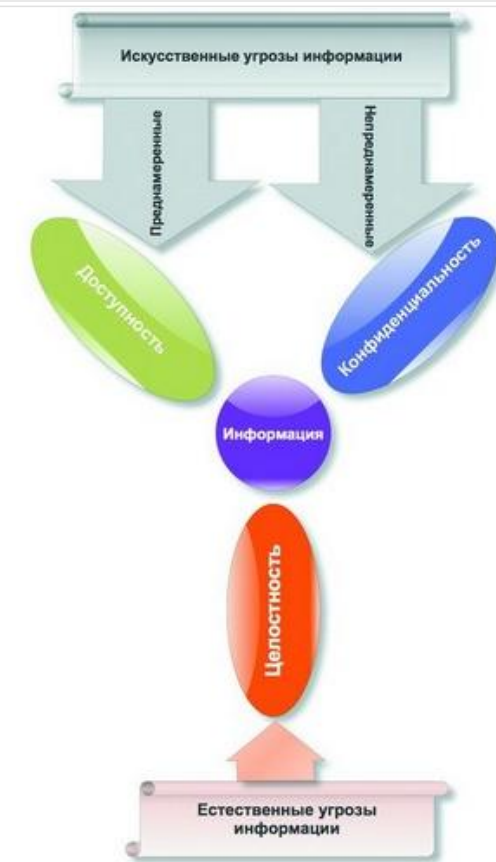

Информационная безопасность



Содержание

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

Комплексный подход к обеспечению информационной безопасности



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 авторизация (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.

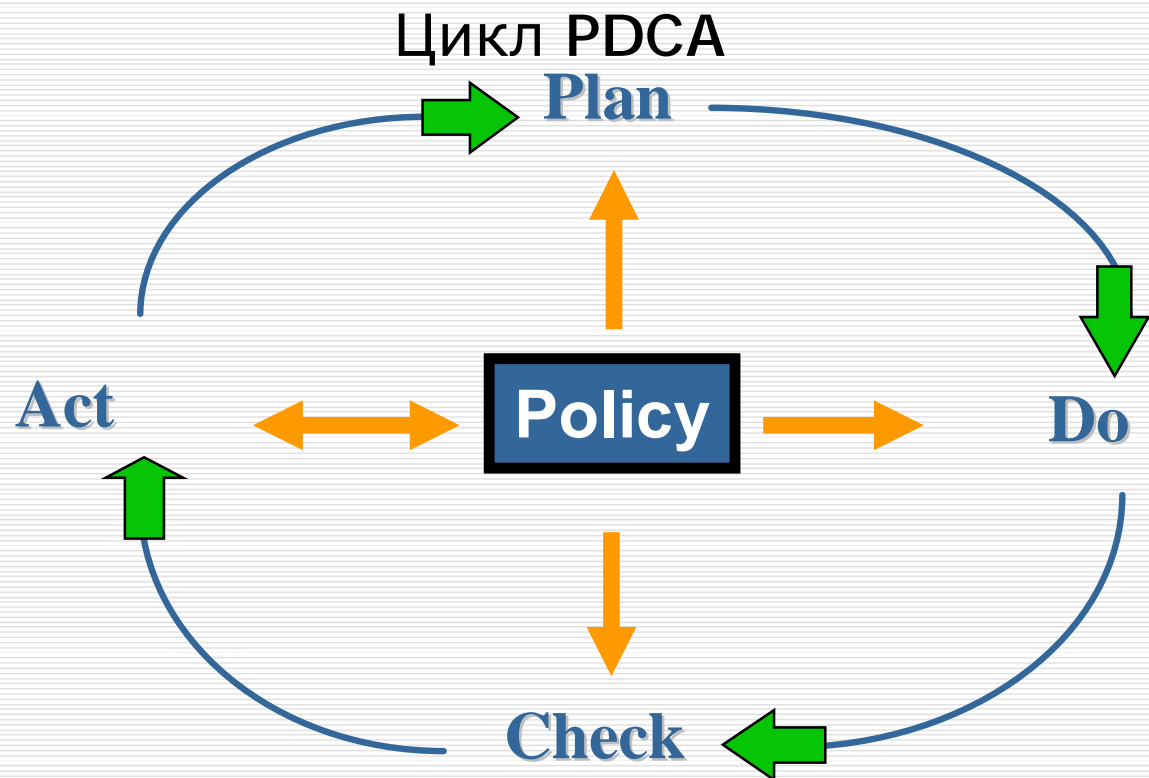
Процессы управления ИБ

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



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

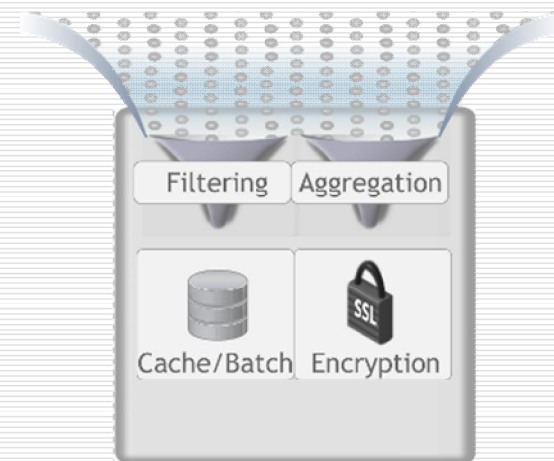
- Предварительный удаленный сбор информации
- Детальное планирование аудита (включая, резервирование рабочего времени сотрудников Заказчика)
- Активное содействие сотрудников Заказчика при проведении интервьюирований и объективных оценок
- Участие сотрудников Заказчика в уточнении данных и согласовании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



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



10/09/2003 17:42:57,146.127.94.13,48352,146.127.97.14,909,,,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

The logo for ArcSight, featuring the word "ArcSight" in a sans-serif font with a stylized red and black symbol to the right.

ArcSight ESM

The Cisco logo, consisting of seven vertical bars of varying heights above the word "CISCO" in a bold, sans-serif font.

Cisco MARS

The RSA logo, featuring the letters "RSA" in white on a red rectangular background.

RSA enVision

The IBM logo, consisting of the letters "IBM" in a blue, striped, sans-serif font.

IBM Tivoli Security Operation Management

The netForensics logo, featuring a red circular icon with a white crosshair and the word "netForensics" in a bold, sans-serif font.

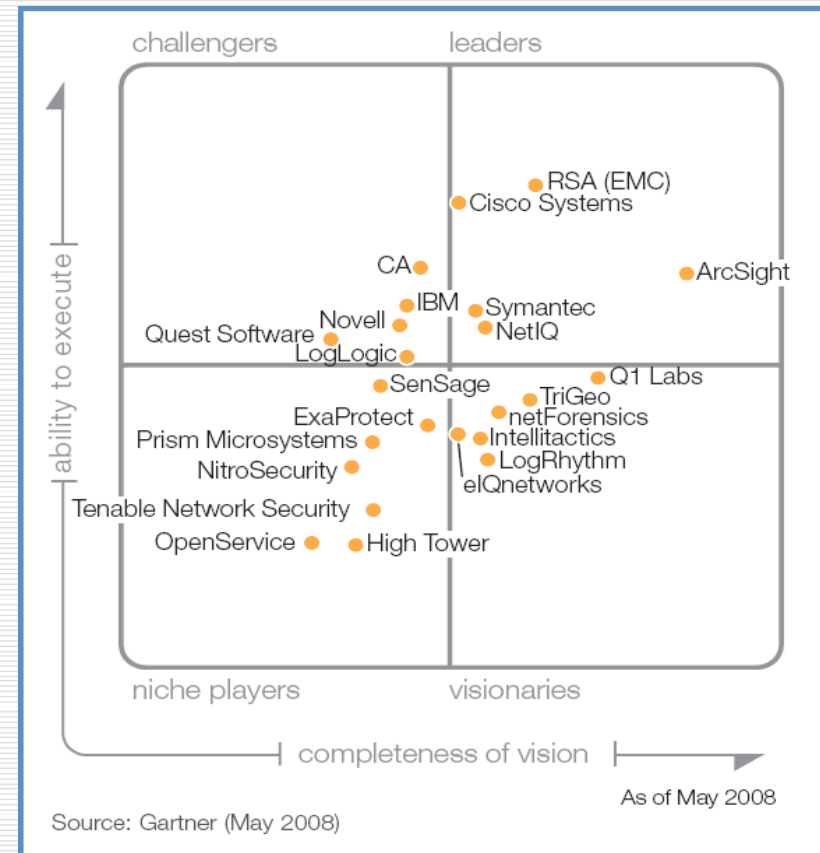
netForensics OSP

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»



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, отсутствие распределенной архитектуры



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



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



Архитектура системы ArcSight ESM

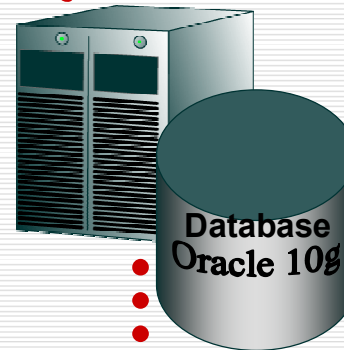
Консоль управления



Web-интерфейс



Анализ и корреляция



Сбор данных



SmartConnector



FlexConnector

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, отсутствие распределенной архитектуры



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



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



Широкий спектр

поддерживаемых продуктов

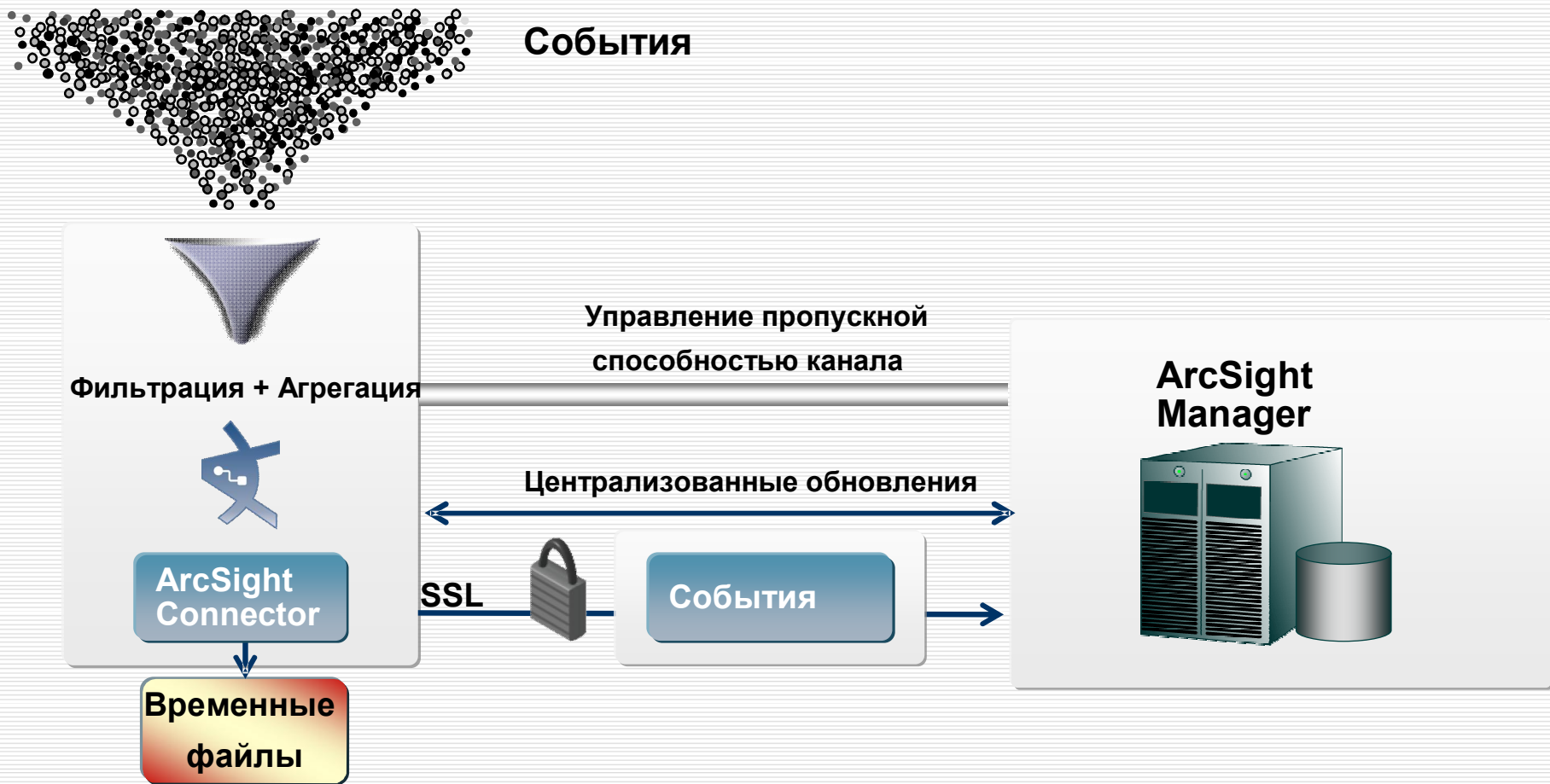
(180+ продуктов в 35+ категориях от 80+ партнеров)



Основные функции ArcSight

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

Схема работы ArcSight



Корреляция

Кто: идентификация

оценка: Что

Когда: анализ

время: Когда

Корреляция



Как

ArcSight

От миллионов
событий к
единицам, которые
действительно
важны

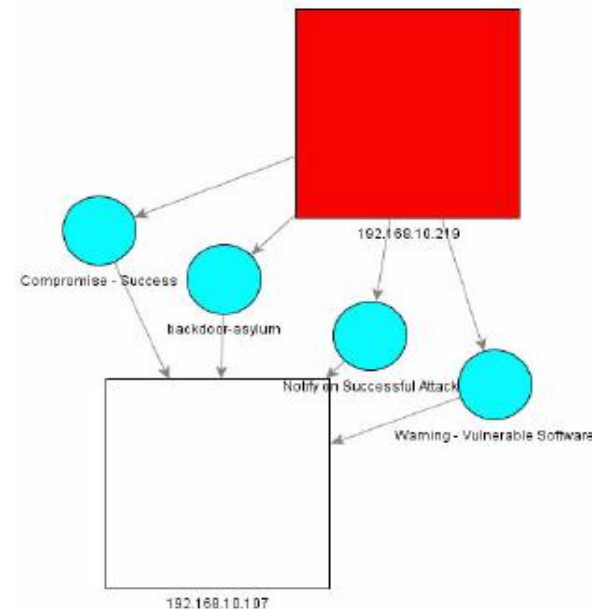
Визуализация

○ Графический и табличный вид

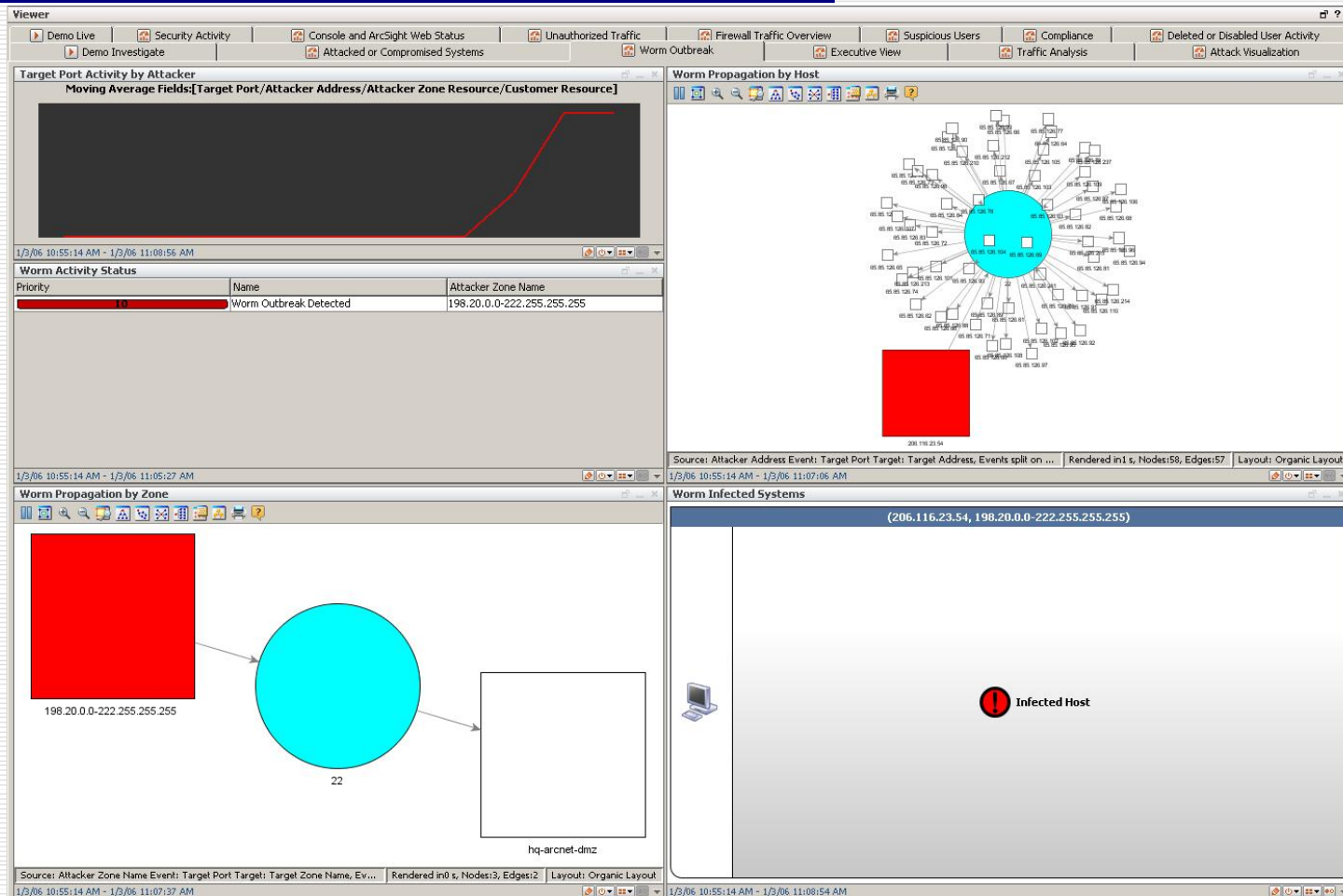
○ Возможности глубокой детализации (drill down)



End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
13 Aug 2007 15:34:43 PDT	SELECT		10.0.111.12	5	ORACLE	Oracle
13 Aug 2007 15:34:39 PDT	Cisco NetFlow Event	10.0.112.53	10.0.20.62	2	CISCO	Cisco NetFlow
13 Aug 2007 15:34:36 PDT	backdoor-asylum	192.168.10.219	192.168.10.107	3	ISS	Internet Scanner
13 Aug 2007 15:34:36 PDT	Warning - Vulnerable Software	192.168.10.219	192.168.10.107	3	ArcSight	ArcSight
13 Aug 2007 15:34:36 PDT	Compromise - Success	192.168.10.219	192.168.10.107	3	ArcSight	ArcSight
13 Aug 2007 15:34:36 PDT	Notify on Successful Attack	192.168.10.219	192.168.10.107	3	ArcSight	ArcSight
13 Aug 2007 15:34:32 PDT	SQL Server Audit			2	Microsoft	SQL 2000



Пример выявления инцидента



Реализация сценариев корреляции

Пример компрометации системы после успешной BruteForce атаки

The screenshot displays a configuration window for a correlation rule. The interface includes a menu bar with tabs: Attributes, Conditions, Aggregation, Actions, Variables, and Notes. Below the menu bar is a toolbar with icons for code, a person, a pause button, an equals sign, and buttons for Filters, Assets, Vulnerabilities, Active Lists, and Joins. The main area is divided into 'Edit' and 'Summary' tabs. The 'Edit' tab is active, showing a tree view of event conditions. The root node is 'Event conditions', which contains three main event types: 'Matching Event', 'Brute_Force', and 'Login_Success'. Each event type has its own set of conditions, often grouped by logical operators like AND or NOT.

- Matching Event**
 - AND
 - Brute_Force.End Time <= Login_Success.End Time
 - Brute_Force.Target Address = Login_Success.Target Address
 - Brute_Force.Attacker Address = Login_Success.Attacker Address
 - Brute_Force.Attacker Zone Resource = Login_Success.Attacker Zone Resource
 - Brute_Force.Target Zone Resource = Login_Success.Target Zone Resource
- Brute_Force**
 - AND
 - Category Technique = /Brute Force/Login [ignore case]
 - Category Outcome = /Attempt [ignore case]
 - NOT
 - InActiveList("/All Active Lists/ArcSight System/Attackers/Trusted List")
- Login_Success**
 - AND
 - Category Behavior = /Authentication/Verify [ignore case]
 - Category Technique != /Brute Force/Login [ignore case]
 - Category Outcome = /Success [ignore case]

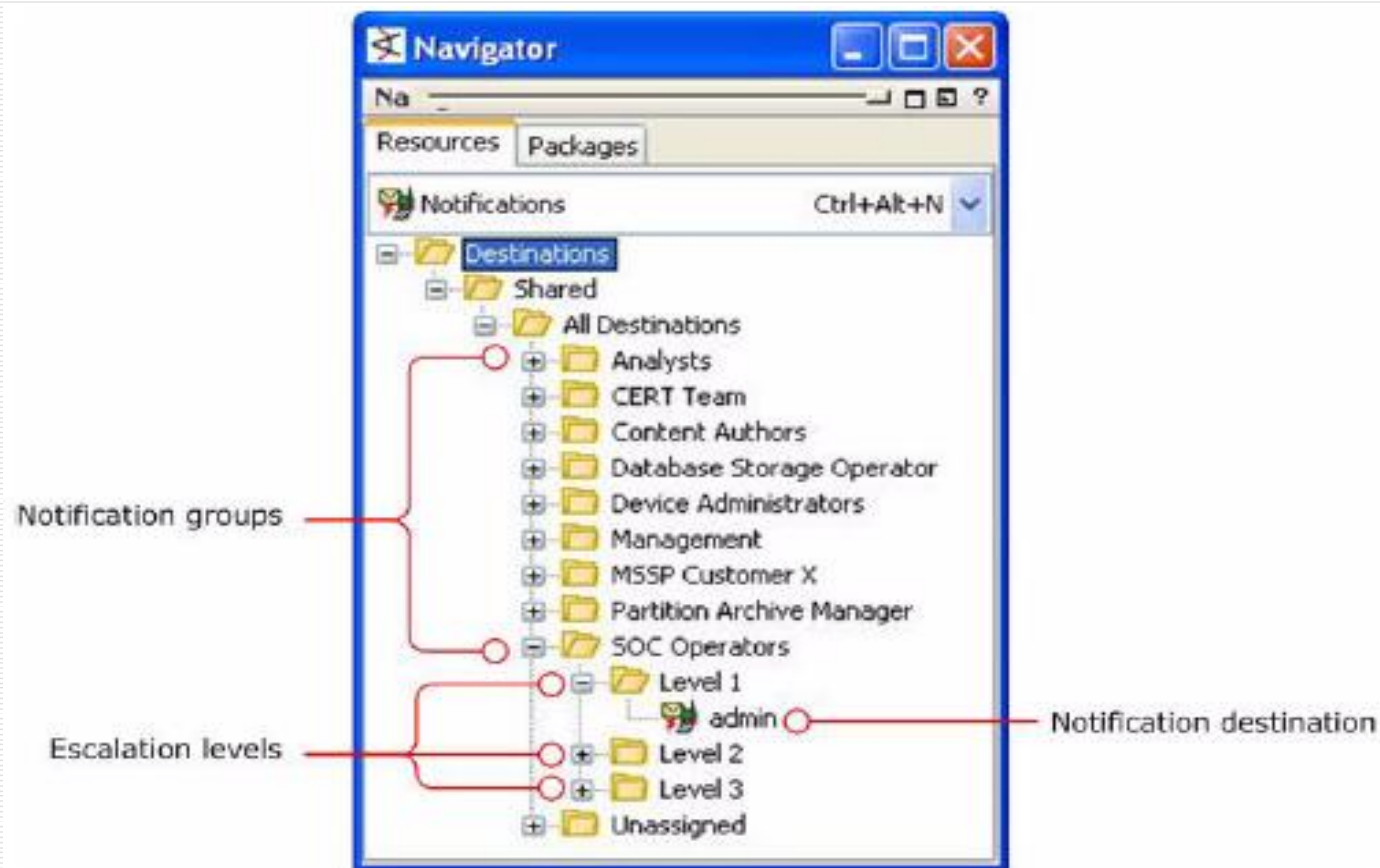
Оповещения

Оповещения в режиме реального времени

Email, SMS
Оповещения в формате SNMP

Возможность интеграции с Service Desk

Entegrum[®]



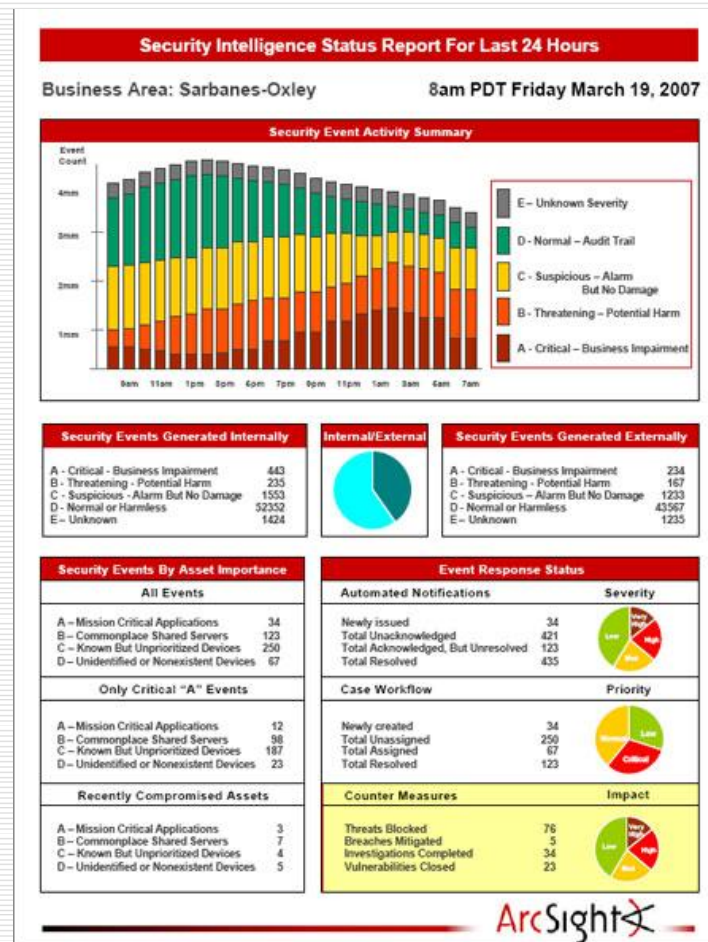
Entegrum[®]

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 процессе 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



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

