ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ СОВРЕМЕННЫХ SIEM-СИСТЕМ

Чехарин Родион
Руководитель проектов
АО «ДиалогНаука»

ДиалогНаука

О КОМПАНИИ «ДИАЛОГНАУКА»

Создана в 1992 году СП «Диалог» и ВЦ 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

Содержание

- Общие сведения о SIEM системах
- Основные требования к данным системам
- Функциональность HP ArcSight Logger \ ESM
- Модель пользователя \ модель ресурса \ сетевая модель
- Дополнительные модули
- Базовые примеры использования

Общие сведения о SIEM

- LMS "Система управления журналами" (Log Management System) – централизованная система сбора и хранения событий, предоставляющая единый интерфейс доступа к поученным и хранимым данным.
- SLM /SEM "Система управления событиями\журналами ИБ" (Security Log/Event Management) - по сути система управления журналами событий, но с минимальным анализом данных.
- SIM "Управление данными ИБ" - система управления активами, ориентированная на ИБ. Содержит сведения об уязвимостях хостов, результаты антивирусных сканирований и т.д.
- SEC "Корреляция событий ИБ" (Security Event Correlation) - Система для поиска и выявления шаблонов повторяющихся действий в журналах событий ИБ.
- SIEM "Система управления информационной безопасностью " (Security Information and Event Management) - Система, включающая в себя возможности всех перечисленных систем, предназначенная для централизованного управления событиями и данными ИБ.

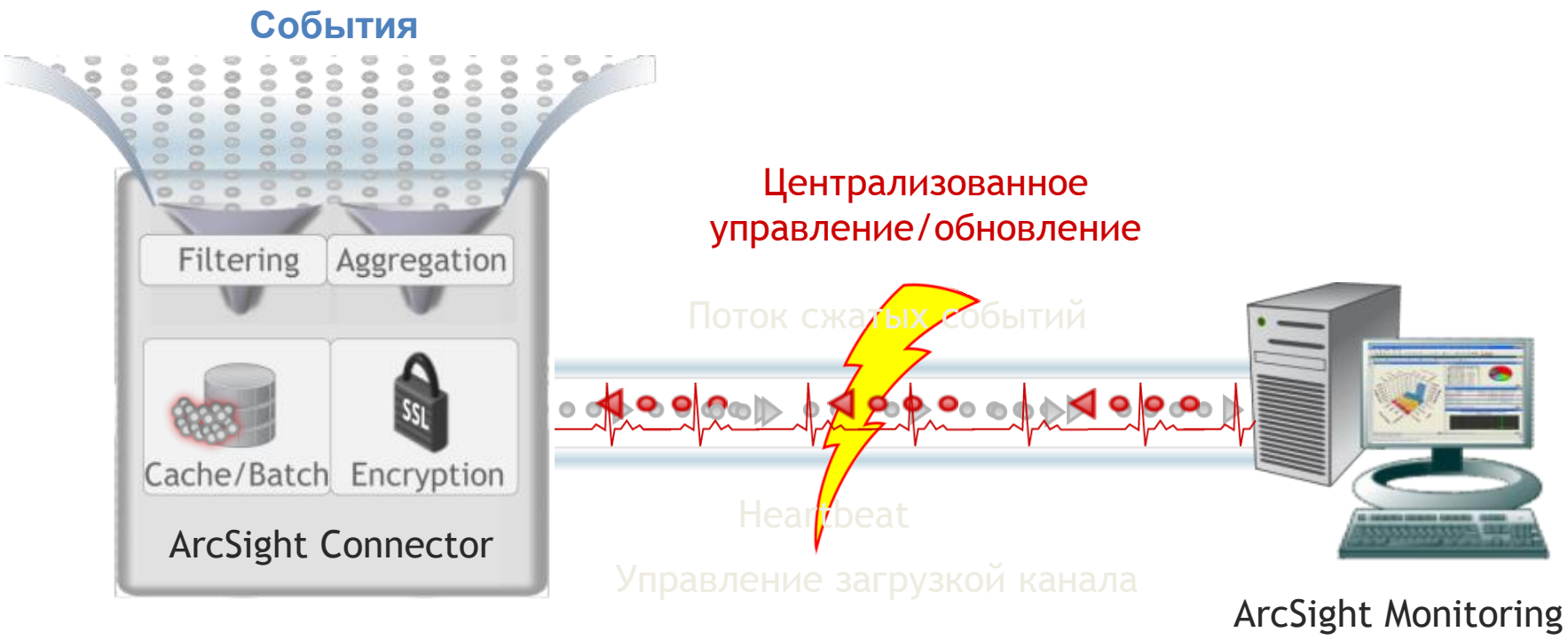
Основные требования к SIEM системам

1. Сбор событий и получение сведений и контексте событий
2. Нормализация полученных данных
3. Корреляция
4. Приоритезация
5. Оповещения
6. Отчетность и визуализация
7. Документооборот

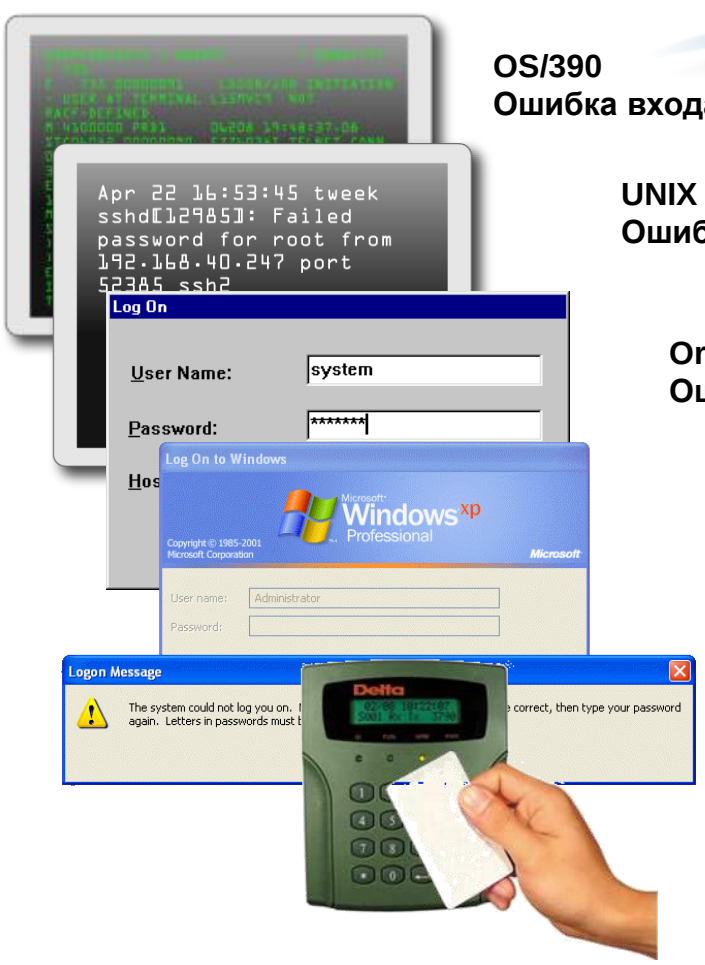
ФУНКЦИОНАЛЬНОСТЬ HP ARCSIGHT

ДиалогНаука

Сбор событий



Нормализация



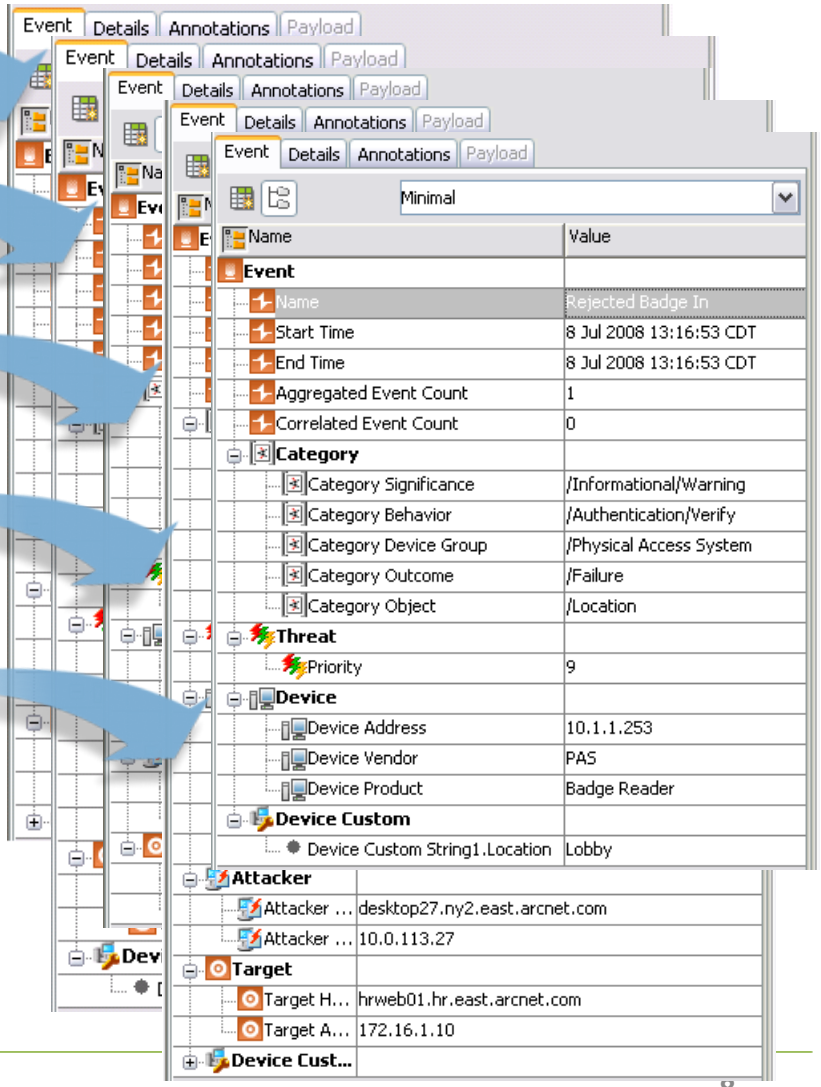
OS/390
Ошибка входа

UNIX
Ошибка входа

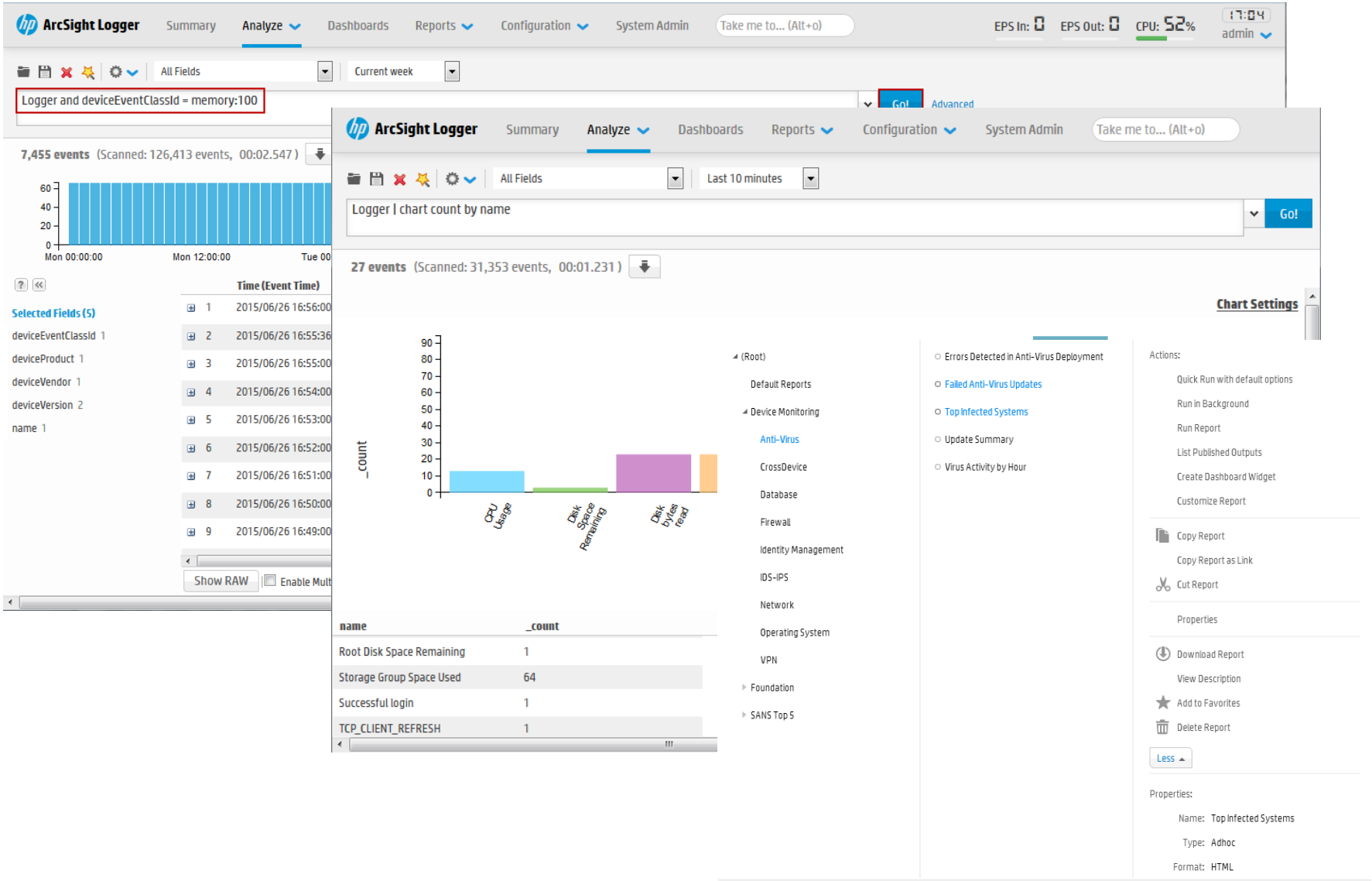
Oracle
Ошибка входа

Windows
Ошибка входа

HID-карты
Вход запрещён



Хранение и поиск:ArcSight Logger



Модель пользователя\ модель ресурса \ сетевая модель

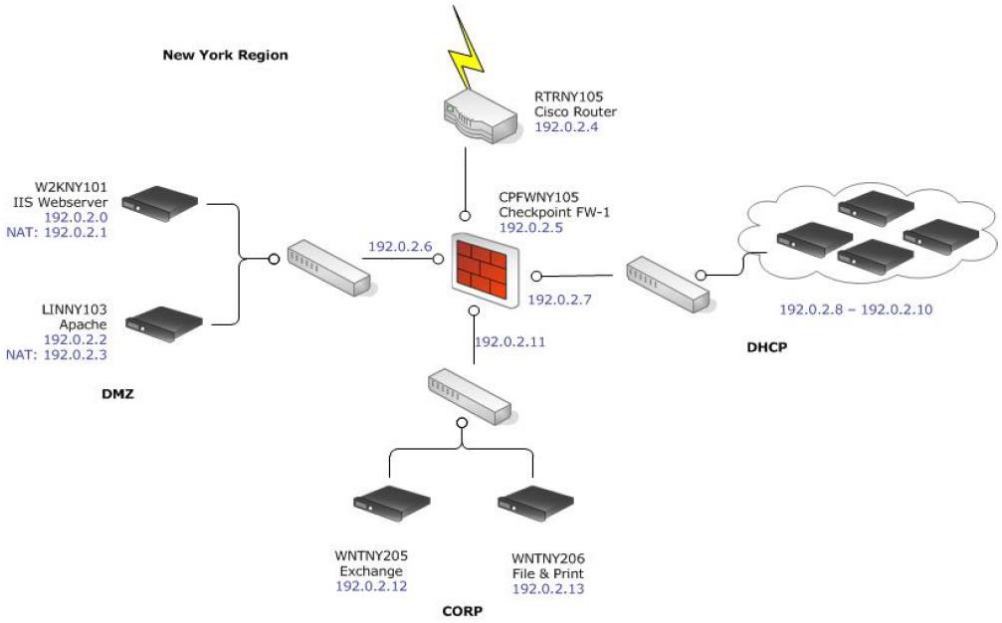
Сетевая модель

Подсеть
Подсеть пользователей или серверный сегмент?

Политики
Каково влияние активности в данной сети на бизнес?

Расположение
Физическое расположение объекта

Атрибуты
Защищаемая сеть
Внешняя сеть
«Тёмная» сеть



Модель пользователя\ модель ресурса \ сетевая модель

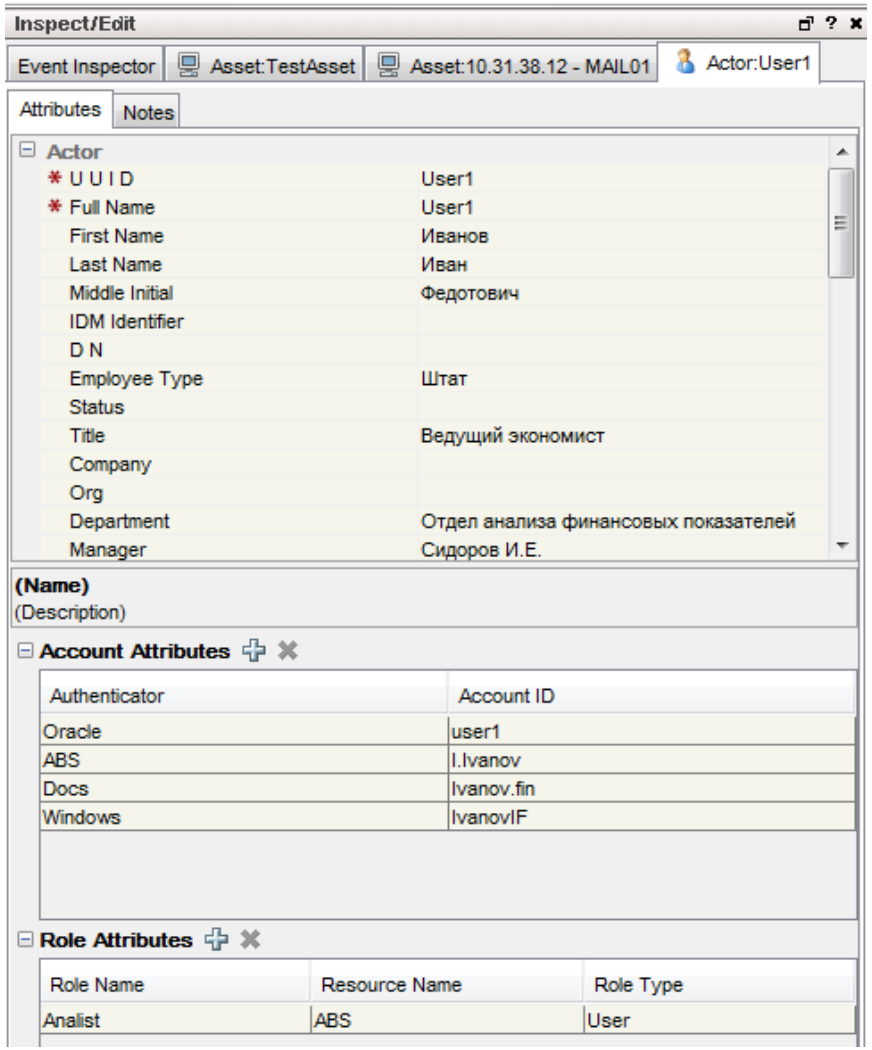
Модель пользователя

Сопоставление
Кто стоит за данным логином?

Политики
Каково влияние события на бизнес?

Роль
Соответствует ли активность роли сотрудника?

Профиль пользователя
С чем обычно работает данный пользователь?



Модель пользователя\ модель ресурса \ сетевая модель

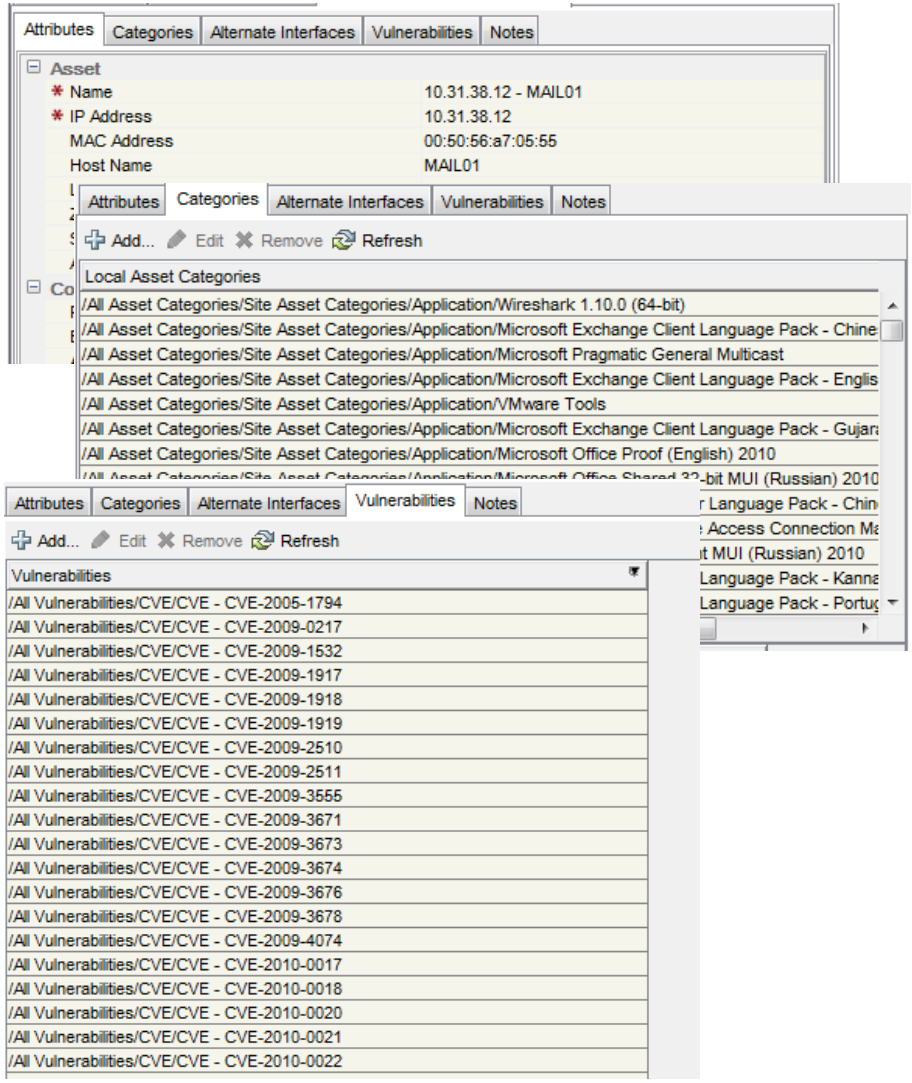
Модель ресурса

Важность ресурса

Репозиторий ресурсов

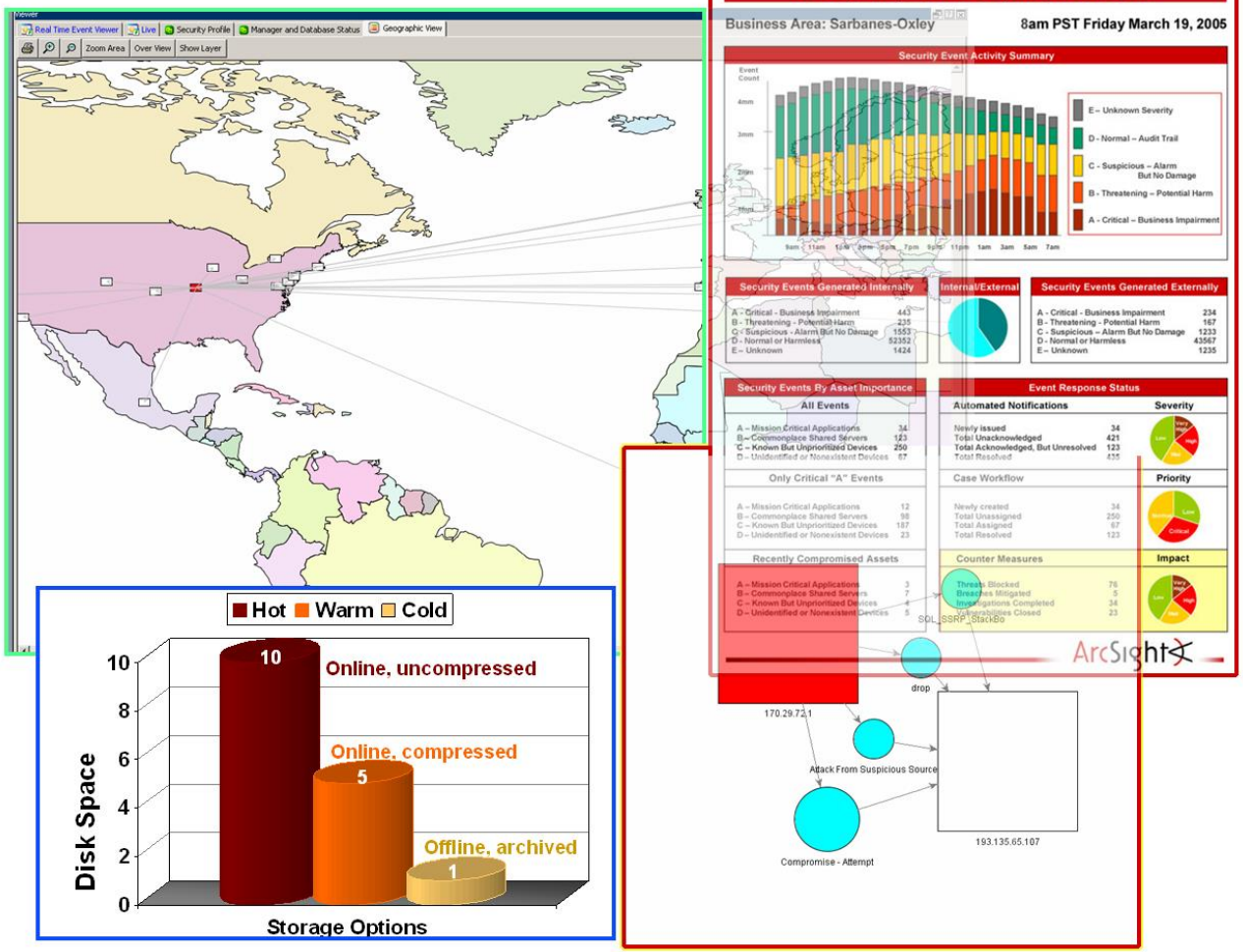
Уязвимости
Подверженность ресурса атакам

Критичность ресурса
Насколько критичен данный ресурс для бизнеса?

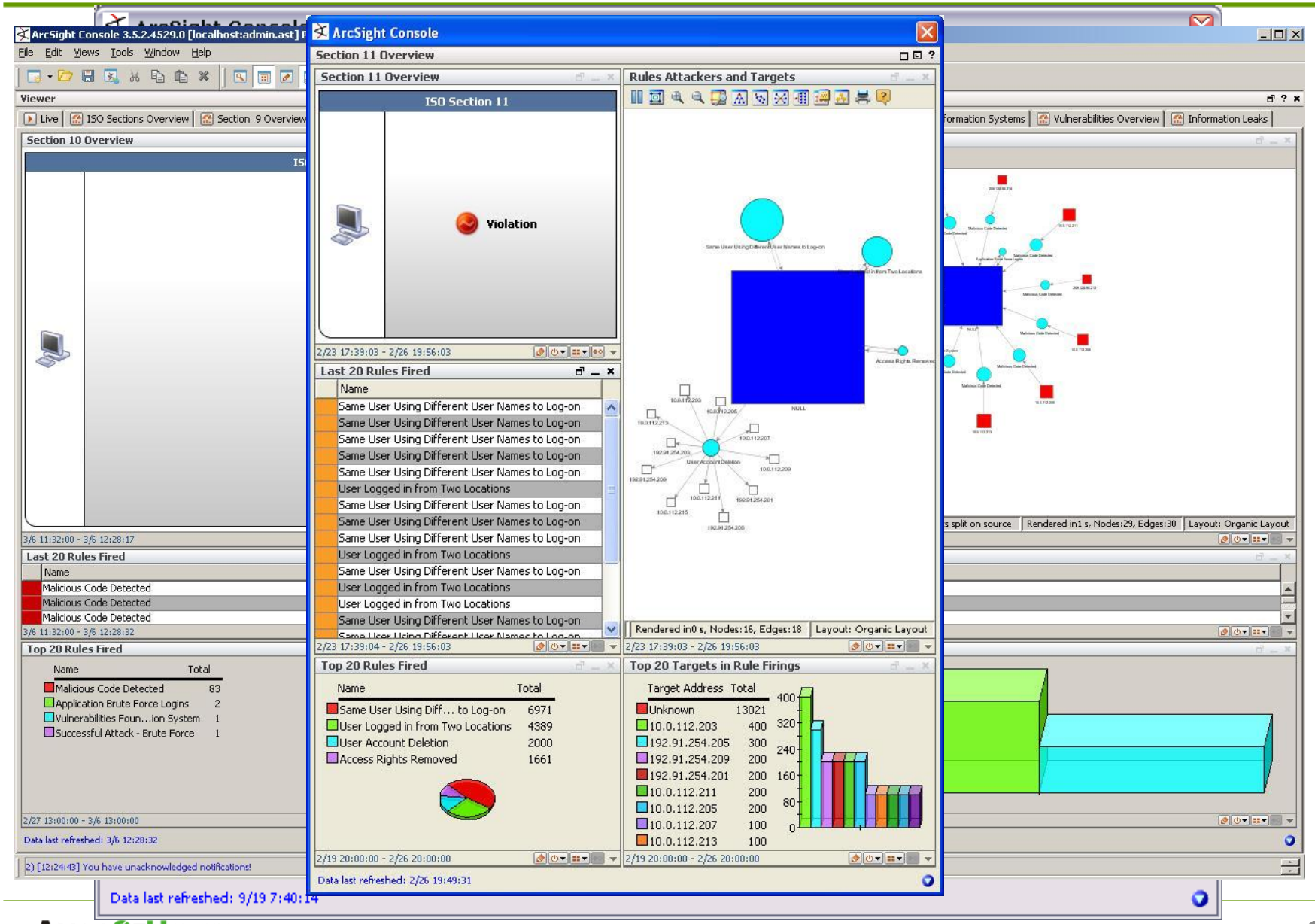


Визуализация

- 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

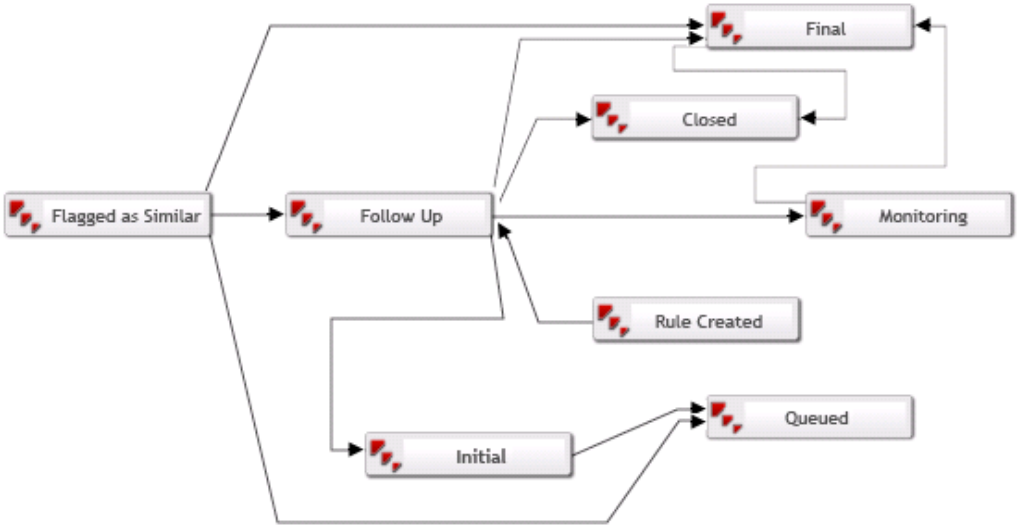


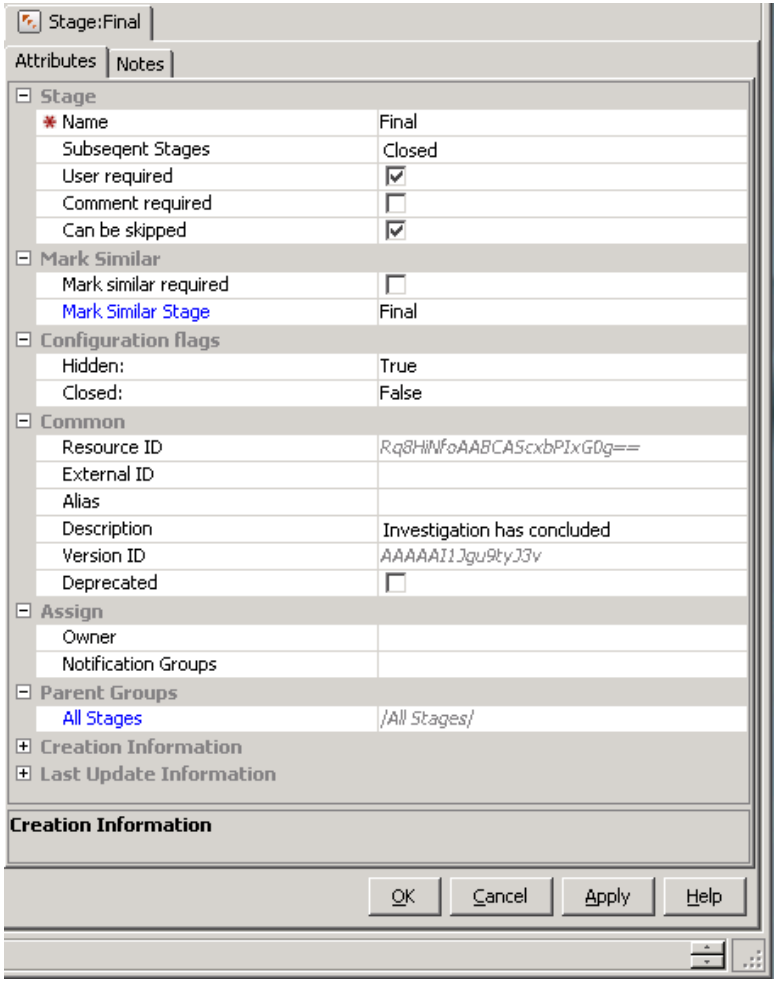
Визуализация



Документооборот

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





Дополнительные модули

- Соответствие стандартам
  - PCI DSS
  - HIPAA…
- Автоматизация и интеграция
  - Threat Detector
  - User Behavior Analytics
  - System Monitoring
  - Reputation Security Monitor
  - Domain Name System Malware Analytics

БАЗОВЫЕ ПРИМЕРЫ ИСПОЛЬЗОВАНИЯ

ДиалогНаука

О возможностях корреляции событий ИБ

Пример 1:

- Будем считать, что некоторая СМ имеет возможность определять географическое расположение объекта по его IP-адресу

- Рассмотрим далее такую ситуацию:

  СМ 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 СМ автоматически сигнализирует о возможной компрометации логина и пароля, при помощи которого был выполнен удаленный доступ

О возможностях корреляции событий ИБ

Пример 2:

- Для операторов связи, предоставляющих доступ в Интернет по логину и паролю, СМ 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:

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

Пример 4:

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

О возможностях корреляции событий ИБ

Пример 5:

- СМ 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:

- СМ 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 СМ может регистрировать факт доступа к информации с одного компьютера, но с разными логинами и паролями

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 СМ 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 СМ позволяет понизить уровень приоритета выявленного события

Вопросы?

Tel: +7 (495) 980-67-76 доб. 151
Web: www.DialogNauka.ru
E-mail: Rodion.Chekharin@DialogNauka.ru
117105, г. Москва, ул. Нагатинская, д.1