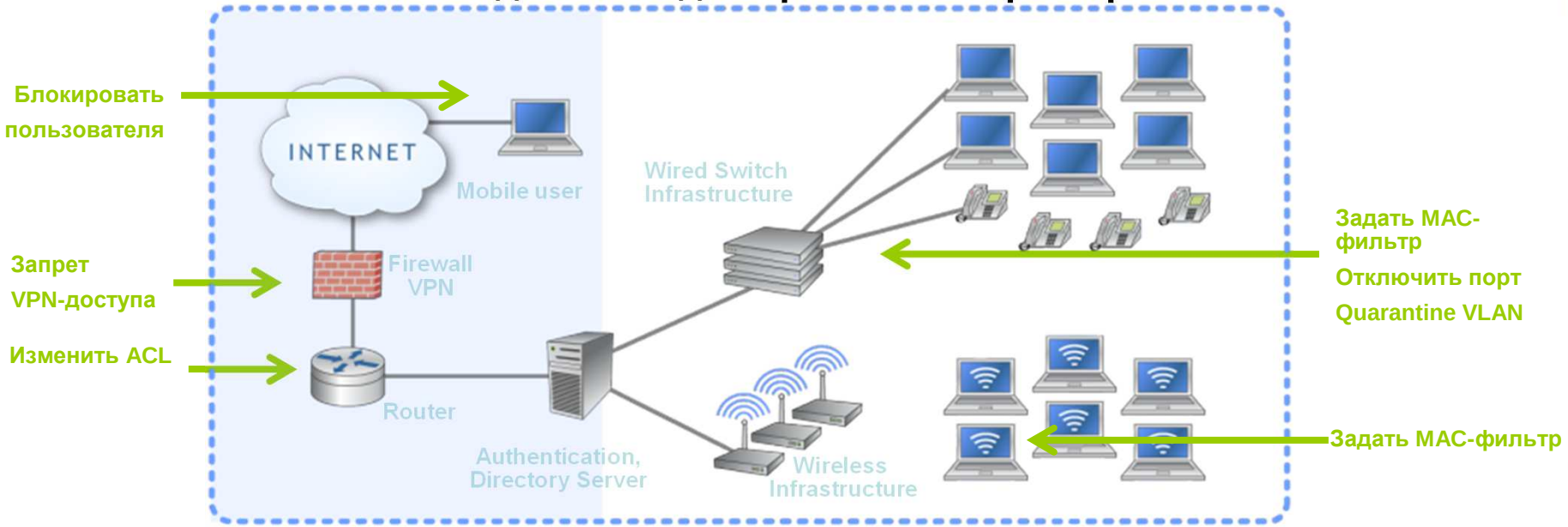
Гибкая, эффективная локализация проблем

ДиалОгНаука

Принцип работы ArcSight Threat Response Manager

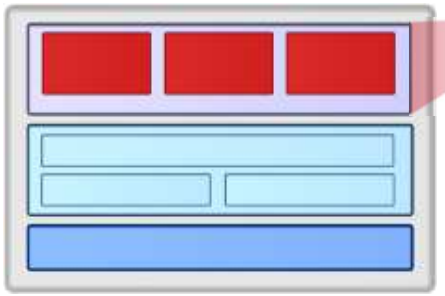
- **Локализация**
  - Определение адреса узла и получение списка коммутаторов/маршрутизаторов, с которыми связан данный узел
- **Анализ**
  - Поиск ближайшей к узлу «контрольной точки»
  - Поиск оптимального способа карантина узла
- **Реагирование**
  - Применение MAC-фильтра
  - Отключение порта
  -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

Несколько воздействий для правильного реагирования



ДиалОгНаука

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
PCI
IT Gov
FISMA

Бизнес:

IdentityView
Fraud Detection
Sensitive Data Protection

Предустановленного устройства

ДиалогНаука

Наличие сертификата соответствия ФСТЭК

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ НФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 2010

Выдан 12 января 2010 г.
Действителен до 12 января 2013 г.

Настоящий сертификат удостоверяет, что **программное обеспечение системы мониторинга и корреляции событий информационной безопасности ArcSight Enterprise Security Manager** (партия из 50 (пятидесяти) экземпляров продукции с серийными номерами с № 451-001 по № 451-050, маркированных знаками соответствия с № Г 082427 по № Г 082476), производства компании ArcSight Inc., является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует требованиям технических условий ТУ 5090-005-11680083-09.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов» (аттестат аккредитации от 13.05.2003 № СЗИ RU.1190.Б032.056) - техническое заключение от 30.11.2009, и экспертного заключения от 07.12.2009 органа по сертификации ЗАО «Лаборатория ППШ» (аттестат аккредитации от 29.09.2007 № СЗИ RU.054.А97.010).

Заявитель: ЗАО «ДиалогНаука»
Адрес: 107066, г. Москва, ул. Спартаковская, дом 13
Телефон: (495) 980-6776

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате технических условий осуществляется испытательной лабораторией ОАО «Безопасность информационных технологий и компонентов».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Гапонов

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 12 января 2010 г.

ДиалогНаука

ArcSight ESM:

- **Обзор данных в реальном режиме времени от всех систем**
- **Централизованное хранилище данных от всех систем**
- **Ранжирование угроз, основанное на серьезности ущерба, позволяющее аналитикам сфокусироваться на реальных угрозах и исключить ложные угрозы.**
- **Увеличивает эффективность ежедневной работы по безопасности уменьшая стоимость такой работы.**
- **Расширяет возможности по мониторингу больших систем**
- **Увеличивает эффективность работ по безопасности уменьшая стоимость владения.**
- **Позволяет осуществлять анализ инцидентов и «исторический» анализ произошедших событий.**

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