SIC enter
System
Integrations
Center

Мониторинг и управление системами защиты информации. Расследование информационных инцидентов

Александр Леуш
SICenter

Особенности современной системы мониторинга и управления системами защиты информации

- Развитая, территориально и регионально рассредоточенная инфраструктура;
- Использование в рамках одной инфраструктуры элементов различных производителей;
- Высокая нагрузка на инфраструктуру;
- Большое количество консолей управления;
- Необходима высокая квалификация и ответственность персонала.

Задачи мониторинга и управления системами защиты информации

Глобальным результатом работы системы мониторинга и управления системами защиты информации является фиксация факта наличия или отсутствия **инцидента информационной безопасности*** в них и его локализация.

***Инцидентом информационной безопасности** называется любое незаконное, неразрешенное (в том числе политикой ИБ) или неприемлемое действие, которое совершается в информационной системе.

При наличии факта инцидента запускаются локализующие его действия, после чего выясняются причины его возникновения – проводится **расследование информационных инцидентов**, чтобы в последствии предпринять те или иные действия (корректирующие или предупреждающие действия в формулировках стандарта ISO27000:2005).

Расследование информационных инцидентов

В ходе расследования информационных инцидентов определяются:

- конкретные уязвимости информационной системы;
- обнаруживаются следы атак и вторжений;
- персонал, ответственный за возникновение инцидента
- проверяется работа защитных механизмов;
- качество архитектуры системы информационной безопасности и ее управления

Расследование информационных инцидентов

Цель расследования информационных инцидентов:

- предупредить нескоординированные действия и в кратчайшие сроки восстановить работоспособность компании при возникновении инцидента;
- подтвердить или опровергнуть факт инцидента ИБ;
- представить детализированный отчет о произошедшем инциденте и полезные рекомендации. Создать условия для накопления и хранения точной информации о компьютерных инцидентах. Обеспечить быстрое обнаружение и/или предупреждение подобных инцидентов в будущем (путем анализа "прошедших уроков", изменения политики ИБ, модернизации системы ИБ и др.);
- обеспечить сохранность и целостность доказательств произошедшего инцидента. Создать условия для возбуждения гражданского или уголовного дела против злоумышленника(-ов). Защитить частные права, установленные законом;
- минимизировать нарушение порядка работы и повреждения данных ИТ-системы. Минимизировать последствия нарушения конфиденциальности, целостности и доступности ИТ-системы;
- защитить репутацию компании и ее ресурсы;
- провести обучение сотрудников компании о процессе реагирования на инцидент.

Расследование информационных инцидентов

Проблемы обусловленные характеристиками системы мониторинга и управления системами защиты информации

- нет единого центра регистрации инцидентов;
- отстает законодательство;
- нет открытых методик и стандартов организации процесса реагирования и расследования инцидентов ИБ;
- трудности при поиске специалистов, которые могли бы провести работы по расследованию компьютерных инцидентов или выстраиванию в компании процесса реагирования на инциденты;
- о возникновении инцидентов в системе информационной безопасности компании стараются не заявлять открыто.

Решение некоторых проблем может быть достигнуто использованием **Encase Enterprise**

Основные задачи решаемые при помощи Encase Enterprise

- **Аудит собственного информационного пространства,** выявление происшествий и устранение последствий
- **Поиск информации любого типа** на рабочих местах сотрудников внутри организации
- **Анализ инцидентов и проведение расследований**
- **Мониторинг отдельных или группы машин** на предмет важной конфиденциальной информации, несанкционированных процессов и подключений к сети
- **Нахождение информации** несмотря на все усилия спрятать, замаскировать или удалить ее
- Эффективный и результативный **поиск доказательств** с помощью автоматизированных операций анализа, сбора и хранения данных.
- Использование единого инструмента для **расследования и анализа компьютеров с системами Windows, Linux и Solaris**
- При необходимости, **обмен найденными доказательствами с представителями правоохранительных органов и закона**

Аудит собственного информационного пространства

- анализ файлов протоколов работы;
- конфигурационных файлов;
- истории Интернет-проводников (включая cookies);
- сообщений электронной почты и прикрепленных файлов;
- инсталлированных приложений;
- графических файлов и прочего.
- провести анализ ПО;
- поиск по ключевым словам;
- проверить дату и время инцидента;
- поиск удаленных файлов и областей;
- потерянных кластеров;
- свободного места;
- анализ восстановленных данных с разрушенных носителей.

Поиск информации

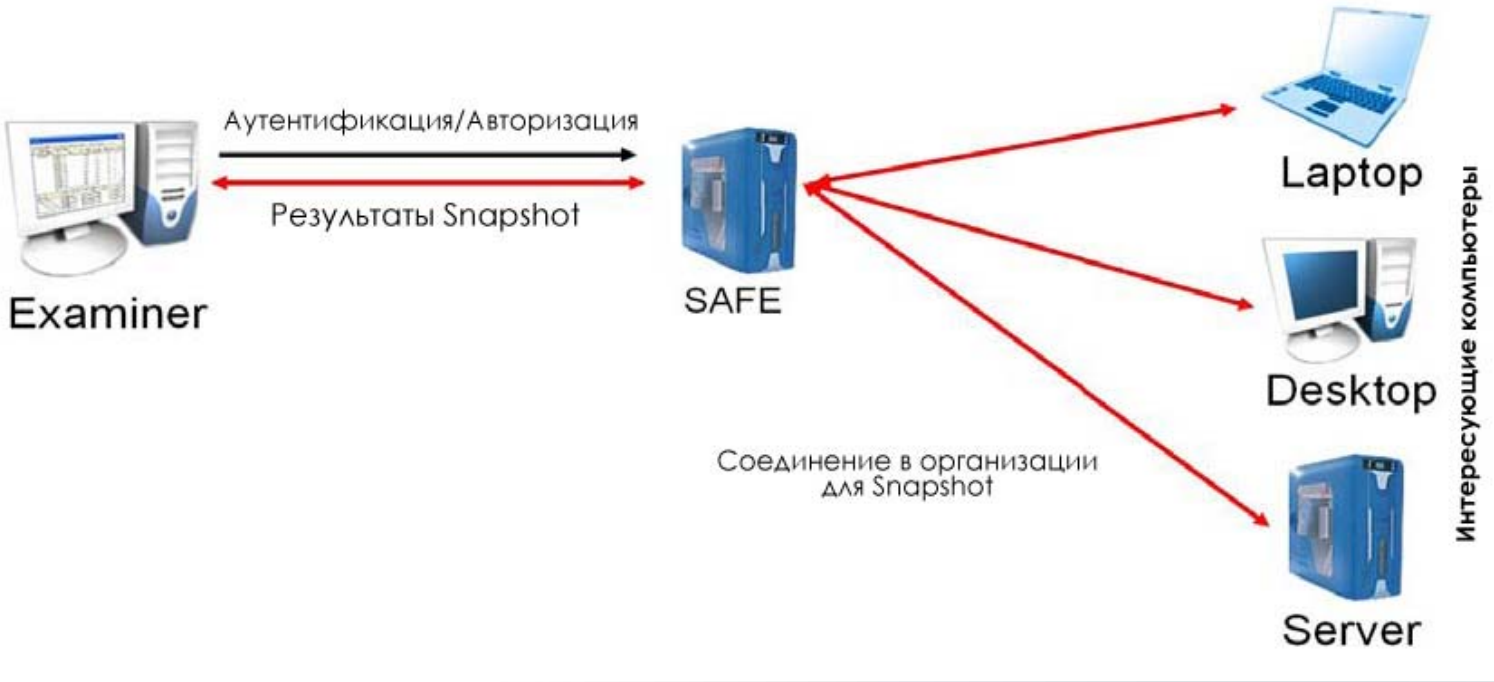
- Одновременный поиск
- Поиск с контекстом
- Поиск в Internet и электронной почте
- Поиск адресов электронной почты
- GREP поиск (Global Regular Expressions Post)
- Поиск и распознавание информации в логических файлах
- Поиск на нескольких накопителях
- Результаты поиска могут быть рассортированы по случаям, ключевым слова, типам устройств или любой комбинации этих показателей
- Тестер ключевых слов

Анализ инцидентов

- Незамедлительный анализ происшествий и получение энергозависимых (временных) данных
- Автоматизированный процесс получения временных (энергозависимых) данных с помощью Snapshot
- Анализ открытых портов
- Анализ активных процессов, включающие перечисление функций и драйверов
- Инвентаризация и анализ открытых файлов
- Автоматическое извлечение информации из системного реестр а Windows в режиме реального времени
- Создание отчетов о пользователях сети и сетевых интерфейсах

Компоненты EnCase Enterprise

- SAFE (Secure Authentication For EnCase – сервер данных и авторизации)
- The EnCase Examiner (Экзаменатор EnCase)
- Servlet (Сервлет – клиентский агент)



Модули EnCase Enterprise

- EnCase eDiscovery
- EnCase Data Audit & Policy Enforcement
- EnCase Bit9 Analyzer
- EnCase® Enterprise Automated Incident Response Suite (AIRS)

Использование EnCase eDiscovery

Оценка происшествия на ранней стадии и выработка стратегии	Получение и хранение: Начальная фильтрация	Обработка: Последующая фильтрация	Обработка: Создание файла улик	Предоставление доказательств
Планирование и Идентификация •Создание модели угроз и политик безопасности •Разработка и введение в эксплуатацию мест хранения найденных доказательств •Разработка и проверка критериев поиска	***Автоматизированный сбор данных по всей сети*** •Портативные компьютеры •Настольные компьютеры •Серверы •Совместно используемые ресурсы •Электронная почта	***Хранение доказательств отвечающих требованиям суда*** •Без прерывания работы •Данные, хранятся в зашифрованных файлах улик •Имеют формат данных используемый правоохранительными органами	***Вторичная фильтрация и устранение дубликатов для последующего уменьшения объема ESI*** •Классификация и сортировка данных •Права доступа •Коммерческая тайна •Конфиденциальность	***Создание файла улик*** •Загрузочный файл XML •Подведение итогов •Унифицированная форма предоставления данных	***Просмотр Адвокатом*** •Права доступа •Релевантность •Конфиденциальность •Шифрование •Редактирование •Присвоение документам во время сканирования или обработки номеров и/или временных меток, дат
EnCase eDiscovery					Платформа просмотра адвоката

EnCase Data Audit & Policy Enforcement

Средство проверки данных и выполнения политики корпорации

- Максимально снижает издержки, связанные с возникновением риска — масштабируемая, целенаправленная технология поиска, способная находить и удалять конфиденциальную информацию с конечного узла без нарушения рабочего процесса
- Один для всех продуктов EnCase скрытый агент, осуществляющий запуск процесса передачи данных (DPL) из мест их хранения
- Создание детализированных отчетов проведения проверок — результаты включают суммарную метрику и точные физические и логические координаты уязвимых данных
- Оптимизированная, распределенная технология поиска данных, позволяющая осуществлять поиск с центрального пункта

EnCase Bit9 Analyzer

Средство идентификации двоичных кодов приложений

- Классифицирует бинарный код независимо от местоположения в сети
- Уменьшает время, затрачиваемое на расследование или проверку
- Уменьшает затраты и повышает эффективность любой операции в ходе расследования
- Распознает опасность, угрожающую безопасности информации и операционным системам организации
- Уменьшает число анализируемых ресурсов посредством использования постоянно обновляемых системных профилей

EnCase® Enterprise Automated Incident Response Suite (AIRS)

Пакет программ автоматического реагирования на события

Поддержка систем IDS/SIM/CMS:

- Intrusion Detection Systems ISS Site Protector, Snort
- Content Monitoring Systems Vericept, Vontu
- Security Information Management Arcsight

Multiple Database Support: SQL Servers 2000/2005, My SQL, Oracle and PostGreSQL.

Спасибо за внимание!

Александр Леуш
Aleksandr.Leush@sicenter.net

ООО «Центр Системных Интеграций»
Горизон Парк Бизнес Центр
ул. Николая Гринченко, 4
03038, Киев, Украина

тел.: +380 44 393-15-60
e-mail: info@sicenter.net
http://sicenter.net