СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 13

Системы управления событиями (SIEM)

Преподаватель: **Батыргалиев Асхат Болатканович, PhD,**
ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»

askhat.b.b@gmail.com

Содержание

Содержание

По завершению лекции Вы будете знать:

1. Понятие SIEM
2. Решаемые SIEM задачи
3. Применение SIEM
4. Источники данных для SIEM
5. Архитектуру SIEM
6. Функционирование SIEM
7. Компоненты SIEM-систем

Понятие SIEM

SIEM представляет собой улучшенную систему обнаружения вредоносной активности и различных системных аномалий. Работа SIEM позволяет увидеть более полную картину активности сети и событий безопасности. Когда обычные средства обнаружения по отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Сотни и тысячи устройств живут своей жизнью и генерируют миллионы событий, сообщая о том, что происходит с ними и вокруг. При этом необходимо реагировать только на часть из них.

Отдельные устройства, операционные системы только предоставляют события без детального анализа

Для полной картины происходящего необходимо собрать воедино состояния с отдельных устройств

Для этого и нужна SIEM система

SIEM - система собирает, анализирует и представляет информацию из сетевых устройств, средств защиты информации и информационных систем.
Также в систему входят приложения для контроля идентификацией и доступом, инструменты управления уязвимостями.

Понятие SIEM

Security Information and Event Management (SIEM)

Системы управления информацией и событиями в безопасности (СУИСБ)

Класс решений в области информационной безопасности, ориентированных на поддержку процессов управления как безопасностью, так и всей IT-инфраструктурой предприятия

Понятие SIEM

Технология SIEM = SIM+ SEM

SIM («управление информацией безопасности»)

- сбор, хранение и анализ данных (взятых из журналов)
- подготовка отчетов по соответствию нормативным требованиям

SEM («управление событиями безопасности»)

- мониторинг событий безопасности в реальном времени
- выявление и реагирование на инциденты безопасности

Рост сложности автоматизированных систем

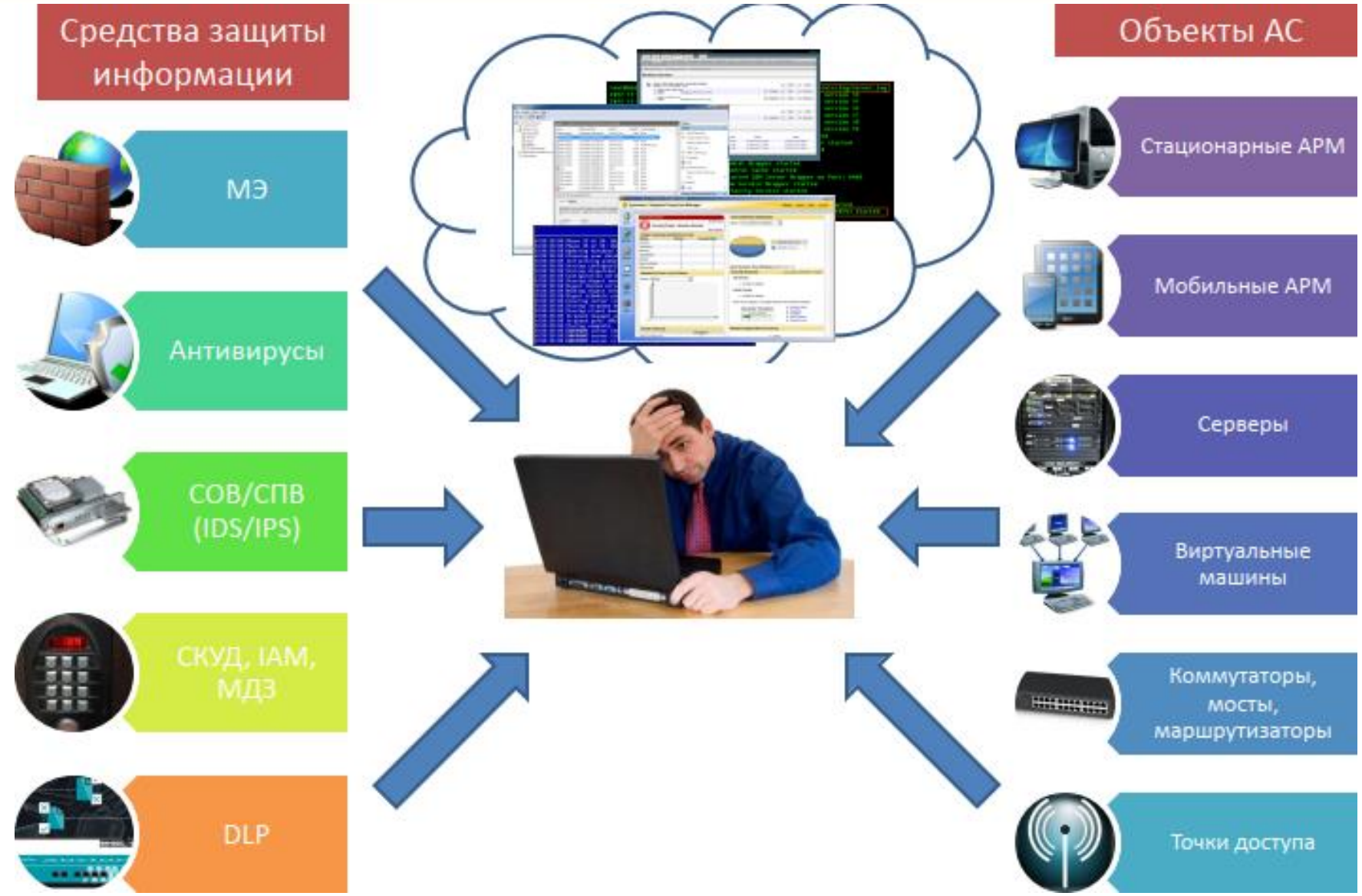
Рост числа сегментов сетей и количества узлов АС

Рост числа типов платформ (гетерогенные сети)

Рост количества виртуальных узлов и топологий (VPN, VRF, VLAN)

Рост требований к квалификации персонала

Традиционное управление автоматизированных систем без SIEM



Проблемы традиционного подхода к безопасности автоматизированных систем

Настройка и контроль работы СЗИ в «ручном режиме»

- Конфигурации и журналы работы антивирусных средств, МЭ, СОВ, DLP, МДЗ, СКУД и IAM просматриваются отдельно для каждого средства
- Точно так же отдельно изучаются параметры их конфигурации

Локальный контроль настроек и журналов узлов сети

- Администратор проверяет настройки и журналы АРМ, сетевого оборудования и серверов, по отдельности подключаясь к каждому из узлов сети

Управление СЗИ и узлами сети не консолидировано

- Немногочисленные исключения:
  - групповые политики ОС в доменах
  - консоли администратора для СЗИ от одного вендора

Нерегулярность операций контроля защищенности

- Аудит безопасности проводится:
  - либо нерегулярной основе (когда вспомнят)
  - либо не проводится вообще

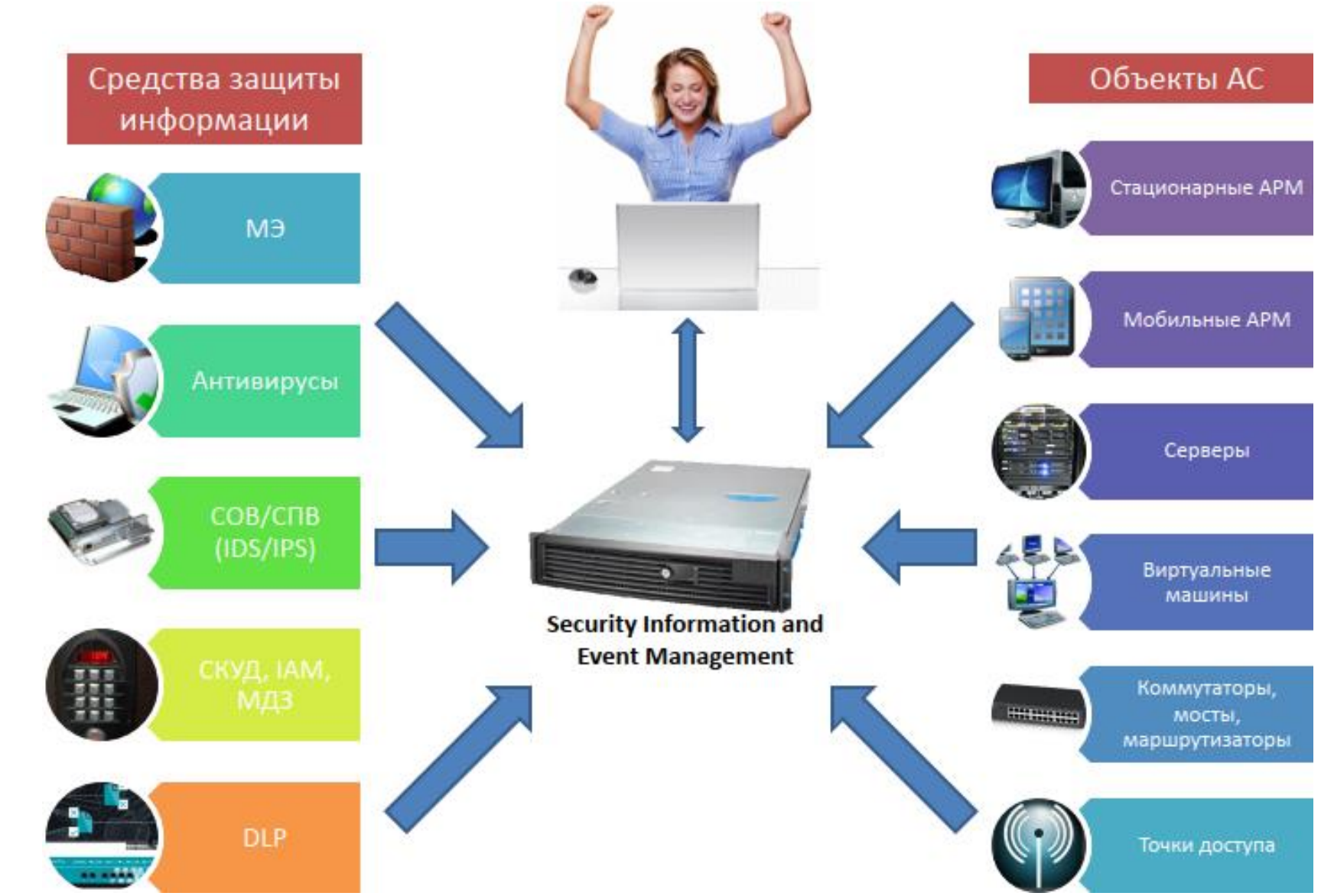
Нет оперативного оповещения о проблемах и угрозах

- Администратор безопасности неделями не заглядывает в журналы работы СЗИ
- Обычно администратор узнаёт о проблеме либо от пользователей, либо уже после инцидента

Решаемые задачи

- ✓ Сбор, обработка и анализ событий безопасности, поступающих в систему из множества источников;
- ✓ Обнаружение в режиме реального времени атак и нарушений критериев и политик безопасности;
- ✓ Оперативная оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов;
- ✓ Анализ и управление рисками безопасности;
- ✓ Проведение расследований инцидентов;
- ✓ Принятие эффективных решений по защите информации;
- ✓ Формирование отчетных документов.

Система управления информацией и событиями в области безопасности



Применение SIEM

ПРИМЕРЫ СОБЫТИЙ

- Сетевые атаки
- Фрод и мошенничество
- Откуда и когда блокировались учетные записи
- Изменение конфигураций «не админами»
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учетной записью уволенного сотрудника)
- Отсутствие антивирусной защиты на новом установленном компьютере
- Изменение критичных конфигураций с VPN подключений
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевых устройств, приложений, ОС)
- Выполнение требований Законодательства и регуляторов (PCI DSS, СТО БР, ISO 27xx)
- Аномальная активность пользователя (массовое удаление/копирование)
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке софта
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределенных по времени атаках
- Влияние отказа в инфраструктуре на бизнес-процессы

Источники данных

- ✓ Access Control, Authentication. Применяются для мониторинга контроля доступа к информационным системам и использования привилегий.
- ✓ DLP-системы. Сведения о попытках инсайдерских утечек, нарушении прав доступа.
- ✓ IDS/IPS-системы. Несут данные о сетевых атаках, изменениях конфигурации и доступа к устройствам.
- ✓ Антивирусные приложения. Генерируют события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном коде.
- ✓ Журналы событий серверов и рабочих станций. Применяются для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности.
- ✓ Межсетевые экраны. Сведения об атаках, вредоносном ПО и прочем.
- ✓ Сетевое активное оборудование. Используется для контроля доступа, учета сетевого трафика.
- ✓ Сканеры уязвимостей. Данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостей, поставка инвентаризационных данных и топологической структуры.
- ✓ Системы инвентаризации и asset-management. Поставляют данные для контроля активов в инфраструктуре и выявления новых.
- ✓ Системы веб-фильтрации. Предоставляют данные о посещении сотрудниками подозрительных или запрещенных веб-сайтов.

Архитектура SIEM

Обычно, SIEM-система разворачивается над защищаемой информационной системой и имеет архитектуру «источники данных» - «хранилище данных» - «сервер приложений». SIEM-решения представляют из себя интегрированные устройства (all-in-one) либо двух-трехкомпонентные комплексы. Распределенная архитектура чаще всего предполагает большую производительность и лучшие возможности по масштабированию, а также позволяет развернуть SIEM-решение в IT-инфраструктурах с несколькими площадками.

Агенты выполняют первоначальную обработку и фильтрацию, а также сбор событий безопасности.

Передача информации от источников данных может осуществляться несколькими способами:

- источник сам инициирует передачу событий (например, отправляет по syslog-протоколу);
- события с источника забираются пассивно.

Собранная и отфильтрованная информация о событиях безопасности поступает в хранилище данных, где она хранится во внутреннем формате представления с целью последующего использования и анализа сервером приложений.

Сервер приложений реализует основные функции защиты информации. Он анализирует информацию, хранимую в репозитории, и преобразует ее для выработки предупреждений или управленческих решений по защите информации.

Исходя из этого, в SIEM-системе выделяются следующие уровни ее построения:

- сбор данных: осуществляется от источников различных типов, например, файловых серверов, межсетевых экранов, антивирусных программ;
- управление данными: данные, хранящиеся в репозитории, выдаются по запросам моделей анализа данных;
- анализ данных: результатом являются отчеты в предопределенной и произвольной форме, оперативная корреляция данных о событиях, а также выдаваемые предупреждения.

Функционирование SIEM

Для решения поставленных задач SIEM-системы первого поколения применяют нормализацию, фильтрацию, классификацию, агрегацию, корреляцию и приоритезацию событий, а также генерацию отчетов и предупреждений. В SIEM-системах нового поколения к их числу следует добавить также анализ событий, инцидентов и их последствий, а также принятие решений и визуализацию.

Нормализация приводит форматы записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки. Фильтрация событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков. Классификация позволяет для атрибутов событий безопасности определить их принадлежность определенным классам. Агрегация объединяет события, схожие по определенным признакам. Корреляция выявляет взаимосвязи между разнородными событиями. Приоритезация определяет значимость и критичность событий безопасности на основании правил, определенных в системе. Анализ событий, инцидентов и их последствий включает процедуры моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов. Генерация отчетов и предупреждений означает формирование, передачу, отображение или печать результатов функционирования. Визуализация предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой системы и ее элементов.

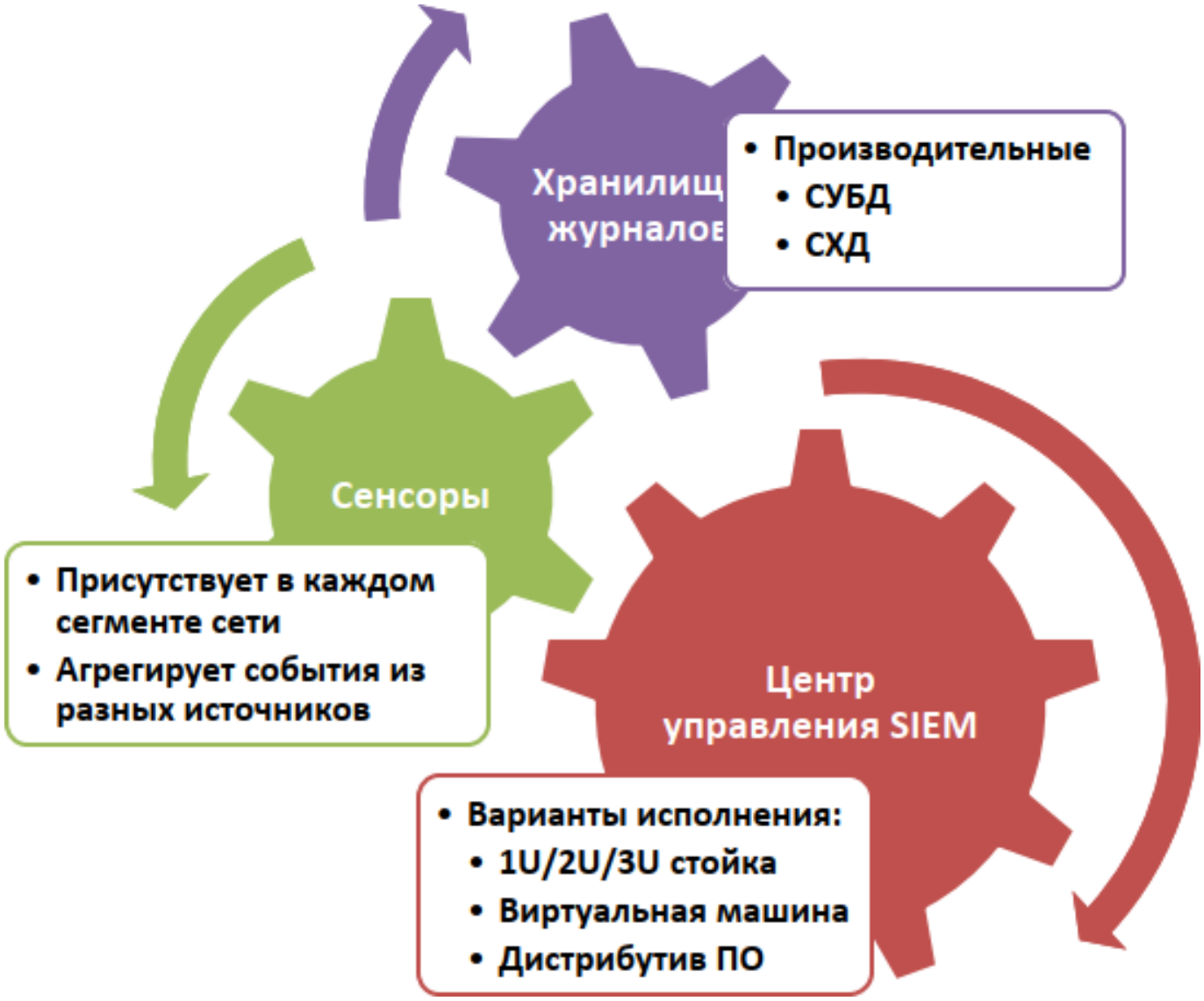
Функциональность SIEM

- **Агрегация данных:** управление журналами данных; данные собираются из различных источников: сетевые устройства и сервисы, датчики систем безопасности, серверы, базы данных, приложения; обеспечивается консолидация данных с целью поиска критических событий.
- **Корреляция:** поиск общих атрибутов, связывание событий в значимые кластеры. Технология обеспечивает применение различных технических приемов для интеграции данных из различных источников для превращения исходных данных в значащую информацию. Корреляция является типичной функцией подмножества Security Event Management.
- **Оповещение:** автоматизированный анализ коррелирующих событий и генерация оповещений (тревог) о текущих проблемах. Оповещение может выводиться на «приборную» панель самого приложения, так и быть направлено в прочие сторонние каналы: e-mail, GSM-шлюз итп.
- **Средства отображения** (информационные панели): отображение диаграмм помогающих идентифицировать паттерны отличные от стандартного поведения.
- **Совместимость (трансформируемость):** применение приложений для автоматизации сбора данных, формированию отчетности для адаптации агрегируемых данных к существующим процессам управления информационной безопасностью и аудита.
- **Хранение данных:** применение долговременного хранилища данных в историческом порядке для корреляции данных по времени и для обеспечения трансформируемости. Долговременное хранение данных критично для проведения компьютерно-технических экспертиз, поскольку расследование сетевого инцидента вряд ли будет проводиться в сам момент нарушения.
- **Экспертный анализ:** возможность поиска по множеству журналов на различных узлах; может выполняться в рамках программно-технической экспертизы.

Функциональность SIEM

- Сбор и объединение данных
- Централизованное хранение журналов
- Интеллектуальный анализ данных (Корреляция событий)
- Оповещение об инцидентах
- Оценка соответствия АС требованиям стандартов и регламентов

Компоненты SIEM-систем



Отличие SIEM от «традиционных» средств защиты информации

Антивирус:

на компьютере С запущен вредоносный код отдельным процессом X, похожий на известный тип червя

Система обнаружения вторжений:

обнаружена атака типа NETBIOS DCERPC LSASS
на узел Y

SIEM-система:

в АС обнаружена активность червя «Sasser Worm», были зафиксированы атаки на узлы A,B,C, на узле С червь смог получить системные привилегии и там продолжил своё распространение. Рекомендуем обновить старое ПО на узлах D и E, выключить узел С и временно отключить сегмент сети Z от общей АС ВН до выяснения обстоятельств инцидента.

Отличие SIEM от «традиционных» средств защиты информации

Антивирус:

на компьютере С запущен вредоносный код отдельным процессом X, похожий на известный тип червя

Система обнаружения вторжений:

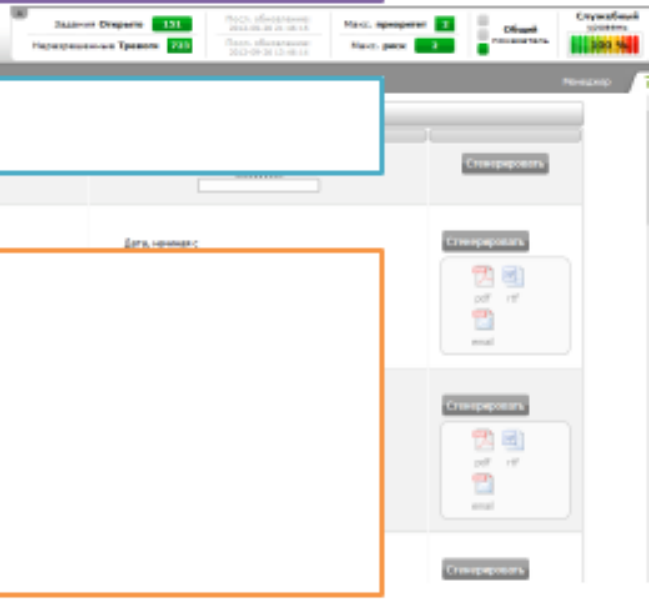
обнаружена атака типа NETBIOS DCERPC LSASS на узел Y

SIEM-система:

в АС обнаружена активность червя «Sasser Worm», были зафиксированы атаки на узлы A,B,C, на узле С червь смог получить системные привилегии и там продолжил своё распространение. Рекомендуем обновить старое ПО на узлах D и E, выключить узел С и временно отключить сегмент сети Z от общей АС ВН до выяснения обстоятельств инцидента.

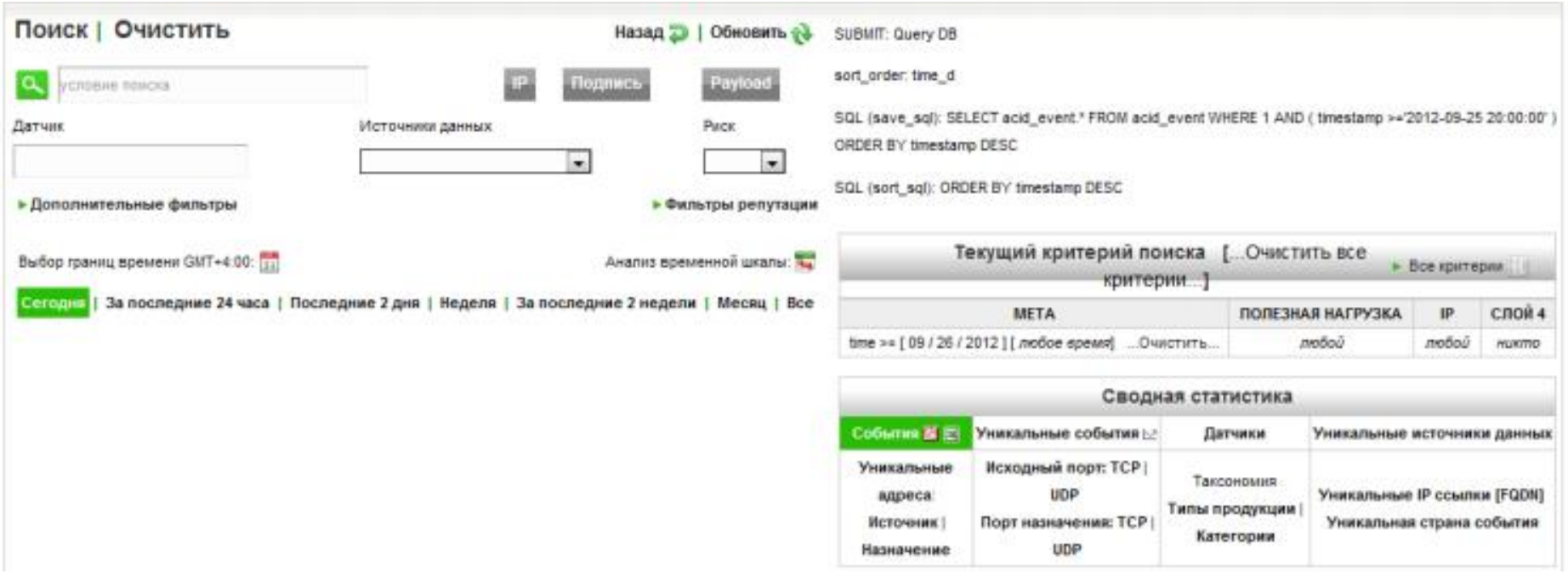
Построение отчетов с выборочной детализацией

- События, тревоги
- Инциденты и связанные с ними точки контроля
- Заключения из данных
- Уязвимости АС
- Ресурсы АС
  - Инфраструктура
  - Сеть
    - Доступность
    - Использование ресурсов



Анализ рисков

Поисковые возможности



Автоматический анализ

Обзор современных систем

Tivoli Security Information and Event Manager (TSIEM) позволяет, с одной стороны, проводить аудит событий безопасности на соответствие внутренним политикам и различным международным стандартам, а с другой стороны - осуществлять обработку инцидентов, связанных с информационной безопасностью, и обнаруживать атаки и другие угрозы для элементов инфраструктуры. В области представления и хранения событий TSIEM использует запатентованную методику W7 (Who, did What, When, Where, Wherefrom, Where to and on What), в соответствии с которой все события трансформируются в единый формат, понятный администраторам безопасности, аудиторам и управленцам. Также TSIEM обладает развитыми возможностями по формированию отчетов и мониторингу активности пользователей.

Splunk - решение для ведения коммерческих журналов событий, которое позиционируется как решение «Поиск в ИТ» и встраивается в такие продукты, как Cisco System IronPort. Благодаря веб-интерфейсу Splunk интуитивно понятен в настройке и управлении. Splunk использует достаточно удобный для пользователя подход к проектированию интерфейсов, упрощая первоначальный опыт для менее опытного администратора. Как и у многих аналогичных продуктов для ведения журналов, возможность создания отчетов является частью базового продукта и, в случае Splunk, она относительно проста в использовании. Распространенные типы форматов представления данных доступны из раскрывающихся меню на экране. Одна из приятных сторон веб-интерфейса Splunk заключается в том, что любой отчет может быть предоставлен в виде URL-адреса, что позволяет другим людям в организации просматривать конкретные отчеты, которые системный администратор создает для них.

Обзор современных систем

LogRhythm, Inc. - американская компания, занимающаяся вопросами безопасности, которая объединяет систему управления информацией и событиями безопасности (SIEM), управление журналами, мониторинг сети и конечных точек, а также аналитику и безопасность. LogRhythm утверждает, что помогает клиентам быстро обнаруживать и реагировать на киберугрозы, прежде чем будет нанесен существенный ущерб. Он также нацелен на обеспечение автоматизации и соответствия нормативным требованиям. Продукты LogRhythm призваны помочь организациям защитить свои сети и оптимизировать работу. Кроме того, они помогают автоматизировать сбор, организацию, анализ, архивирование и восстановление данных журналов, что позволяет компаниям соблюдать правила хранения данных журналов. Компоненты продукта включают в себя сбор данных, мониторинг системы и сети, аналитические модули, управление журналами и событиями.

KOMRAD Enterprise SIEM - способна осуществлять единый контроль событий информационной безопасности, выявлять возникающие инциденты информационной безопасности, оперативно реагировать на появляющиеся угрозы, отвечать требованиям предъявляемым к защите личной информации, способен обеспечивать сохранность государственных информационных систем. Преимуществами использования данной системы можно считать: поддержку большого количества платформ, своевременное информирование и реагирование на различные виды угроз, возможность гибкой настройки, удалённое управление конфигурациями, сбор информации с нестандартных источников событий.

Обзор современных систем

Security Capsule - система контроля за информационной безопасностью. Обладает следующими качествами: выявление сетевых атак как в локальных, так и в глобальных периметрах, обнаружение вирусных заражений, способность регистрировать события в используемой операционной системе, учёт действий лиц, взаимодействующих с системой управления базой данных.

MaxPatrol SIEM - система, имеющая объективную оценку уровня защищённости как отдельно взятых подразделений, узлов и приложений, так и всей системы в целом. Система характеризуется использованием эвристических механизмов анализа и сформированной базой знаний, способной осуществлять проверку большинства распространённых операционных систем и специализированной аппаратуры. В отличие от классических SIEM-систем, она не нуждается в установке программных компонентов на узлах, что существенно облегчает процесс использования и снижает конечную стоимость владения. Обладает легко настраиваемой системой и разграничением прав доступа, что даёт возможность формировать мониторинг ИБ на каждом из уровней иерархии. Для отдельно взятого пользователя MaxPatrol, присутствует возможность создать свой список задач, которые он способен выполнить внутри системы.

RUSIEM - система позволяющая интерпретирование событий в понятный вид, тегирование и весовые показатели, что даёт более удобный и быстрый способ анализировать поступающую информацию. Безлимитное количество источников информации вкупе с компактным хранилищем даёт возможность строить оптимизированные запросы на любой глубине хранилища.