SAFEINSPECT

Средство контроля за действиями привилегированных пользователей!

Зачем нужен SAFEINSPECT?

Он необходим, если Вы хотите:

Контролировать подрядчиков, обслуживающих конечное оборудование

Выявлять нанесение вреда ресурсам компании системными администраторами

Иметь доказательства факта компрометации целевого сервера

Быстро реагировать на инциденты

Минимизировать затраты за счет применения масштабируемого виртуального устройства

Анализировать поведение злоумышленника

Архитектура:

- Законченное решение, поставляется в виде .iso или .ovf (виртуальный appliance)
- Основа – FreeBSD
- Одна машина может иметь две роли – Менеджер либо Коллектор
- Менеджер – хранилище и единая консоль для администрирования, управления политиками,

просмотра подключений

- Коллектор – инспектирует и аудирует подключения администраторов к конечным серверам
- Три режима работы коллектора:
  1. Маршрутизатор (L3)
  2. Сетевой мост/бридж (L2/поддерживает VLAN)
  3. Бастион (user@host)
- Не требует установки агентов
- Не требует специальных клиентов – используется стандартное ПО для подключений

Основные возможности:

Запись и воспроизведение сессий:

- SSH (*nix)
- RDP (Windows)
- HTTP(s)
- Telnet,TN3270 и т.д.

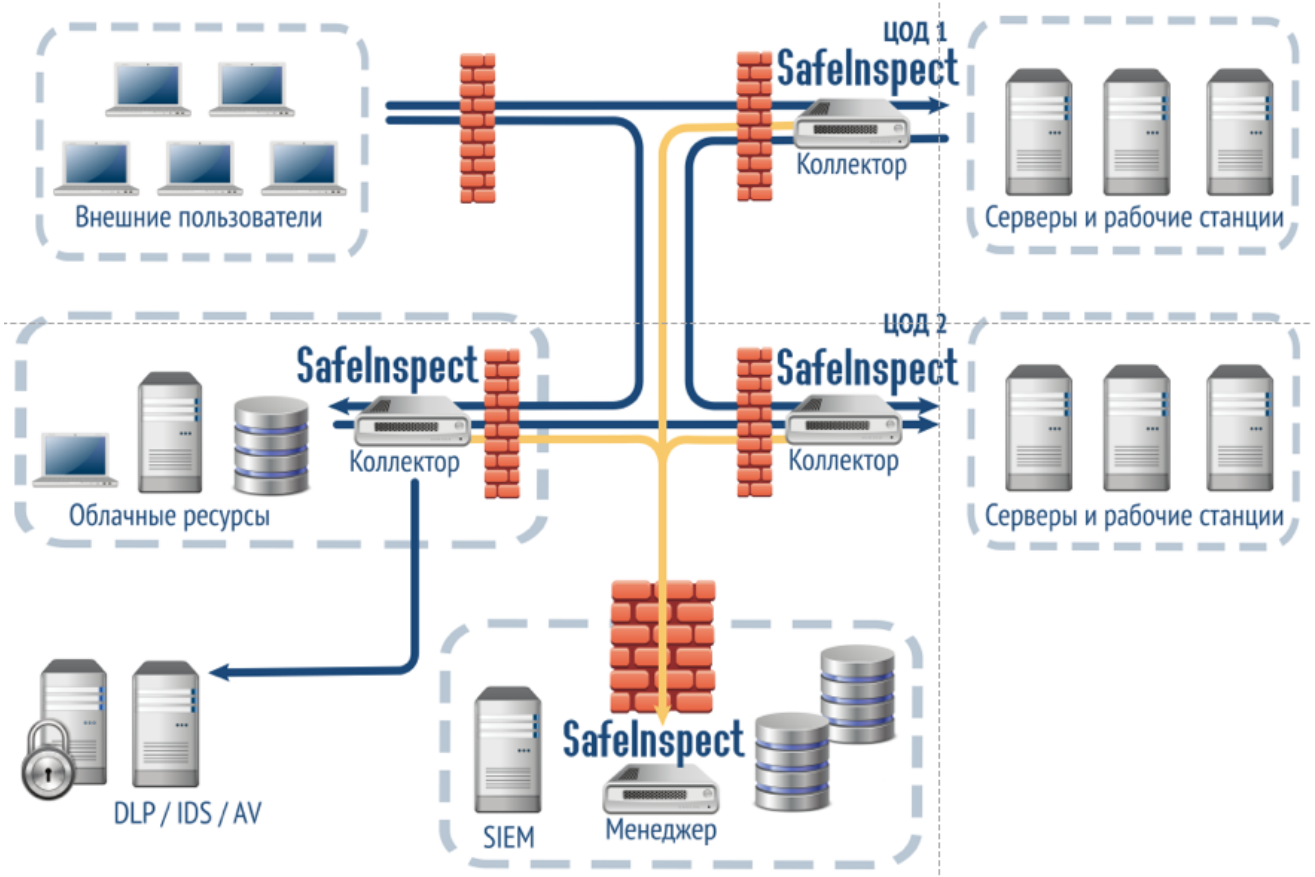
Определение и аудит подканалов:

- SCP,SFTP, X11 и др. (SSH)
- Буфер обмена, подключаемые устройства (RDP)

Индексация содержимого, поиск по ключевым словам

Оптическое распознавание символов в RDP (OCR)

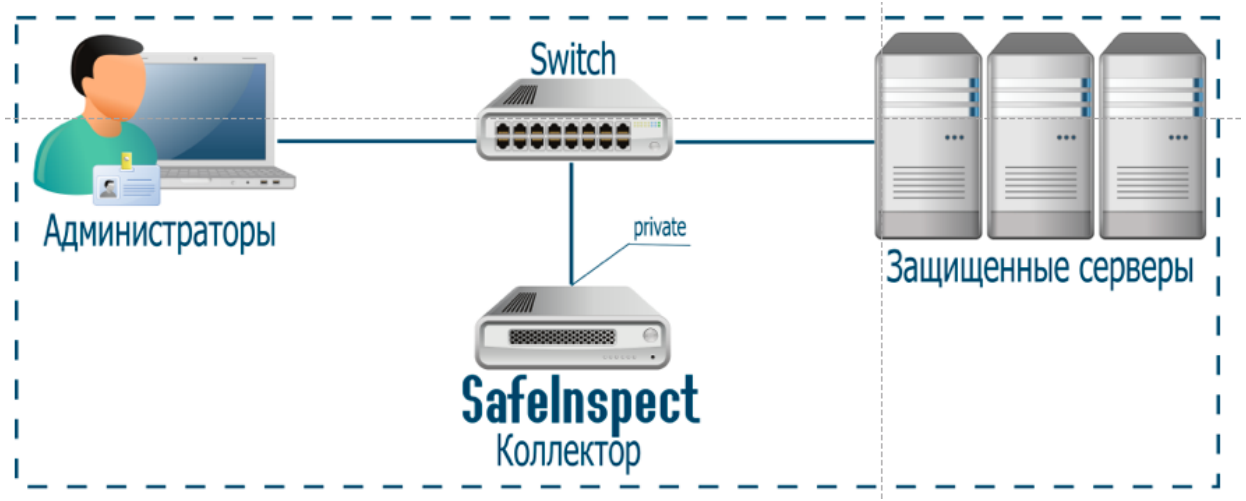
Общая схема:


ЦОД 1
SafeInspect
Коллектор
Внешние пользователи
Серверы и рабочие станции
ЦОД 2
SafeInspect
Коллектор
SafeInspect
Коллектор
Облачные ресурсы
Серверы и рабочие станции
DLP / IDS / AV
SIEM
SafeInspect
Менеджер

Режим L-2 мост:

Режим L-3 маршрутизатор:

РЕЖИМ БАСТИОН



Технические требования

Размер сохраняемых подключений:

SSH:

- 1 Мб/ч (без индекса),
  3 Мб/ч (с индексом)

RDP (для разрешения 1024x768):

- Типичное административное использование: 30 Мб/ч
- С интенсивным использованием графики: 300 Мб/ч

Требования для Менеджера:

- 8 Гб ОЗУ
- 500 Гб диск

Требования для Коллектора:

- 4 Гб ОЗУ
- 50 Гб диск

Производительность Коллектора:

- 6000 SSH подключений
- 600 RDP

(1 Менеджер ~ 12 Коллекторов)

Кейсы

Неосторожные действия со стороны поставщиков ИТ услуг

Проблема:

- Сложность контроля действий на целевых ресурсах
- Возможность скрыть совершённые ошибки
- Совершённые ошибки могут быть обнаружены не сразу

Решение:

- SafeInspect ведёт запись всех действий привилегированных пользователей на целевых ресурсах
- Просмотр сессий доступен из обычного браузера

Злонамеренные действия со стороны поставщиков ИТ услуг

Проблема:

- Отсутствие информации о действиях поставщиков ИТ услуг на целевых ресурсах компании
- Логи межсетевых экранов показывают только факт подключения, но не показывают кто подключался и что делал.

Решение:

- SafeInspect ведёт запись всех действий, включая введённые команды, переданные файлы, просмотренные ресурсы и т.д.
- Просмотр активности может быть доступен в реальном времени или в записи
- Офицер безопасности может прервать сессию в случае совершения несанкционированных или ошибочных действий

Использование учётной записи суперпользователя несколькими лицами

Проблема:

- Невозможность определить администратора, совершившего действия из-под учётной записи суперпользователя
- Сложность в управлении доступом к удалённым ресурсам
- Возможность намеренно или случайно заблокировать доступ к учётной записи суперпользователя для всех лиц.

Решение:

- SafeInspect позволяет назначать соответствие пользователя для каждой административной учётной записи
- Во время записи сессии, отображается логин подключившегося администратора
- Можно сгенерировать отчёт по деятельности конкретного пользователя

Утечка информации

Проблема:

- Администраторы могут скачивать данные (в том числе и в рамках легитимных процессов), и прятать следы своей противоправной деятельности

Решение:

- SafeInspect ведёт запись всех действий привилегированных пользователей на целевых ресурсах
- Все записи содержат временные метки и могут быть соотнесены с деятельностью администраторов

Неэффективные действия аутсорсеров

Проблема:

- Дорогие, но неэффективные действия аутсорсеров
- Сложность в определении времени, потраченного на те или иные действия

Решение:

- SafeInspect позволяет пошагово просмотреть действия администраторов, произвести поиск по вводимым командам и увидеть результаты их применения
- Временные метки в записях сессий позволяют подсчитать потраченное время и минимизировать расходы на аутсорс

Документирование деятельности, подготовка учебных материалов

Проблема:

- Написание отчётов по настройке требует большого количества времени и ресурсов
- Сложность восприятия отчётов по настройке в печатном формате по сравнению с видеозаписью.

Решение:

- Записанные сессии могут быть использованы в качестве документации к внедрённым системам
- Обучение новых сотрудников посредством трансляции и разбора видеозаписи настройки целевых ресурсов происходит более наглядно, чем просмотр распечаток.

Спасибо за внимание!

Контакты:
ООО «Новые технологии безопасности»
Москва, ул. Трубная, 12
Телефон/Факс: +7 (495) 787 99 36
www.newinfosec.ru

АО ДиалогНаука
Москва, ул. Нагатинская 1
+7(495) 980-67-76
info@dialognauka.ru
www.dialognauka.ru