Контур staffcop

Единый источник истины

Платформа расследований как ключевой инструмент управления рисками во всей компании

Даниил Арчибасов

Специалист отдела внедрения
ООО «АТОМ БЕЗОПАСНОСТЬ»

Кто такие инсайдеры

Инсайдеры — это сотрудники, подрядчики или партнёры, которые имеют доступ к конфиденциальной информации компании.

- Случайные утечки
- Преднамеренные действия

Почему инсайдеры опасны

- Имеют доступ к критическим данным.
- Сложнее обнаружить, чем внешних хакеров.
- Используют доверие внутри компании для обхода защитных мер.

Немного статистики

52%

В 2024 году промышленных компаний столкнулись с утечками.

~ 60%

В гос. секторе инцидентов связаны с инсайдерами.

~ 80%

В частных компаниях

И еще немного статистики

30%

Утечки технической информации

15%

Финансовая документация

35%

Данные о клиентах и сделках

20%

Персональные данные

Методы и инструменты

Контур.Эгида

- Безопасность корпоративных учетных записей сотрудников
- Контроль привилегированных пользователей
- Безопасное удаленное подключение и управление конечными устройствами
- Аудит и организация комплексных мер защиты ИБ
- Симуляции атак и обучающий портал для сотрудников

Staffcop

- Расследование инцидентов
- Контроль и анализ действий персонала
- Учет рабочего времени
- Выявление утечек и мошеннических действий
- Предотвращение неправомерных действий

Решаемые задачи

Информационная безопасность

- Раннее обнаружение угроз ИБ
- Расследование инцидентов
- Анализ поведения пользователей

Эффективность работы персонала

- Оценка продуктивности
- Мониторинг бизнес-процессов
- Учет рабочего времени

Администрирование рабочих мест

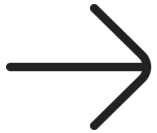
- Удаленное администрирование
- Инвентаризация компьютеров
- Индексирование файлов на ПК

Для кого?

- Собственники бизнеса
- IT специалисты
- ИБ специалисты
- Сотрудники HR

Примеры внутренних инцидентов:

- Фиктивные списания оборудования
- Проекты на стороне
- Утечка персональных данных клиентов
- Утечка коммерческой информации
- Слив клиентской базы
- Слив активных заявок от клиентов
- Вторая работа у сотрудника
- Нарушение трудовой дисциплины



- Репутационные риски
- Штрафы
- Недополученная прибыль компании

Разговоры о важном

Проблема:
Ваши коллеги и подчиненные получают письма от «руководителей» компании

Инцидент:
Риски слить как ценные данные компании, так и подверженность сотрудников финансовым потерям

Функционал Staffcop для расследования:
- Перехват-мессенджеров
- Снимки экрана или пакетные снимки экрана

Итог:

- Перехвачены сообщения от «руководителей»
- Рассылка офицерам безопасности уведомлений об инциденте
- Служба безопасности проанализировала чьи данные есть у мошенников
- Проведены профилактические мероприятия

Утечка конструкторской документации

Проблема:
Слив корпоративных чертежей

Подозреваемый: Сотрудник конструкторского отдела

Инцидент:
Сотрудник отправлял в текстовых документах чертежи, надеясь, что служба безопасности не заметит

Функционал Staffcop для расследования:

- Операции с файлами
- Перехваченный файл
- OCR сервер и политика распознавания
- Созданный словарь

Итог:

- Зафиксировали, что чертежи копируются в документы
- Активировали создание теневых копий файлов
- Создали словарь, наполненный терминами из спецификаций и легенд
- Обнаружили кто ответственен за утечку, сотрудник уволен

Параллельный бизнес

Проблема:
Резко понизилась продуктивность опытного сотрудника

Инцидент:
Подключался к удаленному компьютеру у себя дома. Параллельно занимался делами своего бизнеса

Функционал Staffcop для расследования:

- Время активности
- Снимки экрана

Итог:

- Увидели постоянную активность программы для подключения к удаленному компьютеру
- Проанализировали скриншоты
- Сотрудник переведен на полставки

Работа на конкурента

Проблема:
Дизайнерская студия заметила, что снизилась конверсия между приходом заявки и дальнейшим заказом

Инцидент:
Кто-то из сотрудников «сливает» заявки конкурентам. Большой финансовый ущерб

Функционал Staffcop для расследования:

- Файловая активность
- Интернет пейджер
- Перехваченный файл
- Краулер
- Посещение сайтов
- Снимки экрана

Итог:

- Пометили файл специальной меткой
- Отследили, кто открывал и куда отправлял
- Выявили сотрудника, который передавал данные конкурентам

Staffcop в цифрах

13 лет

Экспертизы в информационной безопасности

3 000

Клиентов в 40 странах мира

>250 тыс

ПК под защитой Staffcop

25

Клиентов из ТОП-100 РБК

Возможности

Расследования

— инцидентов внутренней информационной безопасности
— причин неэффективной работы

Выявление

— коррупционных схем и мошенничества внутри компании
— нелояльных сотрудников, работающих на конкурентов

Уведомления

— на почту или в Telegram по инцидентам, которые вас интересуют

Блокировка

— копирования на съемные носители
— пересылки конфиденциальной информации
— доступа к нерегламентированным ресурсам

Контур staffcop

Спасибо за внимание!

staffcop.ru