ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ СОВРЕМЕННЫХ SIEM-СИСТЕМ

Чехарин Родион
Руководитель проектов
АО «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 АО ДиалогНаука является системным интегратором в области информационной безопасности

Содержание

- Общие сведения о SEM\SIEM ArcSight
- Архитектура сбора событий ArcSight
- ArcSight Quick Flex - быстрое подключение нестандартных источников
- ArcSight Logger - настраиваемое хранение журналов, быстрый поиск, отчёты и оповещения
- ArcSight ESM - модель сети, модель пользователя, корреляция - правила, реагирование, динамические списки
- Взаимодействие Logger и ESM
- ArcSight Marketplace - «кубики» для SIEM

ОБЩИЕ СВЕДЕНИЯ О SIEM

Технологии

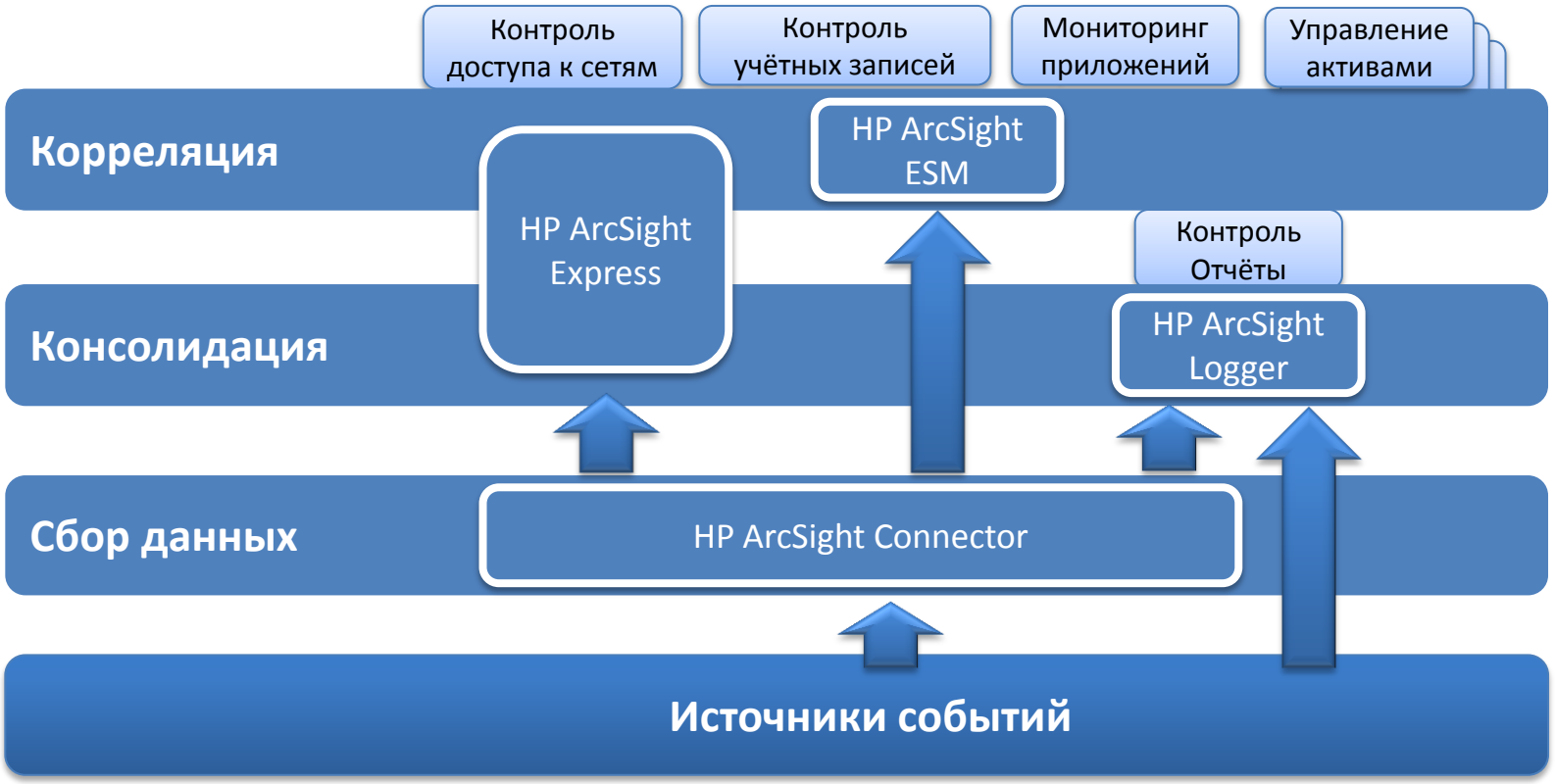
- LMS "Система управления журналами" (Log Management System) – централизованная система сбора и хранения событий, предоставляющая единый интерфейс доступа к поученным и хранимым данным.
- SLM /SEM "Система управления событиями\журналами ИБ" (Security Log/Event Management) - по сути система управления 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

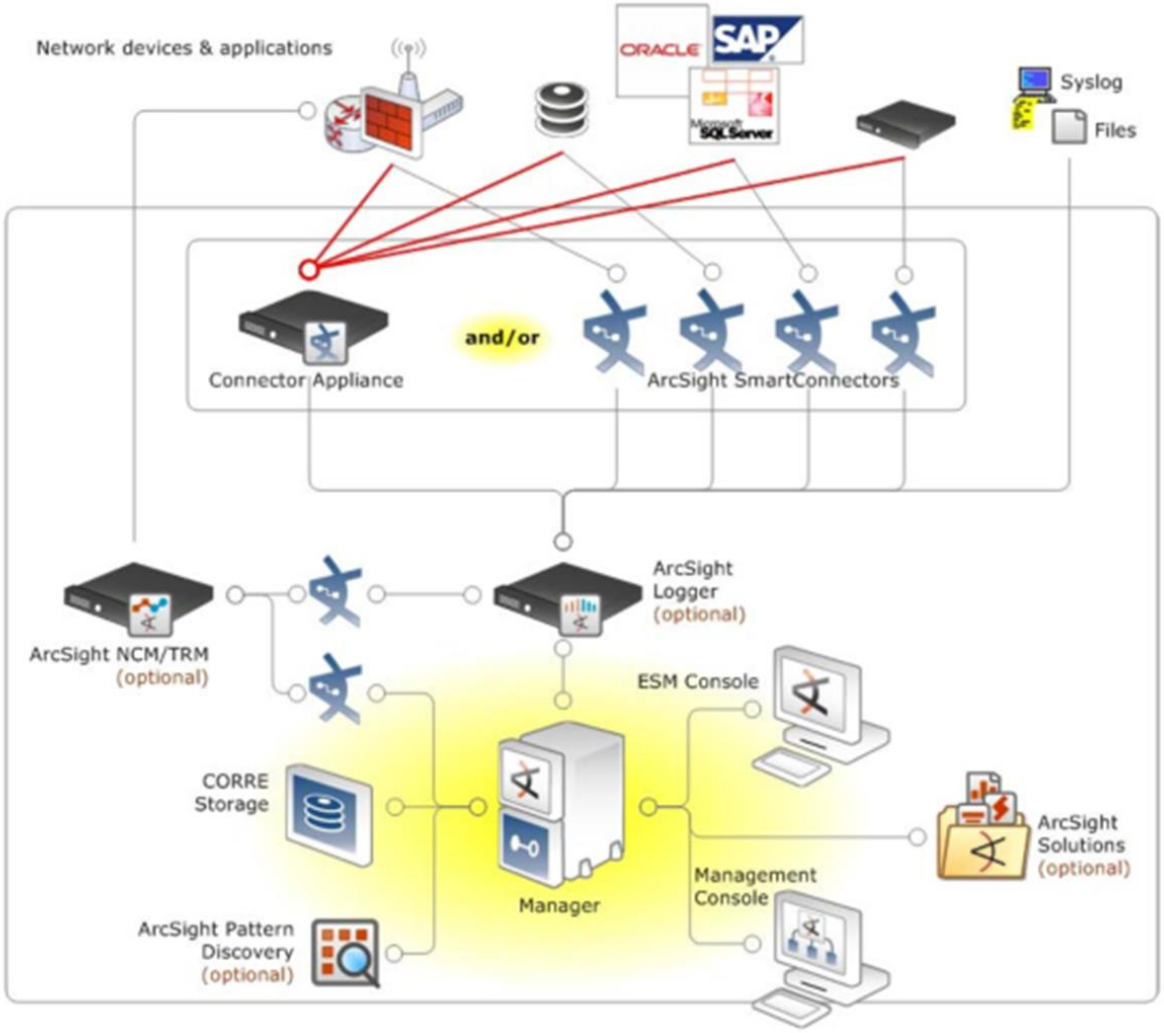
Требования

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

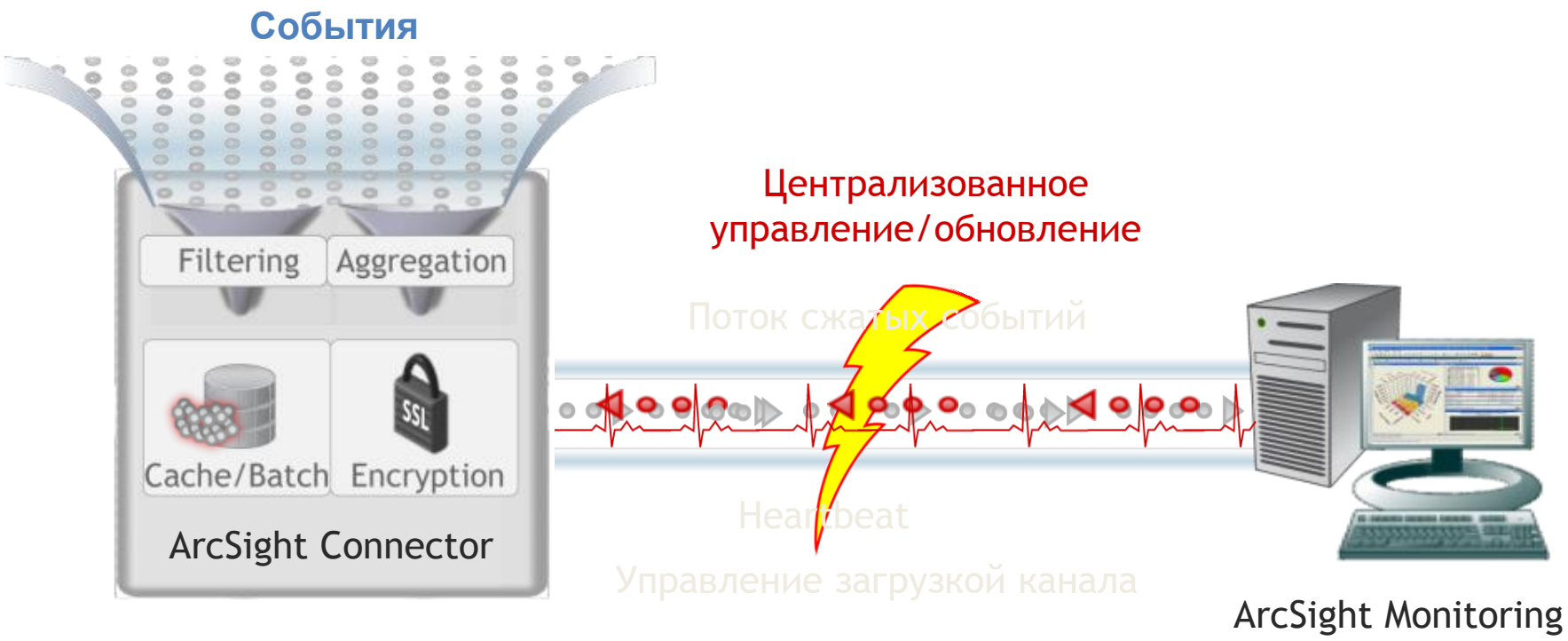
Семейство продуктов HP ArcSight



Потоки данных



Сбор событий



Нормализация

Оригинал…

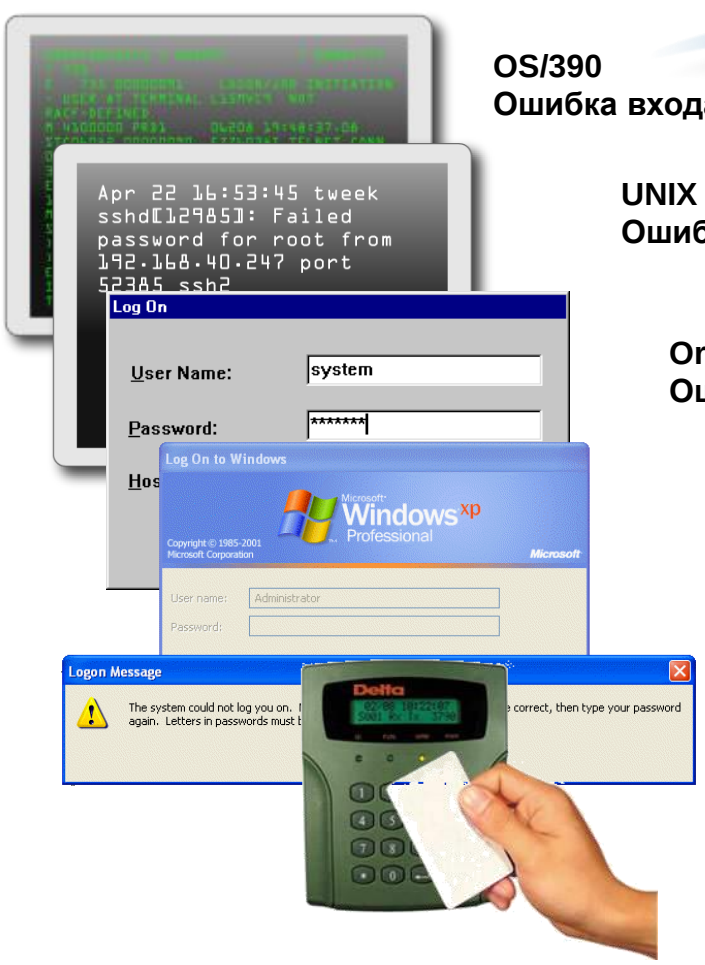
Mar 17 2017 12:16:03: %PIX-6-106015: Deny TCP (no connection) from 10.50.215.102/15605 to 204.110.227.16/443 flags FIN ACK on interface outside
Mar 17 2017 14:53:16 drop gw.foobar.com >eth0 product VPN-1 & Firewall-1 src xxx.xxx.146.12 s_port 2523 dst xxx.xxx.10.2 service ms-sql-m proto udp rule 49

Результат

Time (Event Time)	name	Device Vendor	deviceProduct	Category Behavior	Category DeviceGroup	Category Outcome	Category Significance
3/17/2017 12:16:03	Deny	Cisco	PIX	/Access	/Firewall	/Failure	/Informational/ Warning
3/17/2017 14:53:16	Drop	Checkpoint	Firewall-1/VPN-1	/Access/Start	/Firewall	/Failure	/Informational/ Warning

Выгода: Быстрый анализ и поиск независимо от производителя источника событий

Нормализация



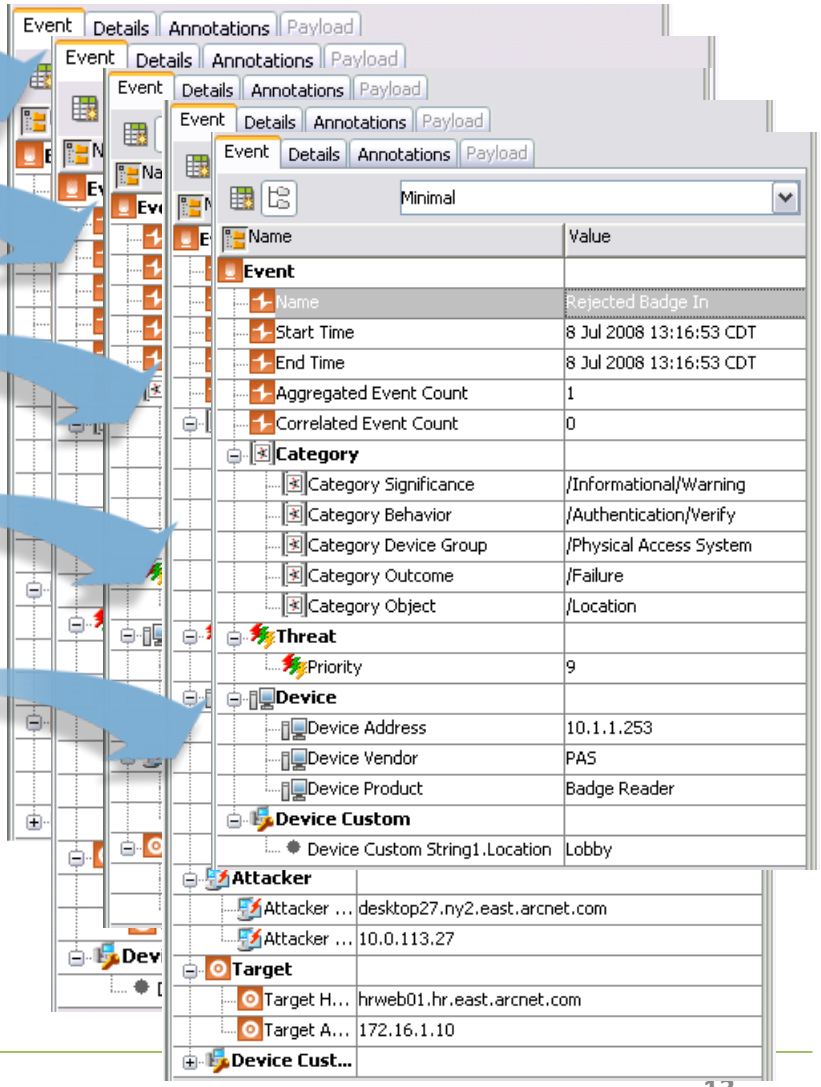
OS/390
Ошибка входа

UNIX
Ошибка входа

Oracle
Ошибка входа

Windows
Ошибка входа

HID-карты
Вход запрещён



QuickFlex - быстрое подключение текстовых источников

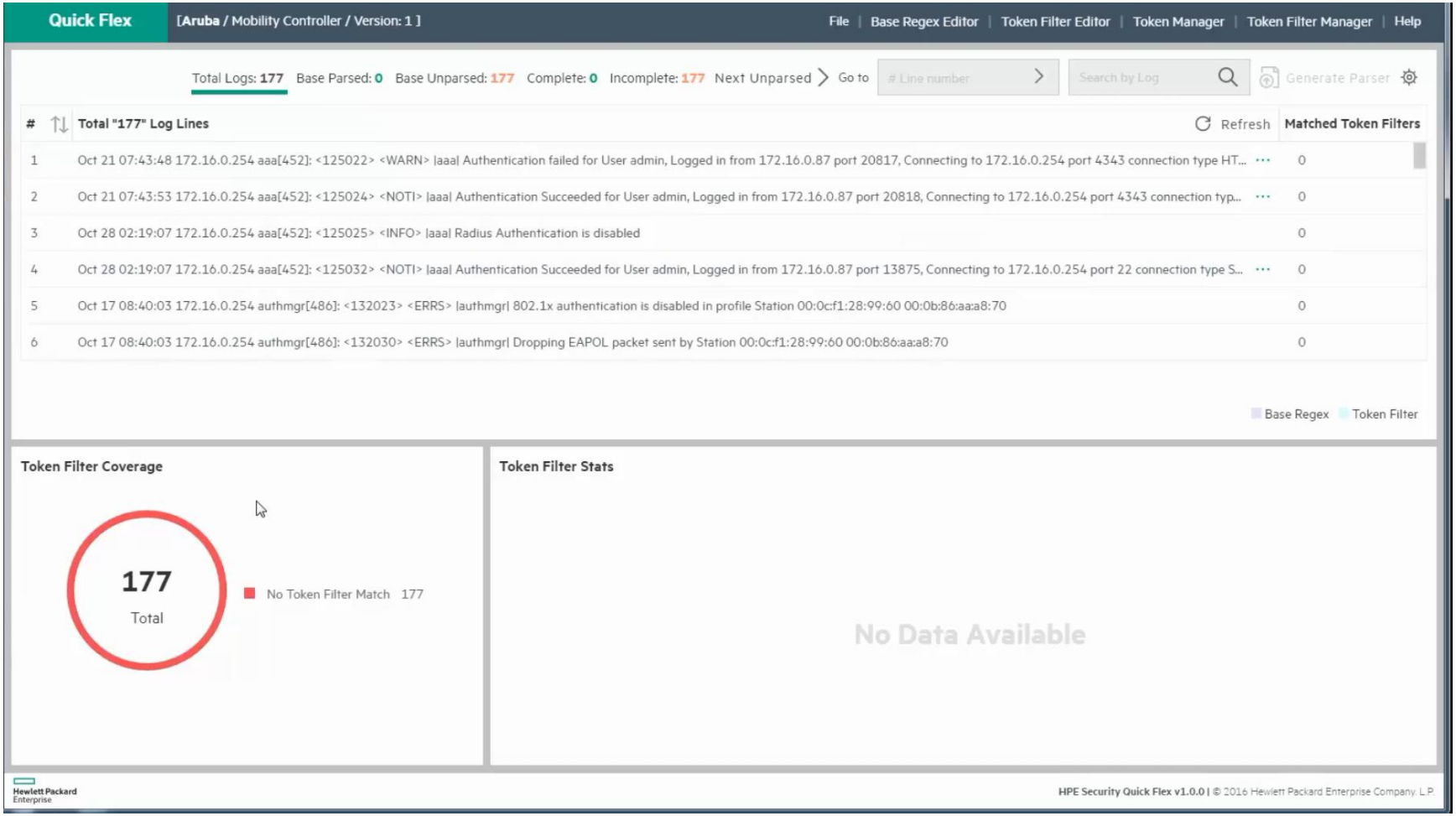
Новый способ создания парсеров для Flex-агентов с возможностями:

- Быстрая разработка
- Корректность
- Гибкость
- Упрощение обслуживания и сопровождения
- Снижения порогового уровня для начала работы

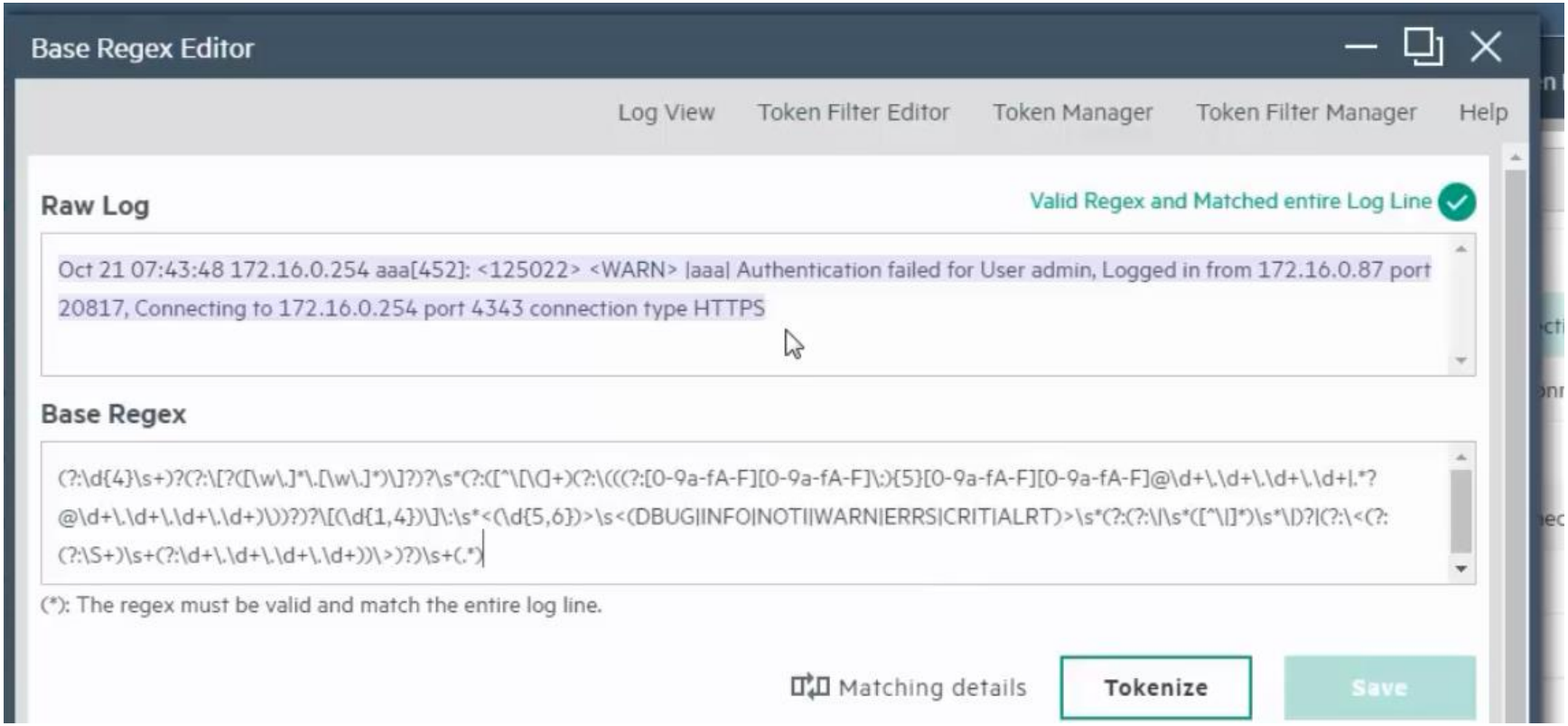
Quick Flex Parser Tool представляет следующие возможности для анализа файлов:

- Подсветка текста сообщений в окнах `Base Regex` и `Token Filter Manager` для оценки правильности разбора сообщения токенами
- Подсветка текста сообщений в окне `Log View` для отображения логики разбора сообщения токенами и фильтрами токенов
- Графическая статистика покрытия сообщений созданными токенами в окне `Log View`
- Тестирования работоспособности токенов и детальное описание выявленных ошибок

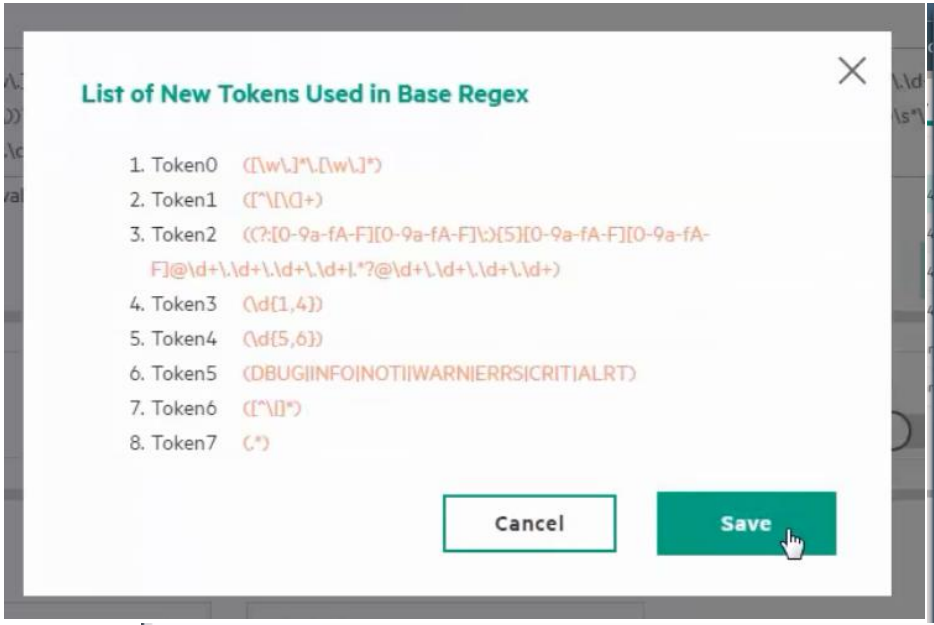
QuickFlex: начало работы

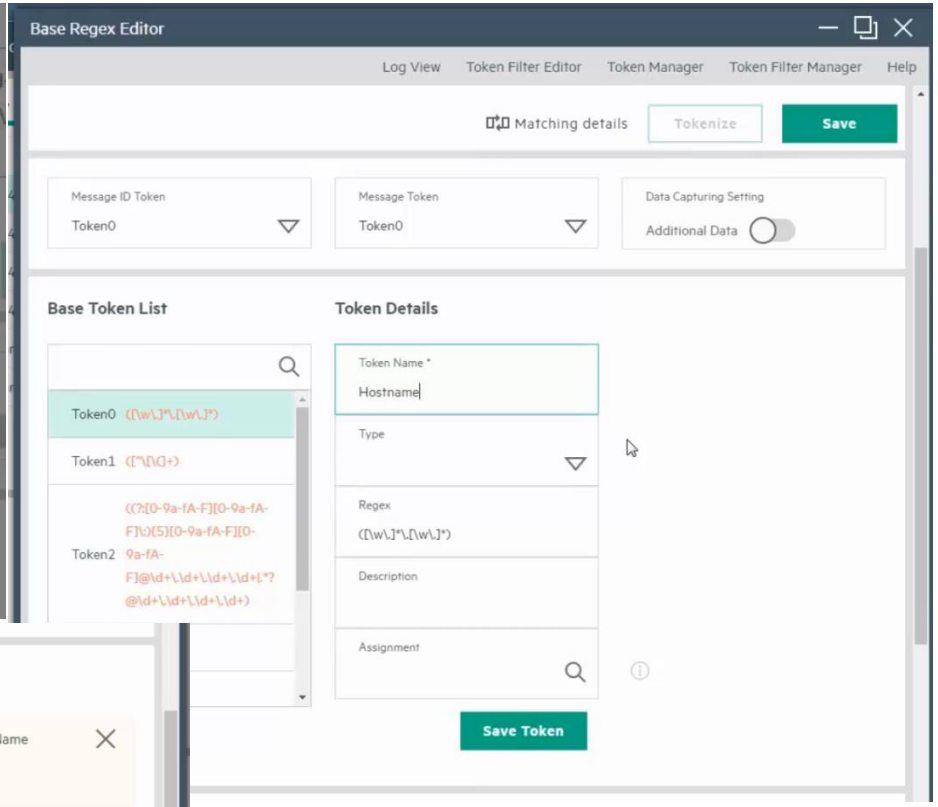


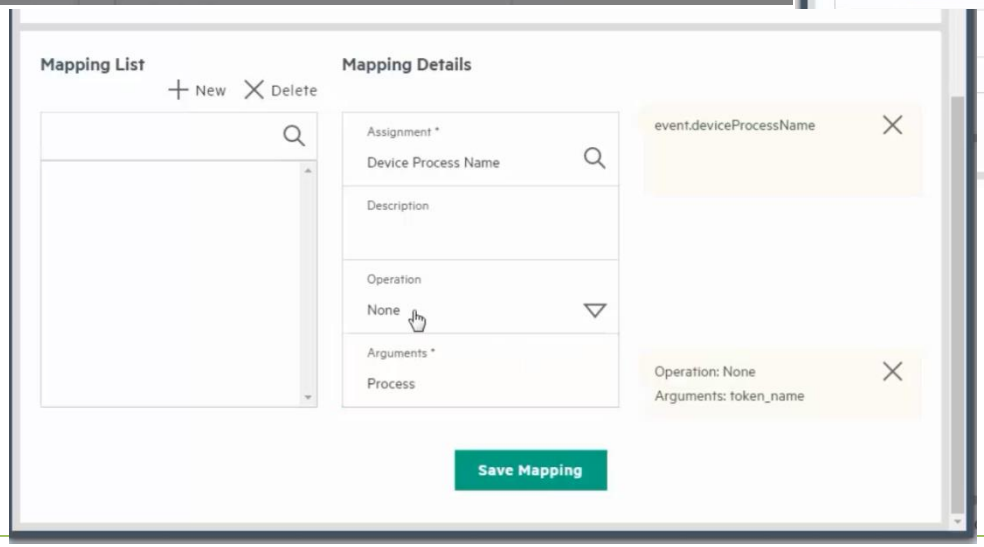
QuickFlex: основное регулярное выражение



QuickFlex: этапы работы







QuickFlex: результат

Flex-агент: дополнительные возможности

- Обработка событий, состоящих из нескольких разных строк:

```
Mon 2013-09-16 00:07:38: ----------
Mon 2013-09-16 00:10:11: SecurityPlus AntiVirus processing c:\mdaemon\queues\local\md50003493074.msg...
Mon 2013-09-16 00:10:11: * Message return-path: bushurovavn@baltech.ru
Mon 2013-09-16 00:10:11: * Message from: bushurovavn@baltech.ru
Mon 2013-09-16 00:10:11: * Message to: moskin.ao@comp.ru
Mon 2013-09-16 00:10:11: * Message subject: Компания "Балтех" Новый курс "Трибодиагностика. Основы смазывания машин и оборудования."
Mon 2013-09-16 00:10:11: * Message ID: <d041a922-1e42-11e3-fc8c-001e8c490aad@tgc1.ru>
Mon 2013-09-16 00:10:11: Start SecurityPlus AntiVirus results
Mon 2013-09-16 00:10:11: * Attachment t1.rar is infected by Troyan.Horse.d1
Mon 2013-09-16 00:10:11: * Total attachments scanned    : 6 (including multipart/alternatives and message body)
Mon 2013-09-16 00:10:11: * Total attachments infected   : 1
Mon 2013-09-16 00:10:11: * Total attachments disinfected: 1
Mon 2013-09-16 00:10:11: * Total errors while scanning  : 0
Mon 2013-09-16 00:10:11: * Total attachments removed    : 0
Mon 2013-09-16 00:10:11: End of SecurityPlus AntiVirus results
Mon 2013-09-16 00:10:11: ----------
```

- Получение данных об одном событии из разных строк журнала:

```
[18/Jul/2005:12:30:20 -0400] conn=8 op=0 msgId=82 - BIND uid=admin
[18/Jul/2005:12:30:25 -0400] conn=7 op=-1 msgId=-1 - LDAP connection from 10.0.20.122
to 10.0.20.122
[18/Jul/2005:12:30:30 -0400] conn=8 op=0 msgId=82 - RESULT err=0
```

Flex-агент: дополнительные возможности

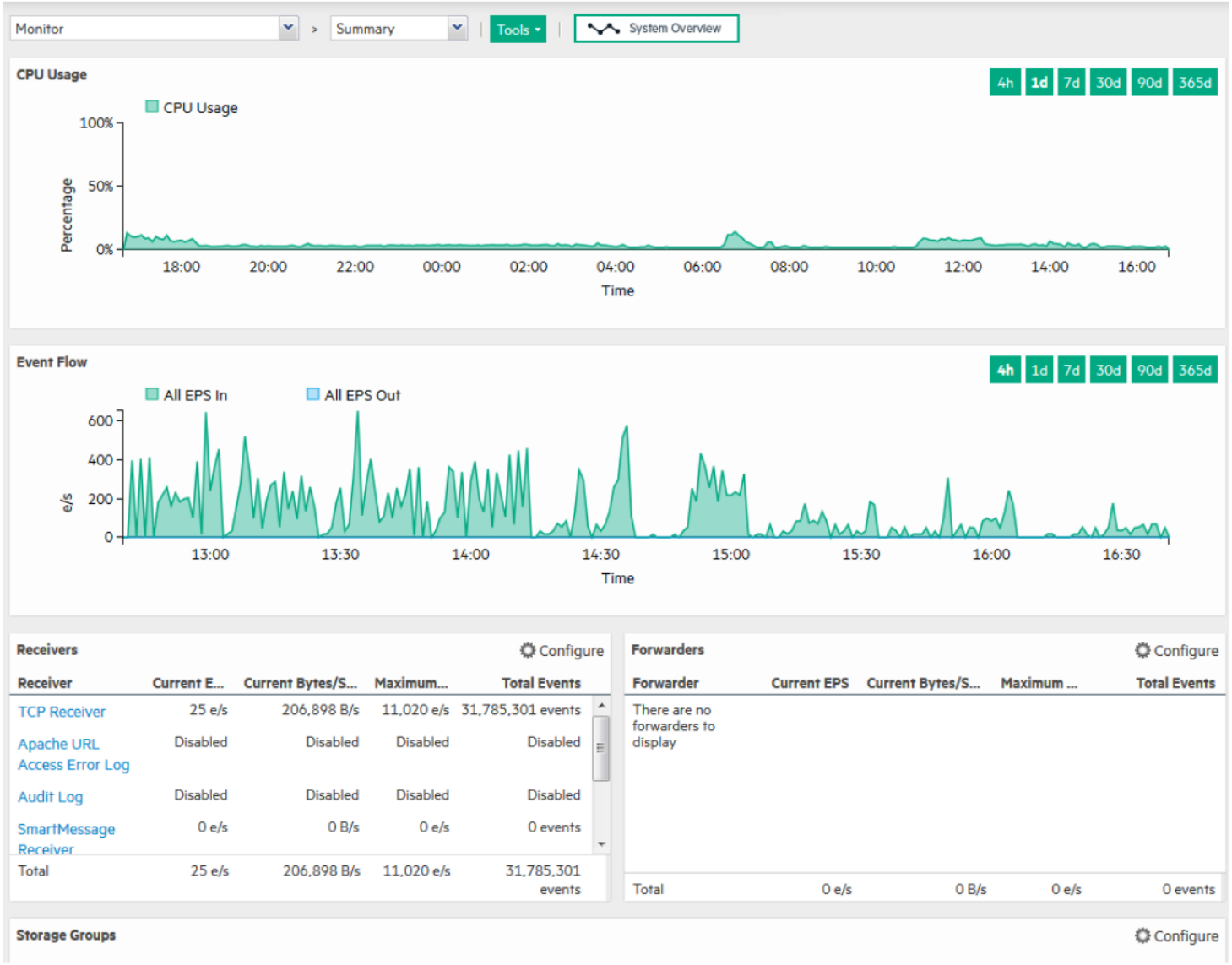
- Запрос данных из внешних источников:

```
type=sql
field.addrs.as.numbers=true
field.getter=oldFileHash
field.setter.count=2
field.setter[0]=targetUserPrivileges
field.setter[1]=oldFilePermission
jdbc.class=org.gjt.mm.mysql.Driver
jdbc.url=jdbc:mysql://localhost:3306/arcsight
jdbc.username=root
jdbc.password=OBFUSCATE.4.0.2:HT1WgEnTJ3sqLcb7jQ3PRA==
jdbc.query=select inn,name,nameshort from "ARCSIGHT"."egr" where inn in (?\u0000?)
```

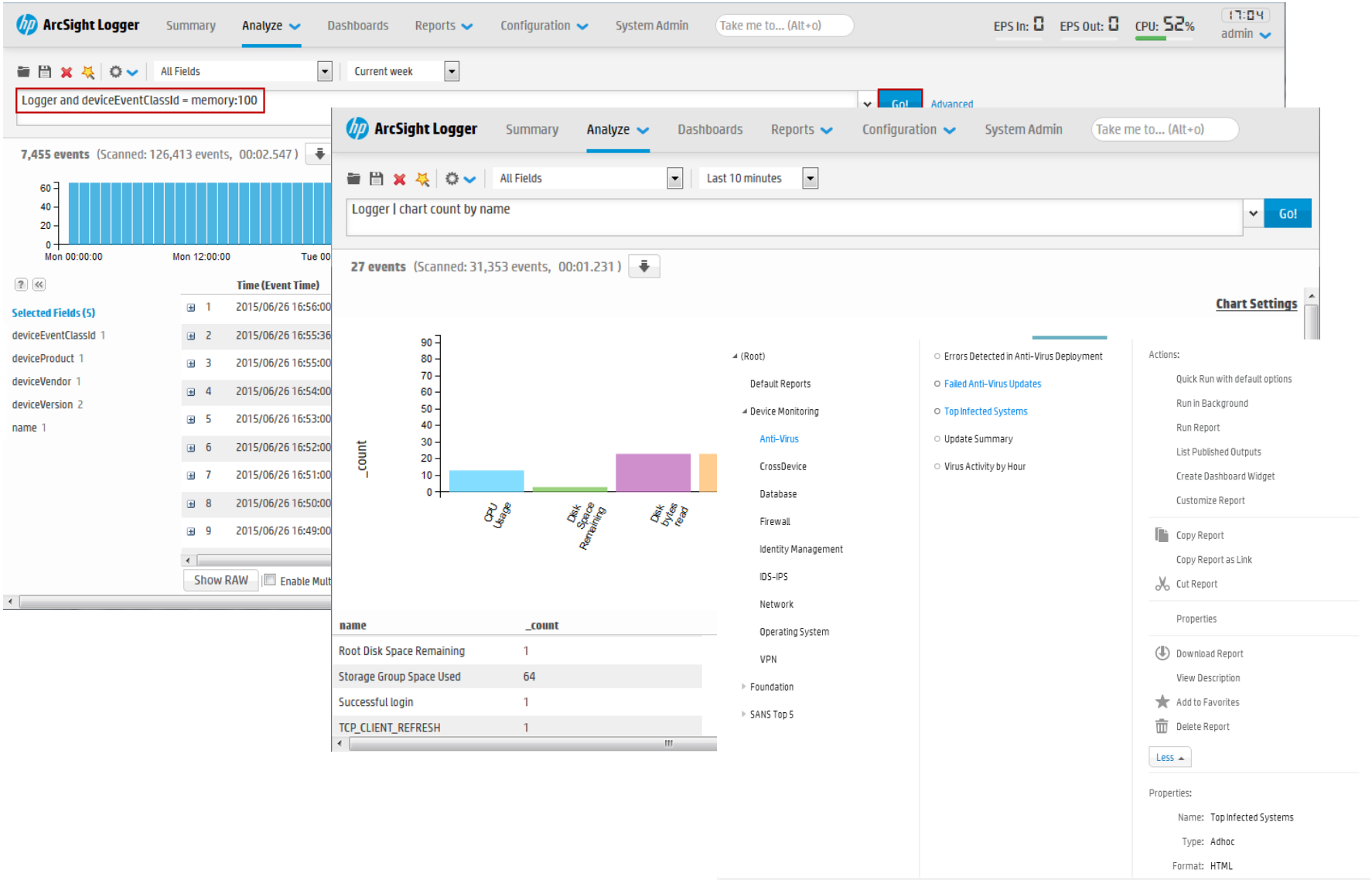
- Табличное соответствие:

```
event.externalId,event.deviceSeverity,set.event.deviceExternalId,set.event.message,set.event.priority,set.event.deviceFacility,
553,Audit_success,WN_03S_0553S,Обнаружена атака с повторением пакетов,6,Access,PCIDSS10
672,Audit_failure,WN_03S_0672F,Неудачная попытка выдачи билета проверки подлинности,4,Access,PCIDSS10
672,Audit_success,WN_03S_0672S,Выдан билет проверки подлинности,2,Access,PCIDSS10
673,Audit_failure,WN_03S_0673F,Неудачная попытка выдачи билета службы,4,Access,PCIDSS10
673,Audit_success,WN_03S_0673S,Удачная попытка выдачи билета службы,2,Access,PCIDSS10
674,Audit_success,WN_03S_0674S,Выданный билет обновлен,2,Access,PCIDSS10
675,Audit_failure,WN_03S_0675F,Ошибка предварительной проверки,4,Access,PCIDSS10
678,Audit_success,WN_03S_0678S,Учетная запись сопоставлена для входа в систему,2,Access,PCIDSS10
679,Audit_failure,WN_03S_0679F,УЗ не удалось сопоставить для входа в систему,4,Access,PCIDSS10
680,Audit_failure,WN_03S_0680F,Контроллер домена неудачно пытался проверить данные для входа в аккаунт ,4,Access,PCIDSS10
680,Audit_success,WN_03S_0680S,Контроллер домена удачно пытался проверить данные для входа в аккаунт,2,Access,PCIDSS10
682,Audit_success,WN_03S_0682S,Сеанс переподключен к станции,2,Access,PCIDSS10
683,Audit_success,WN_03S_0683S,Сеанс отключен от станции ,2,Access,PCIDSS10
640,Audit_success,WN_03S_0640S,Изменение общей базы данных УЗ ,2,Account,PCIDSS8
643,Audit_success,WN_03S_0643S,Изменение политики для домена,6,Privileges,PCIDSS7
```

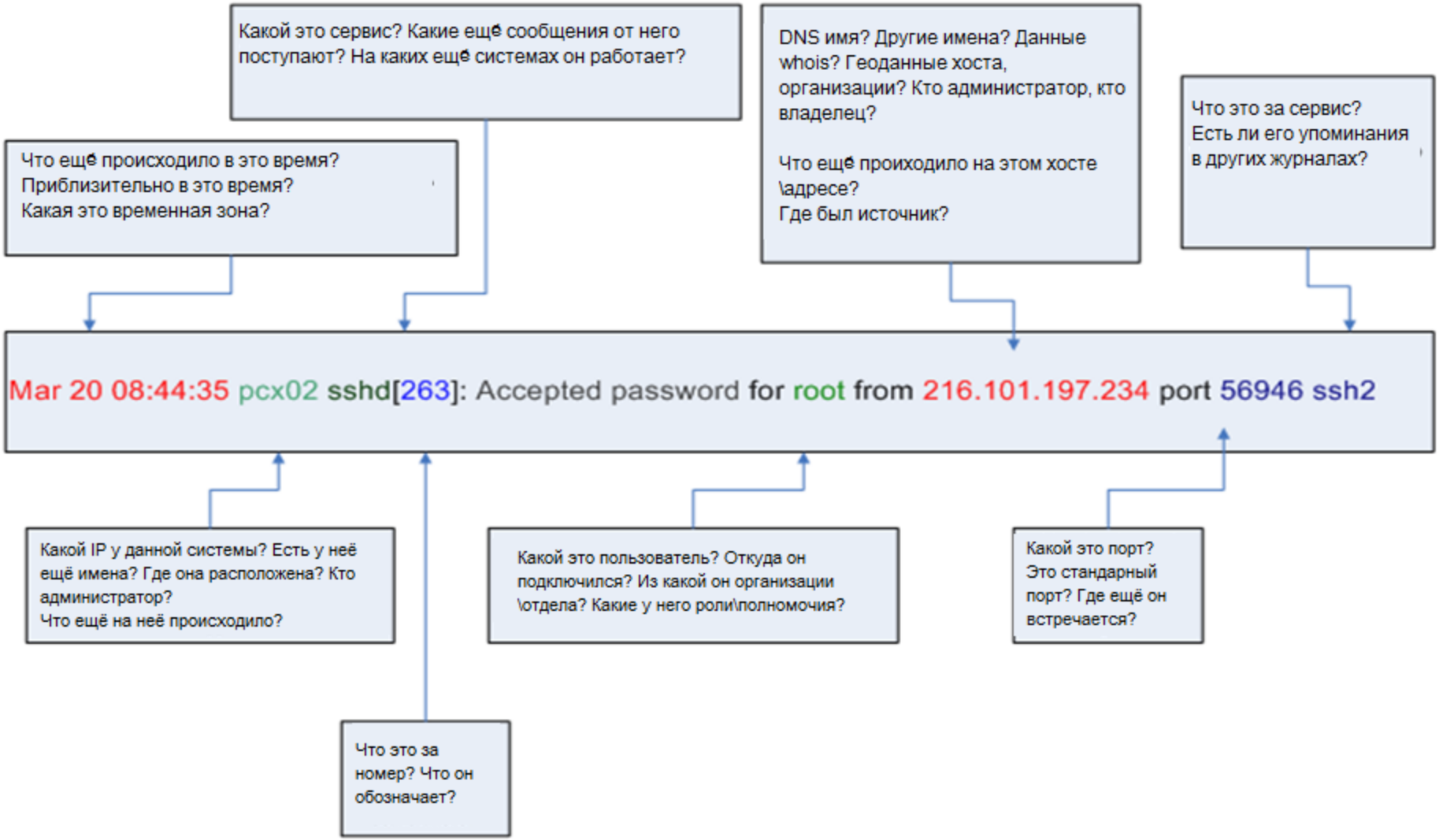
Хранение и поиск: ArcSight Logger



Хранение и поиск: ArcSight Logger



Вопросы, вопросы…



Модель пользователя\ модель ресурса \ сетевая модель

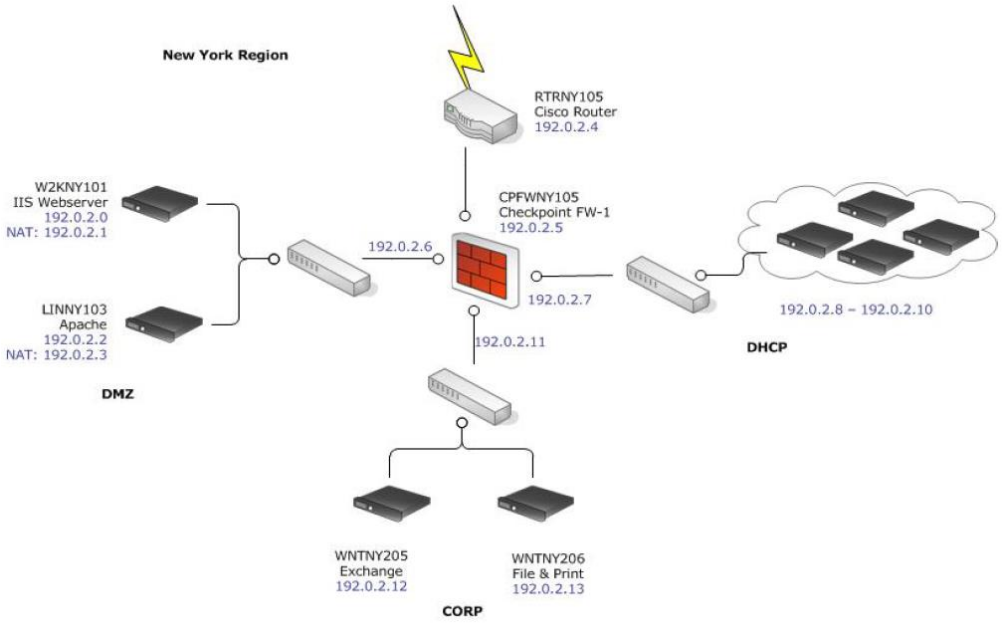
Сетевая модель

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

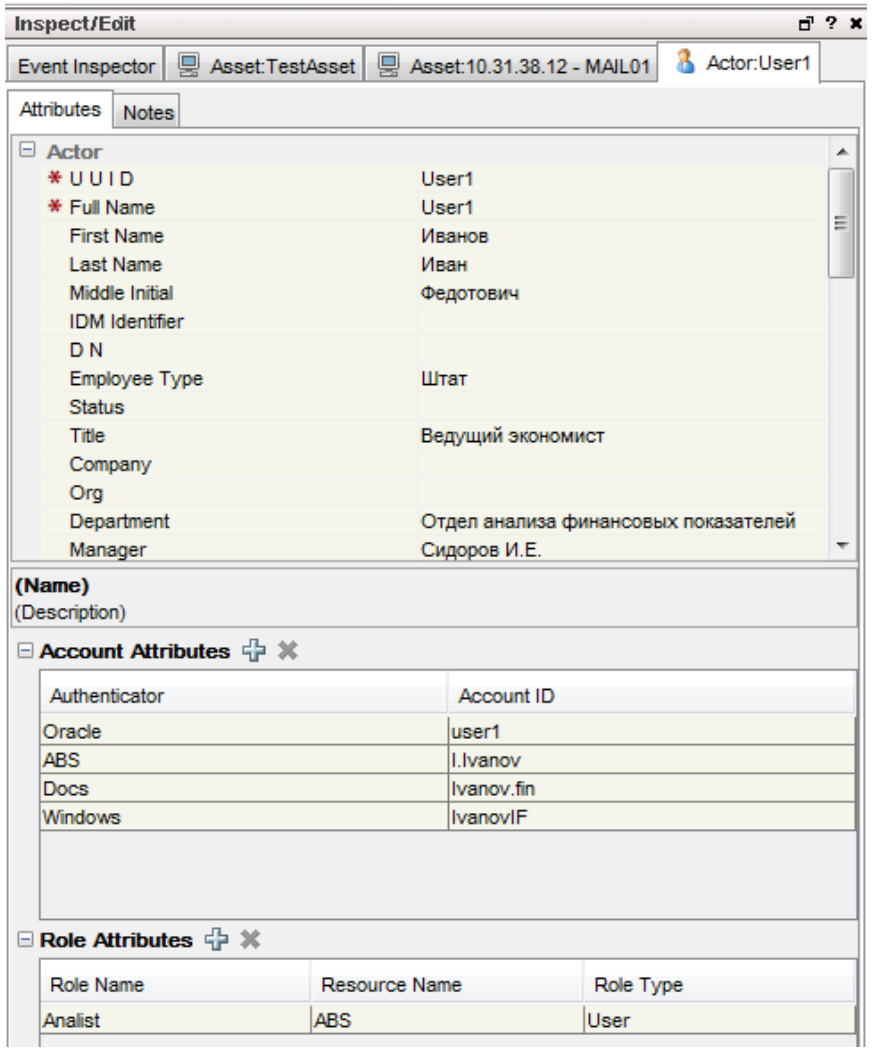
Модель пользователя

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

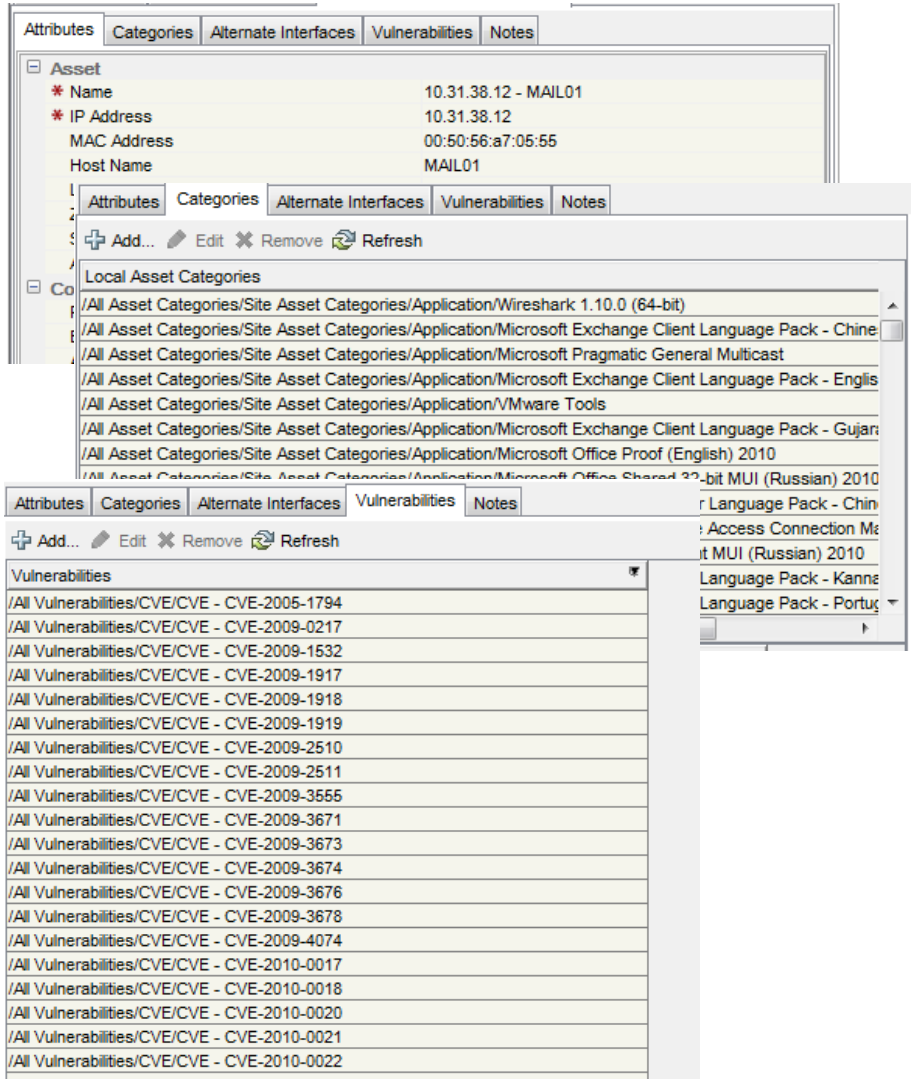
Модель ресурса

Важность ресурса

Репозиторий ресурсов

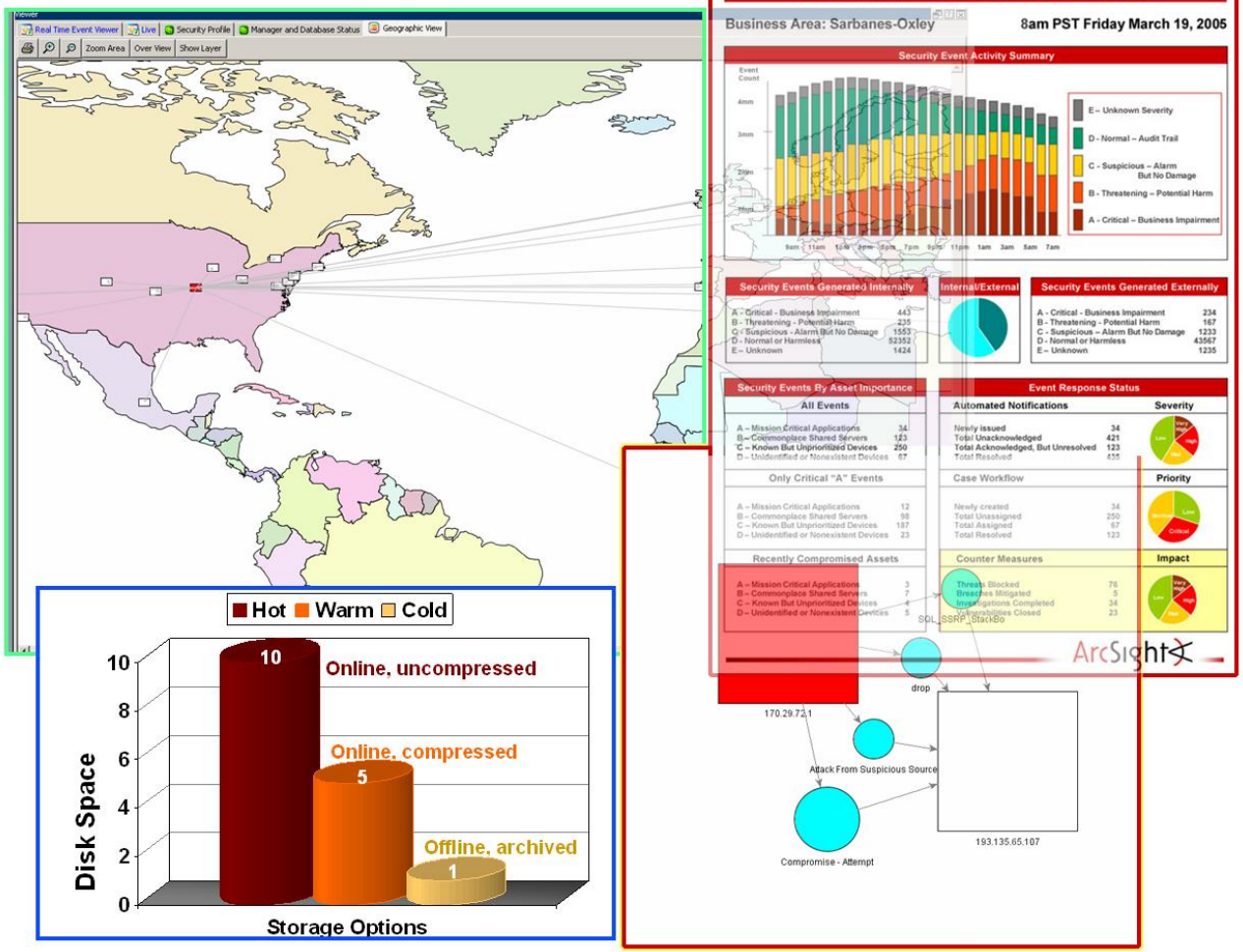
Уязвимости
Подверженность ресурса атакам

Критичность ресурса
Насколько критичен данный ресурс для бизнеса?

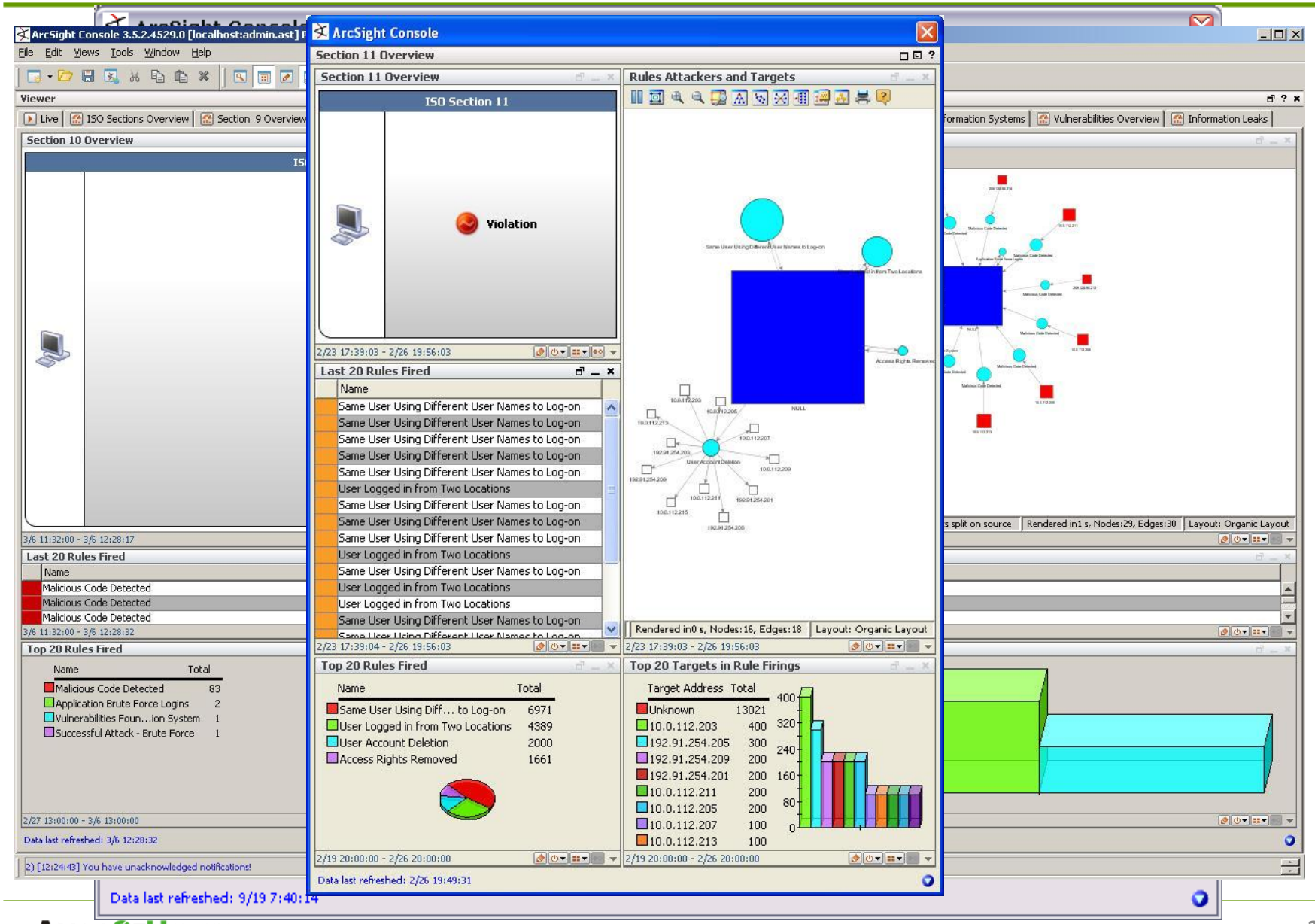


Визуализация

- 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

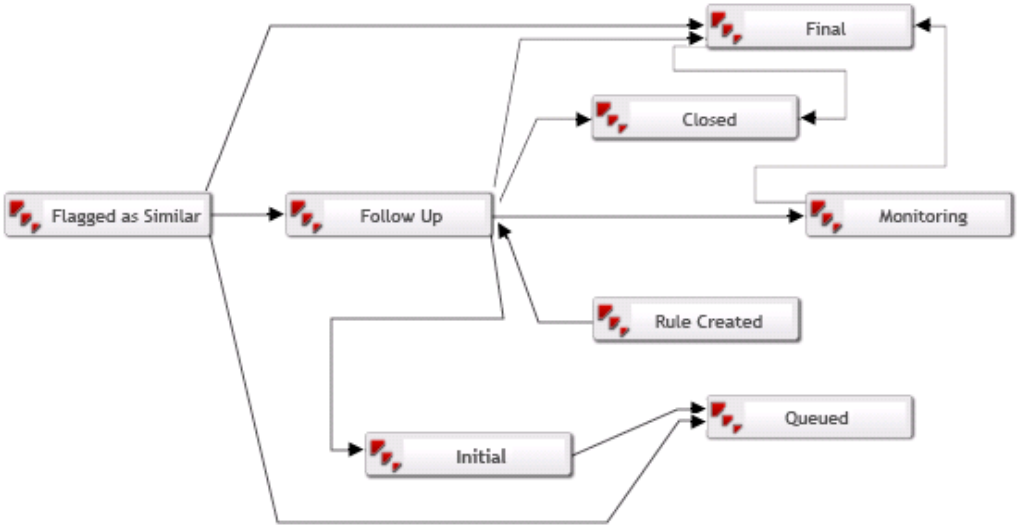


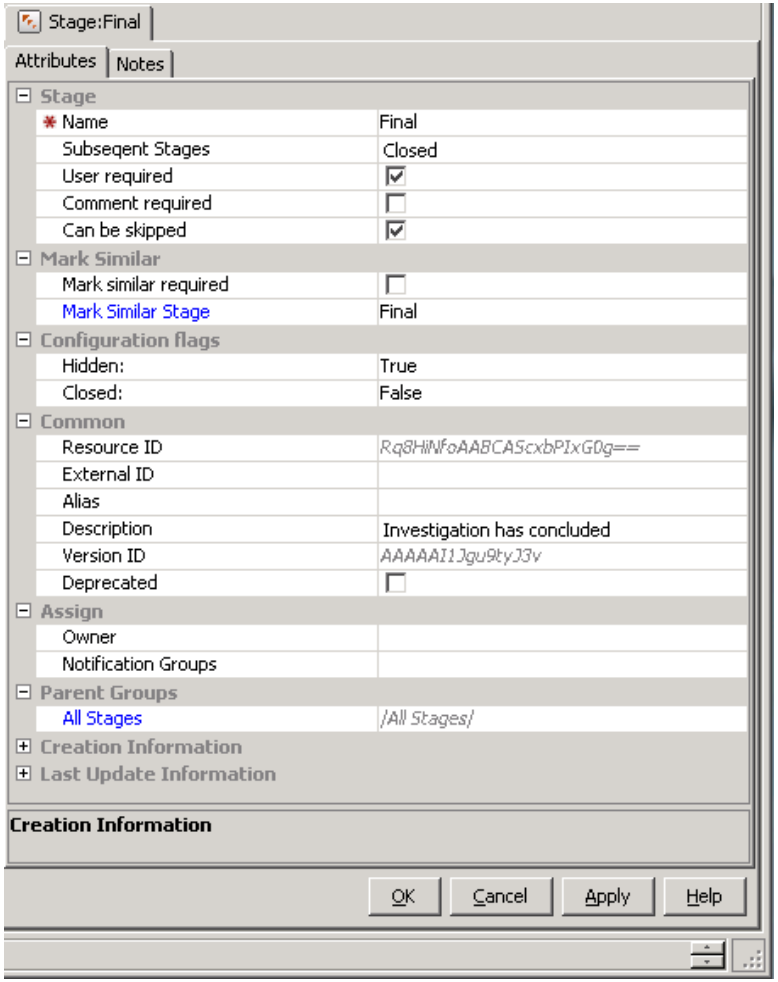
Визуализация



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

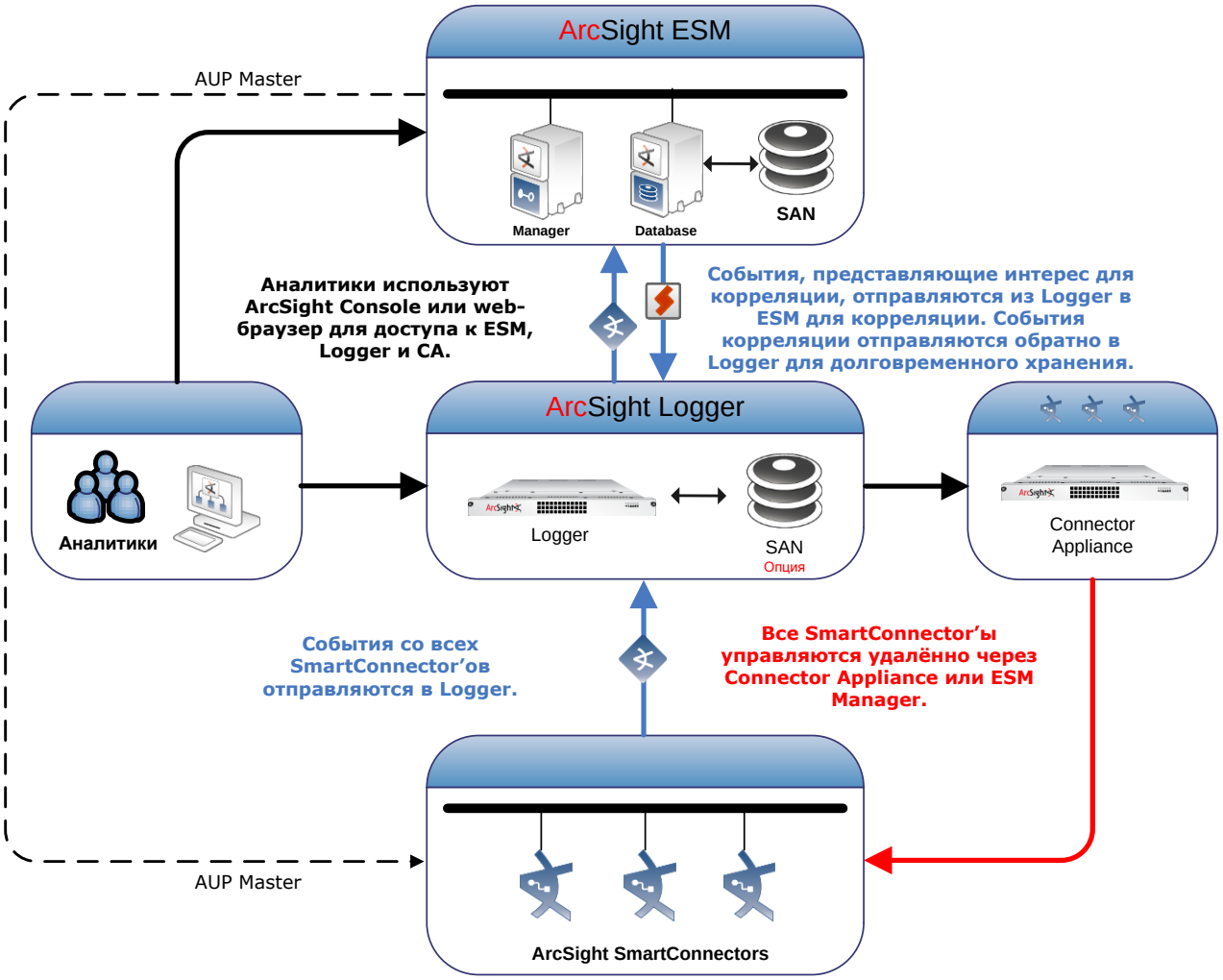




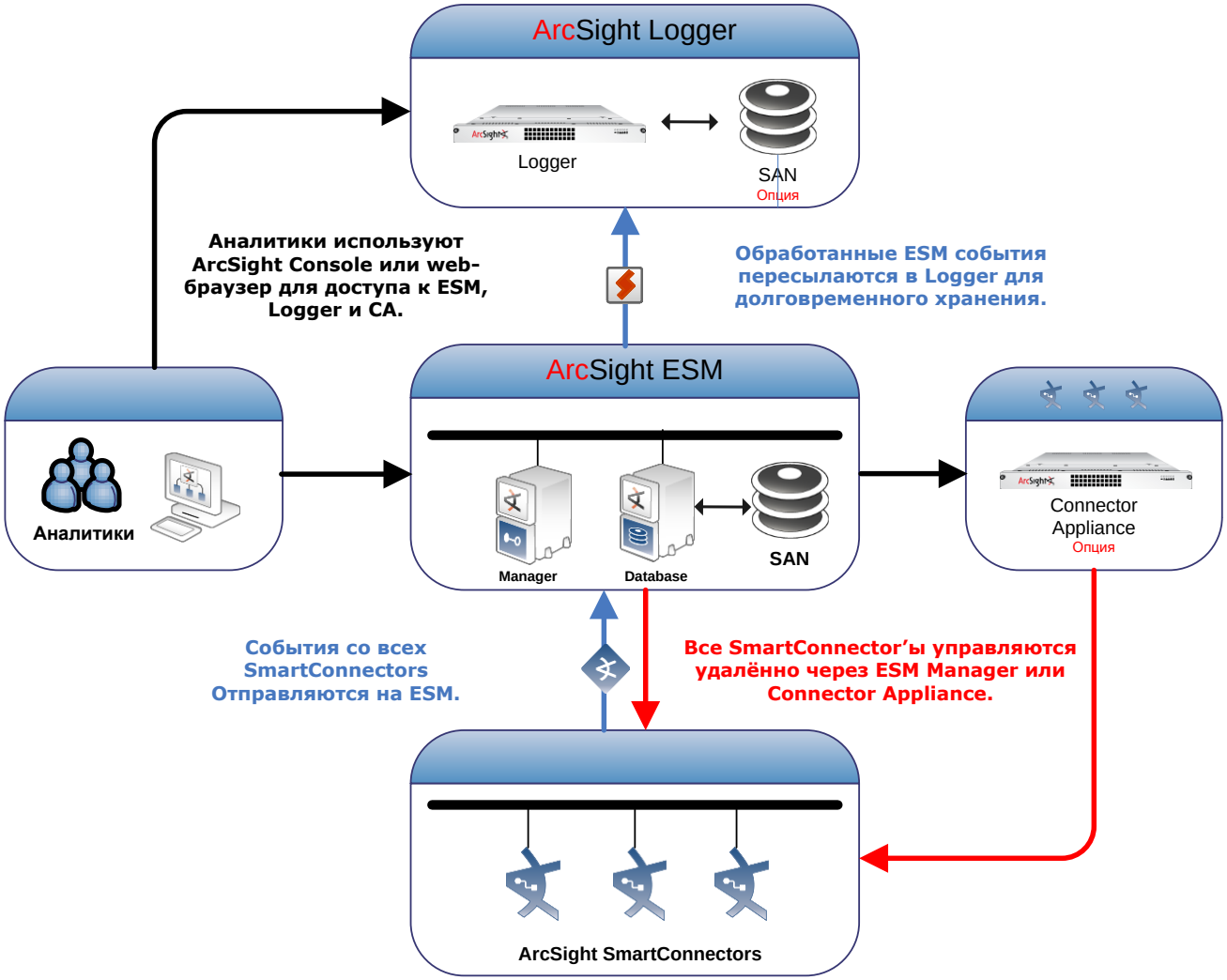
Дополнительные модули

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

ESM + Logger

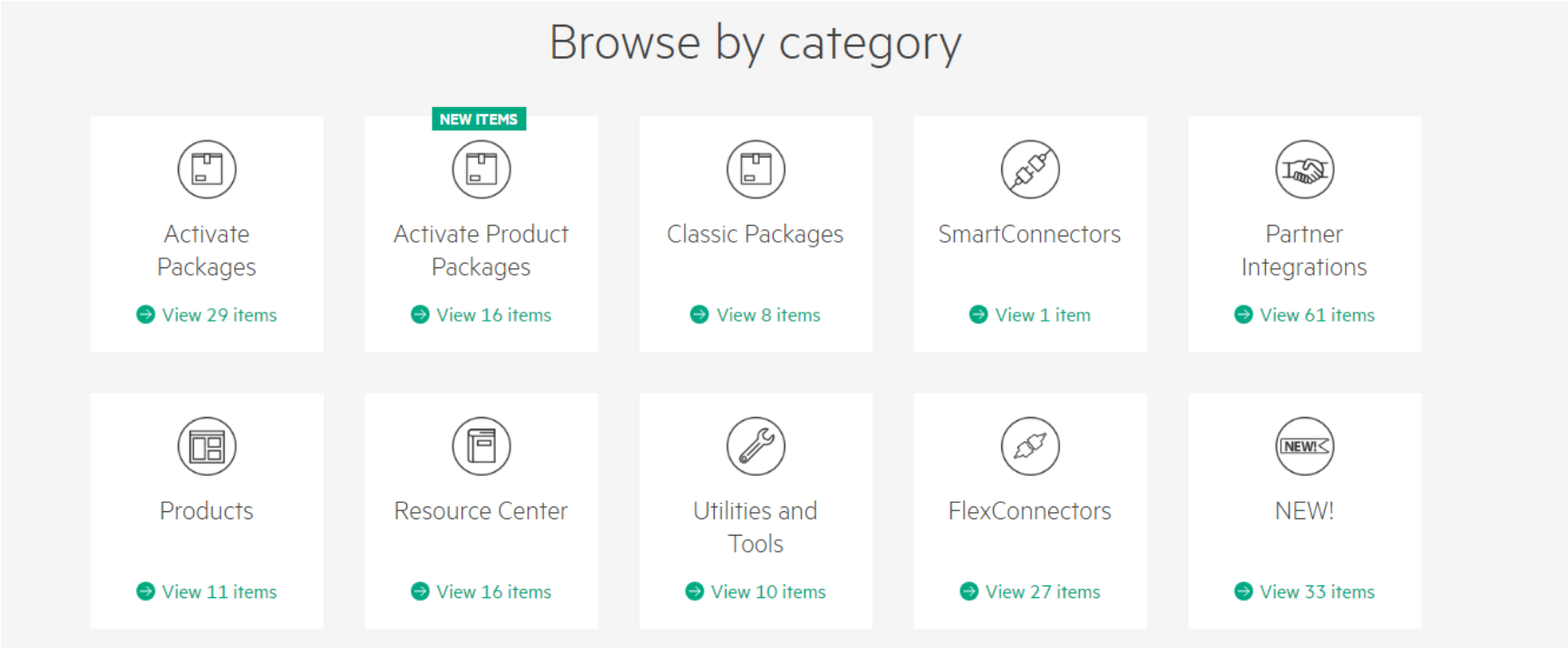

ArcSight ESM
AUP Master
Manager
Database
SAN
Аналитики используют ArcSight Console или web-браузер для доступа к ESM, Logger и CA.
События, представляющие интерес для корреляции, отправляются из Logger в ESM для корреляции. События корреляции отправляются обратно в Logger для долговременного хранения.
ArcSight Logger
Аналитики
Logger
SAN
Опция
Connector Appliance
События со всех SmartConnector'ов отправляются в Logger.
Все SmartConnector'ы управляются удалённо через Connector Appliance или ESM Manager.
AUP Master
ArcSight SmartConnectors

Logger + ESM

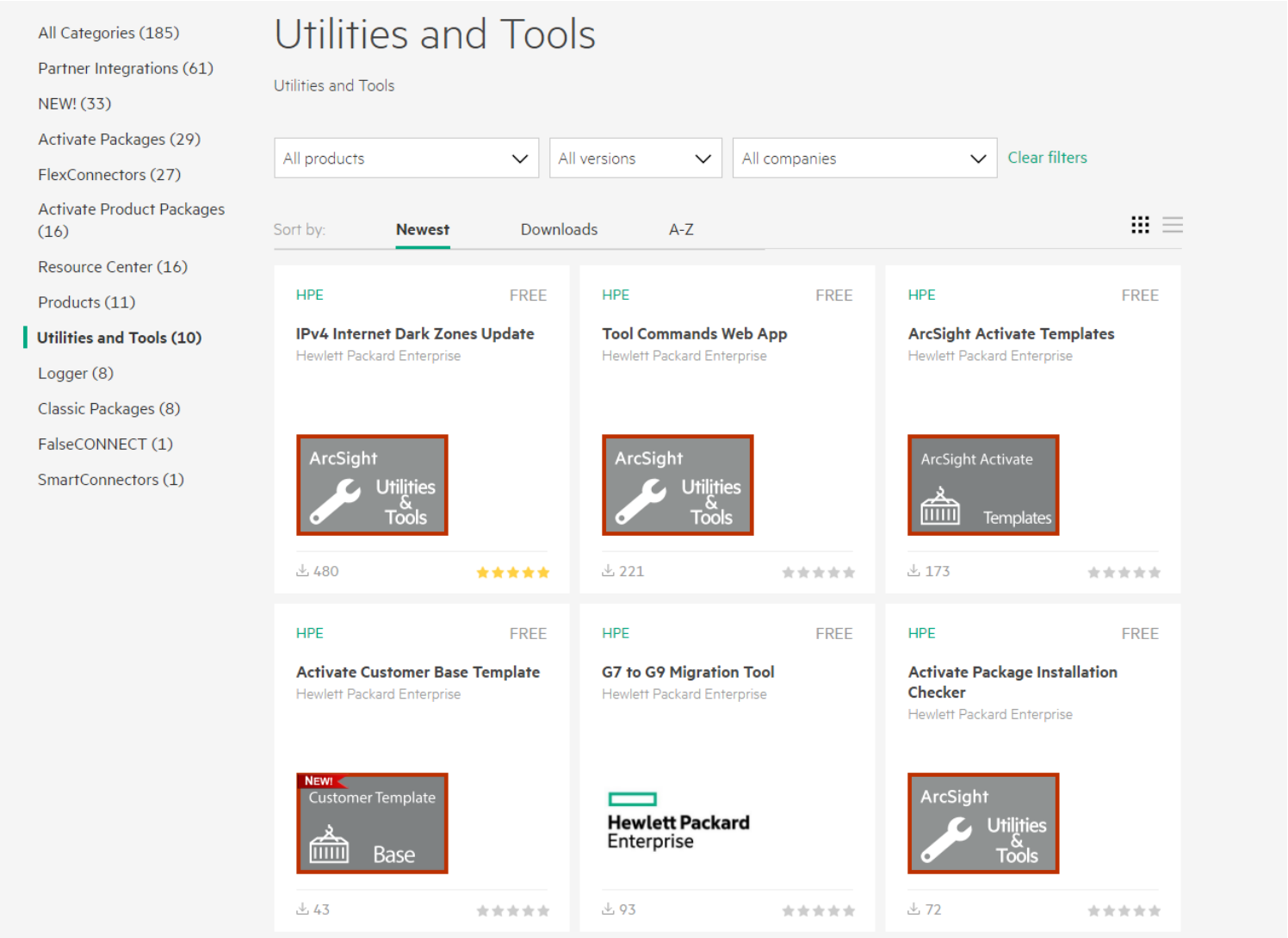

ArcSight Logger
Logger
SAN
Опция
Аналитики используют ArcSight Console или web-браузер для доступа к ESM, Logger и CA.
Обработанные ESM события пересылаются в Logger для долговременного хранения.
ArcSight ESM
Аналитики
Manager
Database
SAN
Connector Appliance
Опция
События со всех SmartConnectors Отправляются на ESM.
Все SmartConnector'ы управляются удалённо через ESM Manager или Connector Appliance.
ArcSight SmartConnectors

ArcSight Marketplace

- Пакеты правил\фильтров
- Нестандартные агенты
- Интеграция со сторонними системами
- Дополнительные утилиты



ArcSight Marketplace



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