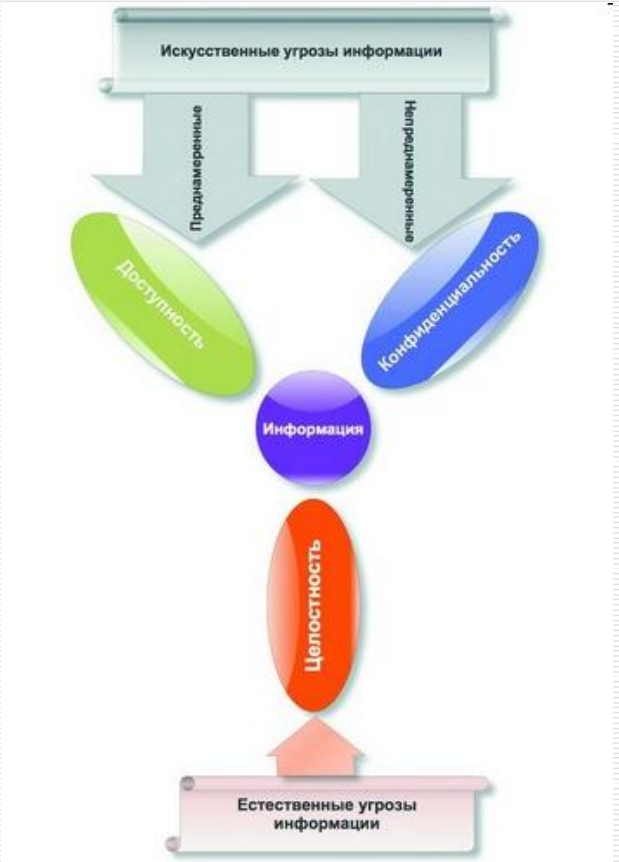
Информационная безопасность

Содержание

- Комплексный подход
- Аудит информационной безопасности
- Система сбора обработки и хранения событий безопасности

Комплексный подход к обеспечению информационной безопасности



Entegrum®

Что такое информационная безопасность?

“Информационная безопасность обеспечивает защиту информации от широкого спектра угроз для обеспечения непрерывности бизнеса, минимизации ущерба для бизнеса и максимизации возврата от инвестиций и возможностей бизнеса” **(ISO/IEC 17799:2005)**

Что такое информационная безопасность?

“Информационная безопасность характеризуется обеспечением:

- Конфиденциальности: информация доступна только лицам, авторизованным на доступ

- Целостности: точность и полнота информации и методов ее обработки

- Доступности: авторизованные пользователи имеют доступ к информации и связанным с ней активам когда им это требуется” **(ISO/IEC 17799:2005)**

Структура ИБ

- Организационные меры
- Документирование
- Программно-технические меры
- Процессы управления ИБ

Организационные меры

- организационная структура
- распределение обязанностей и ответственности
- независимость контроля и исполнения

Документирование

Структура пакета документов:

- Концепция/Политика
- Частные политики
- Стандарты/Положения
- Инструкции/Записи

Программно-технические меры

- аутентификация и аутентификация (управление учетными записями)
- управление доступом (контроль утечек конфиденциальной информации)
- межсетевое экранирование и **VPN**
- системы обнаружения вторжений, контроля и анализа защищенности
- инфраструктура открытых ключей
- системы антивирусной защиты
- и т.д.

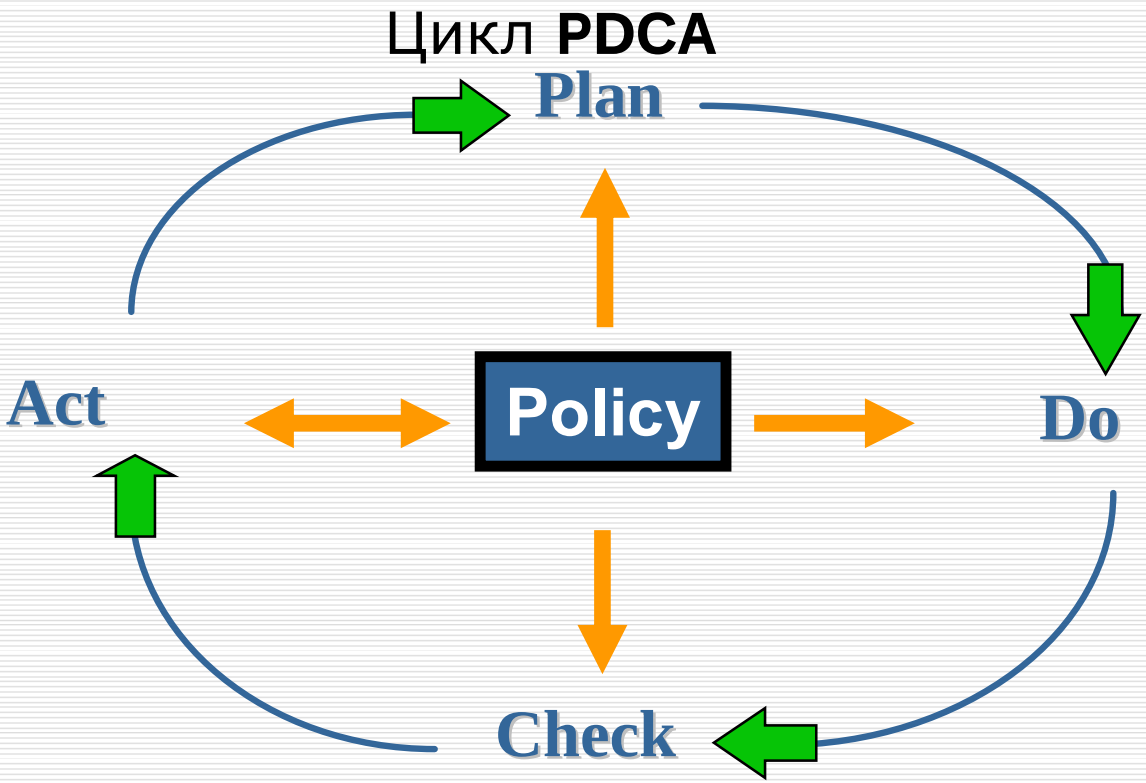
Процессы управления ИБ

Plan – Планирование и оценка рисков

Do – Разработка и внедрение

Check – Мониторинг и анализ

Act – Совершенствование



Процессы управления ИБ

Базовые процессы:

- управление доступом
- управление изменениями
- управление инцидентами

Типовой цикл работ

- Обследование (Аудит информационной безопасности)
- Проектирование
- Внедрение
- Сопровождение

Аудит и оценка защищенности

Entegrum®

Что такое аудит информационной безопасности?

Аудит информационной безопасности – независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций.

Цели аудита

Выявить недостатки и уязвимости в существующем порядке и принятых мерах по обеспечению информационной безопасности в Организации

Виды аудита

- аудит на соответствие требованиям или стандартам:
  - Законодательство и требование федеральных регуляторов (ФСТЭК, ФСБ и т.д.)
  - международные стандарты **(ISO 27001/2)**
  - стандарты производителей **(CiscoSAFE)**
- экспертная оценка положения дел по обеспечению информационной безопасности (лучшие практики)
- тест на проникновение

Критерии успеха аудита

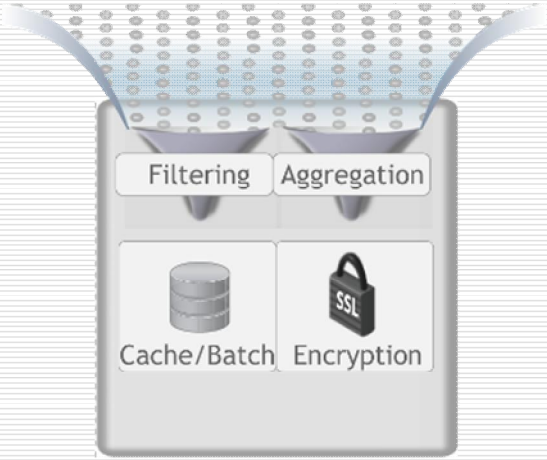
- Предварительный удаленный сбор информации
- Детальное планирование аудита (включая, резервирование рабочего времени сотрудников Заказчика)
- Активное содействие сотрудников Заказчика при проведении интервьюирований и объективных оценок
- Участие сотрудников Заказчика в уточнении данных и согласовании отчетных документов

Тест на проникновение

- Технический тест на проникновение
- Социотехнический тест на проникновение
- Оценка защищённости веб-приложений
- Оценка защищённости беспроводных сетей

ArcSight

Система сбора обработки и хранения событий безопасности



Entegrum®

Основные проблемы

- данные о событиях ИБ генерируют большое количество устройств различного типа
- объем событий ИБ огромен и администратору не может эффективно отслеживать и реагировать на события
- отсутствует или затруднена возможность корреляции (анализ взаимосвязей) событий ИБ
- затруднена возможность анализа ситуации

Различный формат записи схожих событий

10/09/200317:42:57,146.127.94.13,48352,146.127.97.14,909,,,accept,tcp,,,,909,146.127.93.29,,0,,4,3,,' 9Oct2003 17:42:57,accept,labcpngfp3,inbound,eth2c0,0,VPN-1 & FireWall-1,product=VPN-1 & FireWall-1[db_tag={0DE0E532-EEA0-11D7-BDFC-927F5D1DECEC};mgmt= labcpngfp3;date=1064415722;policy_name= Standard],labdragon,48352,146.127.97.14,909, tcp,146.127.93.145,',eth2c0,inbound

Oct 9 16:29:49 [146.127.94.4] Oct 09 2003 16:44:50: %PIX-6-302013: Built outbound TCP connection 2245701 for outside:146.127.98.67/1487 (146.127.98.67/1487) to inside:146.127.94.13/42562 (146.127.93.145/42562)

2003-10-20|15:25:52|dragonapp-nids|TCP-SCAN|146.127.94.10|146.127.94.13|0|0|X|------S-|0|total=484,min=1,max=1024,up=246,down=237,flags=------S-,Oct20-15:25:34,Oct20-15:25:52|

Oct 20 15:35:08 labsnort snort: [1:1421:2] SNMP AgentX/tcp request [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 146.127.94.10:43355 -> 146.127.94.13:705

SENSORDATAID="138715" SENSORNAME="146.127.94.23:network_sensor_1" ALERTID="QPQVIOAJKBNC6OONK6FTNLLESZ" LOCALTIMEZONEOFFSET="14400" ALERTNAME="pcAnywhere_Probe“ ALERTDATETIME="2003-10-20 19:35:21.0" SRCADDRESSNAME="146.127.94.10" SOURCEPORT="42444" INTRUDERPORT="42444" DESTADDRESSNAME="146.127.94.13" VICTIMPORT="5631" ALERTCOUNT="1" ALERTPRIORITY="3" PRODUCTID="3" PROTOCOLID="6" REASON="RSTsent"

Лидирующие системы управления событиями ИБ

ArcSight ESM

Cisco MARS

RSA enVision

IBM Tivoli Security Operation Management

netForensics OSP

Entegrum®

Entegrum®

Аналитический отчет компании Gartner

Gartner : «решения компании **ArcSight** уже **5** лет подряд занимают лидирующие позиции в области систем мониторинга и управления информационной безопасностью»

Entegrum®

Основные конкурентные преимущества ArcSight

ArcSight ESM. Гибкость архитектуры, максимальное количество типов источников, стабильность работы и производительность

Cisco MARS. Сетевая направленность

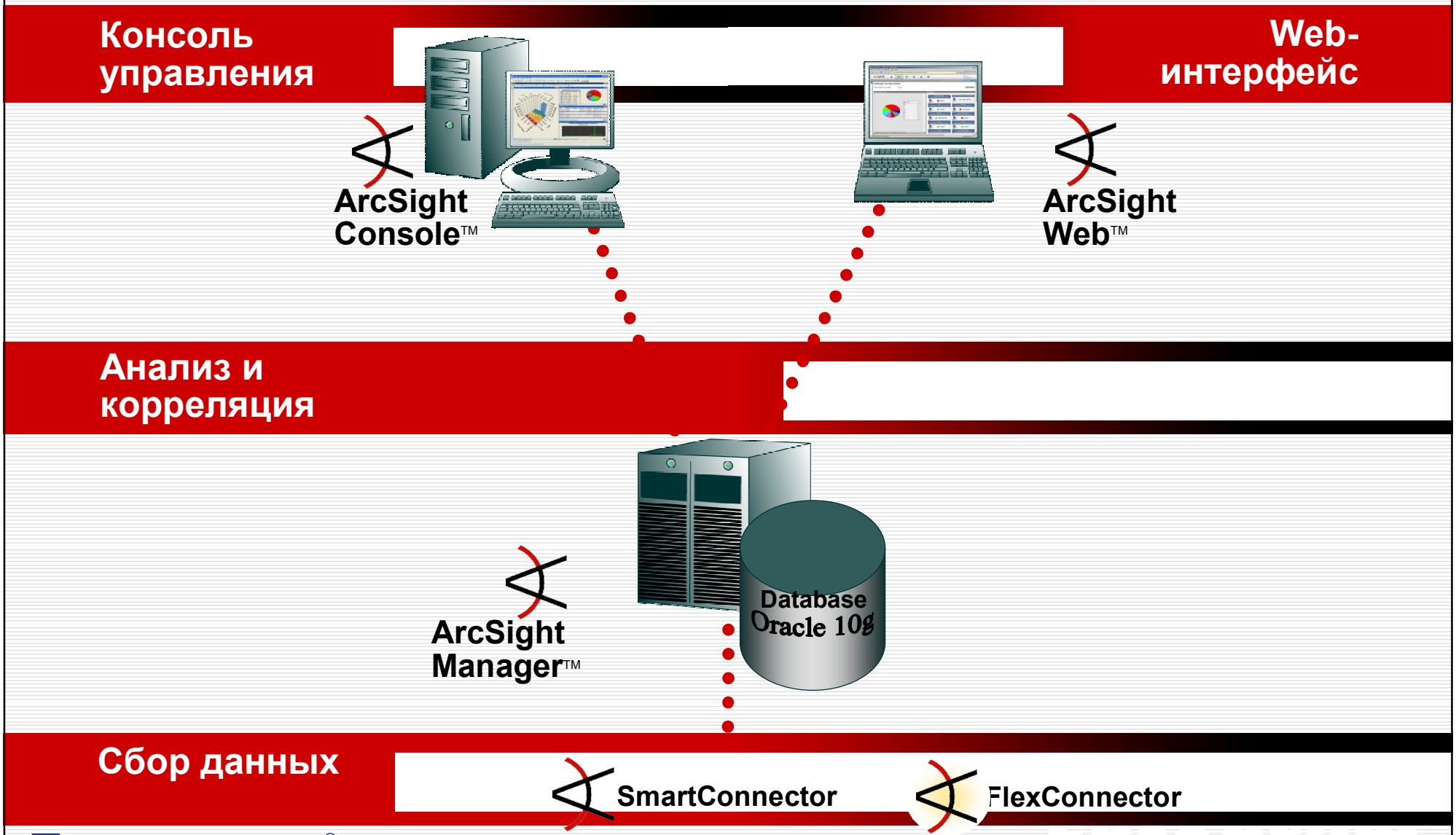
RSA enVision. Неэффективная корреляция,сложность настройки, отстутствие распределенной архитектуры

IBM Tivoli Security Operation Management. Меньшее количество поддерживаемых источников. Сложность разработки коннекторов

netForensics OSP. Нестабильная работа, сложность настройки и создания собственных коннекторов

Entegrum®

Архитектура системы ArcSight ESM



Entegrum®

Основные конкурентные преимущества ArcSight

ArcSight ESM. Гибкость архитектуры, максимальное количество типов источников, стабильность работы и производительность

Cisco MARS. Сетевая направленность

RSA enVision. Неэффективная корреляция,сложность настройки, отстутствие распределенной архитектуры

IBM Tivoli Security Operation Management. Меньшее количество поддерживаемых источников. Сложность разработки коннекторов

netForensics OSP. Нестабильная работа, сложность настройки и создания собственных коннекторов

Entegrum®

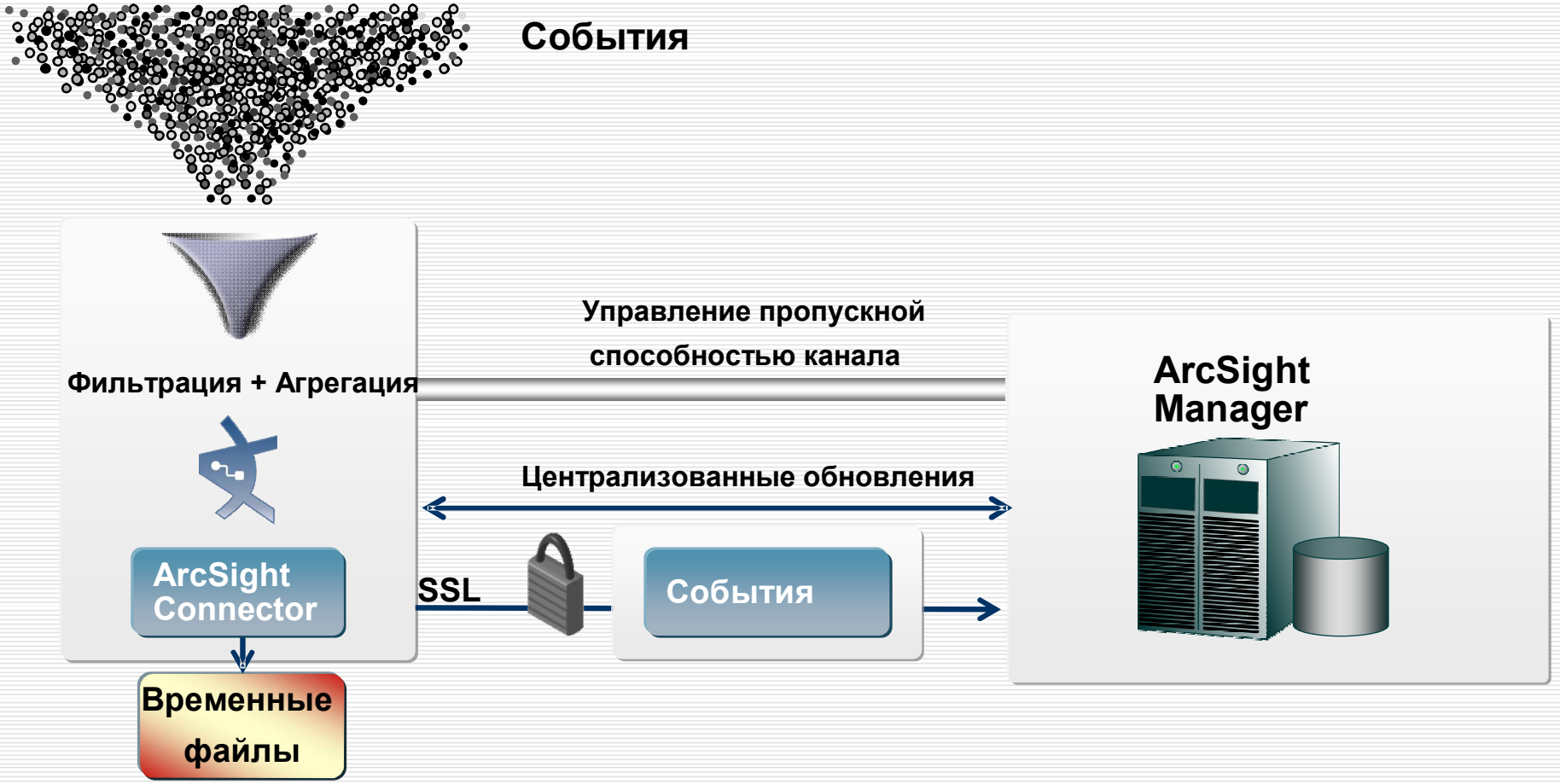
Широкий спектр поддерживаемых продуктов

(180+ продуктов в 35+ категориях от 80+ партнеров)

Основные функции ArcSight

- Приоритезация
- Корреляция
- Визуализация событий
- Мониторинг и Расследования
- Оповещения
- Отчетность

Схема работы ArcSight

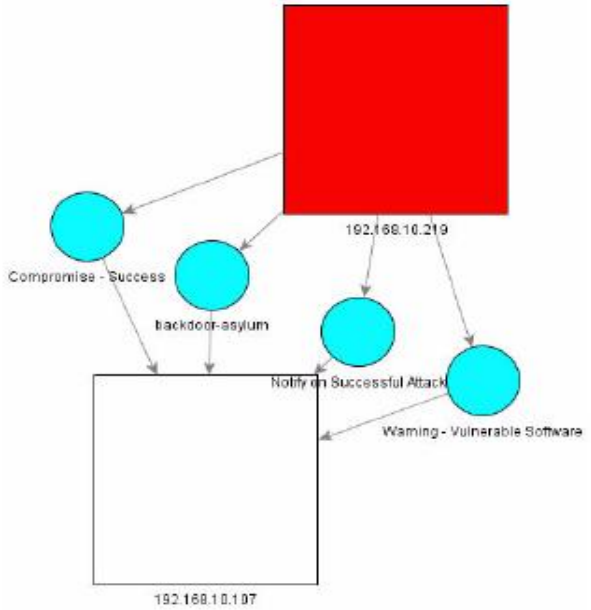


Корреляция

От миллионов событий к единицам, которые действительно важны

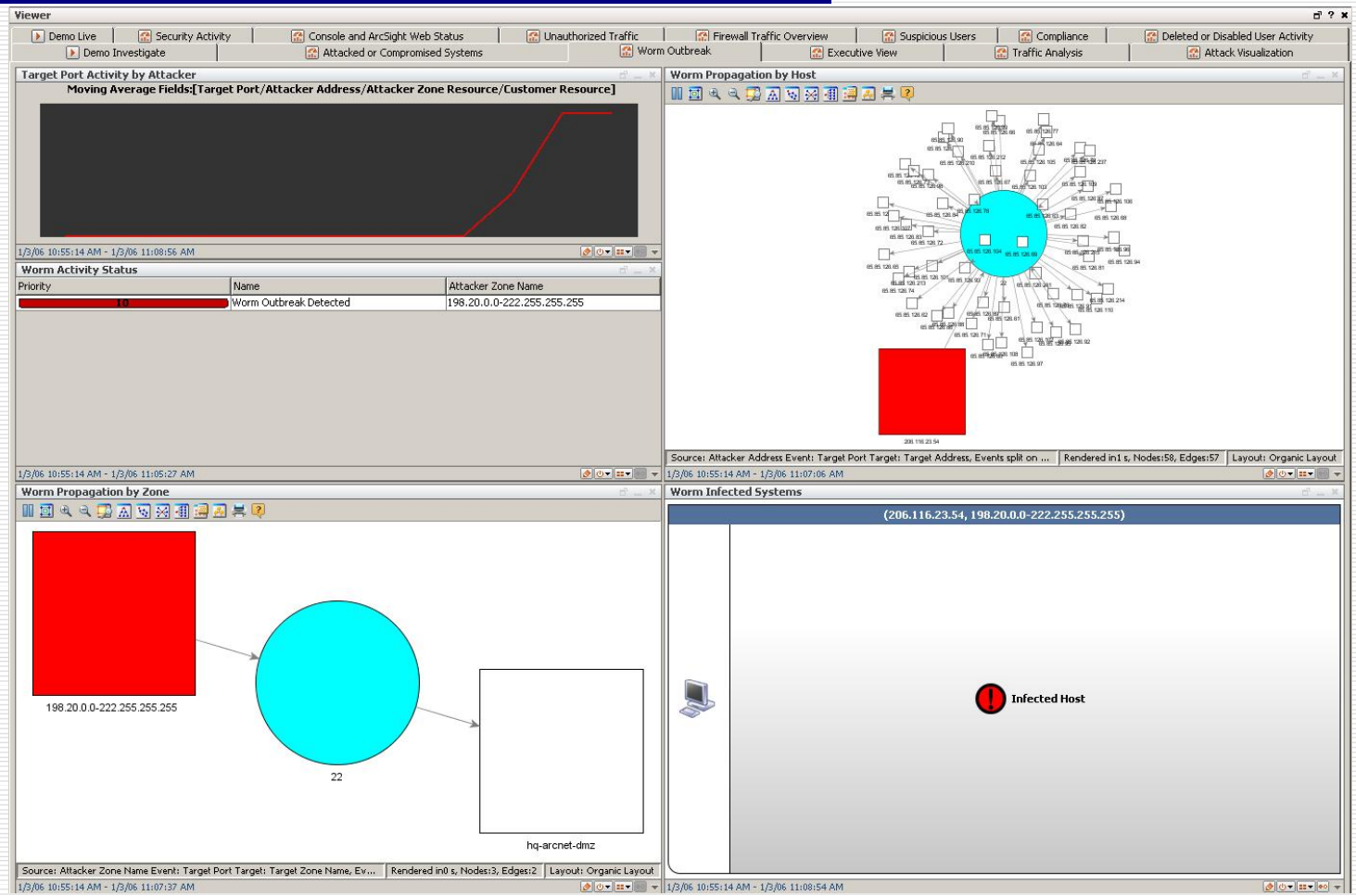
Визуализация

- Графический и табличный вид
- Возможности глубокой детализации **(drill down)**



Entegrum®

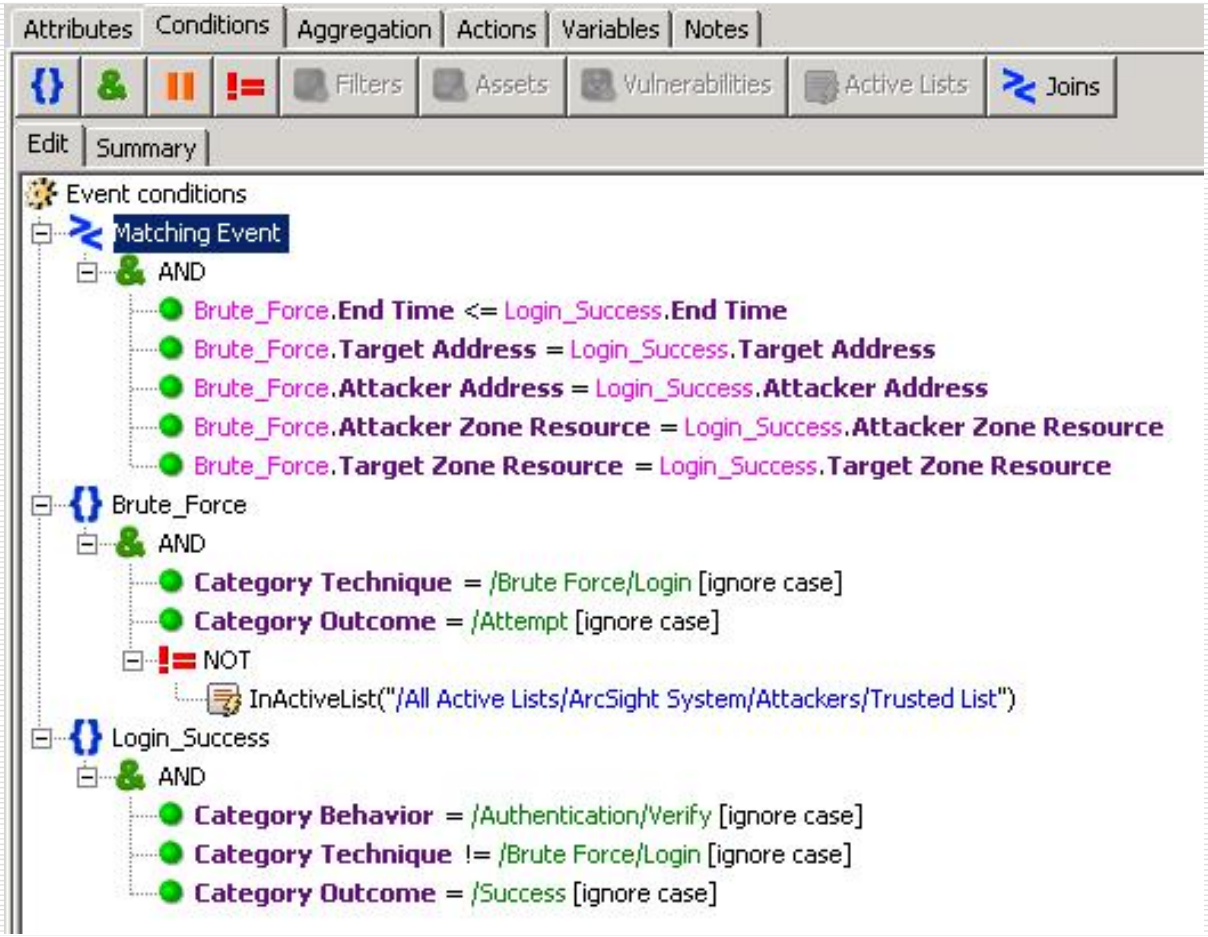
Пример выявления инцидента



Entegrum®

Реализация сценариев корреляции

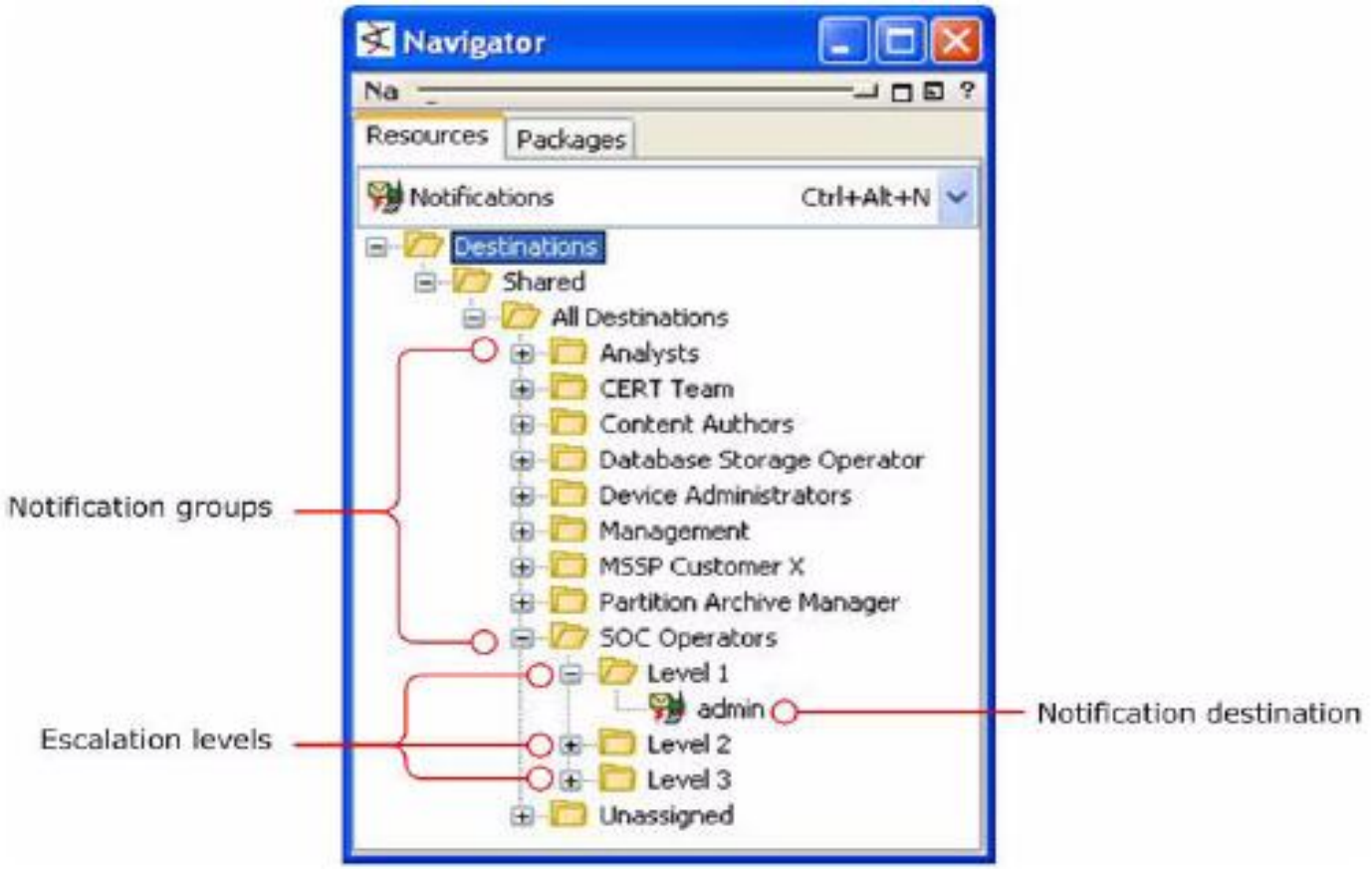
Пример компрометации системы после успешной **BruteForce** атаки



Оповещения

Оповещения в режиме реального времени
- **Email, SMS**
- Оповещения в формате **SNMP**

Возможность интеграции с
- **Service Desk**



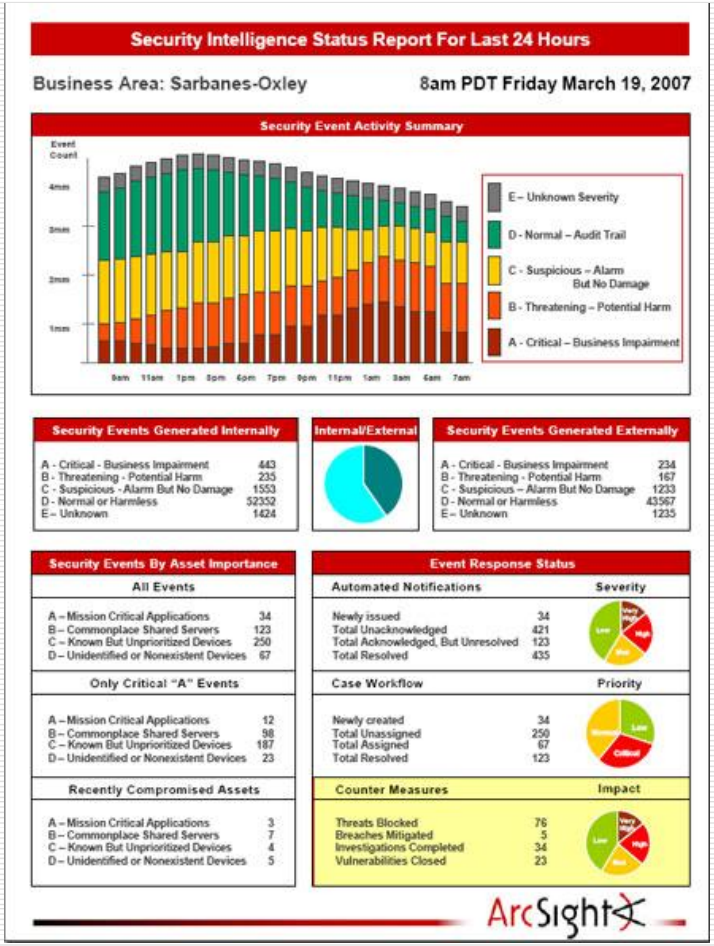
Entegrum®

Расследования и управление инцидентами

- оповещение различных групп сотрудников в зависимости от категории и критичности инцидента
- передача инцидента на обработку и реагирования одному или нескольким сотрудникам
- протоколирование обработки и реагирования на инцидент с отслеживанием статуса инцидента
- закрытие инцидента с оповещением всех заинтересованных лиц и формированием выводов
- архивирование всей информации об инциденте и процессу его обработки/реагирования в базу знаний

Отчетность

- **400** стандартных шаблонов отчетов
- Отчетность касающаяся активов
- Отчетность касающаяся событий
- Отчетность касающаяся соответствия требованиям стандартов **(SOX, PCI DSS, ISO 17799)**
- Графический пользовательский интерфейс
- Гибкая схема создания отчета без использования программирования



Entegrum®

Результаты внедрения ArcSight ESM

- Централизованный сбор, хранение и обработка событий ИБ
- Мониторинг, анализ и корреляции событий информационной безопасности в режиме реального времени
- Использование средств визуализации и детализации инцидента
- Снижение времени расследования и реагирования на инциденты
- Снижение рисков информационной безопасности за счет своевременного обнаружения и обработки инцидентов информационной безопасности

ВОПРОСЫ